

CISCO
CCNA EXPLORATION 4.0
Aspectos Básico de Interworking

0- INTRODUCCION AL CURSO

0.0.1 Introduccion

Bienvenido

Bienvenido al curso Aspectos básicos de networking de CCNA Exploration. El objetivo de este curso es presentar los conceptos y tecnologías básicos de networking. Este material en línea del curso lo ayudará a desarrollar las aptitudes necesarias para planear e implementar pequeñas redes en una gama de aplicaciones. Las aptitudes específicas que se abarcan en cada capítulo se describen al inicio del mismo.

Más que sólo información

Este ambiente de aprendizaje asistido por PC es una parte importante de la experiencia total del curso para estudiantes e instructores de la Academia de Networking. Este material en línea del curso está diseñado para utilizarse junto con muchas otras herramientas y actividades instructivas. Por ejemplo:

- presentaciones en clase, debates y práctica con su instructor,
- prácticas de laboratorio que usan equipos de redes dentro del aula de la Academia de Networking,
- evaluaciones en línea y un libro de calificaciones para cotejar,
- la herramienta de simulación Packet Tracer 4.1, o
- software adicional para actividades en clase.

Una comunidad global

Cuando participa en la Academia de Networking, se suma a una comunidad global conectada por tecnologías y objetivos en común. El programa cuenta con la participación de escuelas, instituciones, universidades y otras entidades de más de 160 países. Para ver la comunidad de la Academia de Networking global visite <http://www.academynetspace.com>.

El material de este curso incluye una amplia gama de tecnologías que facilitan la forma de trabajar, vivir, jugar y aprender de las personas, comunicándose mediante voz, vídeo y otros datos. La red e Internet afectan a las personas de distintas maneras en las distintas partes del mundo. Si bien hemos trabajado con instructores de todo el mundo para crear este material, es importante que trabaje con su instructor y compañeros para que el material de este curso se aplique a su situación local.

Manténgase comunicado

Este material de instrucción en línea, como el resto de las herramientas del curso, son parte de algo más grande: la Academia de Networking. Podrá encontrar el portal del administrador, instructor y estudiante del programa en <http://www.cisco.com/web/learning/netacad/index.html>. Allí tendrá acceso a las demás herramientas del programa como el servidor de evaluación y la libreta de calificaciones del estudiante, al igual que a actualizaciones informativas y otros enlaces relevantes.

Mind Wide Open™

Un objetivo importante en la educación es enriquecer al estudiante (a usted), ampliando lo que sabe y puede hacer. Sin embargo, es importante comprender que el material de instrucción y el instructor sólo pueden facilitarle el proceso. Usted debe comprometerse a aprender nuevas aptitudes. A continuación encontrará algunas sugerencias que lo ayudarán a aprender y crecer.

1. Tome notas. Los profesionales del campo de networking generalmente tienen diarios de ingeniería en donde anotan las cosas que observan y aprenden. La toma de notas es importante como ayuda para mejorar su comprensión con el pasar del tiempo.

2. Reflexione. El curso proporciona información que le permitirá cambiar lo que sabe y lo que puede hacer. A medida que vaya avanzando en el curso, pregúntese qué cosas tienen sentido y cuáles no. Haga preguntas cuando algo resulte confuso. Intente averiguar más sobre los temas que le interesan. Si no está seguro por qué se enseña algo, pregúntele a su instructor o a un amigo. Piense cómo se complementan las distintas partes del curso.

3. Practique. Aprender nuevas aptitudes requiere de práctica. Creemos que practicar es tan importante para el e-learning que le dimos un nombre especial. Lo llamamos e-Doing. Es muy importante que realice las actividades del material de instrucción en línea y que también realice las actividades del Packet Tracer y las prácticas de laboratorio.

4. Practique nuevamente. ¿Alguna vez pensó que sabía cómo hacer algo y luego, cuando llegó el momento de demostrarlo en una prueba o en el trabajo, descubrió que en realidad no había aprendido bien cómo hacerlo? Como cuando se aprende cualquier nueva habilidad, como un deporte, un juego o un idioma, aprender una aptitud profesional requiere paciencia y mucha práctica antes de que pueda decir que realmente la ha aprendido. El material de instrucción en línea de este curso le brinda oportunidades para practicar mucho distintas aptitudes. Aprovéchelas al máximo. También puede trabajar con su instructor para ampliar el Packet Tracer y otras herramientas para práctica adicional según sea necesario.

5. Enseñe. Generalmente, enseñarle a un amigo o colega es una buena forma de reforzar su propio aprendizaje. Para enseñar bien, deberá completar los detalles que puede haber pasado por alto en la primera lectura. Las conversaciones sobre el material del curso con compañeros, colegas y el instructor pueden ayudarlo a fijar los conocimientos de los conceptos de networking.

6. Realice cambios a medida que avanza. El curso está diseñado para proporcionar comentarios mediante actividades y cuestionarios interactivos, el sistema de evaluación en línea y a través de interacciones estructuradas con su instructor. Puede utilizar estos comentarios para entender mejor cuáles son sus fortalezas y debilidades. Si existe un área en la que tiene problemas, concéntrese en estudiar o practicar más esa área. Solicite comentarios adicionales a su instructor y a otros estudiantes.

Explore el mundo de networking

Esta versión del curso incluye una herramienta especial llamada Packet Tracer 4.1. El Packet Tracer es una herramienta de aprendizaje de networking que admite una amplia gama de simulaciones físicas y lógicas. También ofrece herramientas de visualización para ayudar a entender los componentes internos de una red.

Las actividades preelaboradas del Packet Tracer consisten en simulaciones de red, juegos, actividades y desafíos que brindan una amplia gama de experiencias de aprendizaje.

Cree sus propios mundos

También puede usar el Packet Tracer para crear sus propios experimentos y situaciones de red. Esperamos que, con el tiempo, utilice Packet Tracer no sólo para realizar las actividades desarrolladas previamente, sino también para convertirse en autor, explorador e investigador.

Los materiales del curso en línea incluyen actividades para Packet Tracer que se ejecutan en computadoras con sistemas operativos Windows® si Packet Tracer está instalado. Esta integración también puede funcionar en otros sistemas operativos que usan la emulación de Windows.

Descripción general del curso

Como el título del curso lo indica, se centra en el aprendizaje de los aspectos fundamentales de networking. En este curso, aprenderá las habilidades prácticas y conceptuales que constituyen la base para entender lo básico de las redes. Primero, comparará la comunicación humana con la de red y observará las semejanzas. Luego, se presentarán los dos modelos principales que se usan para planear e implementar redes: OSI y TCP/IP. Logrará entender el método "en capas" de las redes y examinar las capas OSI y TCP/IP en detalle para entender sus funciones y servicios. Se familiarizará con los distintos dispositivos de red, esquemas de direccionamiento de red y finalmente con los tipos de medios que se usan para transmitir datos a través de la red.

En este curso, adquirirá experiencia usando las herramientas y utilidades de redes, como el Packet Tracer y Wireshark®, para explorar protocolos y conceptos de redes. Estas herramientas lo ayudarán a comprender cómo fluyen los datos en una red. También se utiliza una "Internet modelo" especial para proporcionar un entorno de prueba en el que se pueda analizar y observar un rango de servicios y datos de red.

Capítulo 1: El Capítulo 1 presenta los temas fundamentales de la comunicación y cómo las redes han cambiado nuestras vidas. Se presentarán los conceptos de redes, datos, Redes de área local (LAN), Redes de área extensa (WAN), Calidad de servicio (QoS), problemas de seguridad, servicios de colaboración de red y actividades del Packet Tracer. En los laboratorios, aprenderá a configurar un wiki y establecer una sesión de mensajería instantánea.

Capítulo 2: El Capítulo 2 se centra en cómo se modelan y se utilizan las redes. Se presentarán los modelos OSI y TCP/IP y el proceso de encapsulación de datos. Se explicará la herramienta de red Wireshark®, que se usa para analizar el tráfico de red, y se explorarán las diferencias entre una red real y una simulada. En la práctica de laboratorio desarrollará su primera red: una pequeña red peer-to-peer.

Capítulo 3: Mediante el uso de un método descendente para enseñar networking, el Capítulo 3 le presenta la capa del modelo de red superior, la capa de aplicación. En este contexto, explorará la interacción de protocolos, servicios y aplicaciones, con un enfoque en HTTP, DNS, DHCP, SMTP/POP, Telnet y FTP. En los laboratorios, practicará la instalación de un cliente/servidor Web y usará Wireshark® para analizar el tráfico de red. Las actividades de Packet Tracer le permiten explorar cómo operan los protocolos en la capa de aplicación.

Capítulo 4: El Capítulo 4 presenta la capa de transporte y se centra en cómo los protocolos TCP y UDP se utilizan en las aplicaciones comunes. En las prácticas de laboratorio y actividades incorporará el uso de Wireshark®, el comando de las utilidades de Windows netstat y Packet Tracer para investigar estos dos protocolos.

Capítulo 5: El Capítulo 5 presenta la capa de red OSI. Examinará los conceptos de direccionamiento y enrutamiento, y aprenderá sobre la determinación de ruta, los paquetes de datos y el protocolo IP. Al finalizar este capítulo, configurará hosts para acceder a la red local y explorar tablas de enrutamiento.

Capítulo 6: En el Capítulo 6, se centrará en el direccionamiento de red en detalle y aprenderá cómo usar la máscara de direcciones, o longitud del prefijo, para determinar la cantidad de subredes y hosts de una red. También se presentarán las herramientas ICMP (Protocolo de mensajes de control de Internet), como comando ping y trace.

Capítulo 7: El Capítulo 7 analiza los servicios proporcionados por la capa de enlace de datos. Se destaca la importancia en los procesos de encapsulación que se producen mientras los datos viajan a través de la LAN y la WAN.

Capítulo 8: El Capítulo 8 presenta la capa física. Descubrirá cómo los datos envían señales y se codifican para viajar por la red. Conocerá sobre el ancho de banda y además sobre los tipos de medios y sus conectores asociados.

Capítulo 9: En el Capítulo 9 analizará las tecnologías y operación de Ethernet. Utilizará Wireshark®, las actividades de Packet Tracer y los ejercicios de la práctica de laboratorio para explorar Ethernet.

Capítulo 10: El Capítulo 10 se centra en el diseño y el cableado de una red. Implementará los conocimientos y aptitudes desarrollados en los capítulos anteriores para determinar qué cables son los adecuados, cómo conectar los dispositivos y desarrollar un esquema de direccionamiento y prueba.

Capítulo 11: En el Capítulo 11 conectará y configurará una pequeña red utilizando los comandos IOS de Cisco para routers y switches. Cuando finalice este último capítulo, estará preparado para realizar los cursos de Enrutamiento o Comunicación de CCNA Exploration.

Wireshark® es una marca comercial registrada de Gerald Combs.

1- La vida en un mundo centrado en la red

1.0 INTRODUCCION DEL CAPITULO

1.0.1 Introducción del capítulo

En la actualidad nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar nuestra red humana. 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, creando nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman Internet tendrán una función cada vez más importante en el éxito de esos proyectos.

Este capítulo presenta la plataforma de las redes de datos, de las cuales dependen cada vez más nuestras relaciones sociales y de negocios. 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.

En este capítulo, aprenderá a:

- describir cómo las redes influyen en nuestra vida cotidiana,
- describir la función de la red de datos en la red humana,
- identificar los componentes clave de cualquier red de datos,
- identificar las oportunidades y los desafíos que presentan las redes convergentes,
- describir las características de las arquitecturas de red: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad, e
- instalar y usar clientes IRC (Internet Relay Chat) y un servidor Wiki.

11.1. LA COMUNICACIÓN EN UN MUNDO CENTRADO EN LA RED

1.1.1 Redes que respaldan la forma que vivimos

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está por debajo 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 compartir ideas e información están en constante cambio y evolución. Mientras la red humana estuvo limitada a conversaciones cara a cara, el avance de los medios ha ampliado el alcance de nuestras comunicaciones. Desde la prensa escrita hasta la televisión, cada nuevo desarrollo ha mejorado la comunicación.

Al igual que con cada avance en la tecnología de comunicación, la creación e interconexión de redes de datos sólidas tiene un profundo efecto.

Las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos. Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona acceso a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

La naturaleza inmediata de las comunicaciones en Internet alienta la formación de comunidades globales. Estas comunidades motivan la interacción social que depende de la ubicación o el huso horario.

Comunidad global

Es quizás el agente de cambio actualmente más significativo del mundo, ya que ayuda a crear un mundo en el cual las fronteras nacionales, las distancias geográficas y las limitaciones físicas son menos relevantes y presentan cada vez menos obstáculos. 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. Debido a que Internet conecta a las personas y promueve la comunicación sin límites, presenta la plataforma donde ejecutar negocios, tratar emergencias, informar a las personas y respaldar la educación, las ciencias y el gobierno.

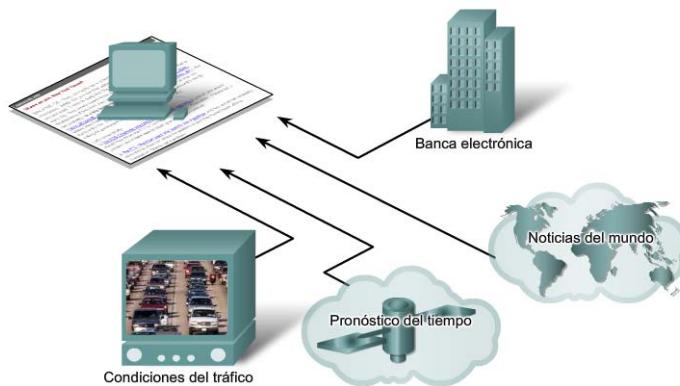
Es increíble la rapidez con la que Internet llegó a ser una parte integral de nuestra rutina diaria. La compleja interconexión de dispositivos y medios electrónicos que abarca la red es evidente para los millones de usuarios que hacen de ésta una parte personal y valiosa de sus vidas.

Las redes de datos que fueron alguna vez el transporte de información entre negocios se replanificaron para mejorar la calidad de vida de todas las personas. En el transcurso del día, los recursos disponibles en Internet pueden ayudarlo a:

- decidir cómo vestirse consultando en línea las condiciones actuales del clima,
- buscar el camino menos congestionado hacia su destino observando videos de cámaras Web que muestran el clima y el tráfico,
- consultar su estado de cuenta bancario y pagar electrónicamente las boletas,
- recibir y enviar correo electrónico o realizar una llamada telefónica a través de Internet durante el almuerzo en un bar con Internet,
- obtener información sobre la salud y consejos sobre nutrición de parte de expertos de todo el mundo y compartir en un foro esa información o tratamientos,
- descargar nuevas recetas y técnicas de cocina para crear cenas fabulosas, o
- enviar y compartir sus fotografías, videos caseros y experiencias con amigos o con el mundo.

Muchos usos de Internet habrían sido difíciles de imaginar sólo unos pocos años atrás. Tome, por ejemplo, la experiencia de una persona que publica un video musical casero:

“Mi objetivo es realizar mis propias películas. Un día, mi amiga Adi y yo hicimos un video sorpresa para el cumpleaños de su novio. Nos grabamos, hicimos mímica con una canción y bailamos. Luego dijimos, ¿por qué no publicarlo en la Web? Bueno, la reacción fue enorme. Hasta el momento más de 9 millones de personas la visitaron y el director de cine Kevin Smith hasta hizo una breve parodia. No sé qué atrajo a la gente al video. Tal vez su simpleza o la canción. Tal vez porque es espontáneo y divertido, y hace sentir bien a las personas. No lo sé. Pero lo que sí sé es que puedo hacer lo que me gusta y compartirlo en línea con millones de personas de todo el mundo. Lo único que necesito es mi computadora, mi cámara de video digital y algún software. Y eso es algo increíble”.



La forma en la que vivimos está respaldada por servicios provistos por la red de datos.

1.1.2 Ejemplos de las herramientas de comunicación mas populares

La existencia y adopción masiva de Internet abrieron paso a nuevas formas de comunicación que permitieron a las personas crear información que puede ser consultada por una audiencia global.

Mensajería instantánea

La mensajería instantánea (IM, Instant messaging) es una forma de comunicación en tiempo real entre dos o más personas en forma de texto escrito. El texto se transmite mediante computadoras conectadas por medio de una red interna privada o una red pública, como por ejemplo Internet. Desarrollada a partir de los servicios de Internet Relay Chat (IRC), IM incorpora características como la transferencia de archivos, comunicación por voz y video. Al igual que un e-mail, IM envía un registro escrito de la comunicación. Sin embargo, mientras que la transmisión de e-mails a veces se retrasa, los mensajes de IM se reciben inmediatamente. La forma de comunicación que usa la IM se denomina comunicación en tiempo real.

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 global sin tener conocimientos técnicos sobre diseño Web. Hay blogs casi sobre cualquier tema que uno pueda imaginar, y generalmente se forman comunidades de personas a través de autores populares de blogs.

Wikis

Las wikis son páginas Web que un grupo de personas puede editar y visualizar. Mientras un blog es más como un diario individual, 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. Existe una wiki pública llamada Wikipedia que se está transformando en un recurso extenso, una enciclopedia en línea de temas contribuidos públicamente. 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. Con Internet global la gente de cualquier credo puede participar en wikis y puede agregar sus propias perspectivas y conocimientos en un recurso compartido.

Podcasting

Podcasting es un medio basado en audio que originalmente permitía a las personas grabar y convertir audio para utilizarlo con los iPod (un dispositivo pequeño y portátil para reproducción de audio fabricado por Apple). La capacidad de grabar audio y guardarlo en un archivo de computadora no es una novedad. Sin embargo, el podcasting permite a las personas difundir sus grabaciones a una vasta audiencia. El archivo de audio se coloca en un sitio Web (o blog o wiki) desde donde otras personas pueden descargarlo y reproducirlo en sus computadoras de escritorio o portátiles y en sus iPod.

Herramientas de colaboración

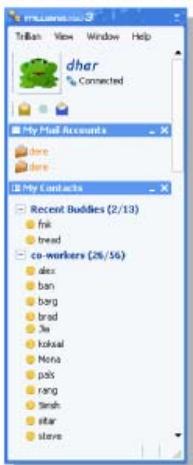
Las herramientas de colaboración permiten a las personas trabajar conjuntamente y compartir documentos. Sin las restricciones de ubicación ni huso horario, las personas conectadas a un sistema compartido pueden hablar entre ellos, compartir textos, gráficos y editar documentos en forma conjunta. Con las herramientas de colaboración siempre disponibles, las organizaciones pueden rápidamente compartir información 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.

Podcasting



Puede escuchar su programa de radio favorito en su reproductor de audio portátil en cualquier lado, siempre que tenga tiempo. Cada vez que un programa nuevo está disponible, puede descargarse automáticamente.

Mensajería instantánea



La mensajería instantánea (IM) está en todos lados y puede incluir conversaciones de audio y video. La IM puede enviar mensajes de texto a teléfonos celulares.

Weblog



Puede expresar sus ideas en línea, compartir sus fotos y sumarse a una comunidad de pensadores.

1.1.3 Redes que respaldan 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. Redes confiables y sólidas respaldan y enriquecen las experiencias de aprendizaje de los estudiantes. Estas redes envían material de aprendizaje en una amplia variedad de formatos. Los materiales de aprendizaje incluyen actividades interactivas, evaluaciones y comentarios.

Los cursos enviados utilizando recursos de Internet o de red generalmente se denominan experiencias de aprendizaje en línea o e-learning.

La disponibilidad del software educativo de e-learning multiplicó los recursos disponibles para estudiantes en todo momento. Los métodos de aprendizaje tradicionales principalmente proporcionan dos fuentes de conocimiento desde 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. Por lo contrario, los cursos en línea pueden contener voz, datos y videos, y se encuentran disponibles para los estudiantes a cualquier hora y en todo lugar. Los estudiantes pueden utilizar enlaces a diferentes referencias y expertos en la materia para mejorar su experiencia de aprendizaje. 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 incluir clases guiadas por un instructor con software educativo en línea para proporcionar lo mejor de los métodos de entrega.

El acceso a una instrucción de alta calidad no está restringido a estudiantes que viven cerca del lugar de instrucción. El aprendizaje a distancia en línea eliminó las barreras geográficas y mejoró la oportunidad de los estudiantes.

El Programa de la Academia de Networking de Cisco, que ofrece este curso, es un ejemplo de experiencia de aprendizaje global en línea. El instructor proporciona un programa y establece un cronograma preliminar para completar el contenido del curso. El Programa de la Academia complementa los conocimientos del instructor con un currículum interactivo que proporciona muchas maneras de experiencias de aprendizaje. El programa proporciona texto, gráficos, animaciones y una herramienta de entorno de networking simulado llamada Packet Tracer. Packet Tracer ofrece una forma de crear representaciones virtuales de redes y de emular muchas de las funciones de los dispositivos de red.

Los estudiantes se pueden comunicar con el instructor y con sus compañeros a través de herramientas en línea, como el correo electrónico, tableros de discusión o de boletín, salas de chat y mensajería instantánea. Los enlaces proporcionan acceso a los recursos de aprendizaje fuera del software educativo. E-learning combinado proporciona los beneficios del aprendizaje asistido por PC y a la vez mantiene las ventajas del currículum guiado por el instructor. Los estudiantes tienen la oportunidad de trabajar en línea a su propio ritmo y nivel de aptitud, incluso con acceso al instructor y a otros recursos en vivo.

Además de los beneficios para el estudiante, las redes también mejoraron la gestión y administración de los cursos. Algunas de estas funciones en línea son: inscripción, entrega de evaluaciones y libros de calificaciones.

En el mundo empresarial, el uso de redes para proporcionar capacitación económica y eficiente a los empleados está siendo cada vez más aceptado. 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.

La entrega y el software educativo en línea ofrecen muchos beneficios a las empresas. Entre los beneficios se encuentran:

Materiales precisos y actuales de capacitación. La colaboración entre distribuidores, fabricantes de equipos y proveedores de capacitación asegura la actualización del software educativo con los últimos procesos y procedimientos. Una vez que se corrigen los errores encontrados en los materiales, inmediatamente se ponen a disposición de los empleados los nuevos cursos.

Disponibilidad de capacitación para una amplia audiencia. La capacitación en línea no depende de horarios de viaje, de la disponibilidad del instructor ni del tamaño físico de la clase. A los empleados se les puede dar plazos en los cuales deben completar la capacitación y ellos pueden acceder a los cursos cuando les sea conveniente. Calidad consistente de instrucción. La calidad de la instrucción no varía de la misma manera que si diferentes instructores dictaran un curso en persona. El currículum en línea proporciona un centro de instrucción consistente al cual los instructores pueden agregar experiencia adicional.

Reducción de costos. Además de reducir el costo de viajes y en consecuencia el tiempo perdido, existen otros factores de reducción de costos para empresas relacionados con la capacitación en línea. Generalmente es más económico revisar y actualizar el software educativo en línea que actualizar el material en papel. También se reducen o eliminan las instalaciones para respaldar la capacitación en persona.

Muchas empresas también ofrecen capacitación de clientes en línea. Este curso permite a los clientes utilizar de la mejor manera los productos y servicios proporcionados por la empresa, reduciendo llamadas a las líneas de ayuda o a los centros de servicio al cliente.

1.1.4 Redes que respaldan la forma en que trabajamos

En principio, las empresas utilizaban redes de datos para registrar y administrar internamente la información financiera, la información del cliente y los sistemas de nómina de empleados. Las redes comerciales evolucionaron para permitir la transmisión de diferentes tipos de servicios de información, como e-mail, video, mensajería y telefonía.

Las intranets, redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales. Las compañías desarrollan extranets o internetwork extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes.

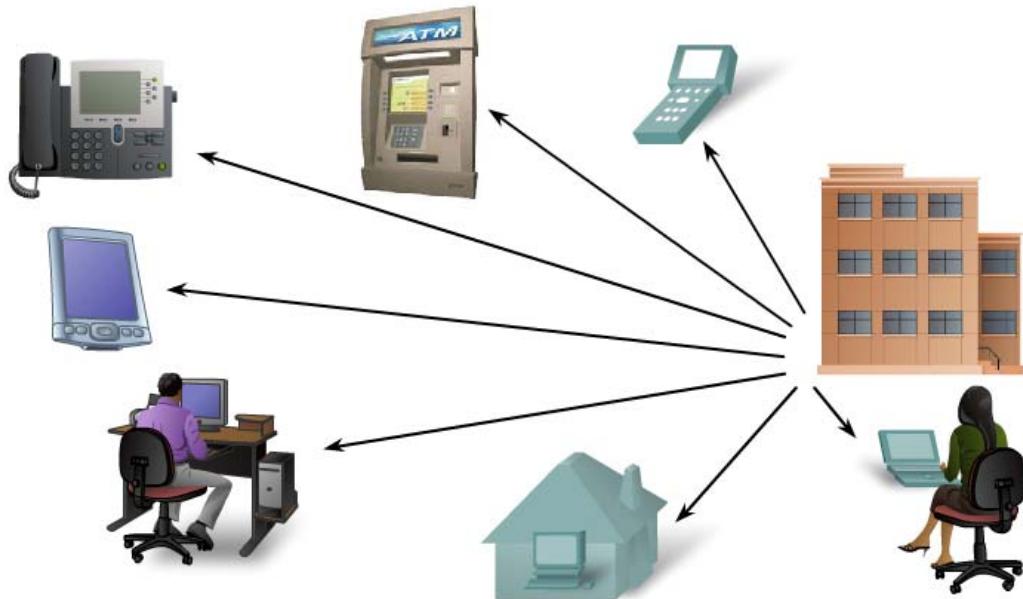
En la actualidad, las redes ofrecen una mayor integración entre funciones y organizaciones relacionadas que la que era posible en el pasado.

Observe estos escenarios de negocios.

Un granjero de trigo en Australia utiliza una computadora portátil con un Sistema de posicionamiento global (GPS) para plantar un cultivo con precisión y eficacia. En la época de la cosecha, el granjero puede coordinar la cosecha contando con transportadores de granos e instalaciones de almacenamiento. A través de la tecnología inalámbrica el transportador de granos puede monitorear el vehículo en ruta para lograr la mejor eficiencia del combustible y una operación segura. Los cambios en el estado se pueden delegar instantáneamente al conductor del vehículo.

Los trabajadores a distancia, denominados teletrabajadores o empleados a distancia, utilizan servicios de acceso remoto seguro desde el hogar o mientras viajan. La red de datos les permiten trabajar como si estuvieran en su propio lugar de trabajo, con acceso a todas las herramientas basadas en red disponibles para realizar sus tareas. Pueden organizarse conferencias y reuniones virtuales incluso con personas en ubicaciones remotas. La red proporciona capacidades de audio y video para que todos los participantes puedan verse y escucharse. La información de esas reuniones puede grabarse en una wiki o blog. Las versiones más recientes de agenda y de minutos se pueden compartir apenas son creadas.

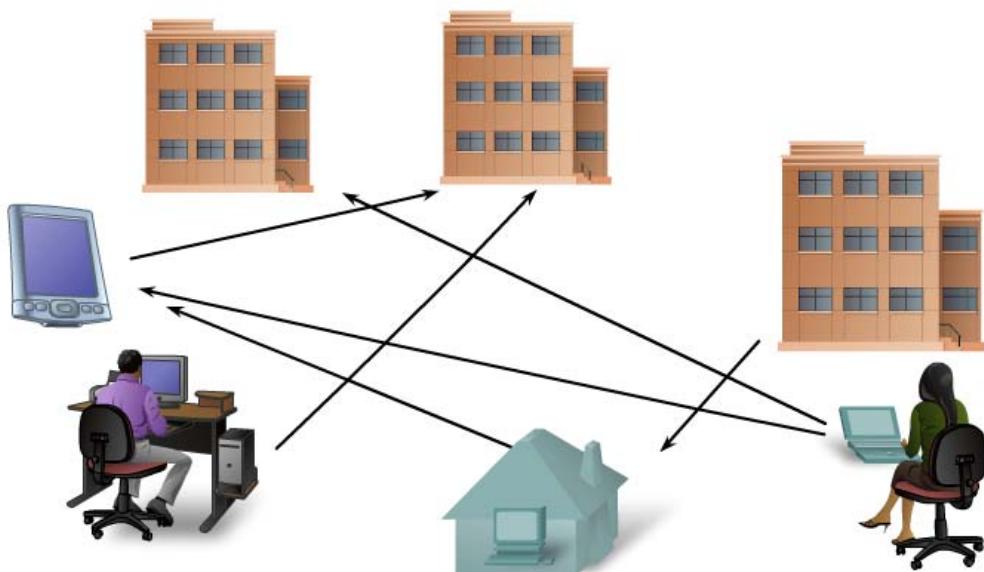
Hay muchas historias que demuestran las formas innovadoras en que se utilizan las redes para hacernos más exitosos en el lugar de trabajo. Algunas de esas situaciones se encuentran disponibles en el sitio Web de Cisco en <http://www.cisco.com>



Se puede acceder remotamente a las aplicaciones comerciales como si los empleados estuvieran en el lugar.

**ACCESO
REMOTO**

**MÚLTIPLES
RECURSOS**



Los trabajadores que se encuentran en cualquier ubicación pueden comunicarse entre sí y acceder a múltiples recursos de la red.

**ACCESO
REMOTO**

**MÚLTIPLES
RECURSOS**

1.1.5 Redes que respaldan 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, como también prever los destinos reales antes de realizar un viaje. Los detalles y las fotografías de estas aventuras pueden publicarse en línea para que otros los vean.

Internet también se utiliza para formas tradicionales de entretenimiento. Escuchamos artistas grabados, vemos o disfrutamos de avances de películas, leemos libros completos y descargamos material para acceder luego sin conexión. Los eventos deportivos y los conciertos en vivo pueden presenciarse mientras suceden, o grabarse y verse cuando lo deseé.

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

Incluso las actividades sin conexión son mejoradas con los servicios de colaboración en red. Las comunidades globales 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 subasta en línea brindan la oportunidad de comprar, vender y comercializar todo tipo de mercancía.

En la red humana podemos disfrutar cualquier forma de recreación, las redes mejoran nuestra experiencia.



La forma en la que jugamos está respaldada por servicios provistos por la red de datos.

1.2 LA COMUNICACIÓN: PARTE ESENCIAL DE NUESTRAS VIDAS

1.2.1 ¿Qué es la comunicación?

La comunicación en nuestra vida cotidiana tiene diferentes formas y existe en muchos entornos. Tenemos diferentes expectativas según si estamos conversando por Internet o participando de una entrevista de trabajo. Cada situación tiene su comportamiento y estilo correspondiente.

Establecimiento de reglas

Antes de comenzar a comunicarnos, establecemos reglas o acuerdos que rigen la conversación. Estas reglas o protocolos deben respetarse para que el mensaje se envíe y comprenda correctamente. Algunos de los protocolos que rigen con éxito las comunicaciones humanas son:

- emisor y receptor identificados,
- método de comunicación consensuado (cara a cara, teléfono, carta, fotografía),
- idioma y gramática comunes,
- velocidad y puntualidad en la entrega, y
- requisitos de confirmación o acuse de recibo.

Las reglas de comunicación pueden variar según el contexto. Si un mensaje transmite un hecho o concepto importante, se necesita una confirmación de que el mensaje se recibió y comprendió correctamente. Los mensajes menos importantes pueden no requerir acuse de recibo por parte del receptor.

Las técnicas utilizadas en las comunicaciones de red comparten estos fundamentos con las conversaciones humanas. Se presuponen algunas reglas debido a que muchos de los protocolos de comunicación humana son implícitos y están arraigados en nuestra cultura. Al establecer las redes de datos, es necesario ser mucho más explícito sobre la forma en que se realizan y juzgan con éxito las comunicaciones.

1.2.2 Calidad de las comunicaciones

La comunicación entre individuos está destinada a ser exitosa cuando el significado del mensaje comprendido por el receptor coincide con el significado del emisor.

Para las redes de datos, utilizamos los mismos criterios básicos que para juzgar el éxito. Sin embargo, debido a que un mensaje se traslada por la red, muchos factores pueden evitar que el mensaje llegue al receptor o distorsionar el significado pretendido. Estos factores pueden ser externos o internos.

Factores externos

Los factores externos que afectan la comunicación están relacionados con la complejidad de la red y el número de dispositivos que debe atravesar un mensaje para llegar al destino final.

Los factores externos que afectan el éxito de las comunicaciones son:

- la calidad de la ruta entre el emisor y el receptor,
- la cantidad de veces que el mensaje tiene que cambiar la forma,
- la cantidad de veces que el mensaje tiene que ser redireccionado o redirigido, y
- la cantidad de mensajes adicionales que se transmiten simultáneamente en la red de comunicación,
- la cantidad de tiempo asignado para una comunicación exitosa.

Factores internos

Los factores internos que interfieren en la comunicación en redes están relacionados con la naturaleza del mensaje.

Diferentes tipos de mensajes pueden variar en complejidad e importancia. Los mensajes claros y concisos son generalmente más fáciles de entender que los mensajes complejos. Las comunicaciones importantes requieren de más atención para asegurarse de que el receptor las comprenda correctamente.

Los factores internos que afectan la comunicación exitosa en la red son:

- el tamaño del mensaje,
- la complejidad del mensaje, y
- la importancia del mensaje.

Los mensajes grandes pueden ser interrumpidos o demorados en diferentes puntos de la red. Un mensaje con baja importancia o prioridad puede perderse si la red está sobrecargada.

Deben anticiparse y controlarse los factores externos e internos que afectan la recepción del mensaje para así obtener una comunicación en red exitosa. Se implementan innovaciones en el hardware y en el software de la red para garantizar la calidad y confiabilidad de las comunicaciones de red.

1.3 LA RED COMO PLATAFORMA

1.3.1 Comunicación a través de redes

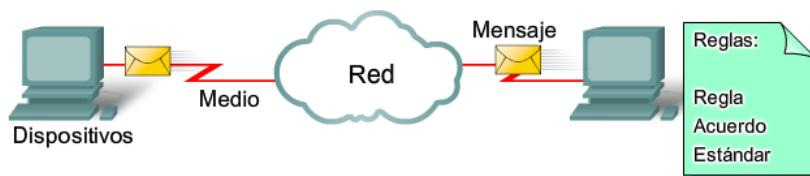
Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para nuestra vida personal y comercial. Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, confiamos en una Web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común:

- reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes,
- los mensajes o unidades de información que viajan de un dispositivo a otro,
- una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un dispositivo a otro, y
- los dispositivos de la red que cambian mensajes entre sí.

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.

1.3.2 Elementos de una red

El diagrama muestra los elementos de una red típica, incluyendo dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar mensajes. Utilizamos la palabra mensajes como un término que abarca las páginas Web, los e-mails, los mensajes instantáneos, las llamadas telefónicas y otras formas de comunicación permitidas por Internet. En este curso, aprenderemos acerca de una variedad de mensajes, dispositivos, medios y servicios que permiten la comunicación de esos mensajes. Aprenderemos además sobre las reglas o protocolos que unen a estos elementos de red.



Los cuatro elementos de una red:

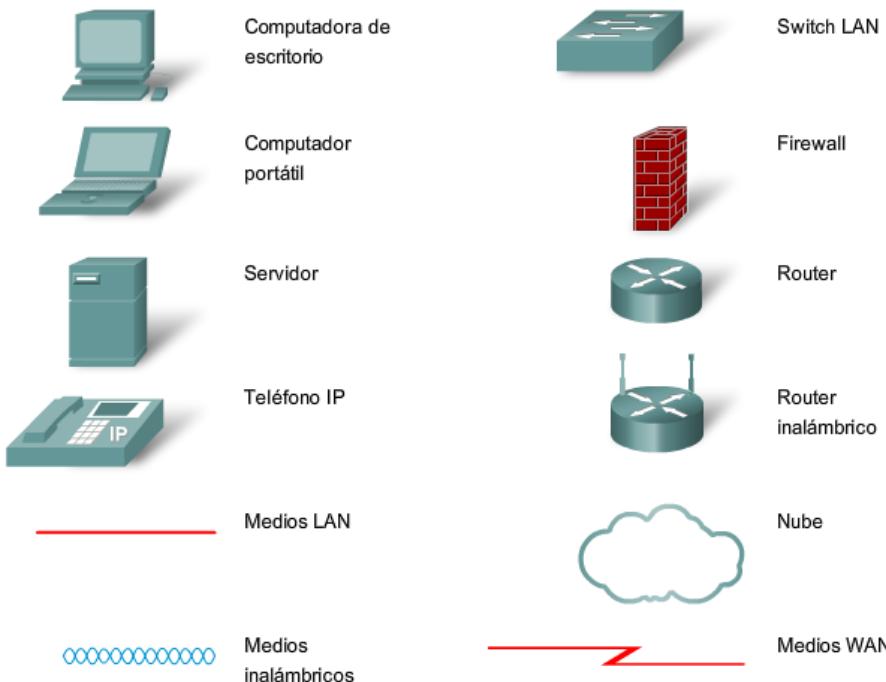
- Reglas
- Medio
- Mensajes
- Dispositivos

En este curso, se analizarán muchos dispositivos de red. La interconexión de redes es un tema orientado gráficamente y los íconos se utilizan comúnmente para representar sus dispositivos. En la parte izquierda del diagrama se muestran algunos dispositivos comunes que generalmente originan mensajes que constituyen nuestra comunicación. Esto incluye diversos tipos de equipos (se muestran íconos de una computadora de escritorio y de una portátil), servidores y teléfonos IP. En las redes de área local, estos dispositivos generalmente se conectan a través de medios LAN (con cables o inalámbricos).

El lado derecho de la figura muestra algunos de los dispositivos intermedios más comunes, utilizados para direccionar y administrar los mensajes en la red, como así también otros símbolos comunes de interconexión de redes. Los símbolos genéricos se muestran para:

- Switch: el dispositivo más utilizado para interconectar redes de área local,
- Firewall: proporciona seguridad a las redes,
- Router: ayuda a direccionar mensajes mientras viajan a través de una red,
- Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas,
- Nube: se utiliza para resumir un grupo de dispositivos de red, sus detalles pueden no ser importantes en este análisis,
- Enlace serial: una forma de interconexión WAN (Red de área extensa), representada por la línea en forma de rayo.

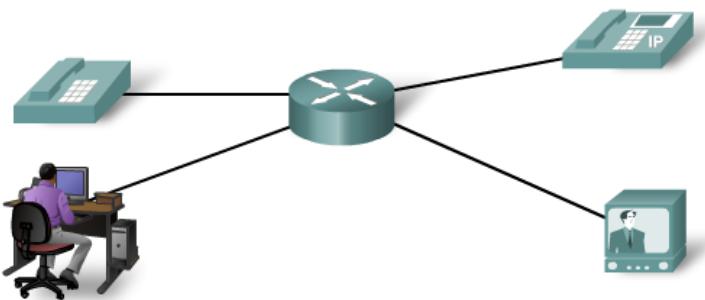
Símbolos comunes de las redes de datos



Para que funcione una red, los dispositivos deben estar interconectados. Las conexiones de red pueden ser con cables o inalámbricas. En las conexiones con cables, el medio puede ser cobre, que transmite señales eléctricas, o fibra óptica, que transmite señales de luz. En las conexiones inalámbricas, el medio es la atmósfera de la tierra o espacio y las señales son microondas. Los medios de cobre incluyen cables, como el par trenzado del cable de teléfono, el cable coaxial o generalmente conocido como cable de par trenzado no blindado (UTP) de Categoría 5. Las fibras ópticas, hebras finas de vidrio o plástico que transmiten señales de luz, son otra forma de medios de networking. Los medios inalámbricos incluyen conexiones inalámbricas domésticas entre un router inalámbrico y una computadora con una tarjeta de red inalámbrica, conexión inalámbrica terrestre entre dos estaciones de tierra o comunicación entre dispositivos en tierra y satélites. En un viaje típico a través de Internet, un mensaje puede viajar en una variedad de medios.

Conexiones de red

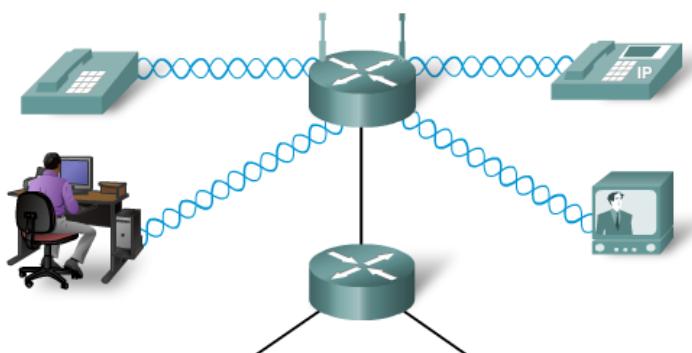
Las redes cableadas usaban cables físicos para conectar los dispositivos.



Las redes inalámbricas usan ondas de radio para la comunicación entre dispositivos.



Las redes inalámbricas, en algún punto, también se conectan con las redes cableadas.



Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, e-mail, mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos. En el cuadro se enumeran algunos servicios y un protocolo vinculado en forma más directa con ese servicio.

Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí. Actuamente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

| Servicio | Protocolo ("Regla") |
|--|--|
| World Wide Web (WWW) | HTTP (Hypertext Transport Protocol) |
| E-mail | SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol) |
| Mensaje instantáneo (Jabber; AIM) | XMPP (Extensible Messaging and Presence Protocol) OSCAR (Sistema abierto para la comunicación en tiempo real) |
| Telefonía IP | SIP (Session Initiation Protocol) |

Cerramos esta sección con un ejemplo para ver cómo los elementos de redes, dispositivos, medios y servicios, están conectados mediante reglas para enviar un mensaje. Las personas generalmente imaginan las redes en el sentido abstracto. Creamos y enviamos un mensaje de texto y en forma casi inmediata se muestra en el dispositivo de destino. Aunque sabemos que entre el dispositivo de emisión y el dispositivo de recepción hay una red mediante la cual viajan nuestros mensajes, raramente pensamos en todas las partes y piezas que forman esa infraestructura.

Mensajes

En la primera etapa del viaje desde la computadora al destino, el mensaje instantáneo se convierte en un formato que puede transmitirse en la red. Todos los tipos de mensajes tienen que ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. Una vez que el mensaje instantáneo se convierte en bits, está listo para ser enviado a la red para su remisión.

Dispositivos

Para comenzar a entender la solidez y complejidad de las redes interconectadas que forman Internet, es necesario empezar por lo más básico. Tomemos el ejemplo del envío de mensajes de texto con un programa de mensajería instantánea en una computadora. Cuando pensamos en utilizar servicios de red, generalmente pensamos en utilizar una computadora para acceder a ellos. Pero una computadora es sólo un tipo de dispositivo que puede enviar y recibir mensajes por una red. Muchos otros tipos de dispositivos pueden conectarse a la red para participar en servicios de red. Entre esos dispositivos se encuentran teléfonos, cámaras, sistemas de música, impresoras y consolas de juegos.

Además de la computadora, hay muchos otros componentes que hacen posible que nuestros mensajes instantáneos sean direccionados a través de kilómetros de cables, cables subterráneos, ondas aéreas y estaciones de satélites que puedan existir entre los dispositivos de origen y de destino. Uno de los componentes críticos en una red de cualquier tamaño es el router. Un router une dos o más redes, como una red doméstica e Internet, y pasa información de una red a otra. Los routers en una red funcionan para asegurar que el mensaje llegue al destino de la manera más rápida y eficaz.

Medio

Para enviar el mensaje instantáneo al destino, la computadora debe estar conectada a una red local inalámbrica o con cables. Las redes locales pueden instalarse en casas o empresas, donde permiten a computadoras y otros dispositivos compartir información y utilizar una conexión común a Internet.

Las redes inalámbricas permiten el uso de dispositivos con redes en cualquier parte, en una oficina, en una casa e inclusive al aire libre. Fuera de la casa o la oficina, la red inalámbrica está disponible en zonas activas públicas como cafés, empresas, habitaciones de hoteles y aeropuertos.

Muchas de las redes instaladas utilizan cables para proporcionar conectividad. Ethernet es la tecnología de red con cable más común en la actualidad. Los hilos, llamados cables, conectan las computadoras a otros dispositivos que forman las redes. Las redes con cables son mejores para transmitir grandes cantidades de datos a alta velocidad y son necesarias para respaldar multimedia de calidad profesional.

Servicios

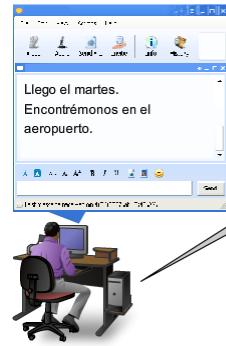
Los servicios de red son programas de computación que respaldan la red humana. Distribuidos en toda la red, estos servicios facilitan las herramientas de comunicación en línea como e-mails, foros de discusión/boletines, salas de chat y mensajería instantánea. Por ejemplo: en el caso un servicio de mensajería instantánea proporcionado por dispositivos en la nube, debe ser accesible tanto para el emisor como para el receptor.

Las Reglas

Aspectos importantes de las redes que no son dispositivos ni medios, son reglas o protocolos. Estas reglas son las normas o protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino. Por ejemplo: en el caso de la mensajería instantánea Jabber, los protocolos XMPP, TCP e IP son importantes conjuntos de reglas que permiten que se realice la comunicación.

Envío de un mensaje instantáneo

Envío de un mensaje instantáneo



Los mensajes instantáneos se convierten en bits binarios antes de que se transmitan por el medio.

1

2

3

4

5

6

7

1

2

3

4

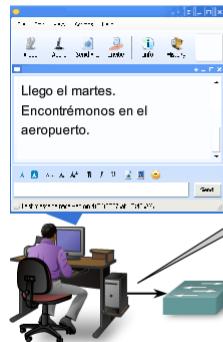
5

6

7

Envío de un mensaje instantáneo

Haga clic para ver los pasos.



La tarjeta de interfaz de red que se encuentra dentro de la PC genera señales eléctricas para representar los bits y ubica los bits en el medio. Los bits llegan al primer dispositivo de red.

1

2

3

4

5

6

7

1

2

3

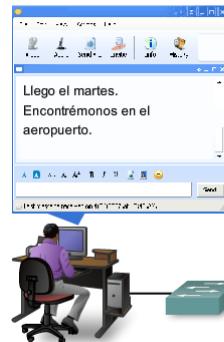
4

5

6

7

Envío de un mensaje instantáneo



Un router cumple un rol fundamental, ya que conecta las redes y garantiza que la comunicación se dirija a su destino.

Los bits pasan de un dispositivo a otro en el área local. Cuando los bits salen del área local, generalmente, pasan por un router.

Envío de un mensaje instantáneo



Desde esta perspectiva, los distintos dispositivos interconectados de todo el mundo, generalmente, se representan con una nube.

Redes de datos

Los bits se transmiten a los dispositivos que conectan las redes locales. Pueden ser docenas e incluso cientos los dispositivos que manejan los bits mientras se enrutan a su destino.

1

2

3

4

5

6

7

Hag



A medida que los bits se acercan a su destino, pasan una vez más por los dispositivos locales.

clic para ver los pasos.



El dispositivo de destino lee los bits y los convierte nuevamente en un mensaje legible para los humanos.

1

2

3

4

5

6

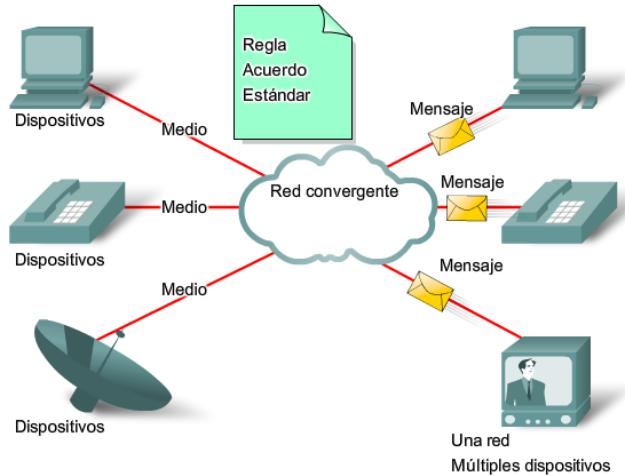
7

Haga clic para ver los pasos.

1.3.3 Redes convergentes

Redes múltiples de múltiples servicios

El teléfono tradicional, la radio, la televisión y las redes de datos informáticos tienen su propia versión individual de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para emitir su señal de comunicación particular. Además, cada servicio tiene su propio conjunto de reglas y estándares para garantizar la comunicación exitosa de su señal a través de un medio específico.



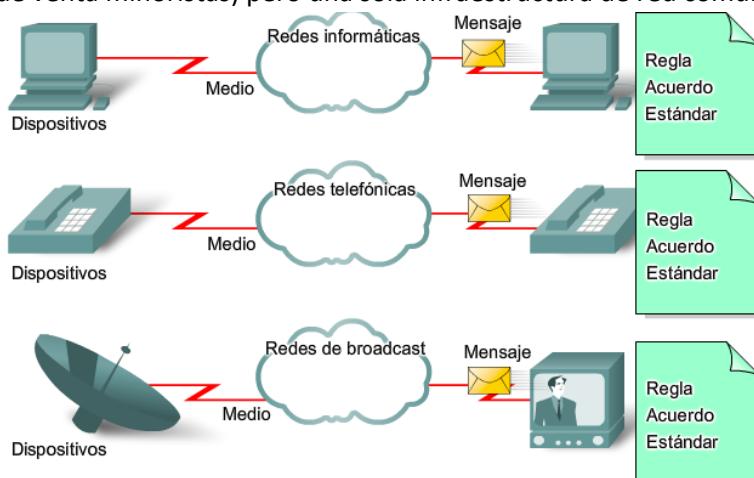
Las redes de datos convergentes transportan múltiples servicios en una red.

Múltiples redes

Redes convergentes

Redes convergentes

Los avances de la tecnología nos permiten consolidar esas redes dispersas en una única plataforma: una plataforma definida como una red convergente. El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas. En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común.



Se ejecutan múltiples servicios en múltiples redes.

Múltiples redes

Redes convergentes

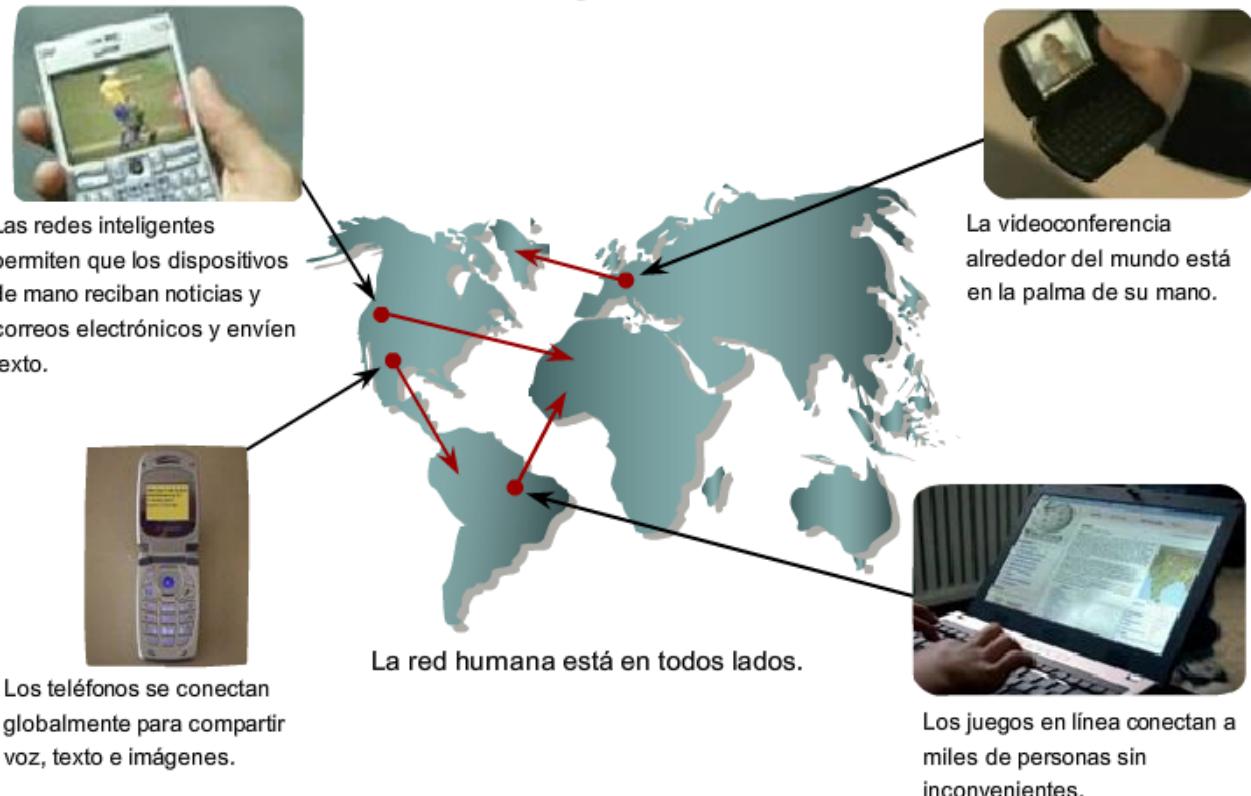
Redes de información inteligentes

La función de la red está evolucionando. La plataforma de comunicaciones inteligentes del futuro ofrecerá mucho más que conectividad básica y acceso a las aplicaciones. 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 resultante proporcionará funcionalidad de aplicaciones de alta calidad a un costo reducido.

Planificación para el futuro

La velocidad a la que se desarrollan nuevas e interesantes aplicaciones de red convergentes se puede atribuir a la rápida expansión de Internet. Esta expansión creó una amplia audiencia y una base de consumo más grande, ya que puede enviarse cualquier mensaje, producto o servicio. Los procesos y mecanismos subyacentes que llevan a este crecimiento explosivo tienen como resultado una arquitectura de red más flexible y escalable. 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.

Las redes inteligentes unen al mundo



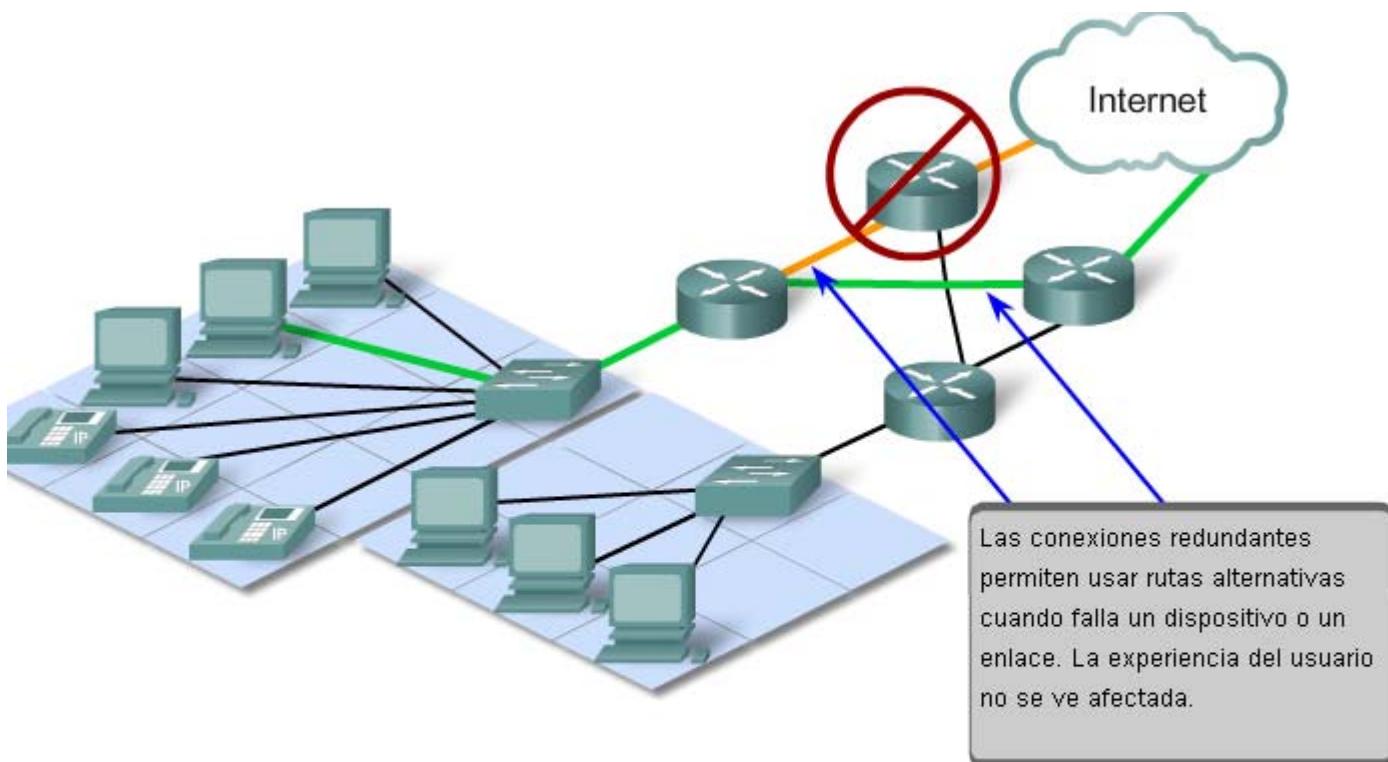
1.4 ARQUITECTURA DE INTERNET

1.4.1 Arquitectura de red

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

Tolerancia a fallas

La expectativa de que Internet está siempre disponible para millones de usuarios que confían en ella requiere de una arquitectura de red diseñada y creada con tolerancia a fallas. Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutararse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Ésta es la premisa básica de la arquitectura de redes actuales.

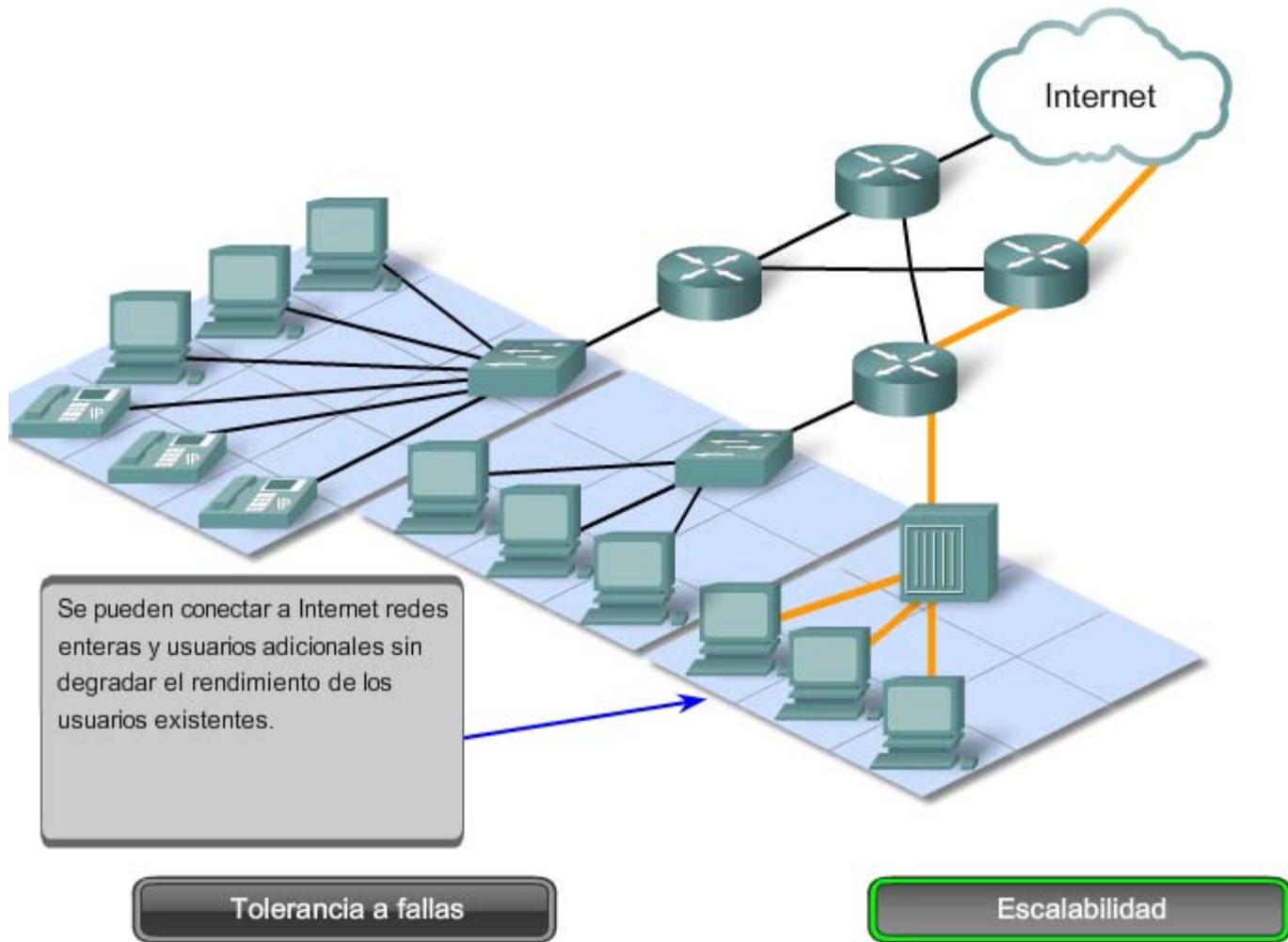


Tolerancia a fallas

Escalabilidad

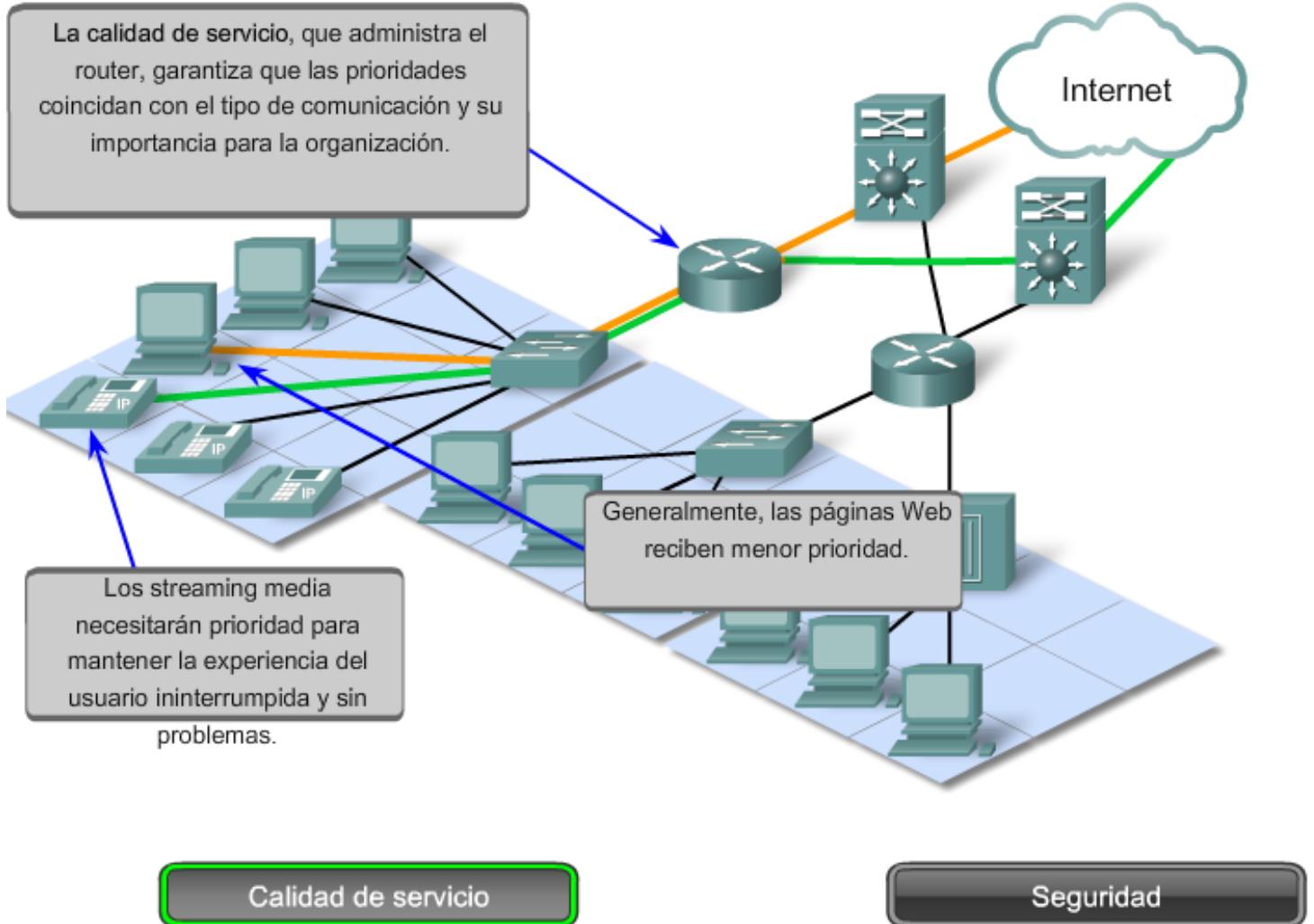
Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar usuarios individuales dentro de una internetwork, permiten a Internet mantenerse al ritmo de la demanda de los usuarios.



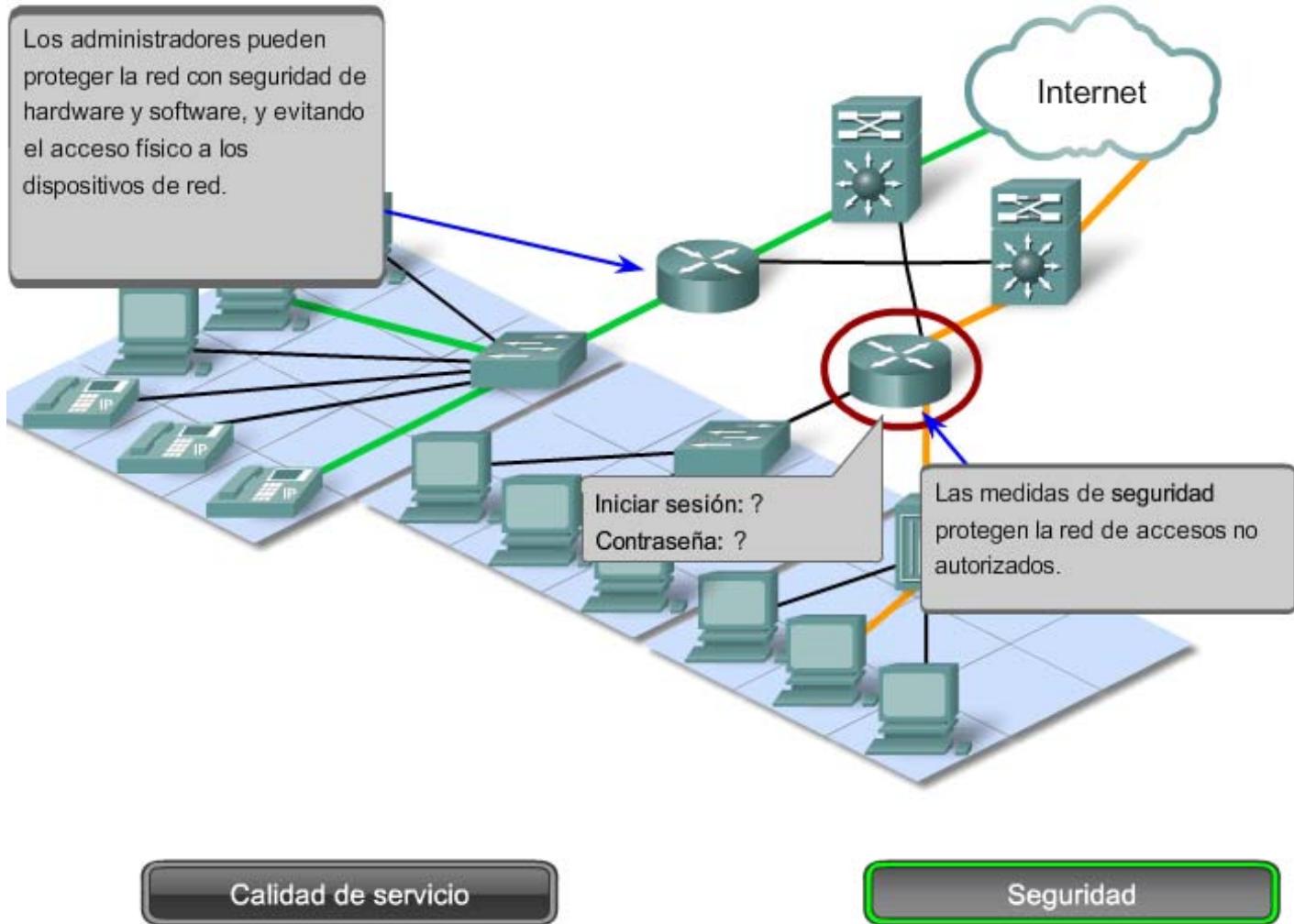
Calidad de servicio (QoS)

Internet actualmente proporciona un nivel aceptable de tolerancia a fallas y escalabilidad para sus usuarios. Pero las nuevas aplicaciones disponibles para los usuarios en internetworks crean expectativas mayores para la calidad de los servicios enviados. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.



Seguridad

Internet evolucionó de una internetwork de organizaciones gubernamentales y educativas estrechamente controlada a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial excede lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.



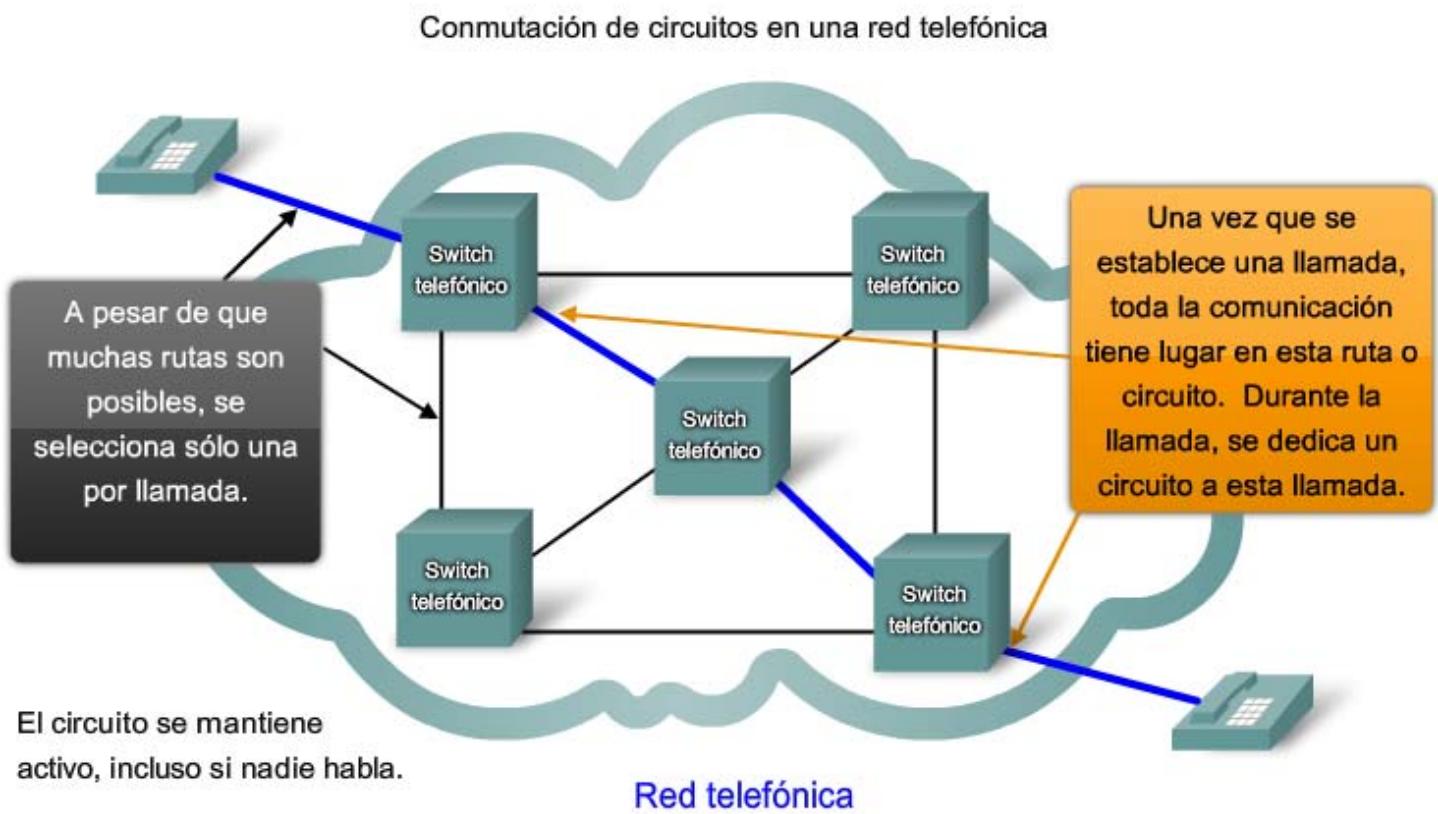
1.4.2 Arquitectura de red tolerante a fallas

Internet, en sus comienzos, era el resultado de una investigación respaldada por el Departamento de Defensa de Estados Unidos (DoD). Su objetivo principal fue tener un medio de comunicación que pudiera soportar la destrucción de numerosos sitios e instalaciones de transmisión sin interrumpir el servicio. Esto implica que la tolerancia a fallas era el foco del esfuerzo del trabajo de diseño de internetwork inicial. Los primeros investigadores de red observaron las redes de comunicación existentes, que en sus comienzos se utilizaban para la transmisión de tráfico de voz, para determinar qué podía hacerse para mejorar el nivel de tolerancia a fallas.

Redes orientadas a la conexión conmutadas por circuito

Para comprender el desafío con el que se enfrentaron los investigadores del DoD, es necesario observar cómo funcionaban los sistemas telefónicos. Cuando una persona realiza una llamada utilizando un teléfono tradicional, la llamada primero pasa por un proceso de configuración en el cual se identifican todas las conmutaciones telefónicas entre la persona y el teléfono al que está llamando. Se crea un ruta temporal o circuito a través de las distintas ubicaciones de conmutación a utilizar durante la duración de la llamada telefónica. Si falla algún enlace o dispositivo que participa en el circuito, la llamada se cae. Para volver a conectarse, se debe realizar una nueva llamada y crear un nuevo circuito entre el teléfono de origen y el de destino. Este tipo de red orientada a la conexión se llama red conmutada por circuito. Las primeras redes conmutadas por circuito no recreaban en forma dinámica los circuitos descartados. Para recuperarse de una falla, se deben iniciar nuevas llamadas y crear nuevos circuitos de extremo a extremo.

Muchas redes conmutadas por circuitos otorgan prioridad al mantenimiento de conexiones de circuitos existentes a expensas de nuevas solicitudes de circuitos. En este tipo de red orientada a la conexión, una vez establecido el circuito, aunque no exista comunicación entre las personas en ningún extremo de la llamada, el circuito permanece conectado y los recursos se reservan hasta que una de las partes desconecta la llamada. Debido a que existe una determinada capacidad para crear nuevos circuitos, es posible que a veces reciba un mensaje de que todos los circuitos están ocupados y no pueda realizar la llamada. El costo que implica crear muchas rutas alternativas con capacidad suficiente para admitir un gran número de circuitos simultáneos y las tecnologías necesarias para recrear en forma dinámica los circuitos descartados en caso de falla, llevaron al DoD a considerar otros tipos de redes.



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

Redes sin conexión conmutadas por paquetes

En la búsqueda de una red que pueda soportar la pérdida de una cantidad significativa de sus servicios de transmisión y conmutación, los primeros diseñadores de Internet reevaluaron las investigaciones iniciales acerca de las redes conmutadas por paquetes. La premisa para este tipo de redes es que un simple mensaje puede dividirse en múltiples bloques de mensajes. Los bloques individuales que contienen información de direccionamiento indican tanto su punto de origen como su destino final. Utilizando esta información incorporada, se pueden enviar por la red a través de diversas rutas esos bloques de mensajes, denominados paquetes, y se pueden rearmar como el mensaje original una vez que llegan a destino.

Utilización de paquetes

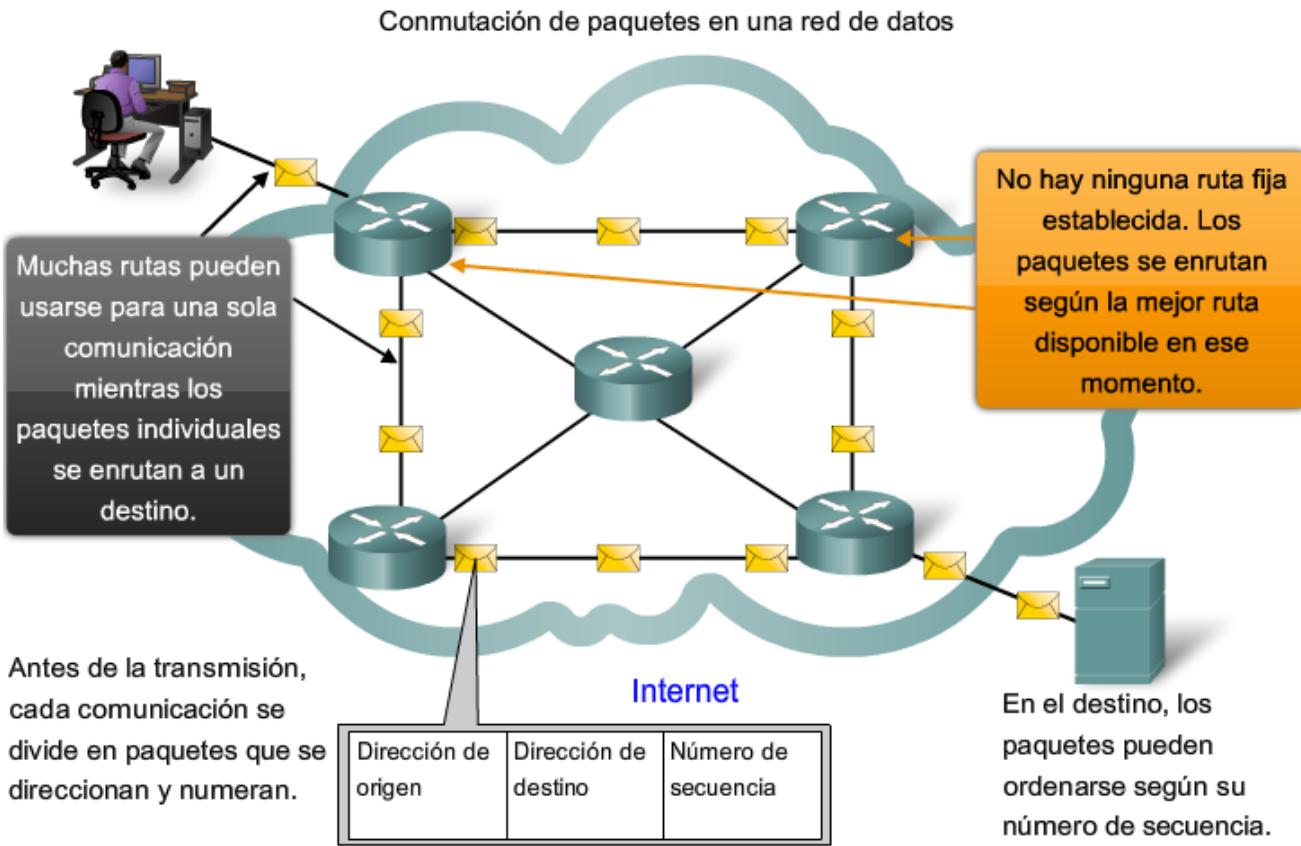
Los dispositivos dentro de la misma red no tienen en cuenta el contenido de los paquetes individuales, sólo es visible la dirección del destino final y del próximo dispositivo en la ruta hacia ese destino. No se genera ningún circuito reservado entre emisor y receptor. Cada paquete se envía en forma independiente desde una ubicación de conmutación a otra. En cada ubicación, se decide qué ruta utilizar para enviar el paquete al destino final. 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 mensaje completo y único, los pocos paquetes que pueden perderse en caso de que se produzca una falla pueden volver a transmitirse a destino por una ruta diferente. En muchos casos, el dispositivo de destino no tiene en cuenta que se ha producido una falla o reenrutamiento.

Redes sin conexión conmutadas por paquetes

Los investigadores del Departamento de Defensa (DoD) se dieron cuenta de que una red sin conexión conmutada por paquetes tenía las características necesarias para admitir una arquitectura de red resistente y tolerante a fallas. 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. Los paquetes que contienen las partes de los mensajes de diferentes orígenes pueden viajar por la red al mismo tiempo. El problema de los circuitos inactivos o no utilizados desaparece; todos los recursos disponibles pueden utilizarse en cualquier momento para enviar paquetes al destino final. Al proporcionar un método para utilizar dinámicamente rutas redundantes sin intervención del usuario, Internet se ha vuelto un método de comunicación tolerante a fallas y escalable.

Redes orientadas a la conexión

Aunque las redes sin conexión conmutadas por paquetes cubren las necesidades de los DoD y siguen siendo la infraestructura primaria de la Internet actual, hay algunos beneficios en un sistema orientado a la conexión como el sistema telefónico conmutado por circuito. 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 consistencia de los mensajes transmitidos en una red orientada a la conexión. Otro beneficio es que el proveedor del servicio puede cargar los usuarios de la red durante el período de tiempo en que la conexión se encuentra activa. La capacidad de cargar los usuarios para conexiones activas a través de la red es una premisa fundamental de la industria del servicio de telecomunicaciones.



Durante los períodos de demanda pico, la comunicación puede demorarse, pero no denegarse.

1.4.3 Arquitectura de red escalable

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, hecho de una colección de redes públicas y privadas interconectadas, tiene una estructura jerárquica en capas para servicios de direccionamiento, designación y conectividad. En cada nivel o capa de la jerarquía, los operadores de red individual mantienen relaciones entre pares con otros operadores en el mismo nivel. 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 pueden duplicarse en diferentes regiones, manteniendo el tráfico de las redes backbone de nivel superior.

Aunque no existe una organización que regule Internet, los operadores de las diferentes redes individuales que proporcionan la conectividad de Internet cooperan para cumplir con los protocolos y estándares aceptados.

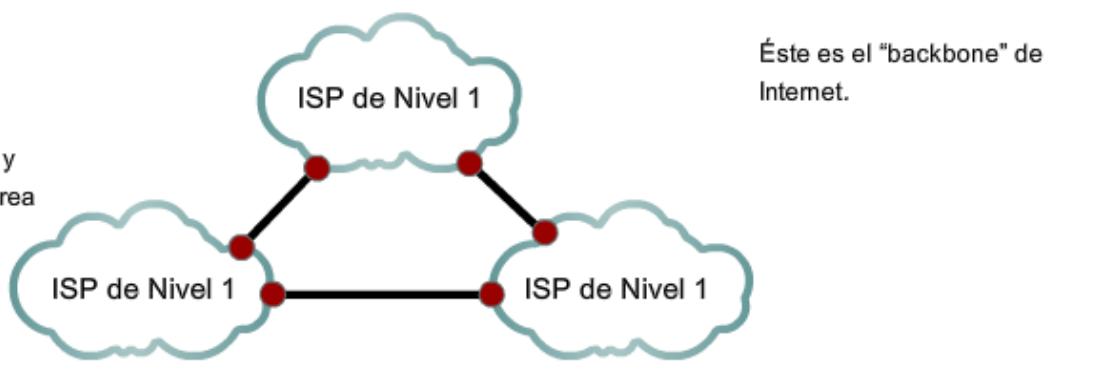
La adherencia a los estándares permite a los fabricantes de hardware y software concentrarse en las mejoras del producto en áreas de rendimiento y capacidad, sabiendo que los nuevos productos pueden integrarse y mejorar la infraestructura existente.

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.

Estructura de Internet: Una red de redes

En el centro de Internet, los ISP de "nivel 1" brindan conexiones nacionales e internacionales. Estos ISP se tratan entre sí como iguales.

Algunos ejemplos son:
Verizon, Sprint, AT&T,
NTT, sistemas de cable y
redes inalámbricas de área
amplia.



Nivel 1

Nivel 2

Nivel 3

Jerárquicos

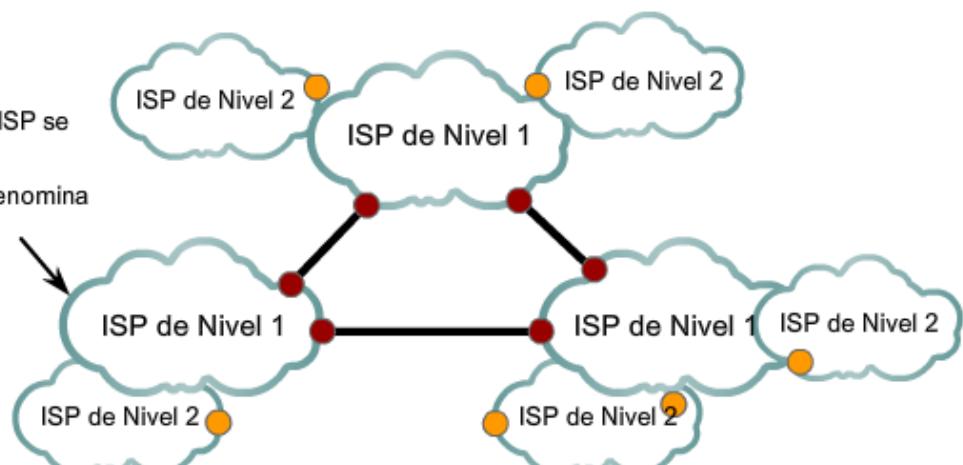
Distribuidos

Pares

Estructura de Internet: Una red de redes

Los ISP de "Nivel 2" son más pequeños y, generalmente, brindan un servicio regional. Los ISP de Nivel 2 generalmente pagan a los ISP de Nivel 1 la conectividad con el resto de Internet.

El punto donde los ISP se interconectan generalmente se denomina "límite".



Nivel 1

Nivel 2

Nivel 3

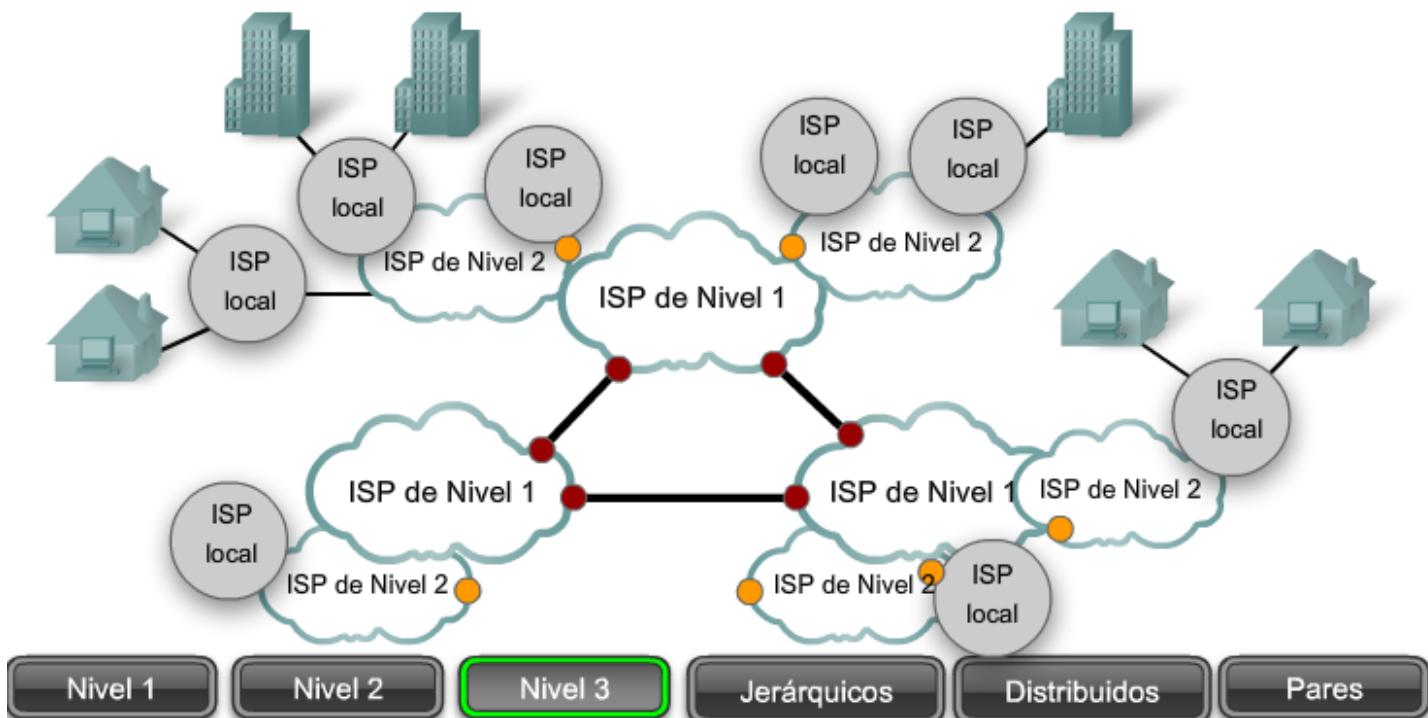
Jerárquicos

Distribuidos

Pares

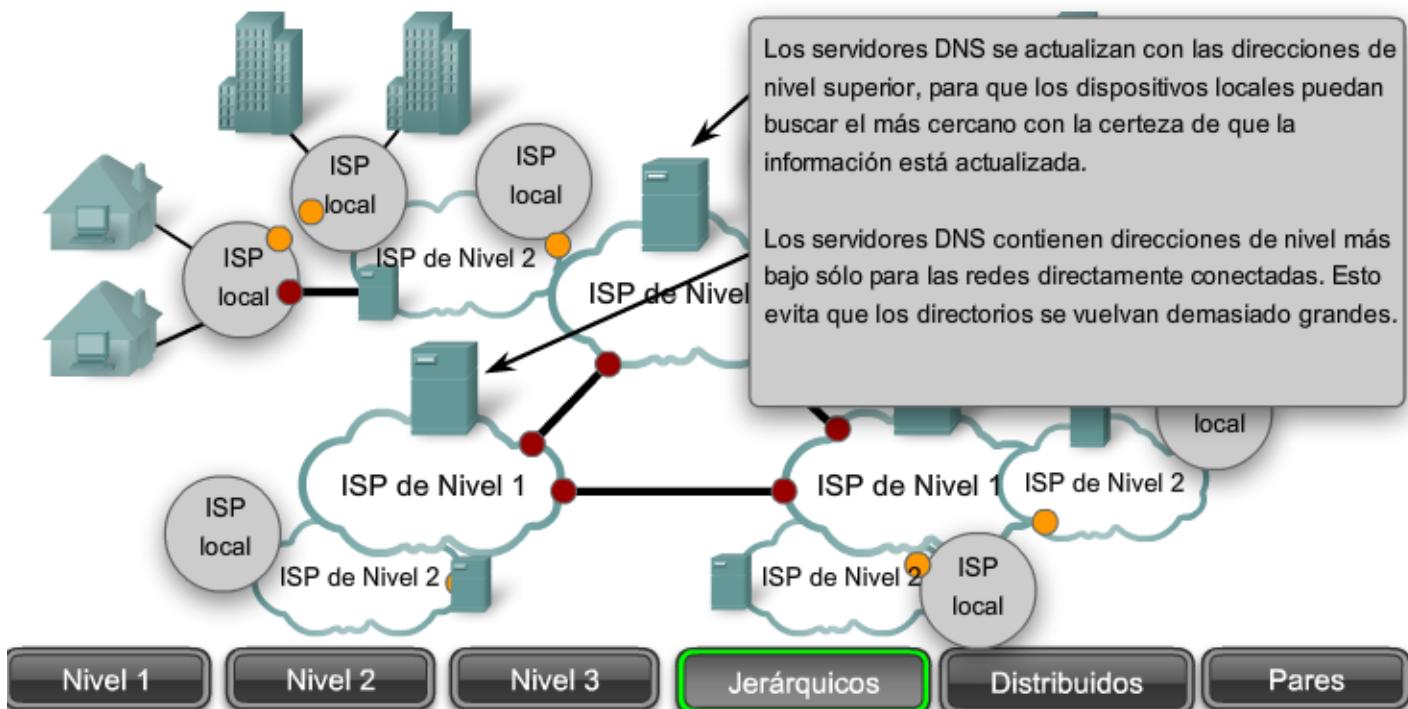
Estructura de Internet: Una red de redes

Los ISP de "Nivel 3" son los proveedores de servicio local directamente a los usuarios finales. Los ISP de Nivel 3, generalmente están conectados a los ISP de Nivel 2 y les pagan a los proveedores de Nivel 2 para acceder a Internet.



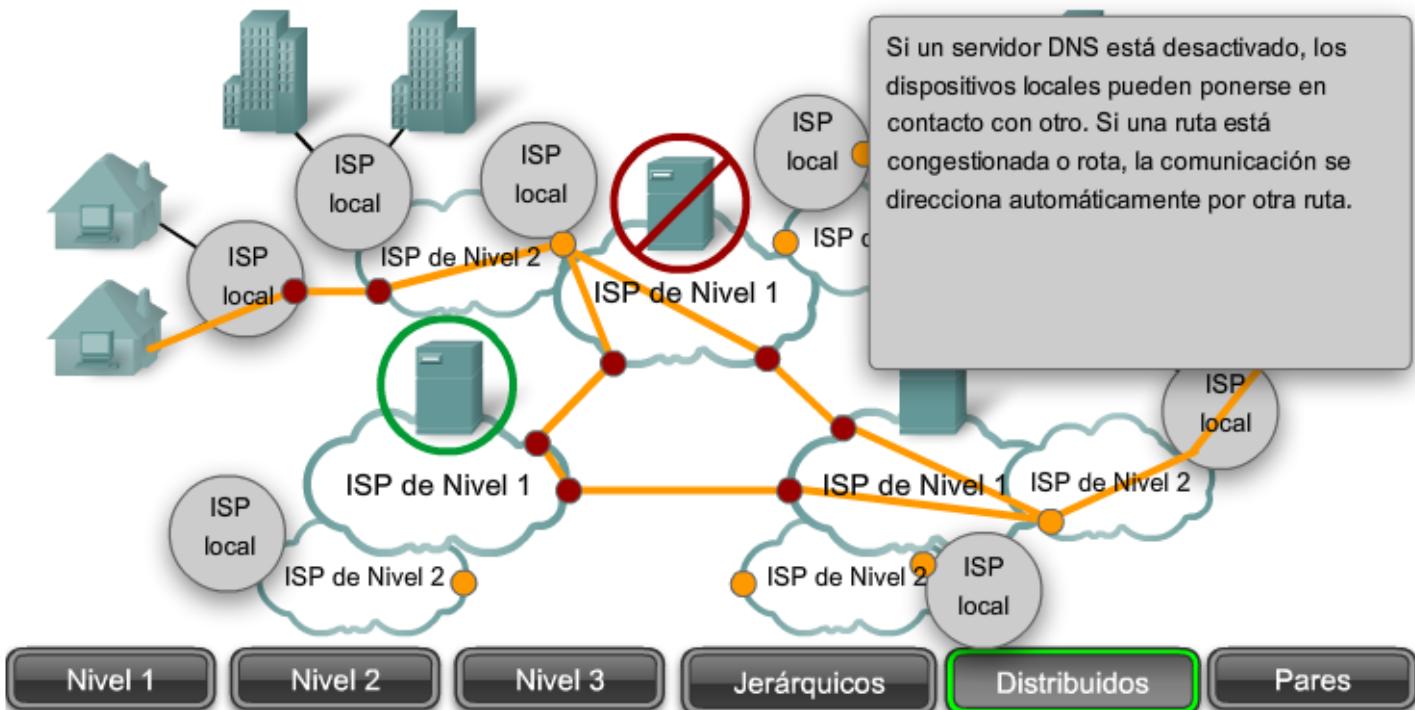
Estructura de Internet: Una red de redes

El Sistema de nombres de dominio (DNS) proporciona un directorio de direcciones jerárquico, es decir, un servidor no tiene que guardar la lista completa de millones de direcciones.



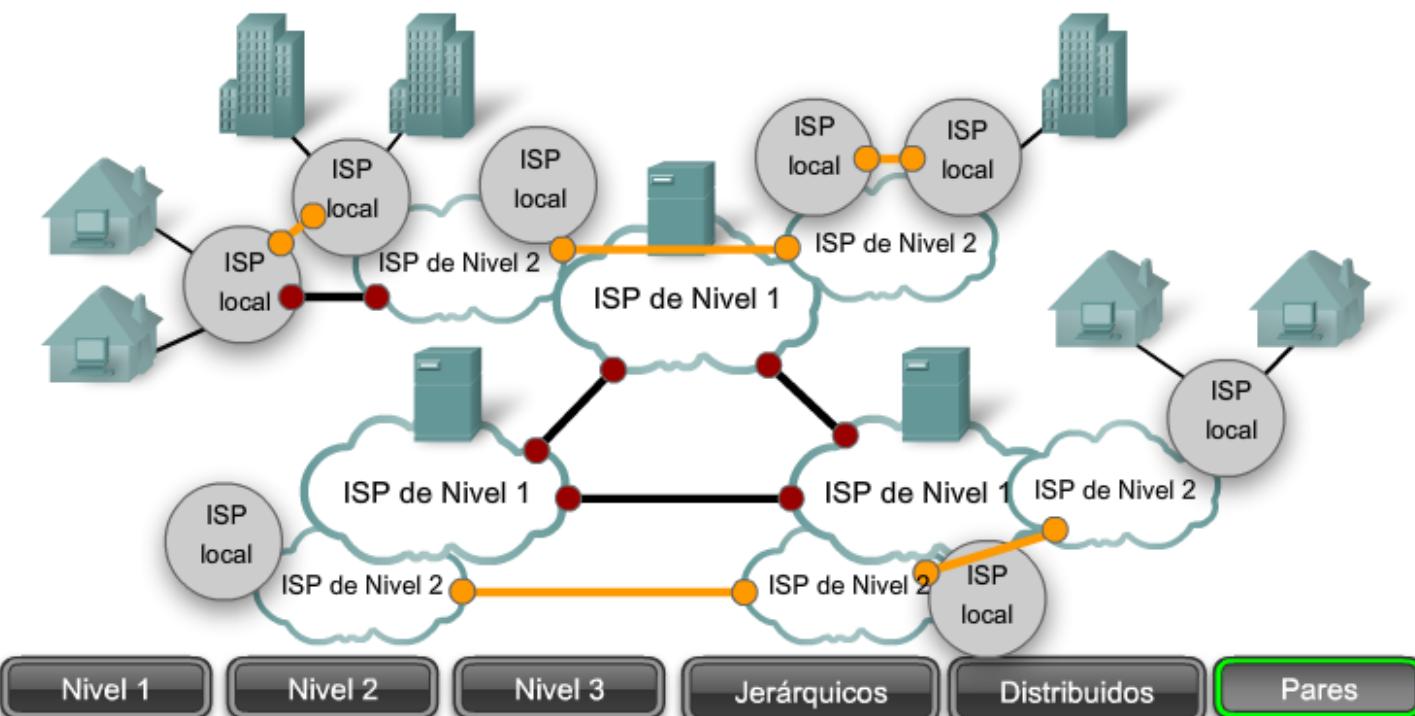
Estructura de Internet: Una red de redes

La naturaleza distribuida de las conexiones y los directorios significa que la comunicación puede evitar los cuellos de botella y las interrupciones. Originalmente diseñado para protegerlo de los ataques militares, el sistema también ha demostrado ser la mejor manera de ofrecer una red civil confiable y escalable.



Estructura de Internet: Una red de redes

Las conexiones de pares entre redes que se encuentran en el mismo nivel brindan conexiones directas y evitan así rutas más largas y la congestión en el backbone.



1.4.4 Previsión de calidad de servicio

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

Las redes también necesitan mecanismos para administrar el tráfico de redes congestionado. La congestión se genera cuando la demanda de recursos de red supera la capacidad disponible.

Si todas las redes tuvieran recursos infinitos no habría necesidad de utilizar mecanismos QoS para garantizar la calidad de servicio. Desafortunadamente, éste no es el caso. Existen algunas restricciones en los recursos de red que no pueden evitarse. Las restricciones incluyen limitaciones tecnológicas, costos y disponibilidad local del servicio de alto ancho de banda. El ancho de banda es la medida de la capacidad de transmisión de datos de la red. Cuando se producen intentos de comunicaciones simultáneas en la red, la demanda de ancho de banda puede exceder su disponibilidad. La solución obvia para esta situación sería aumentar la cantidad de ancho de banda disponible. Pero debido a las restricciones anteriormente mencionadas, esto no siempre es posible.

En la mayoría de los casos, cuando el volumen de paquetes es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos. Los paquetes en cola provocan retrasos. Si el número de paquetes en cola continúa aumentando, las colas de la memoria se llenan y los paquetes se descartan.

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

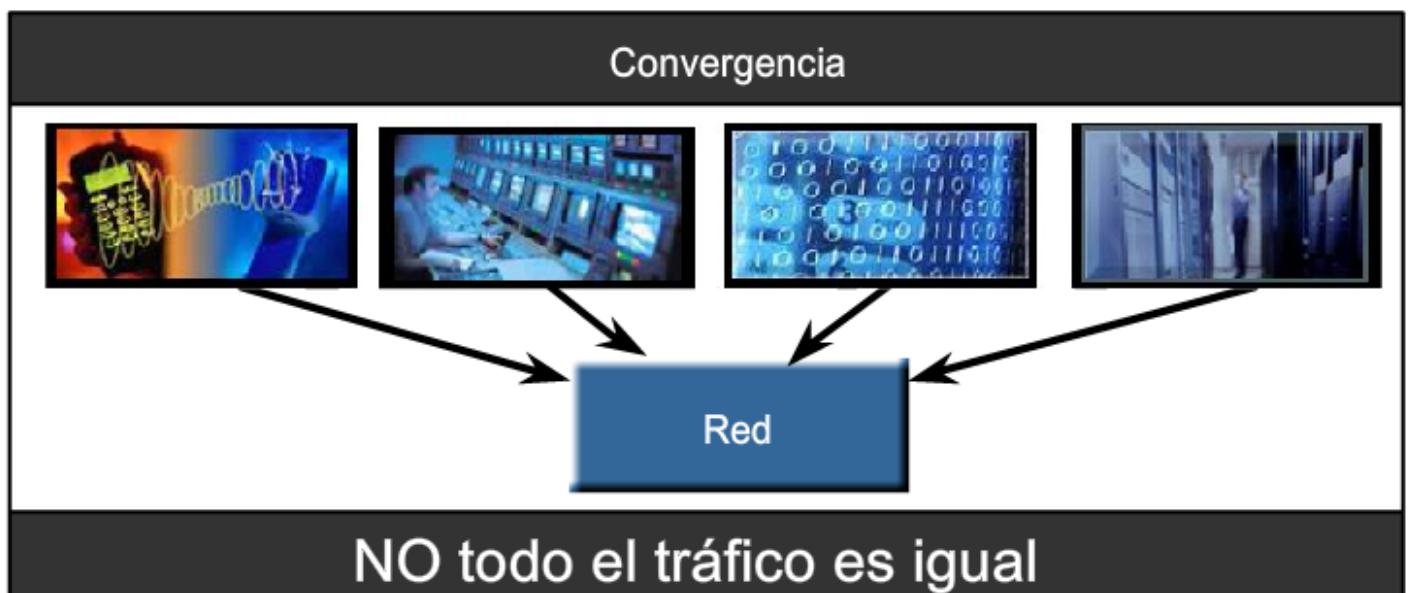
- Contenido Web
- Navegación
 - Compras

Redes convergentes

- Tráfico transaccional
- Procesamiento de pedidos y facturación
 - Inventario y elaboración de informes
 - Contabilidad y elaboración de informes

- Streaming de tráfico
- Video a pedido (VoD)
 - Películas

- Tráfico a granel
- E-mail
 - Copias de respaldo de datos
 - Impresión de archivos



El secreto para llegar a una solución exitosa de calidad de aplicación de extremo a extremo es lograr la Calidad de servicio (QoS) necesaria administrando los parámetros de pérdida de paquetes o de retraso en una red. Por lo tanto, asegurar la QoS requiere de un grupo de técnicas para administrar la utilización de los recursos de red. Para mantener una buena calidad de servicio para las aplicaciones que lo requieren, es necesario priorizar los tipos de paquetes de datos que deben enviarse a expensas de otros tipos de paquetes que puedan retrasarse o descartarse.

Clasificación

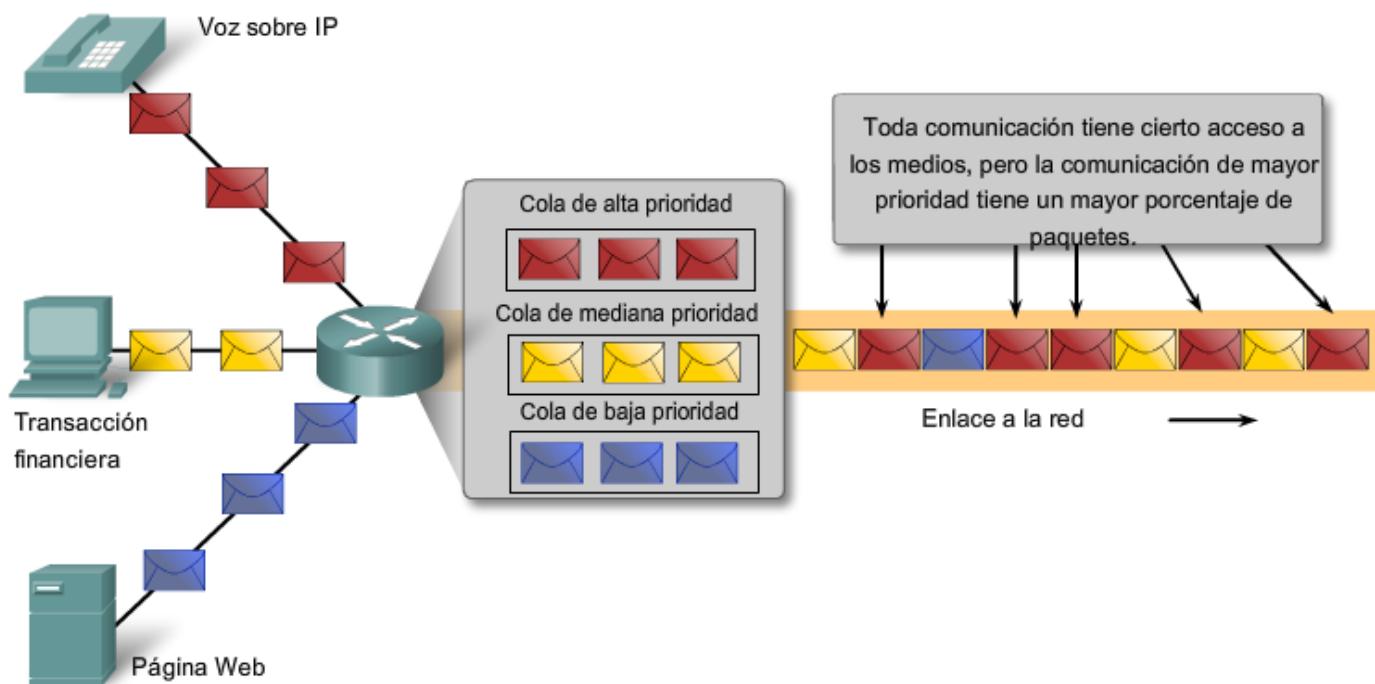
Lo ideal es asignar una prioridad exacta para cada tipo de comunicación. En la actualidad, esto no resulta práctico y posible. Por lo tanto, clasificamos las aplicaciones en categorías según la calidad específica de requisitos de servicios.

Para crear clasificaciones de datos QoS, utilizamos una combinación de características de comunicación y la importancia relativa asignada a la aplicación. Luego incluimos todos los datos en la misma clasificación en base a las mismas reglas. Por ejemplo, la comunicación sensible al tiempo o importante debería clasificarse en forma diferente de la comunicación que puede esperar o es de menor importancia.

Asignación de prioridades

Las características de la información que se comunica también afectan su administración. Por ejemplo, el envío de una película utiliza una importante cantidad de recursos de red cuando se envía en forma continua, sin interrupción. Otros tipos de servicios, los e-mails, por ejemplo, no resultan tan demandantes en la red. En una empresa, el administrador puede decidir asignar la mayor parte de los recursos de red a la película, considerando que ésta es la prioridad para los clientes. El administrador puede decidir que el impacto será mínimo si los usuarios de e-mails tienen que esperar algunos segundos más para que llegue. En otra empresa la calidad del stream de vídeo no es tan importante como la información de control de procesos críticos que operan las máquinas de fabricación.

Uso de colas para priorizar la comunicación



Las colas según los tipos de datos permite que los datos de voz tengan prioridad sobre los datos de transacción, que tienen prioridad sobre los datos de la Web.

Los mecanismos de QoS permiten el establecimiento de estrategias de administración de cola que implementan prioridades para las diferentes clasificaciones de los datos de aplicación. Sin el diseño y la implementación correctos de los mecanismos de QoS, los paquetes de datos se descartan sin considerar las características de la aplicación ni la prioridad. Algunas de las decisiones prioritarias para una organización pueden ser:

- Comunicaciones sensibles al tiempo: aumentan la prioridad por servicios como el teléfono o la distribución de videos.
- Comunicaciones no sensibles al tiempo: disminuyen la prioridad de recuperación de páginas Web o de correos electrónicos.
- Mucha importancia para la empresa: aumenta la prioridad de control de producción o de datos de transacciones comerciales.
- Comunicación indeseable: disminuye la prioridad o bloquea la actividad no deseada como la transferencia de archivos entre pares o el entretenimiento en vivo.

La Calidad de servicio que puede ofrecer una red es un tema vital y, en algunas situaciones, es crucial. Imagine las consecuencias si se descarta una llamada de pedido de ayuda a un centro de emergencias, o si se pierde la señal de control de una pieza automatizada de maquinaria pesada. Una responsabilidad clave para los administradores de red en una organización es establecer una política de calidad de servicio para asegurar que se apliquen los mecanismos para cumplir los objetivos.

La calidad de servicio es importante

| Tipo de comunicación | Sin QoS | Con QoS |
|---|--|---|
| Audio o video streaming |  Imagen entrecortada comienza y se detiene. |  Servicio claro y continuo. |
| Transacciones esenciales | Hora : Precio 02:14:05 \$1.54 Sólo un segundo antes... | Hora : Precio 02:14:04 \$1.52 El precio puede ser mejor. |
| Descarga de páginas Web (generalmente tiene menor prioridad) |  Las páginas Web llegan un poco más tarde... |  Pero el resultado final es el mismo. |

1.4.5 Provisión de seguridad de red

La infraestructura de red, los servicios y los datos contenidos en las computadoras conectadas a la red son activos comerciales y personales muy importantes. Comprometer la integridad de estos activos puede ocasionar serias repercusiones financieras y comerciales.

- Algunas de las consecuencias de la ruptura en la seguridad de la red son:
- interrupciones de red que impiden la realización de comunicaciones y de transacciones, con la consecuente pérdida de negocios,
- mal direccionamiento y pérdida de fondos personales o comerciales,
- propiedad intelectual de la empresa (ideas de investigación, patentes o diseños) que son robados y utilizados por la competencia, o
- detalles de contratos con clientes que se divultan a los competidores o son hechos públicos, generando una pérdida de confianza del mercado de la industria.

La falta de confianza pública en la privacidad, confidencialidad y niveles de integridad de los negocios puede derivar en la pérdida de ventas y, finalmente, en la quiebra de la empresa. Existen dos tipos de cuestiones de seguridad de la red que se deben tratar a fin de evitar serias consecuencias: seguridad de la infraestructura de la red y seguridad del contenido.

Asegurar la infraestructura de la red incluye la protección física de los dispositivos que proporcionan conectividad de red y evitan el acceso no autorizado al software de administración que reside en ellos.

La seguridad del contenido se refiere a la protección de la información contenida en los paquetes que se transmiten en la red y la información almacenada en los dispositivos conectados a ésta. Al transmitir la información en Internet u otra red, los dispositivos y las instalaciones por las que viajan los paquetes desconocen el contenido de los paquetes individuales. Se deben implementar herramientas para proporcionar seguridad al contenido de los mensajes individuales sobre los protocolos subyacentes que rigen la forma en que los paquetes se formatean, direccionan y envían. Debido a que el reensamblaje y la interpretación del contenido se delega a programas que se ejecutan en sistemas individuales de origen y destino, muchos de los protocolos y herramientas de seguridad deben implementarse también en esos sistemas.

Las medidas de seguridad que se deben tomar en una red son:

- evitar la divulgación no autorizada o el robo de información,
- evitar la modificación no autorizada de información, y
- evitar la Denegación de servicio.

Los medios para lograr estos objetivos incluyen:

- garantizar la confidencialidad,
- mantener la integridad de la comunicación, y
- garantizar la disponibilidad.

Garantizar la confidencialidad

La privacidad de los datos se logra permitiendo que lean los datos solamente los receptores autorizados y designados (individuos, procesos o dispositivos).

Un sistema seguro de autenticación de usuarios, el cumplimiento de las contraseñas difíciles de adivinar y el requerimiento a los usuarios para que las cambien frecuentemente ayudan a restringir el acceso a las comunicaciones y a los datos almacenados en los dispositivos adjuntos de la red. Cuando corresponda, el contenido encriptado asegura la confidencialidad y reduce las posibilidades de divulgación no autorizada o robo de información.

Mantener la integridad de las comunicaciones

La integración de datos significa que la información no se alteró durante la transmisión de origen a destino. La integración de datos puede verse comprometida cuando al dañarse la información, ya sea en forma intencional o accidental, antes de que el receptor correspondiente la reciba.

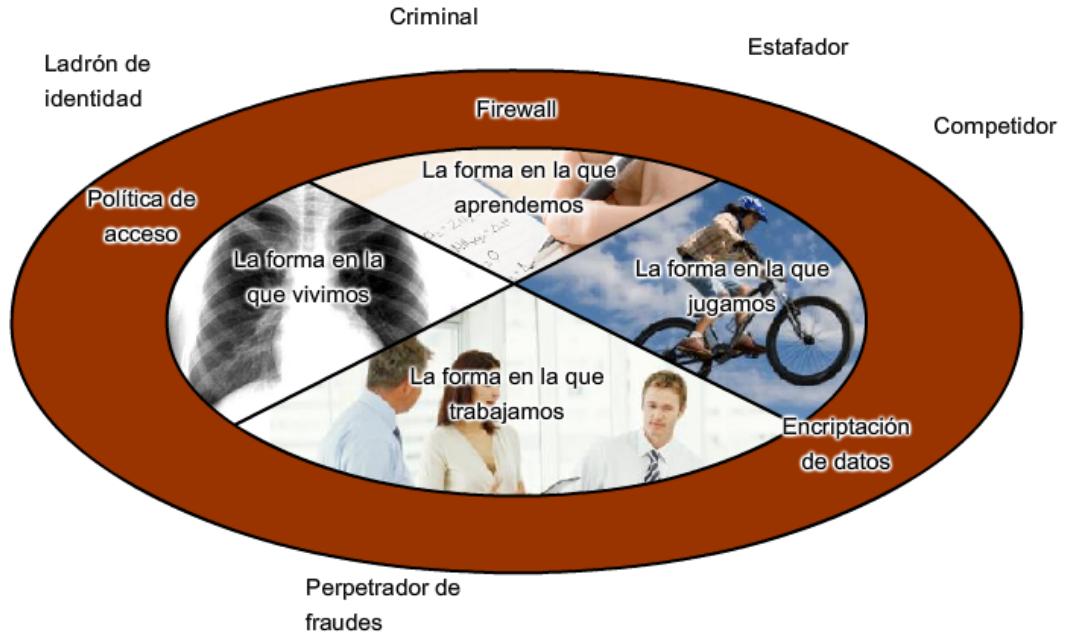
La integridad de origen es la confirmación de que se validó la identidad del emisor. Se compromete la integridad del origen cuando un usuario o dispositivo falsifica su identidad y proporciona información incorrecta al destinatario.

El uso de firmas digitales, algoritmos de hash y mecanismos de checksum son formas de proporcionar integridad de origen y de datos a través de la red para evitar la modificación no autorizada de información

Garantizar disponibilidad

La garantía de confidencialidad e integridad son irrelevantes si los recursos de red están sobrecargados o no disponibles. Disponibilidad significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados. Los recursos pueden no estar disponibles durante un ataque de Denegación de servicio (DoS) o por la propagación de un virus de computadora. Los dispositivos firewall de red, junto con los software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y solidez del sistema para detectar, repeler y resolver esos ataques. La creación de infraestructuras de red completamente redundantes, con pocos puntos de error, puede reducir el impacto de esas amenazas.

El resultado de la implementación de medidas para mejorar tanto la calidad del servicio como la seguridad de las comunicaciones de red es un aumento en la complejidad de la plataforma de red subyacente. Debido a que Internet continúa expandiéndose para ofrecer más y nuevos servicios, su futuro depende de las nuevas y más sólidas arquitecturas en desarrollo que incluyen estas cuatro características: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.



Las comunicaciones y la información que deseamos sean privadas están protegidas de quienes las usan de manera no autorizada.

1.5 TENDENCIAS DE NETWORKING

1.5.1 ¿Hacia donde va todo?

La convergencia de los distintos medios de comunicación en una plataforma de red simple estimula el crecimiento exponencial de las capacidades de red. Existen tres tendencias principales que contribuyen a la futura estructura de las redes de información complejas:

- mayor cantidad de usuarios móviles,
- proliferación de dispositivos aptos para la red, y
- expansión de la gama de servicios.

Usuarios móviles

Con el aumento en la cantidad de trabajadores móviles y en el uso de dispositivos de mano, necesariamente estamos demandando más conectividad móvil a las redes de datos. Esta demanda creó un mercado para servicios inalámbricos que tienen mayor flexibilidad, cobertura y seguridad.

Nuevos y más dispositivos compatibles

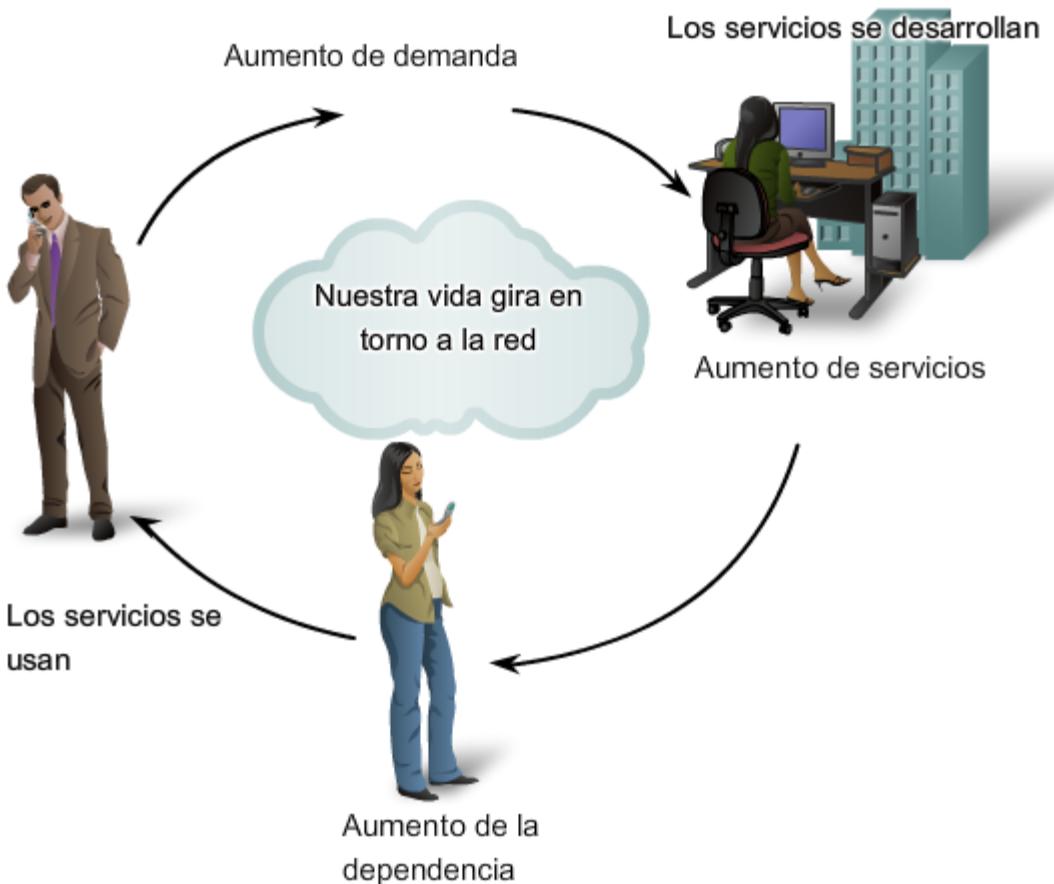
La computadora es sólo uno de los muchos dispositivos en las redes de información actuales. Tenemos un crecimiento de nuevas y emocionantes tecnologías que aprovechan los servicios de red disponibles.

Las funciones realizadas por los teléfonos celulares, asistentes digitales personales (PDA), organizadores y pagers convergen en sencillos dispositivos portátiles con conectividad continua a proveedores de servicios y contenido. Estos dispositivos, alguna vez considerados “juguetes” o elementos de lujo, son ahora una parte integral de la forma en que se comunican las personas. Además de los dispositivos móviles, también tenemos dispositivos de voz sobre IP (VoIP), sistemas de juegos y una gran variedad de dispositivos del hogar y de negocios que se pueden conectar y utilizar servicios de red.

Mayor disponibilidad de servicios

La amplia aceptación de la tecnología y el rápido ritmo de innovación en servicios a través de la red crea una dependencia en espiral. Para cumplir con las demandas del usuario, se presentan nuevos servicios y se mejoran los servicios más viejos. Como los usuarios confían en estos servicios ampliados, desean aún más capacidades. Así, la red crece para respaldar este aumento en la demanda. Las personas dependen de los servicios proporcionados en la red y, en consecuencia, dependen de la disponibilidad y confiabilidad de la infraestructura de red subyacente.

El desafío de mantener el ritmo con una red de usuarios y servicios en continua expansión es responsabilidad de los profesionales de TI y de red capacitados.



Los usuarios móviles dependerán cada vez más de las redes de datos y usarán una variedad de dispositivos.

1.5.2 Oportunidades para la carrera de Networking

Las carreras de networking y Tecnología de Información están en constante crecimiento y evolución, al igual que las tecnologías y los servicios subyacentes. Como las redes crecen en sofisticación, la demanda para las personas con habilidades de networking también continuará creciendo.

Las posiciones de TI tradicionales como programadores, ingenieros de software, administradores de bases de datos y técnicos de red están unidas por nuevos títulos, como por ejemplo: arquitecto de red, diseñador de sitios de e-Commerce, funcionario de seguridad de información y especialista en integración local. Las oportunidades para empresarios de previsión estratégica son ilimitadas.

Incluso los trabajos que no son de TI, como administración de fabricación o diseño de equipamiento médico, ahora requieren de una cantidad significativa de conocimiento acerca del funcionamiento de redes para que resulte exitoso.

Los ejecutivos principales de tecnología en muchas organizaciones grandes enumeran la falta de personal calificado como factor primordial en el retraso de la implementación de nuevos e innovadores servicios.

Como estudiantes de tecnología de red, examinamos los componentes de las redes de datos y los roles que cumplen al habilitar las comunicaciones. Este curso, como otros en la serie de la Academia de Networking, está diseñado para capacitarlo con el conocimiento de redes para crear y administrar estas redes en evolución.

1.6 CAPITULO LABORATORIOS

1.7 RESUMEN

1.7.1 Resumen y revisión

Este capítulo explicó la importancia de las redes de datos como plataforma para admitir la comunicación comercial y las tareas de la vida cotidiana.

Las redes de datos cumplen una función importante en facilitar la comunicación dentro de la red humana global.

Las redes de datos admiten la forma en que vivimos, aprendemos trabajamos y jugamos. Proporcionan la plataforma para los servicios que nos permiten conectarnos, en forma local y global, con nuestra familia y amigos, como así también con nuestro trabajo e intereses. Esta plataforma respalda el uso de textos, gráficos, videos y voz.

Las redes de datos y las redes humanas utilizan procedimientos similares para asegurar que la comunicación llegue al destino en forma precisa y a tiempo. Los acuerdos sobre el idioma, el contenido, la forma y el medio que los humanos generalmente usamos en forma implícita se reflejan en la red de datos.

Los factores que aseguran el envío de los mensajes y la información en la red de datos son los medios de networking que conectan los dispositivos de red y los acuerdos y estándares que rigen su funcionamiento. A medida que crece la demanda para que más personas y dispositivos se comuniquen en un mundo móvil, las tecnologías de red de datos tendrán que adaptarse y desarrollarse.

Las redes convergentes, que transmiten todos los tipos de comunicación (datos, voz y video) en una infraestructura, proporcionan una oportunidad de reducir costos y ofrecer a los usuarios servicios y contenido con muchas características. Sin embargo, el diseño y la administración de redes convergentes requiere de conocimiento y habilidades de networking extensos si todos los servicios deben enviarse a los usuarios según lo esperado.

Diferentes tipos de comunicaciones que fluyen en las redes de datos necesitan tener prioridad para que los datos importantes y sensibles al tiempo tengan el primer uso limitado de recursos de redes.

Integrar la seguridad con las redes de datos es esencial si no queremos que las comunicaciones comerciales, personales y privadas sean interceptadas, robadas o dañadas.

En este capítulo, aprendió a:

- Describir el efecto que tienen las redes en nuestra vida cotidiana.
- Describir la función de las redes de datos en la red humana.
- Identificar los componentes clave de cualquier red de datos.
- Identificar las oportunidades y retos que presentan las redes convergentes.
- Describir las características de las arquitecturas de red: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad.
- Instalar y usar clientes IRC y servidores Wiki.

2 - COMUNICACIÓN A TRAVÉS DE LA RED

2.0 INTRODUCCIÓN DEL CAPÍTULO

2.0.1 Introducción del capítulo

Las redes nos conectan cada vez más. Las personas se comunican en línea desde cualquier lugar. La tecnología confiable y eficiente permite que las redes estén disponibles cuando y donde las necesitemos. A medida que nuestra red humana continúa ampliándose, también debe crecer la plataforma que la conecta y respalda.

En vez de desarrollar sistemas exclusivos e individuales para la entrega de cada nuevo servicio, la industria de networking en su totalidad ha desarrollado los medios para analizar la plataforma existente y mejorarlala progresivamente. Esto asegura que se mantengan las comunicaciones existentes mientras se presentan nuevos servicios económicos y seguros a nivel tecnológico.

En este curso, nos centraremos en estos aspectos de la red de información:

- dispositivos que conforman la red,
- medios que conectan los dispositivos,
- mensajes que se envían a través de la red,
- reglas y procesos que regulan las comunicaciones de red, y
- herramientas y comandos para construir y mantener redes.

El uso de modelos generalmente aceptados que describen funciones de la red es central para el estudio de redes. Estos modelos proporcionan un marco para entender las redes actuales y para facilitar el desarrollo de nuevas tecnologías para admitir futuras necesidades de comunicación.

En este curso, utilizamos estos modelos y las herramientas diseñadas para analizar y simular la funcionalidad de la red. Dos de las herramientas que le permitirán crear e interactuar con redes simuladas son el software Packet Tracer 4.1 y el analizador de protocolos de red Wireshark network.

Este capítulo lo prepara para:

- Describir la estructura de una red, incluso los dispositivos y los medios necesarios para que las comunicaciones sean exitosas.
- Explicar la función de los protocolos en las comunicaciones de red.
- Explicar las ventajas de utilizar un modelo en capas para describir la funcionalidad de la red.
- Describir la función de cada capa en dos modelos de red reconocidos: El modelo TCP/IP y el modelo OSI.
- Describir la importancia de direccionar y nombrar esquemas en las comunicaciones de red.

2.1 Plataforma para las comunicaciones

2.1.1 Elementos de la comunicación

La comunicación comienza con un mensaje o información que se debe enviar desde una persona o dispositivo a otro. Las personas intercambian ideas mediante diversos métodos de comunicación. Todos estos métodos 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.

Considere, por ejemplo, que desea comunicar mediante palabras, ilustraciones y sonidos. Cada uno de estos mensajes puede enviarse a través de una red de datos o de información convirtiéndolos primero en dígitos binarios o bits. Luego, estos bits se codifican en una señal que se puede transmitir por el medio apropiado. En las redes de computadoras, el medio generalmente es un tipo de cable o una transmisión inalámbrica.

El término red en este curso se referirá a datos o redes de información capaces de transportar gran cantidad de diferentes tipos de comunicaciones, que incluye datos informáticos, voz interactiva, video y productos de entretenimiento.



2.1.2 Comunicación de mensajes

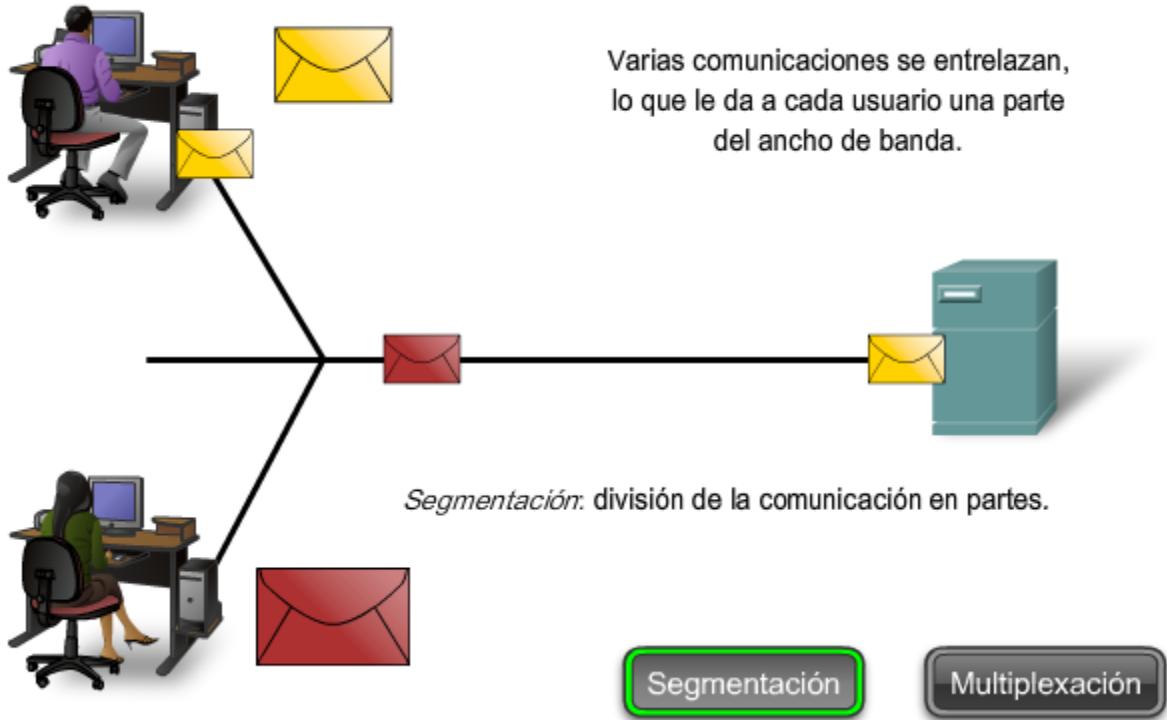
En teoría, una comunicación simple, como un video musical o un e-mail puede enviarse a través de la red desde un origen hacia un destino como un stream de bits masivo y continuo. Si en realidad los mensajes se transmitieron de esta manera, significará que ningún otro dispositivo podrá enviar o recibir mensajes en la misma red mientras esta transferencia de datos está en progreso. Estos grandes streams de datos originarán retrasos importantes. Además, si falló un enlace en la infraestructura de red interconectada durante la transmisión, se perderá todo el mensaje y tendrá que retransmitirse por completo.

Un mejor enfoque para enviar datos a través de la red es dividir los datos en partes más pequeñas y más manejables. La división del stream de datos en partes más pequeñas se denomina segmentación. La segmentación de mensajes tiene dos beneficios principales.

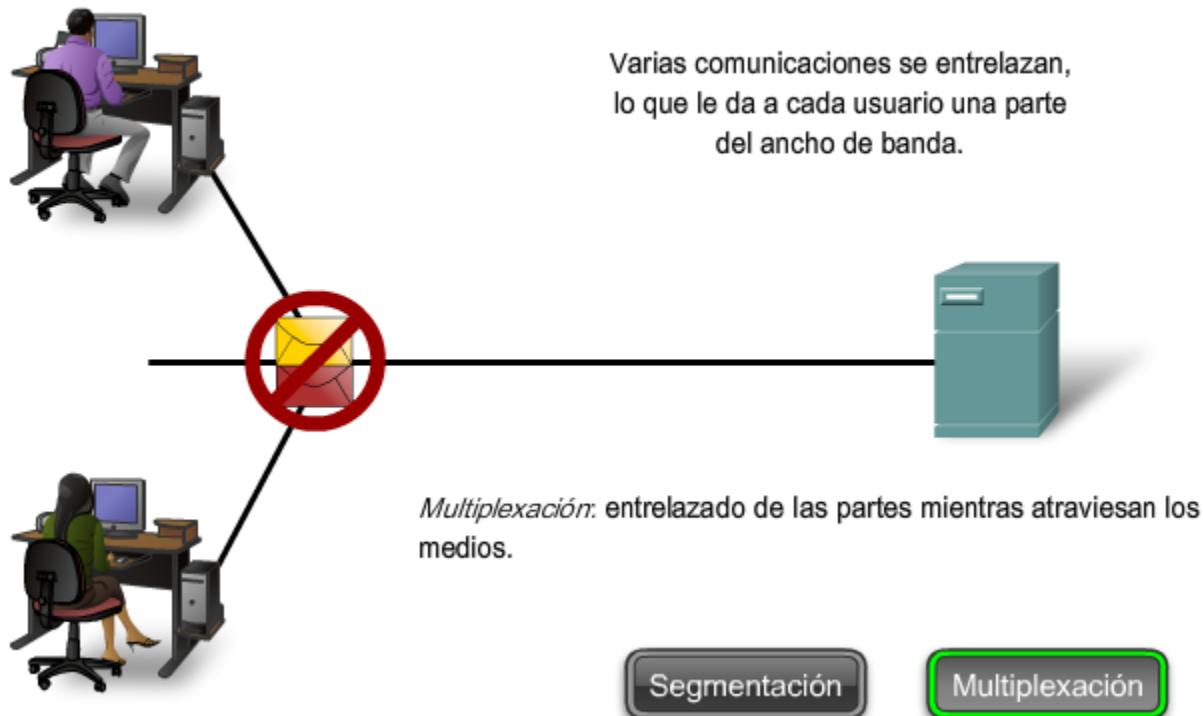
Primero, al enviar partes individuales más pequeñas del origen al destino, se pueden entrelazar diversas conversaciones en la red. El proceso que se utiliza para entrelazar las piezas de conversaciones separadas en la red se denomina multiplexación.

Segundo, 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, sólo se deben retransmitir las partes faltantes.

Comunicación del mensaje



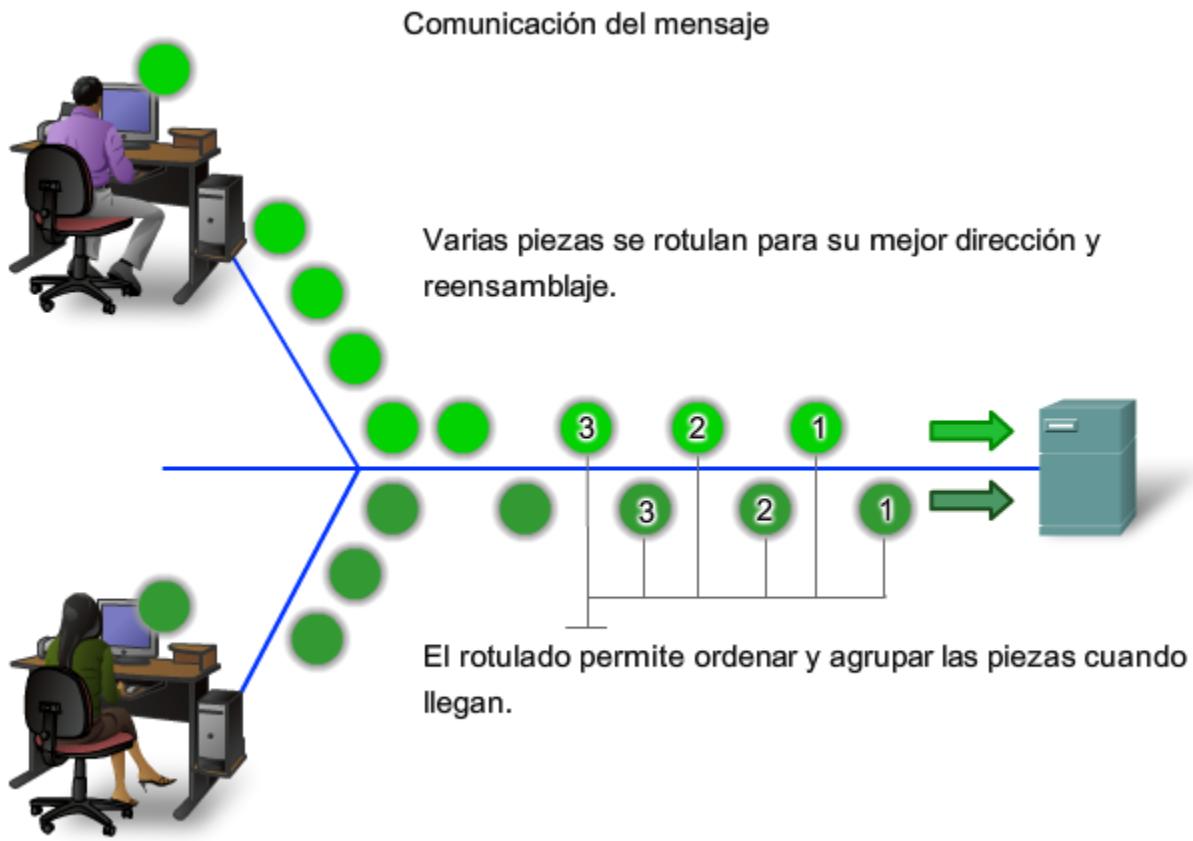
Comunicación del mensaje



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 sólo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir, abrir y leer los cien sobres requerirá mucho tiempo tanto para el remitente 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 puede volverse a ensamblar en el contenido del mensaje original.

Varios tipos de dispositivos en toda la red participan para asegurar que las partes del mensaje lleguen a los destinos de manera confiable.



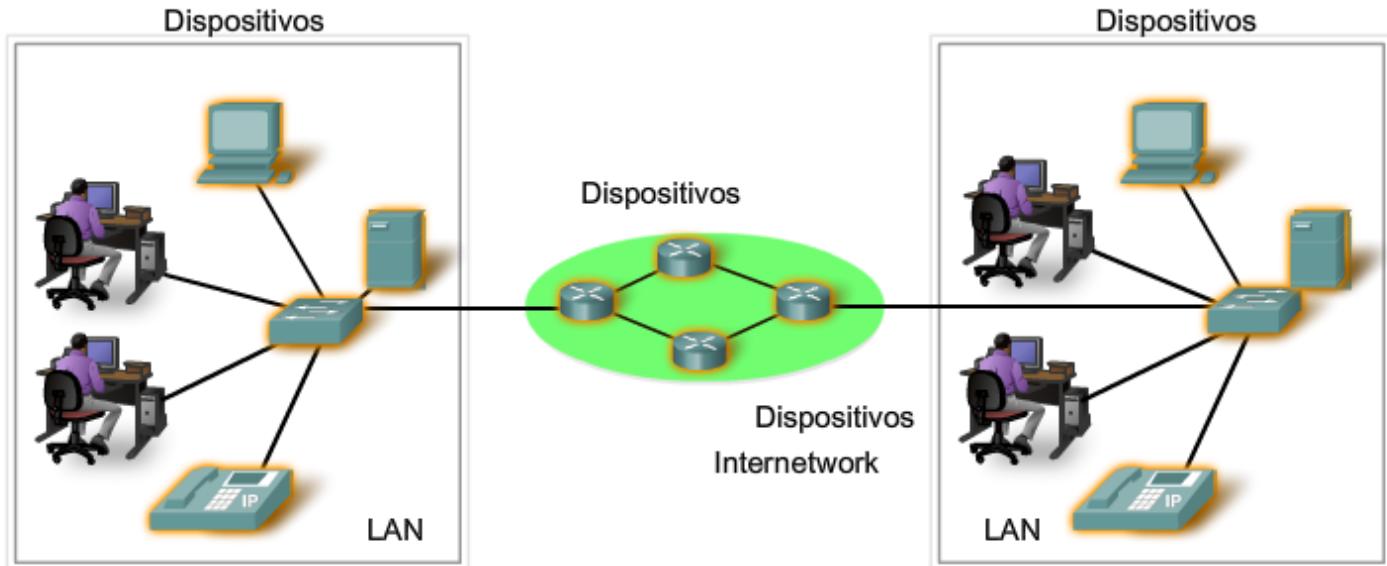
2.1.3 Componentes de la red

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 respalda la red humana. Proporciona el canal estable y confiable por el cual se producen las comunicaciones.

Los dispositivos y los medios son los elementos físicos o hardware de la red. El hardware es generalmente el componente visible de la plataforma de red, como una computadora portátil o personal, un switch, o el cableado que se usa para conectar estos 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 utilizando radio frecuencia invisible u ondas infrarrojas.

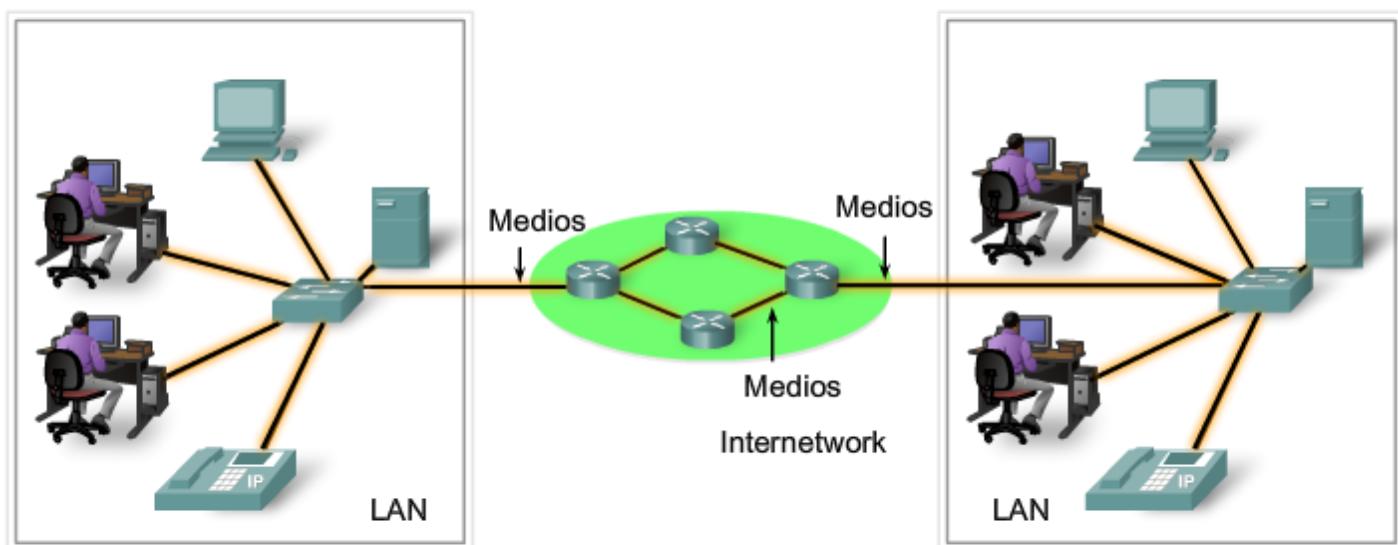
Los servicios y procesos son los programas de comunicación, denominados software, que se ejecutan en los dispositivos conectados a la red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen una gran cantidad de aplicaciones de red comunes que utilizan las personas a diario, como los servicios de e-mail hosting y los servicios de 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.

Las redes usan dispositivos, medios y servicios.



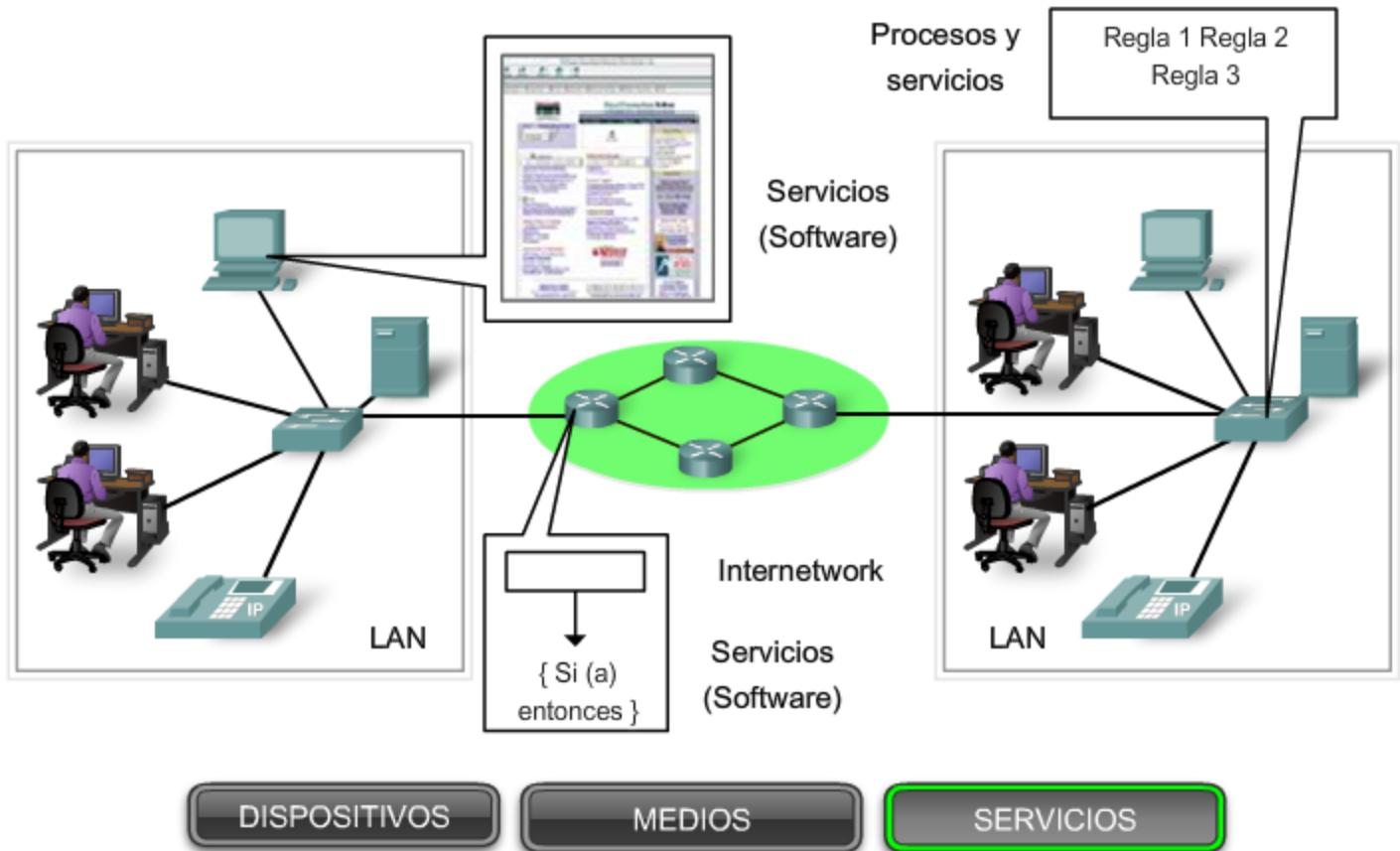
DISPOSITIVOS **MEDIOS** **SERVICIOS**

Haga clic en cada categoría.
Las redes usan dispositivos, medios y servicios.



DISPOSITIVOS **MEDIOS** **SERVICIOS**

Las redes usan dispositivos, medios y servicios.



2.1.4 Dispositivos finales y su rol en la red

Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son:

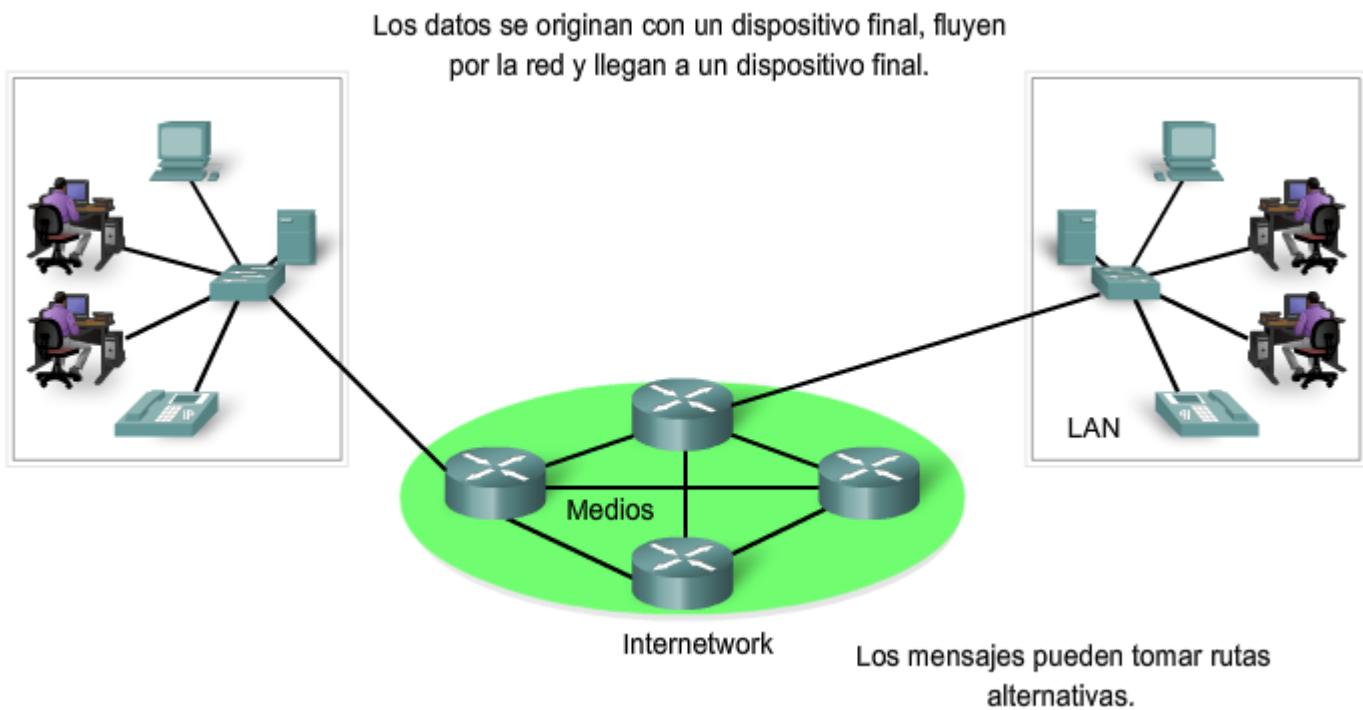
- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

En el contexto de una red, los dispositivos finales se denominan host. Un dispositivo host puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

En las redes modernas, un host puede funcionar como un cliente, como un servidor o como ambos. El software instalado en el host determina qué rol representa en la red.

Los servidores son hosts que tienen software instalado que les permite proporcionar información y servicios, como e-mail o páginas Web, a otros hosts en la red.

Los clientes son hosts que tienen software instalado que les permite solicitar y mostrar la información obtenida del servidor.



2.1.5 Dispositivos intermedios y su rol en la red

Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red. Estos dispositivos 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:

- dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos),
- dispositivos de internetworking (routers),
- servidores de comunicación y módems, y
- dispositivos de seguridad (firewalls).

La administración de datos mientras fluyen a través de la red también es 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:

- regenerar y retransmitir señales de datos,
- mantener información sobre qué rutas existen a través de la red y de la internetwork,
- notificar a otros dispositivos los errores y las fallas de comunicación,
- direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- clasificar y direccionar mensajes según las prioridades de QoS (calidad de servicio), y
- permitir o denegar el flujo de datos en base a configuraciones de seguridad.

2.1.6 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. Estos medios son:

- hilos metálicos dentro de los cables,
- fibras de vidrio o plásticas (cable de fibra óptica), y
- transmisión inalámbrica.

La codificación de señal que se debe realizar para que el mensaje sea transmitido 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.

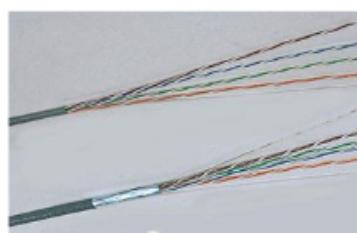
Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- la distancia en la cual el medio puede transportar exitosamente una señal,
- el ambiente en el cual se instalará el medio,
- la cantidad de datos y la velocidad a la que se deben transmitir, y
- el costo del medio y de la instalación.

Medios de red



Cobre



Fibra óptica



Inalámbricos



2.2 LAN (RED DE ÁREA LOCAL), WAN (RED DE ÁREA AMPLIA) E INTERNETWORKS

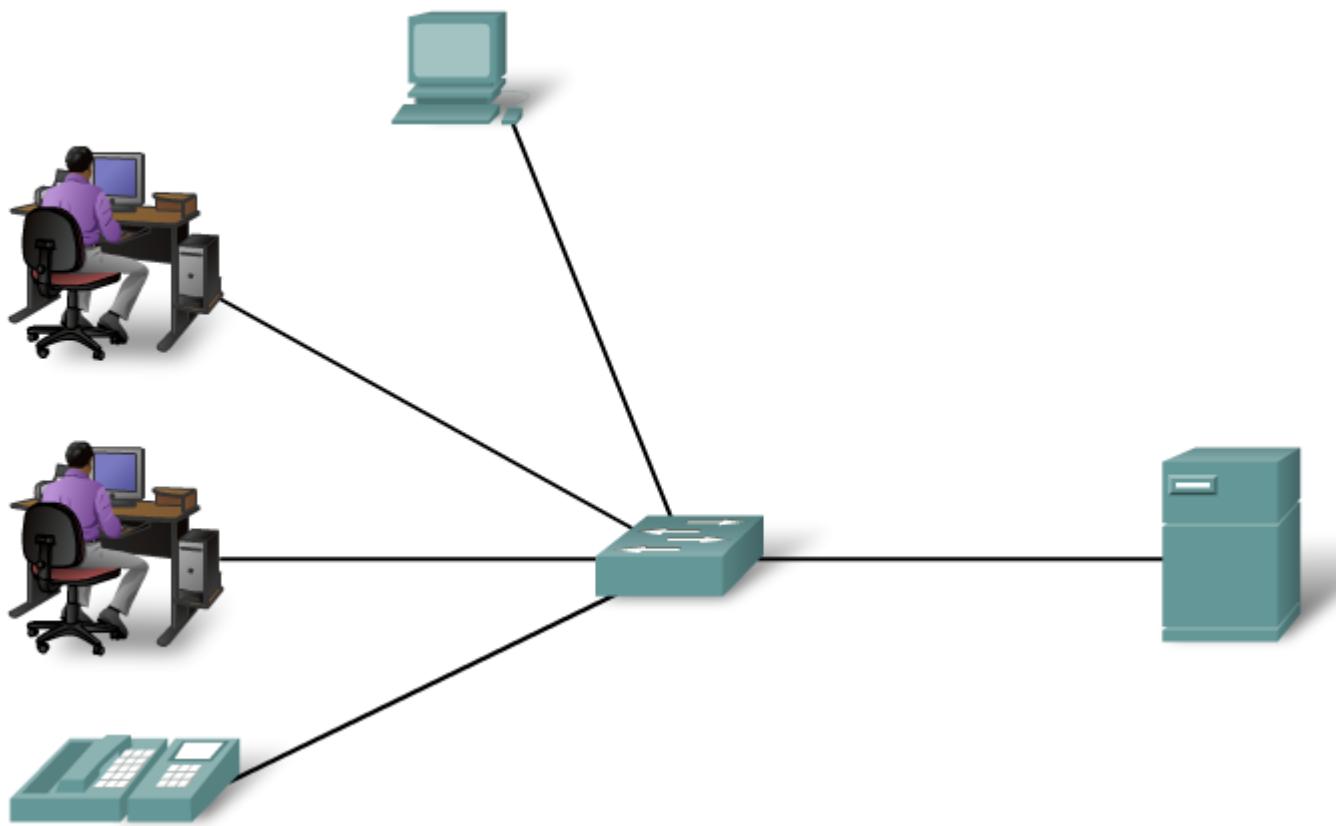
2.2.1 Redes de área local

Las infraestructuras de red pueden variar en gran medida en términos de:

- el tamaño del área cubierta,
- la cantidad de usuarios conectados, y
- la cantidad y tipos de servicios disponibles.

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN). Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

Una red que abastece un hogar, un edificio o un campus es considerada una Red de área local (LAN).



2.2.2 Redes de área amplia

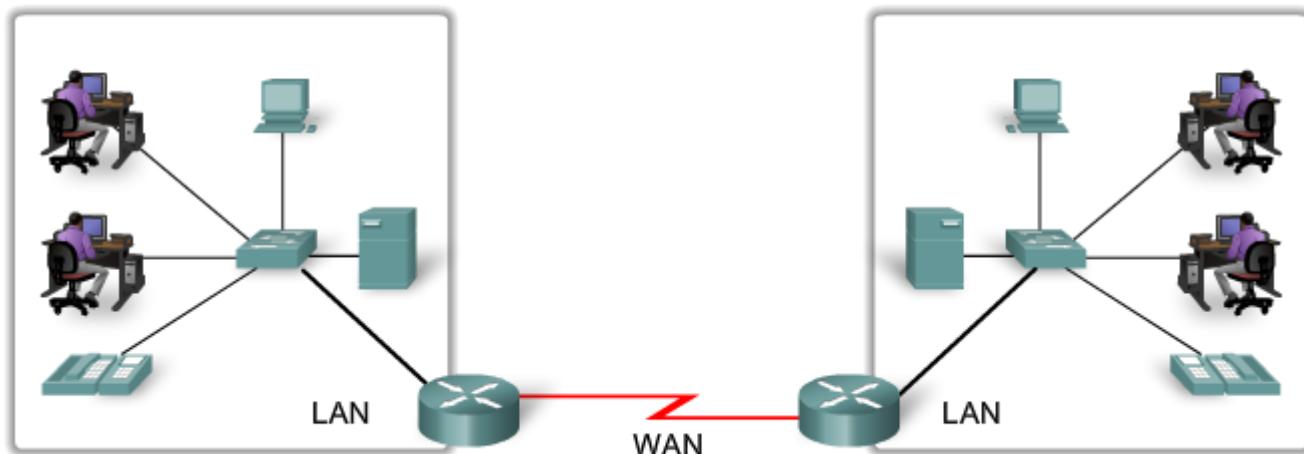
Cuando una compañía o una organización tiene ubicaciones separadas por grandes distancias geográficas, es posible que deba utilizar un proveedor de servicio de telecomunicaciones (TSP) para interconectar las LAN en las distintas ubicaciones. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden abarcar largas distancias. Tradicionalmente, los TSP transportaban las comunicaciones de voz y de datos en redes separadas. Cada vez más, estos proveedores ofrecen a sus subscriptores servicios de red convergente de información.

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP.

Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización.

Las LAN y WAN son de mucha utilidad para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de e-mails, capacitación corporativa y acceso a recursos.

Las LAN separadas por una distancia geográfica están conectadas por una red que se conoce como Red de área extensa (WAN).



2.2.3 Internet: Red de redes

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso u otra red, fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

- enviar un correo electrónico a un amigo en otro país,
- acceder a noticias o productos de un sitio Web,
- obtener un archivo de la computadora de un vecino,
- mensajería instantánea con un pariente de otra ciudad, y
- seguimiento de la actividad de un equipo deportivo favorito a través del teléfono celular.

Internetwork

Una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo. La internetwork más conocida, ampliamente utilizada y a la que accede el público en general es Internet.

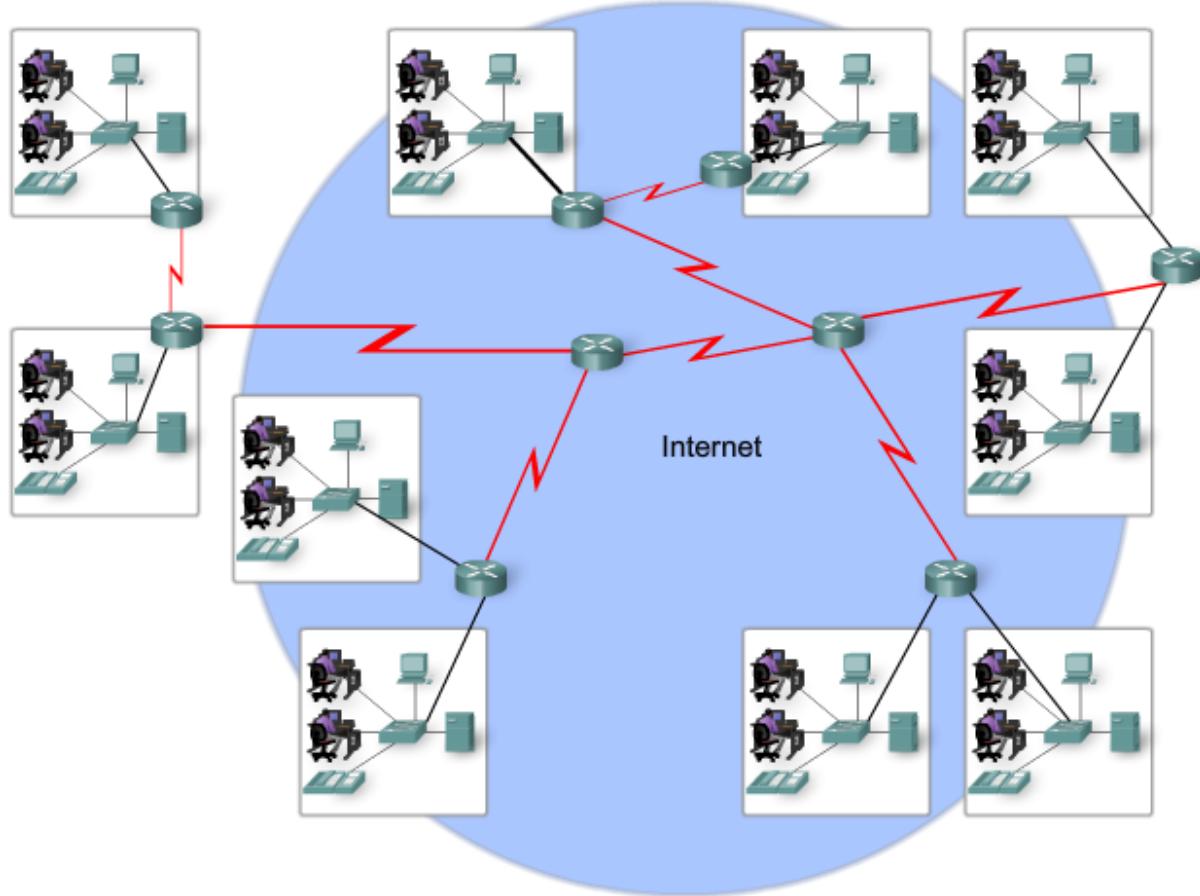
Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación efectiva a través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes.

Intranet

El término intranet se utiliza generalmente para referirse a una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización.

Nota: Es posible que los siguientes términos sean sinónimos: internetwork, red de datos y red. Una conexión de dos o más redes de datos forma una internetwork: una red de redes. También es habitual referirse a una internetwork como una red de datos o simplemente como una red, cuando se consideran las comunicaciones a alto nivel. El uso de los términos depende del contexto y del momento, a veces los términos pueden ser intercambiados.

Las LAN y WAN pueden estar conectadas a internetworks.



2.2.4 Representaciones de red

Cuando se transporta información compleja como la conectividad de red y el funcionamiento de una gran internetwork, es de mucha utilidad utilizar representaciones visuales y gráficos. Como cualquier otro idioma, el lenguaje de interconexión de redes utiliza un grupo común de símbolos para representar los distintos dispositivos finales, los dispositivos de red y los medios. La capacidad de reconocer las representaciones lógicas de los componentes físicos de networking es fundamental para poder visualizar la organización y el funcionamiento de una red. Durante todo este curso y pruebas de laboratorio, aprenderá cómo funcionan estos dispositivos y cómo se realizan con ellos tareas básicas de configuración.

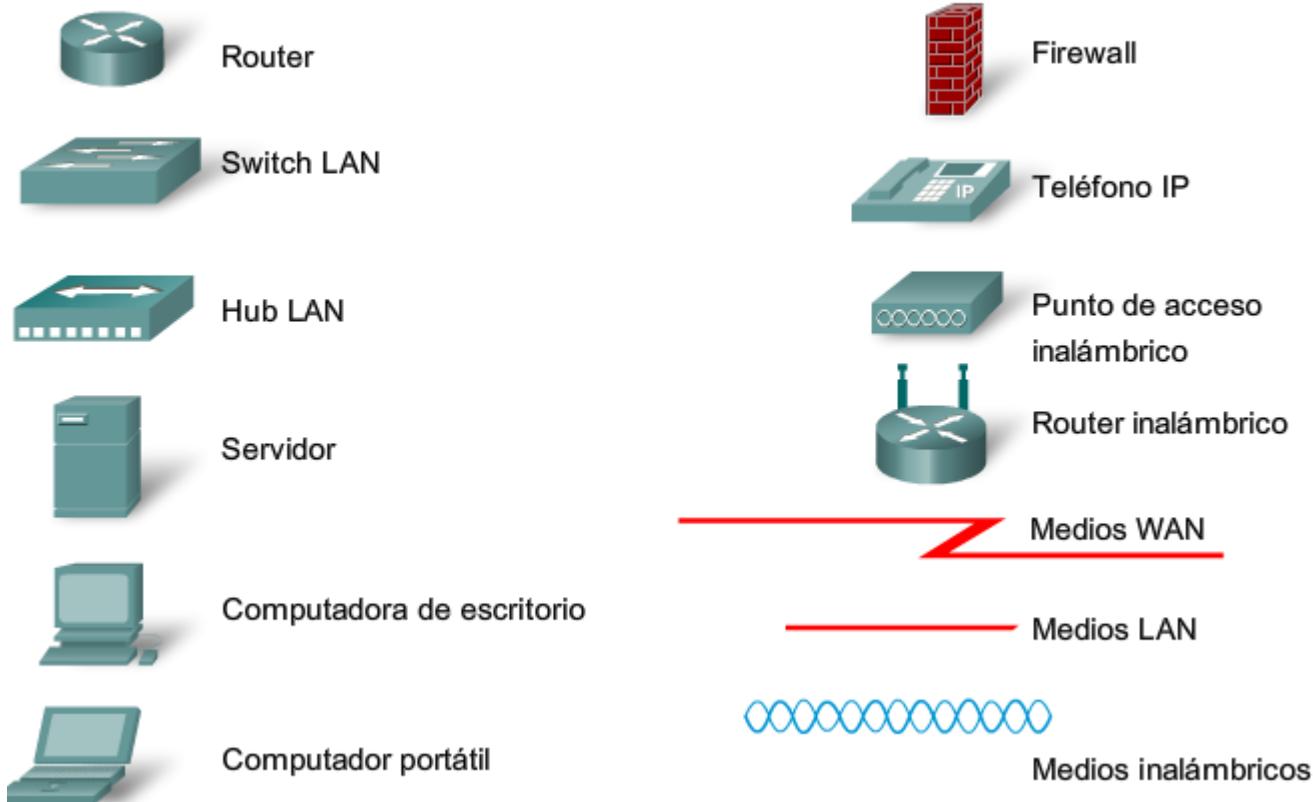
Además de estas representaciones, se utiliza terminología especializada cuando se analiza la manera en que se conectan unos con otros. Algunos términos importantes para recordar son:

Tarjeta de interfaz de red (NIC): una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo host. El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.

Puerto físico: conector o toma en un dispositivo de red en el cual el medio se conecta con un host o con otro dispositivo de red.

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

Símbolos comunes de las redes de datos



2.3 PROTOCOLOS

2.3.1 Reglas que rigen las comunicaciones

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas denominadas protocolos. Estos protocolos son específicos de las características de la conversación. En nuestras comunicaciones personales cotidianas, las reglas que utilizamos para comunicarnos a través de un medio, como el teléfono, no necesariamente son las mismas que los protocolos que se usan en otro medio, como escribir una carta.

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

La comunicación exitosa entre los hosts de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y hardware que está cargado en cada host y dispositivo de red.

Una de las mejores maneras de visualizar de qué manera todos los protocolos interactúan en un host en particular es verlo como un stack. Una stack de protocolos muestra cómo los protocolos individuales de una suite se implementan en el host. Los protocolos se muestran como una jerarquía 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 competen a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz del usuario.

Uso de capas para describir una comunicación cara a cara

Por ejemplo: considere a dos personas comunicándose cara a cara. Como muestra la figura, se pueden utilizar tres capas para describir esta actividad. En la capa inferior, la capa física, puede haber 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 en realidad se pronuncian, el contenido de la comunicación.

Si somos testigos de esta conversación, en realidad no veremos “capas” flotando en el espacio. Es importante entender que el uso de capas es un modelo y, como tal, proporciona una vía para fraccionar convenientemente en partes una tarea compleja y describir cómo funciona.

Los suites de protocolos son conjuntos de reglas que funcionan conjuntamente para ayudar a resolver un problema.

¿Dónde está la cafetería?

Capa de contenido

Suite de protocolo de conversación

1. Use un lenguaje común
2. Espere su turno
3. Señale cuando termine

Capa de reglas



2.3.2 Protocolos de red

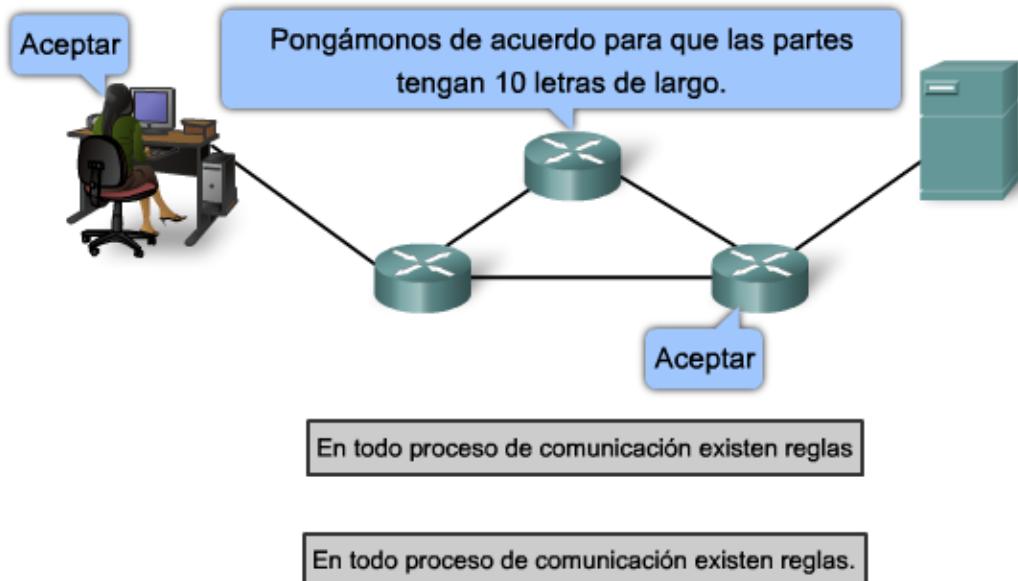
A nivel humano, algunas reglas de comunicación son formales y otras simplemente sobreentendidas o implícitas, basadas en los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, una nueva suite de protocolos debe describir los requerimientos e interacciones precisos.

Las suite de protocolos de networking describen procesos como los siguientes:

- el formato o estructura del mensaje,
- el método por el cual los dispositivos de networking comparten información sobre rutas con otras redes,
- cómo y cuando se pasan los mensajes de error y del sistema entre dispositivos, o
- el inicio y terminación de las sesiones de transferencia de datos.

Los protocolos individuales de una suite de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva. Propietario, en este contexto, significa que una compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos propietarios pueden ser utilizados por distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor propietario.

El rol de los protocolos



Formato o estructura de las piezas de comunicación

Formato

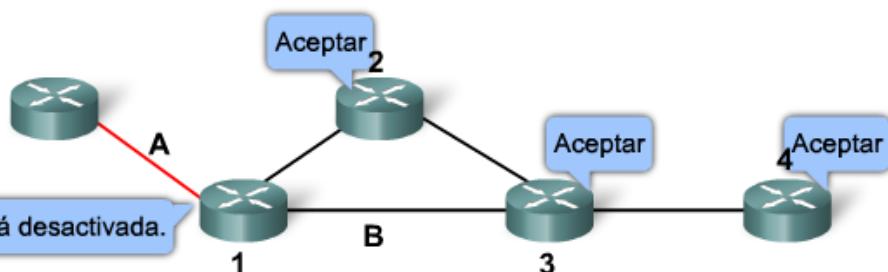
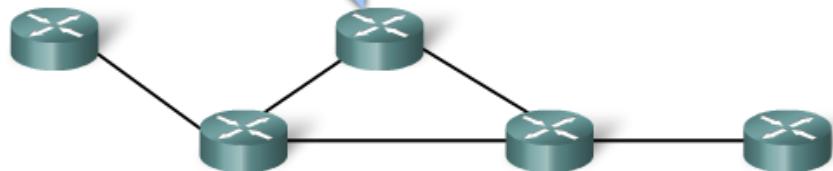
Proceso

Mensajes de error

Terminación

El rol de los protocolos

Convengamos que si una de las rutas está rota, notificaremos a todos los dispositivos conectados.



El proceso por el que los dispositivos de red comparten información sobre trayectos a otras redes

Formato

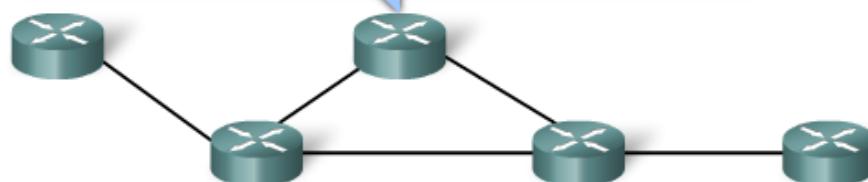
Proceso

Mensajes de error

Terminación

El rol de los protocolos

Convengamos que los mensajes de error tendrán un número de ID único.



Error 1001: La ruta A está desactivada.

Error 1002: La ruta B está lenta.

Cómo y cuándo los mensajes de error y del sistema se pasan entre dispositivos

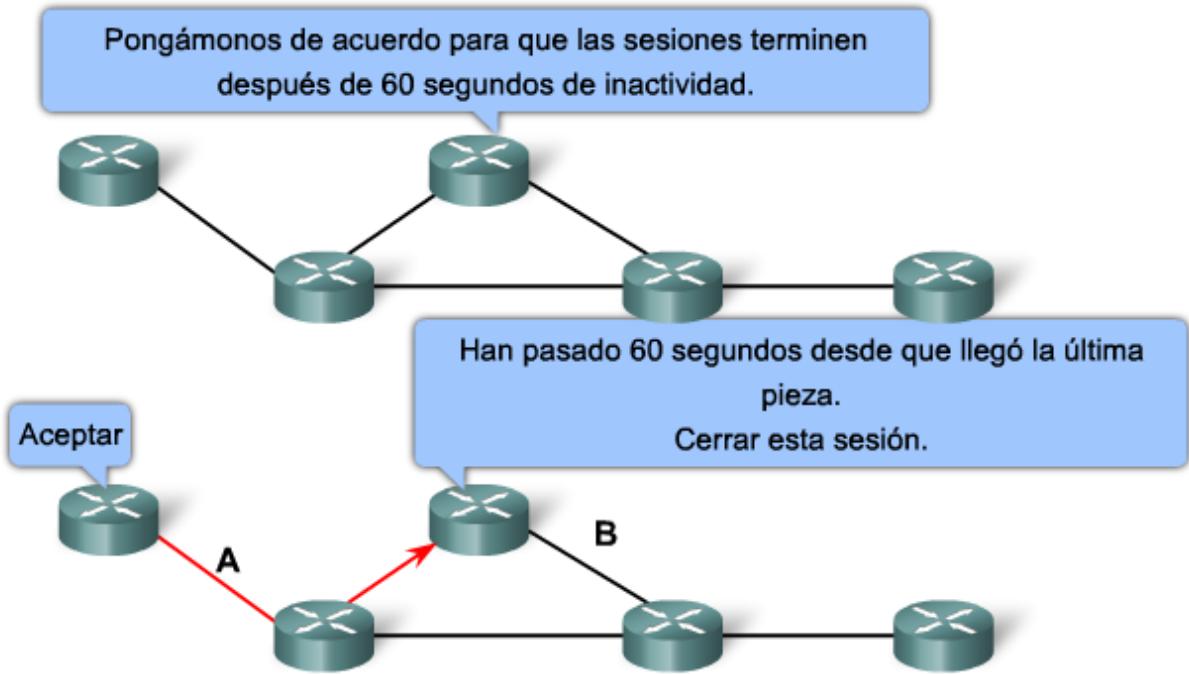
Formato

Proceso

Mensajes de error

Terminación

El rol de los protocolos



La configuración y finalización de las sesiones de transferencia de datos

Formato

Proceso

Mensajes de error

Terminación

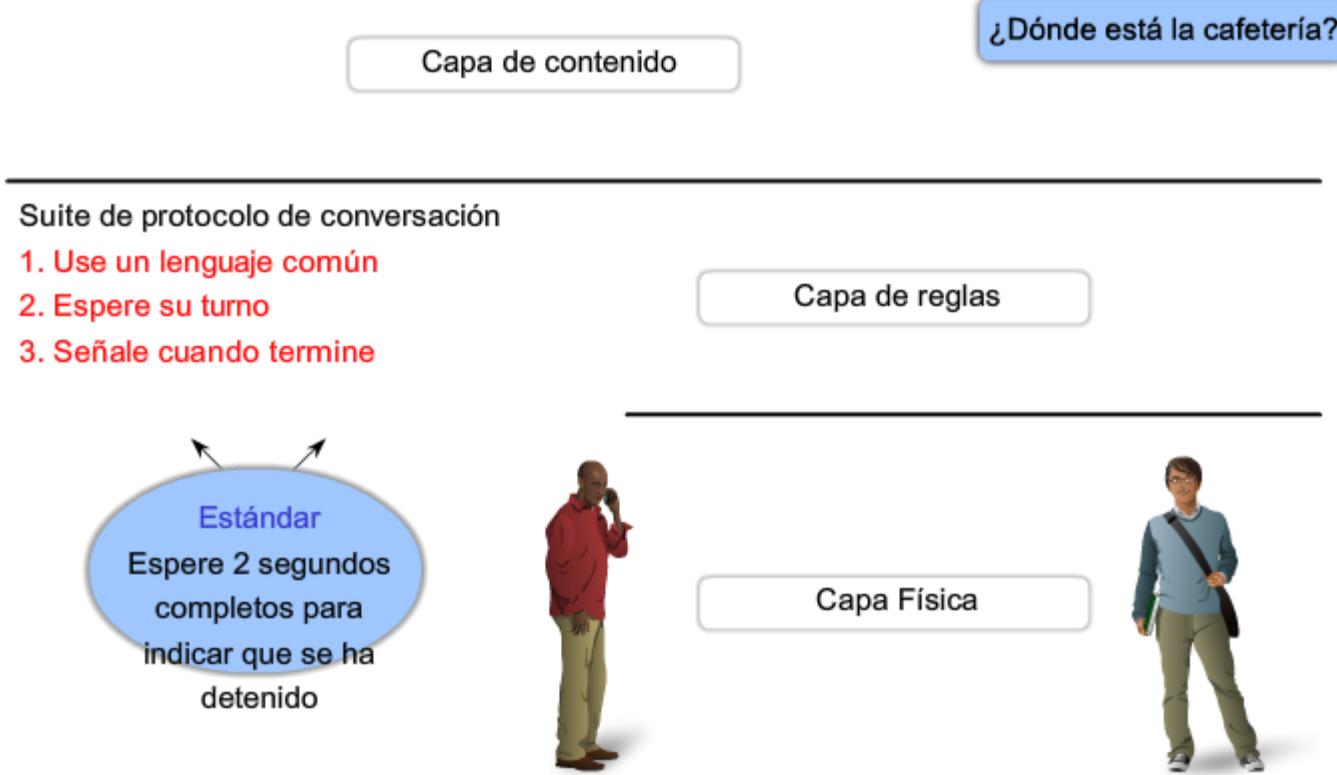
2.3.3 Suites de protocolos y estándares de la industria

Con frecuencia, muchos de los protocolos que comprenden una suite de protocolos aluden a otros protocolos ampliamente utilizados o a estándares de la industria. Un estándar es un proceso o protocolo que ha sido avalado por la industria de networking y ratificado por una organización de estándares, como el Instituto de ingenieros eléctricos y electrónicos (IEEE, Institute of Electrical and Electronics Engineers) o el Grupo de trabajo de ingeniería de Internet (IETF).

El uso de estándares en el desarrollo e implementación de protocolos asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente para lograr comunicaciones eficientes. Si un protocolo no es observado estrictamente por un fabricante en particular, 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 ninguna información.

Los estándares son protocolos y acuerdos muy usados y aceptados.



2.3.4 Interacción de los protocolos

Un ejemplo del uso de una suite de protocolos en comunicaciones de red es la interacción entre un servidor Web y un explorador 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:

Protocolo de transferencia de hipertexto (HTTP) es un protocolo común que regula 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. El protocolo HTTP se basa en otros protocolos para regir de qué manera se transportan los mensajes entre el cliente y el servidor.

Protocolo de transporte:

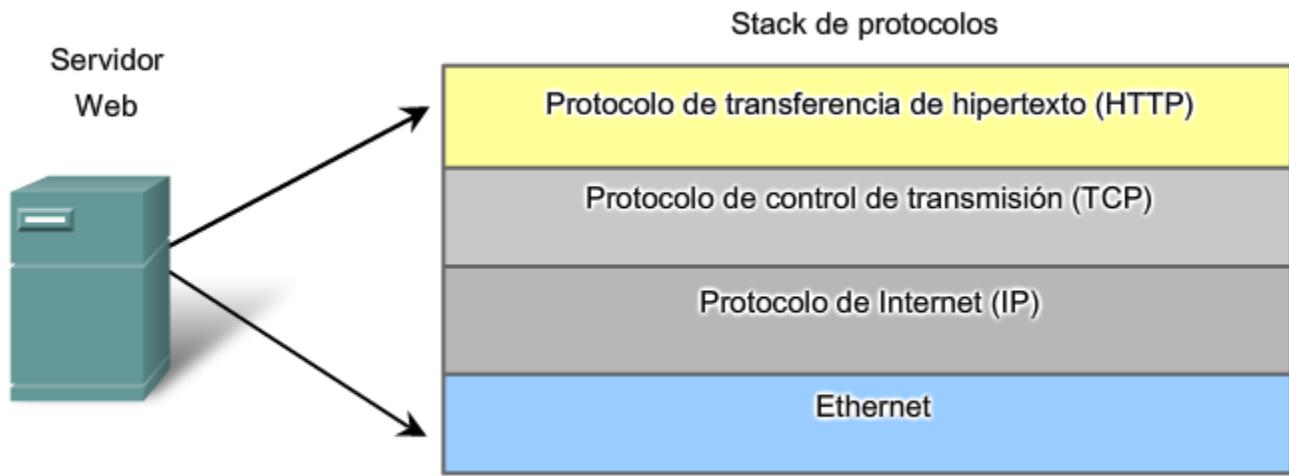
Protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al cliente de destino. También es responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.

Protocolo de internetwork:

El protocolo internetwork más común es el Protocolo de Internet (IP). IP es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia el host de destino.

Protocolos de acceso a la red:

Estos protocolos describen dos funciones principales: administración de enlace de datos y transmisión física de datos en los medios. 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 de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben. Los transceptores de las tarjetas de interfaz de red implementan los estándares apropiados para los medios que se utilizan.



2.3.5 Protocolos independientes de la tecnología

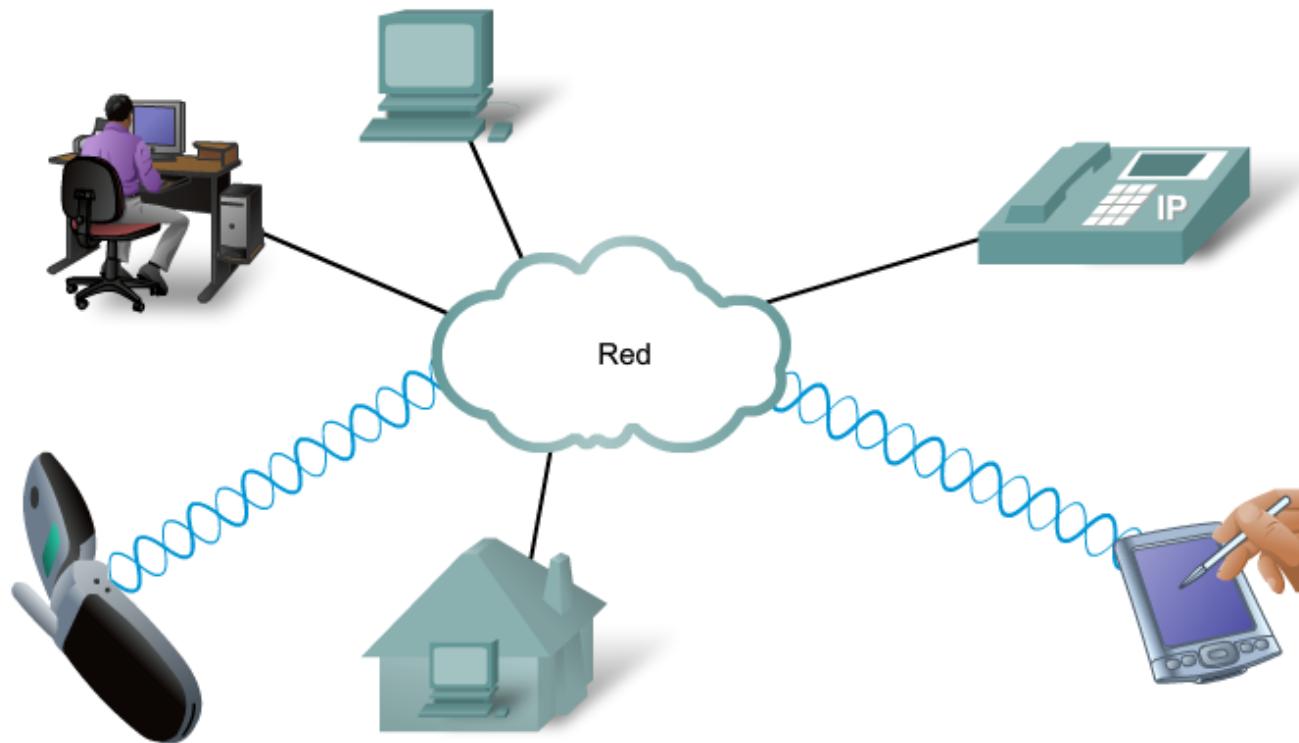
Los protocolos de red describen las funciones que se producen durante las comunicaciones de red. En el ejemplo de la conversación cara a cara, es posible que un protocolo para comunicar establezca que para indicar que la conversación ha finalizado, el emisor debe permanecer en silencio durante dos segundos completos. Sin embargo, este protocolo no especifica cómo el emisor debe permanecer en silencio durante los dos segundos.

Los protocolos generalmente no describen cómo cumplir una función en particular. Al describir solamente qué funciones se requieren de una regla de comunicación en particular pero no cómo realizarlas, es posible que la implementación de un protocolo en particular sea independiente de la tecnología.

En el ejemplo del servidor Web, HTTP no especifica qué lenguaje de programación se utiliza para crear el explorador, qué software de servidor Web se debe utilizar para servir las páginas Web, sobre qué sistema operativo se ejecuta el software o los requisitos necesarios para mostrar el explorador. Tampoco describe cómo detecta errores el servidor, aunque sí describe qué hace el servidor si se produce un error.

Esto significa que una computadora y otros dispositivos, como teléfonos móviles o PDA, pueden acceder a una página Web almacenada en cualquier tipo de servidor Web que utilice cualquier tipo de sistema operativo desde cualquier lugar de Internet.

Muchos tipos de dispositivos pueden comunicarse con los mismos conjuntos de protocolos. Esto se debe a que los protocolos especifican la funcionalidad de red, no la tecnología subyacente para admitir esta funcionalidad.



2.4 USOS DE LOS MODELOS EN CAPAS

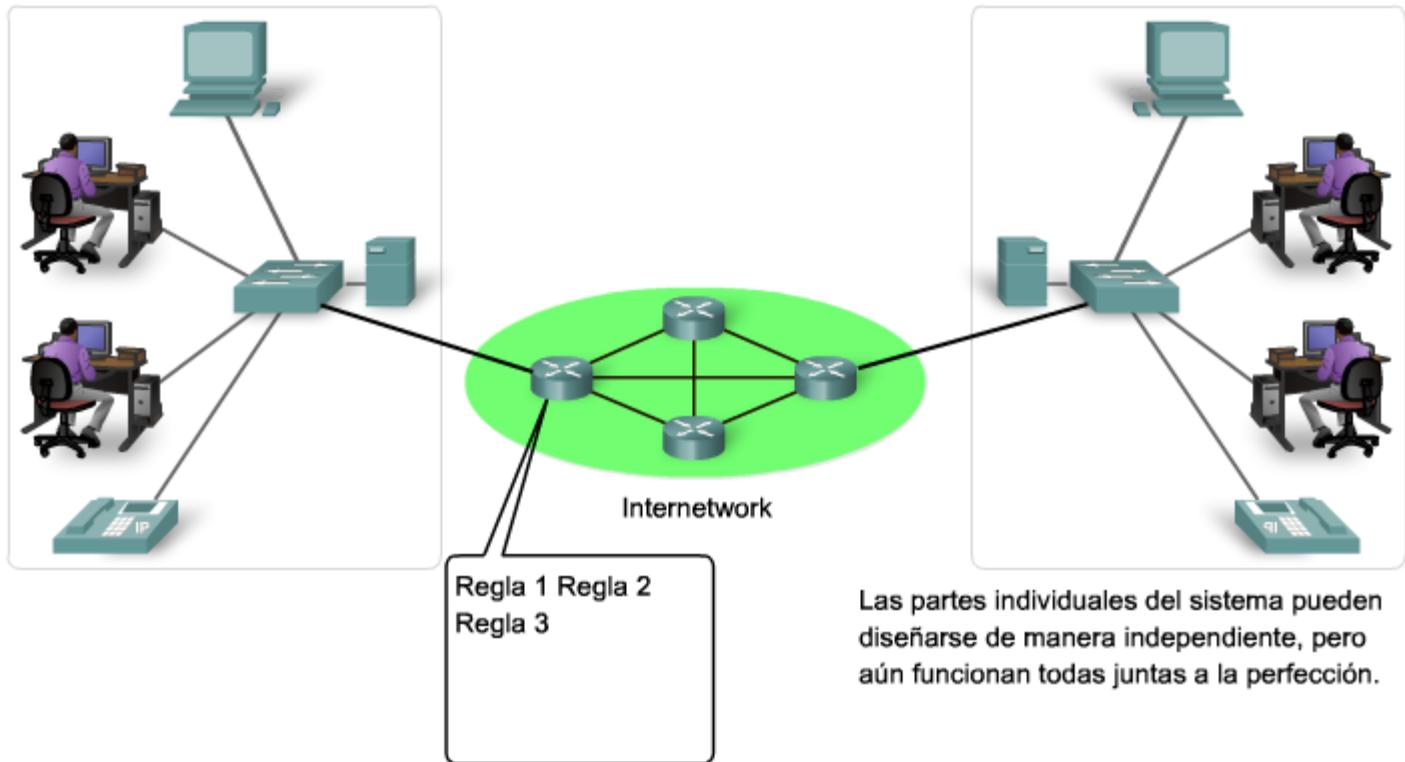
2.4.1 Beneficios del uso de un modelo en capas

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Un modelo en capas muestra el funcionamiento de los protocolos que se produce dentro de cada capa, como así también la interacción de las capas sobre y debajo de él.

Existen beneficios al utilizar un modelo en capas para describir los protocolos de red y el funcionamiento. Uso de un modelo en capas:

- Asiste en el diseño del protocolo, porque los protocolos que operan en una capa específica poseen información definida que van a poner en práctica y una interfaz definida según las capas por encima y por debajo.
- 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 red.

El uso de un modelo en capas ayuda en el diseño de redes complejas, multiuso y de diversos fabricantes.



2.4.2 Modelos de protocolos y referencias

Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

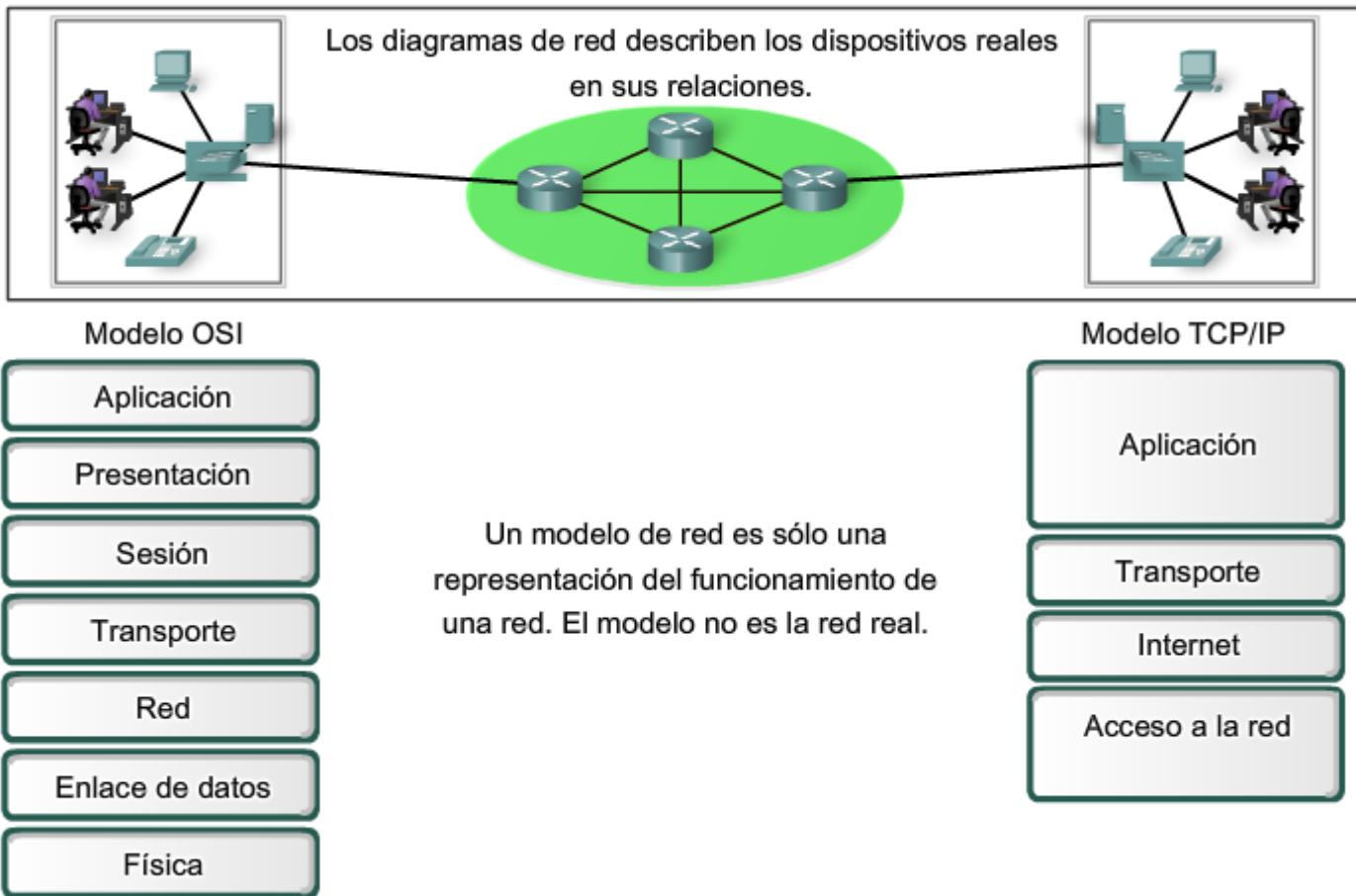
Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. 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 propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

Aunque los modelos TCP/IP y OSI son los modelos principales que se utilizan cuando se analiza la funcionalidad de red, los diseñadores de protocolos de red, servicios o dispositivos 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.

Los modelos proporcionan un guía



2.4.3 Modelo TCP/IP

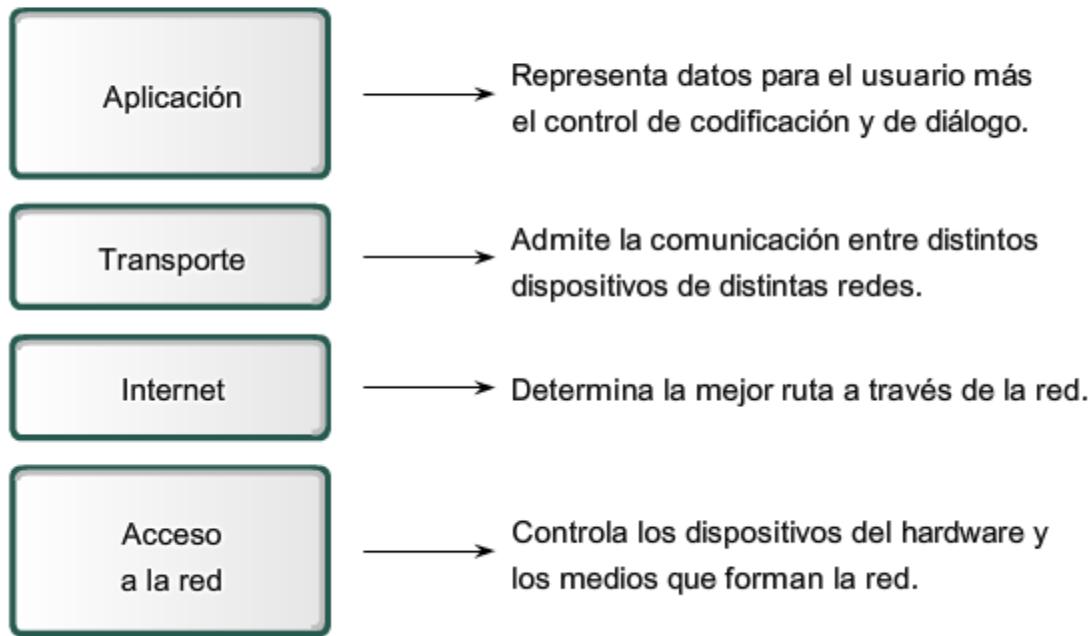
El primer modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca 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 documentos disponibles al público. Estos documentos se denominan *Solicitudes de comentarios* (RFCs). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC (*Solicitudes de comentarios*) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF).

Modelo TCP/IP

Modelo TCP/IP



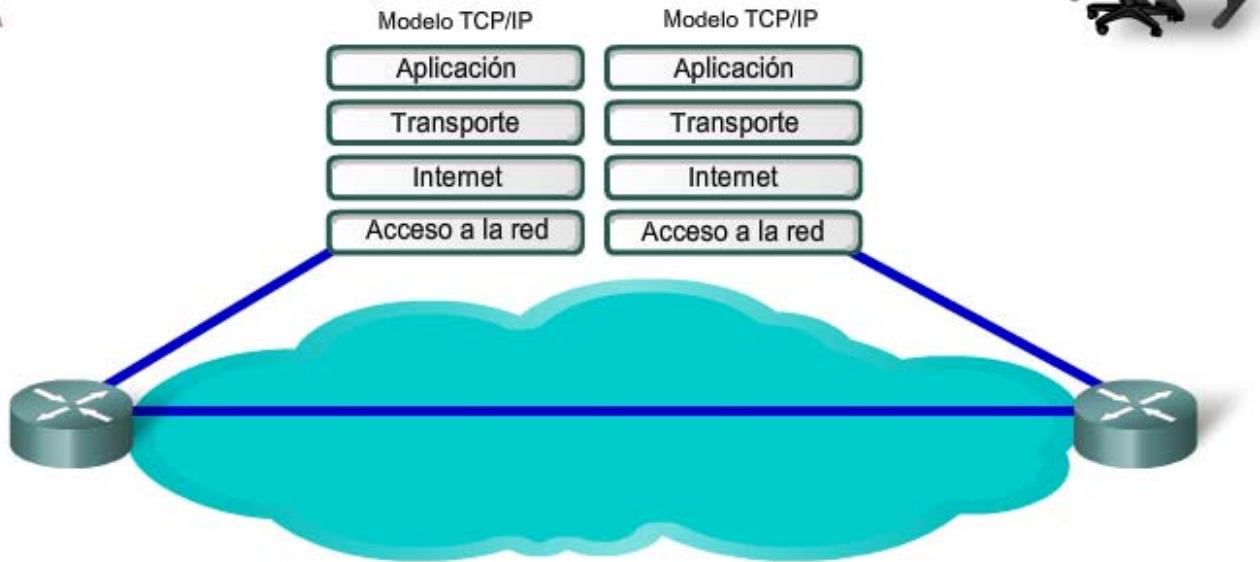
2.4.4 Proceso de comunicación

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Esos protocolos, que se implementan tanto en el host emisor como en el receptor, interactúan para proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye estos pasos:

1. Creación de datos a nivel de la capa de aplicación del dispositivo final origen.
2. Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.
3. Generación de los datos sobre el medio en la capa de acceso a la red de la stack.
4. Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.
5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
6. Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.
7. Traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

Un mensaje sin modificaciones viaja a través de la red



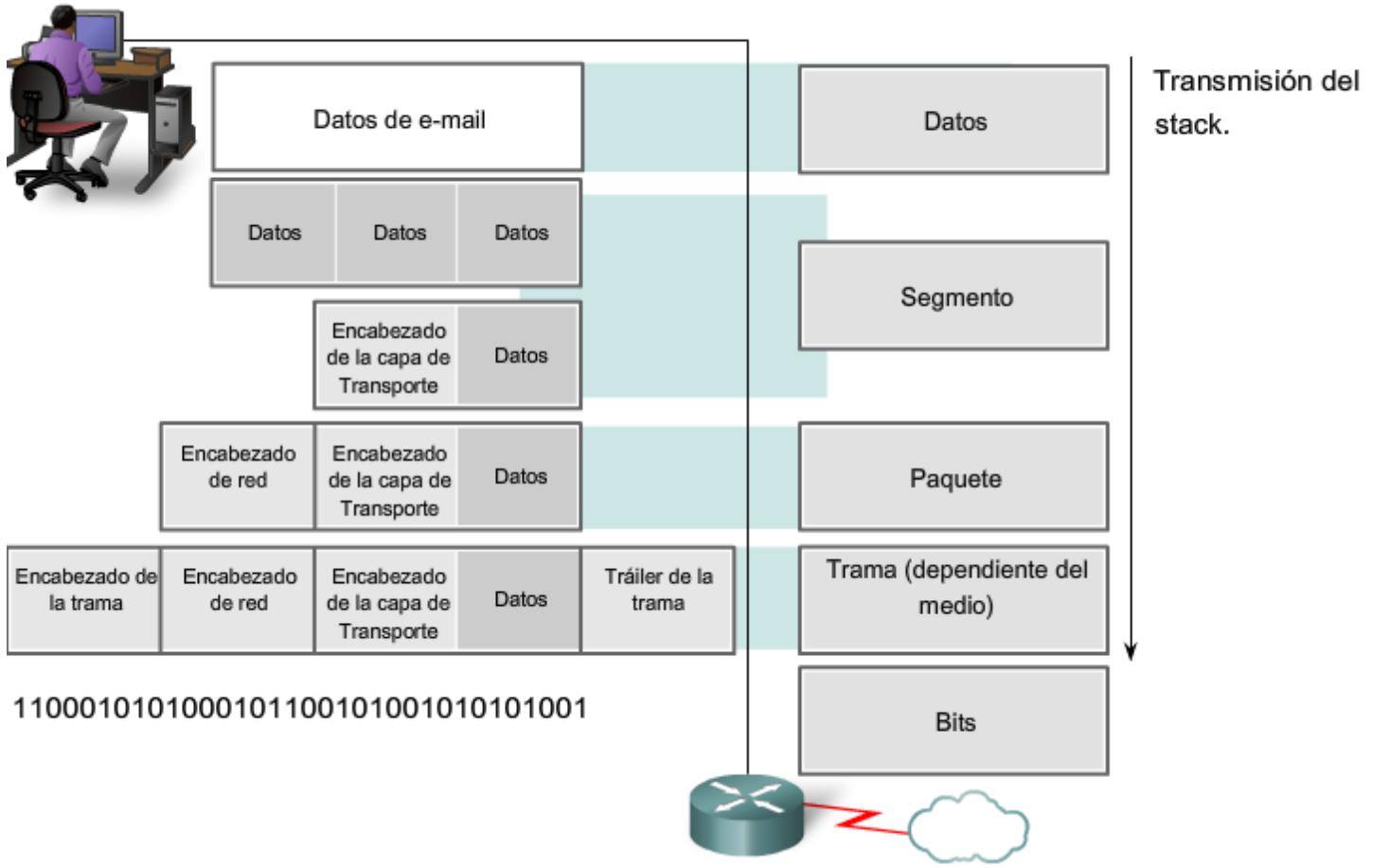
2.4.5 Unidad de dato del protocolo y encapsulación

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 sección 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 su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite TCP/IP.

- Datos: el término general para las PDU que se utilizan en la capa de aplicación.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de Internetwork.
- Trama: PDU de la capa de acceso a la red.
- Bits: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.

Encapsulación



2.4.6 Proceso de envío y recepción

Cuando se envían mensajes en una red, el stack del protocolo de un host funciona desde arriba hacia abajo. 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.

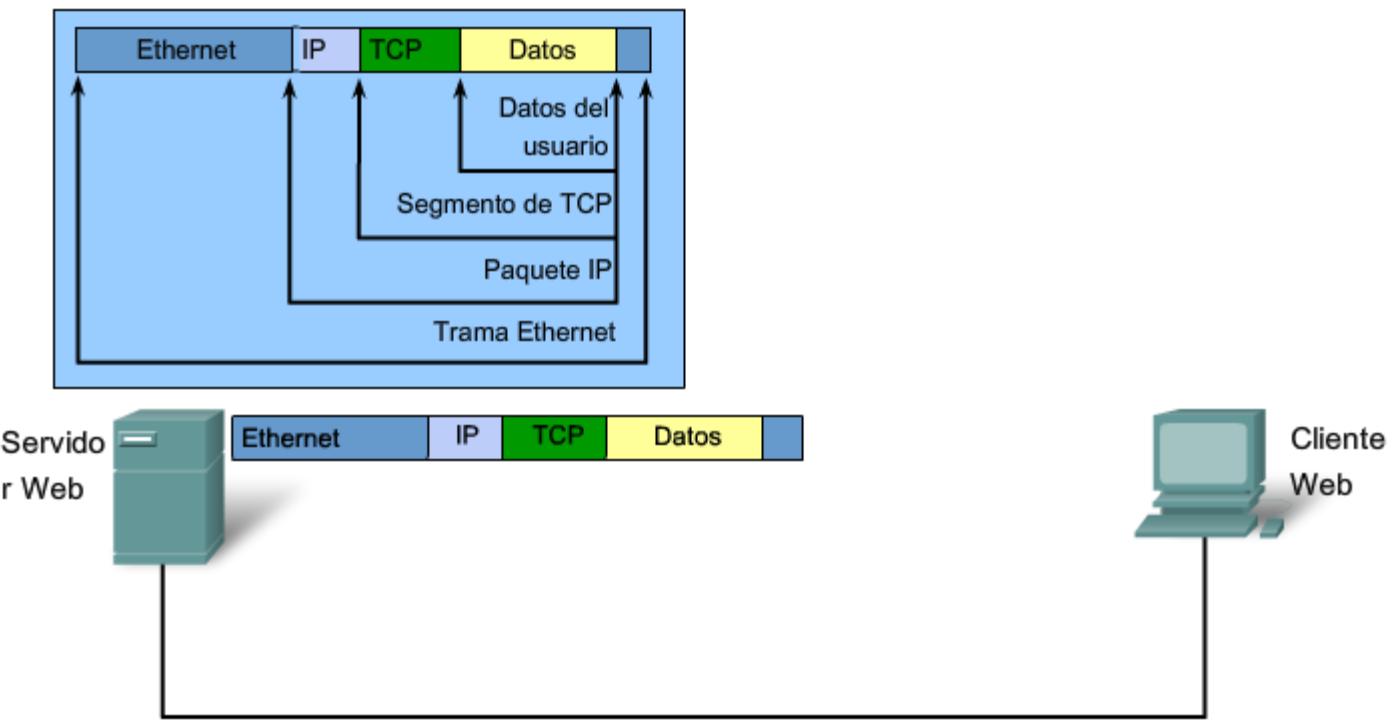
El protocolo de la capa Aplicación, HTTP, comienza el proceso entregando los datos de la página Web con formato HTML a la capa Transporte. Allí, los datos de aplicación se dividen en segmentos TCP. A cada segmento TCP se le otorga una etiqueta, denominada encabezado, que contiene información sobre qué procesos que se ejecutan en la computadora de destino deben recibir el mensaje. También contiene la información para habilitar el proceso de destino para reensamblar nuevamente los datos a su formato original.

La capa Transporte encapsula los datos HTML de la página Web dentro del segmento y los envía a la capa Internet, donde se implementa el protocolo IP. Aquí, el segmento TCP en su totalidad es encapsulado 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 correspondiente proceso de destino.

Luego el paquete IP se envía al protocolo Ethernet de la capa de acceso a la red, donde se encapsula en un encabezado de trama y en 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. Finalmente, los bits se codifican en el medio Ethernet mediante el servidor NIC.

Operación de protocolo de envío y recepción de un mensaje

Términos de la encapsulación de protocolos



Este proceso se invierte en el host receptor. Los datos se encapsulan mientras suben al stack hacia la aplicación del usuario final.

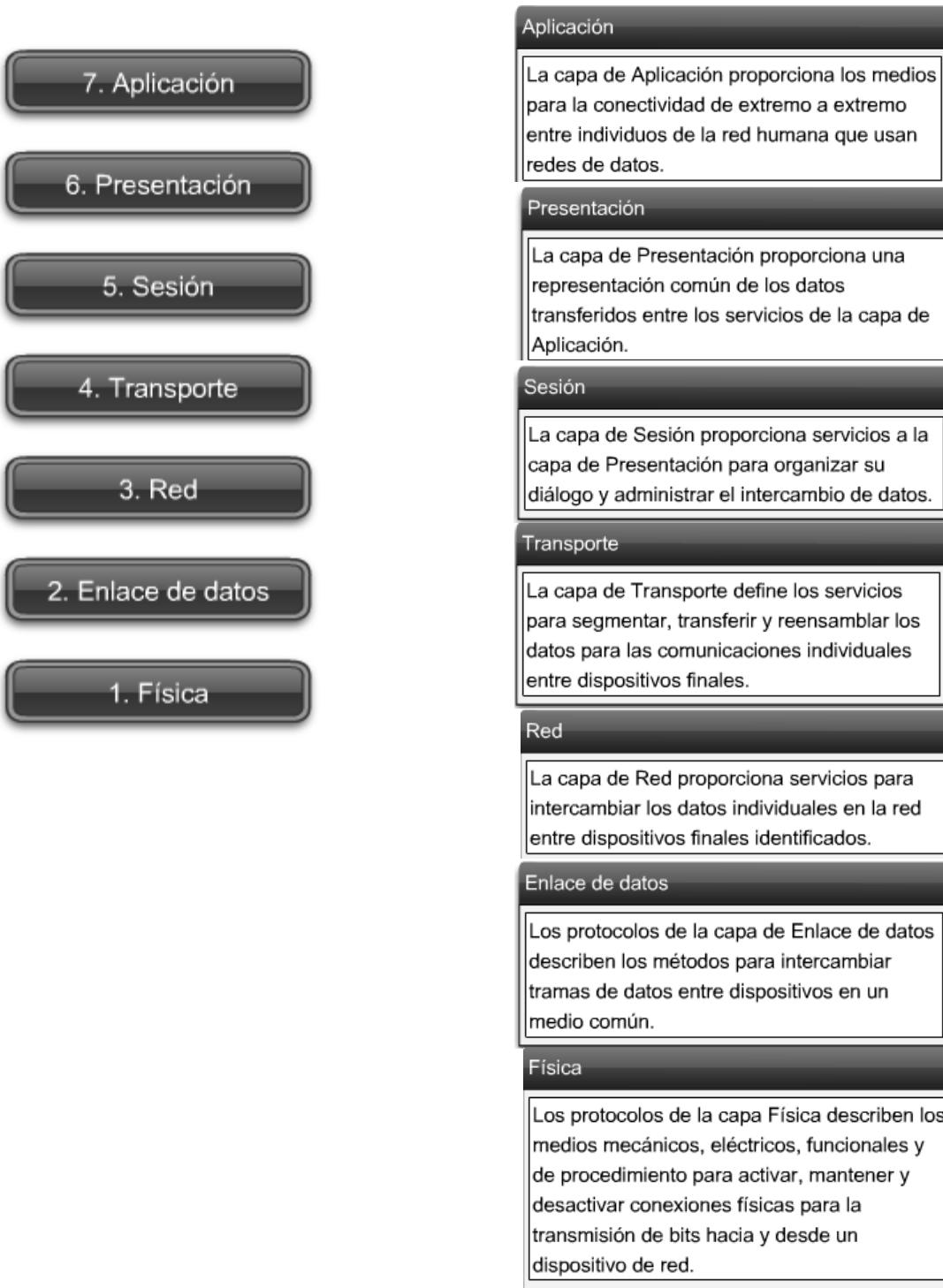
2.4.7 Modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizará para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la 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 desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Aunque el contenido de este curso se estructurará en torno al modelo OSI, el eje del análisis serán los protocolos identificados en el stack de protocolos TCP/IP.

Tenga en cuenta que, mientras las capas del modelo TCP/IP se mencionan sólo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre.



2.4.8 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 Acceso a la red y la capa Aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.

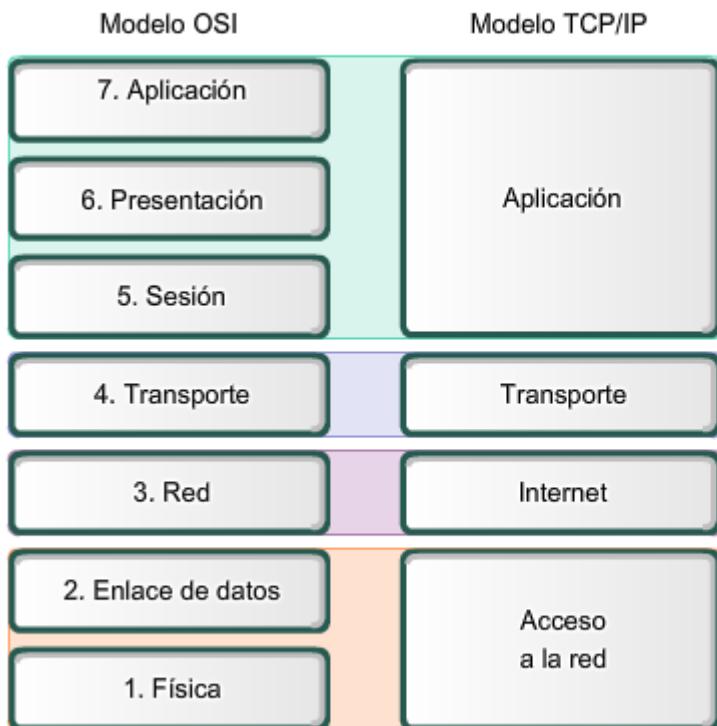
En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

Los paralelos clave entre dos modelos de red se producen en las Capas 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork. El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.

La Capa 4, la capa Transporte del modelo OSI, con frecuencia se utiliza para describir servicios o funciones generales que administran conversaciones individuales 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, Protocolo de control de transmisión (TCP) y Protocolo de datagramas de usuario (UDP) proporcionan la funcionalidad necesaria.

La capa de aplicación TCP/IP incluye una cantidad de protocolos que proporcionan funcionalidad específica para una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

Comparación del modelo OSI con el modelo TCP/IP



Las semejanzas claves están en la capa de Red y de Transporte.

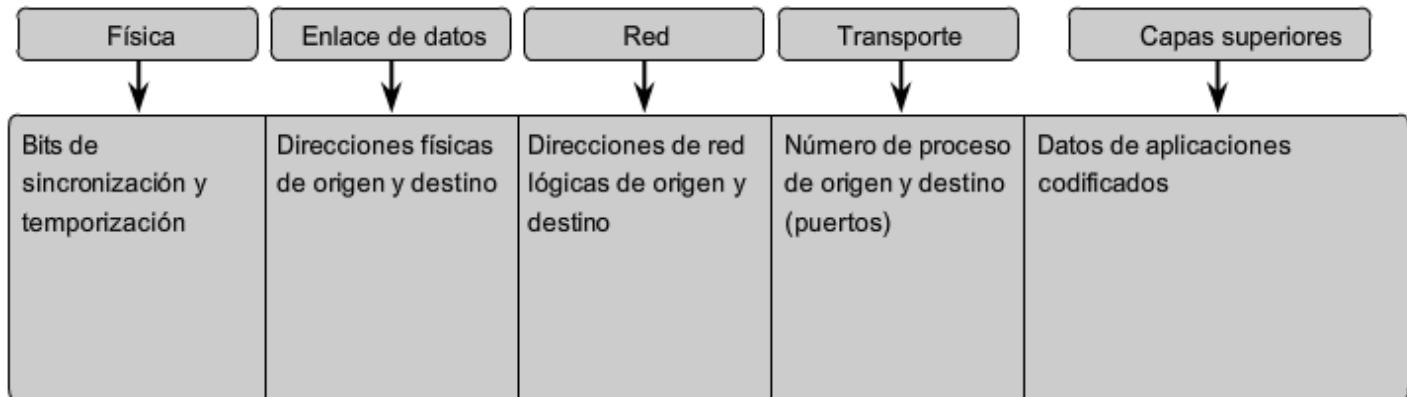
2.5 DIRECCIONAMIENTO DE RED

2.5.1 Direccionamiento en la red

El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan

por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.

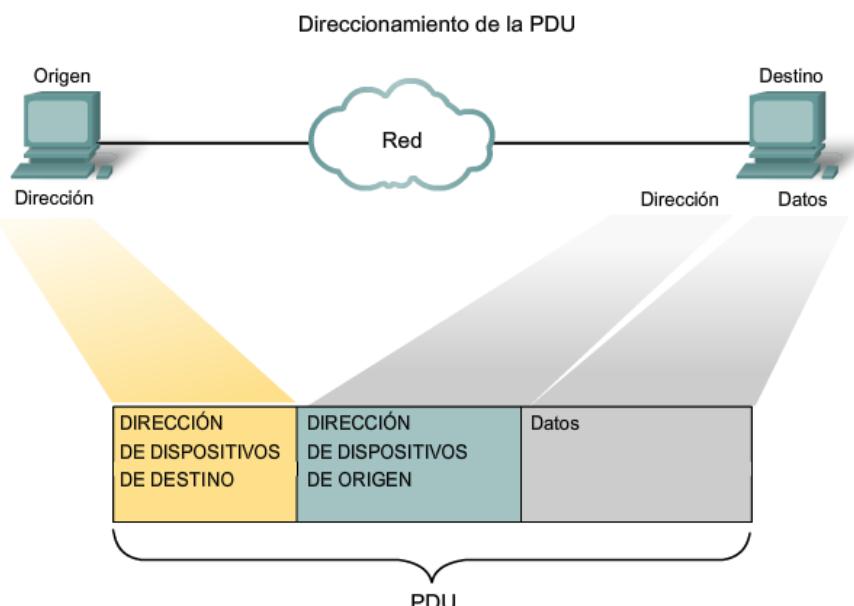
Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizar el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.



2.5.2 Envío de datos al dispositivo final

Durante el proceso de encapsulación, se agregan identificadores de dirección a los datos mientras bajan al stack del protocolo en el host de origen. Así como existen múltiples capas de protocolos que preparan los datos para transmitirlos a sus destinos, existen múltiples capas de direccionamiento para asegurar la entrega.

El primer identificador, la dirección física del host, aparece en el encabezado de la PDU de Capa 2, llamado trama. 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 al medio (MAC). Cuando dos dispositivos se comunican en la red Ethernet local, las tramas que se intercambian entre ellos contienen las direcciones MAC de origen y de destino. Una vez que una trama se recibe satisfactoriamente por el host de destino, la información de la dirección de la Capa 2 se elimina mientras los datos se desencapsulan y suben el stack de protocolos a la Capa 3.



El encabezado de la Unidad de datos del protocolo contiene campos de direcciones de dispositivos.

2.5.3 Transporte de datos a través de internetworks

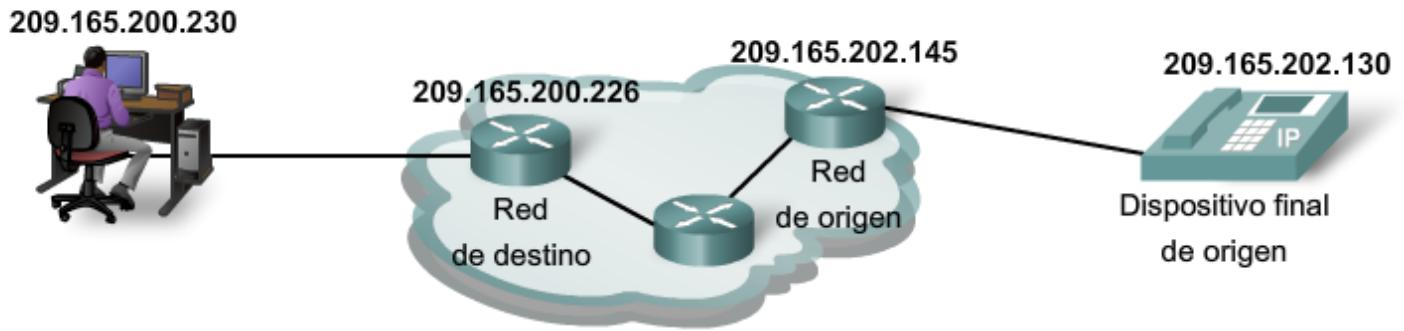
Los protocolos de Capa 3 están diseñados principalmente para mover datos desde una red local a otra red local dentro de una internetwork. Mientras las direcciones de Capa 2 sólo se utilizan para comunicar entre dispositivos de una red local única, las direcciones de Capa 3 deben incluir identificadores que permitan a dispositivos de red intermediarios ubicar hosts en diferentes redes. En la suite de protocolos TCP/IP, cada dirección IP host contiene información sobre la red en la que está ubicado el host.

En los límites de cada red local, un dispositivo de red intermediario, por lo general un router, desencapsula la trama para leer la dirección host de destino contenida en el encabezado del paquete, la PDU de Capa 3. 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 por su trayecto hacia el dispositivo final de destino. Cuando la trama llega a su destino final, la trama y los encabezados del paquete se eliminan y los datos se suben a la Capa 4.

Ubicación de las partes en la red correcta

| Unidad de datos del protocolo (PDU) | | | | |
|-------------------------------------|---------------------------|------------------|---------------------------|-------|
| Destino | | Origen | | Datos |
| Dirección de red | Dirección del dispositivo | Dirección de red | Dirección del dispositivo | |
| | | | | |

El encabezado de la Unidad de datos del protocolo también contiene la dirección de red.



2.5.4 Envío de datos a la aplicación correcta

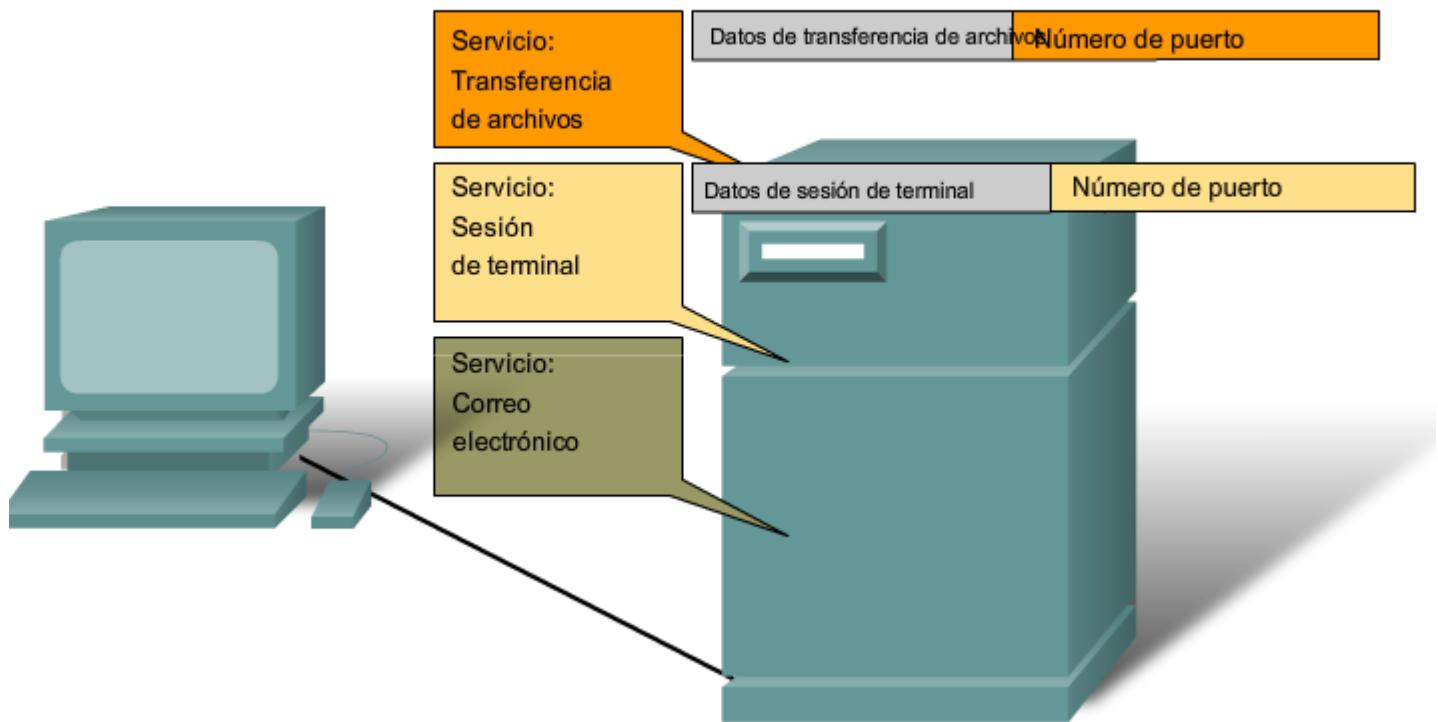
En la Capa 4, la información contenida en el encabezado de la PDU no identifica un host de destino o una red de destino. Lo que sí identifica es el proceso o servicio específico que se ejecuta en el dispositivo host de destino que actuará en los datos que se entregan. Los hosts, sean clientes o servidores en Internet, pueden ejecutar múltiples aplicaciones de red simultáneamente. La gente que utiliza computadoras personales generalmente tiene 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 cliente de correo electrónico esté enviando o recibiendo un e-mail y un colega o amigo enviando un mensaje instantáneo.

Piense en una computadora que tiene sólo una interfaz de red. Todos los streams de datos creados por las aplicaciones que se están ejecutando en la PC ingresan y salen a través de esa sola interfaz, sin embargo los mensajes instantáneos no emergen en el medio del documento del procesador de textos o del e-mail que se ve en un juego.

Esto es así porque los procesos individuales que se ejecutan en los hosts de origen y de destino se comunican entre sí. Cada aplicación o servicio es representado 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.



2.5.5 Guerreros en la red

Un recurso de entretenimiento para ayudar a visualizar los conceptos de networking es la película animada “Warriors of the Net” (Guerreros de la red), por 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.

Segundo, es posible que algunos términos que se mencionan en el video no le sean familiares. Los tipos de paquetes mencionados se refieren al tipo de datos de nivel superior (TCP, UDP, ICMP Ping, PING de la muerte) que se encapsulan en los paquetes IP (en definitiva, todo se convierte en paquetes IP). Los dispositivos que encuentran los paquetes en su

viaje son router, servidor proxy, router switch, Intranet corporativa, el proxy, URL (Localizador uniforme de recursos), firewall, ancho de banda, host, servidor Web.

Tercero, mientras que en el video se hace referencia explícita a los puertos números 21, 23, 25, 53 y 80, solamente se hace referencia implícita a las direcciones IP. ¿Puede ver dónde? ¿Dónde se muestra en el video que las direcciones MAC pueden estar involucradas?

Por último, a pesar de que, con frecuencia, todas las animaciones tienen simplificaciones, en el video hay un error claro. Aproximadamente a los 5 minutos, se formula la siguiente afirmación “Qué sucede cuando el señor IP no recibe un acuse de recibo; simplemente envía un paquete de reemplazo.” Como verá en los capítulos siguientes, ésta no es una función del Protocolo de Internet de Capa 3, que es un protocolo de entrega “no confiable” de máximo esfuerzo, sino una función del Protocolo TCP de la capa Transporte.

Al finalizar este curso, comprenderá mejor la amplitud y profundidad de los conceptos descritos en el video. Esperamos que lo disfrute.

Descargue la película desde <http://www.warriorsofthe.net>

2.7 RESUMEN DEL CAPITULO

2.7.1 Resumen y revisión

Las redes de datos son sistemas de dispositivos finales, de dispositivos intermediarios y de medios que conectan los dispositivos, que proporcionan la plataforma para la red humana.

Estos dispositivos y los servicios que funcionan en ellos pueden interconectarse de manera global y transparente para el usuario ya que cumplen con las reglas y los protocolos.

El uso de modelos en capas como abstracciones significa que las operaciones de los sistemas de red se pueden analizar y desarrollar para abastecer las necesidades de los servicios de comunicación futuros.

Los modelos de networking más ampliamente utilizados son OSI y TCP/IP. Asociar los protocolos que establecen las reglas de las comunicaciones de datos con las distintas capas 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.

A medida que bajan en el stack, los datos se segmentan en partes y se encapsulan con las direcciones y demás rótulos. El proceso se invierte cuando las partes se desencapsulan y suben al stack del protocolo de destino.

La aplicación de los modelos permite a las distintas personas, empresas y asociaciones comerciales analizar las redes actuales y planificar las redes del futuro.

En este capítulo, aprendió a:

- Describir la estructura de una red, incluidos los dispositivos y medios necesarios para lograr comunicaciones exitosas.
- Explicar la función de los protocolos en las comunicaciones de redes.
- Explicar las ventajas de usar un modelo en capas para describir la funcionalidad de red.
- Describir la función de cada capa en los dos modelos de red reconocidos: el modelo TCP/IP y el modelo OSI.
- Describir la importancia de direccionar y nombrar esquemas en las comunicaciones de red.

3-PROTOCOLOS Y FUNCIONALIDAD DE LA CAPA DE APLICACIÓN

3.0 INTRODUCCIÓN DEL CAPITULO

3.0.1 Introducción del capítulo

La mayoría de nosotros experimentamos Internet a través de World Wide Web, servicios de e-mail y programas para compartir archivos. Éstas y muchas otras aplicaciones proporcionan la interfaz humana a la red subyacente, lo que nos permite enviar y recibir información con relativa facilidad. Generalmente, las aplicaciones que utilizamos son intuitivas; es decir, podemos acceder a ellas y usarlas sin saber cómo funcionan. Sin embargo, para los profesionales de redes es importante conocer cómo una aplicación puede formatear, transmitir e interpretar mensajes que se envían y reciben a través de la red.

La visualización de los mecanismos que permiten la comunicación a través de la red se hace más sencilla si utilizamos el marco en capas del modelo Interconexión de sistema abierto (OSI). En este capítulo, enfatizaremos el rol de una capa, la capa de Aplicación, y sus componentes: aplicaciones, servicios y protocolos. Exploraremos cómo esos tres elementos hacen posible la comunicación sólida a través de la red de información.

En este capítulo aprenderá a:

- Describir cómo las funciones de las tres capas superiores del modelo OSI proporcionan servicios de red a las aplicaciones de usuario final.
- Describir cómo los protocolos de la capa de aplicación TCP/IP proporcionan los servicios especificados por las capas superiores del modelo OSI.
- Definir cómo la gente utiliza la capa de aplicación para comunicarse a través de la red de información.
- Describir la función de las conocidas aplicaciones TCP/IP, como la World Wide Web y el correo electrónico, y sus servicios relacionados (HTTP, DNS, SMB, DHCP, SMTP/POP y Telnet).
- Describir los procesos para compartir archivos que utilizan las aplicaciones entre pares y el protocolo Gnutella.
- Explicar cómo los protocolos garantizan que los servicios que se ejecutan en una clase de dispositivo puedan enviar y recibir datos desde y hacia muchos dispositivos de red diferentes.
- Utilizar herramientas de análisis de red para examinar y explicar cómo funcionan las aplicaciones comunes de usuarios.



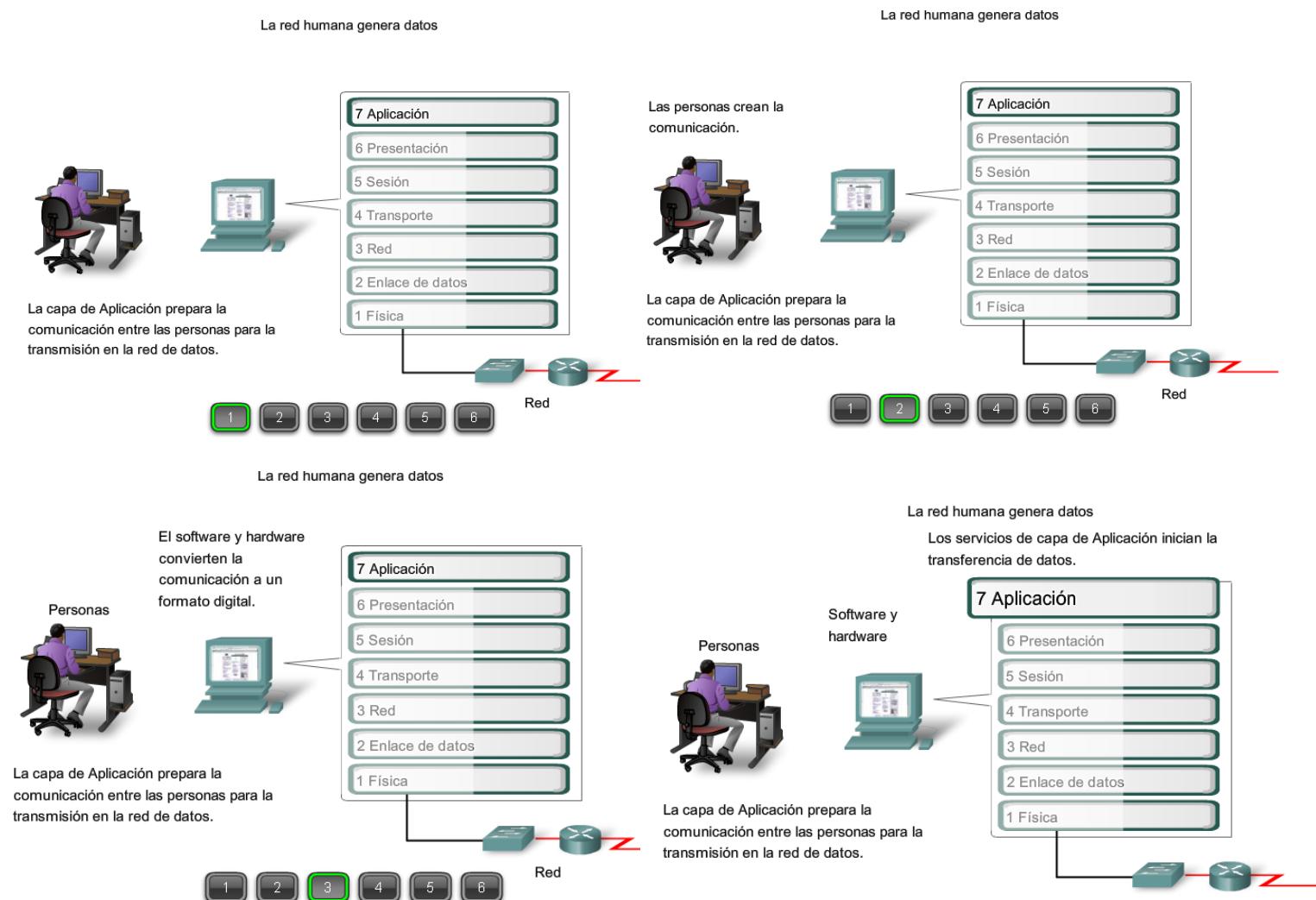
3.1 APPLICACIONES: LA INTERFACE ENTRE REDES

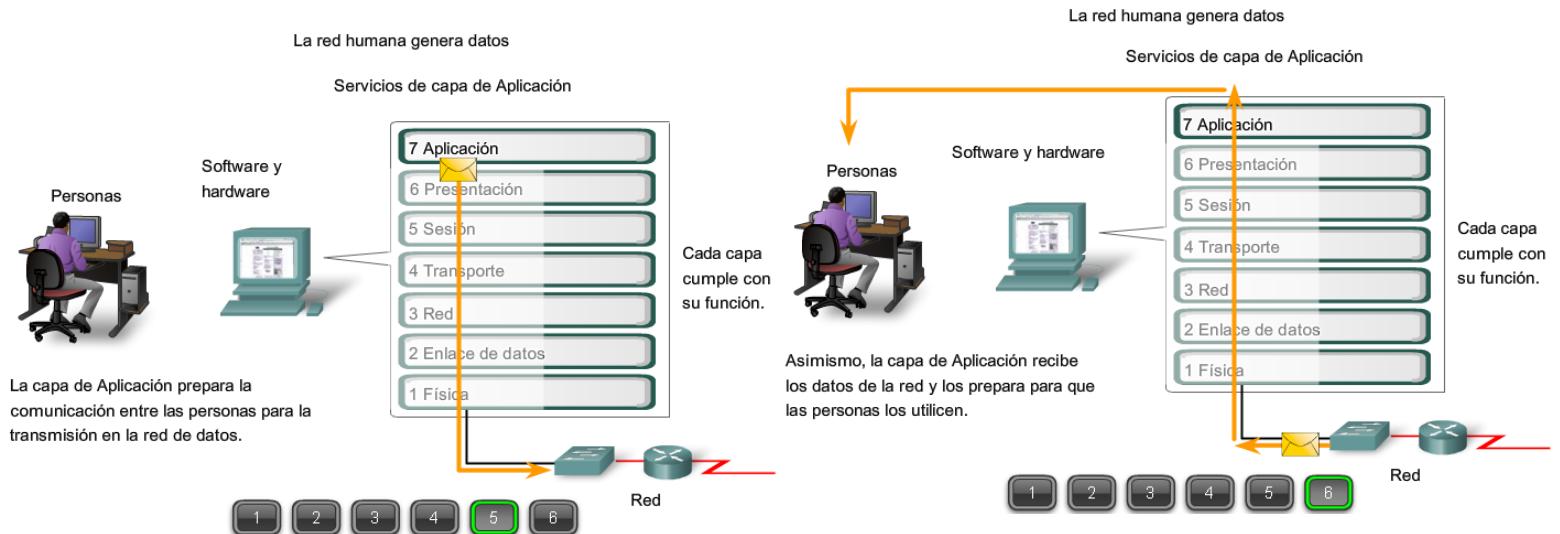
3.1.1 Modelo OSI y Modelo TCP/IP

El modelo de referencia de interconexión de sistemas abiertos es una representación abstracta en capas, creada como guía para el diseño del protocolo de red. El modelo OSI divide el proceso de networking en diferentes capas lógicas, cada una de las cuales tiene una única funcionalidad y a la cual se le asignan protocolos y servicios específicos.

En este modelo, la información se pasa de una capa a otra, comenzando en la capa de Aplicación en el host de transmisión, siguiendo por la jerarquía hacia la capa Física, pasando por el canal de comunicaciones al host de destino, donde la información vuelve a la jerarquía y termina en la capa de Aplicación. La figura ilustra los pasos en este proceso.

La capa de Aplicación, Capa siete, es la capa superior de los modelos OSI y TCP/IP. 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 siempre se desarrollan protocolos nuevos.





Aunque el grupo de protocolos TCP/IP se desarrolló antes de la definición del modelo OSI, la funcionalidad de los protocolos de capa de aplicación de TCP/IP se adaptan aproximadamente a la estructura de las tres capas superiores del modelo OSI: Capas de Aplicación, Presentación y Sesión.

La mayoría de los protocolos de capa de aplicación de TCP/IP se desarrollaron antes de la aparición de computadoras personales, interfaces del usuario gráficas y objetos multimedia. Como resultado, estos protocolos implementan muy poco de la funcionalidad que se especifica en las capas de Sesión y Presentación del modelo OSI.

Capa de Presentación

La capa de Presentación tiene tres funciones primarias:

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
- Encriptación de los datos para transmisión y descifre de los datos cuando se reciben en el destino.

Las implementaciones de la capa de presentación generalmente no se vinculan con una stack de protocolos determinada. Los estándares para videos y gráficos son algunos ejemplos. Dentro de los estándares más conocidos para vídeo encontramos QuickTime y el Grupo de expertos en películas (MPEG). QuickTime es una especificación de Apple Computer para audio y vídeo, y MPEG es un estándar para la codificación y compresión de vídeos.

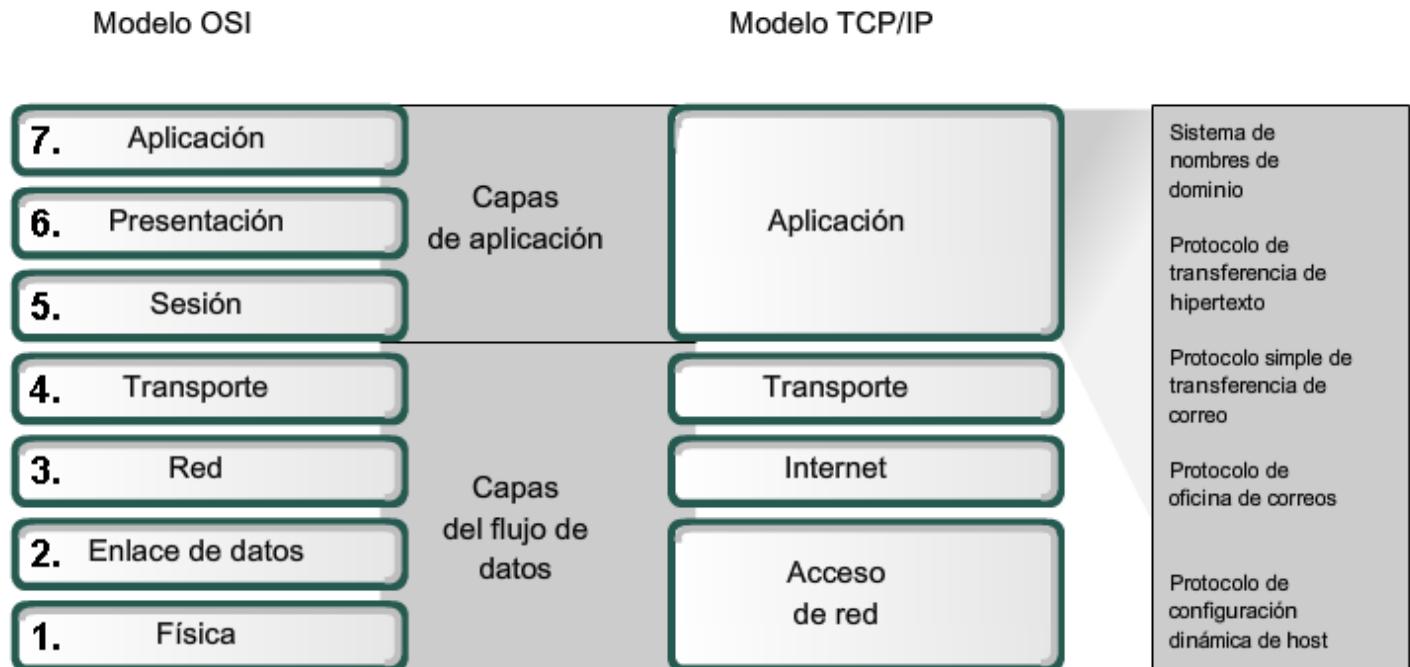
Dentro de los formatos de imagen gráfica más conocidos encontramos Formato de intercambio gráfico (GIF), Grupo de expertos en fotografía (JPEG) y Formato de archivo de imagen etiquetada (TIFF). GIF y JPEG son estándares de compresión y codificación para imágenes gráficas, y TIFF es una formato de codificación estándar para imágenes gráficas.

Capa de Sesión

Como lo indica el nombre de la capa de Sesión, las funciones en esta capa 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 desactivaron durante un periodo de tiempo prolongado.

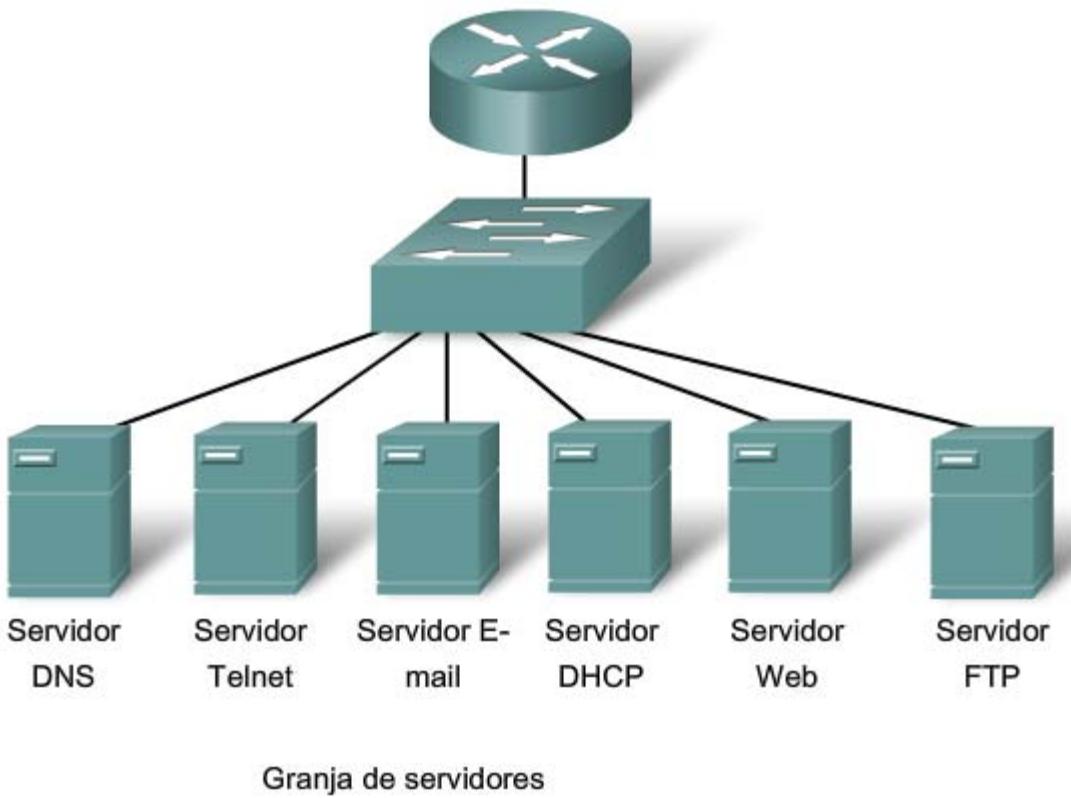
La mayoría de las aplicaciones, como los exploradores Web o los clientes de correo electrónico, incorporan la funcionalidad de las capas 5, 6 y 7 del modelo OSI.



Los protocolos de capa de aplicación de TCP/IP más conocidos son aquellos que proporcionan intercambio de la información del usuario. Estos protocolos especifican la información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes. Algunos de los protocolos TCP/IP son:

- El protocolo Servicio de nombres de dominio (DNS, Domain Name Service) se utiliza para resolver nombres de Internet en direcciones IP.
- El protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) se utiliza para transferir archivos que forman las páginas Web de la World Wide Web.
- El Protocolo simple de transferencia de correo (SMTP) se utiliza para la transferencia de mensajes de correo y adjuntos.
- Telnet, un protocolo de emulación de terminal, se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red.
- El Protocolo de transferencia de archivos (FTP, File Transfer Protocol) se utiliza para la transferencia interactiva de archivos entre sistemas.

Los protocolos de la suite TCP/IP generalmente son definidos por Solicitudes de comentarios (RFCs). El Grupo de trabajo de ingeniería de Internet mantiene las RFCs como los estándares para el conjunto TCP/IP.



Granja de servidores

Servidor de nombres de dominios (DNS)

- Servicio que ofrece la dirección IP de un sitio Web o nombre de dominio para que un host pueda conectarse a éste

Servidor Telnet

- Servicio que permite a los administradores conectarse a un host desde una ubicación remota y controlar el host como si estuvieran registrados en forma local

Servidor E-mail

- Utiliza el Simple Mail Transfer Protocol (SMTP) y Post Office Protocol (POP3) o Internet Message Access Protocol (IMAP)
- Se utiliza para enviar mensajes de e-mail de clientes a servidores a través de Internet
- Los destinatarios se especifican a través del formato `usuario@xyz`

Servidor Dynamic Host Configuration Protocol (DHCP)

- Servicio que asigna el gateway por defecto de la máscara de subred de dirección IP y demás información a los clientes

Servidor Web

- Hypertext Transfer Protocol (HTTP)
- Se utiliza para transferir información entre clientes Web y servidores Web
- Se accede a la mayoría de las páginas Web a través de HTTP

Servidor File Transfer Protocol (FTP)

- Servicio que permite descargar y subir archivos entre un cliente y un servidor

3.1.2 Software de la capa de aplicación

Las funciones asociadas con los protocolos de capa de Aplicación permiten a la red humana comunicarse con la red de datos subyacente. Cuando abrimos un explorador Web o una ventana de mensajería instantánea, se inicia una aplicación, y el programa se coloca en la memoria del dispositivo donde se ejecuta. Cada programa ejecutable cargado a un dispositivo se denomina proceso.

Dentro de la capa de Aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios.

Aplicaciones reconocidas por la red

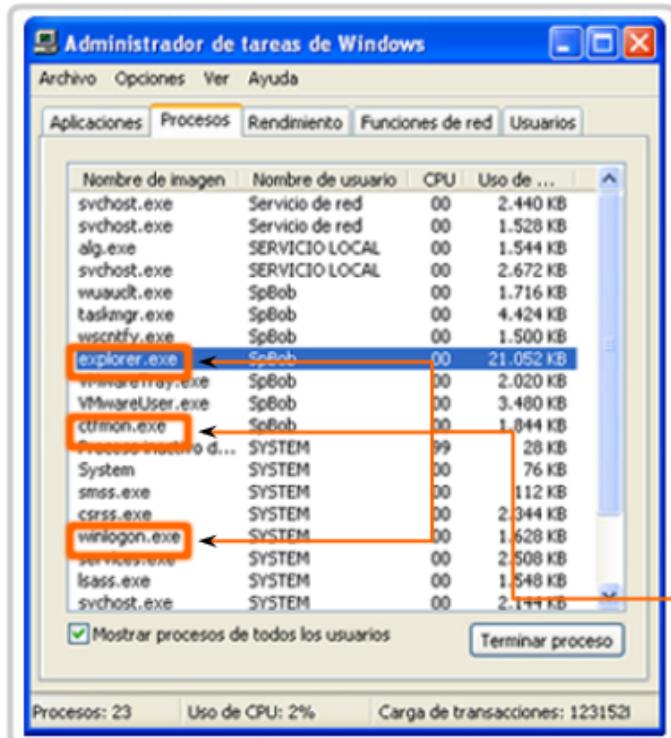
Aplicaciones son los programas de software que utilizan la gente para comunicarse a través de la red. Algunas aplicaciones de usuario final son compatibles con la red, lo cual significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores 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 ayuda de los servicios de la capa de Aplicación para utilizar los recursos de la red, como transferencia de archivos o cola de impresión en red. Aunque son transparentes para el usuario, estos servicios son los programas que se comunican con la red y preparan los datos para la transferencia. Diferentes tipos de datos, ya sea texto, gráfico o vídeo, requieren de diversos servicios de red para asegurarse de que estén bien preparados para procesar las funciones de las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y formatos de datos a utilizarse. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Para comprender la función de los distintos servicios de red, es necesario familiarizarse con los protocolos subyacentes que rigen su operación.

Procesos de software



Ejemplos de procesos en ejecución en el sistema operativo Windows

Los procesos son programas de software individuales que se ejecutan en forma simultánea.

Los procesos pueden ser

- 1 Aplicaciones
- 2 Servicios
- 3 Operaciones del sistema
- 4 Un programa puede estar en ejecución varias veces, cada vez dentro de su propio proceso.

Coloque el cursor sobre un elemento.

3.1.3 Aplicaciones del usuario, servicios y protocolos de capa de Aplicación

Como se mencionó anteriormente, la capa de Aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el tratamiento de los datos. Un único programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre. Por ejemplo: cuando analizamos "Telnet" nos podemos referir a la aplicación, el servicio o el protocolo.

En el modelo OSI, se considera que las aplicaciones que interactúan directamente con las personas se encuentran en la parte superior del stack, al igual que las personas. Al igual que todas las personas dentro del modelo OSI, la capa de Aplicación se basa en la funciones de las capas inferiores para completar el proceso de comunicación. Dentro de la capa de aplicación, los protocolos especifican qué mensajes se intercambian entre los host de origen y de destino, la sintaxis de los comandos de control, el tipo y formato de los datos que se transmiten y los métodos adecuados para notificación y recuperación de errores.

Conexión de interfaz entre redes humanas y de datos



Regreso a las 5



Nuestra compañía se fundó en 2001.



7 Aplicación

6 Presentación

5 Sesión

4 Transporte

3 Red

2 Enlace de datos

1 Física



Las APPLICACIONES proporcionan la interfaz humana.

Los SERVICIOS siguen los protocolos para preparar los datos para la red.

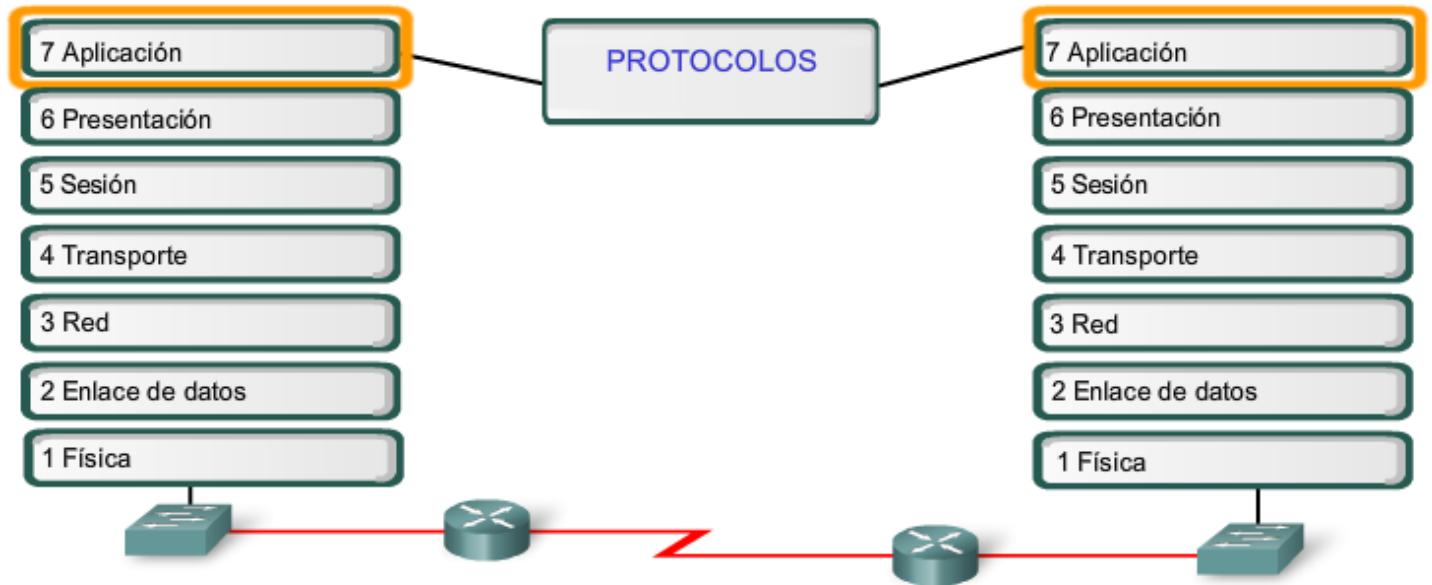
3.1.4 Funciones del protocolo de la Capa de Aplicación

Los protocolos de la capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones sean exitosas, deben coincidir los protocolos de capa de aplicación implementados en el host de origen y destino.

Los protocolos establecen reglas consistentes para intercambiar datos entre las aplicaciones y los servicios cargados en los dispositivos participantes. Los protocolos especifican cómo se estructuran los datos dentro de los mensajes y los tipos de mensajes que se envían entre origen y destino. Estos mensajes pueden ser solicitudes de servicios, acuses de recibo, mensajes de datos, mensajes de estado o mensajes de error. Los protocolos también definen los diálogos de mensajes, asegurando que un mensaje enviado encuentre la respuesta esperada y se invoquen los servicios correspondientes cuando se realiza la transferencia de datos.

Muchos y diversos tipos de aplicaciones se comunican a través de las redes de datos. Por lo tanto, los servicios de la capa de Aplicación deben implementar protocolos múltiples para proporcionar la variedad deseada de experiencias de comunicación. Cada protocolo tiene un fin específico y contiene las características requeridas para cumplir con dicho propósito. Deben seguirse los detalles del protocolo correspondiente a cada capa, así las funciones en una capa se comunican correctamente con los servicios en la capa inferior.

Las aplicaciones y los servicios también pueden utilizar protocolos múltiples durante el curso de una comunicación simple. Un protocolo puede especificar cómo se establece la conexión de redes y otro describir el proceso para la transferencia de datos cuando el mensaje se pasa a la siguiente capa inferior.



Los protocolos de capa de Aplicación proporcionan las reglas para la comunicación entre las aplicaciones.

Protocolos:

- Define los procesos en cada uno de los extremos de la comunicación
- Define los tipos de mensajes
- Define la sintaxis de los mensajes
- Define el significado de los campos de información
- Define la forma en que se envían los mensajes y la respuesta esperada
- Define la interacción con la próxima capa inferior

3.2 TOMA DE MEDIDAS PARA LAS APLICACIONES Y SERVICIOS

3.2.1 El modelo cliente-servidor

Cuando la gente intenta acceder a información en sus dispositivos, ya sean éstos una computadora personal o portátil, un PDA, teléfono celular o cualquier otro dispositivo conectado a la red, los datos pueden no estar físicamente almacenados en sus dispositivos. Si así fuere, se debe solicitar al dispositivo que contiene los datos, permiso para acceder a esa información.

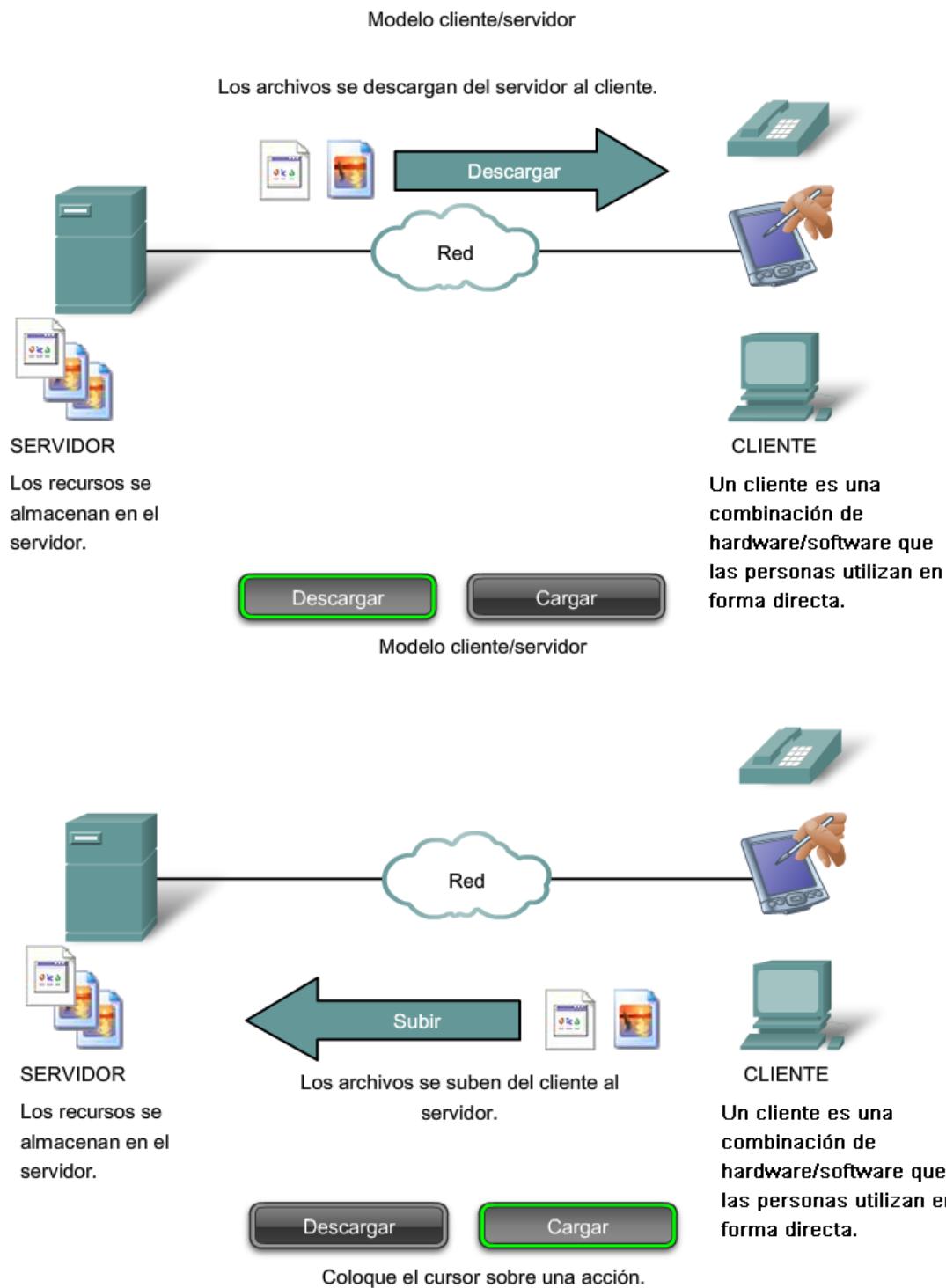
Modelo cliente-servidor

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 una parte de la capa de Aplicación. El cliente comienza el intercambio solicitando los datos al servidor, que responde enviando uno o más streams de datos al cliente. Los protocolos de capa de Aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio puede requerir de información adicional, como la autenticación del usuario y la identificación de un archivo de datos a transferir.

Un ejemplo de una red cliente/servidor es un entorno corporativo donde los empleados utilizan un servidor de e-mail de la empresa para enviar, recibir y almacenar e-mails. El cliente de correo electrónico en la computadora de un empleado

emite una solicitud al servidor de e-mail para un mensaje no leído. El servidor responde enviando el e-mail solicitado al cliente.

Aunque los datos generalmente se describen como un flujo del servidor al cliente, algunos datos siempre fluyen del cliente al servidor. El flujo de datos puede ser el mismo en ambas direcciones o inclusive 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. La transferencia de datos de un cliente a un servidor se conoce como subida y la de los datos de un servidor a un cliente, descarga.

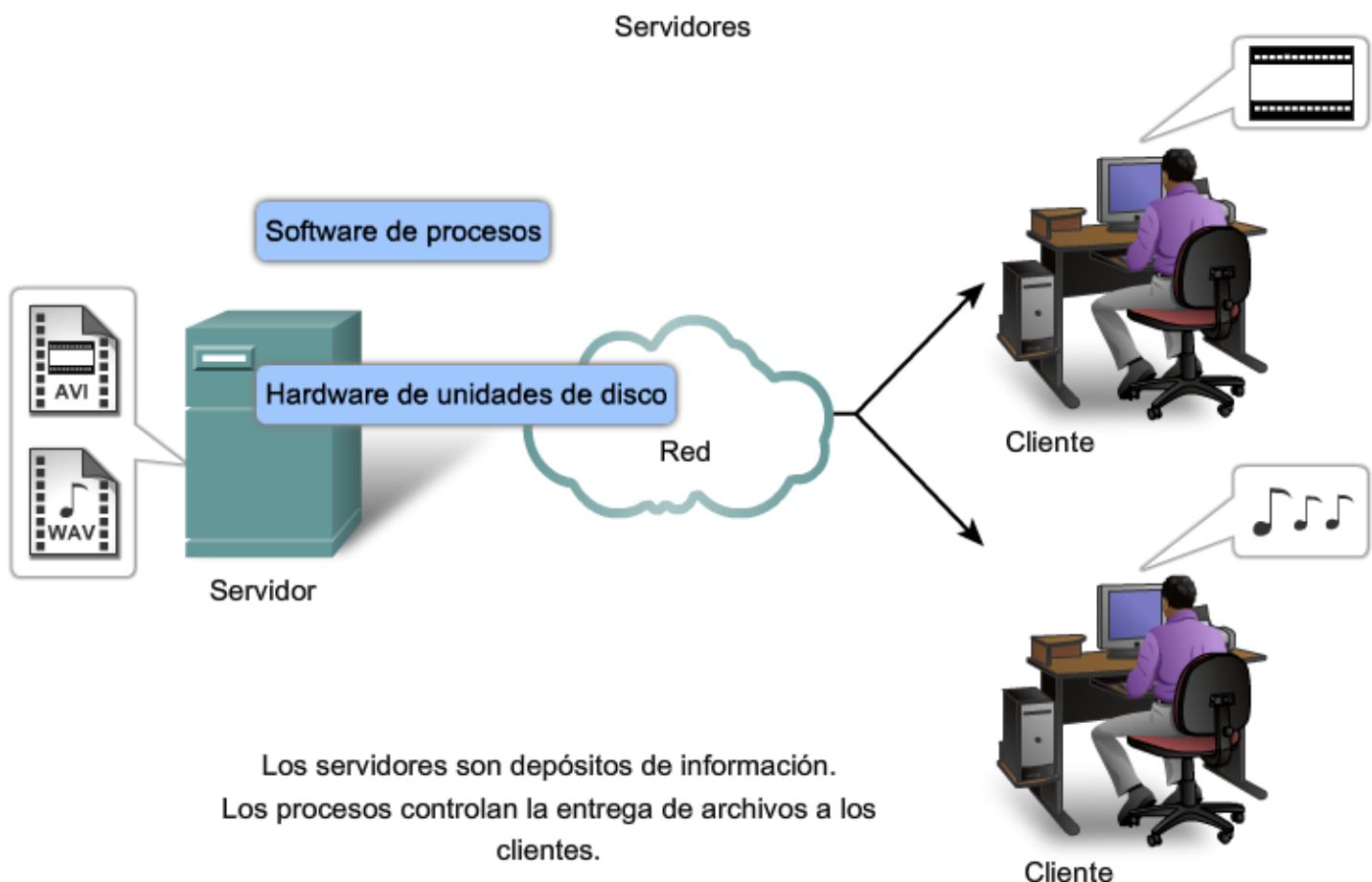


3.2.2 Servidores

En un contexto general de redes, cualquier dispositivo que responde a una solicitud de aplicaciones de cliente funciona como un servidor. Un servidor generalmente es una computadora que contiene información para ser compartida con muchos sistemas de cliente. Por ejemplo, páginas Web, documentos, bases de datos, imágenes, archivos de audio y vídeo pueden almacenarse en un servidor y enviarse a los clientes que lo solicitan. En otros casos, como una impresora de red, el servidor de impresión envía las solicitudes de impresión del cliente a la impresora específica.

Diferentes tipos de aplicaciones del servidor tienen diferentes requerimientos para el acceso de clientes. Algunos servidores pueden requerir de autenticación de la información de cuenta del usuario para verificar si el usuario tiene permiso para acceder a los datos solicitados o para utilizar una operación en particular. Dichos servidores deben contar con una lista central de cuentas de usuarios y autorizaciones, o permisos (para operaciones y acceso a datos) otorgados a cada usuario. Cuando se utiliza un cliente FTP, por ejemplo, si usted solicita subir datos al servidor FTP, se le puede dar permiso para escribir su carpeta personal pero no para leer otros archivos del sitio.

En una red cliente-servidor, el servidor ejecuta un servicio o proceso, a veces denominado daemon de servidor. Al igual que la mayoría de los servicios, los daemons generalmente se ejecutan en segundo plano y no se encuentran bajo control directo del usuario. Los daemons se describen como servidores que “escuchan” una solicitud del cliente, porque están programados para responder cada vez que el servidor recibe una solicitud para el servicio proporcionado por el daemon. Cuando un daemon “escucha” una solicitud de un cliente, intercambia los mensajes adecuados con el cliente, según lo requerido por su protocolo, y procede a enviar los datos solicitados al cliente en el formato correspondiente.

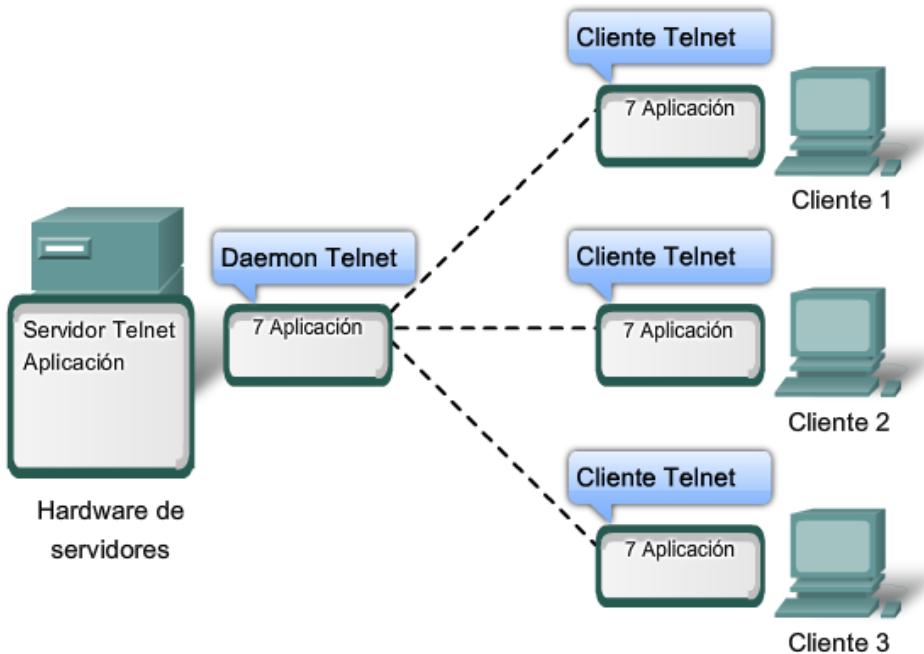


3.2.3 Protocolos y servicios de la capa de Aplicación

Una única aplicación puede emplear diferentes servicios de la capa de Aplicación, así lo que aparece para el usuario como una solicitud para una página Web puede, de hecho, ascender a docenas de solicitudes individuales. Y, para cada solicitud, pueden ejecutarse múltiples procesos. Por ejemplo, un cliente puede necesitar de diversos procesos individuales para formular sólo una solicitud al servidor.

Además, los servidores generalmente tienen múltiples clientes que solicitan información al mismo tiempo. Por ejemplo, un servidor Telnet puede tener varios clientes que requieren conectarse a él. Estas solicitudes individuales del cliente pueden manejarse en forma simultánea y separada para que la red sea exitosa. Los servicios y procesos de capa de Aplicación dependen del soporte de las funciones de la capa inferior para administrar en forma exitosa las múltiples conversaciones.

Los procesos de servidores pueden admitir múltiples clientes.



3.2.4 Redes y aplicaciones entre pares (P2P, Peer-to-Peer)

Modelo Punto a Punto

Además del modelo cliente/servidor para redes, existe también un modelo punto a punto. Las redes punto a punto tienen dos formas distintivas: diseño de redes punto a punto y aplicaciones punto a punto (P2P). Ambas formas tienen características similares pero en la práctica funcionan de forma muy distinta.

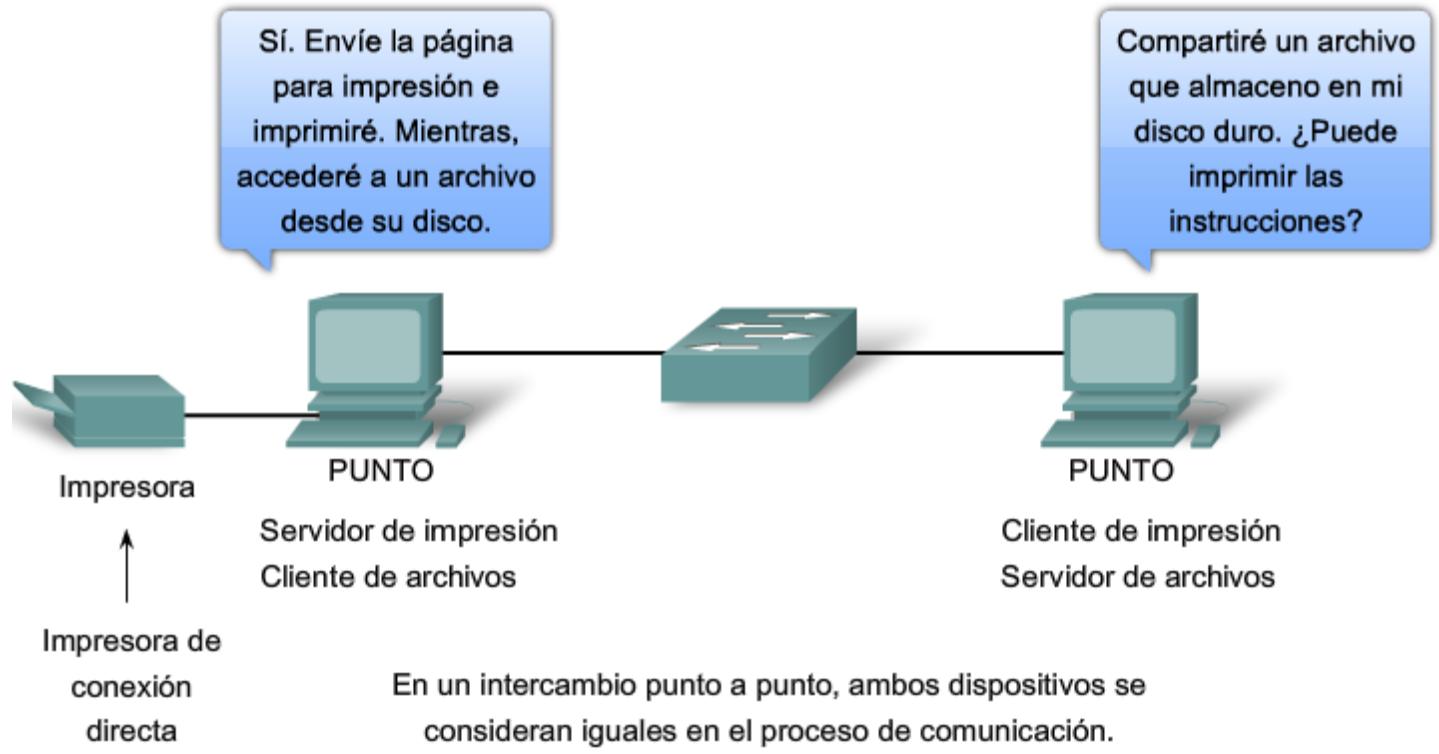
Redes entre pares

En una red entre pares, dos o más computadoras están conectadas a través de una red y pueden compartir recursos (por ejemplo, impresora y archivos) sin tener un servidor dedicado. Cada dispositivo final conectado (conocido como punto) puede funcionar como un servidor o como un cliente. Una computadora puede asumir el rol de servidor para una transacción mientras funciona de forma simultánea como cliente para otra transacción. Los roles del cliente y el servidor se configuran según las solicitudes.

Un ejemplo de una red entre pares es una simple red doméstica con dos computadoras conectadas que comparten una impresora. Cada persona puede configurar su computadora para compartir archivos, habilitar juegos en red o compartir una conexión de Internet. Otro ejemplo sobre la funcionalidad de la red punto a punto son dos computadoras conectadas a una gran red que utilizan aplicaciones de software para compartir recursos entre ellas a través de la red.

A diferencia del modelo cliente/servidor, que utiliza servidores dedicados, las redes punto a punto descentralizan los recursos en una red. En lugar de ubicar información para compartir en los servidores dedicados, la información puede colocarse en cualquier parte de un dispositivo conectado. La mayoría de los sistemas operativos actuales admiten compartir archivos e impresoras sin requerir software del servidor adicional. Debido a que las redes punto a punto generalmente no utilizan cuentas de usuarios centralizadas, permisos ni monitores, es difícil implementar las políticas de acceso y seguridad en las redes que contienen mayor cantidad de computadoras. Se deben establecer cuentas de usuario y derechos de acceso en forma individual para cada dispositivo.

Redes punto a punto



Aplicaciones punto a punto

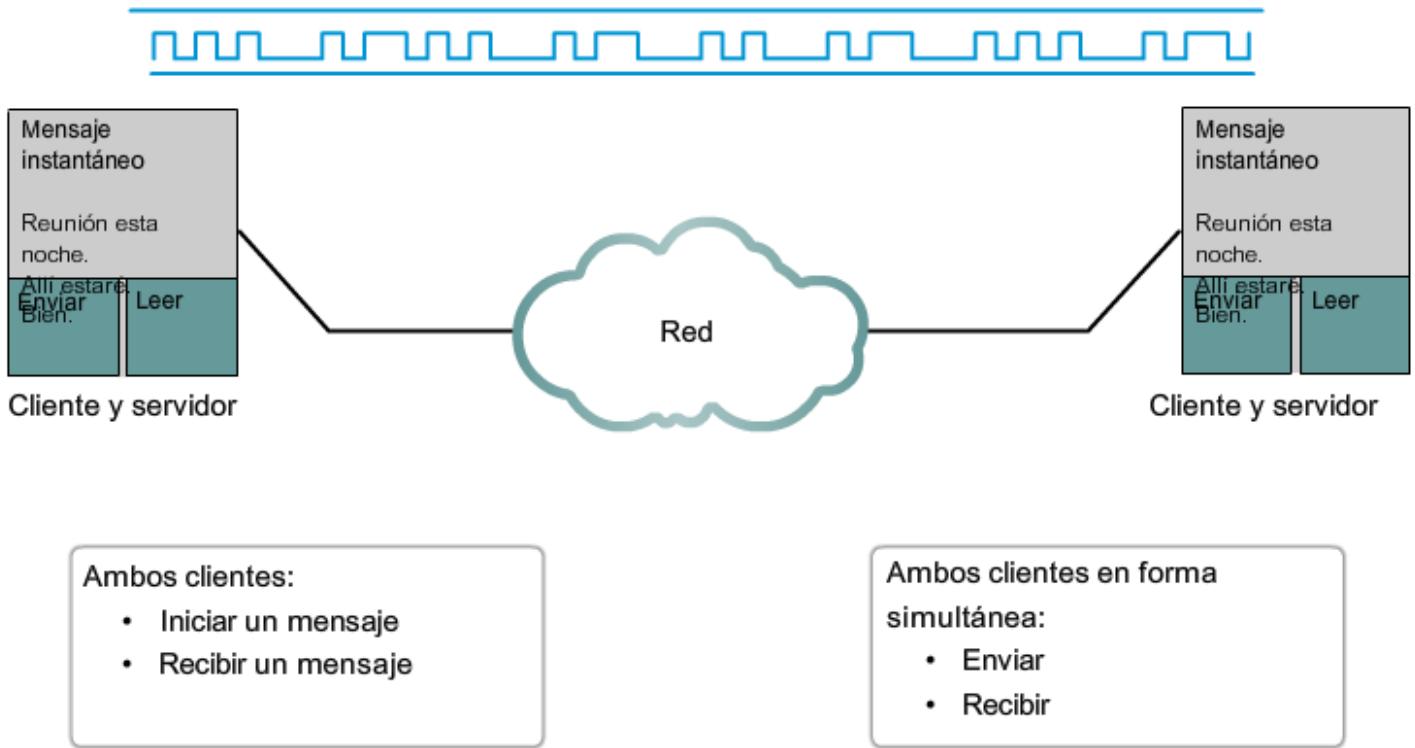
Una aplicación punto a punto (P2P), a diferencia de una red punto a punto, permite a un dispositivo actuar como cliente o como servidor dentro de la misma comunicación. En este modelo, cada cliente es un servidor y cada servidor es un cliente. Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación. Sin embargo, las aplicaciones punto a punto requieren que cada dispositivo final proporcione una interfaz de usuario y ejecute un servicio en segundo plano. Cuando inicia una aplicación punto a punto específica, ésta invoca la interfaz de usuario requerida y los servicios en segundo plano. Luego, los dispositivos pueden comunicarse directamente.

Algunas aplicaciones P2P utilizan un sistema híbrido donde se descentraliza el acceso a los 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 al servidor de índice.

Las aplicaciones punto a punto pueden utilizarse en las redes punto a punto, en redes cliente/servidor y en Internet.

Aplicaciones punto a punto

Cliente y servidor en la misma comunicación



3.3 EJEMPLOS DE SERVICIOS Y PROTOCOLOS DE LA CAPA DE APLICACIÓN

3.3.1 Protocolo y servicios DNS

Ahora que comprendemos mejor cómo las aplicaciones proporcionan una interfaz para el usuario y acceso a la red, veremos algunos protocolos específicos que se utilizan comúnmente.

Como veremos más adelante, la capa de transporte utiliza un esquema de direccionamiento que se llama número de puerto. Los números de puerto identifican las aplicaciones y los servicios de la capa de Aplicación que son los datos de origen y destino. Los programas del servidor generalmente utilizan números de puerto predefinidos comúnmente conocidos por los clientes. Mientras examinamos los diferentes servicios y protocolos de la capa de Aplicación de TCP/IP, nos referiremos a los números de puerto TCP y UDP normalmente asociados con estos servicios. Algunos de estos servicios son:

- Sistema de nombres de dominio (DNS): puerto TCP/UDP 53.
- Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol): puerto TCP 80.
- Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol): puerto TCP 25.

- Protocolo de oficina de correos (POP): puerto UDP 110.
- Telnet: puerto TCP 23.
- Protocolo de configuración dinámica de host: puerto UDP 67.
- Protocolo de transferencia de archivos (FTP, File Transfer Protocol): puertos TCP 20 y 21.

DNS

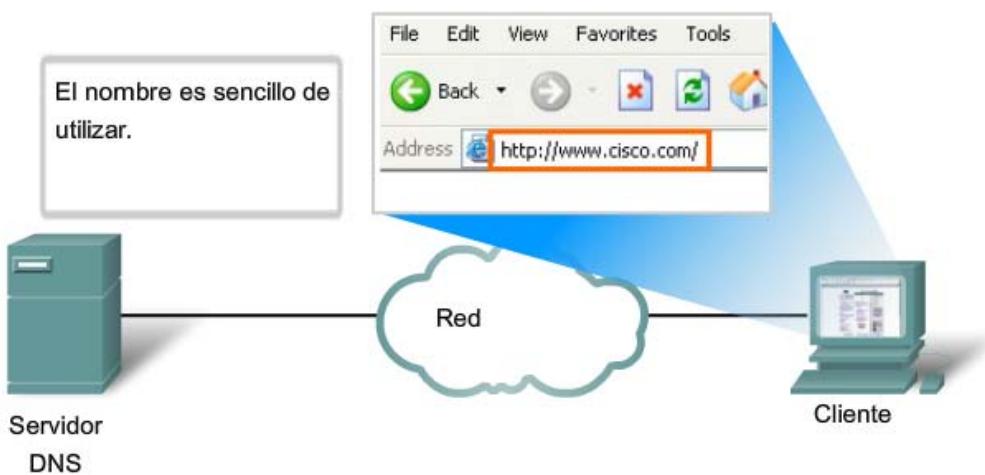
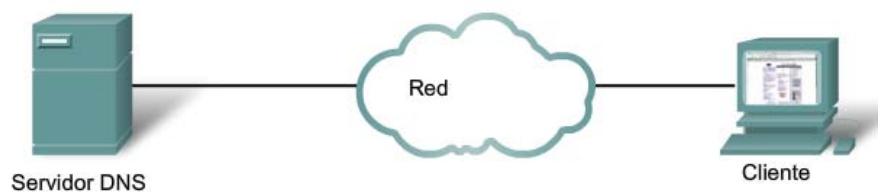
En redes de datos, los dispositivos son rotulados con direcciones IP numéricas para que puedan participar en el envío y recepción de mensajes a través de la red. Sin embargo, la mayoría de las personas pasan mucho tiempo tratando de recordar estas direcciones numéricas. Por lo tanto, los nombres de dominio fueron creados para convertir las direcciones numéricas en nombres simples y reconocibles.

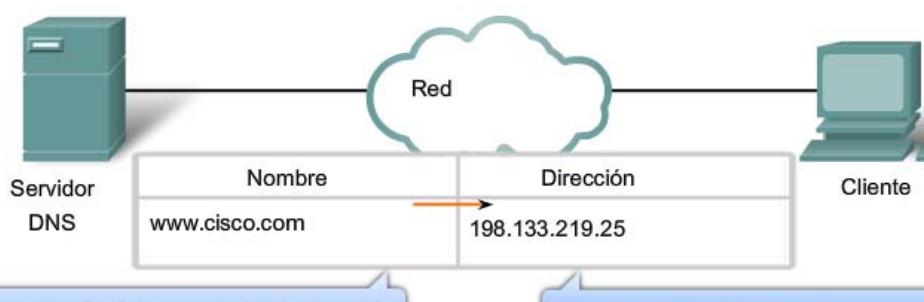
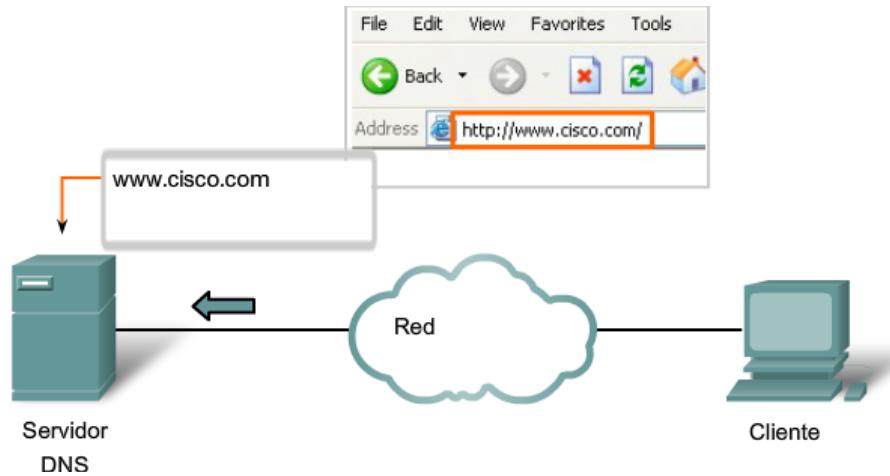
En Internet, esos nombres de dominio, como www.cisco.com, son mucho más sencillos de recordar que 198.133.219.25, que es la dirección numérica real para este servidor. Además, si Cisco decide cambiar la dirección numérica, para el usuario es transparente ya que el nombre de dominio seguirá siendo www.cisco.com. La nueva dirección simplemente estará enlazada con el nombre de dominio existente y la conectividad se mantendrá. Cuando las redes eran pequeñas, resultaba fácil mantener la asignación entre los nombres de dominios y las direcciones que representaban. Sin embargo, a medida que las redes y el número de dispositivos comenzó a crecer, el sistema manual dejó de ser práctico.

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.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye las consultas sobre formato, las respuestas y los formatos de datos. Las comunicaciones del protocolo DNS utilizan un formato simple 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.

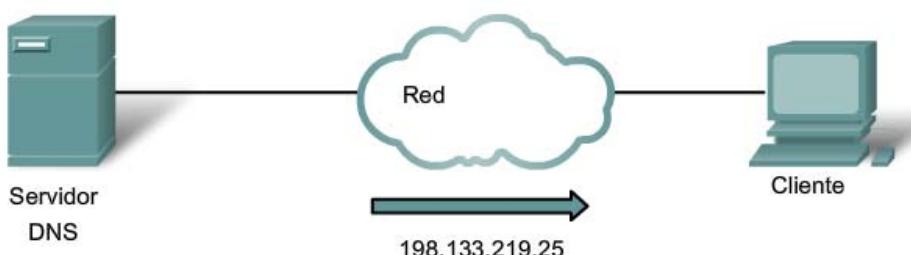
RESOLUCION DE NOMBRES DNS



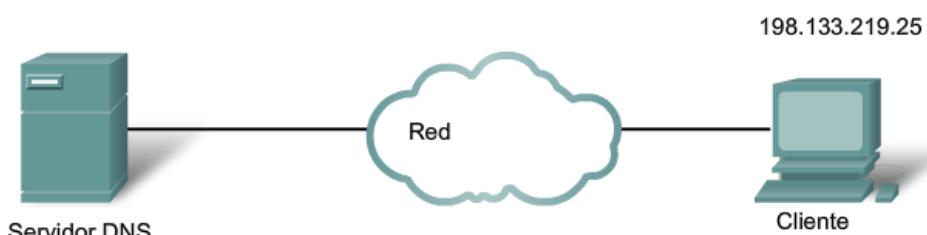


El servidor DNS hace coincidir la dirección de las personas con la dirección numérica.

El dispositivo utiliza números.



El número se envía de regreso al cliente para su utilización en la realización de solicitudes del servidor.



Se resuelve un nombre de persona legible para la dirección del dispositivo de red numérico por parte del protocolo DNS.

DNS es un servicio cliente/servidor; sin embargo, difiere de los otros servicios cliente/servidor que estamos examinando. 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 resolución de nombre para otras aplicaciones de red y servicios que lo necesiten.

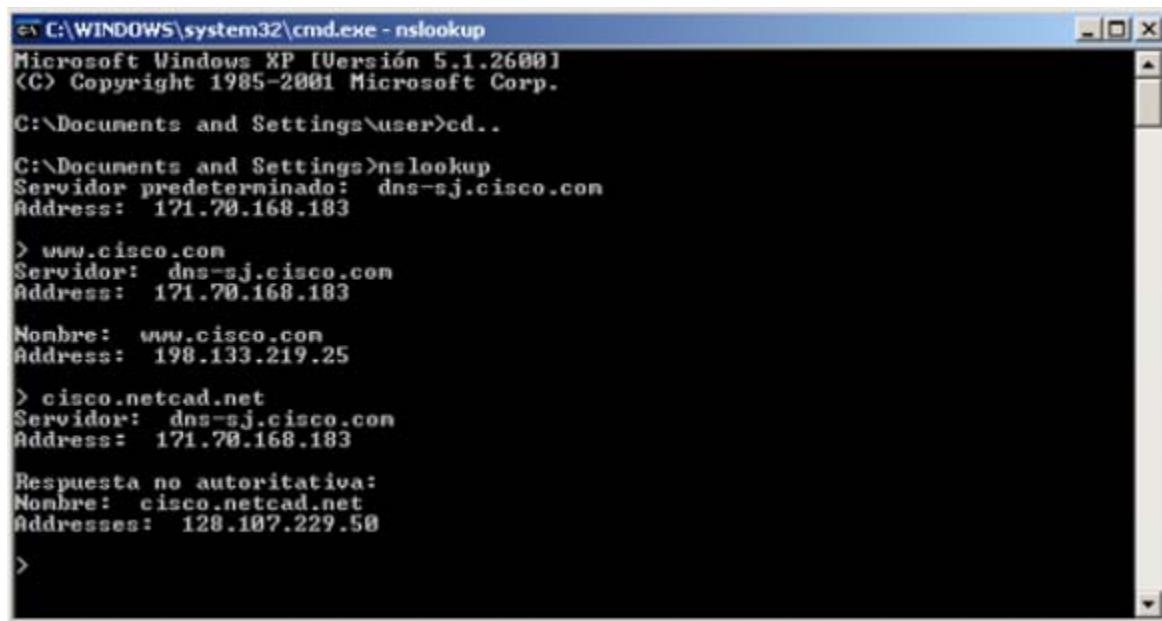
Al configurar un dispositivo de red, generalmente proporcionamos una o más direcciones del servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet provee las direcciones para utilizar con los servidores DNS. Cuando una aplicación de usuario solicita conectarse con un dispositivo remoto por nombre, el cliente DNS solicitante envía una petición a uno de esos servidores de nombre para resolver el nombre en una dirección numérica.

Los sistemas operativos informáticos también tienen una utilidad denominada nslookup que permite al usuario consultar manualmente los servidores de nombre para resolver un determinado nombre de host. Esta utilidad también puede utilizarse para resolver los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En la figura, cuando se ejecuta nslookup, se muestra el servidor DNS por defecto configurado para su host. En este ejemplo, el servidor DNS es dns-sjk.cisco.com que tiene una dirección de 171.68.226.120.

Luego podemos escribir el nombre de un host o dominio para el cual deseamos obtener la dirección. En la primer consulta de la figura, 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 lograr una extensa verificación y prueba del proceso DNS.



The screenshot shows a Windows XP command prompt window titled 'C:\WINDOWS\system32\cmd.exe - nslookup'. The window displays the following output of the nslookup command:

```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd..
C:\Documents and Settings>nslookup
Servidor predeterminado: dns-sj.cisco.com
Address: 171.70.168.183

> www.cisco.com
Servidor: dns-sj.cisco.com
Address: 171.70.168.183

Nombre: www.cisco.com
Address: 198.133.219.25

> cisco.netcad.net
Servidor: dns-sj.cisco.com
Address: 171.70.168.183

Respuesta no autoritativa:
Nombre: cisco.netcad.net
Addresses: 128.107.229.50

>
```

Un servidor DNS proporciona la resolución de nombres utilizando el daemon de nombre que generalmente se llama named (se pronuncia name-dee).

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 registro son:

- A: una dirección de un dispositivo final.
- NS: un servidor de nombre autoritativo.
- CNAME: el nombre ideal (o Nombre de dominio completamente calificado) para un alias, que se utiliza cuando varios servicios tienen una única dirección de red pero cada servicio tiene su propia entrada en DNS.
- MX: registro de intercambio de correos, asigna un nombre de dominio a una lista de servidores de intercambio de correos para ese dominio.

Cuando un cliente realiza una consulta, el proceso “nombrado” del servidor primero observa en sus propios registros para ver si puede resolver el nombre. Si no puede resolver el nombre utilizando los registros almacenados, contacta a otros servidores para hacerlo.

La solicitud puede pasar por un número de servidores, lo cual lleva tiempo adicional y consume ancho de banda. Una vez que se encuentra una coincidencia y se devuelve al servidor solicitante original, el servidor almacena temporalmente en la 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 las PC de Windows optimiza el rendimiento de la resolución de nombres DNS almacenando previamente los nombres resueltos en la memoria. El comando ipconfig /displaydns muestra todas las entradas DNS en caché en un sistema informático con Windows XP o 2000.

Formato del mensaje DNS

DNS utiliza el mismo formato de mensaje para:

- todos los tipos de consultas de clientes y respuestas de servidor
- mensajes de error
- la transferencia de información de registros de recursos entre servidores

| | |
|------------|--|
| Encabezado | |
| Pregunta | La pregunta para el servidor de nombres |
| Respuesta | Registros de recursos que responden la pregunta |
| Autoridad | Registros de recursos que apuntan a una autoridad |
| Adicional | Registros de recursos que poseen información adicional |

El sistema de nombres de dominio utiliza un sistema jerárquico para crear una base de datos para proporcionar una resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo.

En la parte superior de la jerarquía, los servidores raíz mantienen registros sobre cómo alcanzar los servidores de dominio de nivel superior, los cuales a su vez tienen registros que apuntan a los servidores de dominio de nivel secundario y así sucesivamente.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Algunos ejemplos de dominios de primer nivel son:

- .au: Australia
- .co: Colombia
- .com: una empresa o industria
- .jp: Japón
- .org: una organización sin fines de lucro

Después de los dominios de primer nivel se encuentran los dominios de segundo nivel y, debajo de estos, hay otros dominios de nivel inferior.

Cada nombre de dominio es una ruta a través de este árbol invertido que comienza desde la raíz.

Por ejemplo: como se muestra en la figura, el servidor DNS raíz puede no saber exactamente dónde se encuentra el servidor de correo electrónico mail.cisco, pero lleva un registro de los dominios “com” dentro de los dominios de primer nivel. Asimismo, los servidores dentro del dominio “com” pueden no tener un registro de mail.cisco.com, pero sí tienen un registro para el dominio “cisco.com”. Los servidores dentro del dominio cisco.com tienen un registro (un registro MX para ser exactos) para mail.cisco.com.

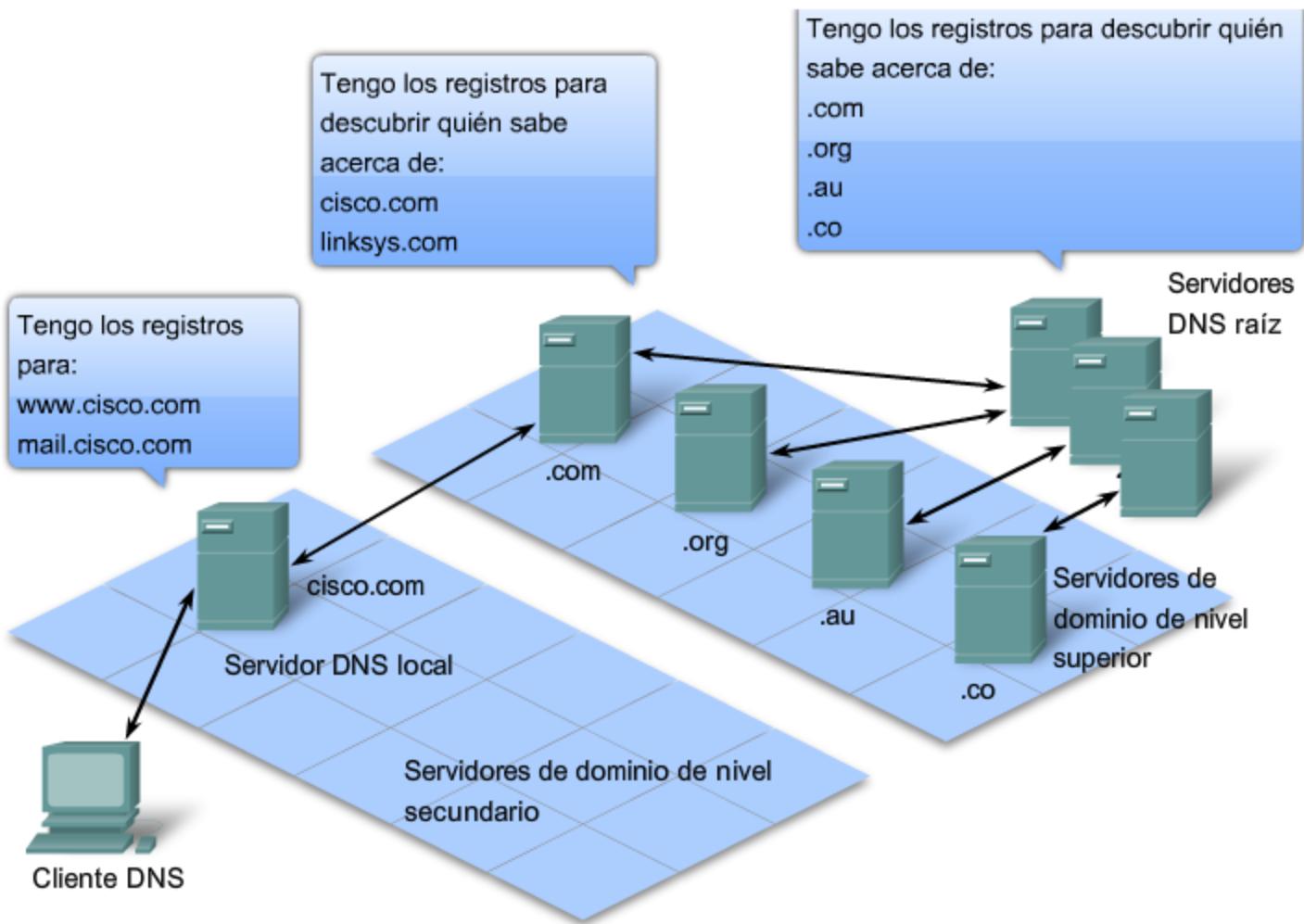
El sistema de nombres de dominio depende de esta jerarquía de servidores descentralizados y mantiene estos registros de recursos. Los registros de recursos enumeran nombres de dominios que el servidor puede resolver y servidores alternativos que también pueden procesar solicitudes. Si un determinado servidor tiene registros de recursos que corresponden a su nivel en la jerarquía de dominios, se dice que es autoritativo para esos registros.

Por ejemplo: un servidor de nombres en el dominio cisco.netacad.net no sería autoritativo para el registro mail.cisco.com porque ese registro se mantiene en un servidor de nivel de dominio superior, específicamente el servidor de nombres en el dominio cisco.com .

Enlaces

<http://www.ietf.org//rfc/rfc1034.txt>

<http://www.ietf.org/rfc/rfc1035.txt>



Una jerarquía de servidores DNS contiene los registros de recursos que coordinan los nombres con las direcciones.

3.3.2 Servicio WWW y HTTP

Cuando se escribe una dirección Web (o URL) en un explorador de Internet, el explorador establece una conexión con el servicio Web del servidor que utiliza el protocolo HTTP. URL (o Localizador uniforme de recursos) y URI (Identificador uniforme de recursos) son los nombres que la mayoría de las personas asocian con las direcciones Web.

El URL <http://www.cisco.com/index.html> es un ejemplo de un URL que se refiere a un recurso específico: una página Web denominada index.html en un servidor identificado como cisco.com (haga clic en las fichas de la figura para ver los pasos utilizados por HTTP).

Los exploradores Web son las aplicaciones de cliente que utilizan nuestras computadoras para conectarse con la World Wide Web y para acceder a los 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 realizan conexiones al servidor y solicitan los recursos deseados. El servidor responde con los recursos y, una vez recibidos, el explorador interpreta los datos y los presenta al usuario.

Los exploradores pueden interpretar y presentar muchos tipos de datos, como texto sin formato o Lenguaje de marcado de hipertexto (HTML, el lenguaje que se utiliza para construir una página Web). Otros tipos de datos, sin embargo, requieren de otro servicio o programa. Generalmente se los conoce como plug-ins o complementos. Para ayudar al

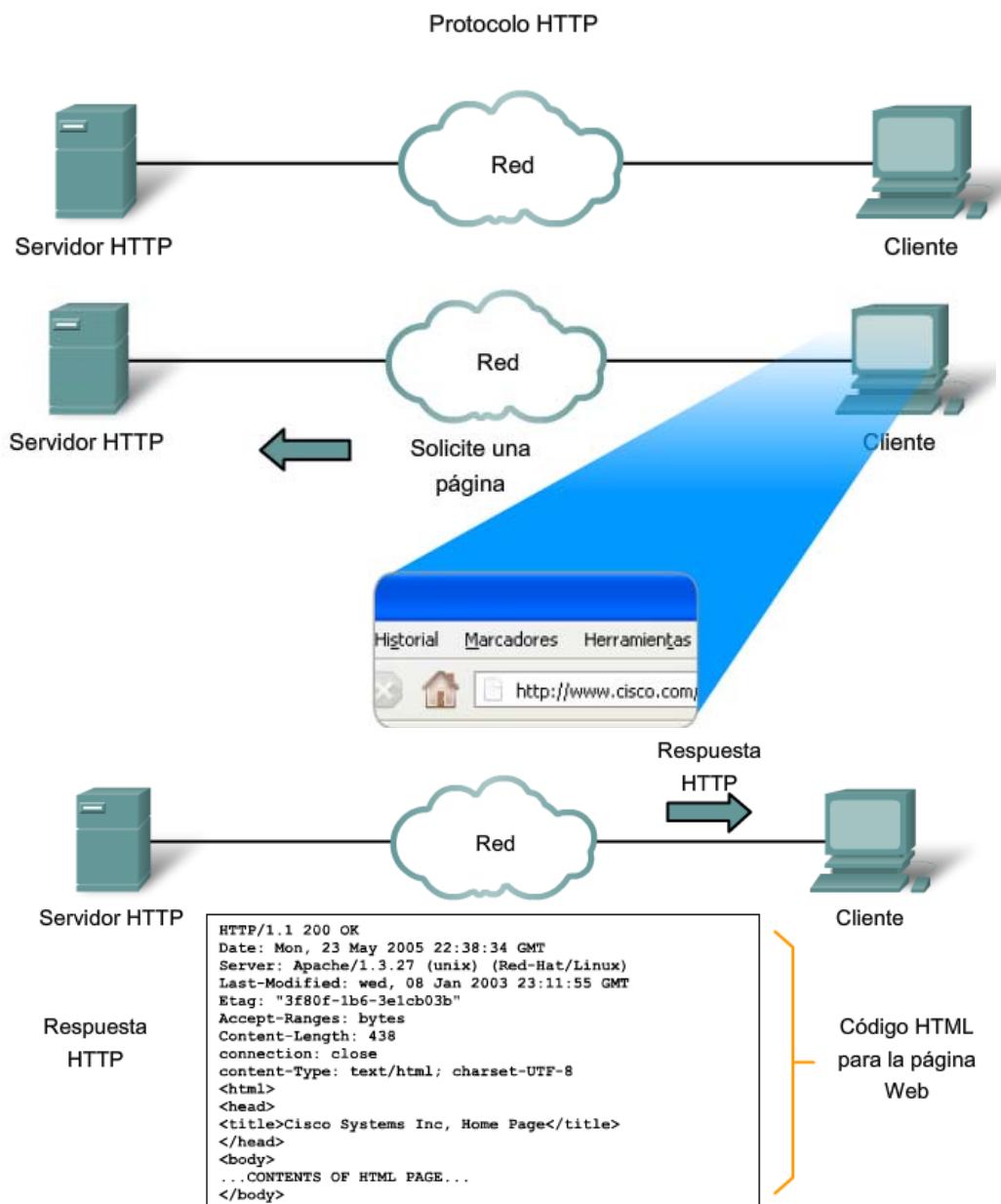
explorador a determinar qué tipo de archivo está recibiendo, el servidor especifica qué clase de datos contiene el archivo.

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, utilizaremos la dirección URL: <http://www.cisco.com/web-server.htm>.

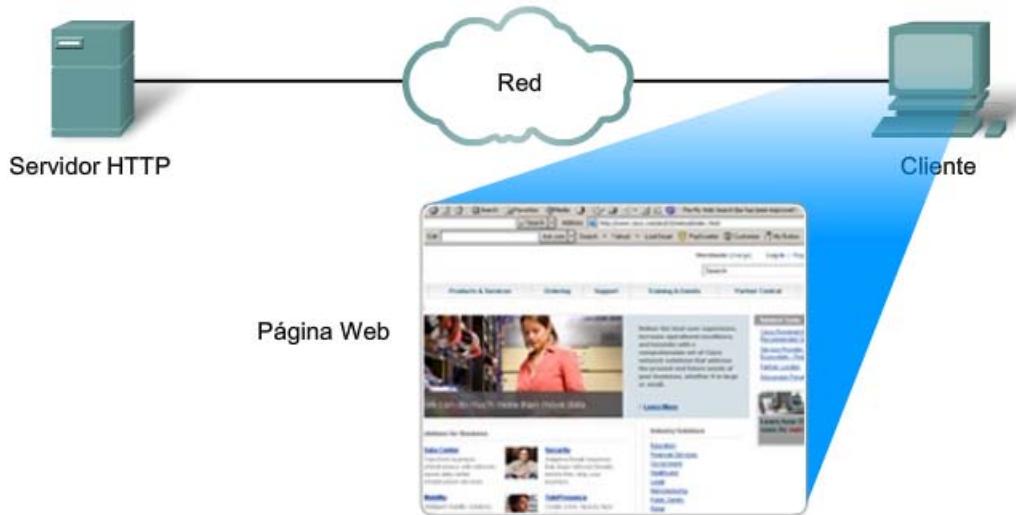
Primero, el explorador interpreta las tres partes de la URL:

1. http (el protocolo o esquema),
2. www.cisco.com (el nombre del servidor), y
3. web-server.htm (el nombre específico del archivo solicitado).

El explorador luego verifica con un servidor de nombres para convertir a www.cisco.com en una dirección numérica que utilizará para conectarse con el servidor. Al utilizar los requerimientos del protocolo HTTP, el explorador envía una solicitud GET al servidor y pide el archivo web-server.htm. El servidor, a su vez, envía al explorador el código HTML de esta página Web. Finalmente, el explorador descifra el código HTML y da formato a la página para la ventana del explorador.



En respuesta a la solicitud, el servidor HTTP envía el código para una página Web.



El navegador interpreta el código HTML y muestra una página Web.

El protocolo de transferencia de hipertexto (HTTP), uno de los protocolos del grupo TCP/IP, se desarrolló en sus comienzos para publicar y recuperar las páginas HTML, y en la actualidad se utiliza para sistemas de información distribuidos y de colaboración. HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados.

HTTP especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador Web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página Web y envía los tipos de mensajes que el servidor utiliza para responder. Los tres tipos de mensajes más comunes son GET, POST y PUT.

GET es una solicitud de datos del cliente. Un explorador Web envía el mensaje GET para solicitar las páginas desde un servidor Web. Como se muestra en la figura, una vez que el servidor recibe la solicitud GET, responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje solo, cuyo cuerpo puede ser el archivo solicitado, un mensaje de error o alguna otra información.

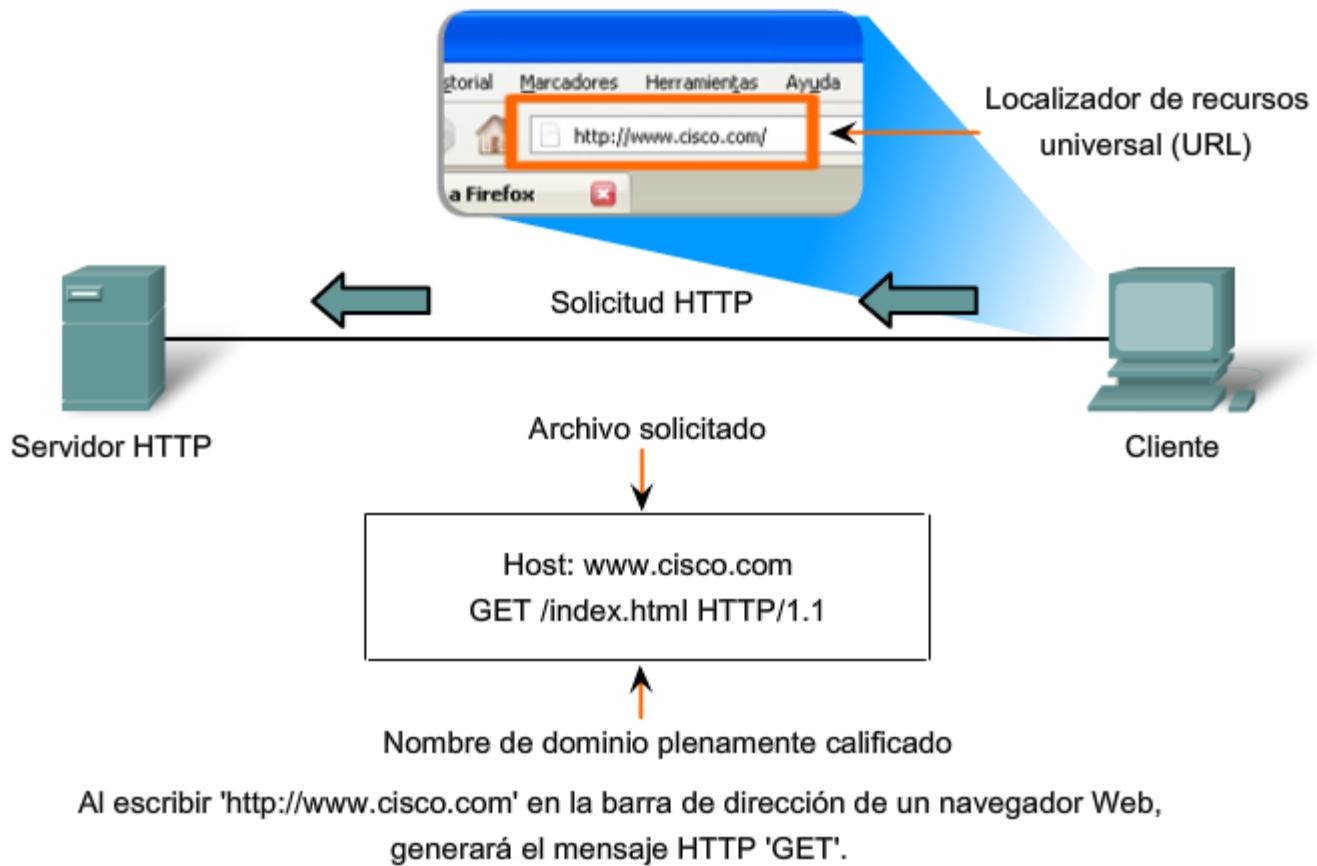
POST y PUT se utilizan para enviar mensajes que cargan los datos al servidor Web. Por ejemplo, cuando el usuario ingresa datos en un formulario incorporado en una página Web, POST incluye los datos en el mensaje enviado al servidor.

PUT carga los recursos o el contenido al servidor Web.

Aunque es muy flexible, HTTP no es un protocolo seguro. Los mensajes POST cargan 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 son descifradas.

Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS) para acceder o subir información al servidor Web. HTTPS puede utilizar autenticación y encriptación para asegurar los datos cuando viajan entre el cliente y el servidor. HTTPS especifica reglas adicionales para pasar los datos entre la capa de Aplicación y la capa de Transporte.

Protocolo HTTP mediante GET

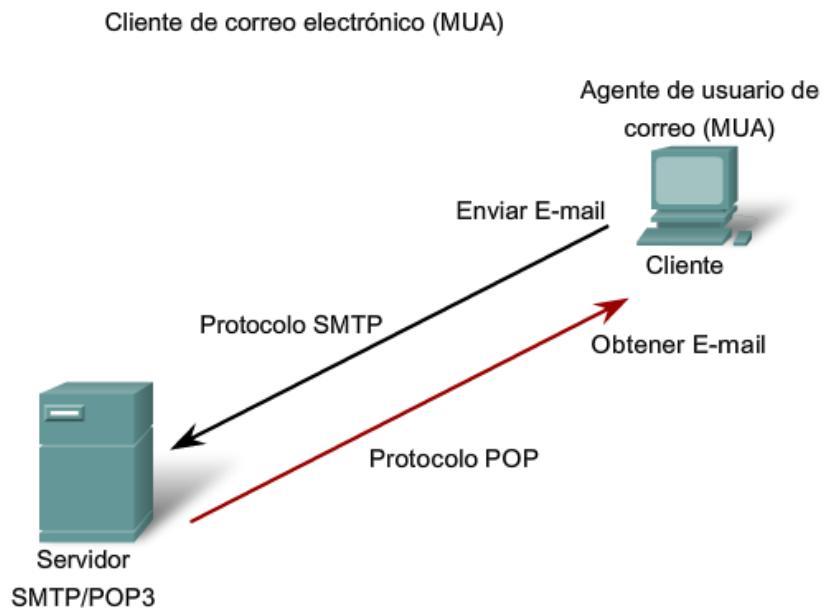


3.3.3 Servicios de email y protocolos SMTP/POP

E-mail, el servidor de red más conocido, ha revolucionado la manera en que nos comunicamos, por su simpleza y velocidad. Inclusive para ejecutarse en una computadora o en otro dispositivo, los e-mails requieren de diversos servicios y aplicaciones. Dos ejemplos de protocolos de capa de aplicación son Protocolo de oficina de correos (POP) y Protocolo simple de transferencia de correo (SMTP), que aparecen en la figura. Como con HTTP, estos protocolos definen procesos cliente-servidor.

Cuando una persona escribe mensajes de correo electrónico, generalmente utiliza una aplicación denominada Agente de usuario de correo (MUA) o cliente de correo electrónico. MUA permite enviar los mensajes y colocar los mensajes recibidos en el buzón del cliente; ambos procesos son diferentes.

Para recibir e-mails desde un servidor de e-mail, el cliente de correo electrónico puede utilizar un POP. Al enviar un e-mail desde un cliente o un servidor, se utilizan formatos de mensajes y cadenas de comando definidas por el protocolo SMTP. En general, un cliente de correo electrónico proporciona la funcionalidad de ambos protocolos dentro de una aplicación.

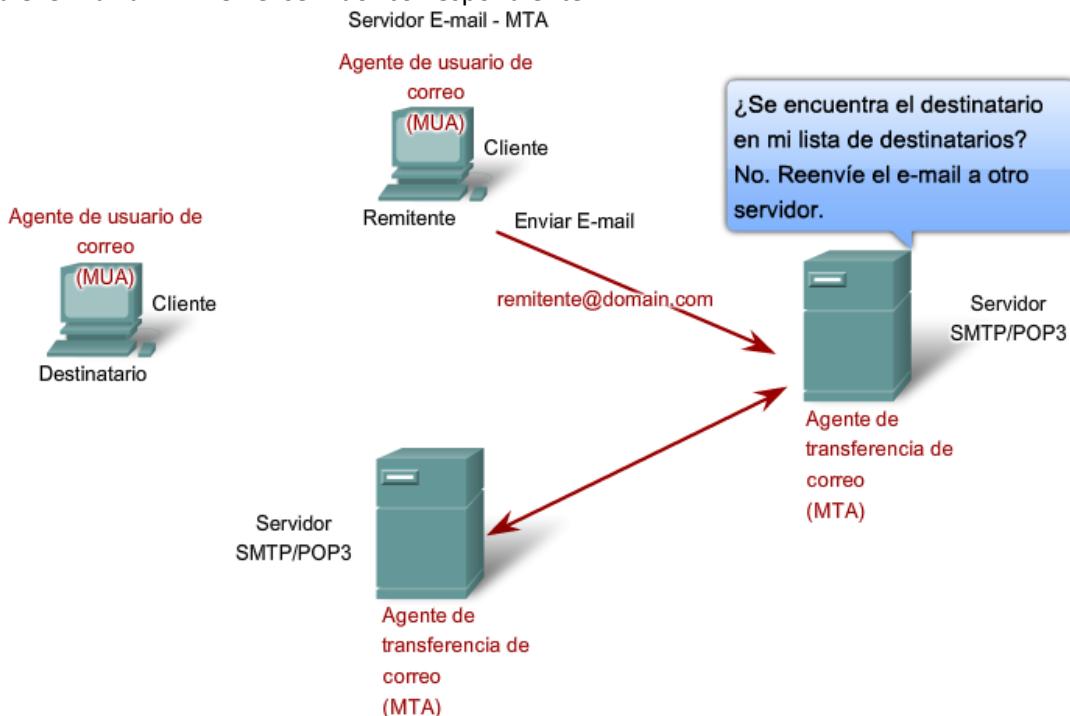


Los clientes envían e-mails a un servidor mediante SMTP y reciben e-mails mediante POP3.

Procesos del servidor de e-mail: MTA y MDA

- El servidor de e-mail ejecuta dos procesos individuales:
- Agente de transferencia de correo (MTA, Mail Transfer Agent).
- Agente de entrega de correo (MDA, Mail Delivery Agent).

El proceso Agente de transferencia de correo (MTA) se utiliza para enviar correos electrónicos. Como se muestra en la figura, el MTA recibe mensajes desde el MUA u otro MTA en otro servidor de e-mail. Según el encabezado del mensaje, determina cómo debe reenviarse un mensaje para llegar a destino. Si el correo está dirigido a un usuario cuyo buzón está en el servidor local, el correo se pasa al MDA. Si el correo es para un usuario que no está en el servidor local, el MTA enruta el e-mail al MTA en el servidor correspondiente.



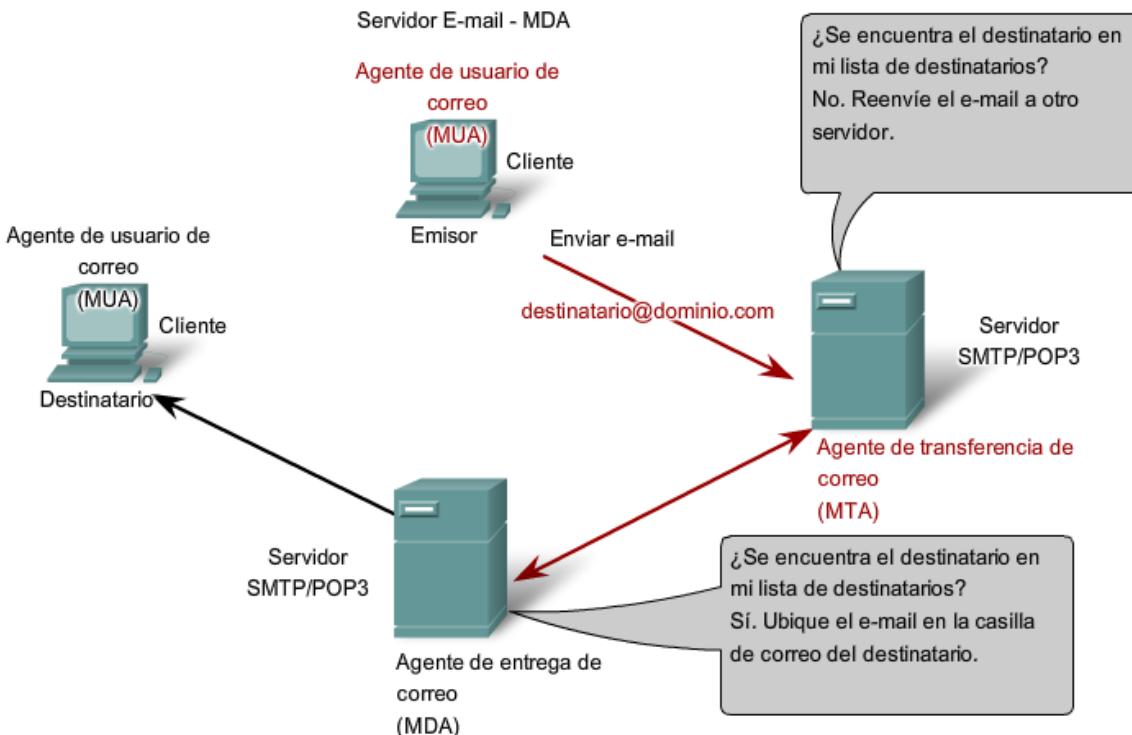
El proceso de agente de transferencia de correo rige el manejo de e-mails entre servidores.

En la figura, vemos que el Agente de envío de correo (MDA) acepta una parte del e-mail desde un Agente de transferencia de correo (MTA) y realiza el envío real. El MDA recibe todo el correo entrante desde el MTA y lo coloca en los buzones de los usuarios correspondientes. El MDA también puede resolver temas de entrega final, como análisis de virus, correo no deseado filtrado y manejo de acuses de recibo. La mayoría de las comunicaciones de e-mail utilizan las aplicaciones MUA, MTA y MDA. Sin embargo, existen otras alternativas para enviar e-mails.

El cliente puede estar conectado a un sistema de e-mails corporativo, como Lotus Notes de IBM, Groupwise de Novell o Microsoft Exchange. Estos sistemas a veces tienen su propio formato interno de correo electrónico y sus clientes generalmente se comunican con el servidor de correo electrónico a través de un protocolo propietario.

El servidor envía o recibe correos electrónicos por Internet a través de la 95ersión de correo de internet del producto, que realiza el reformato que sea necesario. Si, por ejemplo, dos personas que trabajan para la misma empresa intercambian e-mails entre ellos utilizando un protocolo propietario, los mensajes pueden permanecer completamente dentro del sistema de e-mails corporativo de la empresa.

Como segunda alternativa, las computadoras que no tienen un MUA pueden conectarse a un servicio de correo en un explorador Web para así recuperar y enviar mensajes. Algunas computadoras pueden ejecutar su propio MTA y administrar e-mails de dominio interno.



El proceso de agente de entrega de correo rige la entrega de e-mails entre servidores y clientes.

Como se mencionó anteriormente, los e-mails pueden utilizar los protocolos POP y SMTP (vea la figura para saber cómo funcionan). POP y POP3 (Protocolo de oficina de correos v.3) son protocolos de envío de correo entrante y protocolos cliente/servidor típicos. Envían e-mails desde el servidor de e-mail al cliente (MUA). El MDA escucha cuando un cliente se conecta a un servidor. Una vez establecida la conexión, el servidor puede enviar el e-mail al cliente.

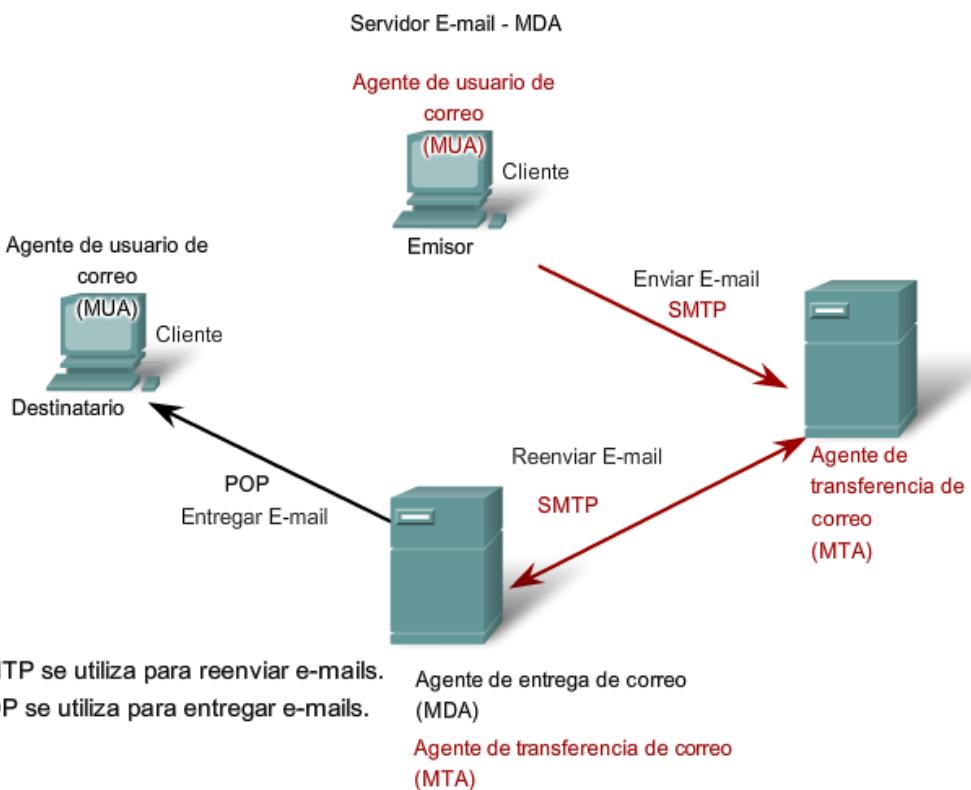
El protocolo simple de transferencia de correo (SMTP), por el contrario, rige la transferencia de e-mails salientes desde el cliente emisor al servidor de e-mail (MDA), como así también el transporte de e-mails entre servidores de e-mail.

(MTA). SMTP permite transportar e-mails por las redes de datos entre diferentes tipos de software de cliente y servidor, y hace posible el intercambio de e-mails en Internet.

El formato de mensajes del protocolo SMTP utiliza un conjunto rígido de comandos y respuestas. Estos comandos admiten los procedimientos utilizados en el SMTP, como inicio de sesión, transacción de correo, reenvío de correo, verificación de nombres de buzones, expansión de listas de correo y apertura y cierre de intercambios.

Algunos de los comandos especificados en el protocolo SMTP son:

- HELO: identifica el proceso de cliente SMTP para el proceso de servidor SMTP.
- EHLO: es la versión más nueva de HELO, que incluye extensiones de servicios, y
- MAIL FROM: identifica al emisor.
- RCPT TO: identifica al receptor, y
- DATA: identifica el cuerpo del mensaje.



3.3.4 FTP

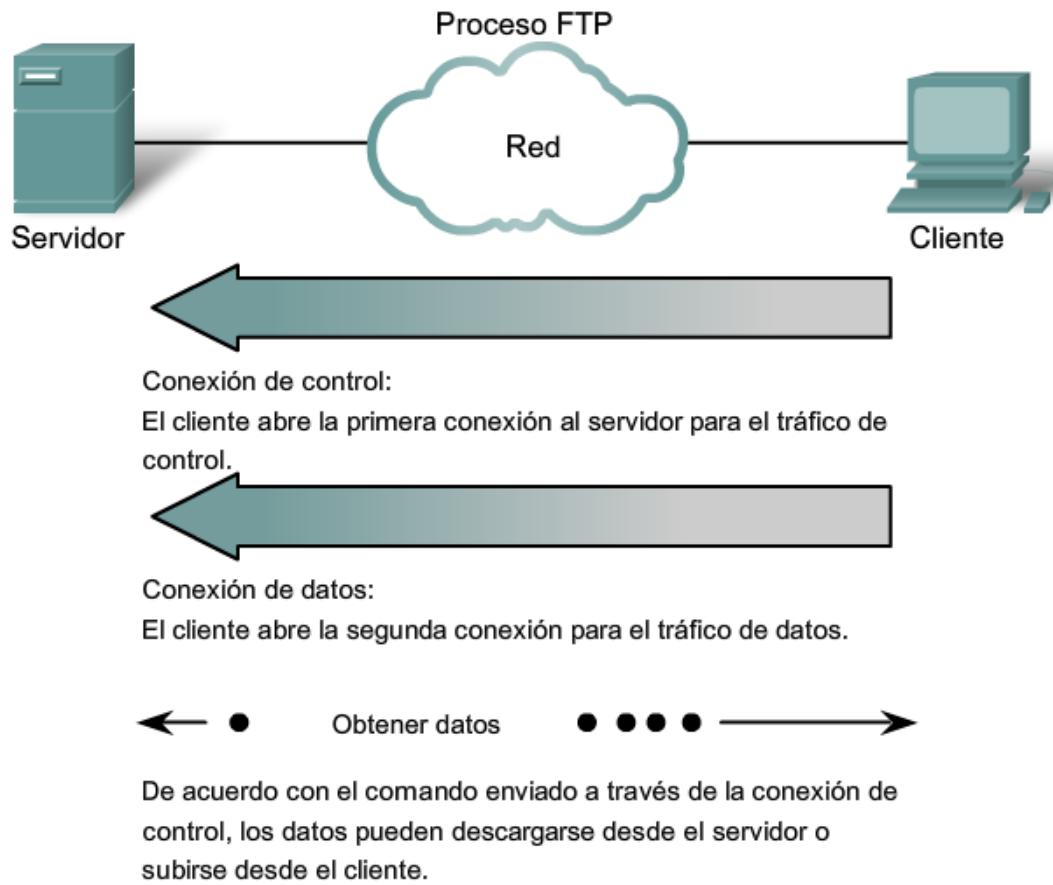
El protocolo de transferencia de archivos (FTP) es otro protocolo de la capa de aplicación comúnmente utilizado. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y se utiliza para cargar y descargar archivos desde un servidor que ejecuta el daemon FTP (FTPd).

Para transferir los archivos en forma exitosa, el FTP requiere de dos conexiones entre cliente y servidor: una para comandos y respuestas, otra para la transferencia real de archivos.

El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor.

El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo.

La transferencia de archivos puede producirse en ambas direcciones. El cliente puede descargar (bajar) un archivo desde el servidor o el cliente puede cargar (subir) un archivo en el servidor.



3.3.5 DHCP

El servicio Protocolo de configuración dinámica de host (DHCP) 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, gateways y otros parámetros de redes IP.

DHCP permite a un host obtener una dirección IP en forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor DHCP elige una dirección de un rango configurado de direcciones denominado “pool” y se la asigna (“alquila”) al host por un período establecido.

En redes locales más grandes o donde cambia frecuentemente la población usuaria, es preferible el DHCP. Los nuevos usuarios llegan con computadoras portátiles y necesitan una conexión. Otros tienen nuevas estaciones de trabajo que necesitan conexión. En lugar de tener direcciones IP asignadas por el administrador de red en cada estación de trabajo, resulta más eficiente tener direcciones IP asignadas en forma automática utilizando un DHCP.

Las direcciones de DHCP distribuidas no se asignan a los hosts en forma permanente, sólo se alquilan durante un período de tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esto es muy útil para los usuarios móviles que entran y salen de la red. 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 realice la conexión del hardware, ya sea mediante una LAN inalámbrica o conectada por cable.

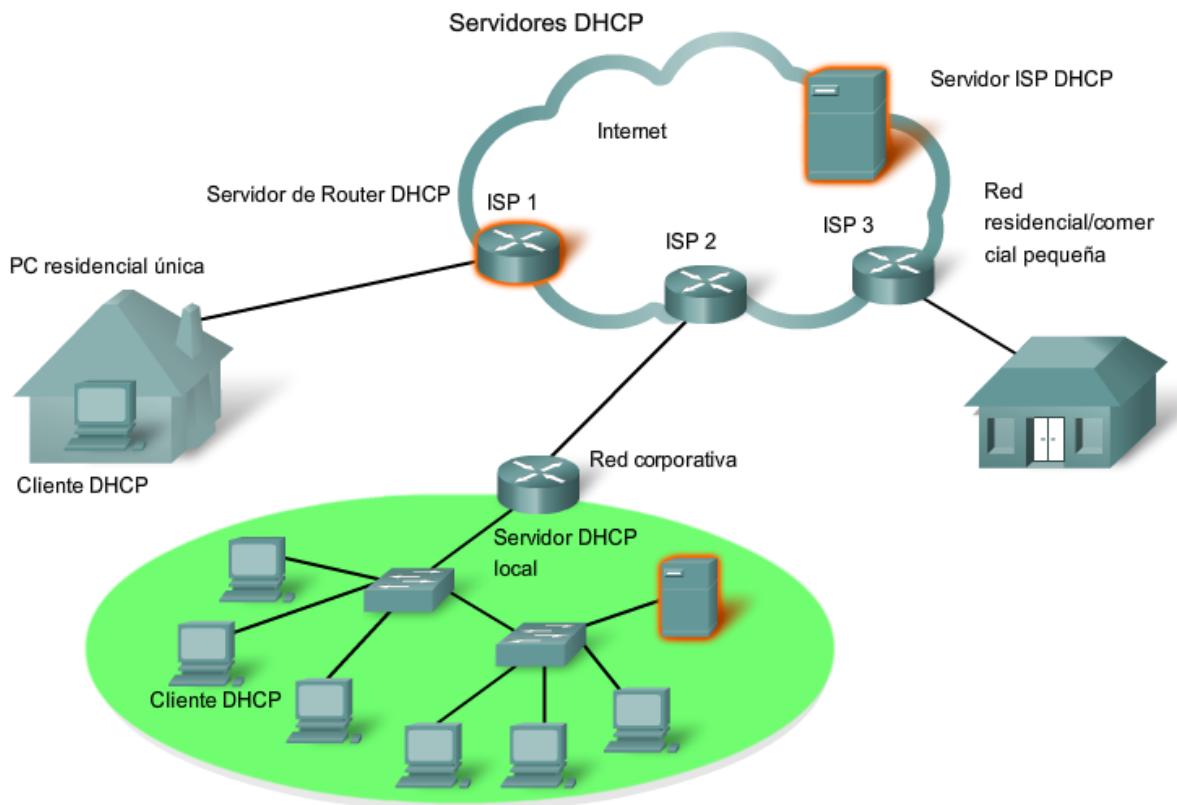
DHCP hace posible el acceso a Internet utilizando zonas activas inalámbricas en aeropuertos o cafés. Una vez que ingresa al área, el cliente de DHCP de la computadora portátil contacta al servidor de DHCP mediante una conexión inalámbrica. El servidor de DHCP asigna una dirección IP a la computadora portátil.

Como muestra la figura, diferentes tipos de dispositivos pueden ser servidores de DHCP al ejecutar el software de servicio de DHCP. El servidor de DHCP en la mayoría de las redes medianas y grandes está generalmente ubicado en un servidor dedicado local basado en PC.

Con las redes domésticas, el servidor de DHCP se ubica en el ISP y un host de la red doméstica recibe la configuración IP directamente desde el ISP.

DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace de la seguridad física un factor importante a la hora de determinar si se utiliza direccionamiento manual o dinámico.

Los direccionamientos dinámico y estático tienen su lugar en los diseños de red. Muchas redes utilizan tanto el direccionamiento estático como el DHCP. DHCP se utiliza para hosts de propósitos generales, como los dispositivos de usuario final, y las direcciones fijas se utilizan para dispositivos de red como gateways, switches, servidores e impresoras.



Sin DHCP los usuarios tiene que ingresar manualmente la dirección IP, la máscara de subred y otras configuraciones para poder unirse a la red. 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 (alquiladas) en lugar de estáticas (asignadas en forma permanente), las direcciones en desuso regresan automáticamente al pool para volver a asignarse. Cuando un dispositivo configurado por DHCP se inicia o conecta a la red, el cliente envía un paquete DESCUBRIMIENTO de DHCP para identificar cualquier servidor de DHCP disponible en la red. Un servidor DHCP

contesta con una oferta de DHCP, que es un mensaje de oferta de alquiler con información asignada de dirección IP, máscara de subred, servidor DNS y 99ersión por defecto, como también la duración del alquiler.

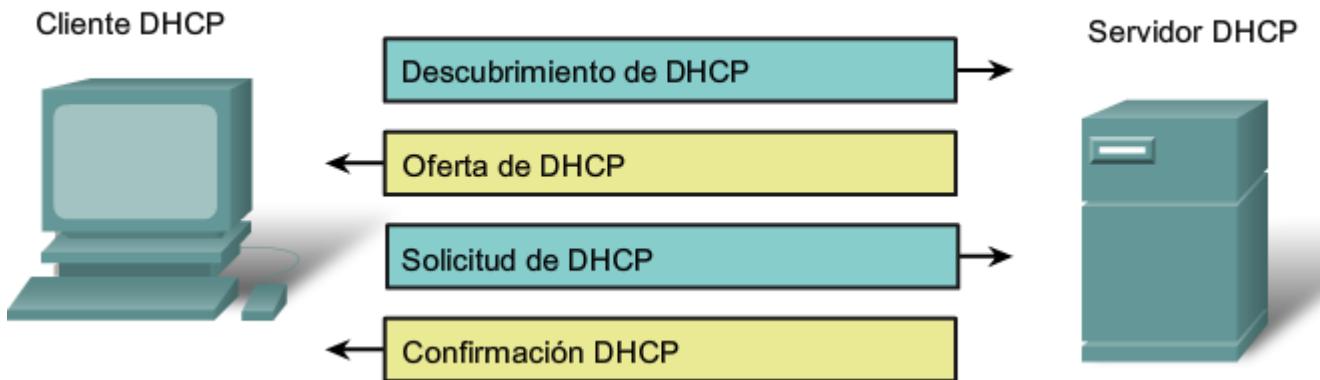
El cliente puede recibir varios paquetes de oferta de DHCP si hay más de un servidor DHCP en la red local, por lo tanto debe escoger entre ellos y enviar un broadcast de paquete con una solicitud de DHCP que identifique el servidor y la oferta de alquiler específicos que el cliente está aceptando. Un cliente puede elegir solicitar una dirección previamente asignada por el servidor.

Teniendo en cuenta que la dirección IP solicitada por el cliente u ofrecida por el servidor, aún es válida, el servidor devolverá un mensaje ACK DHCP que le informa al cliente que finalizó el alquiler. Si la oferta ya no es válida, quizás debido al tiempo o a que a otro cliente se le asignó el alquiler, el servidor seleccionado responderá con un mensaje NAK DHCP (acuse de recibo negativo). Si se envía un mensaje NAK DHCP, el proceso de selección debe comenzar nuevamente con la transmisión de un nuevo mensaje DHCP DISCOVER.

Una vez que el cliente tenga el alquiler, debe renovarse antes de la expiración del alquiler por medio de otro mensaje DHCP REQUEST.

El servidor de DHCP asegura que todas las direcciones son únicas (una dirección IP no puede asignarse a dos dispositivos de red diferentes en 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 las direcciones a sus clientes que no solicitan direcciones estáticas.

El cuarto curso de Exploración de CCNA cubrirá el funcionamiento de DHCP con más detalle.



3.3.6 Protocolo SMB y servicios para compartir archivos

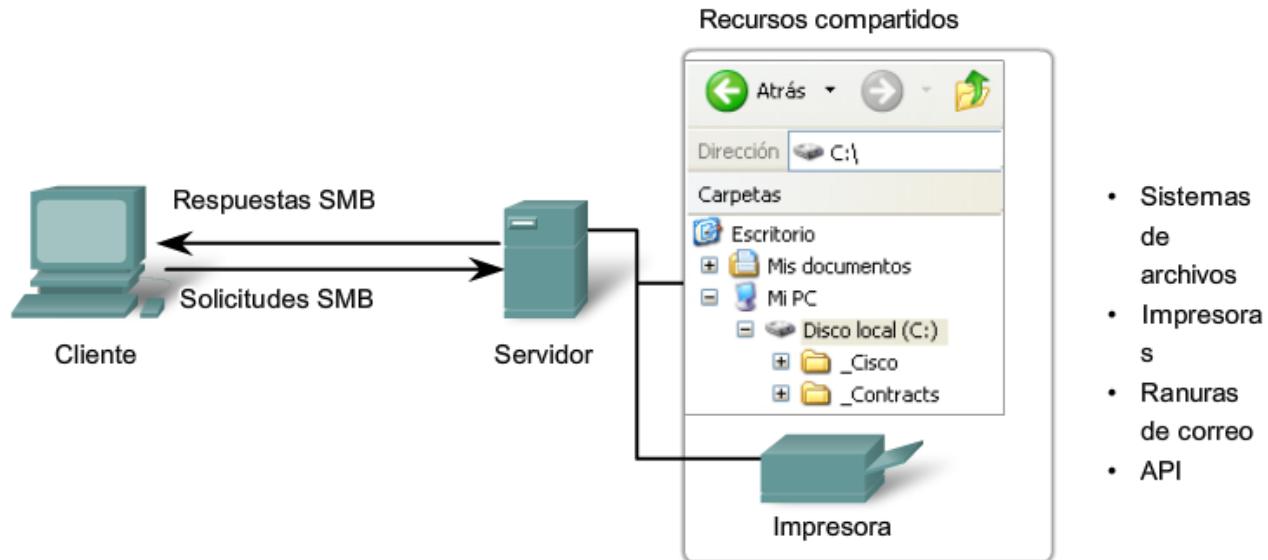
El Bloque de mensajes del servidor (SMB) es un protocolo cliente-servidor para compartir archivos. IBM desarrolló el Bloque de mensajes del servidor (SMB) a fines de la década del '80 para describir la estructura de recursos de red compartidos, como directorios, archivos, impresoras y puertos seriales. Es un protocolo de solicitud-respuesta. A diferencia del protocolo para compartir archivos respaldado por 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 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 Windows 2000 del software, 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. Comenzando con Windows 2000, todos los productos subsiguientes

de Microsoft utilizan denominación DNS. Esto permite a los protocolos TCP/IP admitir directamente el compartir recursos SMB, como se muestra en la figura.

Los sistemas operativos LINUX y UNIX también proporcionan un método para compartir recursos con las redes Microsoft a través de una versión de SMB denominada SAMBA. Los sistemas operativos Macintosh de Apple también admiten recursos compartidos utilizando el protocolo SMB.

Compartir archivos mediante el protocolo SMB



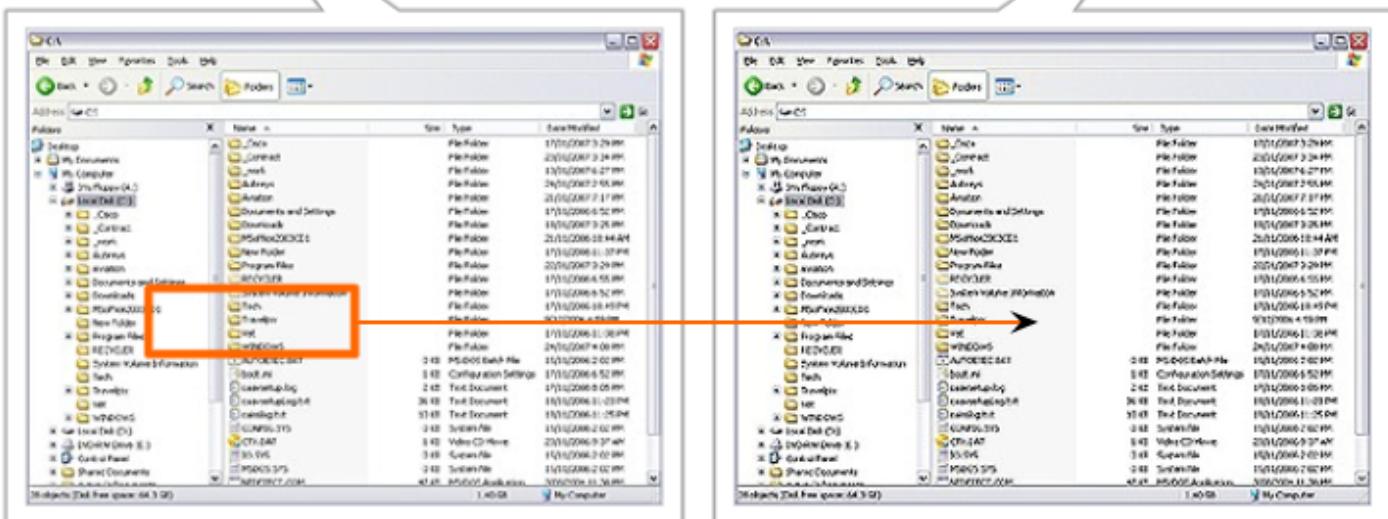
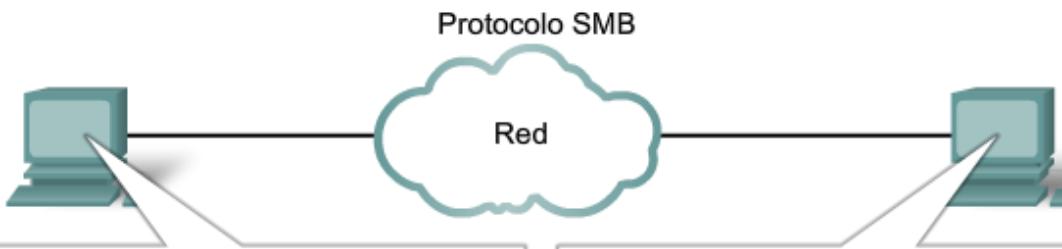
SMB es un protocolo de solicitud-respuesta y cliente-servidor. Los servidores pueden poner sus recursos a disposición de los clientes en la red.

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 por un parámetro de tamaño variable y un componente de datos.

Los mensajes SMB pueden:

- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a archivos e impresoras
- Permitir a una aplicación enviar o recibir mensajes hacia o desde otro dispositivo

El proceso de intercambio de archivos SMB se muestra en la figura.



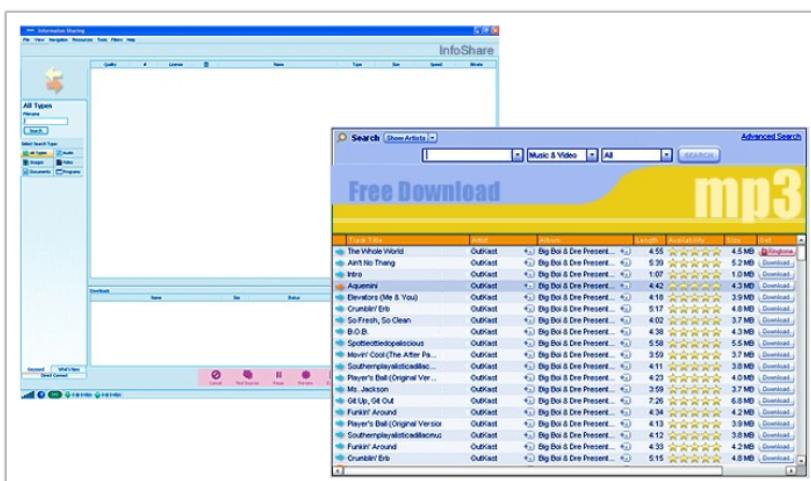
Puede copiarse un archivo desde una PC a otra con Windows Explorer mediante el protocolo SMB.

3.3.7 Protocolo GNUTTELA y servicios P2P

Aprendimos acerca de FTP y SMB como formas de obtener archivos; aquí presentamos otro protocolo de aplicación. Compartir archivos en Internet se ha transformado en algo muy popular. Con las aplicaciones P2P basadas en el protocolo Gnutella, las personas pueden colocar archivos en sus discos rígidos para que otros los descarguen. El software del cliente compatible con Gnutella permite a los usuarios conectarse con los servicios Gnutella en Internet, ubicarlos y acceder a los recursos compartidos por otros pares Gnutella.

Muchas aplicaciones del cliente están disponibles para acceder en la red Gnutella, entre ellas: BearShare, Gnucleus, LimeWire, Morpheus, WinMX y XoloX (consulte una captura de pantalla de LimeWire en la figura). Mientras que el Foro de desarrolladores de Gnutella mantiene el protocolo básico, los proveedores de las aplicaciones generalmente desarrollan extensiones para lograr que el protocolo funcione mejor en las aplicaciones.

Aplicaciones punto a punto

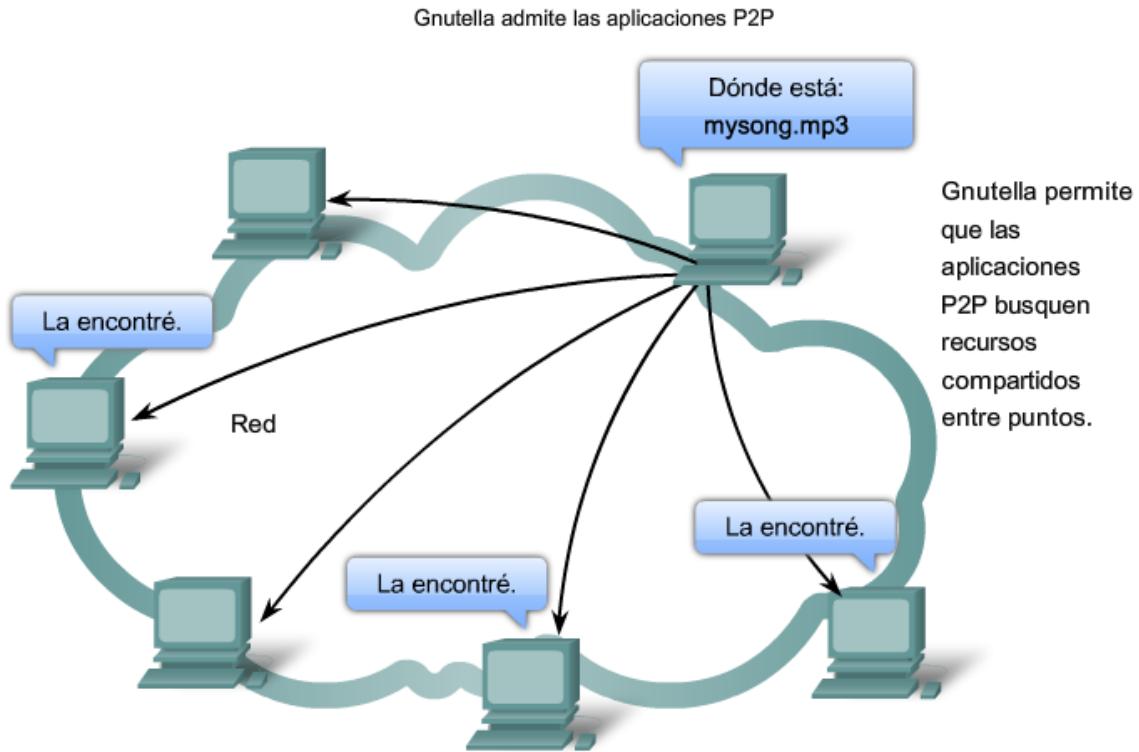


Muchas de las aplicaciones P2P no utilizan una base de datos central para registrar todos los archivos disponibles en los puntos. Por el contrario, los dispositivos en la red se indican entre ellos qué archivos están disponibles cuando hay una consulta, y utilizan el protocolo Gnutella y los servicios para respaldar los recursos ubicados. Consulte la figura.

Cuando un usuario se conecta a un servicio Gnutella, las aplicaciones del cliente buscarán otros nodos Gnutella para conectarse. Estos nodos manejan las consultas para las ubicaciones de los recursos y responden a dichas solicitudes. Además, gobiernan los mensajes de control que ayudan al servicio a descubrir otros nodos. Las verdaderas transferencias de archivos generalmente dependen de los servicios HTTP.

El protocolo Gnutella define cinco tipos de paquetes diferentes:

- ping: para descubrir un dispositivo,
- pong: como respuesta a un ping,
- consulta: para ubicar un archivo,
- query hit: como respuesta a una consulta, y
- push: como una solicitud de descarga.



3.3.8 Protocolo y servicios Telnet

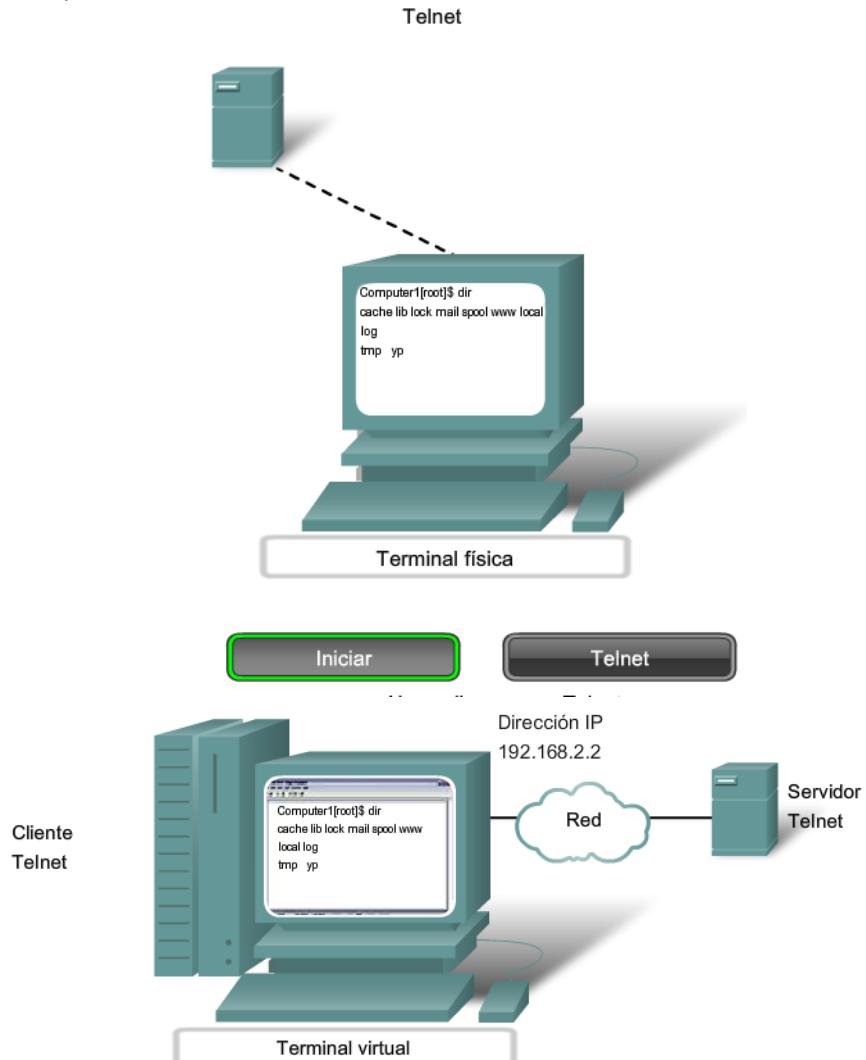
Mucho antes de que existieran las computadoras de escritorio con interfaces gráficas sofisticadas, las personas utilizaban sistemas basados en textos que eran simplemente terminales conectadas físicamente a una computadora central. Una vez que las redes estuvieron disponibles, las personas necesitaban acceder en forma remota a los sistemas informáticos de la misma manera en que lo hacían con las terminales conectadas en forma directa.

Telnet se desarrolló para satisfacer esta necesidad. Telnet se remonta a principios de la década de los setenta y se encuentra entre los servicios y protocolos de capa de aplicación más antiguo dentro del grupo TCP/IP. Telnet proporciona un método estándar de emulación de dispositivos de terminal basados en texto en la red de datos. El protocolo y el software del cliente que implementa el protocolo comúnmente se definen como Telnet.

Y como consecuencia, una conexión que utiliza Telnet se llama Sesión o conexión de terminal virtual (VTY). En lugar de utilizar un dispositivo físico para conectar al servidor, Telnet utiliza software para crear un dispositivo virtual que proporciona las mismas funciones que una sesión terminal con acceso a la Interfaz de línea de comandos (CLI) del servidor.

Para admitir conexiones al cliente Telnet, el servidor ejecuta un servicio llamado daemon de Telnet. Se establece una conexión de terminal virtual desde un dispositivo final utilizando una aplicación del cliente Telnet. La mayoría de los sistemas operativos incluye un cliente de Telnet de la capa de aplicación. En una PC de Microsoft Windows, Telnet puede ejecutarse desde la entrada del comando. Otras aplicaciones de terminal comunes que ejecutan clientes de Telnet son HyperTerminal, Minicom y TeraTerm.

Una vez establecida una conexión Telnet, los usuarios pueden realizar cualquier función autorizada en el servidor, como si utilizaran una sesión de línea de comandos en el servidor mismo. Si están autorizados, pueden iniciar y detener procesos, configurar el dispositivo e incluso correr el sistema.



Telnet proporciona una forma de utilizar una computadora, conectada a través de la red, para acceder a un dispositivo de red como si el teclado y el monitor estuvieran conectados directamente al dispositivo.



Telnet es un protocolo cliente-servidor y especifica cómo se establece y se termina una sesión VTY. Además proporciona la sintaxis y el orden de los comandos utilizados para iniciar la sesión Telnet, como así también los comandos de control que pueden ejecutarse durante una sesión. Cada comando Telnet consiste en por lo menos dos bytes. El primer byte es

un carácter especial denominado Interpretar como comando (IAC). Como su nombre lo indica, el IAC define el byte siguiente como un comando en lugar de un texto.

Algunos de los comandos del protocolo Telnet de muestra son:

Are You There (AYT): Permite al usuario solicitar que aparezca algo en la pantalla del terminal para indicar que la sesión VTY está activa.

Erase Line (EL): Elimina todo el texto de la línea actual.

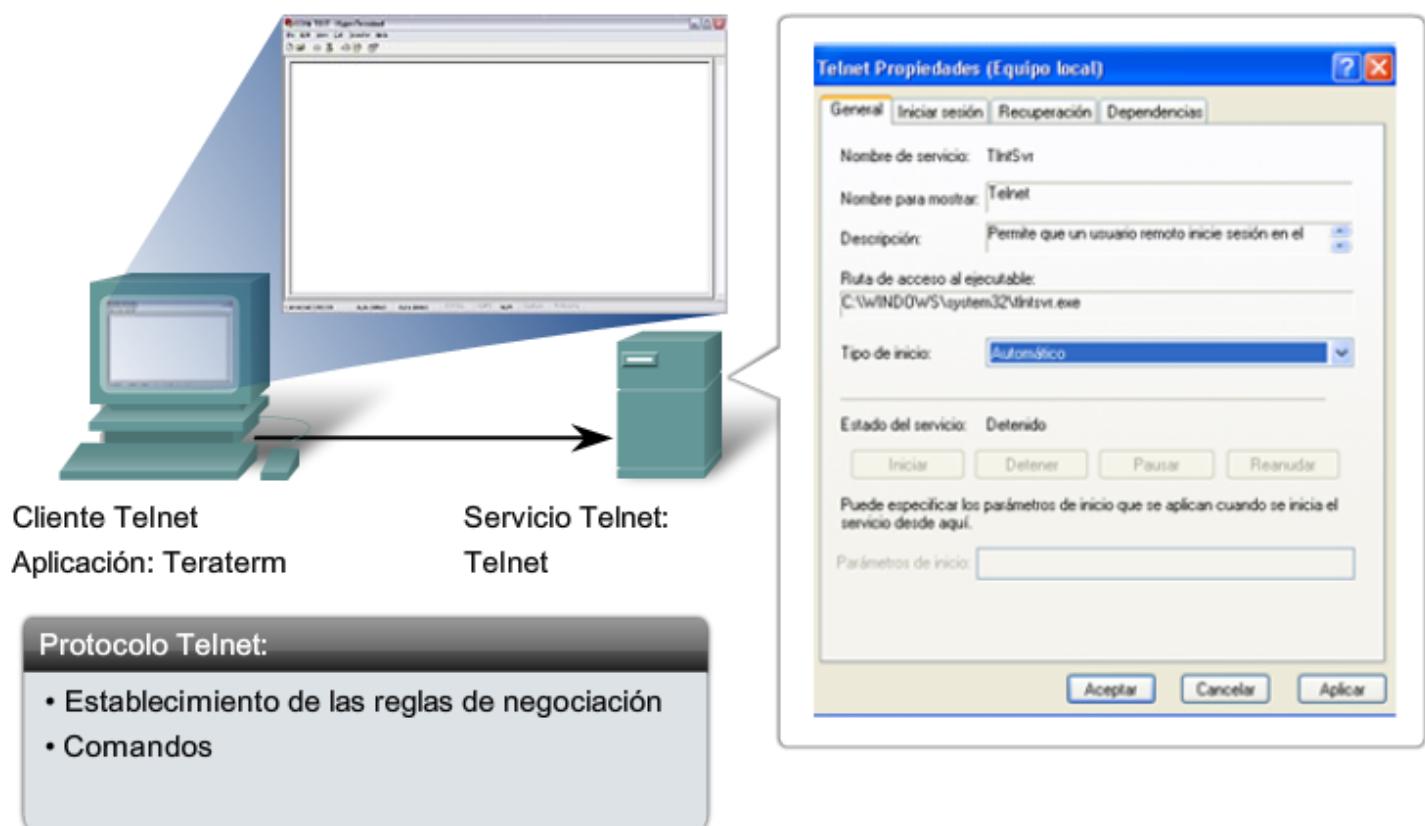
Interrupt Process (IP): Suspende, interrumpe, aborta o termina el proceso al cual se conectó la terminal virtual. Por ejemplo, si un usuario inició un programa en el servidor Telnet por medio de VTY, puede enviar un comando IP para detener el programa.

Aunque el protocolo Telnet admite autenticación de usuario, no admite el transporte de datos encriptados. Todos los datos intercambiados durante una sesión Telnet se transportan como texto sin formato por la red. Esto significa que los datos pueden ser interceptados y entendidos fácilmente.

Si la seguridad es un problema, el protocolo Shell seguro (SSH) ofrece un método seguro y alternativo para acceder al servidor. SSH proporciona la estructura para un inicio de sesión remoto seguro y otros servicios de red seguros. Además proporciona mayor autenticación que Telnet y admite el transporte de datos de sesión utilizando cifrado. Como una mejor práctica, los profesionales de red deberían siempre utilizar SSH en lugar de Telnet, cada vez que sea posible.

Más adelante en este curso, utilizaremos Telnet y SSH para acceder y configurar los dispositivos de red en la red de laboratorios.

Telnet: Aplicación, servicio y protocolo



3.5 RESUMEN DEL CAPITULO

3.5.1 Resumen y revisión

La capa de Aplicación es responsable del acceso directo a los procesos subyacentes que administran y envían la comunicación a la red humana. Esta capa sirve como origen y destino de las comunicaciones en las redes de datos.

Las aplicaciones, los protocolos y servicios de la capa de Aplicación permiten a los usuarios interactuar con la red de datos de manera significativa y efectiva.

Las aplicaciones son programas informáticos con los cuales el usuario interactúa e inicia el proceso de transferencia de datos a pedido del usuario.

Los servicios son programas básicos que proporcionan la conexión entre la capa de Aplicación y las capas inferiores del modelo de networking.

Los protocolos proporcionan una estructura de reglas y procesos acordados previamente que asegura que los servicios que funcionan en un dispositivo en particular puedan enviar y recibir datos desde una variedad de dispositivos de red diferentes.

El envío de datos en la red puede ser solicitado desde un servidor por un cliente o entre dispositivos que funcionan en una conexión punto a punto, donde la relación cliente/servidor se establece según qué dispositivo es el origen y cuál el destino en ese tiempo. Los mensajes se intercambian entre los servicios de la capa de Aplicación en cada dispositivo final según las especificaciones del protocolo para establecer y utilizar estas relaciones.

Los protocolos como HTTP, por ejemplo, admiten el envío de páginas Web a dispositivos finales. Los protocolos SMTP/POP admiten el envío y la recepción de correos electrónicos. SMB permite a los usuarios compartir archivos. DNS resuelve los nombres utilizados para referirse a los recursos de red en direcciones numéricas utilizables por la red.

En este capítulo, aprendió a:

- Describir la manera en que las funciones de las tres capas superiores del modelo OSI proporcionan servicios de red a las aplicaciones de usuario final.
- Describir la manera en que los protocolos de la capa de Aplicación de TCP/IP proporcionan los servicios especificados por las capas superiores del modelo OSI.
- Definir la manera en que las personas utilizan la capa de la Aplicación para comunicarse a través de la red de información.
- Describir la función de las aplicaciones de TCP/IP conocidas, tales como World Wide Web e e-mail, y sus servicios relacionados (HTTP, DNS, SMB, DHCP, STMP/POP y Telnet).
- Describir los procesos de capacidad para compartir archivos que utilizan las aplicaciones punto a punto y el protocolo Gnutella.
- Explicar la manera en que los protocolos garantizan que los servicios que se ejecutan en un tipo de dispositivo puedan enviar y recibir datos desde varios dispositivos de red diferentes.
- Usar herramientas de análisis de red para examinar y explicar la forma en que funcionan las aplicaciones de usuario.

4 Capa de transporte del modelo OSI

4.0 INTRODUCCION DEL CAPITULO

4.0.1 Introducción del capítulo

Las redes de datos e Internet brindan soporte a la red humana al proporcionar la comunicación continua y confiable entre las personas, tanto de manera local como alrededor del mundo. En un único dispositivo, las personas pueden utilizar varios servicios como e-mails, la Web y la mensajería instantánea para enviar mensajes o recuperar información. Las aplicaciones como clientes de correo electrónico, exploradores Web y clientes de mensajería instantánea permiten que las personas utilicen las computadoras y las redes para enviar mensajes y buscar información.

Los datos de cada una de estas aplicaciones se empaquetan, transportan y entregan al daemon de servidor o aplicación adecuados en el dispositivo de destino. Los procesos descritos 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 es responsable de la transferencia de extremo a extremo general de los datos de aplicación.

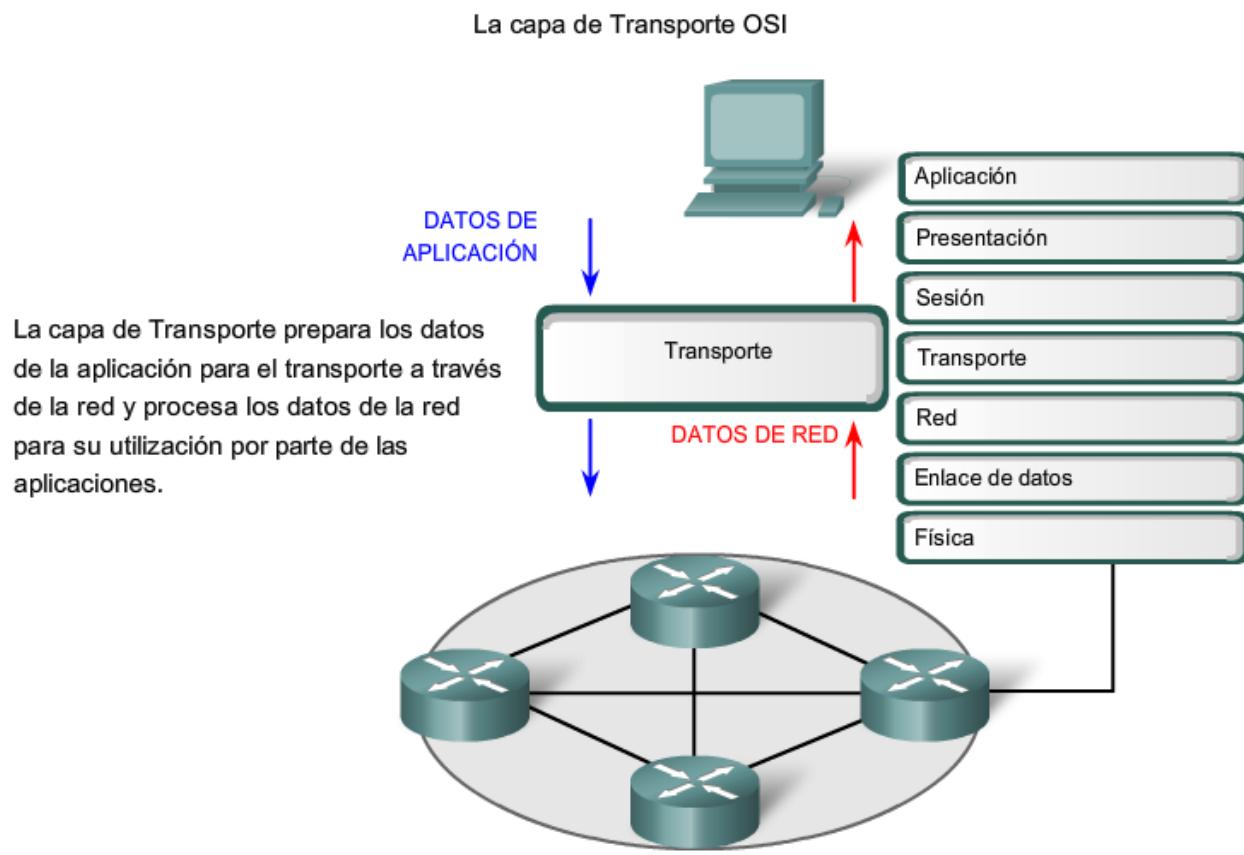
En este capítulo, se examina el rol de la capa de Transporte cuando se encapsulan los datos de aplicación para usarse en la capa de Red. La capa de Transporte incluye también las siguientes funciones:

- permitir múltiples aplicaciones para comunicarse a través de la red al mismo tiempo en un solo dispositivo,
- asegurar que, si se requiere, todos los datos sean recibidos de manera confiable y en orden por la aplicación correcta, y
- emplear mecanismos de manejo de error

Objetivos de aprendizaje

Al completar este capítulo podrá realizar tareas relacionadas con:

- 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 las funciones de dos protocolos TCP/IP de la capa de transporte: TCP y UDP.
- Explicar las funciones clave de la capa de Transporte incluyendo confiabilidad, direccionamiento de puerto y 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.



4.1 FUNCIONES DE LA CAPA DE TRASPORTE

4.1.1 Propósito de la capa de trasporte

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

- seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino,
- segmentación de datos y gestión de cada porción,
- reensamble de segmentos en flujos de datos de aplicación, e
- identificación de las diferentes aplicaciones.

Seguimiento de Conversaciones individuales

Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de Transporte mantener los diversos streams de comunicación entre estas aplicaciones.

Segmentación de datos

Debido a que cada aplicación genera un stream de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables. Los protocolos de la capa de Transporte describen los servicios que segmentan estos datos de la capa de Aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

Reensamblaje de segmentos

En el host de recepción, cada sección de datos puede ser dirigida a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de Aplicación. Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para reensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación.

Identificación de las aplicaciones

Para poder transferir los streams de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador 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. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

La capa de Transporte es el enlace entre la capa de Aplicación y las capas inferiores, que son responsables de la transmisión en la red. Esta capa acepta datos de distintas conversaciones y los transfiere a las capas inferiores como secciones manejables que puedan ser eventualmente multiplexadas a través del medio.

Las aplicaciones no necesitan conocer los detalles de operación de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red.

Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado. Luego la capa de Transporte ordena estas secciones antes de entregarlas a la aplicación adecuada.

Los requerimientos de datos varían

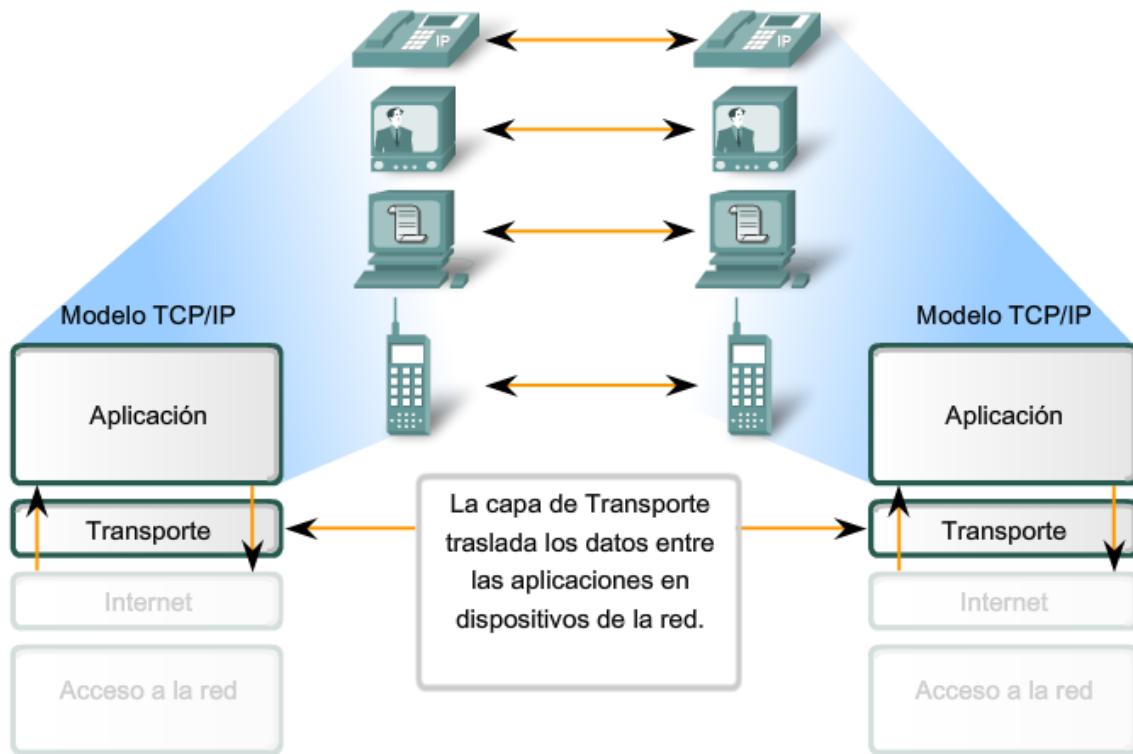
Debido a que las distintas aplicaciones poseen distintos requerimientos, existen varios protocolos de la capa de Transporte. Para algunas aplicaciones, los segmentos deben llegar en una secuencia específica de manera que puedan ser procesados en forma exitosa. En algunos casos, todos los datos deben recibirse para ser utilizados por cualquiera de las mismas. En otros casos, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red.

En las redes convergentes actuales, las aplicaciones con distintas necesidades de transporte pueden comunicarse en la misma red. Los distintos protocolos de la capa de Transporte poseen distintas reglas que permiten que los dispositivos gestionen los diversos requerimientos de datos.

Algunos protocolos proporcionan sólo las funciones básicas para la entrega eficiente de las secciones de datos entre las aplicaciones adecuadas. Estos tipos de protocolos son útiles para aquellas aplicaciones cuyos datos son sensibles a las demoras.

Otros protocolos de la capa de Transporte describen procesos que brindan funciones adicionales, como asegurar la entrega confiable entre las aplicaciones. Si bien estas funciones adicionales proveen una comunicación más sólida entre aplicaciones de la capa de Transporte, representan la necesidad de utilizar recursos adicionales y generan un mayor número de demandas en la red.

Habilitación de aplicaciones en los dispositivos para la comunicación



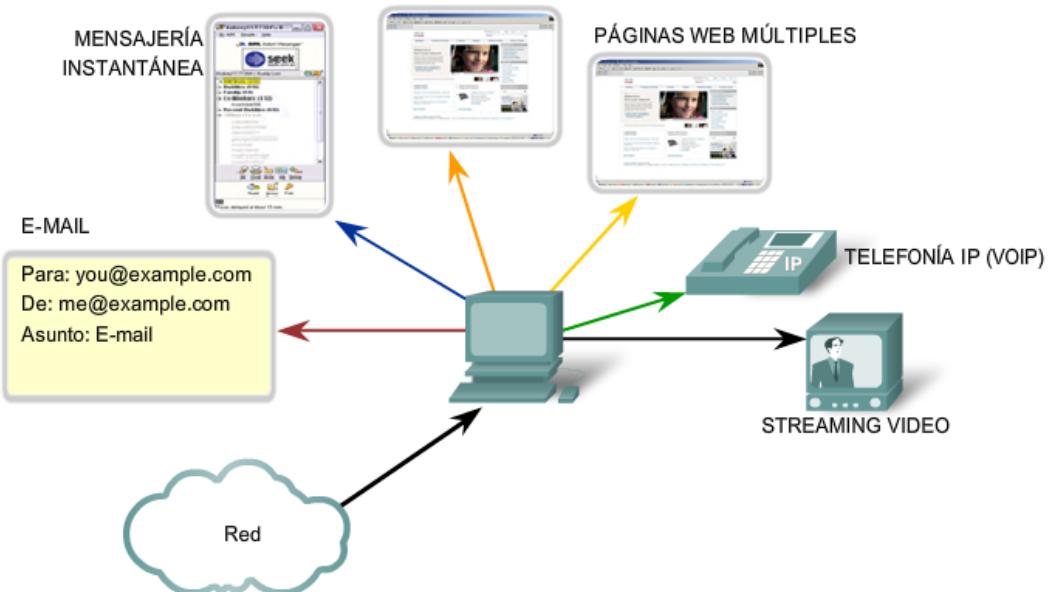
Separación de comunicaciones múltiples

Considere una computadora conectada a una red que recibe y envía e-mails y mensajes instantáneos, explora sitios Web y realiza una llamada telefónica de VoIP de manera simultánea. Cada una de estas aplicaciones envía y recibe datos en la red al mismo tiempo. Sin embargo, los datos de la llamada telefónica no se dirigen al explorador Web y el texto de un mensaje instantáneo no aparece en el e-mail.

Además, los usuarios precisan que un e-mail o una página Web sean recibidos y presentados de manera completa para que la información sea considerada útil. Las demoras leves se consideran aceptables para asegurar que se reciba y presente la información completa.

Por el contrario, la pérdida ocasional de pequeñas partes de una conversación telefónica puede considerarse aceptable. Se puede inferir la parte de audio perdida del contexto de la conversación o se puede solicitar a la otra persona que repita lo que dijo. Es preferible esto último a las demoras que se producirían si se solicita a la red que gestione y vuelva a enviar los segmentos perdidos. En este ejemplo, el usuario, no la red, gestiona el reenvío o reemplazo de información que falta.

Seguimiento de conversaciones



La capa de Transporte segmenta los datos y administra la separación de datos para diferentes aplicaciones. Las aplicaciones múltiples que se ejecutan en un dispositivo reciben los datos correctos.

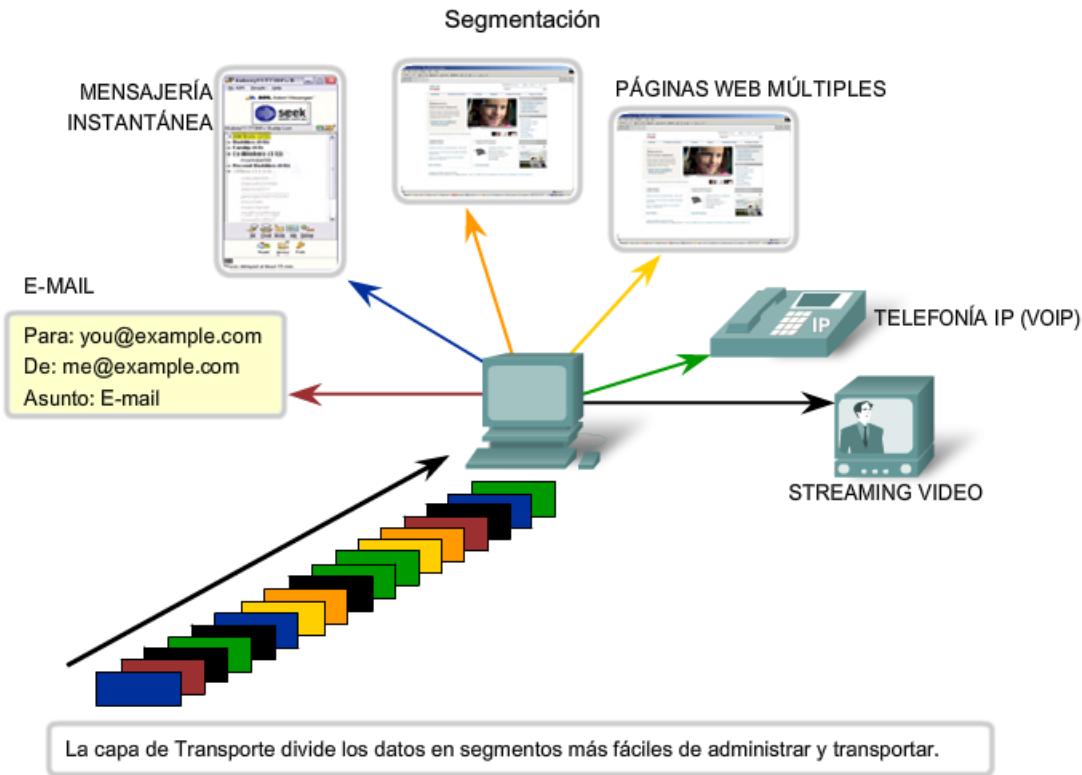
Como se explicó en un capítulo anterior, el envío de algunos tipos de datos, un vídeo por ejemplo, a través de la red como un stream de comunicación completa puede impedir que se produzcan otras comunicaciones al mismo tiempo. También hace difícil la recuperación de errores y la retransmisión de datos dañados.

La división de los datos en partes pequeñas y el envío de estas partes desde el origen hacia el destino permiten que se puedan entrelazar (multiplexar) distintas comunicaciones en la misma red.

La segmentación de los datos, que cumple con los protocolos de la capa de Transporte, proporciona los medios para enviar y recibir datos cuando se ejecutan varias aplicaciones de manera concurrente en una computadora. Sin segmentación, sólo una aplicación, la corriente de vídeo por ejemplo, podría recibir datos. No se podrían recibir correos electrónicos, chats ni mensajes instantáneos ni visualizar páginas Web y ver un vídeo al mismo tiempo.

En la capa de Transporte, cada conjunto de secciones en particular que fluyen desde una aplicación de origen a una de destino se conoce como conversación.

Para identificar todos los segmentos de datos, la capa de Transporte agrega un encabezado a la sección que contiene datos binarios. Este encabezado contiene campos de bits. Son los valores de estos campos los que permiten que los distintos protocolos de la capa de Transporte lleven a cabo las diversas funciones.



4.1.2 Control de las conversaciones

Las funciones principales especificadas por todos los protocolos de la capa de Transporte incluyen:

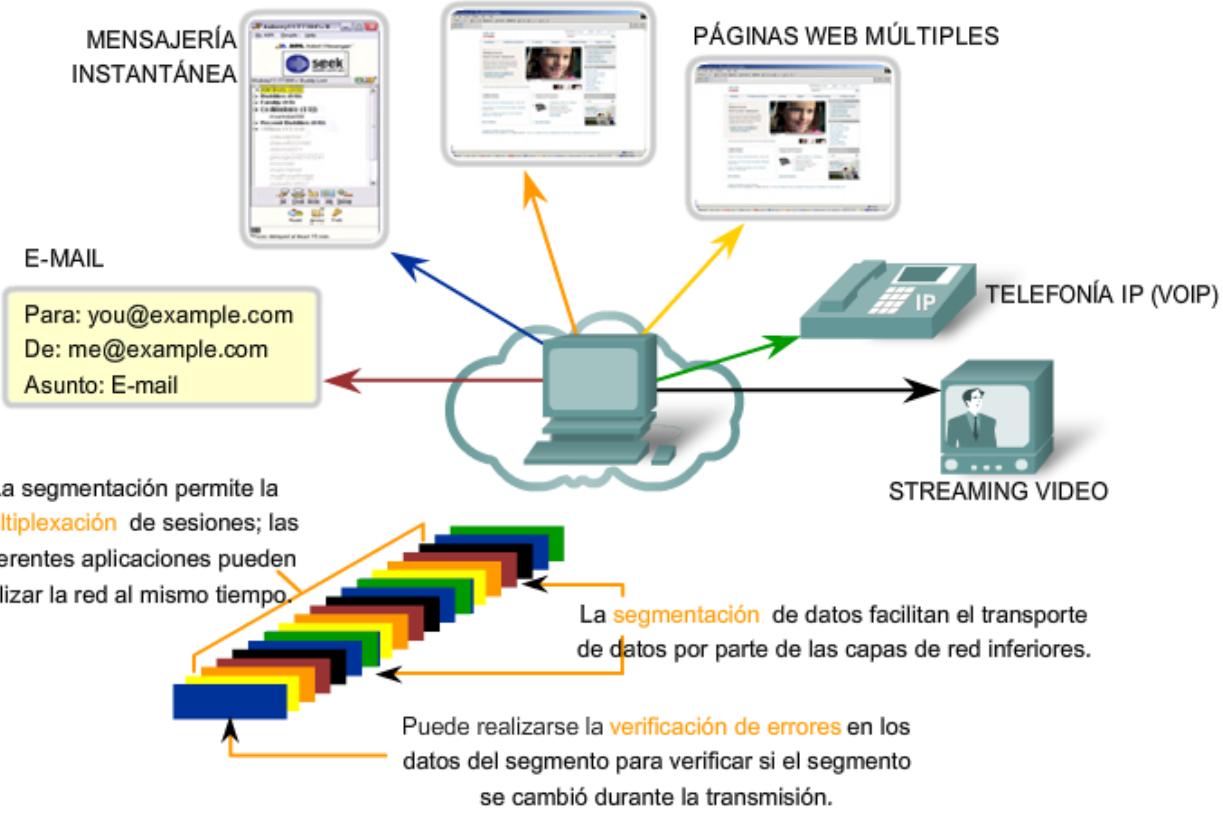
Segmentación y reensamblaje: La mayoría de las redes poseen una limitación en cuanto a la cantidad de datos que pueden incluirse en una única PDU (Unidad de datos del protocolo). La capa de Transporte divide los datos de aplicación en bloques de datos de un tamaño adecuado. En el destino, la capa de Transporte reensambla los datos antes de enviarlos a la aplicación o servicio de destino.

Multiplexación de conversaciones: Pueden existir varias aplicaciones o servicios ejecutándose en cada host de la red. A cada una de estas aplicaciones o servicios se les asigna una dirección conocida como puerto para que la capa de Transporte pueda determinar con qué aplicación o servicio se identifican los datos.

Además de utilizar la información contenida en los encabezados para las funciones básicas de segmentación y reensamblaje de datos, algunos protocolos de la capa de Transporte proveen:

- conversaciones orientadas a la conexión,
- entrega confiable,
- reconstrucción ordenada de datos, y
- control del flujo.

Servicios de la capa de Transporte



Establecimiento de una sesión

La capa de Transporte puede brindar esta orientación a la conexión creando una sesión entre las aplicaciones. Estas conexiones preparan las aplicaciones para que se comuniquen entre sí antes de que se transmitan los datos. Dentro de estas sesiones, se pueden gestionar de cerca los datos para la comunicación entre dos aplicaciones.

Entrega confiable

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. La capa de Transporte puede asegurar que todas las secciones lleguen a destino al contar con el dispositivo de origen para volver a transmitir los datos que se hayan perdido.

Entrega en el mismo orden

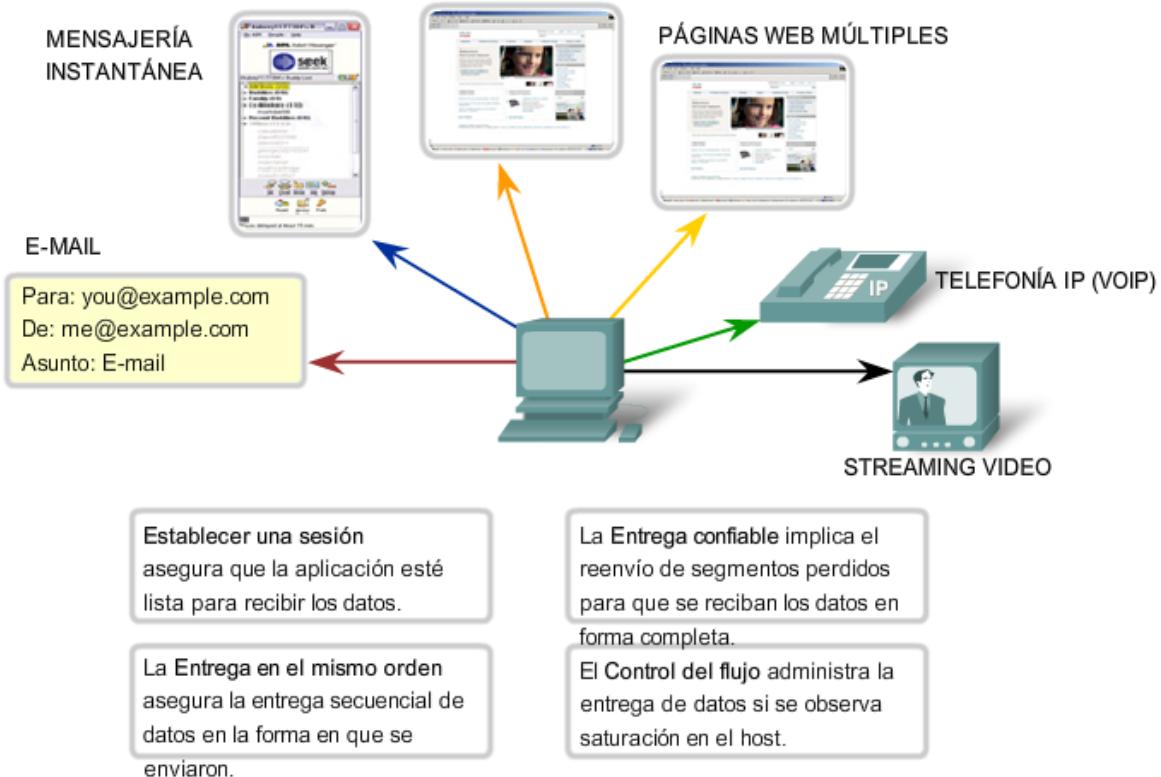
Ya que las redes proveen rutas múltiples que pueden poseer distintos tiempos de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, la capa de Transporte puede asegurar que los mismos se reensamblen en el orden adecuado.

Control del flujo

Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando la capa de Transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación que envía reduzca la velocidad del flujo de datos. Esto se lleva a cabo en la capa de Transporte regulando la cantidad de datos que el origen transmite como grupo. El control del flujo puede prevenir la pérdida de segmentos en la red y evitar la necesidad de retransmisión.

Estos servicios se describirán con más detalle a medida que se expliquen los protocolos en este capítulo.

Servicios de la capa de Transporte



4.1.3 Soporte de comunicación confiable

Cabe recordar que la función principal de la capa de Transporte es administrar los datos de aplicación para las conversaciones entre hosts. Sin embargo, las diferentes aplicaciones tienen diferentes requerimientos para sus datos y, por lo tanto, se han desarrollado diferentes protocolos de Transporte para satisfacer estos requerimientos.

Un protocolo de la capa de Transporte puede implementar un método para asegurar 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. En la capa de Transporte, las tres operaciones básicas de confiabilidad son:

- seguimiento de datos transmitidos,
- acuse de recibo de los datos recibidos, y
- retransmisión de cualquier dato sin acuse de recibo.

Esto requiere que los procesos de la capa de Transporte de origen mantengan el seguimiento de todas las porciones de datos de cada conversación y retransmitan cualquiera de los datos que no dieron acuse de recibo por el destino. La capa de Transporte del host de recepción también debe rastrear los datos a medida que se reciben y reconocer la recepción de los datos.

Estos procesos de confiabilidad generan un uso adicional de los recursos de la red debido al reconocimiento, rastreo y retransmisión. Para admitir estas operaciones de confiabilidad se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está contenida en el encabezado de la Capa 4.

Esto genera un equilibrio (“trade-off”) entre el valor de confiabilidad y la carga que representa para la red. Los desarrolladores de aplicaciones deben elegir qué tipo de protocolo de transporte es adecuado en base a los requerimientos de sus aplicaciones. En la capa de Transporte, existen protocolos que especifican métodos para entrega

confiable, garantizada o de máximo esfuerzo. En el contexto de las redes, la entrega de máximo esfuerzo se considera no confiable, ya que no existe acuse de recibo de que los datos hayan llegado al destino.

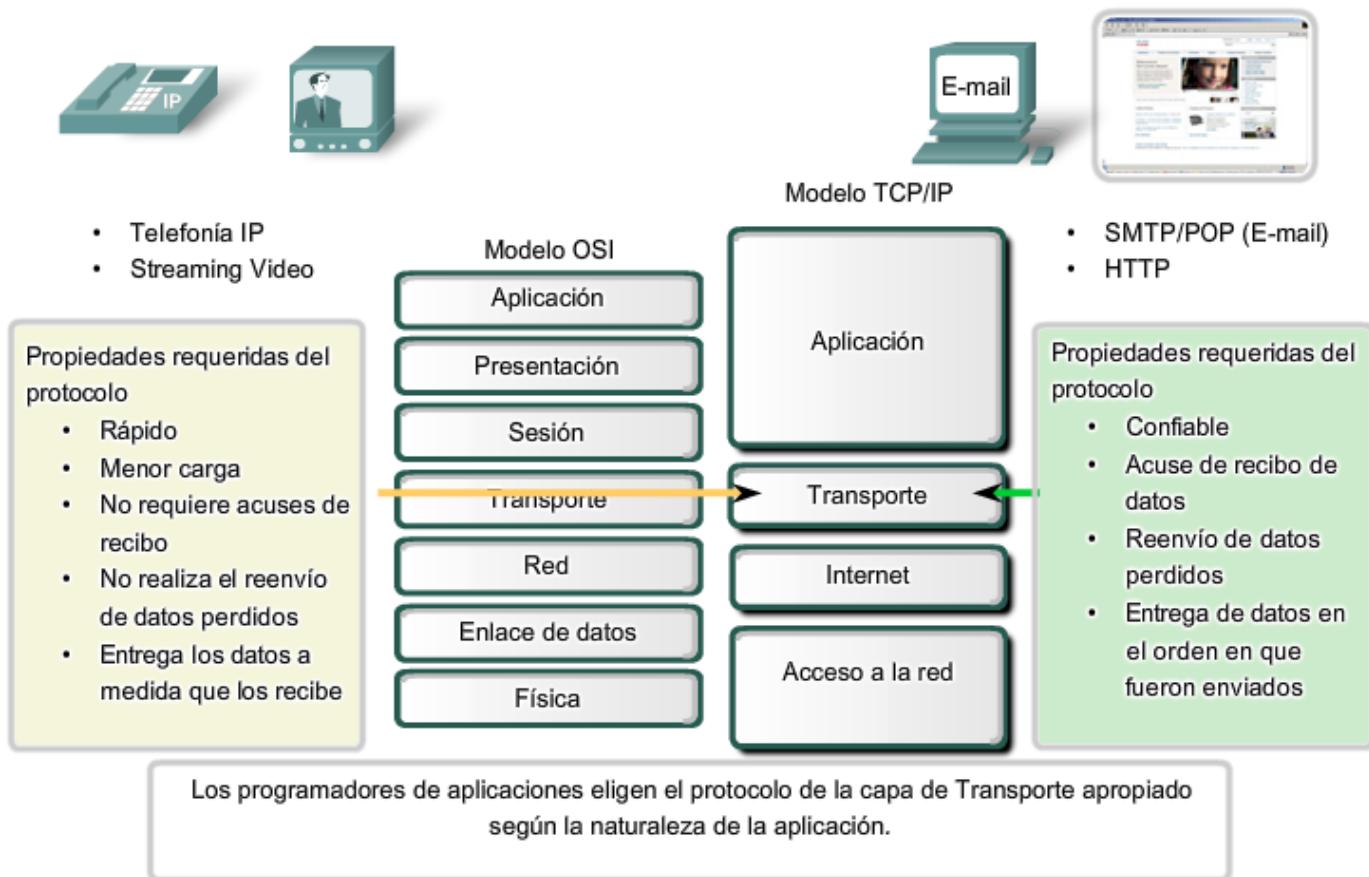
Determinación de la necesidad de confiabilidad

Las aplicaciones, como bases de datos, las páginas Web y los e-mails, requieren que todos los datos enviados lleguen al destino en su condición original, de manera que los mismos sean útiles. Todos los datos perdidos pueden corromper una comunicación y dejarla incompleta o ilegible. Por lo tanto, estas aplicaciones se diseñan para utilizar un protocolo de capa de Transporte que implemente la confiabilidad. El uso de recursos de red adicionales se considera necesario para estas aplicaciones.

Otras aplicaciones son más tolerantes en lo que se refiere a la pérdida de pequeñas cantidades de datos. Por ejemplo, si uno o dos segmentos de un stream de vídeo no llegan al destino, sólo generará una interrupción momentánea en el stream. Esto puede representar distorsión en la imagen pero quizás ni sea advertido por el usuario.

Imponer el uso de recursos adicionales para asegurar la confiabilidad para esta aplicación puede reducir la utilidad de la misma. La imagen en un streaming vídeo se degradaría en gran medida si el dispositivo de destino tuvo que dar cuenta de los datos perdidos y demorar el stream mientras espera que lleguen. Es conveniente proporcionar la mejor imagen posible al momento en que llegan los segmentos y renunciar a la confiabilidad. Si por algún motivo se requiere confiabilidad, estas aplicaciones pueden proveer verificación de errores y solicitudes de retransmisión.

Protocolos de la capa de Transporte



4.1.4 TCP y UDP

Los dos protocolos más comunes de la capa de Transporte del conjunto de protocolos TCP/IP son el Protocolo de control de transmisión (TCP) y el Protocolos de datagramas de usuario (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de Transporte envía estos datagramas como “mejor intento”.

Entre las aplicaciones que utilizan UDP se incluyen:

sistema de nombres de dominios (DNS),

streaming de vídeo, y

Voz sobre IP (VoIP).

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión, descrito en la RFC 793. TCP incurre en el uso adicional de recursos para agregar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de Aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga. Ver la figura para obtener una comparación.

Las aplicaciones que utilizan TCP son:

exploradores Web,

e-mail, y

transferencia de archivos

Encabezados TCP y UDP

Segmento de TCP

| Bit (0) | Bit (15) Bit (16) | Bit (31) |
|--|---------------------------------|----------|
| Puerto de origen (16) | Puerto de destino (16) | |
| Número de secuencia (32) | | |
| Número de acuse de recibo (32) | | |
| Longitud del encabezado (4) Reservado (6) Bits de código (6) | Bits de código (6) Ventana (16) | |
| Checksum (16) | Urgente (16) | |
| Opciones (0 ó 32 si las hay) | | |
| DATOS DE LA CAPA DE APLICACIÓN (el tamaño varía) | | |

↑
20
Bytes
↓

Datagrama de UDP

| Bit (0) | Bit (15) Bit (16) | Bit (31) |
|--|------------------------|----------|
| Puerto de origen (16) | Puerto de destino (16) | |
| Longitud (16) | Checksum (16) | |
| DATOS DE LA CAPA DE APLICACIÓN (el tamaño varía) | | |

↑
8 Bytes
↓

4.1.5 Direccionamiento del puerto

Identificación de las conversaciones

Considere el ejemplo anterior de una computadora que recibe y envía e-mails, mensajes instantáneos, páginas Web y llamadas telefónicas VoIP de manera simultánea.

Los servicios basados en TCP y UDP mantienen un seguimiento de las varias 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 los números de los puertos.

En el encabezado de cada segmento o datagrama hay un puerto de origen y 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. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino en el host remoto.

Los números de puerto se asignan de varias maneras, en función de si el mensaje es una solicitud o una respuesta. Mientras que los procesos en el servidor poseen números de puertos estáticos asignados a ellos, los clientes eligen un número de puerto de forma dinámica para cada conversación.

Cuando una aplicación de cliente envía una solicitud a una aplicación de servidor, el puerto de destino contenido en el encabezado es el número de puerto que se asigna al daemon de servicio que se ejecuta en el host remoto. El software del cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto. Este número de puerto de destino se puede configurar, ya sea de forma predeterminada o manual. Por ejemplo, cuando una aplicación de explorador Web realiza una solicitud a un servidor Web, el explorador utiliza TCP y el número de puerto 80 a menos que se especifique otro valor. Esto sucede porque el puerto TCP 80 es el puerto predeterminado asignado a aplicaciones de servidores Web. Muchas aplicaciones comunes tienen asignados puertos predeterminados.

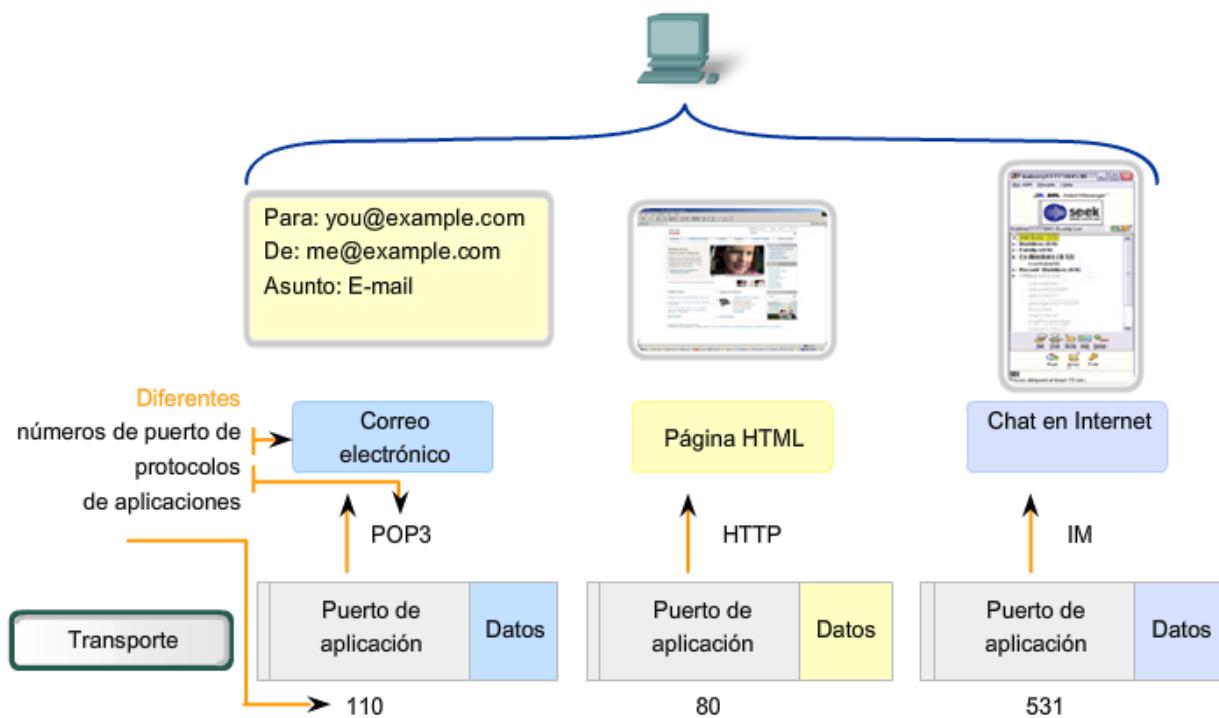
El puerto de origen del encabezado de un segmento o datagrama de un cliente se genera de manera aleatoria. Siempre y cuando no entre en conflicto con otros puertos en uso en el sistema, el cliente puede elegir cualquier número de puerto. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de Transporte mantiene un seguimiento de este puerto y de la aplicación que generó la solicitud, de manera que cuando se devuelva una respuesta, pueda ser enviada 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.

La combinación del número de puerto de la capa de Transporte y de la dirección IP de la capa de Red asignada al host identifica de manera exclusiva un proceso en particular que se ejecuta en un dispositivo host específico. Esta combinación se denomina socket. Eventualmente, los términos número de puerto y socket se utilizan en forma indistinta. En el contexto de este curso, el término socket hace referencia sólo a la combinación exclusiva de dirección IP y número de puerto. Un par de sockets, que consiste en las direcciones IP y los números de puerto de origen y de destino, también es exclusivo e identifica la conversación entre dos hosts.

Por ejemplo, una solicitud de página Web HTTP que se envía a un servidor Web (puerto 80) y que se ejecuta en un host con una dirección IPv4 de Capa 3 192.168.1.20 será destinada al socket 192.168.1.20:80.

Si el explorador Web que solicita la página Web se ejecuta en el host 192.168.100.48 y el número de puerto dinámico asignado al explorador Web es 49.152, el socket para la página Web será 192.168.100.48:49152.

Direccionamiento de puertos



Los datos de las distintas aplicaciones se dirigen a la aplicación correcta, ya que cada aplicación tiene un número de puerto único.

La Autoridad de números asignados de Internet (IANA) asigna números de puerto. IANA es un organismo de estándares responsable de la asignación de varias normas de direccionamiento.

Existen distintos tipos de números de puerto:

Puertos bien conocidos (Números del 0 al 1 023): estos números se reservan para servicios y aplicaciones. Por lo general, se utilizan para aplicaciones como HTTP (servidor Web), POP3/SMTP (servidor de e-mail) y Telnet. Al definir estos puertos conocidos para las aplicaciones del servidor, las aplicaciones del cliente pueden ser programadas para solicitar una conexión a un puerto específico y su servicio asociado.

Puertos Registrados (Números 1024 al 49151): estos números de puertos están asignados a procesos o aplicaciones del usuario. Estos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un puerto bien conocido. Cuando no se utilizan para un recurso del servidor, estos puertos también pueden utilizarse si un usuario los selecciona de manera dinámica como puerto de origen.

Puertos dinámicos o privados (Números del 49 152 al 65 535): también conocidos como puertos efímeros, suelen asignarse de manera dinámica a aplicaciones de cliente cuando se inicia una conexión. No es muy común que un cliente se conecte a un servicio utilizando un puerto dinámico o privado (aunque algunos programas que comparten archivos punto a punto lo hacen).

Utilización de los dos protocolos TCP y UDP

Algunas aplicaciones pueden utilizar los dos protocolos: TCP y UDP. 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 53 de puerto conocido es utilizado por ambos protocolos con este servicio.

Enlaces

Se puede encontrar un lista actual de números de puertos en <http://www.iana.org/assignments/port-numbers>.

Números de puerto

| Rango de números de puerto | Grupo de puertos |
|----------------------------|-----------------------------------|
| De 0 a 1023 | Puertos bien conocidos (Contacto) |
| De 1024 a 49151 | Puertos registrados |
| De 49152 a 65535 | Puertos privados y/o dinámicos |

Puertos TCP registrados:
1863 MSN Messenger
8008 HTTP alternativo
8080 HTTP alternativo

Puertos TCP bien conocidos:
21 FTP
23 Telnet
25 SMTP
80 HTTP
110 POP3
194 Internet Relay Chat (IRC)
443 HTTP seguro (HTTPS)

| Rango de números de puerto | Grupo de puertos |
|----------------------------|-----------------------------------|
| De 0 a 1023 | Puertos bien conocidos (Contacto) |
| De 1024 a 49151 | Puertos registrados |
| De 49152 a 65535 | Puertos privados y/o dinámicos |

Puertos UDP registrados:
1812 Protocolo de autenticación RADIUS
2000 Cisco SCCP (VoIP)
5004 RTP (Voice and Video Transport Protocol)
5060 SIP (VoIP)

Puertos UDP bien conocidos:
69 TFTP
520 RIP

| Rango de números de puerto | Grupo de puertos |
|----------------------------|-----------------------------------|
| De 0 a 1023 | Puertos bien conocidos (Contacto) |
| De 1024 a 49151 | Puertos registrados |
| De 49152 a 65535 | Puertos privados y/o dinámicos |

Puertos TCP/UDP registrados comunes:
1433 MS SQL
2948 WAP (MMS)

Puertos comunes TCP/UDP bien conocidos:
53 DNS
161 SNMP
531 Mensajería instantánea de AOL, IRC

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 en uso, la dirección y el número de puerto locales, la dirección y el número de puerto ajenos y el estado de la conexión.

Las conexiones TCP no descritas pueden representar una importante amenaza a la seguridad. Esto se debe a que pueden indicar que algo o alguien está conectado al host local. Además, las conexiones TCP innecesarias pueden consumir

recursos valiosos del sistema y por lo tanto disminuir el rendimiento del host. Netstat debe utilizarse para determinar las conexiones abiertas de un host cuando el rendimiento parece estar comprometido.

Existen muchas opciones útiles para el comando netstat.

```
C:\>netstat  
Active Connections  
  
Proto Local Address          Foreign Address        State  
TCP   kenpc:3126            192.168.0.2:netbios-ssn ESTABLISHED  
TCP   kenpc:3158            207.138.126.152:http  ESTABLISHED  
TCP   kenpc:3159            207.138.126.169:http  ESTABLISHED  
TCP   kenpc:3160            207.138.126.169:http  ESTABLISHED  
TCP   kenpc:3161            sc.msn.com:http       ESTABLISHED  
TCP   kenpc:3166            www.cisco.com:http    ESTABLISHED  
  
C:\>
```

4.1.6 Segmentación y reensamblaje: Divide y vencerás

Un capítulo anterior explicaba cómo se construyen las PDU enviando datos de una aplicación a través de los varios protocolos para crear una PDU que luego se transmita en el medio. En el host de destino, este proceso se invierte hasta que los datos puedan enviarse a la aplicación.

Algunas aplicaciones transmiten grandes cantidades de datos; en algunos casos, varios 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 hubiera algún error, el archivo de datos completo se perdería o tendría que ser reenviado. 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 en función de la tecnología de la red y del medio físico específico que se utiliza.

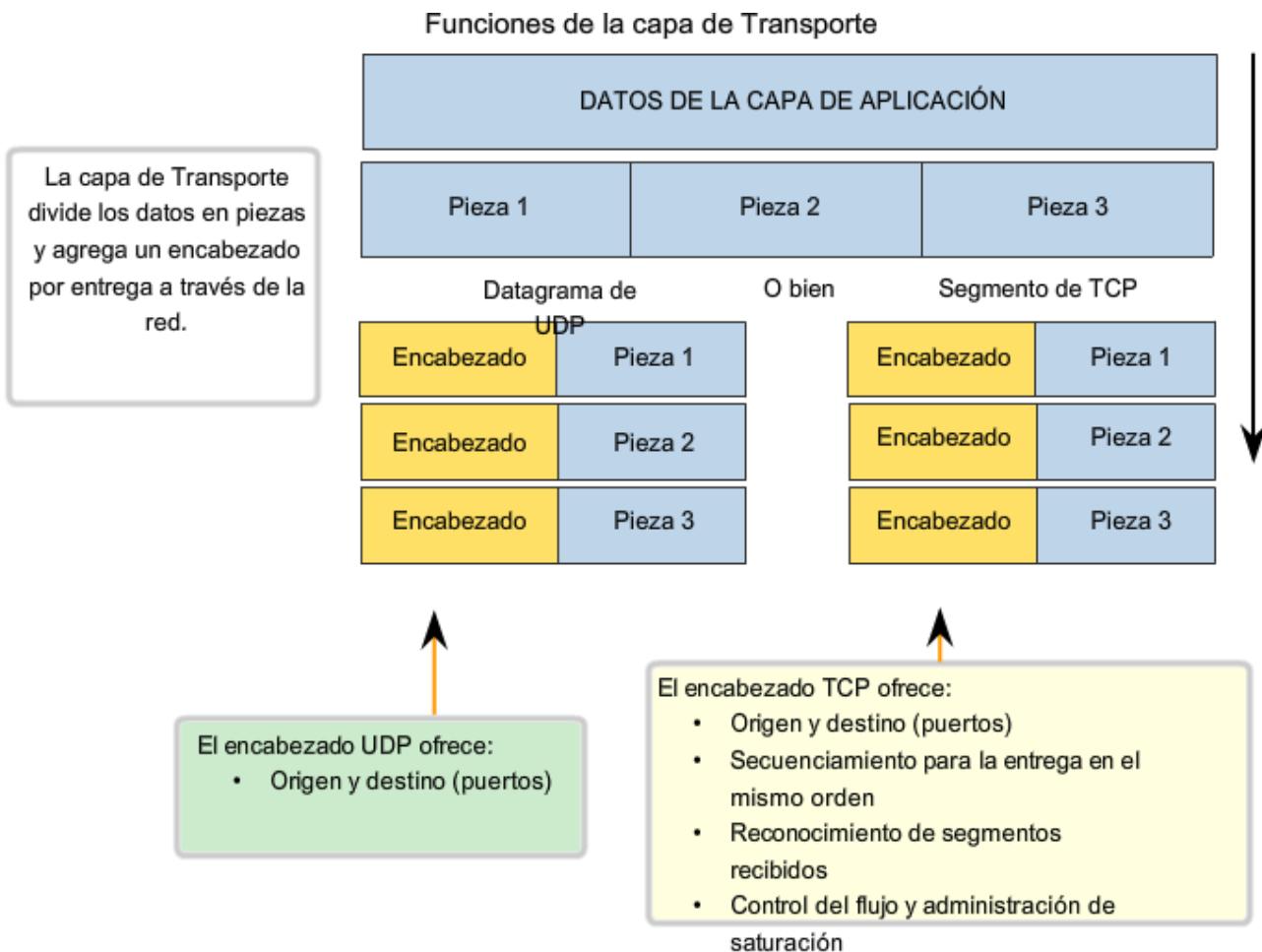
Dividir los datos de aplicación en secciones garantiza que los datos se transmitan dentro de los límites del medio y que los datos de distintas aplicaciones puedan ser multiplexados en el medio.

TCP y UDP gestionan la segmentación de forma distinta.

Con TCP, cada encabezado de segmento contiene un número de secuencia. Este número de secuencia permite que las funciones de la capa de Transporte del host de destino reensamblen los segmentos en el mismo orden en el que fueron transmitidos. Esto asegura que la aplicación de destino cuente con los datos en la forma exacta en la que se enviaron.

A pesar de que los servicios que utilizan UDP también rastrean las conversaciones entre aplicaciones, no tienen en cuenta el orden en el que se transmitió la información ni el mantenimiento de la 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 al que fue transmitida, ya que los paquetes pueden tomar diversas 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.



4.2 PROTOCOLO TCP: COMUNICACIÓN CON CONFIABILIDAD

4.2.1 TCP: Cómo generar conversaciones confiables

La diferencia clave entre TCP y UDP es la confiabilidad

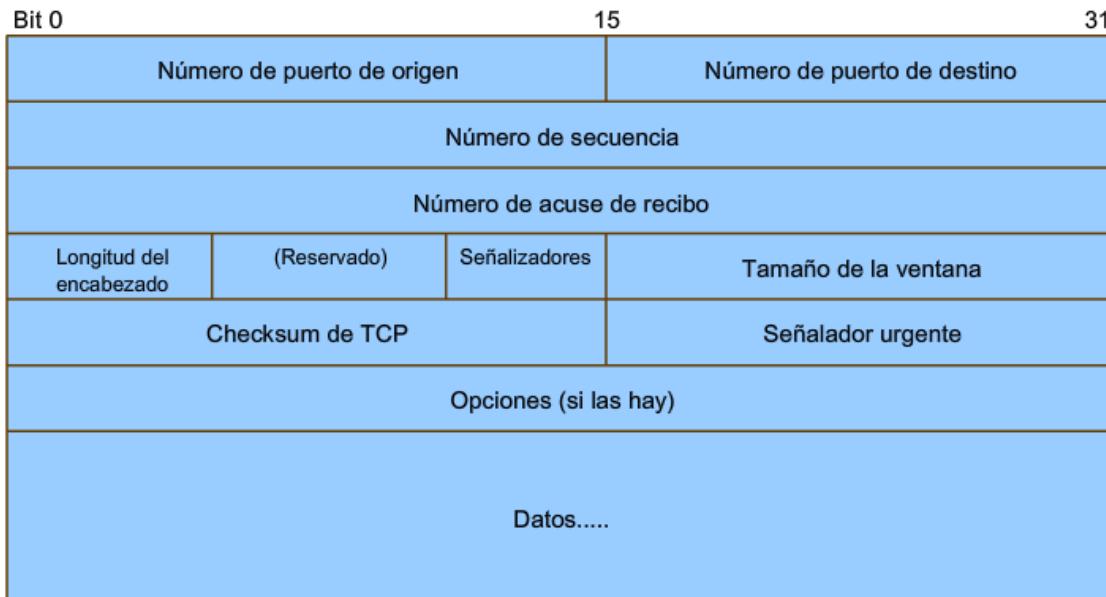
La confiabilidad de la comunicación TCP se lleva a cabo utilizando sesiones orientadas a la conexión. Antes de que un host que utiliza TCP envíe datos a otro host, la capa de Transporte inicia un proceso para crear una conexión con el destino. Esta conexión permite el rastreo de una sesión o stream de comunicación entre los hosts. Este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare. Una conversación TCP completa requiere el establecimiento de una sesión entre los hosts en ambas direcciones.

Luego de establecida la sesión, el destino envía acuses de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino.

Parte de la carga adicional que genera el uso de TCP es el tráfico de red generado por los acuses de recibo y las retransmisiones. El establecimiento de las sesiones genera cargas en forma de segmentos adicionales intercambiados. También existen cargas adicionales en los hosts individuales, generadas por la necesidad de mantener un seguimiento de los segmentos que esperan acuse de recibo y por el proceso de retransmisión.

Esta confiabilidad se logra contando con campos en el segmento TCP, cada uno con una función específica, como se muestra en la figura. Estos campos se explicarán más adelante en esta sección.

Campos del encabezado del segmento de TCP



Los campos del encabezado de TCP habilitan TCP para suministrar comunicaciones de datos confiables orientados a la comunicación.

| | |
|---|---|
| Número de puerto de origen | Número de puerto de destino |
| Sesión TCP en el dispositivo que abrió una conexión - normalmente un valor aleatorio superior a 1023. | Identifica el protocolo de la capa superior o la aplicación del sitio remoto. |
| Número de secuencia | |
| Especifica el número del último octeto (byte) en un segmento. | |
| Número de acuse de recibo | |
| Especifica el próximo octeto esperado por el receptor. | |
| Longitud del encabezado | Señalizadores |
| Longitud del encabezado: especifica la longitud del encabezado del segmento en bytes | Utilizados en la administración de sesiones y el tratamiento de segmentos. |
| Tamaño de la ventana | |
| | Es el valor de la ventana dinámica; la cantidad de octetos que pueden enviarse antes de esperar el acuse de recibo. |
| Checksum de TCP | Señalador urgente |
| Utilizada para la verificación de errores en el encabezado y los datos. | Utilizado únicamente con una señalización URG (Urgente). |
| Opciones | |
| Información opcional | |
| Datos | |
| Datos de aplicación | |

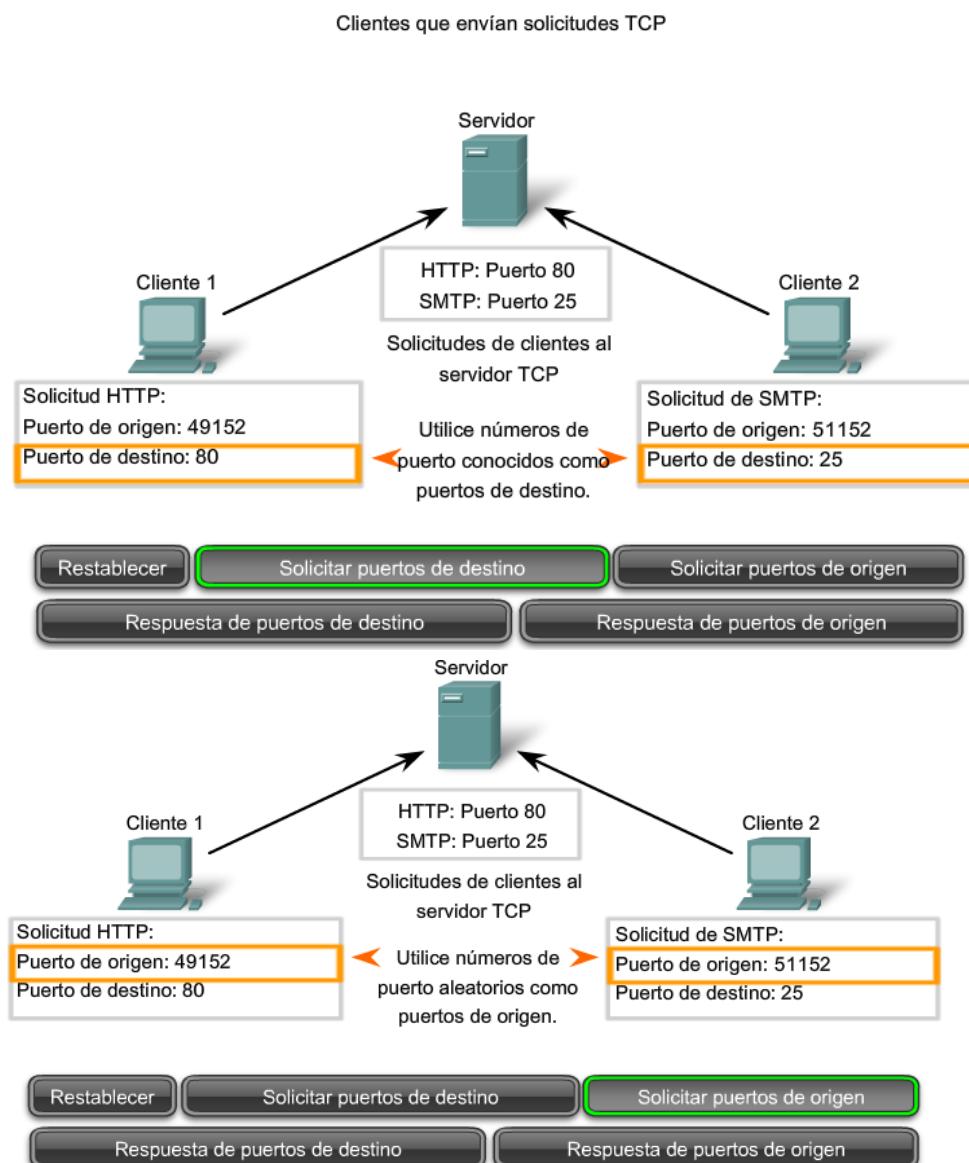
4.2.2 Procesos del servidor TCP

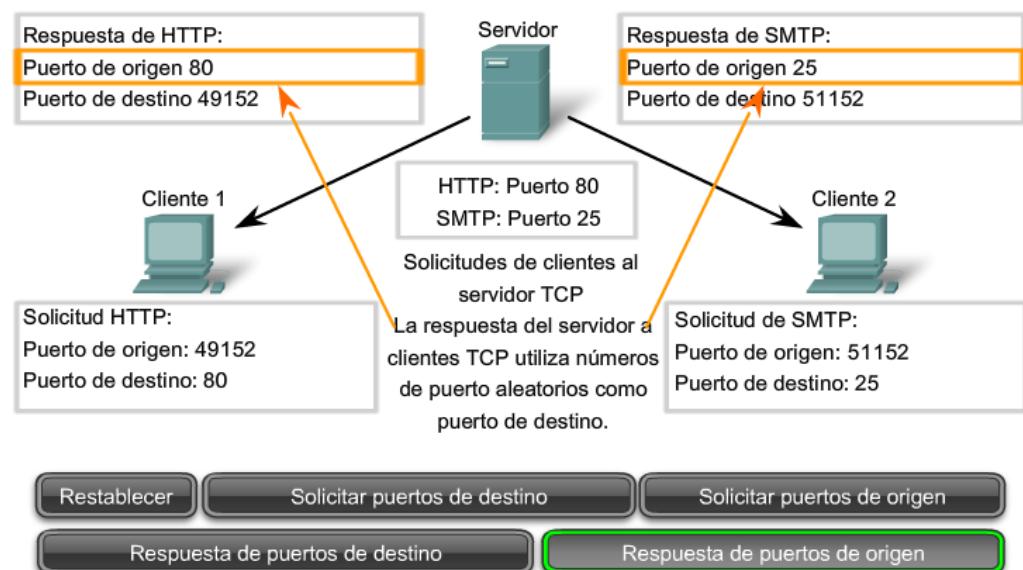
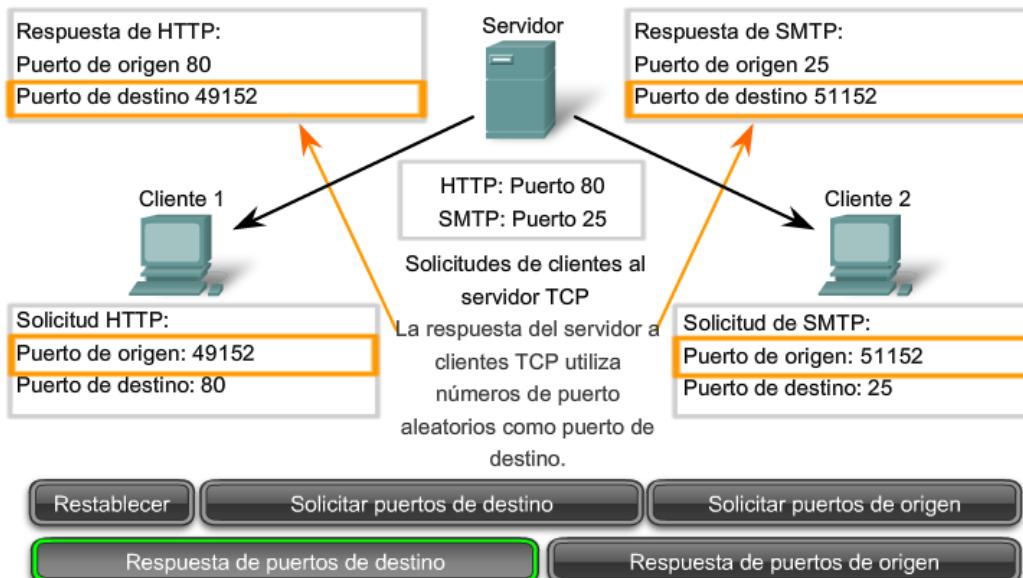
Como se explicó en el capítulo anterior, los procesos de aplicación se ejecutan en servidores. Estos procesos esperan hasta que un cliente inicie comunicación con una solicitud de información o de otros servicios.

Cada proceso de aplicación que se ejecuta en el servidor es configurado por el administrador del sistema para utilizar un número de puerto, de forma predeterminada o manual. **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). Cuando una aplicación de servidor activa se asigna a un puerto específico, este puerto se considera “abierto” para el servidor. Esto significa que la capa de Transporte acepta y procesa segmentos direccionados a ese puerto. Toda solicitud entrante de un cliente dirigida 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 provea más de un servicio, como un servidor Web y un servidor FTP, al mismo tiempo.

Una manera de mejorar la seguridad en un servidor es restringir el acceso al servidor a sólo aquellos puertos asociados con los servicios y aplicaciones accesibles a solicitantes autorizados.

La figura muestra la asignación típica de puertos de origen y destino en operaciones de cliente o servidor TCP.





4.2.3 Establecimiento y finalización de la conexión TCP

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 de sesión habilitan la función de confiabilidad de TCP.

Ver la figura para observar los pasos para establecer y finalizar una conexión TCP.

El host rastrea cada segmento de datos dentro de una sesión e intercambia información sobre los datos recibidos por cada host a través de la información del encabezado TCP.

Cada conexión representa dos streams de comunicación de una vía o sesiones. Para establecer la conexión los hosts realizan un intercambio de señales 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 esté presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y esté aceptando las peticiones en el número de puerto de destino que el cliente que lo inicia intente usar para la sesión.

- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en ese número de puerto.

En conexiones TCP, el host que brinde el servicio como cliente inicia la sesión al servidor. Los tres pasos para el establecimiento de una conexión TCP son:

1. El cliente que inicia la conexión envía un segmento que contiene un valor de secuencia inicial, que actúa como solicitud para el servidor para comenzar una sesión de comunicación.
2. El servidor responde con un segmento que contiene un valor de reconocimiento igual al valor de secuencia recibido más 1, además de su propio valor de secuencia de sincronización. El valor es uno mayor que el número de secuencia porque el ACK es siempre el próximo Byte u Octeto esperado. Este valor de reconocimiento permite al cliente unir la respuesta al segmento original que fue enviado al servidor.
3. El cliente que inicia la conexión responde con un valor de reconocimiento igual al valor de secuencia que recibió más uno. Esto completa el proceso de establecimiento de la conexión.

Para entender el proceso de enlace de tres vías, es importante observar los distintos valores que intercambian los dos 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: Urgente campo de señalizador significativo,

ACK: Campo significativo de acuse de recibo,

PSH: Función de empuje,

RST: Reconfiguración de la conexión,

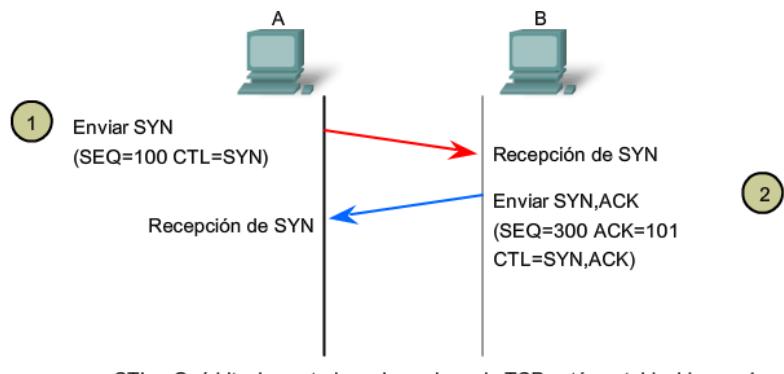
SYN: Sincronizar números de secuencia,

FIN: No hay más datos desde el emisor.

A estos campos se los denomina señaladores porque el valor de uno de estos campos es sólo de 1 bit, entonces tiene sólo dos valores: 1 ó 0. Si el valor del bit se establece en 1, indica la información de control que contiene el segmento.

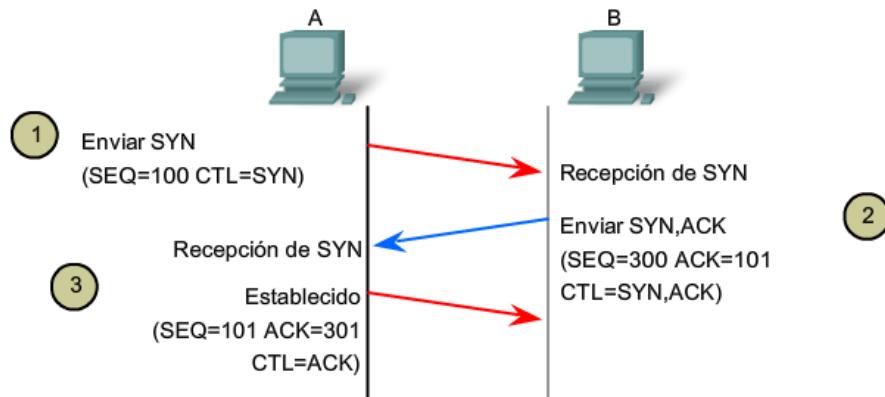
Si se utiliza un proceso de cuatro pasos, los señaladores se intercambian para finalizar la conexión TCP.





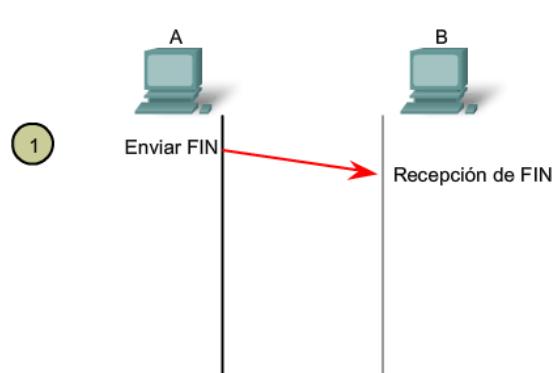
CTL = Qué bits de control en el encabezado TCP están establecidos en 1

B envía la respuesta de ACK y la solicitud de SYN a A.

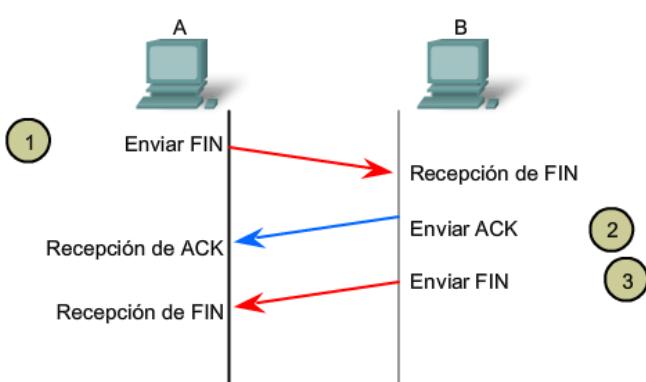


CTL = Qué bits de control en el encabezado TCP están establecidos en 1

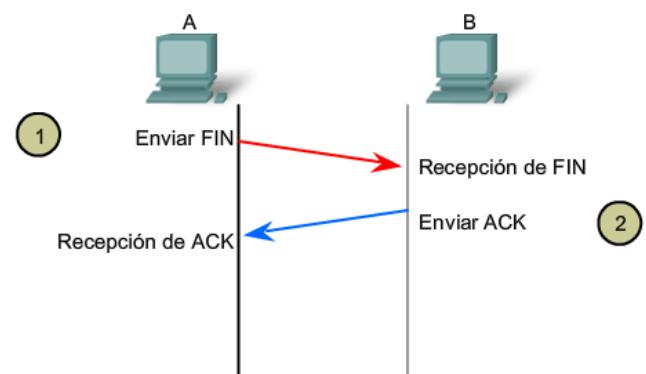
A envía la respuesta de ACK a B.



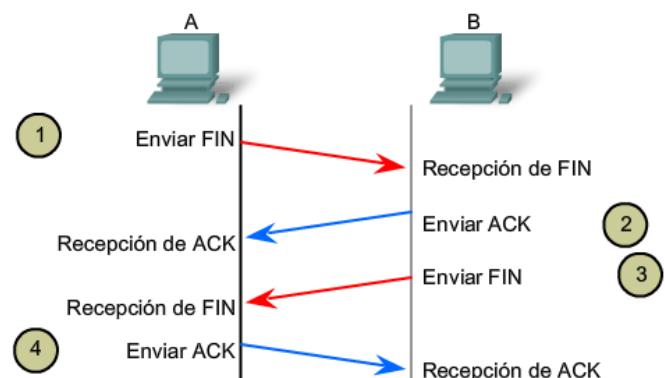
A envía la solicitud de FIN a B.



B envía FIN a A.



B envía la respuesta de ACK a A.



A envía la respuesta de ACK a B.

4.2.4 Protocolo TCP de enlace de tres vías

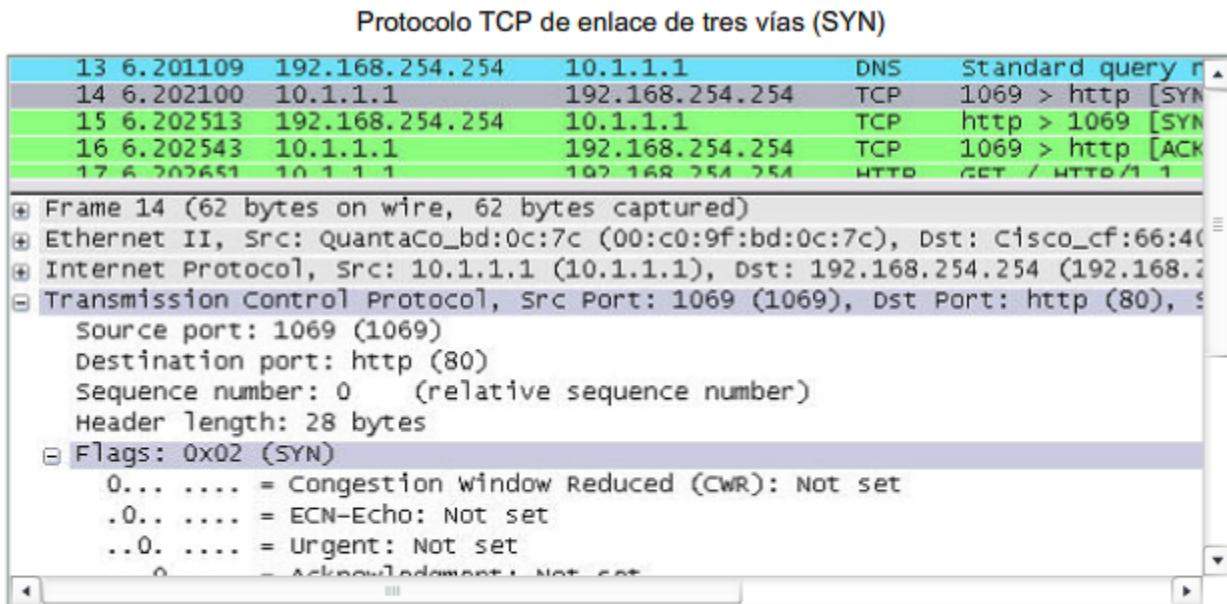
Con los resultados Wireshark, podrá examinar el funcionamiento del protocolo TCP de enlace de tres vías:

Paso 1

Un cliente TCP comienza el enlace de tres vías enviando un segmento con el señalizador de control SYN (Sincronizar números de secuencia) establecido, indicando un valor inicial en el campo de número de secuencia del 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 desde el cliente al servidor para esta sesión. 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.

Se establece el señalizador de control SYN y el número de secuencia relativa en 0. A pesar de que el analizador de protocolos en el gráfico indica los valores relativos para los números de secuencia y de acuse de recibo, los valores reales son números binarios de 32 bits. Se pueden determinar los números reales enviados en los encabezados de los segmentos examinando el panel de bytes del paquete. Aquí se pueden ver los cuatro bytes representados en hexadecimal.



El analizador de protocolo muestra la solicitud del cliente inicial para la sesión en la trama 14.

El segmento TCP en esta trama muestra:

- El señalizador SYN establecido para validar un número de secuencia inicial
- Número de secuencia aleatorio válido (el valor relativo es 0)
- Puerto de origen aleatorio 1069
- El puerto de destino conocido es 80 (puerto HTTP) según indica el servidor Web (httpd)

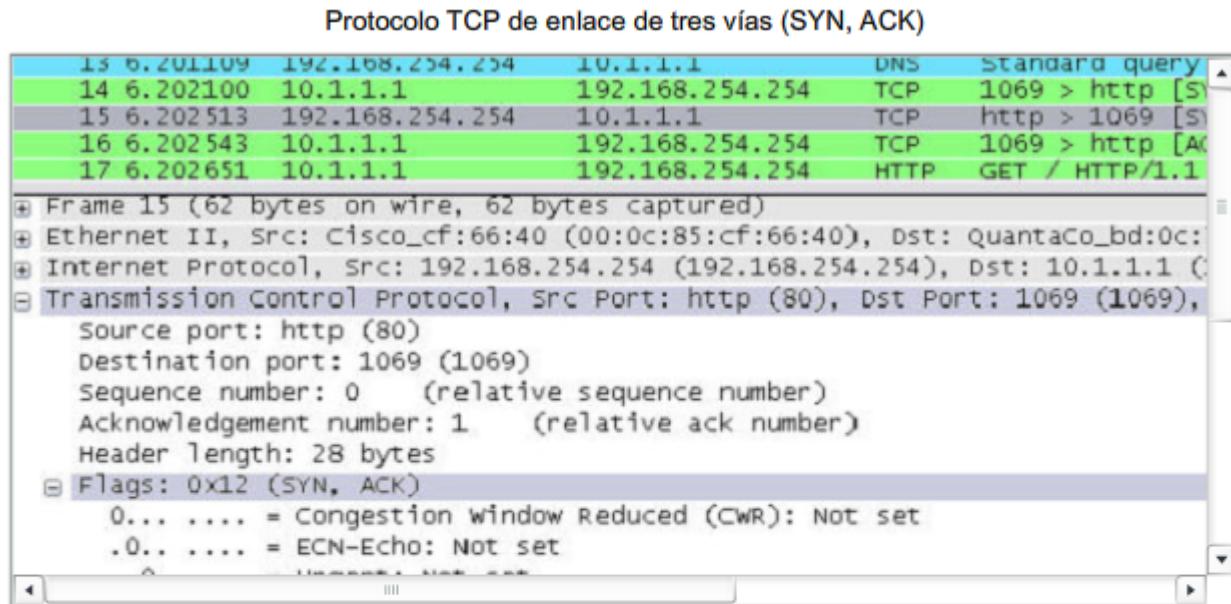
Paso 2

El servidor TCP necesita reconocer la recepción del segmento SYN del cliente para establecer la sesión de cliente a servidor. Para hacerlo, el servidor envía un segmento al cliente con el señalizador ACK establecido indicando 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 número de campo del acuse de recibo es igual al número de secuencia inicial del cliente más 1. Esto establece una sesión desde el cliente al servidor. El señalizador ACK permanecerá establecido para mantener el equilibrio de la sesión. Cabe recordar que la conversación entre el cliente y el servidor está compuesta en realidad por dos sesiones de una vía: una del cliente al servidor y la otra del servidor al cliente. En este segundo paso del enlace de tres vías, el servidor debe iniciar la respuesta del servidor 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 utilizará para rastrear el flujo de datos en esta sesión del servidor al cliente.

Como se muestra en la figura, el resultado del analizador de protocolos muestra que están establecidos los señalizadores de control ACK y SYN y se muestran los números relativos de secuencia y reconocimiento.



Un analizador de protocolos muestra la respuesta del servidor en la trama 15

- El señalizador ACK está establecido para indicar un número de acuse de recibo válido
- Respuesta del número de acuse de recibo al número de secuencia inicial como valor relativo de 1
- Señalizador SYN establecido para indicar el número de secuencia inicial para el servidor a la sesión del cliente
- Número de puerto de destino de 1069 para la correspondencia con los puertos de origen de clientes
- Número de puerto de origen de 80 (HTTP) que indica el servicio del servidor Web (httpd)

Paso 3

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 número de acuse de recibo contiene uno más que el número de secuencia inicial recibido del servidor. Una vez establecidas ambas sesiones entre el cliente y el servidor, todos los segmentos adicionales que se intercambien en la comunicación tendrán establecido el señalizador ACK.

Como se muestra en la figura, el resultado del analizador de protocolos muestra el señalizador de control ACK establecido y se muestran los números relativos de secuencia y reconocimiento.

Se puede añadir seguridad a la red de datos de la siguiente manera:

- denegar el establecimiento de sesiones TCP,
- sólo permitir sesiones para ser establecidas por servicios específicos, o
- sólo permitir tráfico como parte de sesiones ya establecidas.

Esta 128versión128o puede implementarse para todas las sesiones o sólo para las sesiones seleccionadas.

| Protocolo TCP de enlace de tres vías (ACK) | | | | | |
|--|----------|-----------------|-----------------|------|-------------------|
| 13 | 6.201109 | 192.168.254.254 | 10.1.1.1 | DNS | Standard query re |
| 14 | 6.202100 | 10.1.1.1 | 192.168.254.254 | TCP | 1069 > http [SYN] |
| 15 | 6.202513 | 192.168.254.254 | 10.1.1.1 | TCP | http > 1069 [SYN, |
| 16 | 6.202543 | 10.1.1.1 | 192.168.254.254 | TCP | 1069 > http [ACK] |
| 17 | 6.202651 | 10.1.1.1 | 192.168.254.254 | HTTP | GET / HTTP/1.1 |

Frame 16 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40
Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
Transmission Control Protocol, Src Port: 1069 (1069), Dst Port: http (80), Seq: 1, Ack: 1, Len: 54
Source port: 1069 (1069)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
 0... = Congestion window Reduced (CWR): Not set
 .0. = ECN-Echo: Not set
 ..0. = Urgent: Not set

El analizador de protocolo muestra la respuesta del cliente inicial para la sesión en

Trama 16 El segmento TCP en esta trama muestra:

- El señalizador ACK está establecido para indicar un número de acuse de recibo válido
- Respuesta del número de acuse de recibo al número de secuencia inicial como valor relativo de 1
- Número de puerto de origen de 1069 para la correspondencia
- Número de puerto de destino de 80 (HTTP) que indica el servicio del servidor Web (httpd)

4.2.5 Terminación de la sesión TCP

Para cerrar la conexión se debe establecer el señalizador de control FIN (Finalizar) 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 conversación simple admitida por TCP, se requieren cuatro intercambios para finalizar ambas sesiones.

Nota: En esta explicación se usan los términos cliente y servidor como referencia por simplicidad pero la finalización del proceso puede ser iniciada por cualquiera de los dos hosts que completen la sesión:

1. Cuando el cliente no tiene más datos para enviar al stream, envía un segmento con el señalizador FIN establecido.
2. El servidor envía un ACK para acusar recibo de Fin y terminar la sesión del cliente al servidor.
3. El servidor envía un FIN al cliente para finalizar la sesión del servidor al cliente.

4. El cliente responde con un ACK para dar acuse de recibo de FIN desde el servidor.

Cuando la finalización de sesión del cliente no tiene más datos para transferir, establece el señalizador FIN en el encabezado de un segmento. Luego, el servidor finaliza la conexión y envía un segmento normal que contiene datos con el señalizador ACK establecido utilizando el número de acuse de recibo, confirmando así que se han recibido todos los bytes de datos. Cuando se produce el acuse de recibo de todos los segmentos, se cierra la sesión.

La sesión en la otra dirección se cierra mediante 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 de retorno confirma que todos los bytes de datos han sido recibidos y, por lo tanto, se ha cerrado la sesión.

Como se muestra en la figura, los señalizadores de control FIN y ACK se establecen en el encabezado del segmento, cerrando por lo tanto la sesión HTTP.

También es posible terminar la conexión mediante 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. El cliente responde con un ACK.

Terminación de la sesión TCP (FIN)

A screenshot of a network protocol analyzer (Wireshark) showing a list of network frames. Frame 20 is selected, which is a TCP segment with the FIN flag set. The details pane shows the following information:

- Frame 20 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Cisco_cf:66:40 (00:0c:85:cf:66:40), Dst: QuantaCo_bd:0c:7c
- Internet Protocol, Src: 192.168.254.254 (192.168.254.254), Dst: 10.1.1.1 (10.1.1.1)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 1069 (1069), Seq: 440, Ack: 414, Len: 20, Flags: 0x11 (FIN, ACK)

The bottom section of the interface shows two tabs: "FIN" and "ACK". The "FIN" tab is highlighted. Below the tabs, it says "Terminación de la sesión TCP (FIN)".

Un analizador de protocolo muestra los detalles de la trama 20, solicitud TCP FIN.

Puertos de destino y origen

Contenido y valores del campo del encabezado

FIN ACK
Terminación de la sesión TCP (ACK)

A screenshot of a network protocol analyzer (Wireshark) showing a list of network frames. Frame 21 is selected, which is a TCP segment with the ACK flag set. The details pane shows the following information:

- Frame 21 (54 bytes on wire, 54 bytes captured)
- Ethernet II, Src: QuantaCo_bd:0c:7c (00:0c:9f:bd:0c:7c), Dst: Cisco_cf:66:40
- Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
- Transmission Control Protocol, Src Port: 1069 (1069), Dst Port: http (80), Seq: 414, Ack: 441, Len: 20, Flags: 0x10 (ACK)

The bottom section of the interface shows two tabs: "FIN" and "ACK". The "ACK" tab is highlighted. Below the tabs, it says "Terminación de la sesión TCP (ACK)".

Un analizador de protocolo muestra los detalles de la trama 21, respuesta TCP ACK.

Puertos de destino y origen

Contenido y valores del campo del encabezado

FIN ACK
Haga clic para ver los detalles.

4.3 ADMINISTRADOR DE SESIONES TCP

4.3.1 Reensamblaje de segmentos TCP

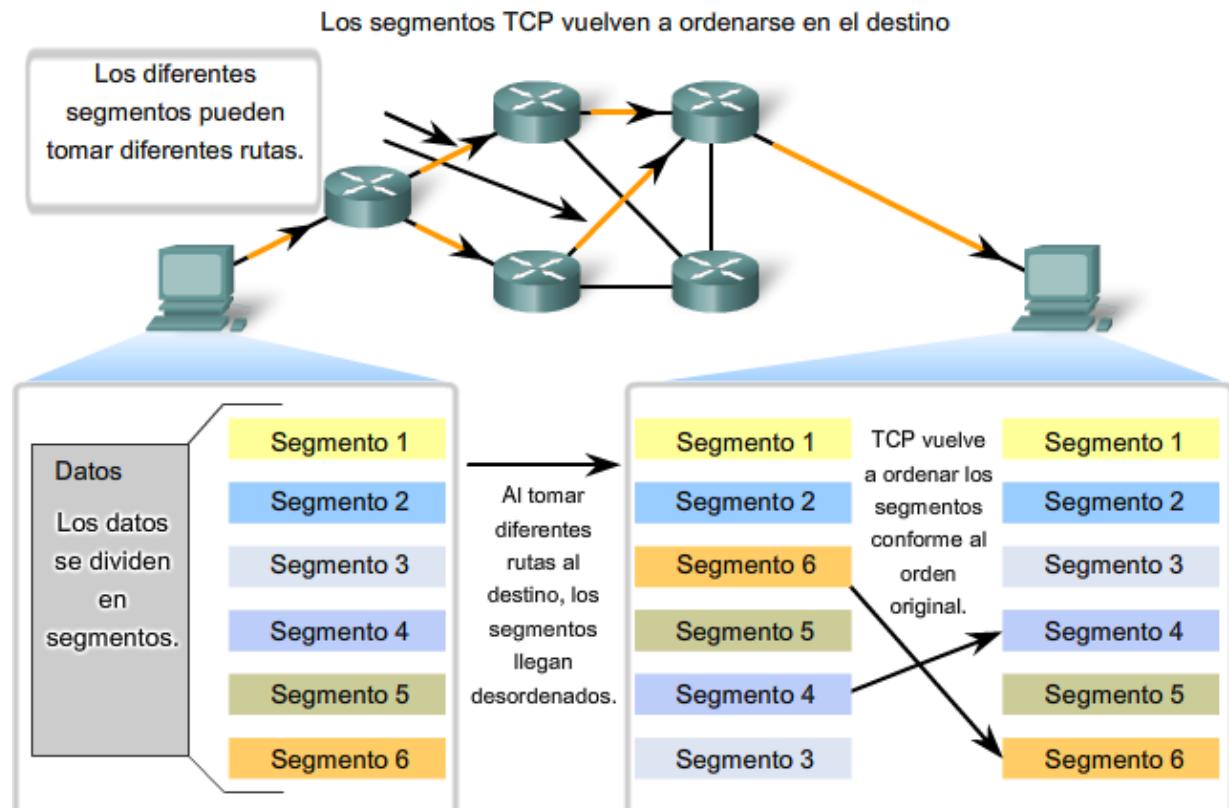
Resecuenciamiento de segmentos al orden transmitido

Cuando los servicios envían datos utilizando TCP, los segmentos pueden llegar a destinos desordenados. 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 número de secuencia inicial representa el valor de inicio para los bytes de esta sesión que se transmitirán 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 rastreo de bytes de datos permite que cada segmento se identifique y se envíe acuse de recibo de manera exclusiva. Se pueden identificar segmentos perdidos.

Los números de secuencia de segmento permiten la confiabilidad indicando cómo reensamblar y reordenar los segmentos recibidos, como se muestra en la figura.

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 adecuado y se pasa a la capa de Aplicación cuando son reensamblados. Todos los segmentos que llegan con números de secuencia no contiguos se mantienen para su procesamiento posterior. Luego, se procesan los segmentos cuando llegan con los bytes perdidos.



4.3.2 Acuse de recibo

Confirmación de recepción de segmentos

Una de las funciones de TCP es asegurar que cada segmento llegue a su destino. Los servicios TCP en el host de destino envían a la aplicación de origen un acuse de recibo de los datos recibidos.

El número de secuencia y el número de acuse de recibo del encabezado del segmento se utilizan para confirmar la recepción de los bytes de datos contenidos en los segmentos. El número de secuencia es el número relativo de bytes que ha sido transmitido en esta sesión más 1 (que es el número del primer byte de datos en el segmento actual). TCP utiliza el número de reconocimiento en segmentos que se vuelven a enviar al origen para indicar el próximo byte de esta sesión que espera el receptor. Esto se llama acuse de recibo de expectativa.

Se le informa al origen que el destino ha recibido todos los bytes de este stream de datos, pero sin incluir, el byte especificado por el número de acuse de recibo. Se espera que el host emisor envíe un segmento que utilice un número de secuencia igual al número de acuse de recibo.

Recuerde que cada conexión se representa en realidad por dos sesiones de una vía. Los números de secuencia y de acuse de recibo se intercambian en ambas direcciones.

En el ejemplo de la figura, el host en 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 de la derecha recibe el segmento en la Capa 4 y determina que el número de secuencia es 1 y que posee 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 acuse de recibo en 11 para indicar que el próximo byte de datos que espera recibir en esta sesión es el byte número 11.

Cuando el host emisor de la izquierda recibe este acuse de recibo, puede enviar el próximo segmento que contiene datos para esta sesión a partir del byte 11.

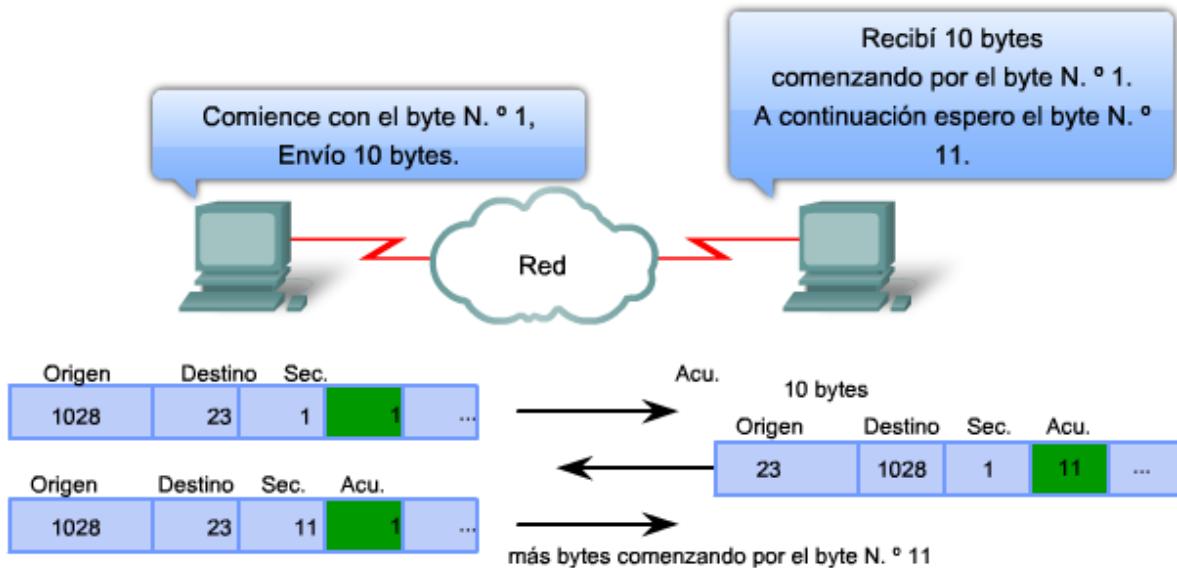
Observando este ejemplo, si el host emisor tuviera que esperar el acuse de recibo por la recepción de cada uno de los 10 bytes, la red estaría demasiado sobrecargada. Para reducir la sobrecarga de estos acuses de recibo, los segmentos de datos múltiples pueden enviarse previamente y ser reconocidos con un mensaje TCP simple en la dirección opuesta. Este reconocimiento contiene un número de acuse de recibo en base al número 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 reconocimiento igual a 12001.

La cantidad de datos que un origen puede transmitir antes de que un acuse de recibo deba ser recibido se denomina tamaño de la ventana. El tamaño de la ventana es un campo en el encabezado TCP que permite la administración de datos perdidos y el control del flujo.

Acuse de recibo de segmentos TCP

| Puerto de origen | Puerto de destino | Número de secuencia | Números de acuse de recibo | ... |
|------------------|-------------------|---------------------|----------------------------|-----|
|------------------|-------------------|---------------------|----------------------------|-----|



4.3.3 Retransmisión TCP

Manejo de la pérdida de segmentos

Por óptimo que sea el diseño de una red, siempre se producirán pérdidas ocasionales de datos. Por lo tanto, TCP cuenta con métodos para gestionar dichas pérdidas de segmentos. Entre los mismos existe un mecanismo para retransmitir segmentos con datos no reconocidos.

Un servicio de host de destino que utiliza TCP, por lo general sólo reconoce datos para secuencias de bytes contiguas. Si uno o más segmentos se pierden, sólo se acusa recibo de los datos de los segmentos que completan el stream.

Por ejemplo, si se reciben los segmentos con números de secuencia de 1500 a 3000 y de 3400 a 3500, el número de acuse de recibo será 3001. Esto sucede porque existen segmentos con números de secuencia de 3001 a 3399 que no se recibieron.

Cuando TCP en el host de origen no recibe un acuse de recibo pasado un tiempo predeterminado, volverá al último número de acuse de recibo que recibió y retransmitirá los datos a partir de éste.

El proceso de retransmisión no es especificado por RFC, sino que depende de la implementación de TCP en particular.

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.

La animación demuestra la retransmisión de segmentos perdidos.

Los hosts actuales también suelen emplear una función opcional llamada Acuses de recibo selectivos. Si ambos hosts admiten el Acuse de recibo selectivo, es posible que el destino reconozca los bytes de segmentos discontinuos y el host sólo necesitará retransmitir los datos perdidos.

4.3.2 Control de congestión de TCP: Cómo minimizar la perdida de segmentos

Control del flujo

TCP también provee mecanismos para el control del flujo. El control del flujo contribuye con la confiabilidad de la transmisión TCP ajustando la tasa efectiva de flujo de datos entre los dos servicios de la sesión. Cuando el origen advierte que se recibió la cantidad de datos especificados en los segmentos, puede continuar enviando más datos para esta sesión.

El campo Tamaño de la ventana en el encabezado TCP especifica la cantidad de datos que puede transmitirse antes de que se reciba el acuse de recibo. El tamaño de la ventana inicial se determina durante el comienzo de la sesión a través del enlace de tres vías.

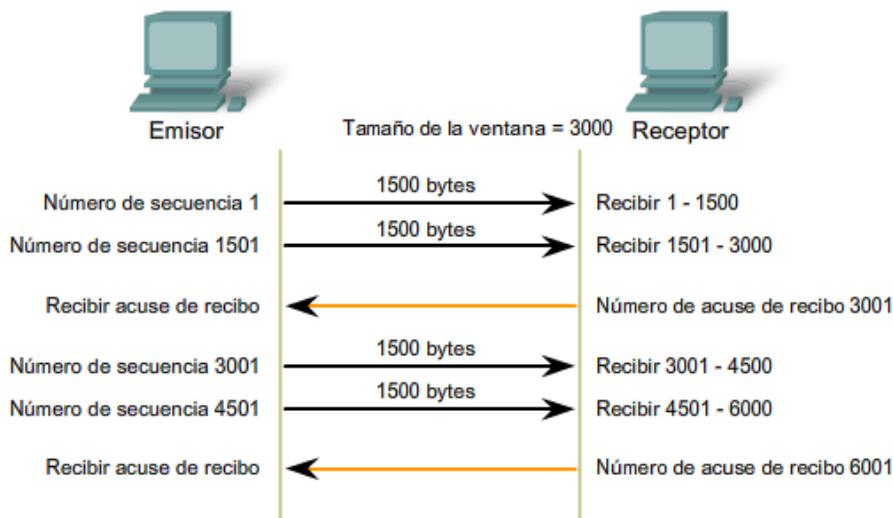
El mecanismo de retroalimentación de TCP ajusta la tasa de transmisión de datos efectiva al flujo máximo que la red y el dispositivo de destino pueden soportar sin sufrir pérdidas. TCP intenta gestionar la tasa de transmisión de manera que todos los datos se reciban y se reduzcan las retransmisiones.

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 ha recibido este acuse de recibo del receptor, ya puede transmitir 3000 bytes adicionales.

Durante la demora en la recepción del acuse de recibo, el emisor no enviará ningún segmento adicional para esta sesión. 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 la tasa de datos ayuda a reducir la contención de recursos.

Acuse de recibo de segmentos TCP y tamaño de la ventana



El tamaño de la ventana determina la cantidad de bytes enviados antes de esperar un acuse de recibo.

El número de acuse de recibo es el número del próximo byte esperado.

Reducción del tamaño de la ventana

Otra forma de controlar el flujo de datos es utilizar tamaños dinámicos de ventana. 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 disminuye de manera efectiva la tasa de transmisión, ya que el origen espera que los datos sean recibidos con más frecuencia.

El host receptor TCP envía el valor del tamaño de la ventana al TCP emisor para indicar el número de bytes que está preparado para recibir como parte de la sesión. Si el destino necesita disminuir la tasa de comunicación debido a limitaciones de memoria del búfer, puede enviar un valor de tamaño de la ventana menor al origen como parte de un acuse de recibo.

Como se muestra en la figura, si un host de recepción sufre una congestión, puede responder al host emisor con un segmento con el tamaño de la ventana reducido. En este gráfico, se produjo la pérdida de uno de los segmentos. El receptor cambió el campo ventana en el encabezado de los mensajes devueltos en esta conversación de 3000 a 1500. Esto hizo que el emisor redujera el tamaño de la ventana a 1500.

Después de períodos de transmisión sin pérdidas de datos o recursos limitados, el receptor comenzará a aumentar el tamaño de la ventana. Esto reduce la sobrecarga de la red, ya que se requiere enviar menos acuses de recibo. El tamaño de la ventana continuará aumentando hasta que haya pérdida de datos, lo que producirá una disminución del tamaño de la ventana.

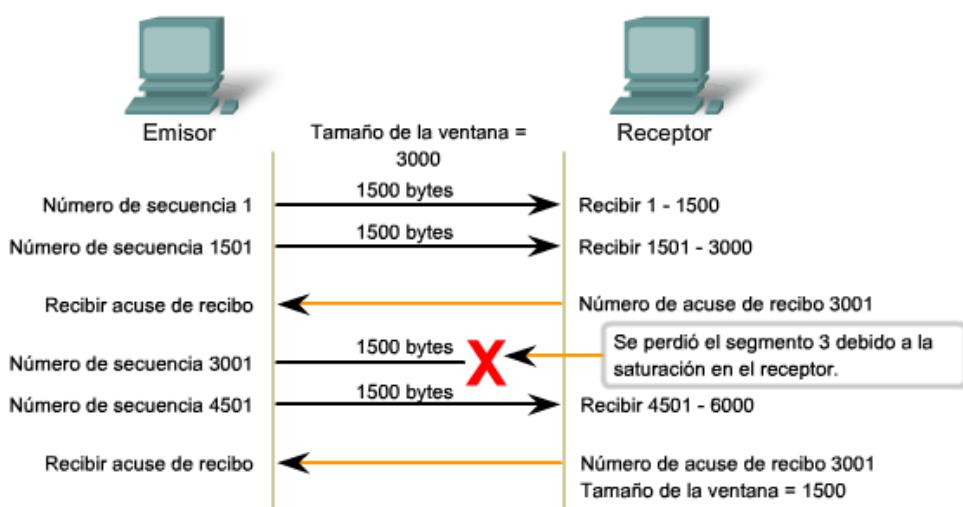
Estas disminuciones y aumentos dinámicos del tamaño de la ventana representan un proceso continuo en TCP, que determina el tamaño de la ventana óptimo para cada sesión TCP. En redes altamente eficientes, los tamaños de la ventana pueden ser muy grandes porque no se pierden datos. En redes donde se está estresando la infraestructura subyacente, el tamaño de la ventana probablemente permanecerá pequeño.

Enlaces

Detalles de las varias características de administración de la congestión de TCP se pueden encontrar en RFC 2581.

<http://www.ietf.org/rfc/rfc2581.txt>

Saturación de TCP y control del flujo



Si se pierden segmentos debido a la saturación, el receptor acusará recibo del último segmento secuencial recibido y responderá con un tamaño de ventana reducido.

4.4 PROTOCOLO UDP: COMUNICACIÓN CON BAJA SOBRECARGA

4.4.1 UDP: Baja sobrecarga Vs Confiabilidad

UDP es un protocolo simple que provee las funciones básicas de la capa de Transporte. Genera mucho menos sobrecarga que TCP, ya que no es orientado a la conexión y no cuenta con los sofisticados mecanismos de retransmisión, secuenciación y control del flujo.

Esto no significa que las aplicaciones que utilizan UDP no sean confiables. Sólo quiere decir que estas funciones no son contempladas por el protocolo de la capa de Transporte y deben implementarse aparte, si fuera necesario.

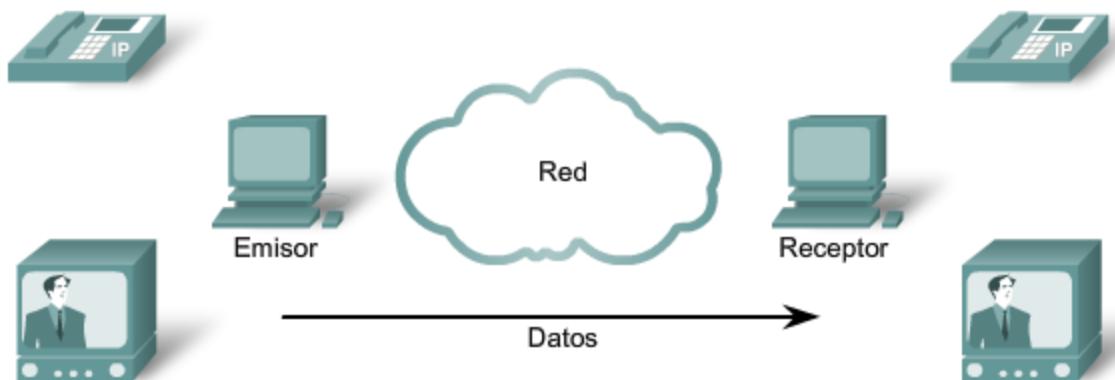
Pese a que es relativamente baja la cantidad total de tráfico UDP que puede encontrarse en una red típica, entre los protocolos principales de la capa de Aplicación que utilizan UDP se incluyen:

- sistema de denominación de dominio (DNS),
- protocolo simple de administración de red (SNMP),
- protocolo de configuración dinámica de host (DHCP),
- protocolo de información de enrutamiento (RIP),
- protocolo trivial de transferencia de archivos (TFTP), y
- juegos en línea.

Algunas aplicaciones como los juegos en línea o VoIP pueden tolerar algunas pérdidas 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 la aplicación que las pequeñas pérdidas de datos. Algunas aplicaciones, como DNS, simplemente reintentan enviar la solicitud si no obtienen respuesta y, por lo tanto, no necesitan TCP para garantizar la entrega del mensaje.

La baja sobrecarga de UDP lo hacen deseable para dichas aplicaciones.

Transporte de datos con baja sobrecarga de UDP



UDP no establece ninguna conexión
antes de enviar datos.

UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.

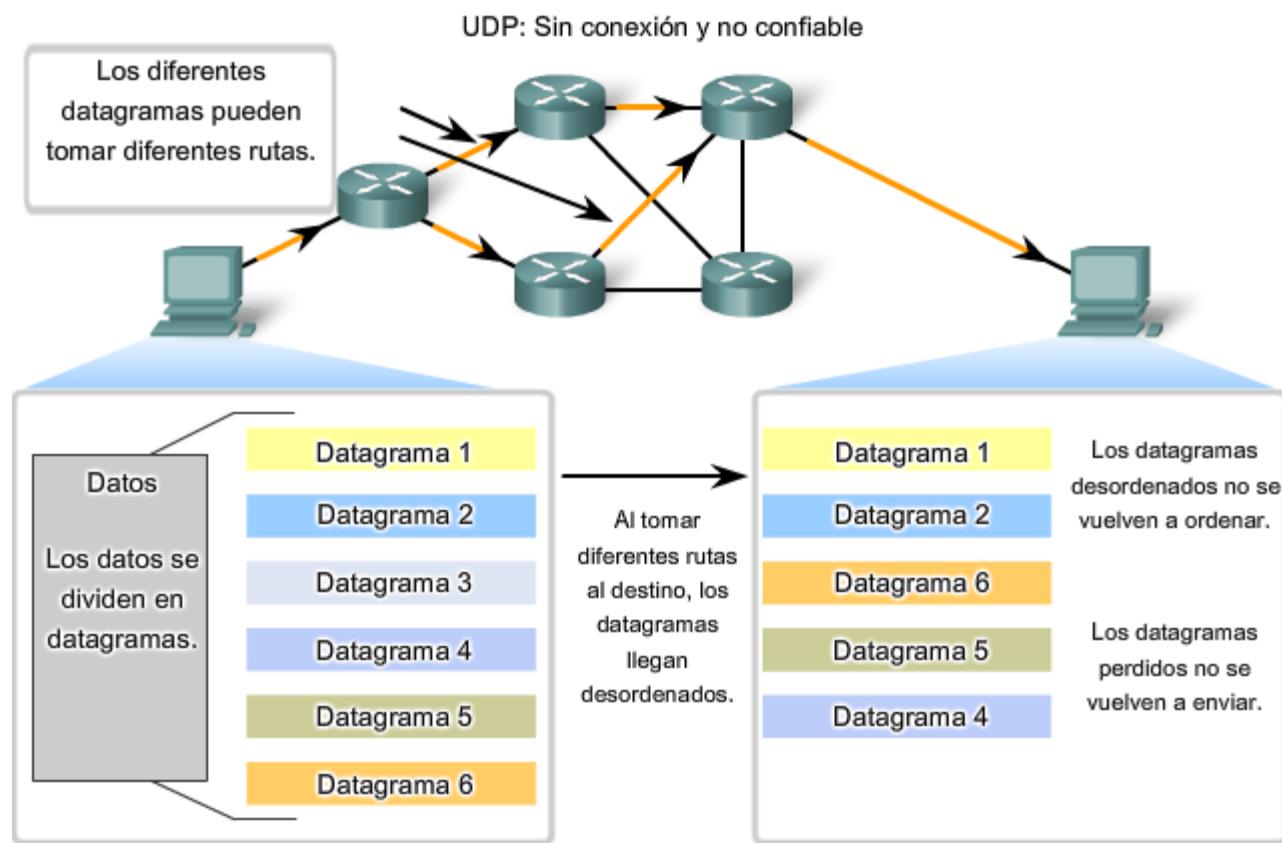
4.4.2 Reensamblaje de datagrama de UDP

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 es basado en transacciones. En otras palabras, cuando una aplicación posee datos para enviar, simplemente los envía.

Muchas aplicaciones que utilizan UDP envían pequeñas cantidades de datos que pueden ocupar un segmento. Sin embargo, algunas aplicaciones enviarán cantidades mayores de datos que deben dividirse en varios segmentos. La PDU de UDP se conoce como datagrama, pese a que los términos segmento y datagrama a veces se utilizan de manera indistinta para describir una PDU de la capa de Transporte.

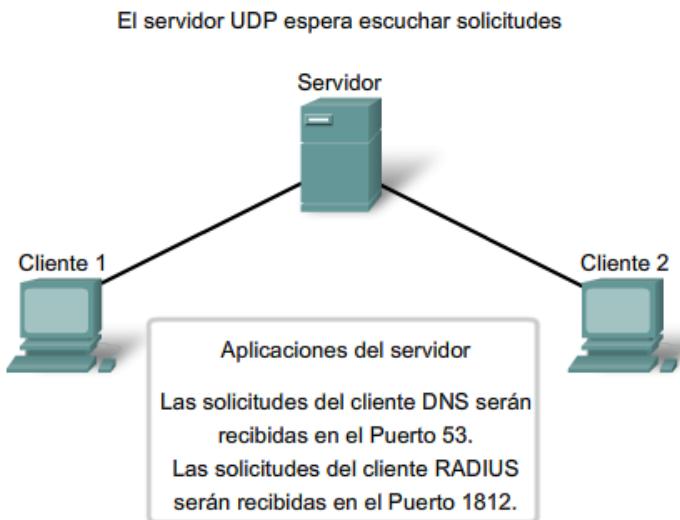
Cuando se envían múltiples datagramas a un destino, los mismos pueden tomar rutas distintas y llegar en el orden incorrecto. UDP no mantiene un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no puede reordenar los datagramas en el orden de la transmisión. Ver la figura.

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 los datos es importante para la aplicación, la misma deberá identificar la secuencia adecuada de datos y determinar cómo procesarlos.



4.4.3 Procesos y solicitudes del servidor UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asigna números de puerto bien conocidos o registrados. Cuando se ejecutan estas aplicaciones o procesos, aceptan los datos que coincidan 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.



Las solicitudes de clientes a servidores utilizan números de puerto bien conocidos como puerto de destino.

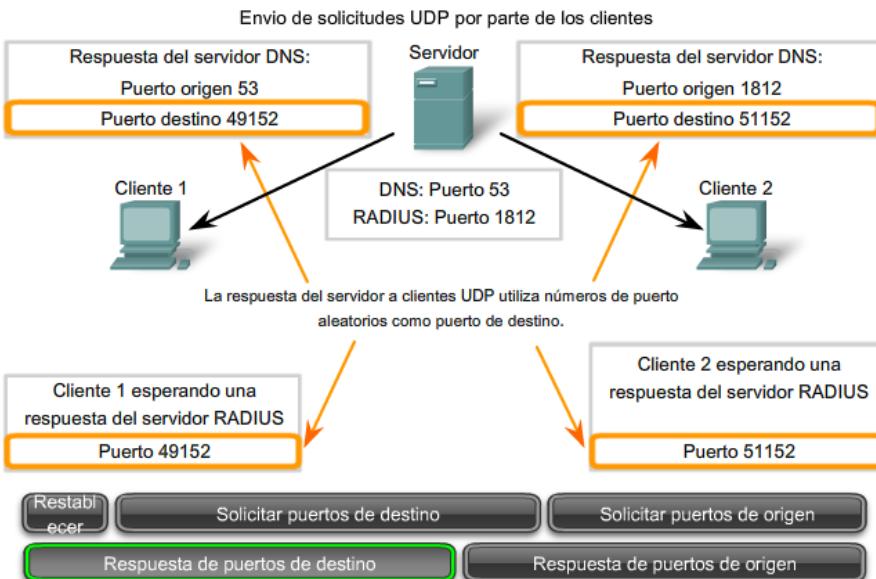
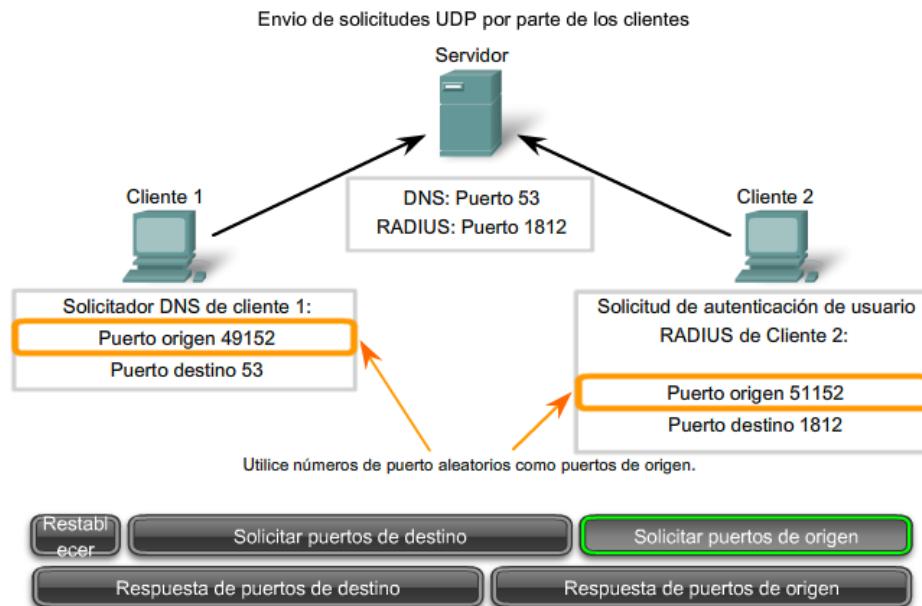
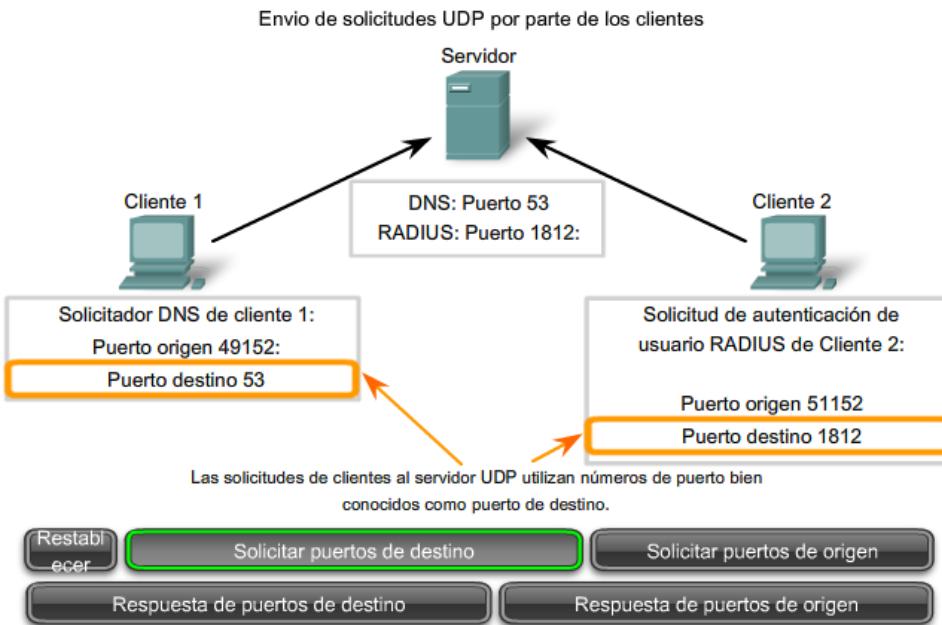
4.4.4 Procesos de cliente UDP

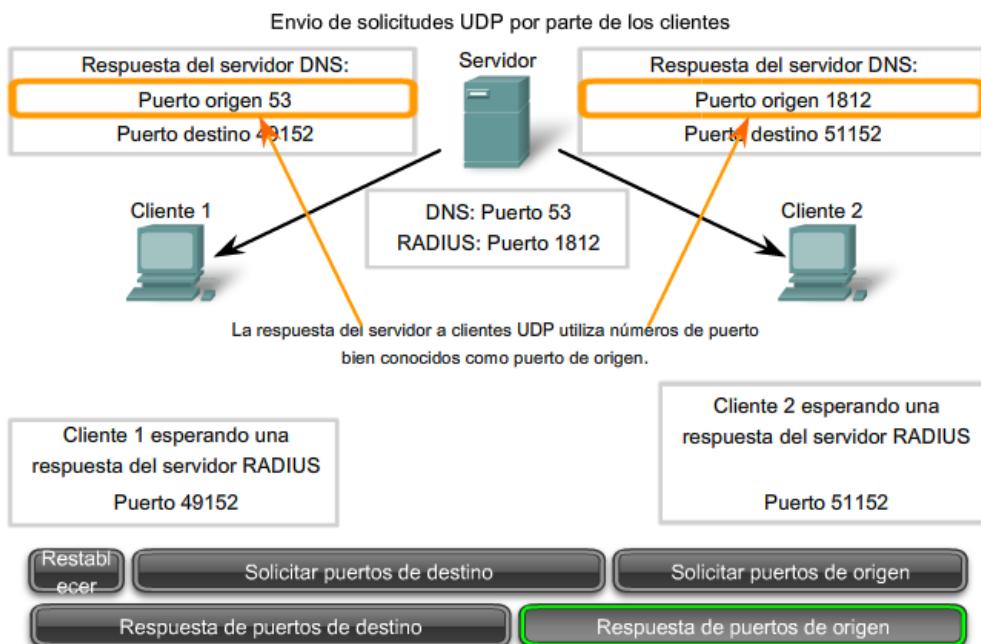
Como en TCP, la comunicación cliente/servidor se inicia por una aplicación cliente que solicita datos de un proceso del servidor. El proceso de cliente UDP selecciona al azar un número de puerto del rango dinámico de números de puerto y lo utiliza como puerto de origen para la conversación. El puerto de destino por lo general será el número de puerto bien conocido o registrado asignado al proceso del 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.

Ya que no se crean sesiones con UDP, tan pronto como los datos están listos para ser enviados y los puertos estén identificados, UDP puede formar el datagrama y enviarlo a la capa de Red para direccionamiento y envío a la red.

Cabe recordar que una vez que el cliente ha elegido los puertos de origen y destino, estos mismos puertos se utilizarán en el encabezado de todos los datagramas que se utilicen 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.





4.6 RESUMEN DEL CAPÍTULO

4.6.1 Resumen y revisión

La capa de Transporte satisface las necesidades de las redes de datos mediante:

- división de datos recibidos desde la aplicación en segmentos,
- agregado de un encabezado para identificar y administrar cada segmento,
- uso de la información del encabezado para recomponer los segmentos en datos de aplicación, y
- paso de los datos ensamblados a la aplicación correcta.

UDP y TCP son protocolos comunes de la capa de Transporte.

Los datagramas UDP y los segmentos TCP tienen encabezados prefijados a los datos que incluyen un número de puerto origen y un número de puerto destino. Estos números de puertos permiten que los datos sean direccionados a la aplicación correcta que se ejecuta en la computadora de destino.

TCP no envía datos a la red hasta que advierte que el destino está preparado para recibirlas. 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 y acuses de recibo y uso dinámico de ventanas para llevar a cabo estas funciones confiables. Sin embargo, esta confiabilidad representa cierta sobrecarga en la red en términos de encabezados de segmentos más grandes y mayor tráfico de red entre el origen y el destino que administra el transporte de datos.

Si los datos de aplicación necesitan ser entregados a 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 será el protocolo de la capa de Transporte preferido por el desarrollador. Esto es así porque UDP no rastrea ni reconoce la recepción de datagramas en el destino, sólo envía los datagramas recibidos a la capa de Aplicación a medida que llegan, y no reenvía datagramas perdidos. Sin embargo, esto no significa necesariamente que la comunicación no es confiable; puede haber

mecanismos en los protocolos y servicios de la capa de Aplicación que procesan datagramas perdidos o demorados si la aplicación cuenta con esos requerimientos.

El desarrollador de la aplicación toma una decisión en cuanto al protocolo de la capa de Transporte en base a los requerimientos del usuario. Sin embargo, el desarrollador tiene en cuenta que las otras capas cumplen un rol importante en las comunicaciones de redes de datos y tendrán influencia en el rendimiento.

5- CAPA DE RED DE OSI

5.0-INTRODUCCION AL CAPITULO

5.0.1 Introducción del capítulo

Hemos visto cómo los servicios y aplicaciones de red en un dispositivo final pueden comunicarse con aplicaciones y servicios que se ejecutan en otro dispositivo final.

A continuación, según se muestra en la figura, consideraremos cómo se transportan estos datos a través de la red: desde el dispositivo final de origen (o host) hasta el host de destino, de manera eficiente.

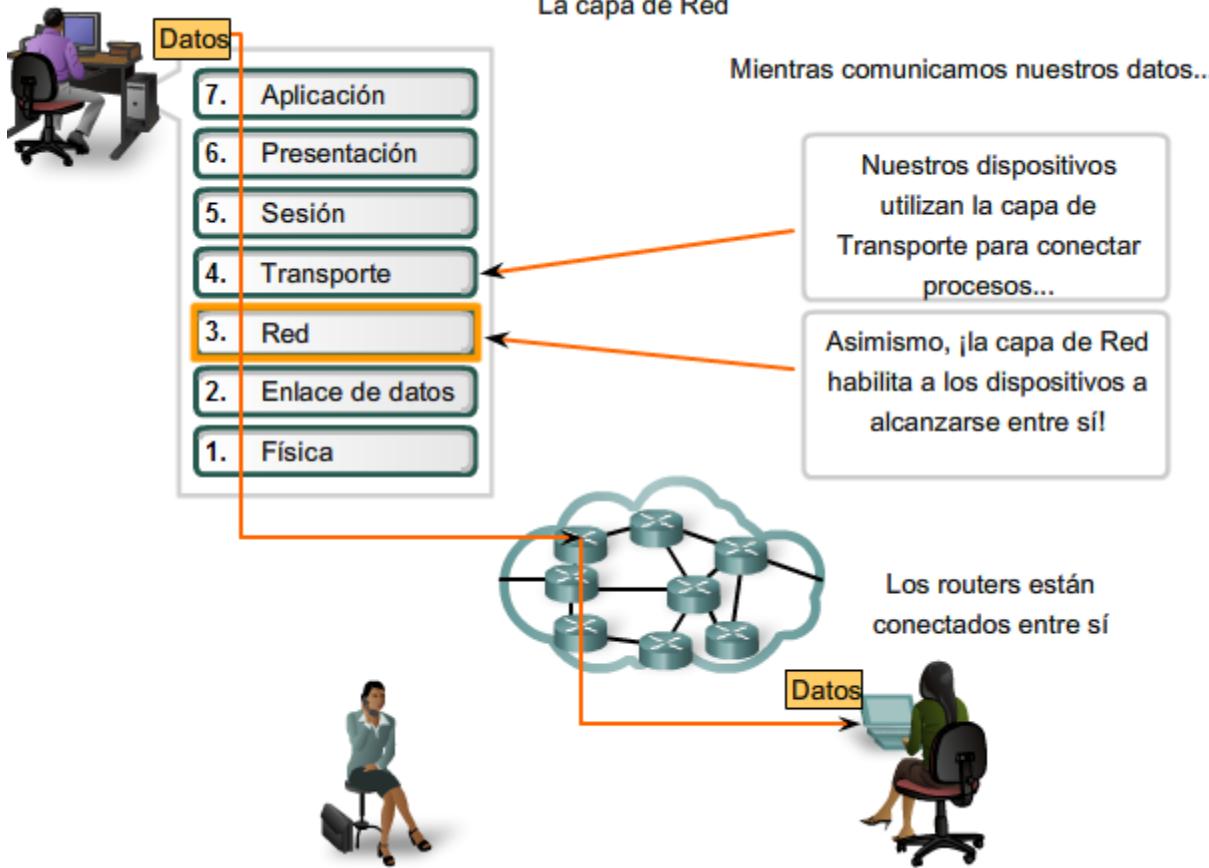
Los protocolos de la capa de Red del modelo OSI especifican el direccionamiento y los procesos que permiten que los datos de la capa de Transporte sean empaquetados y transportados. La encapsulación de la capa de Red permite que su contenido pase al destino dentro de una red o sobre otra red con una carga mínima.

Este capítulo aborda la función de la capa de Red, analizando cómo esta capa divide las redes en grupos de hosts para administrar el flujo de paquetes de datos dentro de una red. Además, consideraremos cómo se facilita la comunicación entre redes. A esta comunicación entre redes se la denomina enrutamiento.

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

- Identificar la función de la capa de Red, ya que describe la comunicación desde un dispositivo final a otro dispositivo final.
- Examinar el protocolo de Capa de red más común, Protocolo de Internet (IP) y sus características de proveer servicio sin conexión y de máximo esfuerzo.
- Comprender los principios utilizados para guiar la división o agrupamiento de dispositivos en redes.
- Comprender el direccionamiento jerárquico de dispositivos y cómo esto permite la comunicación entre redes.
- Comprender los fundamentos de rutas, direcciones de próximo salto y envío de paquetes a una red destino.



5.1 IPv4

5.1.1 Capa de red: Comunicación de host a host

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- direccionamiento,
- encapsulamiento,
- enrutamiento , y
- desencapsulamiento.

La animación en la figura muestra el intercambio de datos.

Direccionamiento

Primero, la Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red Ipv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación

Segundo, la capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de Red, deben, además, contener estas direcciones. Durante el proceso de

encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen.

Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

Enrutamiento

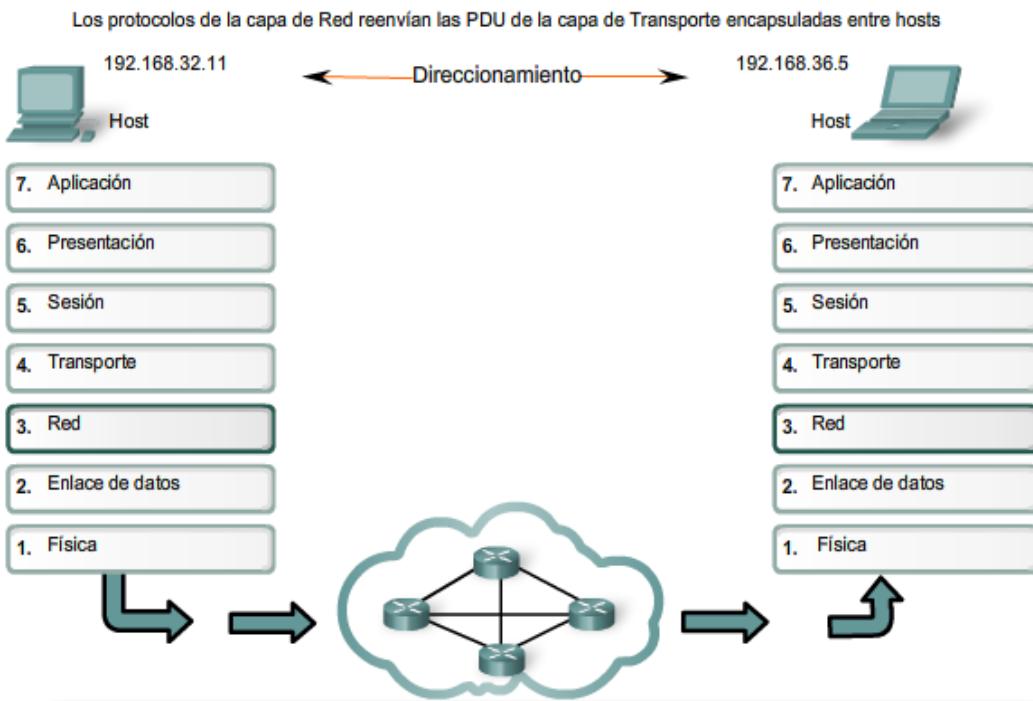
Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que el paquete es enviado, su contenido (la PDU de la Capa de transporte) permanece intacto hasta que llega al host destino.

Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado 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 final, los protocolos específicos especifican la estructura y el procesamiento del paquete utilizados para llevar los datos desde un host hasta otro host. Operar ignorando los datos de aplicación llevados en cada paquete permite a la capa de Red llevar paquetes para múltiples tipos de comunicaciones entre hosts múltiples.

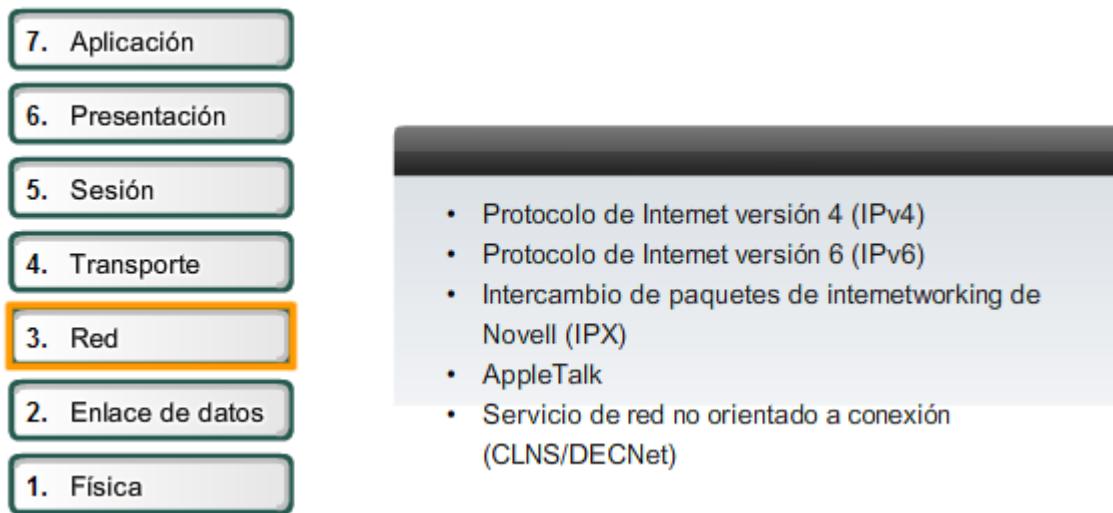


Protocolos de capa de Red

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- versión 4 del Protocolo de Internet (Ipv4),
- versión 6 del Protocolo de Internet (Ipv6),
- Intercambio Novell de paquetes de internetwork (IPX),
- AppleTalk, y
- servicio de red sin conexión (CLNS/DECNet).

El Protocolo de Internet (Ipv4 y Ipv6) es el protocolo de transporte de datos de la capa 3 más ampliamente utilizado y será el tema de este curso. Los demás protocolos no serán abordados en profundidad.



5.1.2 Protocolo Ipv4: Ejemplo de protocolo de capa de Red

Rol del Ipv4

Como se muestra en la figura, los servicios de capa de Red implementados por el conjunto de protocolos TCP/IP son el Protocolo de Internet (IP). La versión 4 de IP (Ipv4) es la versión de IP más ampliamente utilizada. Es el único protocolo de Capa 3 que se utiliza para llevar datos de usuario a través de Internet y es el tema de CCNA. Por lo tanto, será el ejemplo que usamos para protocolos de capa de Red en este curso.

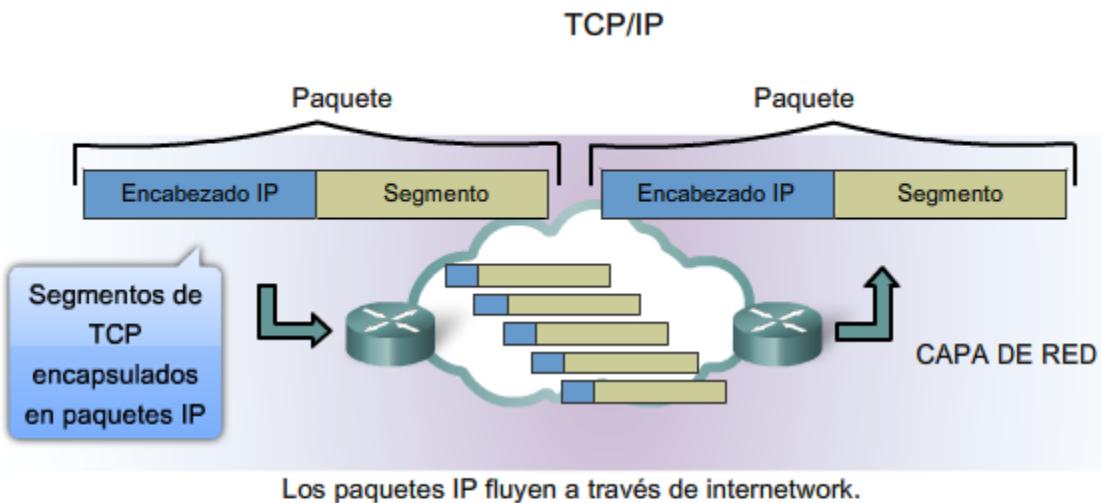
La versión 6 de IP (Ipv6) está desarrollada y se implementa en algunas áreas. Ipv6 operará junto con el Ipv4 y puede reemplazarlo en el futuro. Los servicios provistos por IP, así como también la estructura y el contenido del encabezado de los paquetes están especificados tanto por el protocolo Ipv4 como por el Ipv6. Estos servicios y estructura de paquetes se usan para encapsular datagramas UDP o segmentos TCP para su recorrido a través de una internetwork.

Las características de cada protocolo son diferentes. Comprender estas características le permitirá comprender la operación de los servicios descritos por este protocolo.

El Protocolo de Internet fue diseñado como un protocolo con bajo costo. 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. Estas funciones son realizadas por otros protocolos en otras capas.

Características básicas de Ipv4:

- Sin conexión: No establece conexión antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): No se usan encabezados para garantizar la entrega de paquetes.
- Medios independientes: Operan independientemente del medio que lleva los datos.



- Sin conexión: sin establecimiento de conexión en forma previa al envío de paquetes de datos.
- Mejor intento (no confiable): sin sobrecarga para garantizar la entrega de paquetes.
- Independiente de los medios: funciona en forma independiente de los medios que transportan los datos.

5.1.3 Protocolo Ipv4: Sin conexión

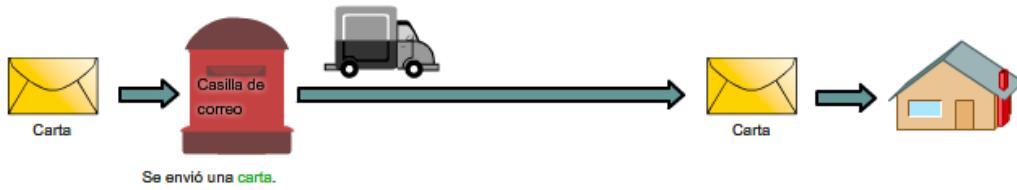
Servicio sin conexión

Un ejemplo de comunicación sin conexión es enviar una carta a alguien sin notificar al receptor con anticipación. Como se muestra en la figura, el servicio postal aún lleva la carta y la entrega al receptor. Las comunicaciones de datos sin conexión funcionan en base al mismo principio. Los paquetes IP se envían sin notificar al host final que están llegando.

Los protocolos orientados a la conexión, como TCP, requieren el intercambio del control de datos para establecer la conexión así como también los campos adicionales en el encabezado de la PDU. Como IP trabaja sin conexión, no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que los paquetes sean enviados, ni requiere campos adicionales en el encabezado de la PDU para mantener esta conexión. Este proceso reduce en gran medida la sobrecarga del IP.

Sin embargo, la entrega del paquete sin conexión puede hacer que los paquetes lleguen a destino fuera de secuencia. Si los paquetes que no funcionan o están perdidos crean problemas para la aplicación que usa los datos, luego los servicios de las capas superiores tendrán que resolver estas cuestiones.

Comunicación sin conexión



El emisor no sabe:

- si el receptor está presente
- si llegó la carta
- si el receptor puede leer la carta

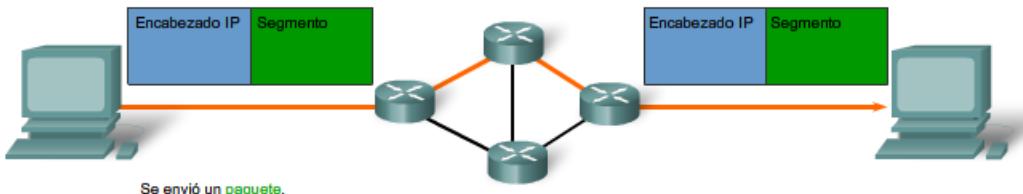
El receptor no sabe:

- cuándo llegará

RUTAS POSTALES

REDES DE DATOS

Comunicación sin conexión



El emisor no sabe:

- si el receptor está presente
- si llegó el paquete
- si el receptor puede leer el paquete

El receptor no sabe:

- cuándo llegará

RUTAS POSTALES

REDES DE DATOS

5.1.4 Protocolo Ipv4: Mejor Intento

Servicio de mejor intento (no confiable)

El protocolo IP no sobrecarga el servicio IP suministrando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño. Transportar estos encabezados más pequeños genera una menor sobrecarga. Menor sobrecarga significa menos demora en la entrega. Esta característica es preferible para un protocolo de Capa 3.

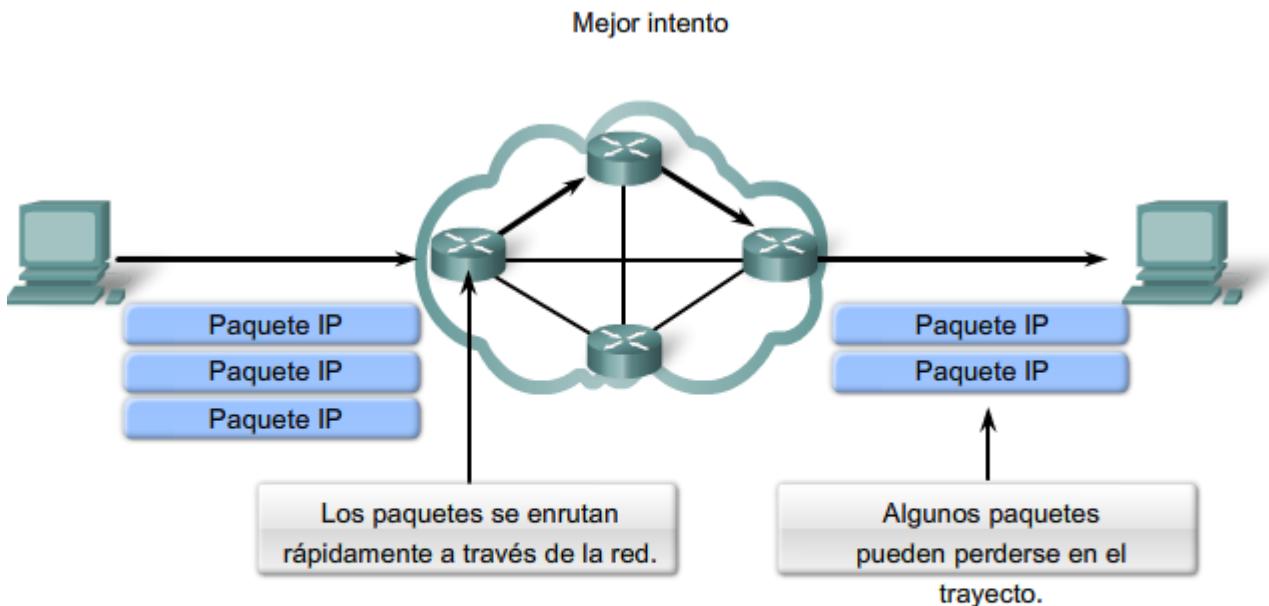
La función de la Capa 3 es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La Capa 3 no se ocupa de ni advierte el tipo de comunicación contenida dentro de un paquete. Esta responsabilidad es la función de las capas superiores a medida que se requieren. Las capas superiores pueden decidir si la comunicación entre servicios necesita confiabilidad y si esta comunicación puede tolerar la sobrecarga que la confiabilidad requiere.

Al IP a menudo se lo considera un protocolo no confiable. No confiable en este contexto no significa que el IP funciona adecuadamente algunas veces y no funciona bien en otras oportunidades. Tampoco significa que no es adecuado como

protocolo de comunicaciones de datos. **No confiable significa simplemente que IP no tiene la capacidad de administrar ni recuperar paquetes no entregados o corruptos.**

Como los protocolos en otras capas pueden administrar la confiabilidad, se le permite a IP funcionar con mucha eficiencia en la capa de Red. Si incluimos la sobrecarga de confiabilidad en el protocolo de la Capa 3, las comunicaciones que no requieren conexiones o confiabilidad se cargarían con el consumo de ancho de banda y la demora producida por esta sobrecarga. En el conjunto TCP/IP, la capa de Transporte puede elegir entre TCP o UDP, basándose en las necesidades de la comunicación. Como con toda separación de capa provista por los modelos de redes, dejar la decisión de confiabilidad a la capa de Transporte hace que IP sea más adaptable y se acomode según los diferentes tipos de comunicación.

El encabezado de un paquete IP no incluye los campos requeridos para la entrega confiable de datos. No hay acuses de recibo de entrega de paquetes. No hay control de error para datos. Tampoco hay forma de rastrear paquetes; por lo tanto, no existe la posibilidad de retransmitir paquetes.



Al ser un protocolo no confiable de capa de Red, IP no garantiza la recepción de todos los paquetes enviados.

Otros protocolos administran el proceso de seguimiento de paquetes y garantizan su entrega.

5.1.5 Protocolo Ipv4: Independiente de los medios

Independiente de los medios

La capa de Red tampoco está cargada con las características de los medios mediante los cuales se transportarán los paquetes. Ipv4 y Ipv6 operan independientemente de los medios que llevan los datos a capas inferiores del stack del protocolo. 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 las señales de radio.

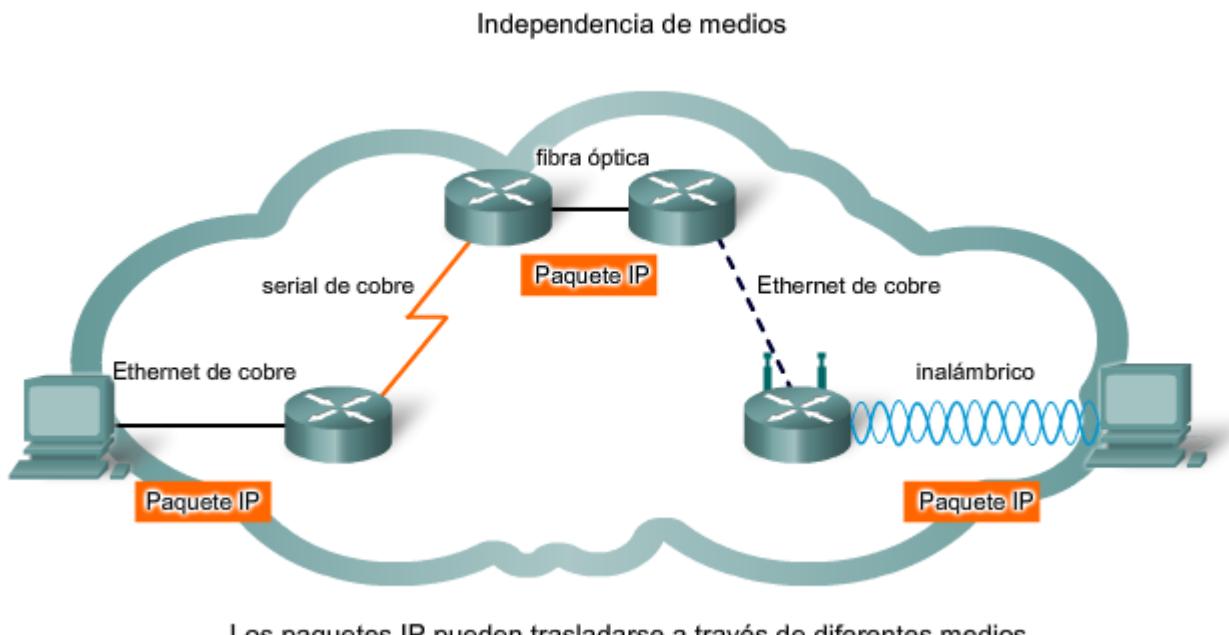
Es responsabilidad de la capa de Enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

Existe, no obstante, una característica principal de los medios que la capa de Red considera: el tamaño máximo de la PDU que cada medio puede transportar. A esta característica se la denomina Unidad máxima de transmisión (MTU). Parte de la comunicación de control entre la capa de Enlace de datos y la capa de Red es establecer un tamaño máximo para el paquete. La capa de Enlace de datos pasa la MTU hacia arriba hasta la capa de Red. La capa de Red entonces determina de qué tamaño crear sus paquetes.

En algunos casos, un dispositivo intermedio, generalmente un router, necesitará separar un paquete cuando se lo envía desde un medio a otro medio con una MTU más pequeña. A este proceso se lo llama fragmentación de paquetes o fragmentación.

Enlaces

RFC-791 <http://www.ietf.org/rfc/rfc0791.txt>



5.1.6 Protocolo IPv4: Empaque de la PDU de la capa de Transporte

Ipv4 encapsula o empaqueta el datagrama o segmento de la capa de Transporte para que la red pueda entregarlo a su host de destino. Haga clic en los pasos dentro de la figura para ver este proceso. La encapsulación de Ipv4 permanece en su lugar desde el momento en que el paquete deja la capa de Red del host de origen hasta que llega a la capa de Red del host de destino.

El proceso de encapsular datos por capas permite que los servicios en las diferentes capas se desarrollen y escalen sin afectar otras capas. Esto significa que los segmentos de la capa de Transporte pueden ser empaquetados fácilmente por los protocolos de la capa de Red existentes, como Ipv4 e Ipv6, o por cualquier protocolo nuevo que pueda desarrollarse en el futuro.

Los routers pueden implementar estos protocolos de la capa de Red para operar concurrentemente en una red hacia y desde el mismo host u otro. El enruteamiento realizado por estos dispositivos intermedios sólo considera el contenido del encabezado de paquetes que encapsula el segmento.

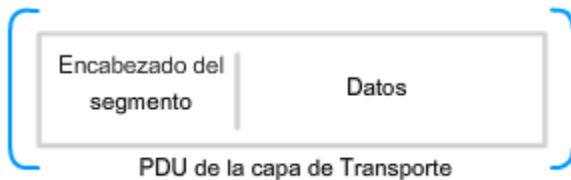
En todos los casos, la porción de datos del paquete, es decir, el PDU de la Capa de transporte encapsulada, permanece sin cambios durante los procesos de la capa de red.

Enlaces

RFC-791 <http://www.ietf.org/rfc/rfc0791.txt>

Generación de paquetes IP

Encapsulación de la capa de Transporte

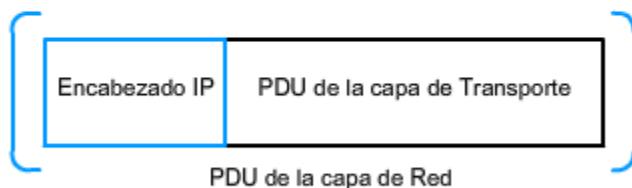


La **capa de Transporte** agrega un encabezado para que puedan incluirse los segmentos y vuelvan a ordenarse en el destino.

Encapsulación de la capa de Transporte

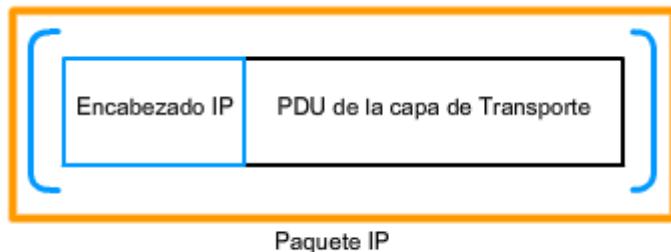


Encapsulación de la capa de Red



La **capa de Red** agrega un encabezado para que puedan enrutararse los paquetes a través de redes complejas y lleguen a destino.

Encapsulación de la capa de Red



En **redes basadas en TCP/IP**, la PDU de la capa de Red es el **paquete IP**.

5.1.7 Encabezado de paquete IPv4

Como se muestra en la figura, un protocolo Ipv4 define muchos campos diferentes en el encabezado del paquete. Estos campos contienen valores binarios que los servicios Ipv4 toman como referencia a medida que envían paquetes a través de la red.

Este curso considerará estos 6 campos clave:

- dirección IP origen,
- dirección IP destino,
- tiempo de existencia (TTL),
- tipo de servicio (ToS),
- protocolo, y
- desplazamiento del fragmento.

Campos Ipv4 de encabezados clave

Coloque el cursor sobre cada campo en el gráfico para ver su propósito.

Dirección IP destino

El campo de Dirección IP destino contiene un valor binario de 32 bits que representa la dirección de host de capa de red de destino del paquete.

Dirección IP origen

El campo de Dirección IP origen contiene un valor binario de 32 bits que representa la dirección de host de capa de red de origen del paquete.

Tiempo de vida

El tiempo de vida (TTL) es un valor binario de 8 bits que indica el tiempo remanente de “vida” del paquete. El valor TTL disminuye al menos en uno cada vez que el paquete es procesado por un router (es decir, en cada salto). Cuando el valor se vuelve cero, el router descarta o elimina el paquete y es eliminado del flujo de datos de la red. Este mecanismo evita que los paquetes que no pueden llegar a destino sean enviados indefinidamente entre los routers en un routing loop. Si se permitiera que los loops de enrutamiento continúen, la red se congestionaría con paquetes de datos que nunca llegarían a destino. Disminuyendo el valor TTL en cada salto se asegura que eventualmente se vuelva cero y que se descartará el paquete con el campo TTL vencido.

Protocolo

Este valor binario de 8 bits indica el tipo de relleno de carga que el paquete traslada. El campo de protocolo permite a la Capa de red pasar los datos al protocolo apropiado de la capa superior.

Los valores de ejemplo son:

- 01 ICMP,
- 06 TCP, y
- 17 UDP.

Tipo de servicio

El campo de tipo de servicio contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de Calidad del Servicio (QoS) a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía. El router que procesa los paquetes puede ser configurado para decidir qué paquete es enviado primero basado en el valor del Tipo de servicio.

Desplazamiento de fragmentos

Como se mencionó antes, un router puede tener que fragmentar un paquete cuando lo envía desde un medio a otro medio que tiene una MTU más pequeña. Cuando se produce una fragmentación, el paquete IPv4 utiliza el campo Desplazamiento de fragmento y el señalizador MF en el encabezado IP para reconstruir el paquete cuando llega al host destino. El campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

Señalizador de Más fragmentos

El señalizador de Más fragmentos (MF) es un único bit en el campo del señalizador usado con el Desplazamiento de fragmentos para la fragmentación y reconstrucción de paquetes. Cuando está configurado el señalizador Más fragmentos, significa que no es el último fragmento de un paquete. Cuando un host receptor ve un paquete que llega con MF = 1, analiza el Desplazamiento de fragmentos para ver dónde ha de colocar este fragmento en el paquete reconstruido. Cuando un host receptor recibe una trama con el MF = 0 y un valor diferente a cero en el desplazamiento de fragmentos, coloca ese fragmento como la última parte del paquete reconstruido. Un paquete no fragmentado tiene toda la información de fragmentación cero (MF = 0, desplazamiento de fragmentos = 0).

Señalizador de No Fragmentar

El señalizador de No Fragmentar (DF) es un solo bit en el campo del señalizador que indica que no se permite la fragmentación del paquete. Si se establece el bit del señalizador No Fragmentar, entonces la fragmentación de este paquete NO está permitida. Si un router necesita fragmentar un paquete para permitir el paso hacia abajo hasta la capa de Enlace de datos pero el bit DF se establece en 1, entonces el router descartará este paquete.

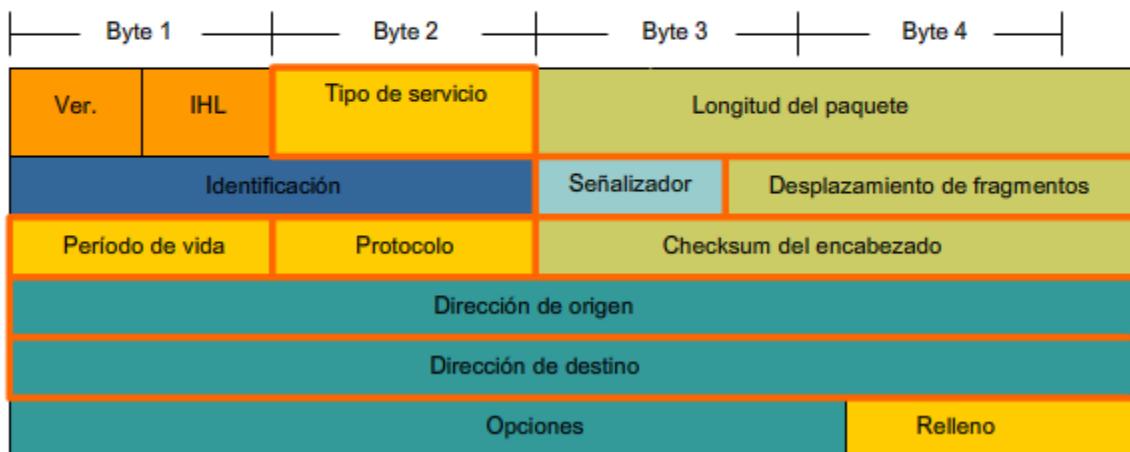
Enlaces:

RFC 791 <http://www.ietf.org/rfc/rfc0791.txt>

Para obtener una lista completa de valores del campo IP de número de protocolo

<http://www.iana.org/assignments/protocol-numbers>

Campos del encabezado de paquetes IPv4



| | |
|---|--|
| Tipo de servicio | Prioridad de QoS de datos: Habilita al router para dar prioridad a la información de ruta de red y voz sobre los datos comunes. |
| Señalizador | Estos 3 bits representan los señalizadores de control, tales como DF y MF. |
| Período de vida | Cantidad de saltos antes de que se descarte el paquete: Este valor se reduce en cada salto para evitar que los paquetes se transmitan a través de la red en routing loops. |
| Desplazamiento de fragmentos | Estos 13 bits habilitan a un receptor para determinar el lugar de un fragmento particular en el datagrama IP original. |
| Protocolo | Dirección de origen |
| Tipo de protocolo de contenido de datos: Indica si los datos son un datagrama UDP o segmento TCP, ya que estos protocolos de la capa de Transporte administran la recepción de sus PDU de manera diferente. | Dirección IPv4 del host que envía el paquete: Se mantiene inalterable a lo largo de todo el recorrido del paquete a través de internetwork. Habilita al host de destino para responder al de origen si es necesario. |
| Dirección de destino | Dirección IPv4 del host que recibe el paquete: Se mantiene inalterable a lo largo de todo el recorrido del paquete a través de internetwork. Habilita a los routers de cada salto para reenviar el paquete hacia el destino. |

Otros Campos IPv4 del encabezado

Coloque el cursor sobre cada campo en el gráfico para ver su propósito.

Versión: Contiene el número IP de la versión (4).

Longitud del encabezado (IHL). Especifica el tamaño del encabezado del paquete.

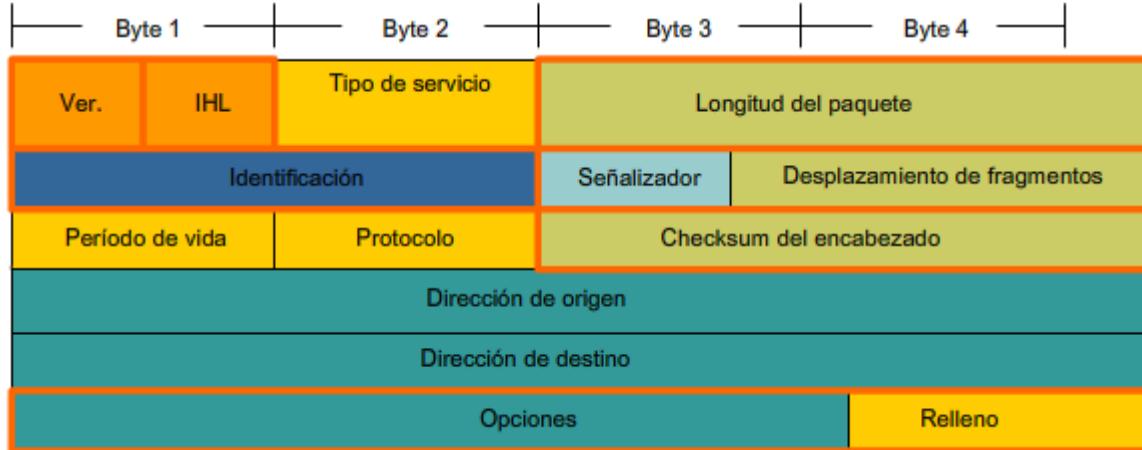
Longitud del Paquete: Este campo muestra el tamaño completo del paquete, incluyendo el encabezado y los datos, en bytes.

Identificación: Este campo es principalmente utilizad para identificar únicamente fragmentos de un paquete IP original.

Checksum del encabezado: El campo de checksum se utiliza para controlar errores del encabezado del paquete.

Opciones: Existen medidas para campos adicionales en el encabezdo Ipv4 para proveer otros servicios pero éstos son rara vez utilizados.

Campos del encabezado de paquetes IPv4



| IHL (Longitud del encabezado) | |
|---|--------------------------|
| Versión | El número de versión IP. |
| Longitud del paquete | |
| Tamaño del paquete completo, que incluye el encabezado y los datos, en bytes. La longitud mínima del paquete es de 20 bytes (20 bytes de encabezado + 0 bytes de datos) y el máximo es 65.535; el valor máximo que puede tener este campo de 16 bits. | |
| Identificación | |
| Identifica fragmentos de forma exclusiva en un paquete IP original. | |
| Checksum del encabezado | |
| Se utiliza para la verificación de errores en el encabezado de paquetes. En cada salto, la checksum del encabezado debe compararse con el valor de este campo. Si el valor de la checksum del encabezado no coincide con la checksum calculada, el paquete se descartará. En cada salto, el campo TTL disminuye y la fragmentación se vuelve posible; por lo tanto, debe volver a calcularse la checksum en cada salto. Nota: esta checksum sólo se aplica al encabezado y no a los datos encapsulados. | |
| Opciones | |
| Encabezado de campos adicional para suministrar otros servicios, utilizado con escasa frecuencia. | |

Paquete IP típico

La figura representa un paquete IP completo con valores típicos de campo del encabezado.

Ver = 4; versión IP.

IHL = 5; tamaño del encabezado en palabras de 32 bits (4 bytes). Este encabezado tiene $5 \times 4 = 20$ bytes, el tamaño mínimo válido.

Longitud total = 472; tamaño del paquete (encabezado y datos) de 472 bytes.

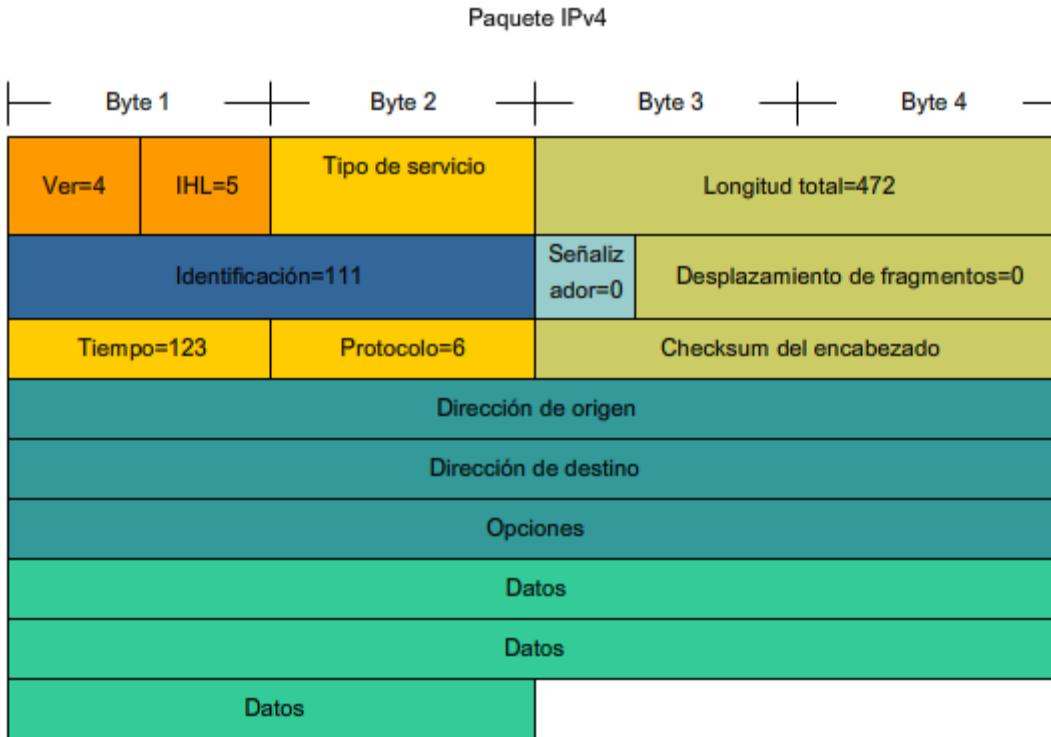
Identificación = 111; identificador original del paquete (requerido si se fragmenta posteriormente).

Señalizador = 0; significa que el paquete puede ser fragmentado si se requiere.

Desplazamiento de fragmentos = 0; significa que este paquete no está actualmente fragmentado (no existe desplazamiento).

Período de vida = 123; es el tiempo de procesamiento en segundos de la Capa 3 antes de descartar el paquete (disminuye en al menos 1, cada vez que el dispositivo procesa el encabezado del paquete).

Protocolo = 6; significa que los datos llevados por este paquete son un segmento TCP.



5.2 REDES: DIVISION DE HOST EN GRUPOS

5.2.1 Redes: Separación de los host en grupos comunes

Una de las principales funciones de la capa de Red es proveer un mecanismo para direccionar hosts. A medida que crece el número de hosts de la red, se requiere más planificación para administrar y direccionar la red.

División de redes

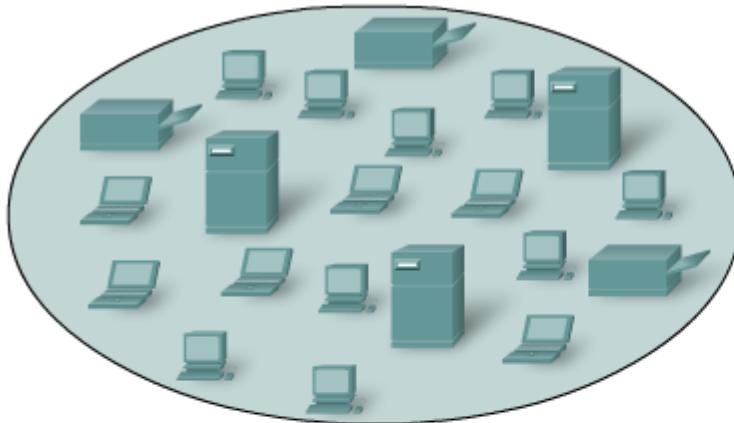
En lugar de tener todos los hosts conectados en cualquier parte a una vasta red global, es más práctico y manejable agrupar los hosts en redes específicas. Históricamente, las redes basadas en IP tienen su raíz como una red grande. Como esta red creció, también lo hicieron los temas relacionados con su crecimiento. Para aliviar estos problemas, la red grande fue separada en redes más pequeñas que fueron interconectadas. Estas redes más pequeñas generalmente se llaman subredes.

Red y subred son términos utilizados indistintamente para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP.

De manera similar, a medida que nuestras redes crecen, pueden volverse demasiado grandes para manejarlas como una única red. En ese punto, necesitamos dividir nuestra red. Cuando planeamos la división de la red, necesitamos agrupar aquellos hosts con factores comunes en la misma red.

Como muestra la figura, las redes pueden agruparse basadas en factores que incluyen:

- ubicación geográfica,
- propósito, y
- propiedad.



Los diseñadores de redes deben preguntar: ¿en función de qué debe dividirse la red?

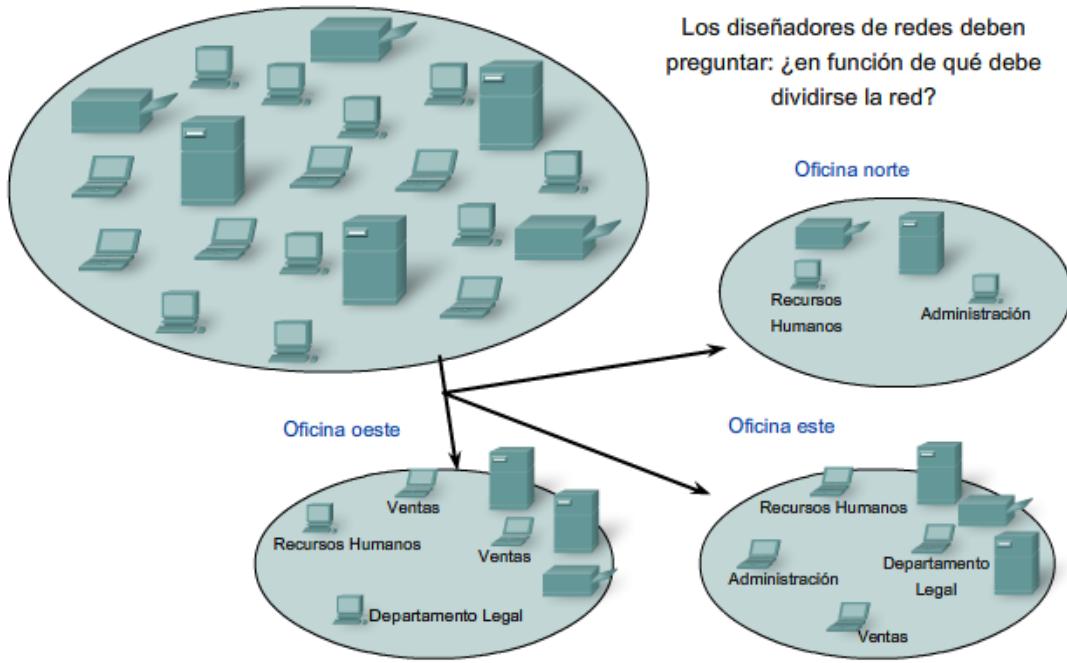
Una red amplia es demasiado compleja para que se opere y administre en forma eficiente.

INICIAR

GEOGRÁFICO

PROPÓSITO

PROPIEDAD

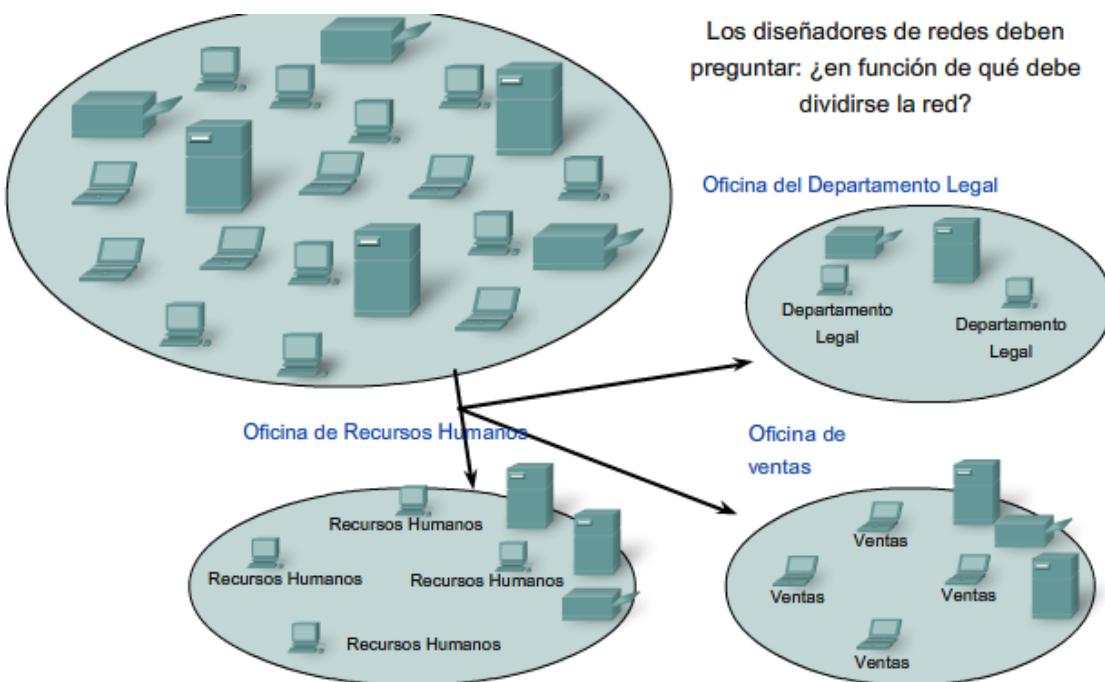


INICIAR

GEOGRÁFICO

PROPÓSITO

PROPIEDAD

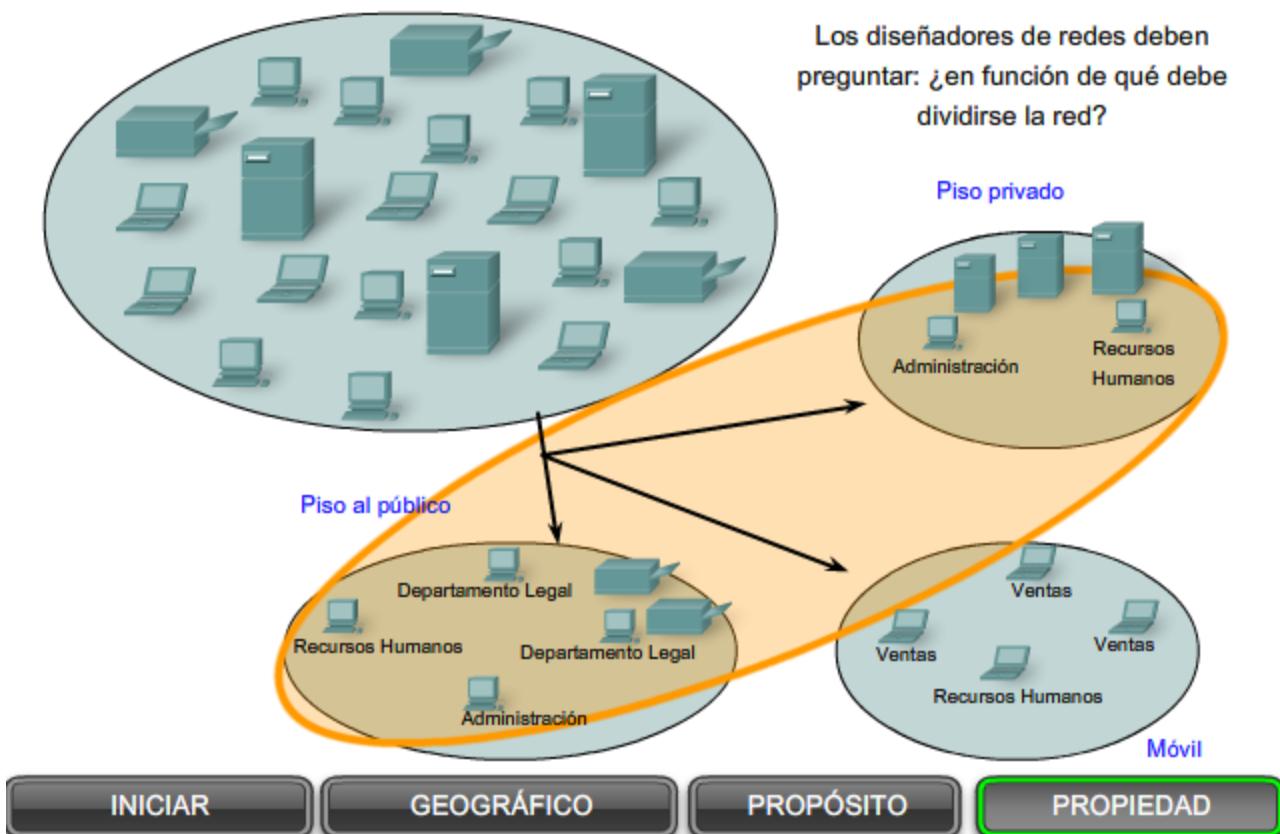


INICIAR

GEOGRÁFICO

PROPÓSITO

PROPIEDAD



Agrupación de hosts de manera geográfica

Podemos agrupar hosts de redes geográficamente. El agrupamiento de hosts en la misma ubicación, como cada construcción en un campo o cada piso de un edificio de niveles múltiples, en redes separadas puede mejorar la administración y operación de la red.

Haga clic en el botón GEOGRÁFICO de la figura.

Agrupación de hosts para propósitos específicos

Los usuarios que tienen tareas similares usan generalmente software común, herramientas comunes y tienen patrones de tráfico común. A menudo podemos reducir el tráfico requerido por el uso de software y herramientas específicos, ubicando estos recursos de soporte en la red con los usuarios.

El volumen del tráfico de datos de la red generado por las diferentes aplicaciones puede variar significativamente. Dividir redes basadas en el uso facilita la ubicación efectiva de los recursos de la red así como también el acceso autorizado a esos recursos. Los profesionales en redes necesitan equilibrar el número de hosts en una red con la cantidad de tráfico generado por los usuarios. Por ejemplo, considere una empresa que emplea diseñadores gráficos que utilizan la red para compartir archivos multimedia muy grandes. Estos archivos consumen la mayoría del ancho de banda disponible durante gran parte del día laboral. La empresa también emplea vendedores que se conectan una vez al día para registrar sus transacciones de ventas, lo que genera un tráfico mínimo de red. En este escenario, el mejor uso de los recursos de la red sería crear varias redes pequeñas a las cuales unos pocos diseñadores tengan acceso y una red más grande para que usen todos los vendedores.

Haga clic en el botón PROPÓSITO de la figura.

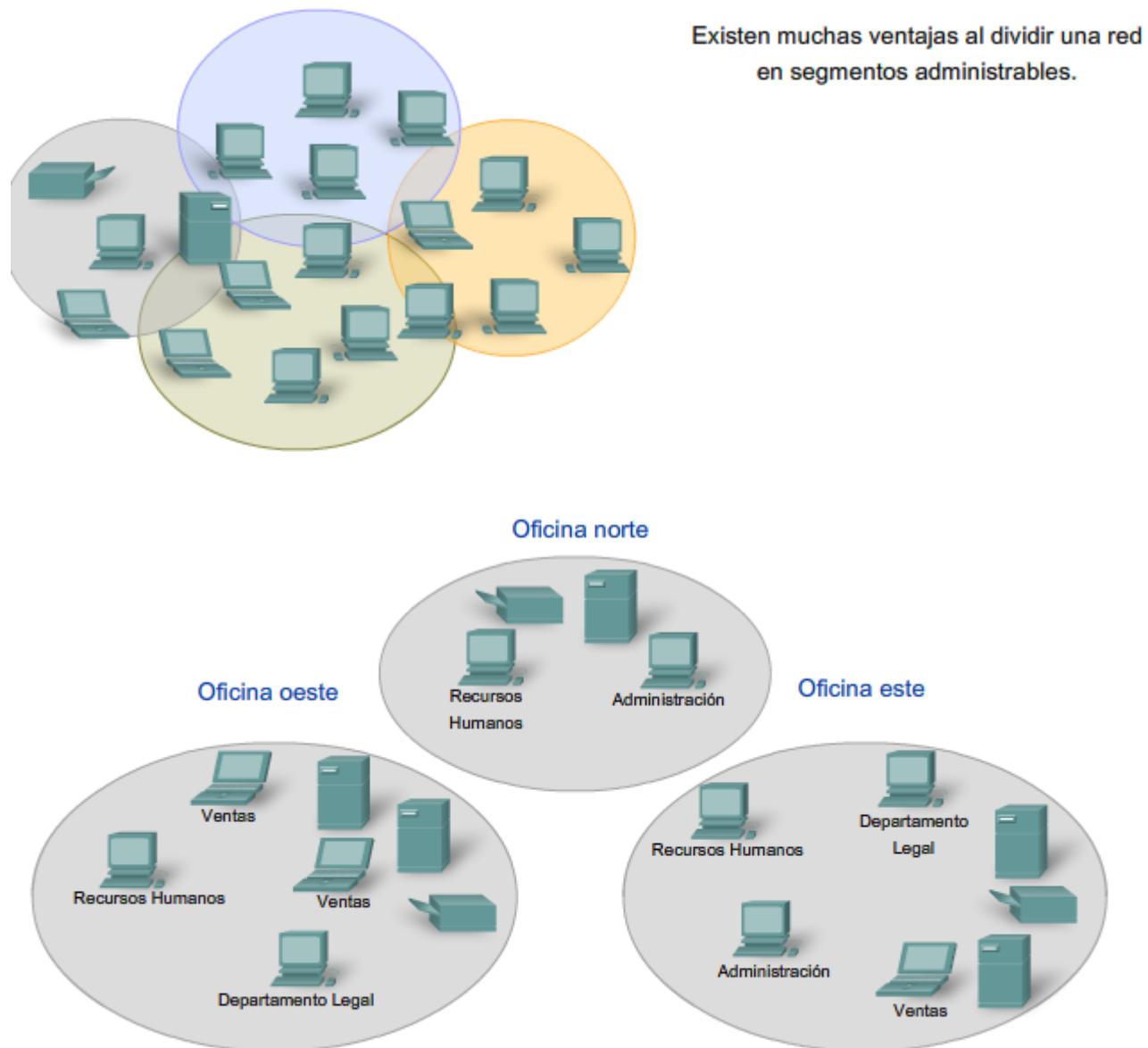
Agrupación de hosts para propiedad

Utilizar una base organizacional (compañía, departamento) para crear redes ayuda a controlar el acceso a los dispositivos y datos como también a la administración de las redes. En una red grande, es mucho más difícil definir y limitar la responsabilidad para el personal de la red. Dividir hosts en redes separadas provee un límite de cumplimiento y administración de seguridad de cada red.

Haga clic en el botón PROPIEDAD en la figura.

Enlaces:

Diseño de red <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm>



El simple hecho de conectar por cables la red física puede convertir la ubicación geográfica en un lugar lógico para realizar el inicio de la segmentación de una red.

INICIAR

GEOGRÁFICO

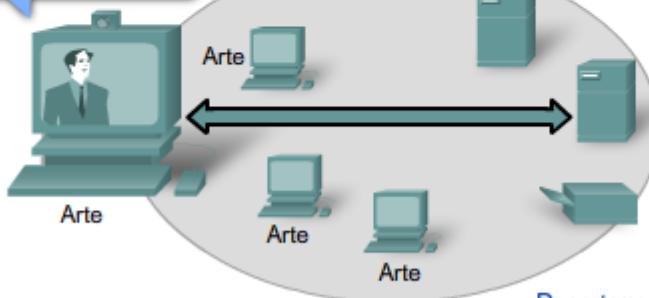
PROPÓSITO

PROPIEDAD

El volumen y el tipo de datos generados por una clase de usuarios pueden hacer que sea adecuada la agrupación de usuarios similares en una red.

Los vendedores necesitan el 100% de confiabilidad y velocidad.

Los artistas necesitan un ancho de banda elevado para crear videos.



Oficina de ventas

Departamento de arte

INICIAR

GEOGRÁFICO

PROpósito

PROPIEDAD

La agrupación de hosts en redes según la propiedad puede mejorar la seguridad de los datos.

Somos "propietarios" de estos servidores.

Quiero sus archivos.



¡DETENER!

Sin ingreso público

Ingrese con autorización



Registros corporativos

Somos "propietarios" de estos servidores.

Sitio Web público

INICIAR

GEOGRÁFICO

PROpósito

PROPIEDAD

5.2.2 ¿Por qué separar host en redes? – Rendimiento

Como se mencionó anteriormente, a medida que las redes crecen, presentan problemas que pueden reducirse al menos parcialmente dividiendo la red en redes interconectadas más pequeñas.

Los problemas comunes con las redes grandes son:

- Degradación de rendimiento
- Temas de seguridad
- Administración de direcciones

Mejoramiento del rendimiento

Grandes números de hosts conectados a una sola red pueden producir volúmenes de tráfico de datos que pueden extender, si no saturan, los recursos de red como la capacidad de ancho de banda y enrutamiento.

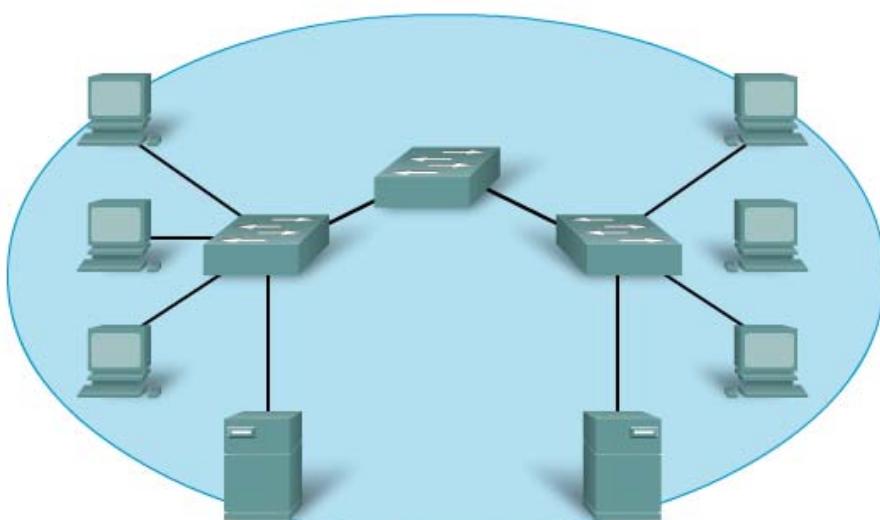
La división de grandes redes para que los host que necesitan comunicarse estén agrupados reduce el tráfico a través de los internetworks.

Además de las comunicaciones de datos reales entre los hosts, la administración de la red y el tráfico de control (sobrecarga) también aumentan con la cantidad de hosts. Los factores que contribuyen de manera significativa con esta sobrecarga pueden ser los broadcasts de redes.

Un broadcast es un mensaje desde un host hacia todos los otros hosts en la red. Comúnmente, un host inicia un broadcast cuando se requiere información sobre otro host desconocido. Los broadcasts son una herramienta necesaria y útil utilizada por protocolos para permitir la comunicación de datos en redes. Sin embargo, grandes cantidades de hosts generan grandes cantidades de broadcasts que consumen el ancho de banda de la red. Y como los otros hosts tienen que procesar el paquete de broadcast que reciben, las otras funciones productivas que un host realiza son también interrumpidas o degradadas.

Los broadcasts están contenidos dentro de una red. En este contexto, a una red también se la conoce como un dominio de broadcast. La administración del tamaño de los dominios broadcast dividiendo una red en subredes asegura que el rendimiento de la red y de los host no se degraden hasta niveles inaceptables.

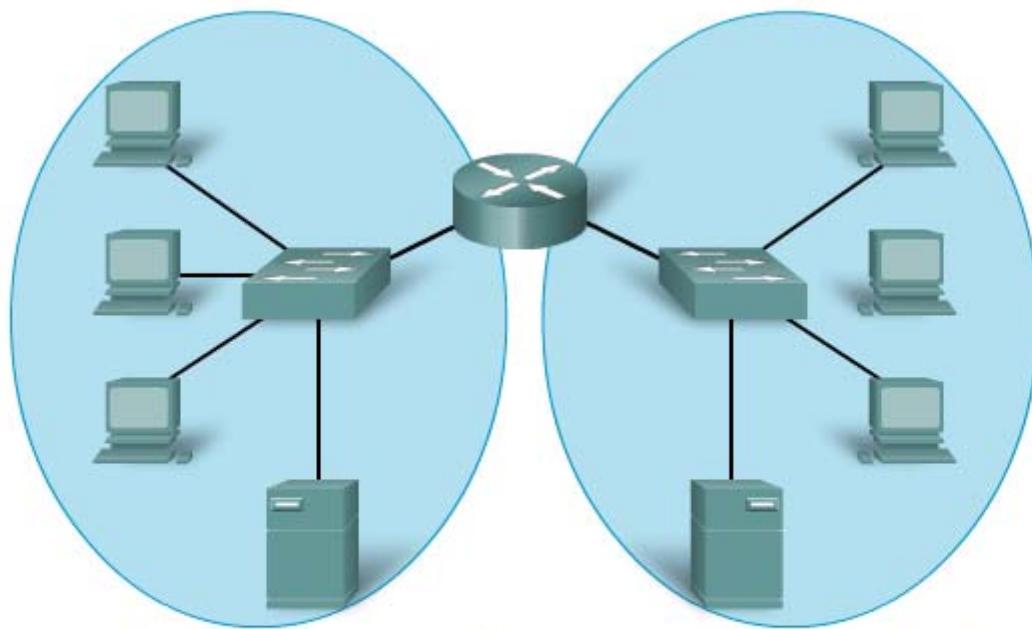
Coloque el cursor sobre Optimizar agrupamiento en la figura para ver cómo aumenta el rendimiento.



Todos los dispositivos de esta red se conectan en un dominio de broadcast cuando se establece el switch según la configuración predeterminada de fábrica. Debido a que los switches reenvían broadcasts en forma predeterminada, todos los dispositivos de esta red procesan los broadcasts.

Comenzar

Optimizar agrupación



El reemplazo del switch central por un router crea 2 subredes IP; por lo tanto, 2 dominios de broadcast diferentes. Todos los dispositivos están conectados pero se incluyen los broadcasts locales.

[Comenzar](#)

[Optimizar agrupación](#)

5.2.3 ¿Por qué separar hosts en redes? – Seguridad

La red basada en IP, que luego se convirtió en Internet, antiguamente tenía un pequeño número de usuarios confiables en agencias gubernamentales de EE.UU. y las organizaciones de investigación por ellas patrocinadas. En esta pequeña comunidad, la seguridad no era un problema importante.

La situación ha cambiado porque las personas, las empresas y las organizaciones han desarrollado sus propias redes IP que se conectan a Internet. Los dispositivos, servicios, comunicaciones y datos son propiedad de esos dueños de redes. Los dispositivos de red de otras compañías y organizaciones no necesitan conectarse a su red.

La división de redes basada en la propiedad significa que el acceso a y desde los recursos externos de cada red pueden estar prohibidos, permitidos o monitoreados.

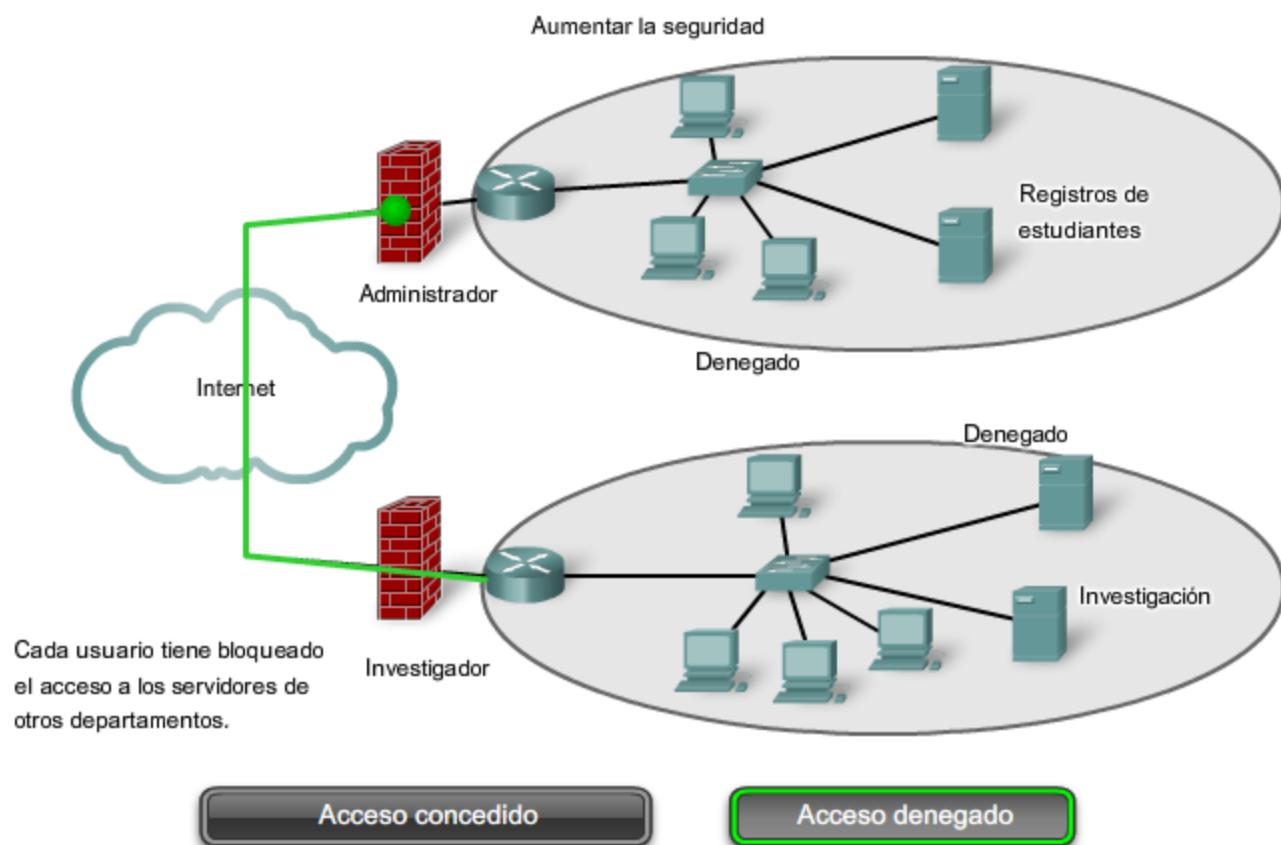
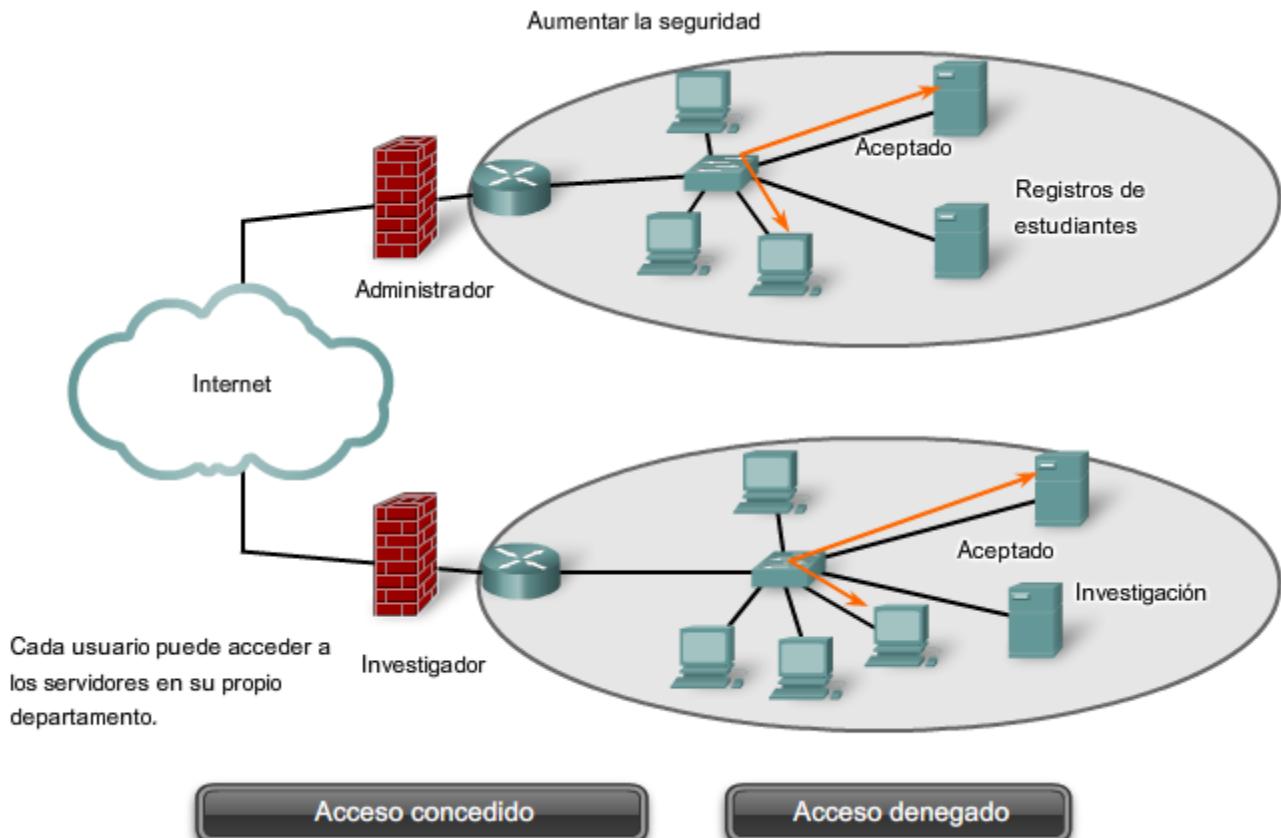
Coloque el cursor sobre los botones de Acceso otorgado y Acceso denegado en la figura para ver los diferentes niveles de seguridad.

El acceso a internetwork dentro de una compañía u organización puede estar asegurado de manera similar. Por ejemplo, la red de una universidad puede dividirse en subredes para la administración, investigación y los estudiantes. Dividir una red basada en el acceso a usuarios es un medio para asegurar las comunicaciones y los datos del acceso no autorizado, ya sea por usuarios dentro de la organización o fuera de ella.

La seguridad entre redes es implementada en un dispositivo intermediario (router o firewall) en el perímetro de la red. La función del firewall realizada por este dispositivo permite que datos conocidos y confiables accedan a la red.

Enlaces:

[Seguridad IP de red](#)

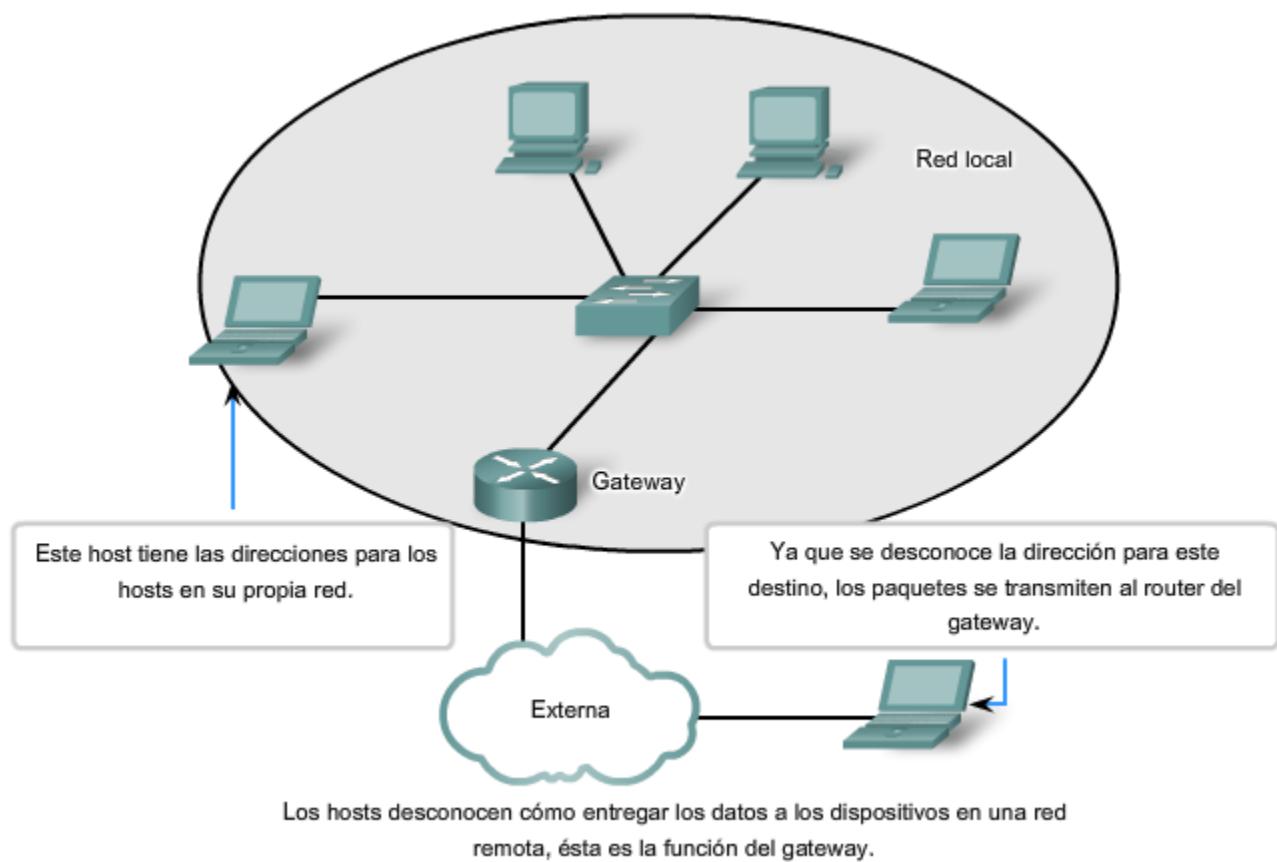


5.2.4 ¿Por qué separar hosts en redes? – Administración de direcciones

Internet está compuesta por millones de hosts y cada uno está identificado por su dirección única de capa de red. Esperar que cada host conozca la dirección de cada uno de los otros hosts sería imponer una carga de procesamiento sobre estos dispositivos de red que degradarían gravemente su rendimiento.

Dividir grandes redes para que estén agrupados los hosts que necesitan comunicarse, reduce la carga innecesaria de todos los hosts para conocer todas las direcciones.

Para todos los otros destinos, los hosts sólo necesitan conocer la dirección de un dispositivo intermediario al que envían paquetes para todas las otras direcciones de destino. Este dispositivo intermediario se denomina 162ersión. El 162ersión es un router en una red que sirve como una salida desde esa red.



5.2.5 ¿Por qué separar hosts en redes? – Direccionamiento Jerárquico

Para poder dividir redes, necesitamos el direccionamiento jerárquico. Una dirección jerárquica identifica cada host de manera exclusiva. También tiene niveles que ayudan a enviar paquetes a través de internetworks, lo que permite que una red sea dividida en base a esos niveles.

Para mantener las comunicaciones de datos entre redes por medio de internetworks, los esquemas de direccionamiento de capa de red son jerárquicos.

Como se ve en la figura, las direcciones postales son los principales ejemplos de direcciones jerárquicas.

Consideremos el caso de enviar una carta de Japón a un empleado que trabaja en Cisco Systems, Inc.

La carta estaría dirigida de la siguiente manera:

Nombre del empleado

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134

USA

Cuando una carta se envía por correo postal en el país de origen, la autoridad postal sólo observaría el país de destino y notaría que la carta está destinada para EE. UU. En este nivel, no se necesita ningún otro detalle de dirección.

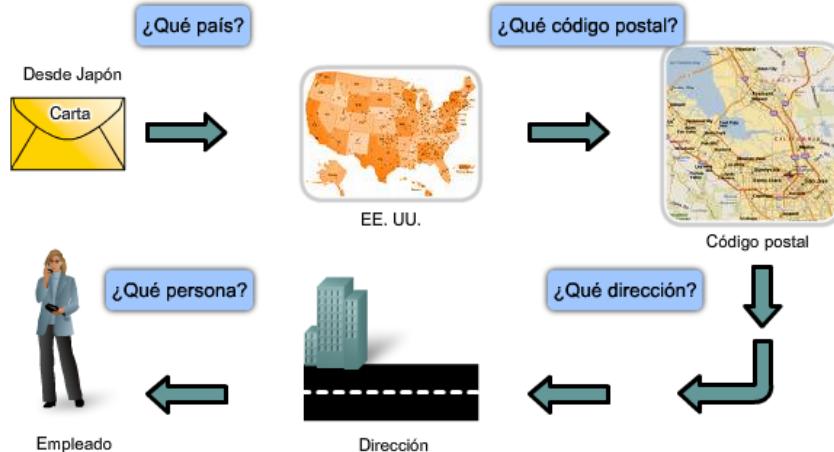
Cuando llega a EE.UU., la oficina postal primero observa el estado, California. La ciudad, calle, y nombre de la compañía no serían analizados si la carta todavía necesitara ser enviada al estado correcto. Una vez que la carta llega a California, será enviada a San Jose. Allí la portadora de correo local podría tomar la carta hacia West Tasman Drive y luego consultar la dirección y entregarla al 170. Cuando la carta esté realmente en las instalaciones de Cisco, se podría utilizar el nombre del empleado para enviarla a su último destino.

Con relación sólo al nivel de dirección relevante (país, estado, ciudad, calle, número y empleado) en cada etapa al dirigir la carta hacia el próximo salto hace que este proceso sea muy eficiente. No existe la necesidad de que cada paso en el envío conozca la ubicación exacta del destino; la carta fue dirigida a la dirección general hasta que el nombre del empleado fue finalmente utilizado en el destino.

Las direcciones jerárquicas de la red funcionan de manera muy similar. Las direcciones de la Capa 3 suministran la porción de la red de la dirección. Los routers envían paquetes entre redes refiriéndose sólo a la parte de la dirección de la capa de Red que se requiere para enviar el paquete hacia la red de destino. Para cuando llega el paquete a la red del host de destino, la dirección de destino completa del host habrá sido utilizada para entregar el paquete.

Si una red grande necesita ser dividida en redes más pequeñas, se pueden crear capas de direccionamiento adicionales. Usar el esquema de direccionamiento jerárquico significa que pueden conservarse los niveles más altos de la dirección (similar al país en una dirección postal), con el nivel medio denotando las direcciones de la red (estado o ciudad) y el nivel más bajo, los hosts individuales.

Dirección jerárquico
PARA: Jane Doe 170 West Tasman Drive, San Jose, CA 95134, USA



En cada paso de la entrega, la oficina de correos sólo necesita examinar el siguiente nivel jerárquico

5.2.6 División de redes: redes a partir de redes

Si se tiene que dividir una red grande, se pueden crear capas de direccionamiento adicionales. Usar direccionamiento jerárquico significa que se conservan los niveles más altos de la dirección; con un nivel de subred y luego el nivel de host.

La dirección lógica Ipv4 de 32 bits es jerárquica y está constituida por dos partes. La primera parte identifica la red y la segunda parte identifica al host en esa red. Se requiere de las dos partes para completar una dirección IP.

Por comodidad, las direcciones Ipv4 se dividen en cuatro grupos de ocho bits (octetos). Cada uno se convierte a su valor decimal y la dirección completa escrita como los cuatro valores decimales separados por punto (punto).

Por ejemplo: 192.168.18.57

En este ejemplo, como muestra la figura, los tres primeros octetos, (192.168.18) pueden identificar la porción de la red de la dirección, y el último octeto (57) identifica al host.

Esto es direccionamiento jerárquico porque la porción de la red indica a la red donde se ubica cada dirección de host única. Los routers sólo necesitan conocer cómo llegar a cada red en lugar de conocer la ubicación de cada host individual.

Con el direccionamiento jerárquico de Ipv4, la porción de la red de la dirección para todos los hosts en una red es la misma. Para dividir una red, la porción de la red de la dirección es extendida para usar bits desde la porción del host de la dirección. Estos bits de host pedidos prestados luego se usan como bits de red para representar las diferentes subredes dentro de un rango de red original.

Dado que una dirección Ipv4 es de 32 bits, cuando los bits del host se usan para dividir una red, cuanto más subredes se crean, menos hosts pueden utilizarse para cada subred. Sin considerar el número de subredes creadas, se requiere que cada uno de los 32 bits identifique un host individual.

Al número de bits de una dirección utilizada como porción de red se lo denomina longitud del prefijo. Por ejemplo, si una red usa 24 bits para expresar la porción de red de una dirección, se dice que el prefijo es /24. En los dispositivos de una red Ipv4, un número separado de 32 bits llamado máscara de subred indica el prefijo.

Nota: El Capítulo 6 en este curso cubrirá el direccionamiento y subdirecciónamiento Ipv4 de red en detalle.

La extensión de la longitud del prefijo o máscara de subred permite la creación de estas subredes. De esta manera, los administradores de red tienen la flexibilidad de dividir redes para satisfacer las diferentes necesidades, como ubicación, administración del rendimiento de la red y seguridad, mientras asegura que cada host tenga una dirección única.

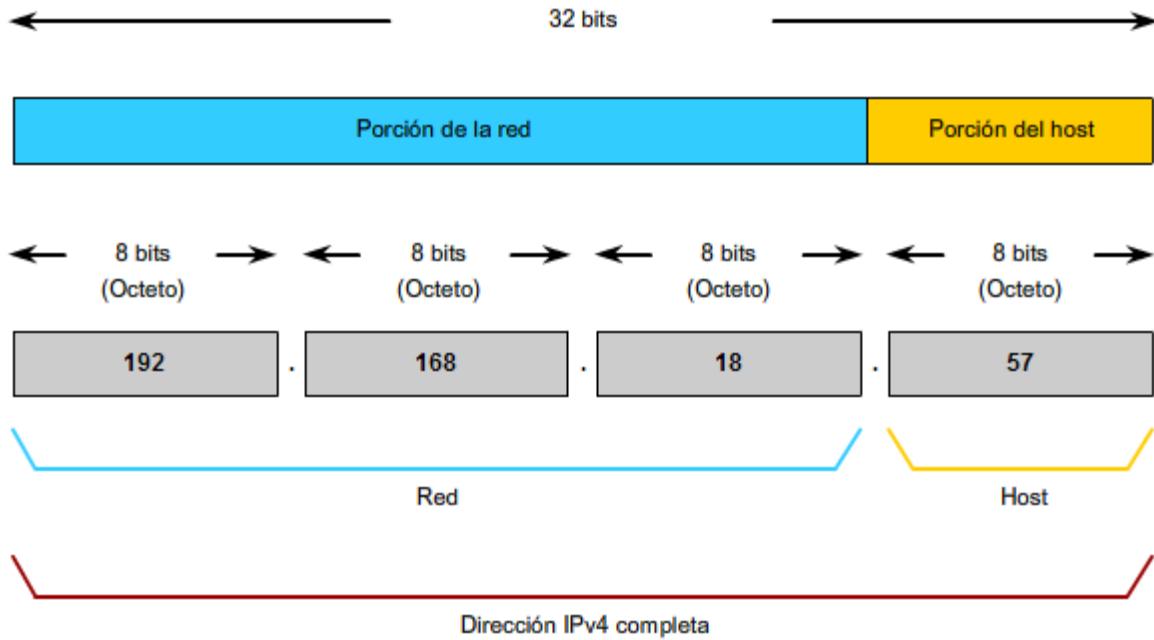
Para propósitos explicativos, en este capítulo, los primeros 24 bits de una dirección Ipv4 se utilizarán como porción de red.

Enlaces:

Agencia de asignación de números por Internet

<http://www.iana.org/>

Dirección IPv4 jerárquica



5.3 Enrutamiento: Cómo se manejan nuestros paquetes de datos

5.3.1 Parámetros de dispositivos: Cómo respaldar la comunicación fuera de nuestra red

Dentro de una red o subred, los hosts se comunican entre sí sin necesidad de un dispositivo intermediario de capa de red. Cuando un host necesita comunicarse con otra red, un dispositivo intermediario o router actúa como un enlace de red hacia la otra red.

Como parte de su configuración, un host tiene una dirección de enlace de red por defecto definida. Como se muestra en la figura, esta dirección de enlace de red es la dirección de una interfaz de router que está conectada a la misma red que el host.

Tenga en cuenta que no es factible para un host particular conocer la dirección de todos los dispositivos en Internet con los cuales puede tener que comunicarse. Para comunicarse con un dispositivo en otra red, un host usa la dirección de este enlace de red, o enlace de red por defecto, para enviar un paquete fuera de la red local.

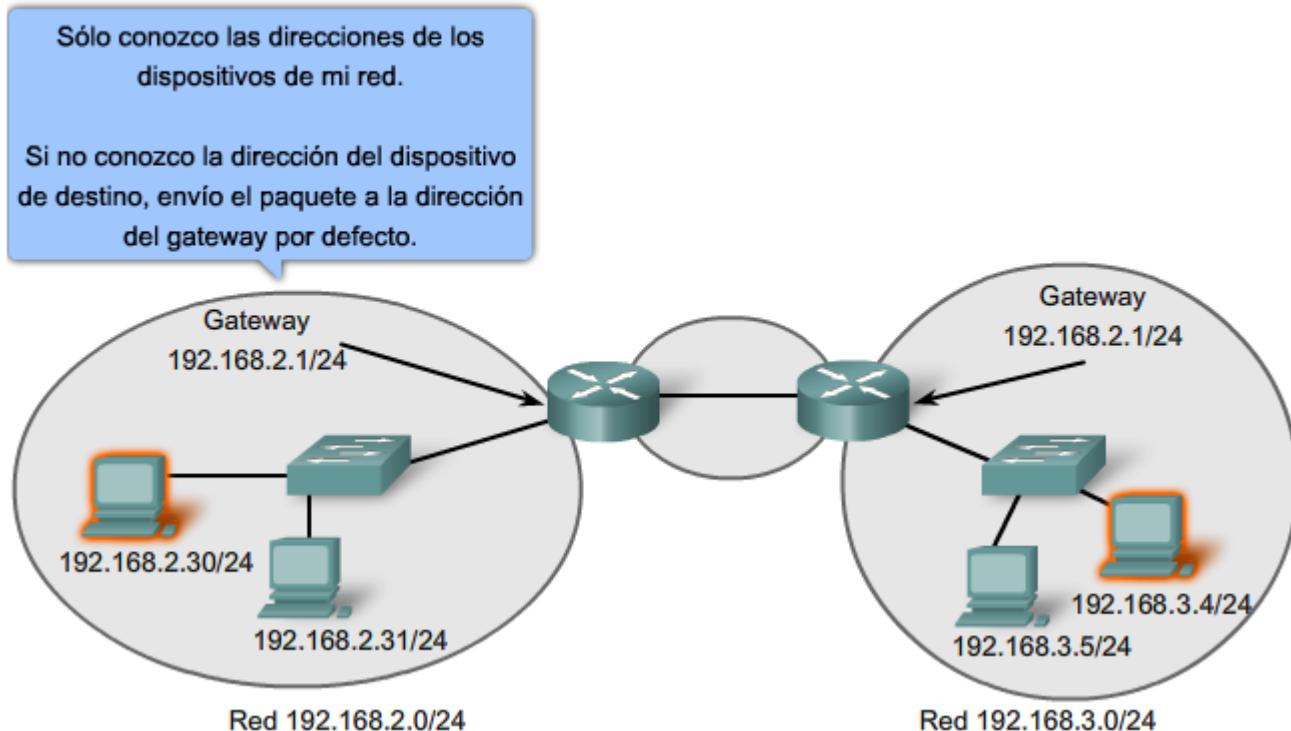
El router también necesita una ruta que defina dónde enviar luego el paquete. A esto se lo denomina dirección del siguiente salto. Si una ruta está disponible al router, el router enviará el paquete al router del próximo salto que ofrece una ruta a la red de destino.

Enlaces;

RFC 823

<http://www.ietf.org/rfc/rfc0823.txt>

Los gateways permiten las comunicaciones entre redes



5.3.2 Paquetes IP: Cómo llevar datos de extremo a extremo

Como ya sabe, la función de la capa de Red es transferir datos desde el host que origina los datos hacia el host que los usa. Durante la encapsulación en el host origen, un paquete IP se construye en la Capa 3 para transportar el PDU de la Capa 4. 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 puede llevar una PDU de la capa de Transporte a través de muchas redes y muchos routers. Si es así, la información que contiene no está alterada por ningún router cuando se toman las decisiones de envío.

En cada salto, las decisiones de envío están basadas en la información del encabezado del paquete IP. El paquete con su encapsulación de capa de Red también se mantiene básicamente intacto a través de todo el proceso desde el host de origen hasta el host de destino.

Si la comunicación se produce entre dos hosts de diferentes redes, la red local envía el paquete desde el origen hasta su router de conexión. El router examina la porción de la red de la dirección de destino del paquete y envía el paquete a la interfaz adecuada. Si la red de destino está conectada directamente a este router, el paquete es enviado directamente a ese host. Si la red de destino no está conectada directamente, el paquete es enviado a un segundo router, que es el router del siguiente salto.

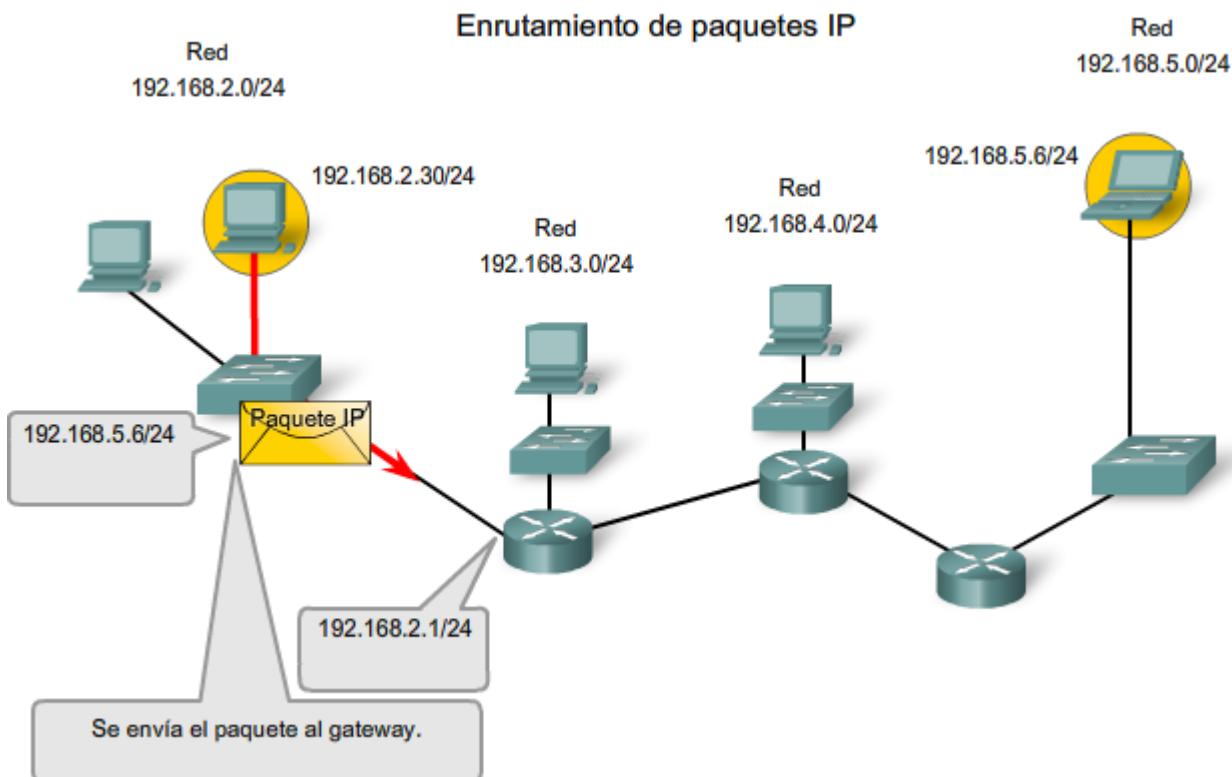
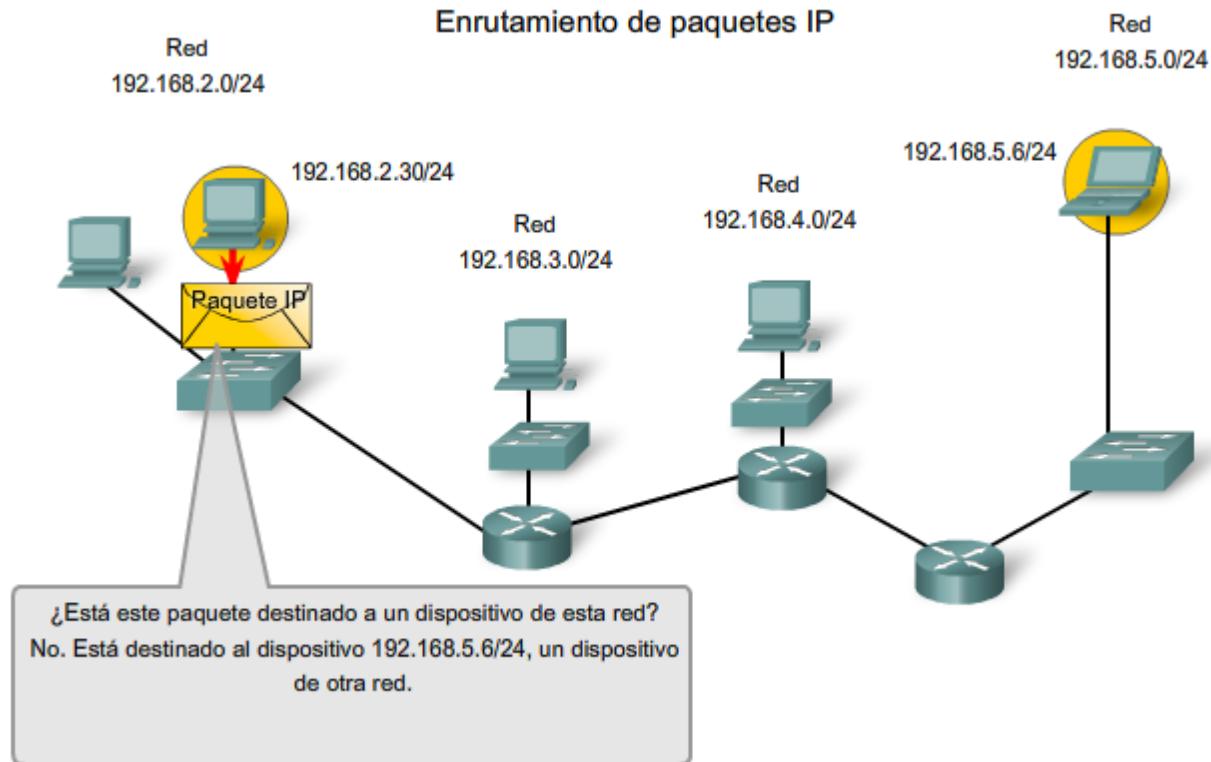
El paquete que se envía pasa a ser responsabilidad de este segundo router. Muchos routers o saltos a lo largo del camino pueden procesar el paquete antes de llegar a destino.

Haga clic en los pasos de la figura para seguir la ruta del paquete IP.

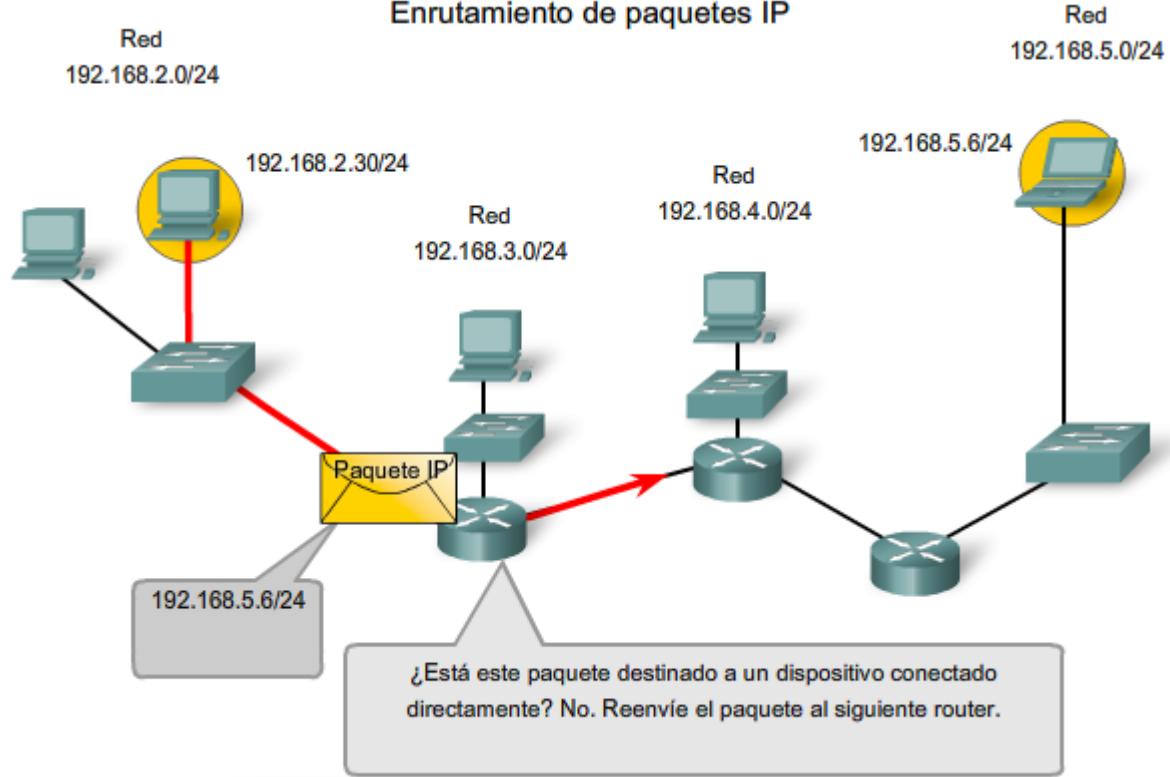
Enlaces:

RFC 791 <http://www.ietf.org/rfc/rfc0791.txt>

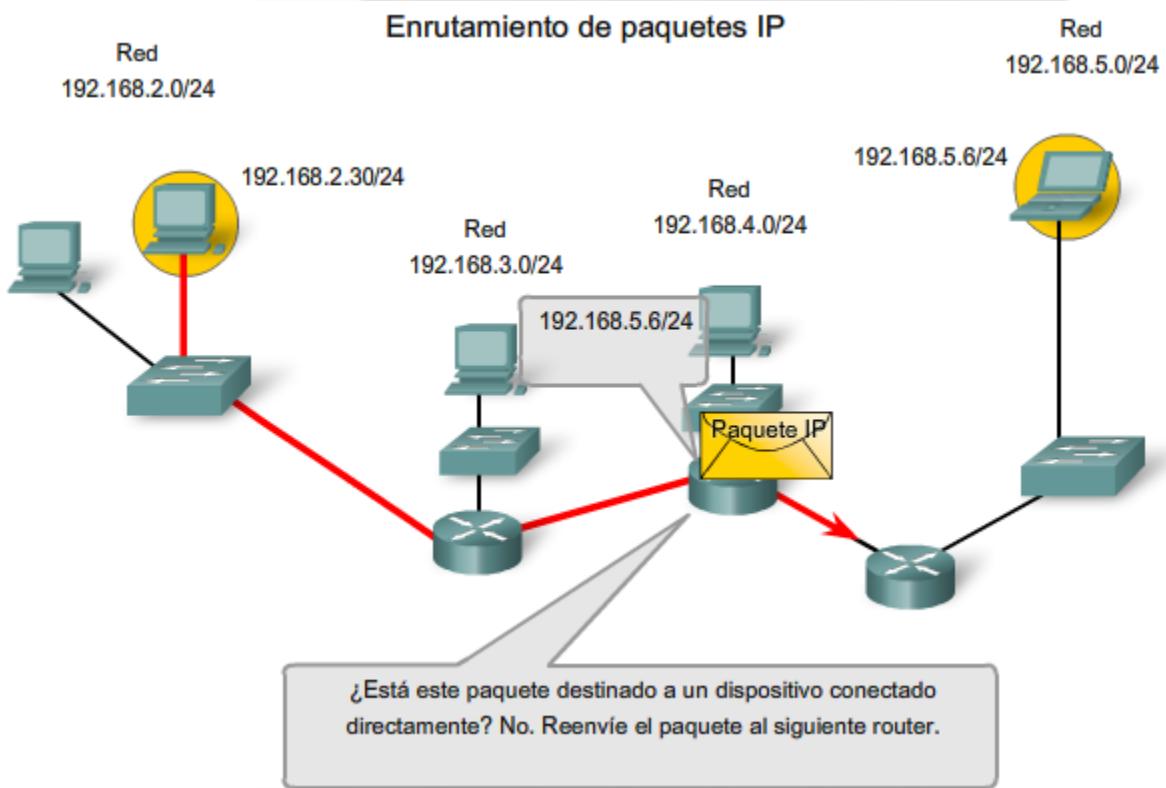
RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

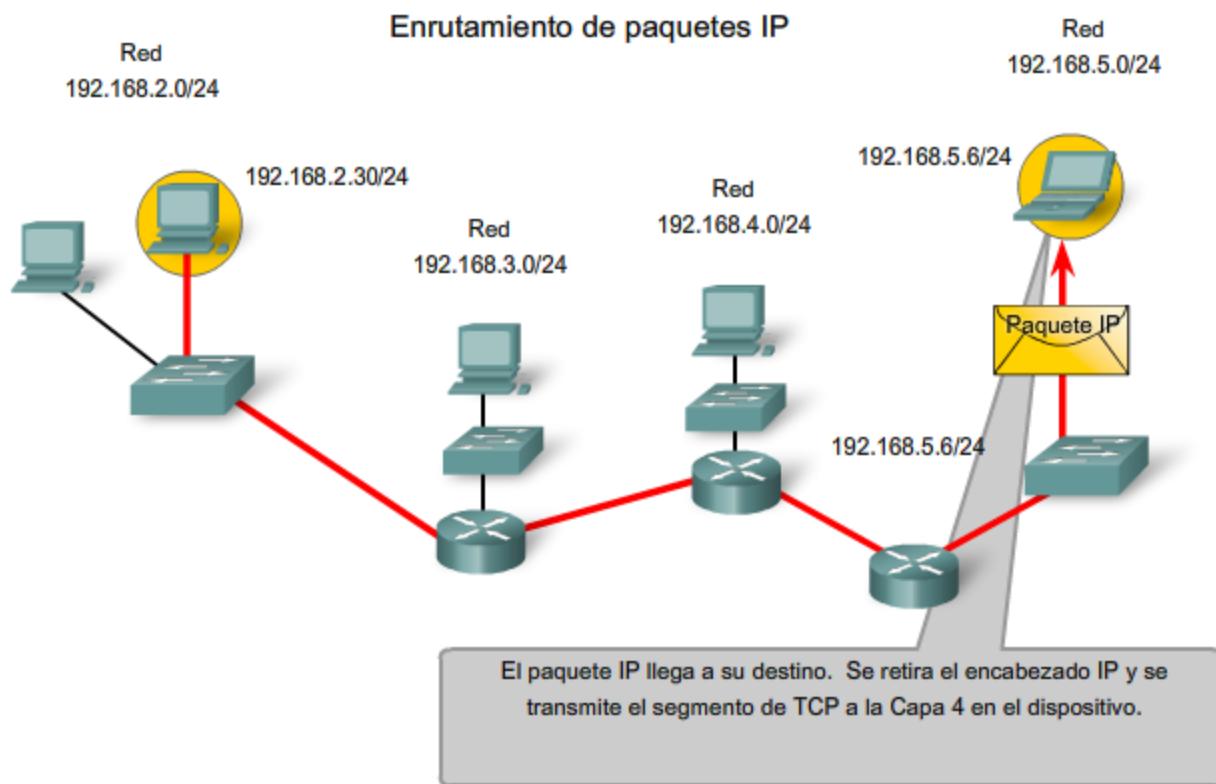
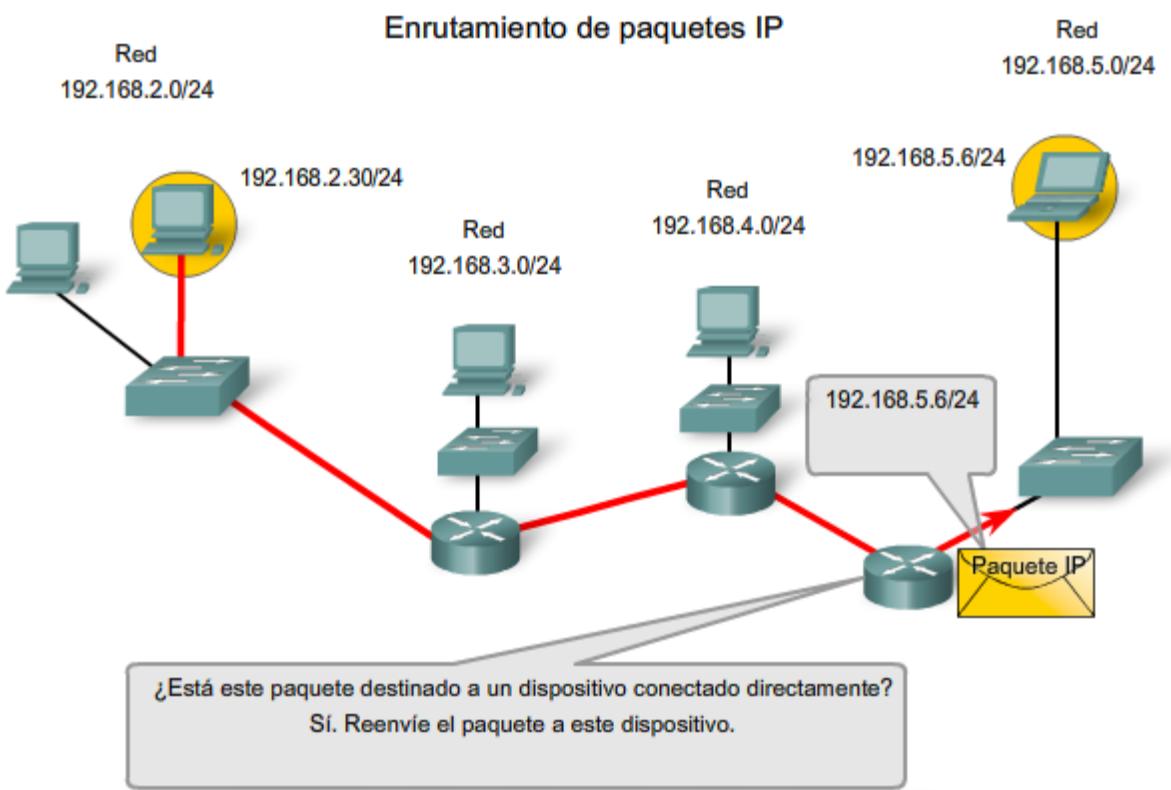


Enrutamiento de paquetes IP



Enrutamiento de paquetes IP





5.3.3 Gateway: La salida de nuestra red

El 169ersión, también conocido como 169ersión por defecto, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host de origen, el paquete tiene que hallar la salida fuera de la red original. Para esto, el paquete es enviado al 169ersión. Este 169ersión es una interfaz del

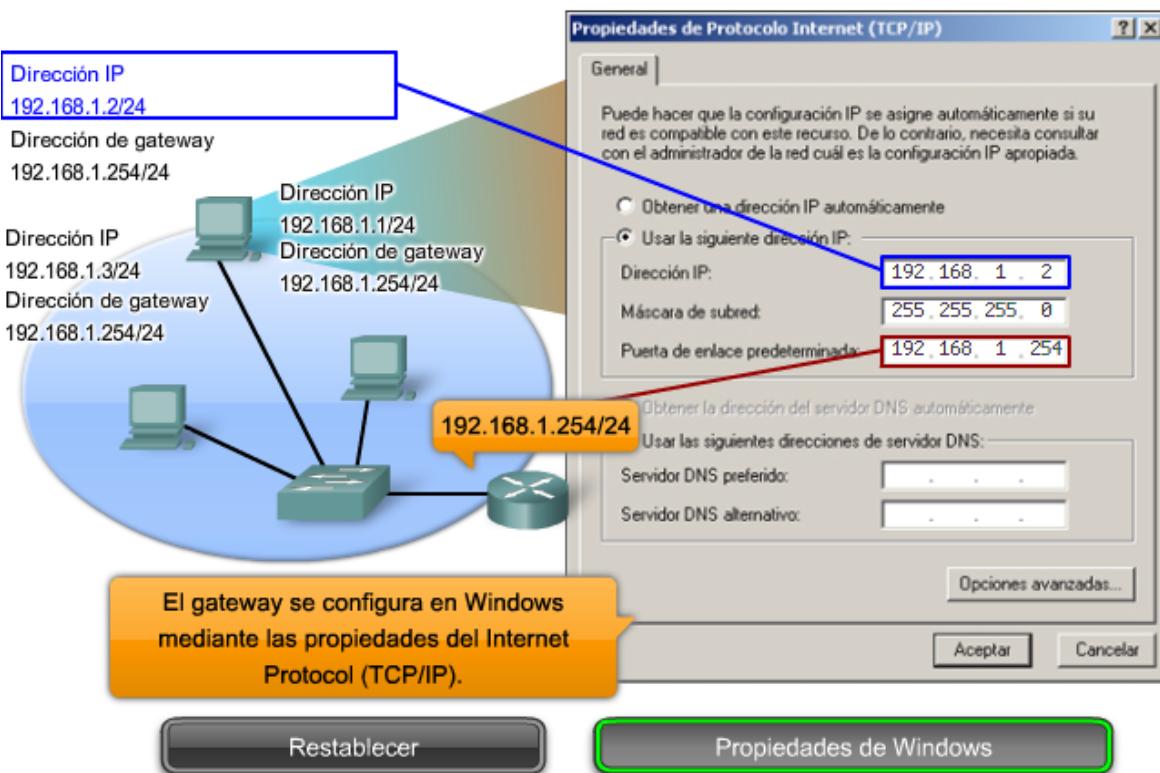
router conectada a la red local. La interfaz del 170ersión tiene una dirección de capa de Red que concuerda con la dirección de red de los hosts. Los hosts están configurados para reconocer que la dirección es un 170ersión.

Gateway por defecto

El 170ersión por defecto está configurado en el host. En una computadora con Windows, se usan las herramientas de las Propiedades del Protocolo de Internet (TCP/IP) para ingresar la dirección Ipv4 del 170ersión por defecto. Tanto la dirección Ipv4 de host como la dirección de 170ersión deben tener la misma porción de red (y subred si se utiliza) de sus respectivas direcciones.

Haga clic sobre el gráfico para ver las Propiedades de Windows.

Configuración de la 170ersión del host <http://www.microsoft.com/technet/community/columns/cableguy/cg0903.mspx>



Confirmación del gateway y la ruta

Como muestra la figura, la dirección IP desde el 170ersión por defecto de un host se puede ver introduciendo los comandos ipconfig o route en la línea de comandos de un computadora con Windows. El comando de ruta también se usa en un host Linux o UNIX.

```
C:\>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
Connection-specific DNS Suffix . :  
① IP Address . . . . . : 192.168.1.2  
② Subnet Mask . . . . . : 255.255.255.0  
③ Default Gateway . . . . . : 192.168.1.254
```

Ningún paquete puede ser enviado sin una ruta. Si el paquete se origina en un host o se reenvía por un dispositivo intermediario, el dispositivo debe tener una ruta para identificar dónde enviar el paquete.

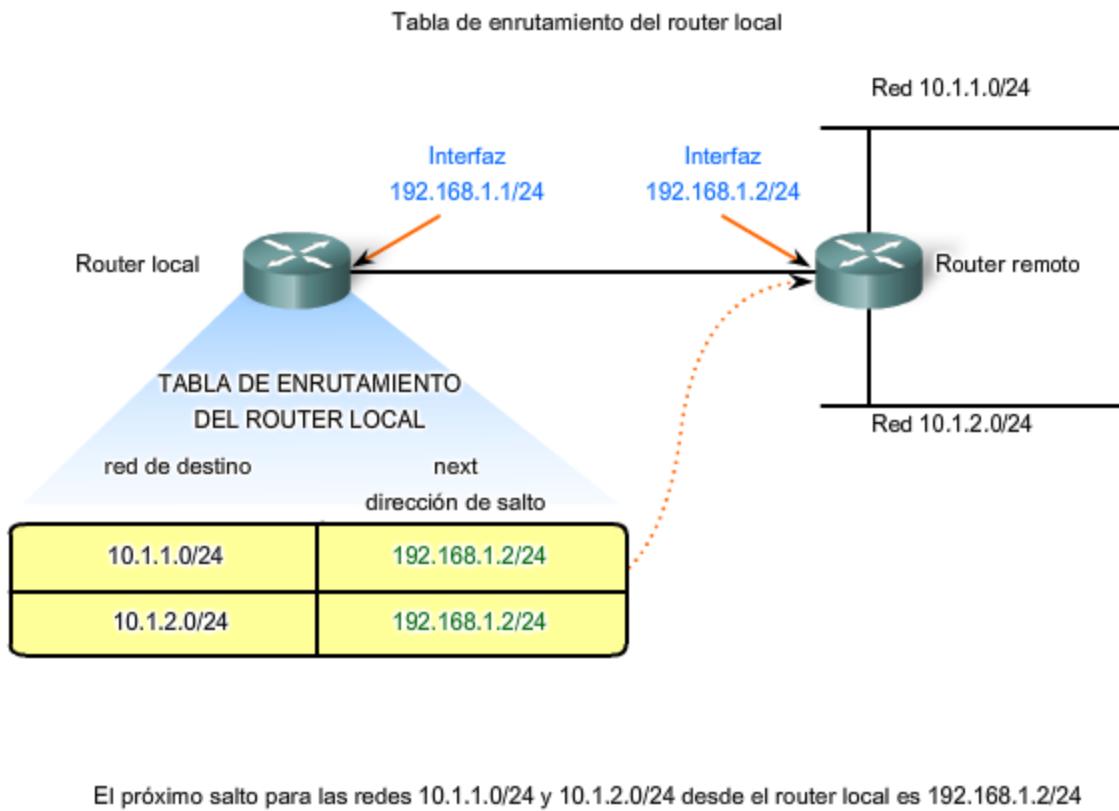
Un host debe reenviar el paquete ya sea al host en la red local o al 171ersión, según sea lo adecuado. Para reenviar los paquetes, el host debe tener rutas que representan estos destinos.

Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del 171ersión. Este proceso de reenvío es denominado enrutamiento. Para reenviar un paquete a una red de destino, el router requiere una ruta hacia esa red. Si una ruta a una red de destino no existe, el paquete no puede reenviarse.

La red de destino puede ser un número de routers o saltos fuera del 171ersión. La ruta hacia esa red sólo indicaría el router del siguiente salto al cual el paquete debe reenviarse, no el router final. El proceso de enrutamiento usa una ruta para asignar una dirección de red de destino hacia el próximo salto y luego envía el paquete hacia esta dirección del próximo salto.

Enlaces:

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>



5.3.4 Ruta: el camino hacia una red

Una ruta para paquetes para destinos remotos se agrega usando la dirección de 171ersión por defecto como el siguiente salto. Aunque usualmente no se hace, un host puede tener también rutas agregadas manualmente a través de configuraciones.

Al igual que los dispositivos finales, los routers también agregan rutas para las redes conectadas a su tabla de enrutamiento. Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz se vuelve parte de esa red. La tabla de enrutamiento ahora incluye esa red como red directamente conectada. Todas las

otras rutas, sin embargo, deben ser configuradas o adquiridas por medio del protocolo de enrutamiento. Para reenviar un paquete, el router debe saber dónde enviarlo. Esta información está disponible como rutas en una tabla de enrutamiento.

La tabla de enrutamiento almacena la información sobre las redes conectadas y remotas. Las redes conectadas están directamente adjuntas a una de las interfaces del router. Estas interfaces son los gateways para los hosts en las diferentes redes locales. Las redes remotas son redes que no están conectadas directamente al router. Las rutas a esas redes se pueden configurar manualmente en el router por el administrador de red o aprendidas automáticamente utilizando protocolos de enrutamiento dinámico.

Los routers en una tabla de enrutamiento tienen tres características principales:

- red de destino,
- próximo salto, y
- métrica.

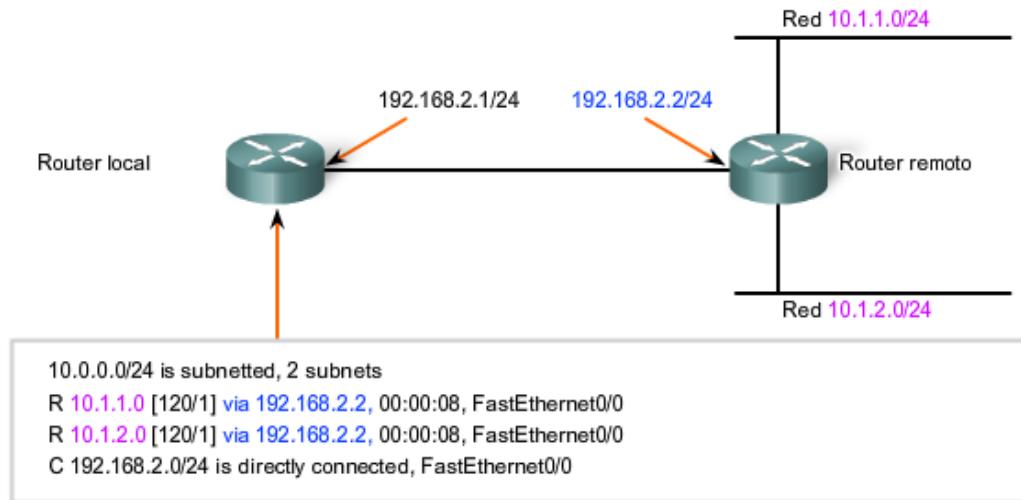
El router combina la dirección de destino en el encabezado del paquete con la red de destino de una ruta en la tabla de enrutamiento y envía el paquete al router del próximo salto especificado por esa ruta. Si hay dos o más rutas posibles hacia el mismo destino, se utiliza la métrica para decidir qué ruta aparece en la tabla de enrutamiento.

Como se muestra en la figura, la tabla de enrutamiento en un router Cisco puede ser analizada con el comando `show ip route`.

Nota: El proceso de enrutamiento y el rol de la métrica son tema de un curso posterior y se abarcará en detalle más adelante.

Como sabemos, los paquetes no pueden reenviarse por el router sin una ruta. Si una ruta que representa la red de destino no está en la tabla de enrutamiento, el paquete será descartado (es decir, no se reenviará). La ruta encontrada puede ser una ruta conectada o una ruta hacia una red remota. El router también puede usar una ruta por defecto para enviar el paquete. La ruta default se usa cuando la ruta de destino no está representada por ninguna otra ruta en la tabla de enrutamiento.

Confirmación de la ruta y el gateway



Este es el resultado de la tabla de enrutamiento del router local cuando se emite "show ip route".

El próximo salto para las redes 10.1.1.0/24 y 10.1.2.0/24 desde el router local es 192.168.2.2.

Tabla de enrutamiento de host

Un host crea las rutas usadas para reenviar los paquetes que origina. Estas rutas derivan de la red conectada y de la configuración del 173ersión por defecto.

Los hosts agregan automáticamente todas las redes conectadas a las rutas. Estas rutas para las redes locales permiten a los paquetes ser entregados a los hosts que están conectados a esas redes.

Los hosts también requieren una tabla de enrutamiento para asegurarse de que los paquetes de la capa de Red estén dirigidos a la red de destino correcta. A diferencia de la tabla de enrutamiento en un router, que contiene tanto rutas locales como remotas, la tabla local del host comúnmente contiene su conexión o conexiones directa(s) a la red y su propia ruta por defecto al 173ersión. La configuración de la dirección de 173ersión por defecto en el host crea la ruta default local.

Como muestra la figura, la tabla de enrutamiento de un host de computadora puede ser analizada en la línea de comando introduciendo los comandos netstat -r, route, o route PRINT.

En algunos casos, puede necesitar indicar rutas más específicas desde un host. Puede utilizar las siguientes opciones para el comando de ruta para modificar el contenido de la tabla de enrutamiento:

route ADD

route DELETE

route CHANGE

Enlaces:

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

5.3.5 Red de destino

Entradas en la tabla de enrutamiento

La red de destino que aparece en la entrada de la tabla de enrutamiento, llamada ruta, representa un rango de direcciones de hosts y, algunas veces, un rango de direcciones de red y de host.

La naturaleza jerárquica del direccionamiento de la Capa 3 significa que una entrada de ruta podría referirse a una red general grande y otra entrada podría referirse a una subred de la misma red. Cuando se reenvía un paquete, el router seleccionará la ruta más específica.

Volviendo a nuestro primer ejemplo de dirección postal, consideremos enviar la misma carta de Japón a 170 West Tasman Drive San Jose, California USA. ¿Qué dirección usaría? "USA" o "San Jose California USA" o "West Tasman Drive San Jose, California USA" o "170 West Tasman Drive San Jose, California USA"

Se usaría la cuarta y más específica dirección. Sin embargo, para otra carta donde el número de la calle es desconocido, la tercera opción suministraría la mejor coincidencia de dirección.

De la misma forma, un paquete destinado a la subred de una red más grande sería enrutado usando la ruta a la subred. No obstante, un paquete direccionado a una subred diferente dentro de la misma red más grande sería enrutado usando la entrada más general.

Como se muestra en la figura, si un paquete llega a un router con una dirección de destino de 10.1.1.55, el router reenvía el paquete al router del siguiente salto asociado con una ruta a la red 10.1.1.0. Si una ruta a 10.1.1.0 no está enumerada en el enrutamiento, pero está disponible una ruta a 10.1.0.0, el paquete se reenvía al router del siguiente salto para esa red.

Entonces, la prioridad de la selección de una ruta para el paquete que va a 10.1.1.55 sería:

1. 10.1.1.0
2. 10.1.0.0
3. 10.0.0.0
4. 0.0.0.0 (ruta default si estuviera configurada)
5. Descartada

Entradas de ruta en una tabla de enrutamiento

```
10.0.0.0/24 is subnetted, 2 subnets
R 10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R 10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

La tabla de enrutamiento muestra las redes de destino.

Los paquetes con direcciones host de destino en uno de los rangos de red mostrados se harán coincidir con el próximo salto que conduce a dicha red.

Ruta default

Un router puede ser configurado para que tenga una ruta default. Una ruta default es una ruta que coincide con todas las redes de destino. En redes Ipv4 se usa la dirección 0.0.0.0 para este propósito. La ruta default se usa para enviar paquetes para los que no hay entrada en la tabla de enrutamiento para la red de destino. Los paquetes con una dirección de red de destino que no combinan con una ruta más específica en la tabla de enrutamiento son enviados al router del próximo salto asociados con la ruta por defecto.

Enlaces:

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

La tabla de enrutamiento muestra la ruta predeterminada 0.0.0.0.

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
  10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.2.2
```

Los paquetes con las direcciones hosts de destino que no se encuentren en los rangos de la red mostrados se reenviarán al gateway como último recurso.

5.3.6 Siguiente salto: Dónde se envía luego el paquete

Un siguiente salto es la dirección del dispositivo que procesará luego el paquete. Para un host en una red, la dirección de 175ersión por defecto (interfaz de router) es el siguiente salto para todos los paquetes destinados a otra red.

En la tabla de enrutamiento de un router, cada ruta enumera un siguiente salto para cada dirección de destino abarcada por la ruta. A medida que cada paquete llega al router, la dirección de la red de destino es analizada y comparada con las rutas en la tabla de enrutamiento. Cuando se determina una ruta coincidente, la dirección del siguiente salto para esa ruta se usa para enviar el paquete hacia ese destino. El router luego envía el paquete hacia la interfaz a la cual está conectado el router del siguiente salto. El router del siguiente salto es el 175ersión a las redes fuera del destino intermedio.

Las redes conectadas directamente a un router no tienen dirección del siguiente salto porque no existe un dispositivo de Capa 3 entre el router y esa red. El router puede reenviar paquetes directamente hacia la interfaz por esa red al host de destino.

Algunas rutas pueden tener múltiples siguientes saltos. Esto indica que existen múltiples pasos hacia la misma red de destino. Éstas son rutas alternativas que el router puede utilizar para reenviar paquetes.

Enlaces:

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

Resultado de la tabla de enrutamiento con los siguientes saltos

```
10.0.0.0/24 is subnetted, 2 subnets
R  10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R  10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C  192.168.1.0/24 is directly connected, FastEthernet0/0
```

5.3.7 Envío de paquetes: Traslado del paquete hacia su destino

El enrutamiento se hace paquete por paquete y salto por salto. Cada paquete es tratado de manera independiente en cada router a lo largo de la ruta. En cada salto, el router analiza la dirección IP de destino para cada paquete y luego controla la tabla de enrutamiento para reenviar información.

El router hará una de tres cosas con el paquete:

- Envíelo al router del próximo salto
- Envíelo al host de destino
- Descártelo

Examen del paquete

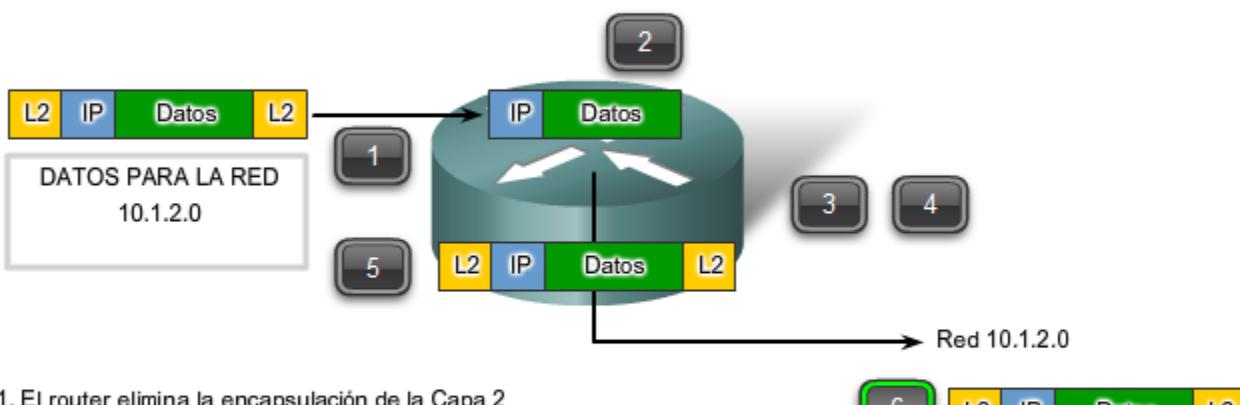
Como dispositivo intermediario, un router procesa el paquete en la Capa de red. No obstante, los paquetes que llegan a las interfaces del router están encapsulados como PDU (Capa 2) de la capa de Enlace de datos. Como muestra la figura, el router primero descarta la encapsulación de la Capa 2 para poder examinar el paquete.

Selección del siguiente salto

En el router, se analiza la dirección de destino en el encabezado del paquete. Si una ruta coincidente en la tabla de enrutamiento muestra que la red de destino está conectada directamente al router, el paquete es reenviado a la interfaz a la cual está conectada la red. En este caso, no existe siguiente salto. Para ubicarlo en la red conectada, el paquete primero debe ser reencapsulado por el protocolo de la Capa 2 y luego reenviado hacia la interfaz.

Si la ruta que coincide con la red de destino del paquete es una red remota, el paquete es reenviado a la interfaz indicada, encapsulado por el protocolo de la Capa 2 y enviado a la dirección del siguiente salto.

Existe una entrada de ruta



1. El router elimina la encapsulación de la Capa 2
2. El router extrae la dirección IP de destino
3. El router verifica la tabla de enrutamiento para detectar una coincidencia
4. Se encuentra la red 10.1.2.0 en la tabla de enrutamiento
5. El router vuelve a encapsular el paquete
6. Se envía el paquete a la red 10.1.2.0

Uso de una ruta default

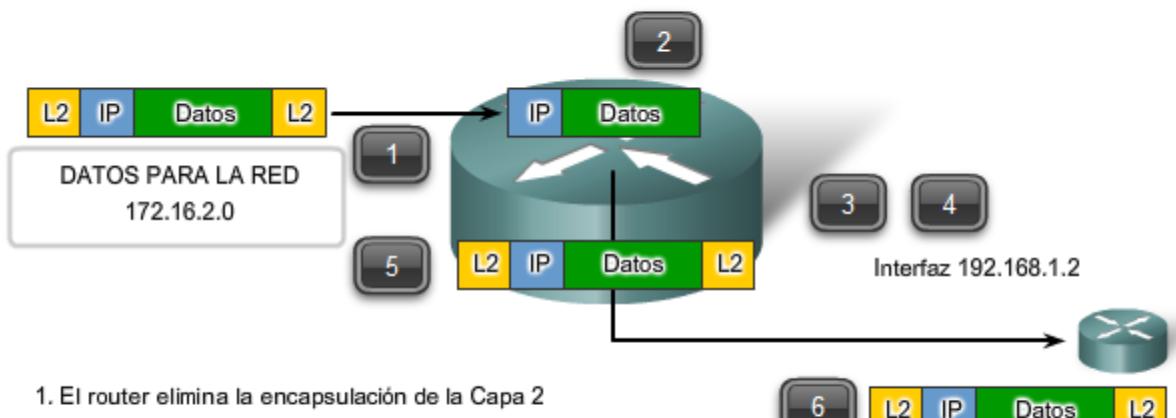
Como muestra la figura, si la tabla de enrutamiento no contiene una entrada de ruta más específica para un paquete que llega, el paquete se reenvía a la interfaz indicada por la ruta default, si la hubiere. En esta interfaz, el paquete es encapsulado por el protocolo de la Capa 2 y es enviado al router del siguiente salto. La ruta default es también conocida como Gateway de último recurso.

Este proceso puede producirse varias veces hasta que el paquete llega a su red de destino. El router en cada salto conoce sólo la dirección del siguiente salto; no conoce los detalles de la ruta hacia el host del destino remoto. Además, no todos los paquetes que van al mismo destino serán enviados hacia el mismo siguiente salto en cada router. Los routers a lo largo del trayecto pueden aprender nuevas rutas mientras se lleva a cabo la comunicación y reenvían luego los paquetes a diferentes siguientes saltos.

Las rutas default son importantes porque el router del 177ersión no siempre tiene una ruta a cada red posible en Internet. Si el paquete es reenviado usando una ruta default, eventualmente llegará a un router que tiene una ruta específica a la red de destino. Este router puede ser el router al cual esta red está conectada. En este caso, este router reenviará el paquete a través de la red local hacia el host de destino.

No existe una entrada de ruta pero sí una ruta predeterminada

Coloque el cursor para ver los pasos que lleva a cabo el router.



1. El router elimina la encapsulación de la Capa 2
2. El router extrae la dirección IP
3. El router verifica la tabla de enrutamiento para detectar una coincidencia
4. La red 172.16.2.0 no se encuentra en la tabla de enrutamiento pero la ruta por defecto a 192.168.1.2 existe
5. El router vuelve a encapsular el paquete
6. Se envía el paquete a la interfaz 192.168.1.2

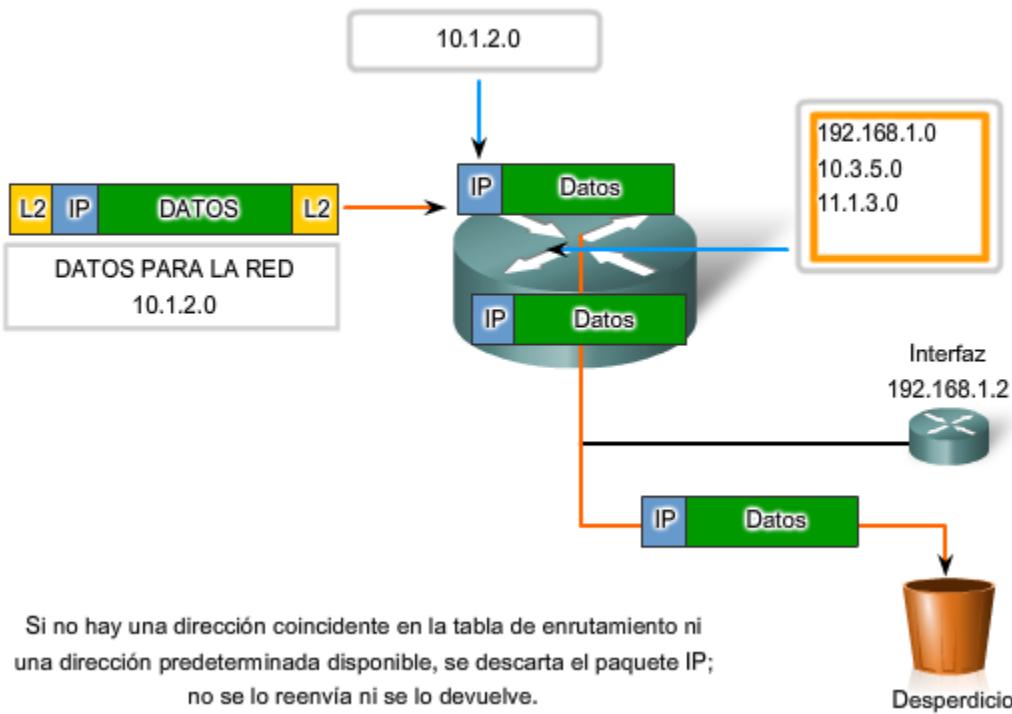
A medida que el paquete pasa a través de saltos en la internetwork, todos los routers necesitan una ruta para reenviar un paquete. Si, en cualquier router, no se encuentra una ruta para la red de destino en la tabla de enrutamiento y no existe una ruta default, ese paquete se descarta.

IP no tiene previsto devolver el paquete al router anterior si un router particular no tiene dónde enviar el paquete. Tal función va en detrimento de la eficiencia y baja sobrecarga del protocolo. Se utilizan otros protocolos para informar tales errores.

Enlaces:

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

No existe una entrada de ruta ni una ruta predeterminada



5.4 PROCESOS DE ENRUTAMIENTO: CÓMO COMPARTIR RUTAS

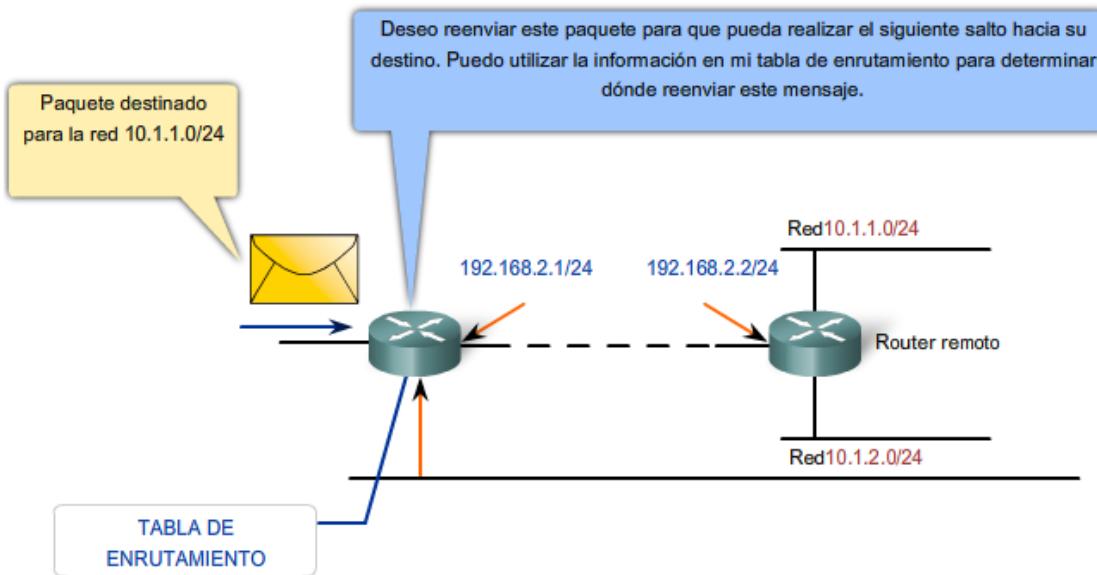
5.4.1 Protocolos de enrutamiento: Cómo compartir rutas

El enrutamiento requiere que cada salto o router a lo largo de las rutas hacia el destino del paquete tenga una ruta para reenviar el paquete. De otra manera, el paquete es descartado en ese salto. Cada router en una ruta no necesita una ruta hacia todas las redes. Sólo necesita conocer el siguiente salto en la ruta hacia la red de destino del paquete.

La tabla de enrutamiento contiene información que un router usa en sus decisiones al reenviar paquetes. Para las decisiones de enrutamiento, la tabla de enrutamiento necesita representar el estado más preciso de rutas de red a las que el router puede acceder. La información de enrutamiento desactualizada significa que los paquetes no pueden reenviarse al siguiente salto más adecuado, causando demoras o pérdidas de paquetes.

Esta información de ruta puede configurarse manualmente en el router o aprenderse dinámicamente a partir de otros routers en la misma internetwork. Después de que se configuran las interfaces de un router y éstas se vuelven operativas, se instala la red asociada con cada interfaz en la tabla de enrutamiento como una ruta conectada directamente.

Tablas de enrutamiento



5.4.2 Enrutamiento estatico

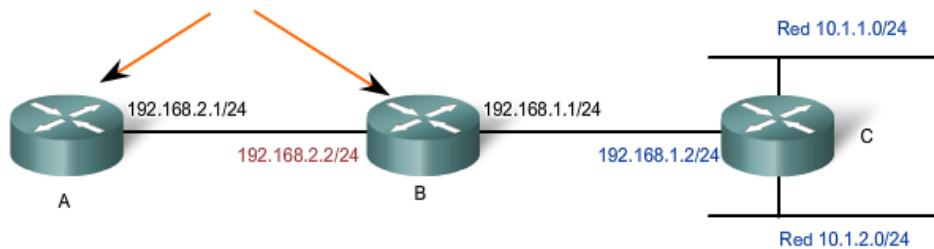
Las rutas a redes remotas con los siguientes saltos asociados se pueden configurar manualmente en el router. Esto se conoce como enrutamiento estático. Una ruta default también puede ser configurada estáticamente.

Si el router está conectado a otros routers, se requiere conocimiento de la estructura de internetworking. Para asegurarse de que los paquetes están enrutados para utilizar los mejores posibles siguientes saltos, cada red de destino necesita tener una ruta o una ruta default configurada. Como los paquetes son reenviados en cada salto, cada router debe estar configurado con rutas estáticas hacia los siguientes saltos que reflejan su ubicación en la internetwork.

Además, si la estructura de internetwork cambia o si se dispone de nuevas redes, estos cambios tienen que actualizarse manualmente en cada router. Si no se realiza la actualización periódica, la información de enrutamiento puede ser incompleta e inadecuada, causando demoras y posibles pérdidas de paquetes.

Enrutamiento estático

Routers configurados con las rutas



Router A:
192.168.2.2/24 configurado de manera manual como siguiente salto a las redes 10.1.1.0/24 y 10.1.2.0/24

Router B:
192.168.1.2/24 configurado de manera manual como siguiente salto a las redes 10.1.1.0/24 y 10.1.2.0/24

5.4.3 Enrutamiento dinámico

Aunque es esencial que todos los routers en una internetwork posean conocimiento actualizado, no siempre es factible mantener la tabla de enrutamiento por configuración estática manual. Por eso, se utilizan los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento son un conjunto de reglas por las que los routers comparten dinámicamente su información de enrutamiento. Como los routers advierten los cambios en las redes para las que actúan como 180ersión, o los cambios en enlaces entre routers, esta información pasa a otros routers. Cuando un router recibe información sobre rutas nuevas o modificadas, actualiza su propia tabla de enrutamiento y, a su vez, pasa la información a otros routers. De esta manera, todos los routers cuentan con tablas de enrutamiento actualizadas dinámicamente y pueden aprender sobre las rutas a redes remotas en las que se necesitan muchos saltos para llegar. La figura muestra un ejemplo de rutas que comparten un router.

Entre los protocolos de enrutamiento comunes se incluyen:

- protocolo de información de enrutamiento (RIP),
- protocolo de enrutamiento de 180ersión interior mejorado (EIGRP), y
- Open Shortest Path First (OSPF).

Aunque los protocolos de enrutamiento proveen routers con tablas de enrutamiento actualizadas, existen costos. Primero, el intercambio de la información de la ruta agrega una sobrecarga que consume el ancho de banda de la red. Esta sobrecarga puede ser un problema, particularmente para los enlaces del ancho de banda entre routers. Segundo, la información de la ruta que recibe un router es procesada extensamente por protocolos como EIGRP y OSPF para hacer las entradas a las tablas de enrutamiento. Esto significa que los routers que emplean estos protocolos deben tener suficiente capacidad de procesamiento como para implementar los algoritmos del protocolo para realizar el enrutamiento oportuno del paquete y enviarlo.

El enrutamiento estático no produce sobrecarga de la red ni ubica entradas 180ersión1800 n180180 en la tabla de enrutamiento; el router no necesita ningún tipo de procesamiento. El costo para un enrutamiento estático es administrativo, la configuración manual y el mantenimiento de la tabla de enrutamiento aseguran un enrutamiento eficiente y efectivo.

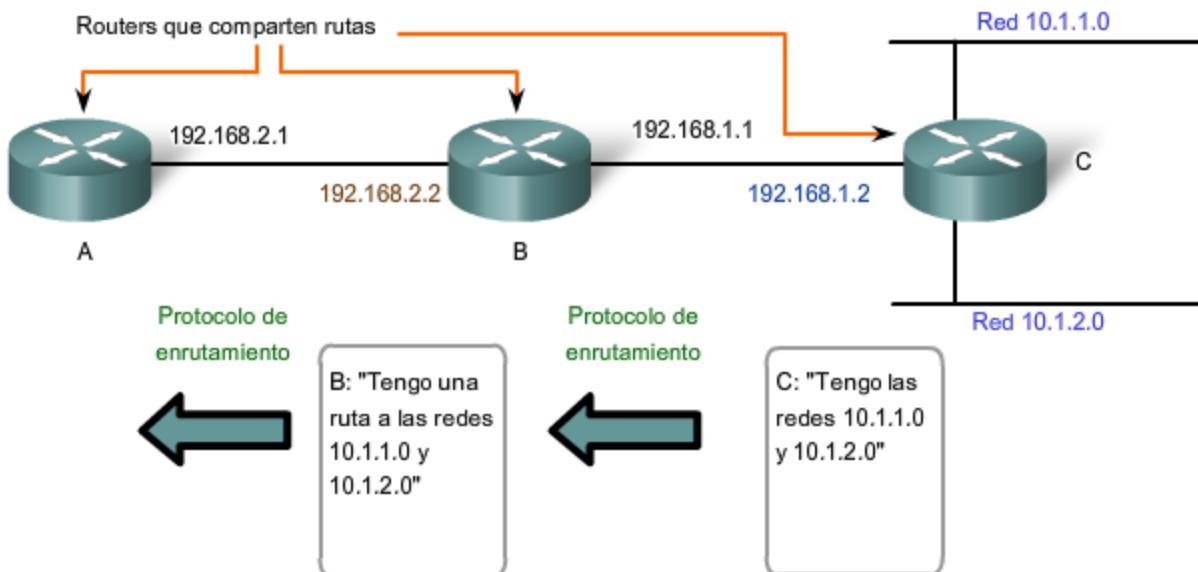
En muchas internetworks, la combinación de rutas estáticas, dinámicas y default se usa para proveer las rutas necesarias. La configuración de los protocolos de enrutamiento en routers es un componente integral del CCNA y será cubierta extensivamente en un curso posterior.

Enlaces;

RFC 823 <http://www.ietf.org/rfc/rfc0823.txt>

Principios de enrutamiento http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm

Enrutamiento dinámico



El Router B obtiene información sobre las redes del Router C en forma dinámica.

El siguiente salto del Router B a 10.1.1.0 y 10.1.2.0 es 192.168.1.2 (Router C).

El Router A obtiene información sobre las redes del Router C en forma dinámica desde el Router B.

El siguiente salto del Router A hacia 10.1.1.0 y 10.1.2.0 es 192.168.2.2 (Router B).

5.6 RESUMEN

5.6.1 Resumen

El protocolo de capa de Red más significativo (Capa 3 de OSI) es el Protocolo de Internet (IP). La versión 4 (Ipv4) de IP es el protocolo de capa de Red que se utilizará como ejemplo a lo largo de este curso.

El enrutamiento de IP de Capa 3 no garantiza una entrega confiable ni establece una conexión antes de transmitir los datos. Esta comunicación no confiable sin conexión es rápida y flexible, pero las capas superiores deben proveer mecanismos para garantizar la entrega de datos si se necesita.

La función de la capa de Red es llevar datos desde un host a otro sin tener en cuenta el tipo de datos. Los datos están encapsulados en un paquete. El encabezado del paquete tiene campos que incluyen la dirección de destino del paquete.

El direccionamiento jerárquico de la capa de Red con las porciones de red y host facilita la división de redes en subredes y permite el uso de la dirección de red para enviar paquetes hacia el destino en lugar de usar cada dirección de host individual.

Si la dirección de destino no está en la misma red como host de origen, el paquete pasa al 181ersión por defecto para ser enviado a la red de destino. El 181ersión es una interfaz de un router que analiza la dirección de destino. Si la red de destino tiene una entrada en su tabla de enrutamiento, el router envía el paquete ya sea a una red conectada o al 181ersión del siguiente salto. Si no hay entrada de enrutamiento, el router puede enviar el paquete a una ruta default o descartar el paquete.

Las entradas de la tabla de enrutamiento se pueden configurar manualmente en cada router para proveer enrutamiento estático, o los routers pueden comunicar la información de la ruta de manera dinámica entre ellos utilizando un protocolo de enrutamiento.

En este capítulo, aprendió a:

- Identificar la función de la capa de Red mientras describe la comunicación desde un dispositivo final hasta otro.
- Examinar el protocolo de capa de Red más común, el Internet Protocol (IP) y sus características para el suministro de un servicio sin conexión de mejor intento.
- Describir los principios utilizados para guiar la división o la agrupación de dispositivos en redes.
- Explicar la función del direccionamiento jerárquico de dispositivos y la forma en que éste permite la comunicación entre redes.
- Describir los aspectos básicos de las rutas, las direcciones de siguiente salto y el reenvío de paquetes a una red de destino.

6- DIRECCIONAMIENTO DE LA RED: IPv4

6.0 INTRODUCCIÓN DEL CAPÍTULO

6.0.1 Introducción del capítulo

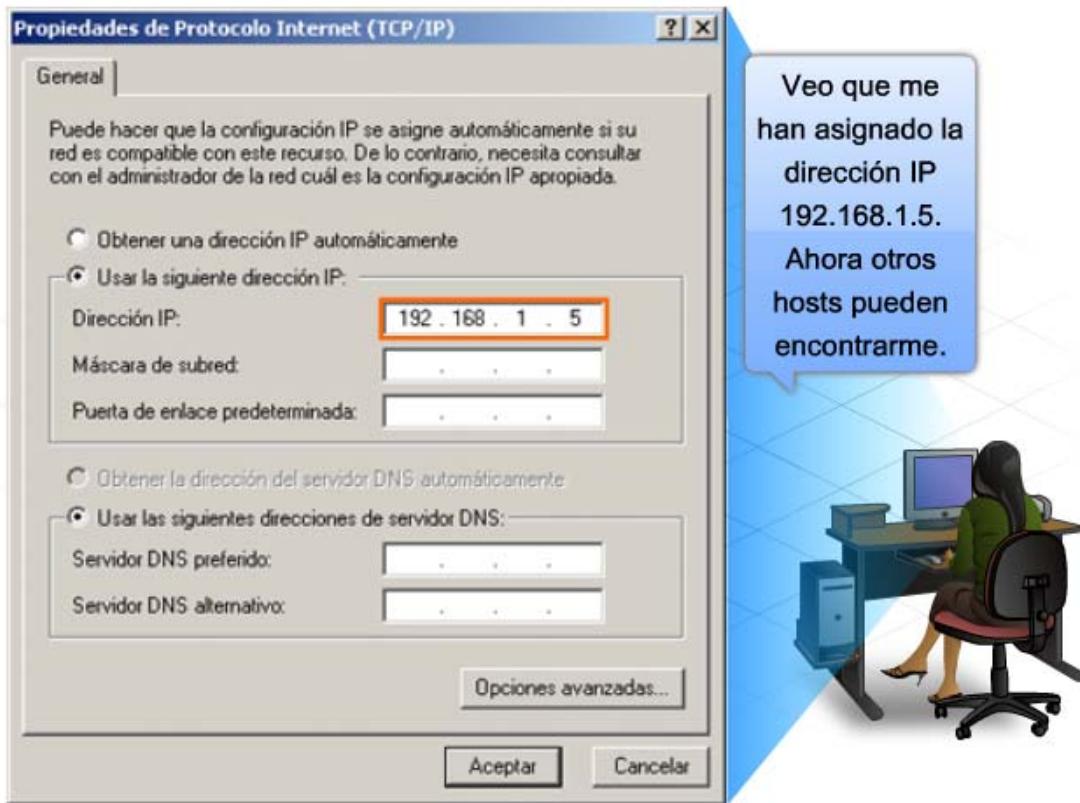
El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (Ipv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento Ipv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente.

Este capítulo examina detalladamente la estructura de las direcciones Ipv4 y su aplicación en la construcción y prueba de redes y subredes IP.

En este capítulo, usted aprenderá a:

- Explicar la estructura del direccionamiento IP y a convertir entre números binarios de 8 bits y números decimales.
- Clasificar por tipo una dirección Ipv4 y describir cómo se utiliza en la red.
- Explicar cómo las direcciones son asignadas a redes por los ISP y dentro de redes por los administradores.
- Determinar la porción de red de la dirección de host y explicar la función de la máscara de subred en la división de subredes.
- Calcular los componentes de direccionamiento adecuados de acuerdo con la información de la dirección Ipv4 y los criterios de diseño.
- Usar las utilidades comunes de comprobación para verificar la conectividad de red y estado operativo de la stack de protocolo IP en un host.



La versión IP 4 (IPv4) es la forma actual de direccionamiento utilizada en Internet.

6.1 DIRECCIONES IPv4

6.1.1 Estructura de una dirección IPv4

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con Ipv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes formamos parte de la red humana, una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones Ipv4 utilizando el formato decimal punteada.

Punto Decimal

Los patrones binarios que representan direcciones Ipv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

Por ejemplo: la dirección

10101100000100000000010000010100

es expresada en puntos decimales como

172.16.4.20

Tenga en cuenta que los dispositivos usan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

Porciones de red y de host

En cada dirección Ipv4, alguna porción de los bits de orden superior representa la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones.

A pesar de que los 32 bits definen la dirección host Ipv4, existe una cantidad variable de bits que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

Coloque el cursor sobre las etiquetas para ver las diferentes partes de la dirección.

Por ejemplo: si necesitamos tener al menos 200 hosts en una red determinada, necesitaríamos utilizar suficientes bits en la porción del host para poder representar al menos 200 patrones diferentes de bits.

Para asignar una dirección exclusiva a 200 hosts, se utilizará el último octeto entero. Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red.

Nota: Más adelante en este capítulo se verá cómo calcular la cantidad de hosts y cómo determinar qué porción de los 32 bits se refiere a la red.

| | | | | | | |
|----------|---|----------|---|----------|---|----------|
| 192 | . | 168 | . | 10 | . | 1 |
| 11000000 | | 10101000 | | 00001010 | | 00000001 |

La computadora que utiliza esta dirección se encuentra en la red
192.168.10.0.

6.1.2 Conocer los números: conversión de binario en decimal

Para comprender el funcionamiento de un dispositivo en una red, es necesario considerar las direcciones y otros datos de la manera en que lo hace un dispositivo: en notación binaria. Esto significa que es necesario ser hábil en la conversión de binario en decimal.

Los datos representados en el sistema binario pueden representar muchas formas diferentes de datos en la red humana. En este tema, se hace referencia al sistema binario por estar relacionado con el direccionamiento Ipv4. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255.

Notación de posición

El Aprendizaje de la notación de posición para convertir binario a decimal requiere una comprensión de los fundamentos matemáticos de un sistema de numeración llamado notación de posición. Notación de posición significa que un dígito representa diferentes valores según la posición que ocupa. 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 ejemplos ayudarán a aclarar cómo funciona este sistema.

Para el número decimal 245, el valor que el 2 representa es $2 * 10^2$ (2 multiplicado por 10 elevado a la segunda potencia). El 2 se encuentra en lo que comúnmente llamamos la posición “100”. Notación de posición se refiere a esta posición como posición $base^2$ porque la base o raíz es 10 y la potencia es 2.

Usando la notación de posición en el sistema de numeración con base 10, 245 representa:

$$245 = (2 * 10^2) + (4 * 10^1) + (5 * 10^0)$$

o

$$245 = (2 * 100) + (4 * 10) + (5 * 1)$$

Sistema de numeración binaria

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa potencias incrementadas 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 tiene solamente 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.

11.. 1 1 1 1 1 1

128 64 32 16 8 4 2 1

Un 1 en cada posición significa que el valor para esa posición se suma al total. Ésta es la suma cuando hay un 1 en cada posición de un octeto. El total es 255.

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$$

Un 0 en cada posición indica que el valor para esa posición no se suma al total. Un 0 en cada posición produce un total de 0.

0 0 0 0 0 0 0 0

128 64 32 16 8 4 2 1

$$0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$$

Note en la figura que una combinación diferente de unos y ceros producirá un valor decimal diferente.

Conversión binaria a decimal

| Exponente | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
|--------------------------------------|-------|-------|-------|-------|-------|-------|-------|-------------------|
| Posición | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Bits | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| Agregue estos números juntos | | | | | | | | 1 BYTE / 1 octeto |
| $128 + 64 + 32 + 16 + 0 + 4 + 0 + 1$ | | | | | | | | 245 |
| Decimal | | | | | | | | |

Un 1 en esta posición significa que 64 se agrega al total.

Un 0 en cualquier posición significa que 0 se agrega al total.

11110101 en binario = Número decimal 245

Observe la figura para obtener los pasos para convertir una dirección binaria en una dirección decimal.

En el ejemplo, el número binario:

10101100000100000000010000010100

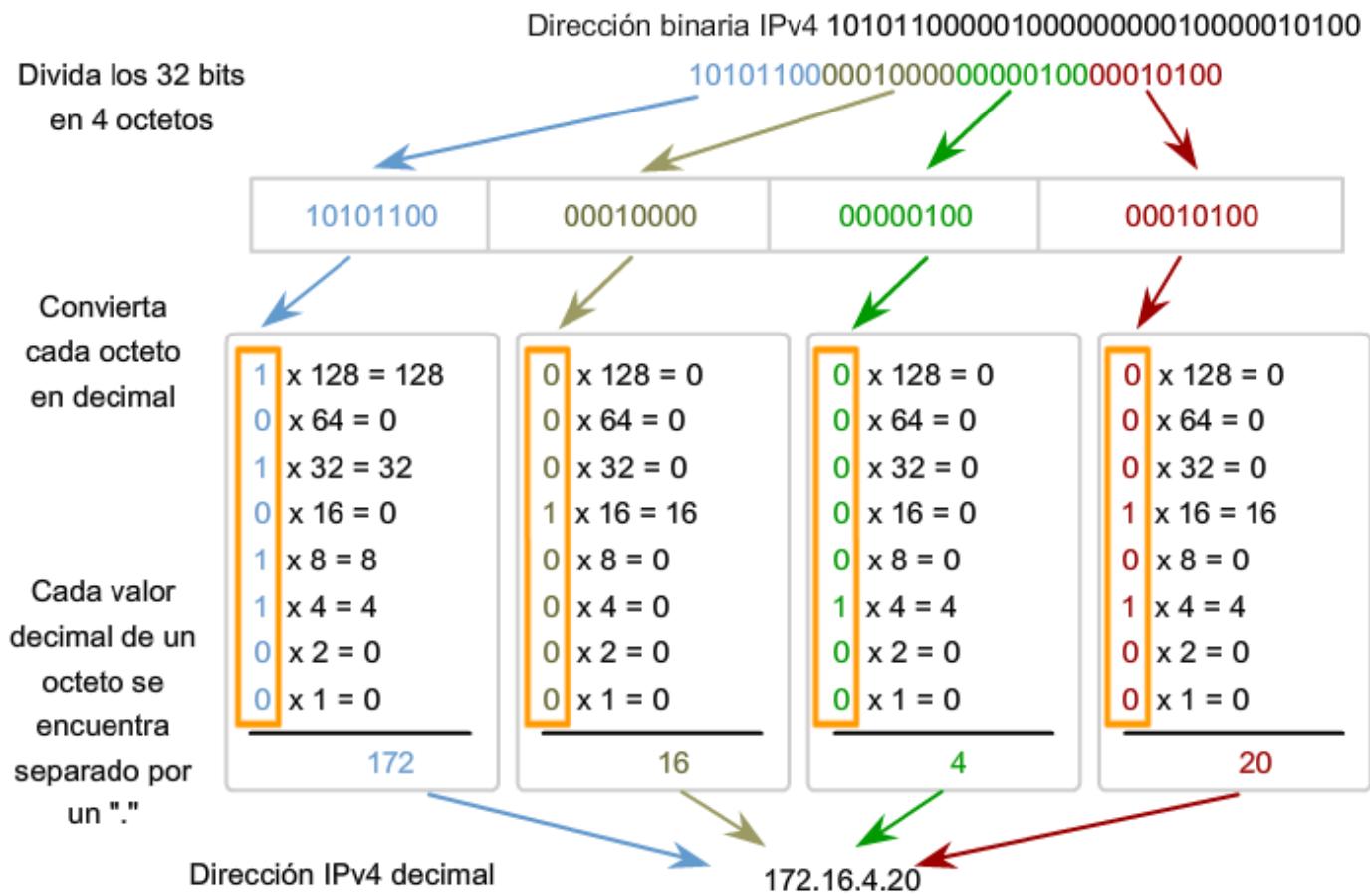
se convierte en:

172.16.4.20

Tenga en cuenta estos pasos:

- Divida los 32 bits en 4 octetos.
 - Convierta cada octeto a decimal.
 - Agregue un “punto” entre cada decimal.

Conversión de un IPv4 de binario a notación decimal punteada



6.1.4 Conocer los números: conversión de decimal en binario

No sólo es necesario poder realizar una conversión de binario en decimal, sino que también es necesario poder realizar una conversión de decimal en binario. Con frecuencia es necesario examinar un octeto individual de una dirección que se proporciona en notación decimal punteada. Tal es el caso cuando los bits de red y los bits de host dividen un octeto.

Por ejemplo: si un host 172.16.4.20 utilizara 28 bits para la dirección de red, sería necesario examinar los datos binarios del último octeto para descubrir que este host está en la red 172.16.4.16. Este proceso de extraer la dirección de red de una dirección de host se explicará más adelante.

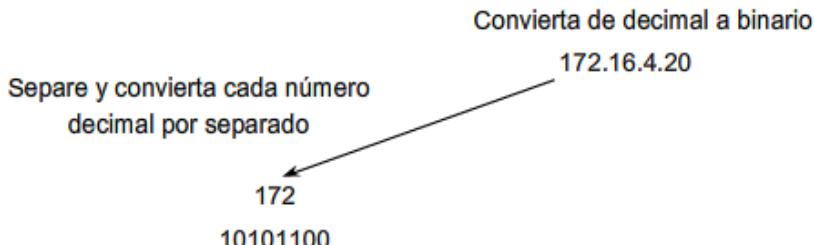
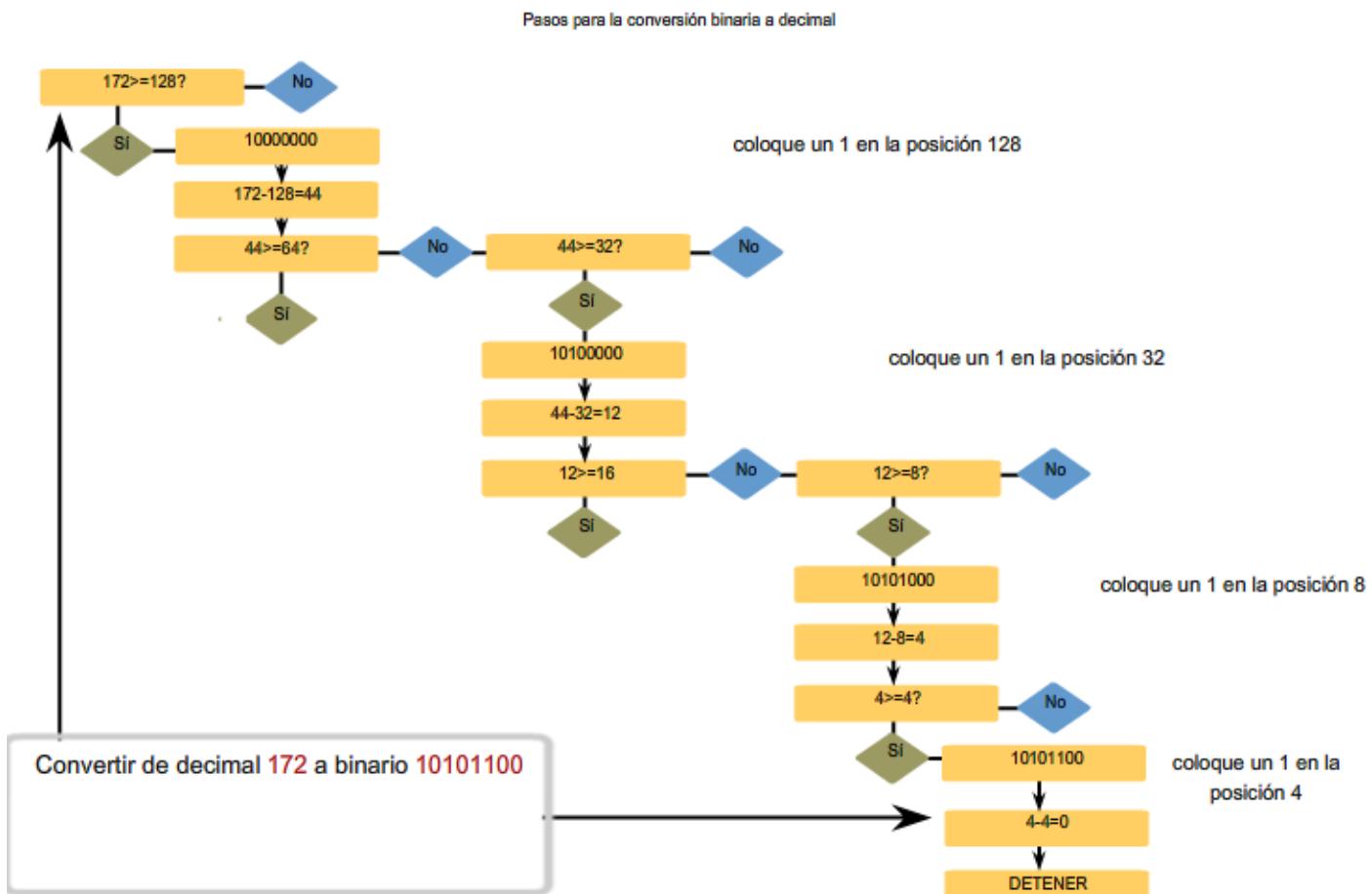
Los valores de la dirección están entre 0 y 255

Examinaremos sólo el proceso de conversión binaria de 8 bits a valores decimales de 0 a 255, porque nuestra representación de direcciones está limitada a valores decimales para un solo octeto.

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 valor es igual o mayor que 128. Si el valor es menor que 128, se coloca un 0 en la posición de 128 bits y se mueve a la posición de 64 bits.

Si el valor en la posición de 128 bits es mayor o igual que 128, se coloca un 1 en la posición 128 y se resta 128 del número que se está convirtiendo. Luego se comparan los valores restantes de esta operación con el siguiente valor más pequeño, 64. Se continúa con este proceso para todas las posiciones de bits restantes.

Ver la figura para obtener un ejemplo de estos pasos. Se convierte 172 en 10101100.



Comenzamos con el 172.

172 es mayor que 128, coloque un 1 en la posición 128
 $\underline{-128}$ y reste 128

$\underline{-44}$ es menor que 64, coloque un 0 en la posición 64

$\underline{-0}$ es mayor que 32, coloque un 1 en la posición 32

$\underline{-32}$ yreste 32

$\underline{-12}$ es menor que 16, coloque un 0 en la posición 16

$\underline{-0}$ es mayor que 8, coloque un 1 en la posición 8

$\underline{-8}$ yreste 8

$\underline{-4}$ es igual a 4, coloque un 1 en la posición 4

$\underline{-4}$ yreste 4

$\underline{-0}$ es menor que 2, coloque un 0 en la posición 2

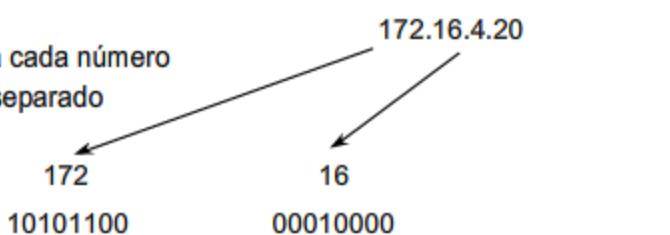
$\underline{-0}$ es menor que 1, coloque un 0 en la posición 1

$\underline{-0}$ LISTO

Respuesta: 172 = 10101100

Convierta de decimal a binario

Separe y convierta cada número decimal por separado



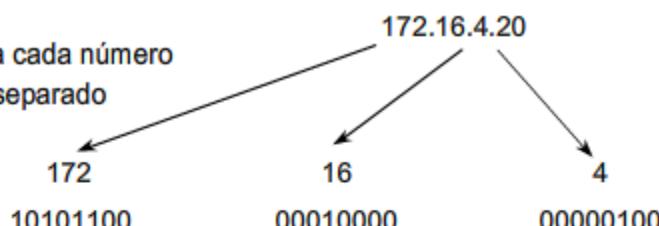
Luego, convertimos el 16.

- 16 es menor que 128, coloque un 0 en la posición 128
- 0
- 16 es menor que 64, coloque un 0 en la posición 64
- 0
- 16 es menor que 32, coloque un 0 en la posición 32
- 0
- 16 es igual a 16, coloque un 1 en la posición 16
- 16 y reste 16
- 0 es menor que 8, coloque un 0 en la posición 8
- 0
- 0 es menor que 4, coloque un 0 en la posición 4
- 0
- 0 es menor que 2, coloque un 0 en la posición 2
- 0
- 0 es menor que 1, coloque un 0 en la posición 1
- 0
- 0 LISTO

Respuesta: 16 = 00010000

Convierta de decimal a binario

Separe y convierta cada número decimal por separado



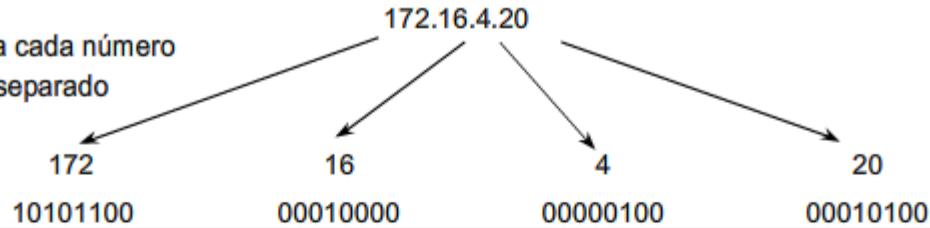
Luego, convertimos el 4.

- 4 es menor que 128, coloque un 0 en la posición 128
- 0
- 4 es menor que 64, coloque un 0 en la posición 64
- 0
- 4 es menor que 32, coloque un 0 en la posición 32
- 0
- 4 es menor que 16, coloque un 0 en la posición 16
- 0
- 4 es menor que 8, coloque un 0 en la posición 8
- 0
- 4 es igual a 4, coloque un 1 en la posición 4
- 4 yreste 4
- 0 es menor que 2, coloque un 0 en la posición 2
- 0
- 0 es menor que 1, coloque un 0 en la posición 1
- 0
- 0 LISTO

Respuesta: 4 = 00000100

Convierta de decimal a binario

Separar y convierta cada número decimal por separado



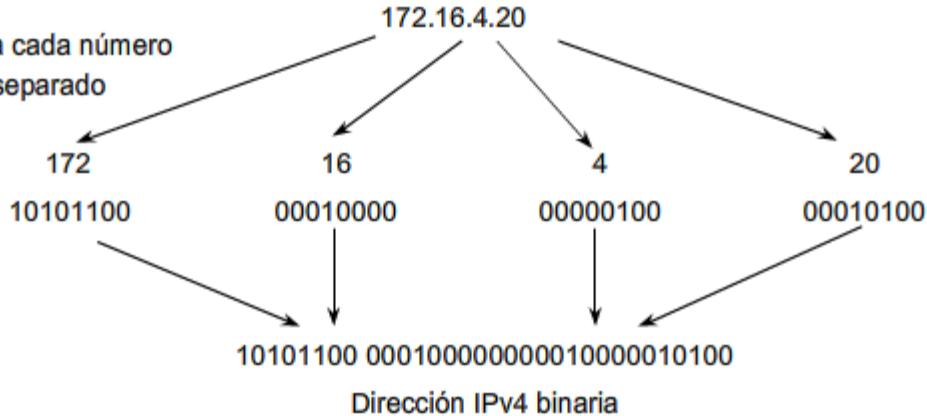
Finalmente, convertimos el 20.

20 es menor que 128, coloque un 0 en la posición 128
- 0
20 es menor que 64, coloque un 0 en la posición 64
- 0
20 es menor que 32, coloque un 0 en la posición 32
- 0
20 es mayor que 16, coloque un 1 en la posición 16
- 16 y reste 16
4 es menor que 8, coloque un 0 en la posición 8
- 0
4 es igual a 4, coloque un 1 en la posición 4
- 4 y reste 4
0 es menor que 2, coloque un 0 en la posición 2
- 0
0 es menor que 1, coloque un 0 en la posición 1
- 0
0 LISTO

Respuesta: 20 = 00010100

Convierta de decimal a binario

Separar y convierta cada número decimal por separado



Resumen de conversión

La figura resume la conversión completa de 172.16.4.20 de notación decimal punteada a notación binaria.

Convierte de decimal a binario

Dirección IPv4 decimal 172.16.4.20

Separé y convierta cada número decimal por separado

| Convierte 172 | Convierte 16 | Convierte 4 | Convierte 20 |
|---|---------------------------------------|------------------------------------|---------------------------------------|
| $172 - 128 = 44 \rightarrow 1 \times 128$ | $16 < 128 \rightarrow 0 \times 128$ | $4 < 128 \rightarrow 0 \times 128$ | $20 < 128 \rightarrow 0 \times 128$ |
| $44 < 64 = 0 \rightarrow 0 \times 64$ | $16 < 64 \rightarrow 0 \times 64$ | $4 < 64 \rightarrow 0 \times 64$ | $20 < 64 \rightarrow 0 \times 64$ |
| $44 - 32 = 12 \rightarrow 1 \times 32$ | $16 < 32 \rightarrow 0 \times 32$ | $4 < 32 \rightarrow 0 \times 32$ | $20 < 32 \rightarrow 0 \times 32$ |
| $12 < 16 = 0 \rightarrow 0 \times 16$ | $16 - 16 = 0 \rightarrow 1 \times 16$ | $4 < 16 \rightarrow 0 \times 16$ | $20 - 16 = 4 \rightarrow 1 \times 16$ |
| $12 - 8 = 4 \rightarrow 1 \times 8$ | $0 < 8 \rightarrow 0 \times 8$ | $4 < 8 \rightarrow 0 \times 8$ | $4 < 8 \rightarrow 0 \times 8$ |
| $4 - 4 = 0 \rightarrow 1 \times 4$ | $0 < 4 \rightarrow 0 \times 4$ | $4 - 4 = 0 \rightarrow 1 \times 4$ | $4 - 4 = 0 \rightarrow 1 \times 4$ |
| $0 < 2 = 0 \rightarrow 0 \times 2$ | $0 < 2 \rightarrow 0 \times 2$ | $0 < 2 \rightarrow 0 \times 2$ | $0 < 2 \rightarrow 0 \times 2$ |
| $0 < 1 = 0 \rightarrow 0 \times 1$ | $0 < 1 \rightarrow 0 \times 1$ | $0 < 1 \rightarrow 0 \times 1$ | $0 < 1 \rightarrow 0 \times 1$ |

10101100

00010000

00000100

00010100

La dirección IPv4 binaria 10101100 00010000000010000010100

6.2 DIRECCIONES PARA DIFERENTES PROPOSITOS

6.2.1 Tipos de direcciones de una red IPv4

Dentro del rango de direcciones de cada red Ipv4, existen tres tipos de direcciones:

Dirección de red: la dirección en la que se hace referencia a la red.

Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.

Direcciones host: las direcciones asignadas a los dispositivos finales de la red.

Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como “red 10.0.0.0”. Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como “la primera red”. Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

Dentro del rango de dirección Ipv4 de una red, la dirección más baja 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.

Coloque el cursor sobre la ficha DIRECCIÓN DE RED en la figura.

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 de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

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. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido.

Coloque el cursor del mouse sobre la ficha BROADCAST ADDRESS (dirección de broadcast) en la figura.

Direcciones host

Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones Ipv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

Coloque el cursor del mouse sobre la ficha HOST ADDRESS (dirección host) en la figura.

Tipos de direcciones

| Red | Host |
|----------------------------|----------|
| 10 0 0 0 | 0 |
| 00001010 00000000 00000000 | 00000000 |
| | |
| 10 0 0 255 | 255 |
| 00001010 00000000 00000000 | 11111111 |
| | |
| 10 0 0 1 | 1 |
| 00001010 00000000 00000000 | 00000001 |

Dirección de red

Dirección de broadcast

Dirección host

Coloque el cursor del mouse aquí para obtener más información.

10.0.0.0 se utiliza para referirse a la red en su totalidad.
Todos los dispositivos en esta red poseen los mismos bits de dirección de red.

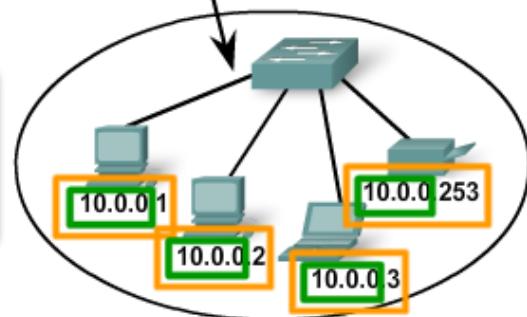
The diagram illustrates a local network segment enclosed in an orange oval. It features a central switch-like device at the top, connected to four computer icons below it. The IP addresses assigned to these hosts are 10.0.0.1, 10.0.0.2, 10.0.0.3, and 10.0.0.253. An arrow originates from the 'Host' column of the table and points directly to the host with the address 10.0.0.253.

Tipos de direcciones

| Dirección de red | Red | Host |
|------------------------|----------------------------|----------|
| | 10 0 0 | 0 |
| Dirección de broadcast | 00001010 00000000 00000000 | 00000000 |
| Dirección host | 10 0 0 | 255 |
| | 00001010 00000000 00000000 | 11111111 |
| | 10 0 0 | 1 |
| | 00001010 00000000 00000000 | 00000001 |

Coloque el cursor del mouse aquí para obtener más información.

La dirección de broadcast se utiliza para enviar paquetes a cada host en la red que comparta la misma porción de red de la dirección.

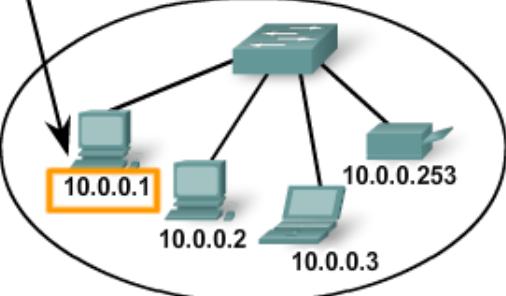


Tipos de direcciones

| Dirección de red | Red | Host |
|------------------------|----------------------------|----------|
| | 10 0 0 | 0 |
| Dirección de broadcast | 00001010 00000000 00000000 | 00000000 |
| Dirección host | 10 0 0 | 255 |
| | 00001010 00000000 00000000 | 11111111 |
| | 10 0 0 | 1 |
| | 00001010 00000000 00000000 | 00000001 |

Coloque el cursor del mouse aquí para obtener más información.

Cada host en esta red posee una dirección única.



Prefijos de red

Una pregunta importante es: ¿Cómo es posible saber cuántos bits representan la porción de red y cuántos bits representan la porción de host? Al expresar una dirección de red Ipv4, se agrega una longitud de prefijo a la dirección de red. **La longitud de prefijo es la cantidad de bits en la dirección que conforma la porción de red.** Por ejemplo: en 172.16.4.0 /24, /24 es la longitud de prefijo e indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host. Más adelante en este capítulo, el usuario aprenderá más acerca de otra entidad que se utiliza para especificar la porción de red de una dirección Ipv4 en los dispositivos de red. Se llama máscara de subred. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza unos y ceros para indicar cuáles bits de la dirección son bits de red y cuáles bits son bits de host.

No siempre a las redes se le asigna un prefijo /24. 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.

Coloque el cursor del mouse sobre las direcciones en la figura para ver los resultados de utilizar diferentes prefijos en una dirección.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes longitudes de prefijos. En esta figura puede ver también que el número de hosts que puede ser direccionado a la red también cambia.

Utilización de diferentes prefijos para la red 172.16.4.0

| Red | Dirección de red Todos los bits de hosts (rojo) = 0 | Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos | Dirección de broadcast Todos los bits de host (en rojo) = 1 |
|--|--|--|--|
| 172.16.4.0 /24 | 172.16.4.0 | 172.16.4.1 – 172.16.4.254 | 172.16.4.255 |
| 172.16.4.0 /25 | 172.16.4.0 | 172.16.4.1 – 172.16.4.126 | 172.16.4.127 |
| Representación binaria 25 bits de red | 10101100.00010000.000001 00.00000000 | 10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.01111110 | 10101100.00010000.00000100.01111111 |
| 172.16.4.0 /26 | 172.16.4.0 | 172.16.4.1 – 172.16.4.62 | 172.16.4.63 |
| 172.16.4.0 /27 | 172.16.4.0 | 172.16.4.1 – 172.16.4.30 | 172.16.4.31 |

MISMA DIRECCIÓN DE RED
PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE
BROADCAST PARA CADA
PREFIJO

126 hosts

DIFERENTE CANTIDAD DE HOSTS PARA CADA
PREFIJO

Coloque el cursor del mouse sobre las filas para ver los números binarios de las direcciones y la cantidad de hosts.

6.2.2 Cálculo de direcciones de host, de red y de broadcast

Hasta ahora, el usuario podría preguntarse: ¿Cómo se calculan estas direcciones? Este proceso de cálculo requiere que el usuario considere estas direcciones como binarias.

En las divisiones de red de ejemplo, se debe considerar el octeto de la dirección donde el prefijo divide la porción de red de la porción de host. En todos estos ejemplos, es el último octeto. A pesar de que esto es frecuente, el prefijo también puede dividir cualquiera de los octetos.

Para comenzar a comprender este proceso para determinar asignaciones de dirección, se desglosarán algunos ejemplos en datos binarios.

Observe la figura para obtener un ejemplo de la asignación de dirección para la red 172.16.20.0 /25.

En el primer cuadro, se encuentra la representación de la dirección de red. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la dirección de red, todos estos bits de host son "0". Esto hace que el último octeto de la dirección sea 0. De esta forma, la dirección de red es 172.16.20.0 /25.

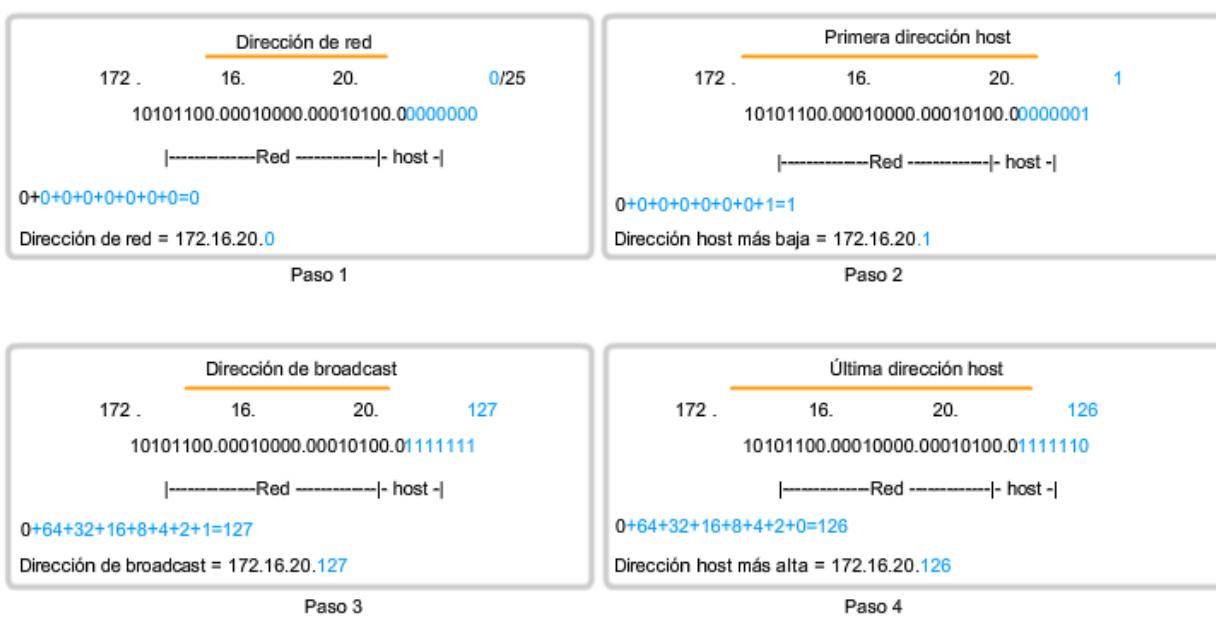
En el segundo cuadro, se observa el cálculo de la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.

El tercer cuadro muestra el cálculo de la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

El cuarto cuadro representa el cálculo de la dirección host más alta. La dirección host más alta de una red es siempre un número menor que la dirección de broadcast. Esto significa que el bit más bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

A pesar de que para este ejemplo se ampliaron todos los octetos, sólo es necesario examinar el contenido del octeto dividido.

Asignación de direcciones



6.2.3 Unicast, broadcast, multicast: tipos de comunicación

En una red Ipv4, los hosts pueden comunicarse de tres maneras diferentes:

Unicast: el proceso por el cual se envía un paquete de un host a un host individual.

Broadcast: el proceso por el cual se envía un paquete de un host a todos los hosts de la red.

Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

Estos tres tipos de comunicación se usan con diferentes 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 una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutararse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internetwork.

Reproduzca la animación para ver un ejemplo de transmisión unicast.

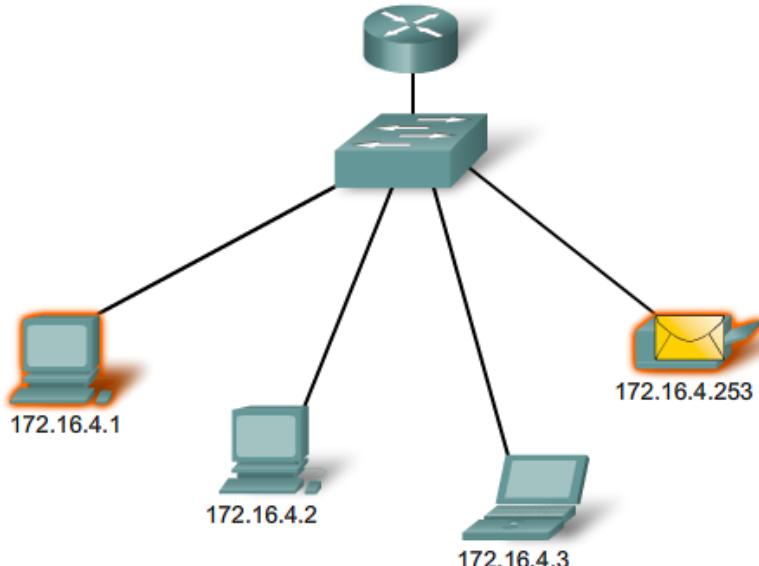
En una red Ipv4, a la dirección unicast aplicada a un dispositivo final se le denomina dirección de host. En la comunicación unicast, las direcciones host asignadas a dos dispositivos finales se usan como direcciones Ipv4 de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección Ipv4 en el encabezado del paquete unicast como la dirección host de origen y la dirección Ipv4 del host de destino en el encabezado del paquete como la dirección de destino. Es posible enviar la comunicación utilizando un paquete unicast por medio de una internetwork con las mismas direcciones.

Nota: En este curso, todas las comunicaciones entre dispositivos son comunicaciones unicast a menos que se indique lo contrario.

Transmisión unicast

Origen: 172.16.4.1

Destino: 172.16.4.253



Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

La transmisión de broadcast se usa para ubicar servicios/dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe brindar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección
- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast.

De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente están restringidos a la red local. Esta restricción depende de la configuración del router que bordea la red y del tipo de broadcast. Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

Broadcast dirigido

Se envía un broadcast dirigido a todos los hosts en 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 se comunique con los hosts dentro de la red 172.16.4.0 /24, la dirección de destino del paquete sería 172.16.4.255. Esto se muestra en la figura. Aunque los routers no envían broadcasts dirigidos por defecto, se los puede configurar para que lo hagan.

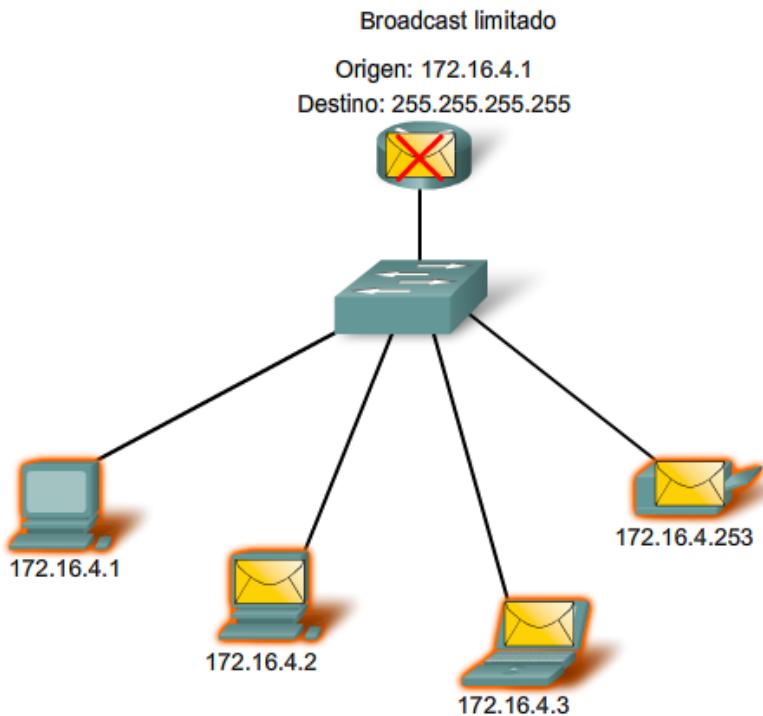
Broadcast limitado

El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección Ipv4 de destino 255.255.255.255. Los routers no envían estos broadcasts. Los paquetes dirigidos a la dirección de broadcast limitada sólo aparecerán en la red local. Por esta razón, también se hace referencia a una red Ipv4 como un dominio de broadcast. Los routers son 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.

Como se mostró anteriormente, cuando se transmite un paquete, éste utiliza recursos de la red y de esta manera obliga a cada host de la red que lo recibe a procesar 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.



Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de la red Ipv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. 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.

Algunos ejemplos de transmisión de multicast son:

- Distribución de audio y video
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
- Distribución de software
- Suministro de noticias

Clients Multicast

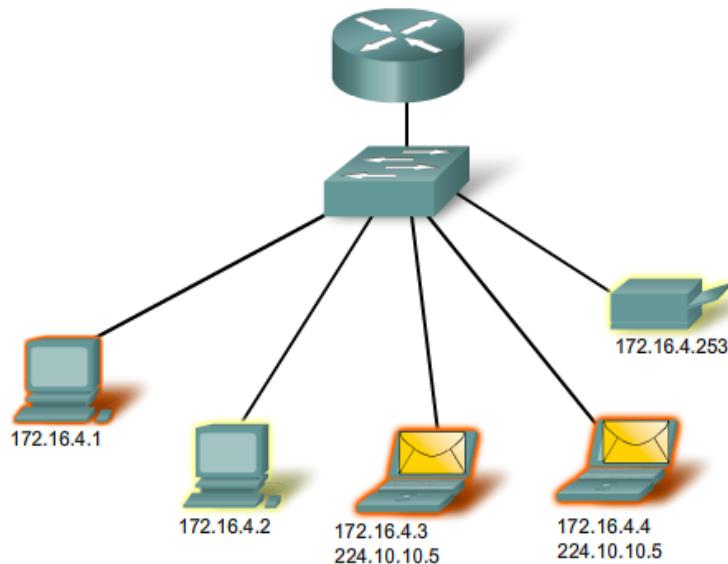
Los hosts que desean recibir datos multicast específicos se denominan clientes multicast. Los clientes multicast usan servicios iniciados por un programa cliente para suscribirse al grupo multicast.

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 exclusivamente asignada. Como se puede ver, Ipv4 ha apartado un bloque especial de direcciones desde 224.0.0.0 a 239.255.255.255 para direccionamiento de grupos multicast.

La animación muestra clientes que aceptan paquetes multicast.

Transmisión multicast

Origen: 172.16.4.1



6.2.4 Rangos de direcciones IPv4 reservadas

Expresado en formato decimal punteado, el rango de direcciones Ipv4 es de 0.0.0.0 a 255.255.255.255. Como se pudo observar anteriormente, no todas estas direcciones pueden usarse como direcciones host para la comunicación unicast.

Direcciones experimentales

Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones Ipv4 experimentales de 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones se mencionan como reservadas para uso futuro (RFC 3330). Esto sugiere que podrían convertirse en direcciones utilizables. En la actualidad, no es posible utilizarlas en redes Ipv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

Direcciones multicast

Como se mostró antes, otro bloque importante de direcciones reservado con objetivos específicos es el rango de direcciones Ipv4 multicast de 224.0.0.0 a 239.255.255.255. Además, el rango de direcciones multicast se subdivide en diferentes tipos de direcciones: direcciones de enlace locales reservadas y direcciones agrupadas globalmente. Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de alcance limitado.

Las direcciones Ipv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones reservadas de enlace local. Estas direcciones se utilizarán con grupos multicast en una red local. Los paquetes enviados a estos destinos siempre se transmiten con un valor de período de vida (TTL) de 1. Por lo tanto, un router conectado a la red local nunca debería enviarlos. Un uso común de direcciones de enlace local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones de alcance global son de 224.0.1.0 a 238.255.255.255. Se las puede usar para transmitir datos en Internet mediante multicast. Por ejemplo: 224.0.1.1 ha sido reservada para el Protocolo de hora de red (NTP) para sincronizar los relojes con la hora del día de los dispositivos de la red.

Direcciones host

Después de explicar los rangos reservados para las direcciones experimentales y las direcciones multicast, queda el rango de direcciones de 0.0.0.0 a 223.255.255.255 que podría usarse con hosts Ipv4. Sin embargo, dentro de este rango existen muchas direcciones que ya están reservadas con objetivos específicos. A pesar de que se han tratado algunas de estas direcciones anteriormente, las principales direcciones reservadas se tratan en la próxima sección.

Rangos de direcciones IPv4 reservadas

| Tipo de dirección | Uso | Rango de direcciones IPv4 reservadas | RFC |
|----------------------------|--|--------------------------------------|--------------|
| Dirección host | utilizada en hosts IPv4 | De 0.0.0.0 a 223.255.255.255 | 790 |
| Dirección multicast | utilizada en grupos multicast en una red local | De 224.0.0.0 a 239.255.255.255 | 1700 |
| Direcciones experimentales | <ul style="list-style-type: none">utilizada para investigación o experimentaciónactualmente no se puede utilizar para los hosts en las redes IPv4 | De 240.0.0.0 a 255.255.255.254 | 1700 3330 |

6.2.5 Direcciones 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. A estas direcciones se las denomina 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)

Los bloques de direcciones de espacio privadas, como se muestra en la figura, se separa para utilizar en redes privadas. No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas. Por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones. Sin embargo, las redes internas aún deben diseñar esquemas de direcciones de red para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de networking.

Muchos hosts en diferentes 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 hacerse camino hacia Internet, los routers no tendrían rutas para enviarlos a la red privada correcta.

Traducción de direcciones de red (NAT)

Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

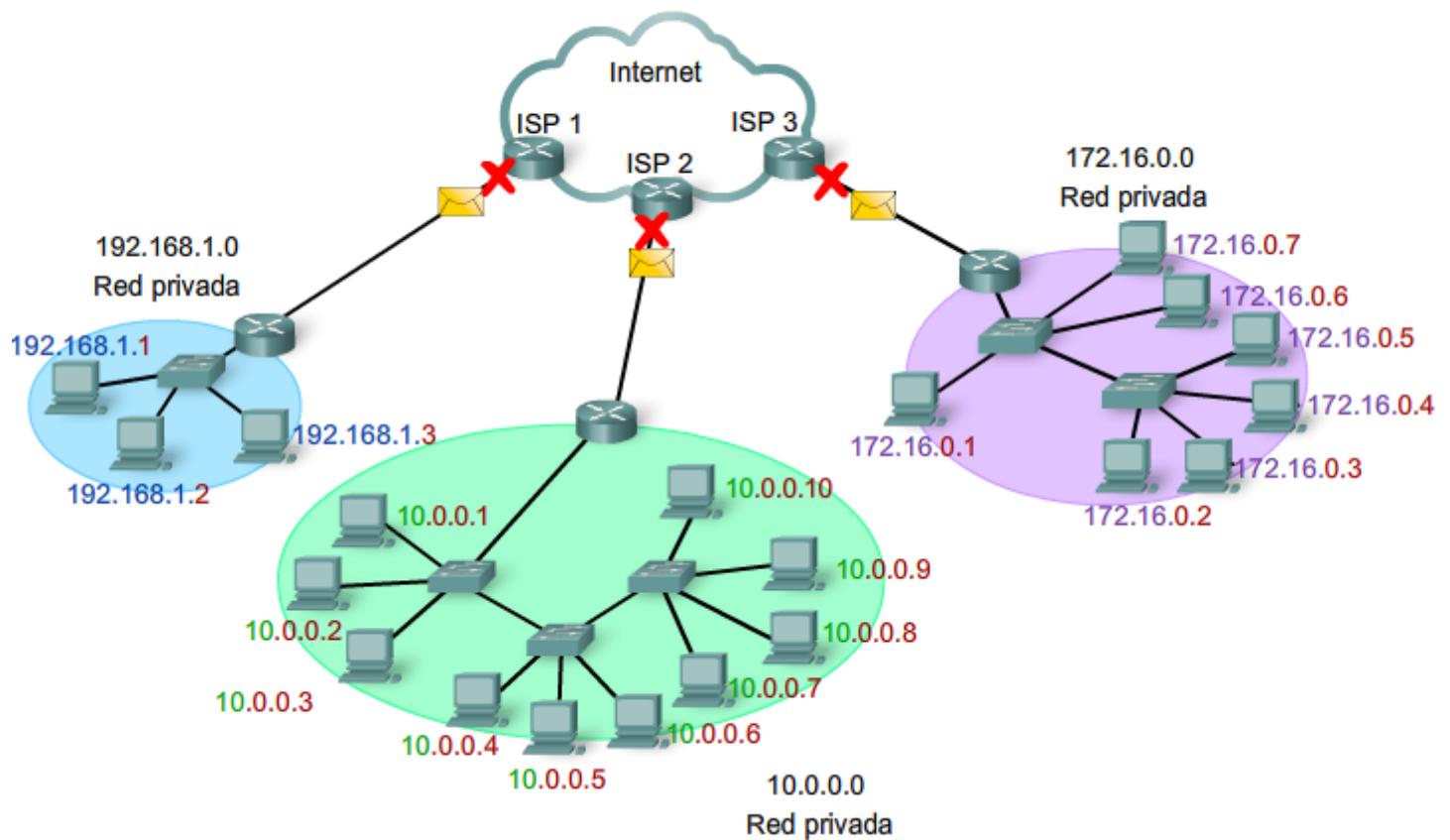
NAT permite a los hosts de la red “pedir prestada” una dirección pública para comunicarse con redes externas. A pesar de que existen algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

Nota: NAT será tratado en detalle en un curso posterior.

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, existen muchas direcciones designadas para otros fines específicos.

Direcciones privadas utilizadas en redes sin NAT



6.2.6 Direcciones IPv4 especiales

Hay determinadas direcciones que no pueden ser asignadas a los hosts por varios motivos. También hay direcciones especiales que pueden ser asignadas a los hosts pero con restricciones en la interacción de dichos hosts 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 la dirección de red y la dirección de broadcast, respectivamente.

Ruta predeterminada

También anteriormente presentada, se representa la ruta predeterminada Ipv4 como 0.0.0.0. La ruta predeterminada se usa como ruta “comodín” cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 – 0.255.255.255 (0.0.0.0 /8).

Loopback

Una de estas direcciones reservadas es la dirección Ipv4 de loopback 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 dentro del host local. Ni siquiera debe aparecer ninguna dirección en ninguna red dentro de este bloque.

Direcciones de enlace local

Las direcciones Ipv4 del bloque de direcciones de 169.254.0.0 a 169.254.255.255 (169.254.0.0 /16) son designadas como direcciones de enlace local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Éstas pueden usarse en una pequeña red punto a punto o con un host que no podría obtener automáticamente una dirección de un servidor de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host, DHCP).

La comunicación mediante direcciones de enlace 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 de enlace local Ipv4 a ningún router para ser enviado, y debería establecer el TTL de Ipv4 para estos paquetes en 1.

Las direcciones de enlace local no ofrecen 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

Se establece el bloque de direcciones de 192.0.2.0 a 192.0.2.255 (192.0.2.0 /24) 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

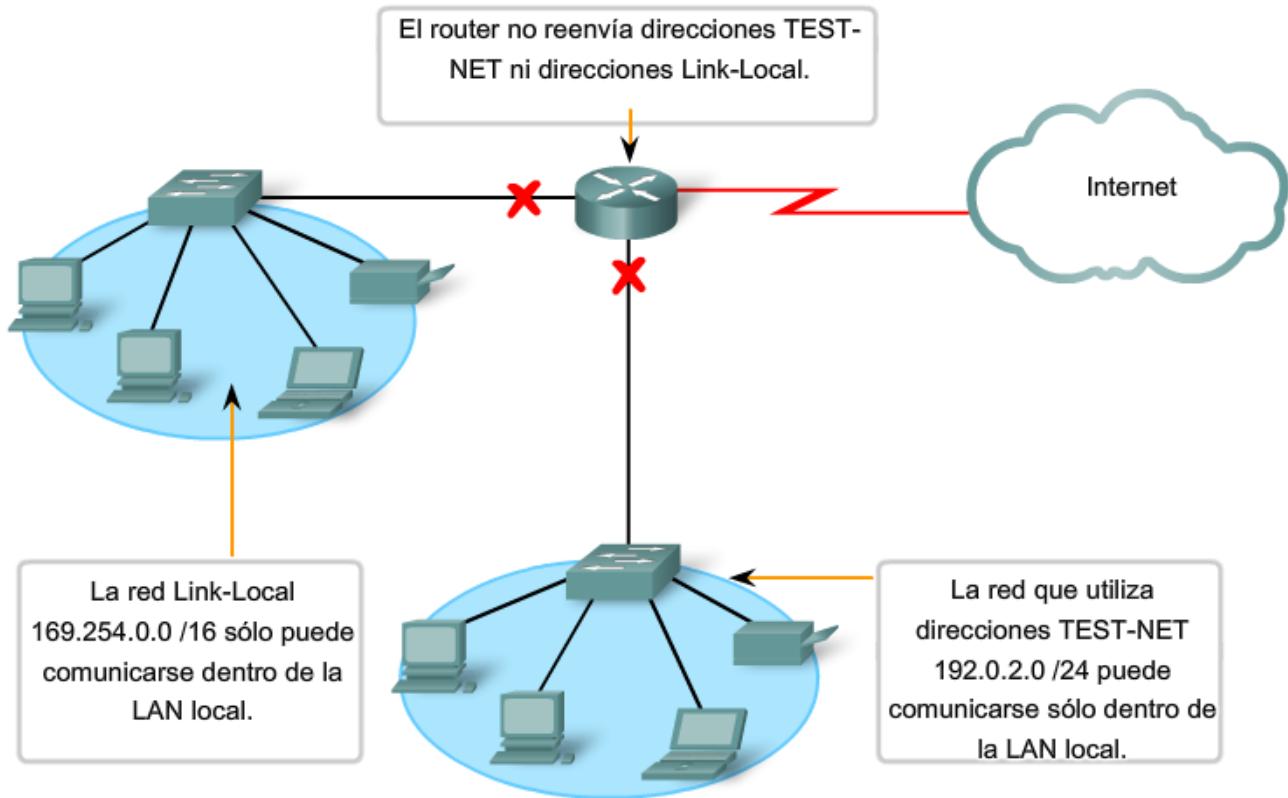
direcciones se usan con los nombres de dominio example.com o example.net en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

Enlaces:

Direcciones de enlace local <http://www.ietf.org/rfc/rfc3927.txt?number=3927>

Direcciones Ipv4 de uso especial <http://www.ietf.org/rfc/rfc3330.txt?number=3330>

Ubicación multicast: <http://www.iana.org/assignments/multicast-addresses>
Direcciones IPv4 especiales



6.2.7 Direccionamiento de IPv4 de legado

Clases de redes antiguas

Históricamente, la RFC1700 agrupaba rangos de 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, así como bloques de direcciones específicos para estas redes, como se muestra en la figura. 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 es denominado 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.

Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que sólo había 128 redes de clase A posibles, de 0.0.0.0 /8 a 127.0.0.0 /8, antes de excluir los bloques de direcciones reservadas. 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 satisfacer las necesidades de las redes de tamaño moderado a grande con más de 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. De esta forma, se 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 un tanto más eficiente que la clase A debido a que dividía equitativamente el 25% del total del espacio de direcciones Ipv4 entre aproximadamente 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 direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0 /16 a 223.255.255.0 /16. A pesar de que ocupaba sólo el 12.5% del total del espacio de direcciones Ipv4, podía suministrar direcciones a 2 millones de redes.

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: al asignar una dirección Ipv4 a una computadora, el sistema operativo examina la dirección que se está asignando para determinar si es de clase A, clase B o clase C. Luego, el sistema operativo adopta el prefijo utilizado por esa clase y realiza la asignación de la máscara de subred adecuada.

Otro ejemplo es la adopción de la máscara por parte de algunos protocolos de enrutamiento. Cuando algunos protocolos de enrutamiento reciben una ruta publicada, se puede adoptar la longitud del prefijo de acuerdo con la clase de dirección.

Direccionamiento sin clase

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema classless, se asignan los bloques de direcciones adecuados para la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase de unicast.

Clases de direcciones IP

| Clase de direcciones | 1er rango del octeto (decimal) | 1eros bits del octeto (los bits verdes no cambian) | Partes de las direcciones de red(N) y de host(H) | Máscara de subred predeterminada (decimal y binaria) | Número de posibles redes y hosts por red |
|----------------------|--------------------------------|--|--|--|---|
| A | 1-127** | 00000000-01111111 | N.H.H.H | 255.0.0.0 | 128 redes (2^7) 16,777,214 hosts por red ($2^{24}-2$) |
| B | 128-191 | 10000000-10111111 | N.N.H.H | 255.255.0.0 | 16,384 redes (2^{14}) 65,534 hosts por red ($2^{16}-2$) |
| C | 192-223 | 11000000-11011111 | N.N.N.H | 255.255.255.0 | 2,097,150 redes (2^{21}) 254 hosts por red ($2^{8}-2$) |
| D | 224-239 | 11000000-11011111 | ND (multicast) | | |
| E | 240-255 | 11100000-11111111 | ND (experimental) | | |

** Todos los ceros (0) y los unos (1) son direcciones hosts no válidas.

6.3 ASIGNACION DE DIRECCIONES

6.3.1 Planificación del direccionamiento de una red

Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red corporativa esté bien diseñada. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

- Evitar duplicación de direcciones.
- Proveer y controlar el acceso.
- Monitorear seguridad y rendimiento.

Evitar duplicación de direcciones

Como se sabe, cada host en una interwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

Brindar acceso y controlarlo

Algunos hosts ofrecen recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. El acceso a estos recursos puede ser controlado por la dirección de la Capa 3. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Por ejemplo: si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a su dirección y es posible que los clientes no puedan ubicar este recurso.

Monitorear la seguridad y el rendimiento

De igual manera, es necesario monitorear la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

Asignación de direcciones dentro de una red

Como ya se ha explicado, los hosts se asocian con una red Ipv4 por medio de una porción de red en común de la dirección. Dentro de una red, existen diferentes tipos de hosts.

Algunos ejemplos de diferentes tipos de hosts son:

- Dispositivos finales para usuarios.
- Servidores y periféricos.
- Hosts a los que se accede desde Internet.
- Dispositivos intermediarios.

Cada uno de los diferentes tipos de dispositivos debe ser asignado en un bloque lógico de direcciones dentro del rango de direcciones de la red.

Una parte importante de la planificación de un esquema de direccionamiento Ipv4 es decidir cuándo utilizar direcciones privadas y dónde se deben aplicar.

Se debe tener en cuenta lo siguiente:

¿Habrá más dispositivos conectados a la red que direcciones públicas asignadas por el ISP de la red?

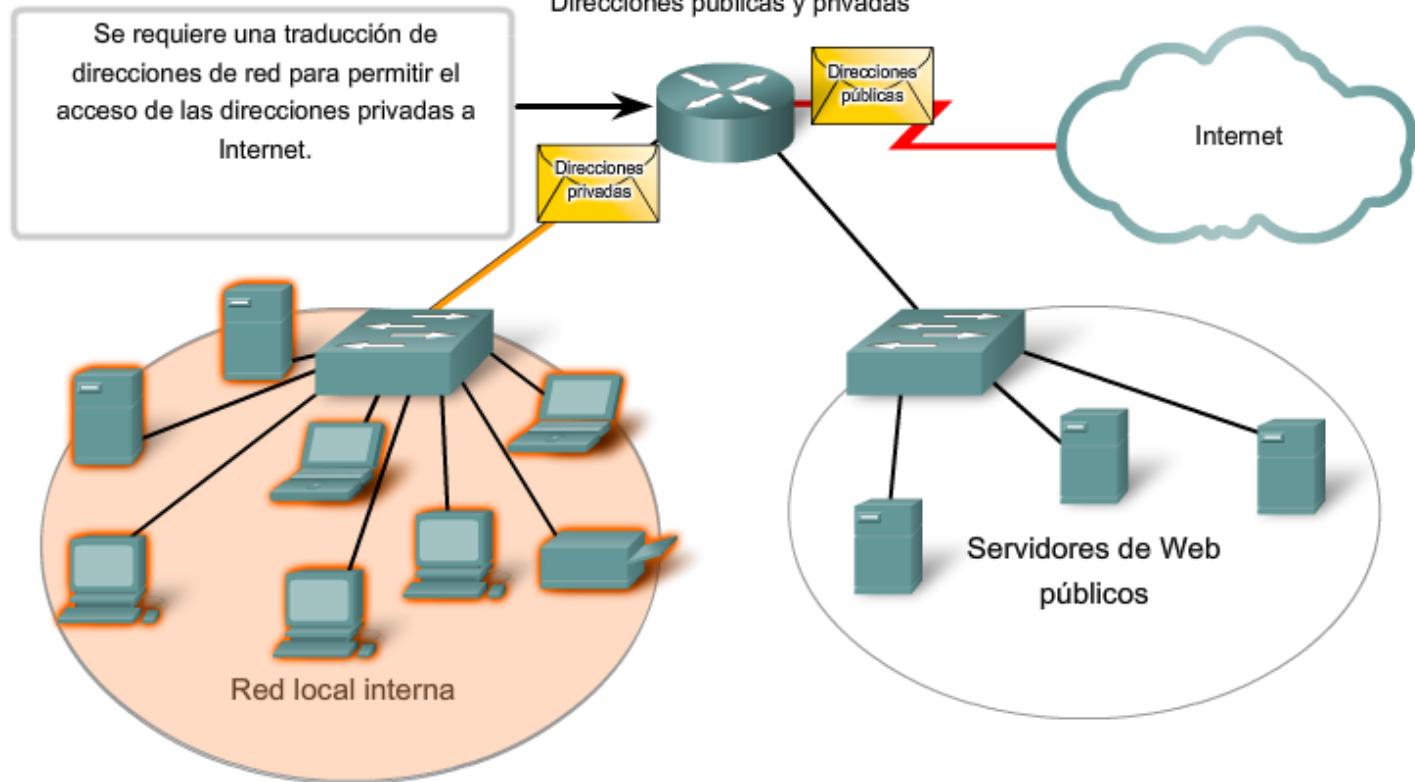
¿Se necesitará acceder a los dispositivos desde fuera de la red local?

Si los dispositivos a los que se pueden asignar direcciones privadas requieren acceso a Internet, ¿está la red capacitada para proveer el servicio de Traducción de dirección de red (NAT)?

Si hay más dispositivos que direcciones públicas disponibles, sólo esos dispositivos que accederán directamente a Internet, como los servidores Web, requieren una dirección pública. Un servicio NAT permitiría a esos dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.

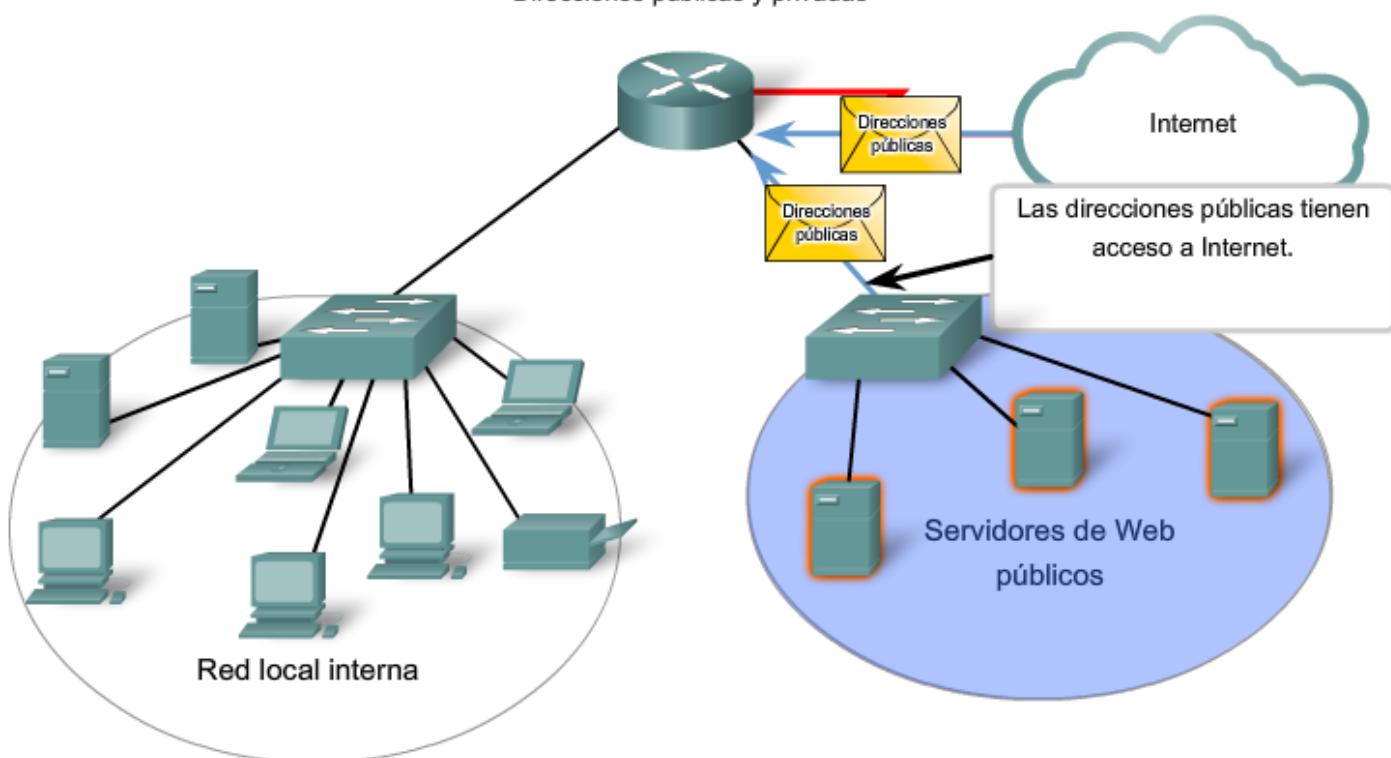
Planificación y asignación de direcciones IPv4

Direcciones públicas y privadas



Planificación y asignación de direcciones IPv4

Direcciones públicas y privadas



6.3.2 Direccionamiento estático y dinámico para dispositivos de usuario final

Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos IP, impresoras y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

Las direcciones IP pueden asignarse de manera estática o dinámica.

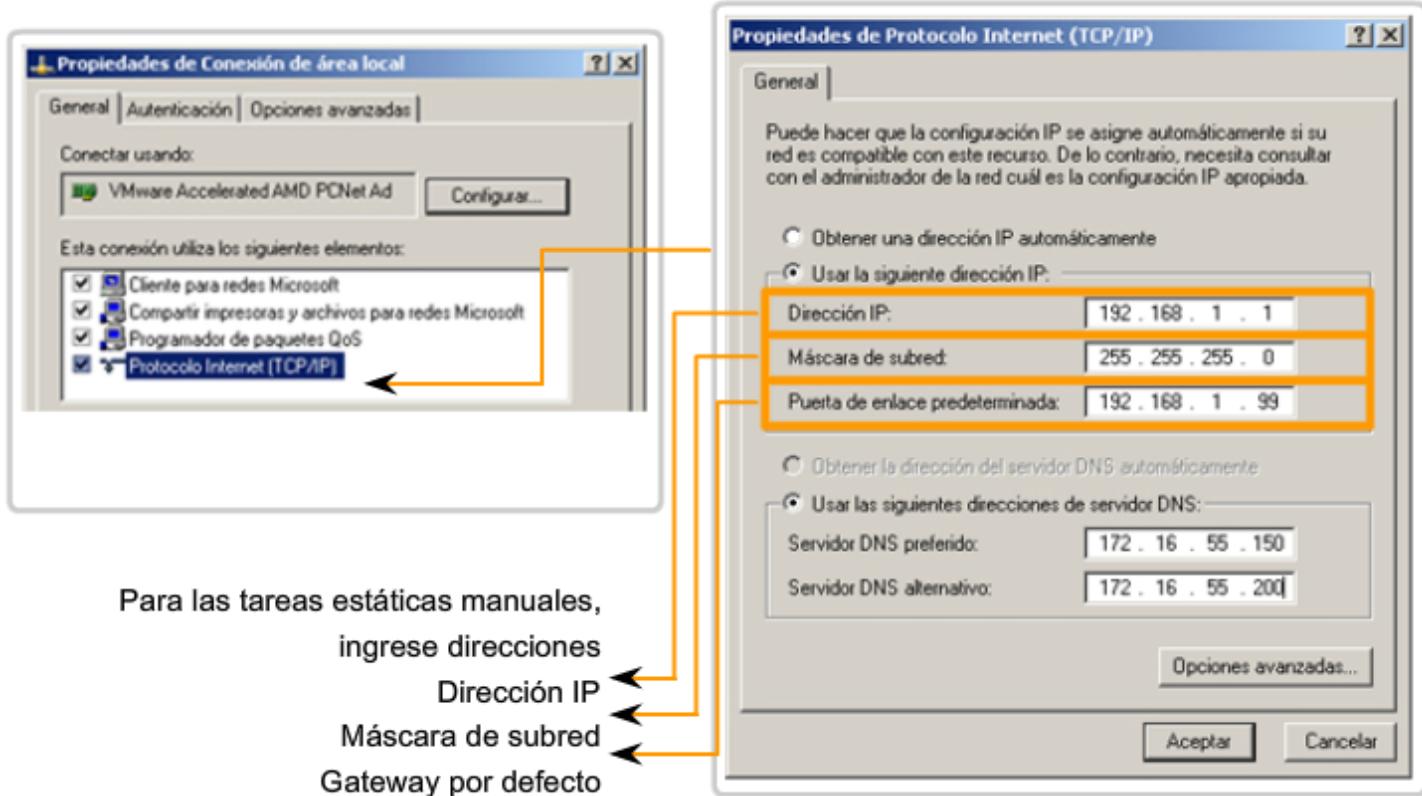
Asignación estática de direcciones

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto.

Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red. 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. Sin embargo, puede llevar mucho tiempo ingresar la información en cada host.

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.

Direccionamiento de dispositivos finales



Asignación dinámica de direcciones

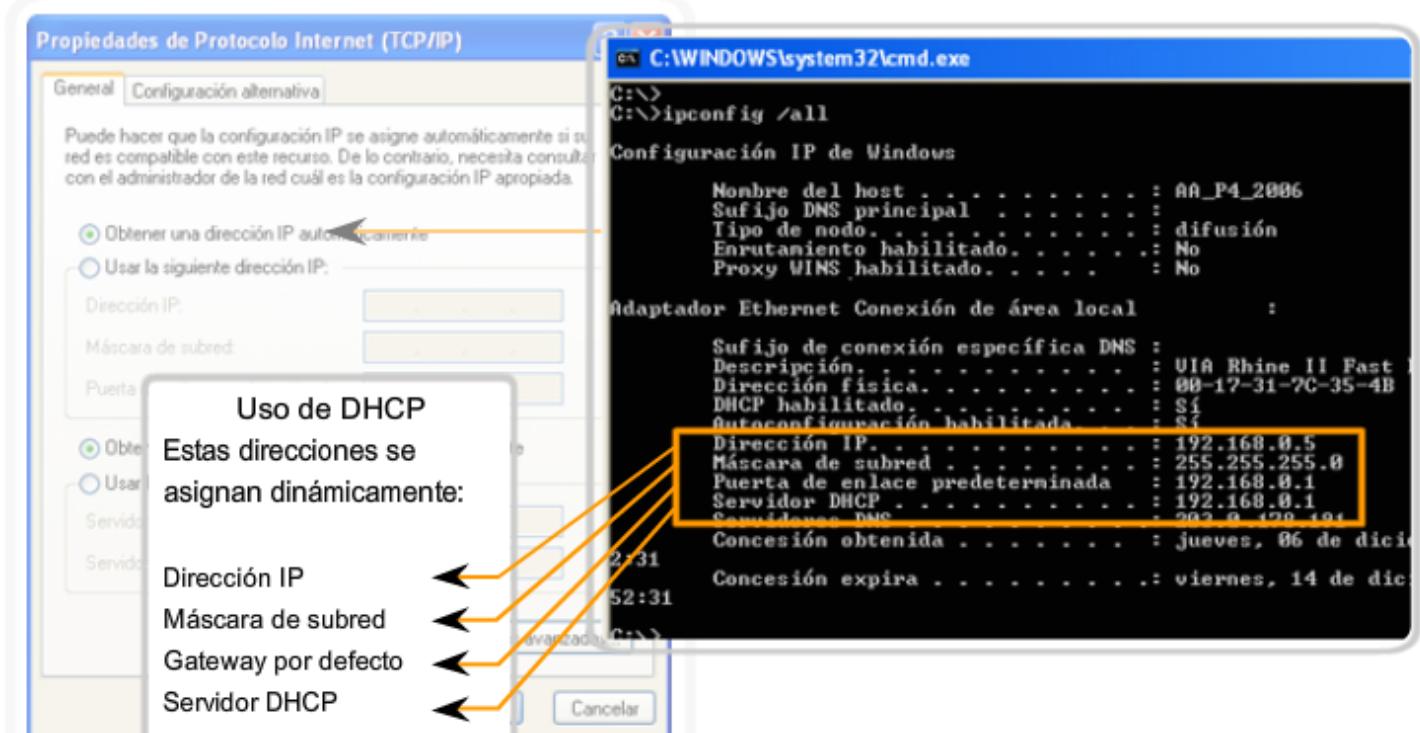
Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el Protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el 209ersión por defecto y otra información de configuración. La configuración del servidor DHCP requiere que un bloque de direcciones, llamado conjunto de direcciones, sea definido para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

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 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.

Asignación de direcciones dinámicas



6.3.3 Asignación de direcciones a otros dispositivos

Direcciones para servidores y periféricos

Cualquier recurso de red como un servidor o una impresora debe tener una dirección Ipv4 estática, como se muestra en la figura. Los hosts clientes acceden a estos recursos utilizando las direcciones Ipv4 de estos dispositivos. Por lo tanto, son necesarias 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 Ipv4 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 red. Casi todo el tráfico dentro de las 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 asigna direcciones de Capa 3. Ya sea para la administración del dispositivo o para su operación. Los dispositivos como hubs, switches y puntos de acceso inalámbricos no requieren direcciones Ipv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar, monitorear o resolver problemas de funcionamiento de la red, éstos deben tener direcciones asignadas.

Debido a que es necesario saber cómo comunicarse con dispositivos intermedios, éstos 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.

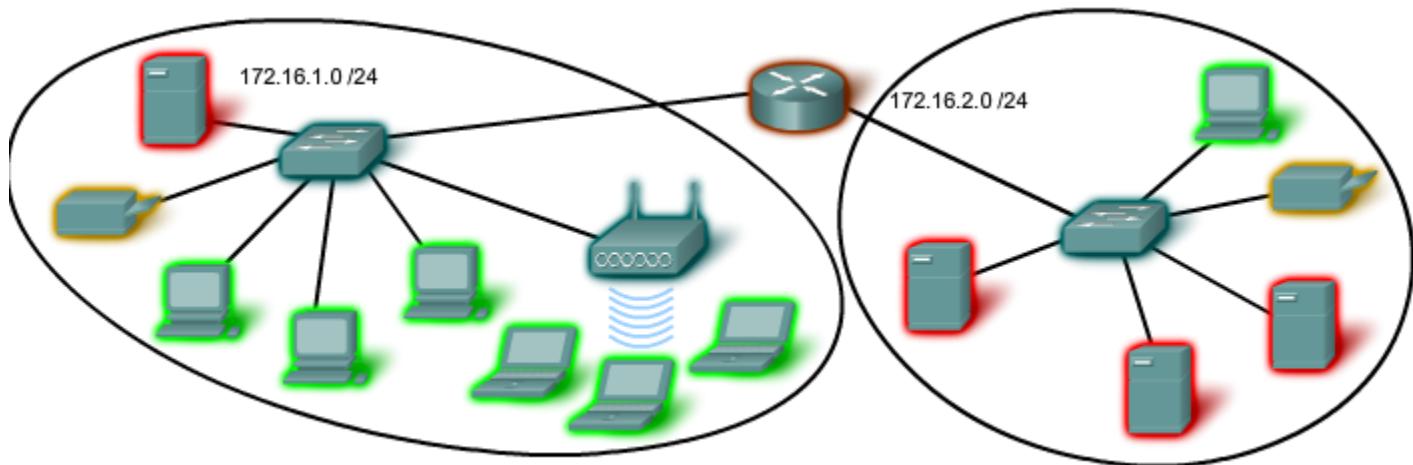
Routers y firewalls

A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall una dirección Ipv4 para cada interfaz. Cada interfaz se encuentra en una red diferente y funciona como una versión 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 dirección 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 una versión 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 Ipv4 de origen y destino. Agrupar los diferentes tipos de dispositivos en grupos de direccionamiento lógico hace que la asignación y el funcionamiento del filtrado de paquetes sea más eficiente.

Rangos de direcciones IP de los dispositivos

| Uso | Primera dirección | Última dirección | Dirección de resumen |
|----------------------------------|-------------------|------------------|----------------------|
| Dirección de red | 172.16.x.0 | | |
| Hosts de usuarios (pool de DHCP) | 172.16.x.1 | 172.16.x.127 | 172.16.x.0 /25 |
| Servidores | 172.16.x.128 | 172.16.x.191 | 172.16.x.128 /26 |
| Periféricos | 172.16.x.192 | 172.16.x.223 | 172.16.x.192 /27 |
| Dispositivos de red | 172.16.x.224 | 172.16.x.253 | |
| Router (gateway) | 172.16.x.254 | | 172.16.x.224 /27 |
| Broadcast | 172.16.x.255 | | |



6.3.4 ¿Quién asigna las diferentes direcciones?

Una compañía u organización que desea acceder a la red mediante hosts desde Internet debe tener un bloque de direcciones públicas asignado. El uso de estas direcciones públicas es regulado y la compañía u organización debe tener un bloque de direcciones asignado. Esto es lo que sucede con las direcciones Ipv4, Ipv6 y multicast.

Autoridad de números asignados a Internet (IANA) (<http://www.iana.net>) es un soporte maestro de direcciones IP. Las direcciones IP multicast y las direcciones Ipv6 se obtienen directamente de la IANA. 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 de África <http://www.afrinic.net>
- APNIC (Asia Pacific Network Information Centre) – Región de Asia/Pacífico <http://www.apnic.net>
- ARIN (American Registry for Internet Numbers) – Región de Norte América <http://www.arin.net>
- LACNIC (Registro de dirección IP de la Regional Latinoamericana y del Caribe) – 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>

Enlaces:

asignaciones de registros de direcciones Ipv4:

<http://www.ietf.org/rfc/rfc1466.txt?number=1466>

<http://www.ietf.org/rfc/rfc2050.txt?number=2050>

Asignación de direcciones Ipv4: <http://www.iana.org/ipaddress/ip-addresses.htm>

Búsqueda de direccionamiento IP: <http://www.arin.net/whois/>

| IANA | | | | | |
|---|------------------|--------------------------|--------------------------------------|-----------------------------|---|
| Global | AfriNIC | APNIC | LACNIC | ARIN | RIPE NCC |
| Registros de Internet regionales | Región de África | Asia/Región del Pacífico | Región de América Latina y el Caribe | Región de América del Norte | Europa, Medio Oriente, Región de Asia Central |

6.3.5 Proveedores de servicios de Internet (ISP)

El papel de 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.

Servicios 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 servicios que un ISP generalmente ofrece a sus clientes se encuentran los servicios DNS, servicios de correo electrónico y un sitio Web. Dependiendo del nivel de servicio requerido y disponible, los clientes usan diferentes niveles de un ISP.

ISP Tiers

Los ISP son designados por una jerarquía basada en su nivel de conectividad a la 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 la figura.

Nivel 1

En la parte superior de la jerarquía de ISP están los ISP de nivel 1. Éstos 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

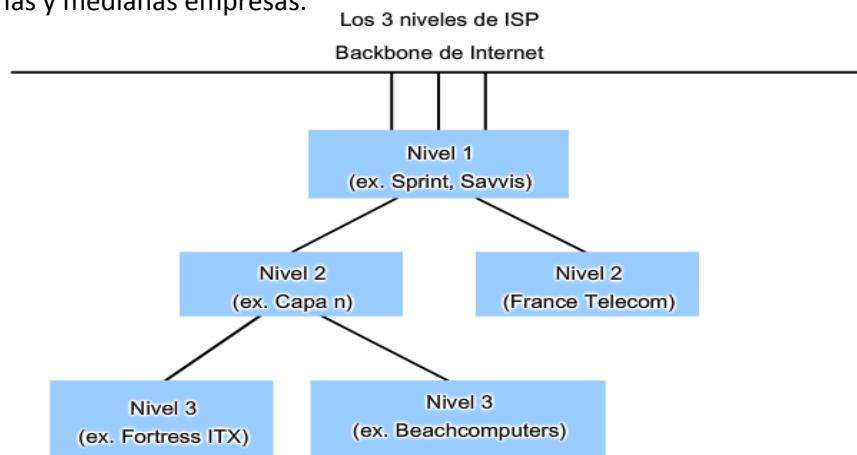
Los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1. Los ISP de nivel 2 generalmente se centran en los clientes empresa. Los ISP de nivel 2 normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus 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 backbone de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1.

Nivel 3

Los ISP de nivel 3 compran 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.



6.3.6 Direccionamiento IPv6

A principios de los años noventa, el Grupo de trabajo de ingeniería de Internet (IETF) centró su interés en el agotamiento de direcciones de red Ipv4 y comenzó a buscar un reemplazo para este protocolo. Esta actividad produjo el desarrollo de lo que hoy se conoce como Ipv6.

Crear mayores capacidades de direccionamiento fue la motivación inicial para el desarrollo de este nuevo protocolo. También se consideraron otros temas durante el desarrollo de Ipv6, como:

- Manejo mejorado de paquetes
- Escalabilidad y longevidad mejoradas
- Mecanismos QoS (Calidad del Servicio)
- Seguridad integrada

Para proveer estas características, Ipv6 ofrece:

- Direccionamiento jerárquico de 128 bits: para expandir las capacidades de direccionamiento
- Simplificación del formato de encabezado: para mejorar el manejo de paquetes
- Soporte mejorado para extensiones y opciones: para escalabilidad/longevidad mejoradas y manejo mejorado de paquetes
- Capacidad de rotulado de flujo: como mecanismos QoS
- Capacidades de autenticación y privacidad: para integrar la seguridad

Ipv6 no es meramente un nuevo protocolo de Capa 3: es un nuevo conjunto de aplicaciones de protocolo Se han desarrollado nuevos protocolos en varias capas del stack para admitir este nuevo protocolo. Hay un nuevo protocolo de mensajería (ICMPv6) y nuevos protocolos de enrutamiento. Debido al mayor tamaño del encabezado de Ipv6, también repercute en la infraestructura de red subyacente.

Transición a Ipv6

Como se puede ver en esta breve introducción, Ipv6 ha sido diseñado con escalabilidad para permitir años de crecimiento de la internetwork. Sin embargo, Ipv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, Ipv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro. Sin embargo, Ipv6 podrá eventualmente reemplazar a Ipv4 como protocolo de Internet dominante.

Enlaces:

Ipv6: <http://www.ietf.org/rfc/rfc2460.txt?number=2460>

direccionamiento Ipv6: <http://www.ietf.org/rfc/rfc3513.txt?number=3513>

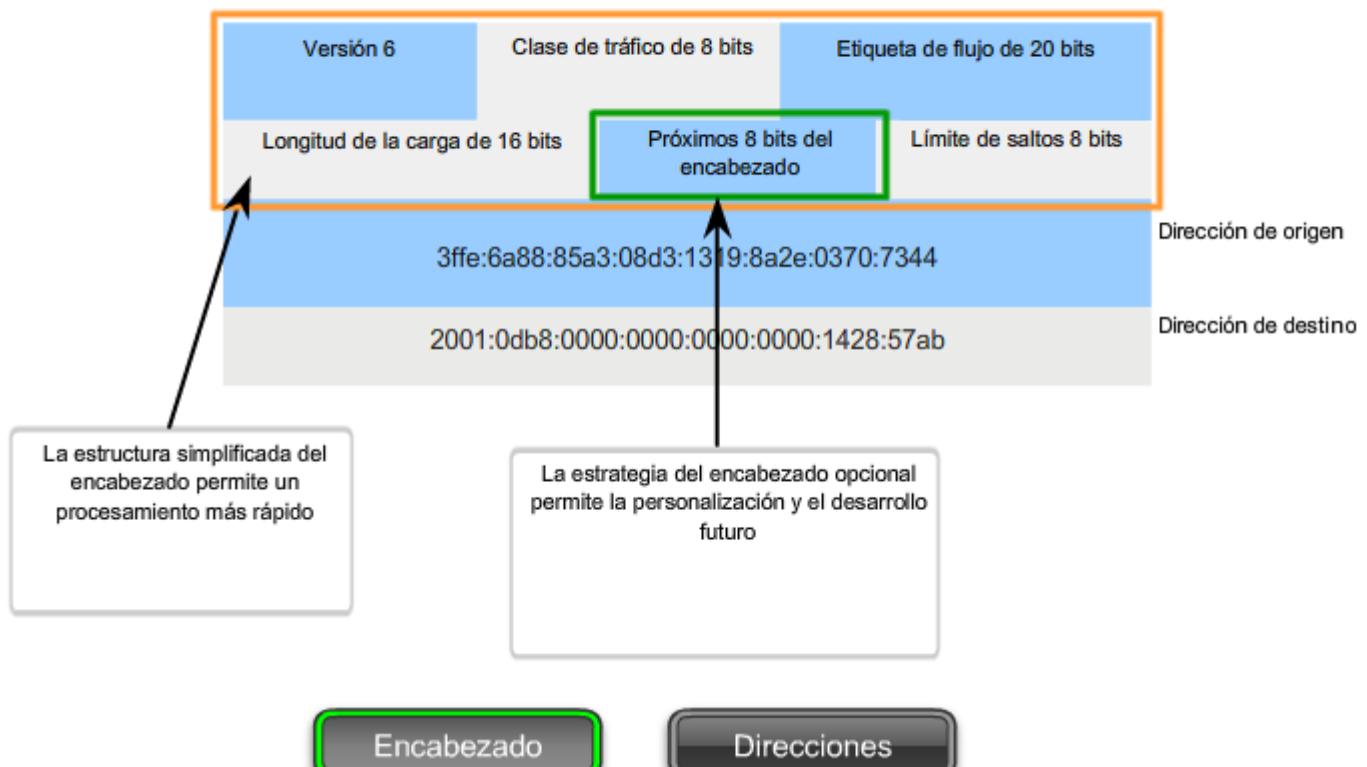
seguridad Ipv6: <http://www.ietf.org/rfc/rfc2401.txt?number=2401>

seguridad Ipv6: <http://www.ietf.org/rfc/rfc3168.txt?number=3168>

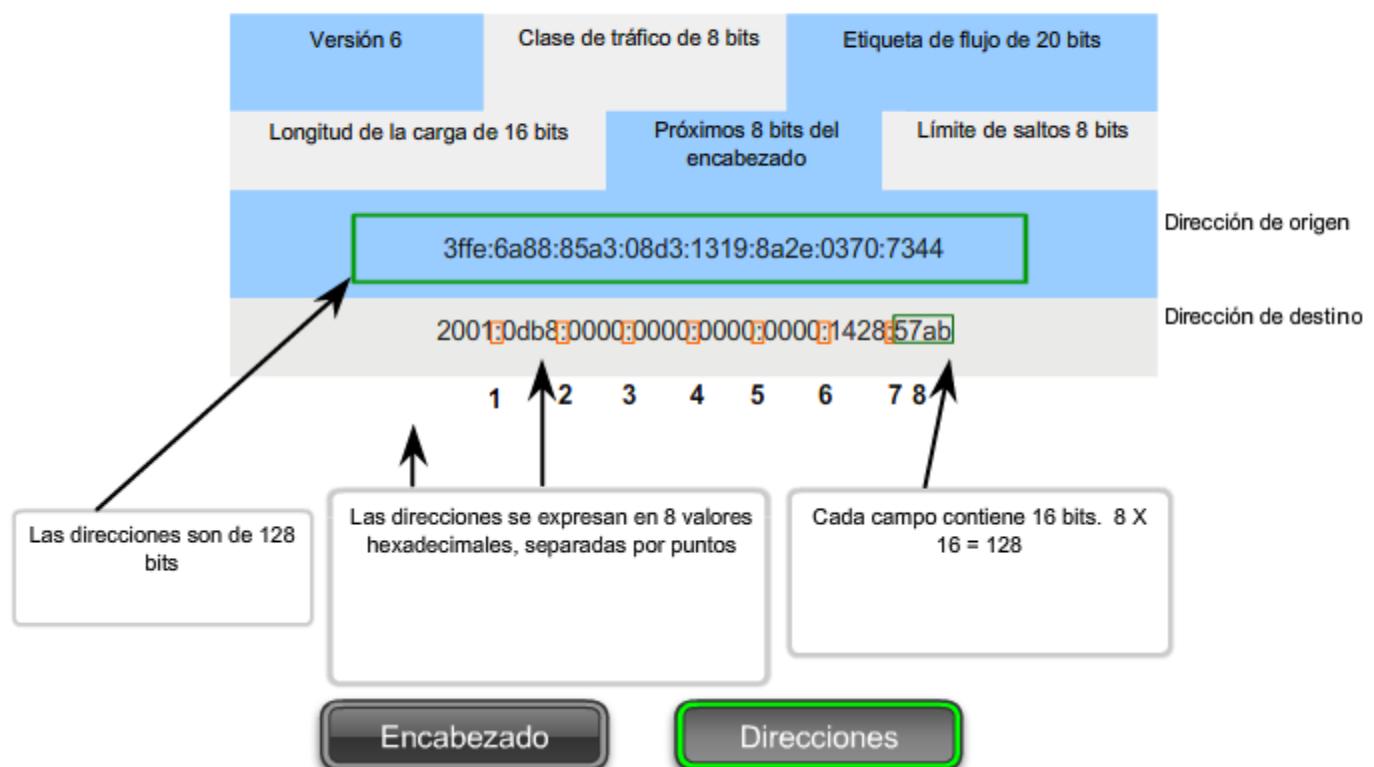
seguridad Ipv6: <http://www.ietf.org/rfc/rfc4302.txt?number=4302>

ICMPv6: <http://www.ietf.org/rfc/rfc4443.txt?number=4443>

Encabezado IPv6



Encabezado IPv6



6.4 ¿ESTÁ EN MI RED?

6.4.1 Máscara de subred: definición de las porciones de red y host

Como se enseñó anteriormente, una dirección Ipv4 tiene una porción de red y una porción de host. Se hizo referencia a la duración del prefijo como la cantidad de bits en la dirección que conforma la porción de red. El prefijo es una forma de definir la porción de red para que los humanos la pueden leer. La red de datos también debe tener esta porción de red de las direcciones definidas.

Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred, como se muestra en la figura. La máscara de subred se expresa con el mismo formato decimal punteado que la dirección Ipv4. 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.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Como se muestra en la figura, un prefijo /24 se expresa como máscara de subred de esta forma 255.255.255.0 (11111111.11111111.11111111.00000000). Los bits restantes (orden inferior) de la máscara de subred son números cero, que indican la dirección host dentro de la red.

La máscara de subred se configura en un host junto con la dirección Ipv4 para definir la porción de red de esa dirección.

Por ejemplo: veamos el host 172.16.4.35/27:

dirección

172.16.20.35

10101100.00010000.00010100.00100011

máscara de subred

255.255.255.224

11111111.11111111.11111111.11100000

dirección de red

172.16.20.32

10101100.00010000.00010100.00100000

Como los bits de orden superior de las máscaras de subred son contiguos números 1, existe solamente un número limitado de valores de subred dentro de un octeto. Sólo es necesario ampliar un octeto si la división de red y host entra en dicho octeto. Por lo tanto, se usan patrones de 8 bits limitados en las máscaras de subred.

Estos patrones son:

00000000 = 0

10000000 = 128

11000000 = 192

11100000 = 224

11110000 = 240

11111000 = 248

11111100 = 252

11111110 = 254

11111111 = 255

Si la máscara de subred de un octeto está representada por 255, entonces todos los bits equivalentes de ese octeto de la dirección son bits de red. De igual manera, si la máscara de subred de un octeto está representada por 0, entonces todos los bits equivalentes de ese octeto de la dirección son bits de host. En cada uno de estos casos, no es necesario ampliar este octeto a binario para determinar las porciones de red y host.

Porciones de red y de hosts de una dirección IP

Estos valores se encuentran en la porción de red de la dirección. Pueden ser "0" o "1".

Dirección IP

| | | | | | | |
|----------|---|----------|---|----------|---|----------|
| 172 | . | 16 | . | 4 | . | 1 |
| 10101100 | | 00010000 | | 00000100 | | 00000001 |

Máscara de subred

| | | | | | | |
|----------|---|----------|---|----------|---|----------|
| 255 | . | 255 | . | 255 | . | 0 |
| 11111111 | | 11111111 | | 11111111 | | 00000000 |

Prefijo /24 (24 bits de orden superior)

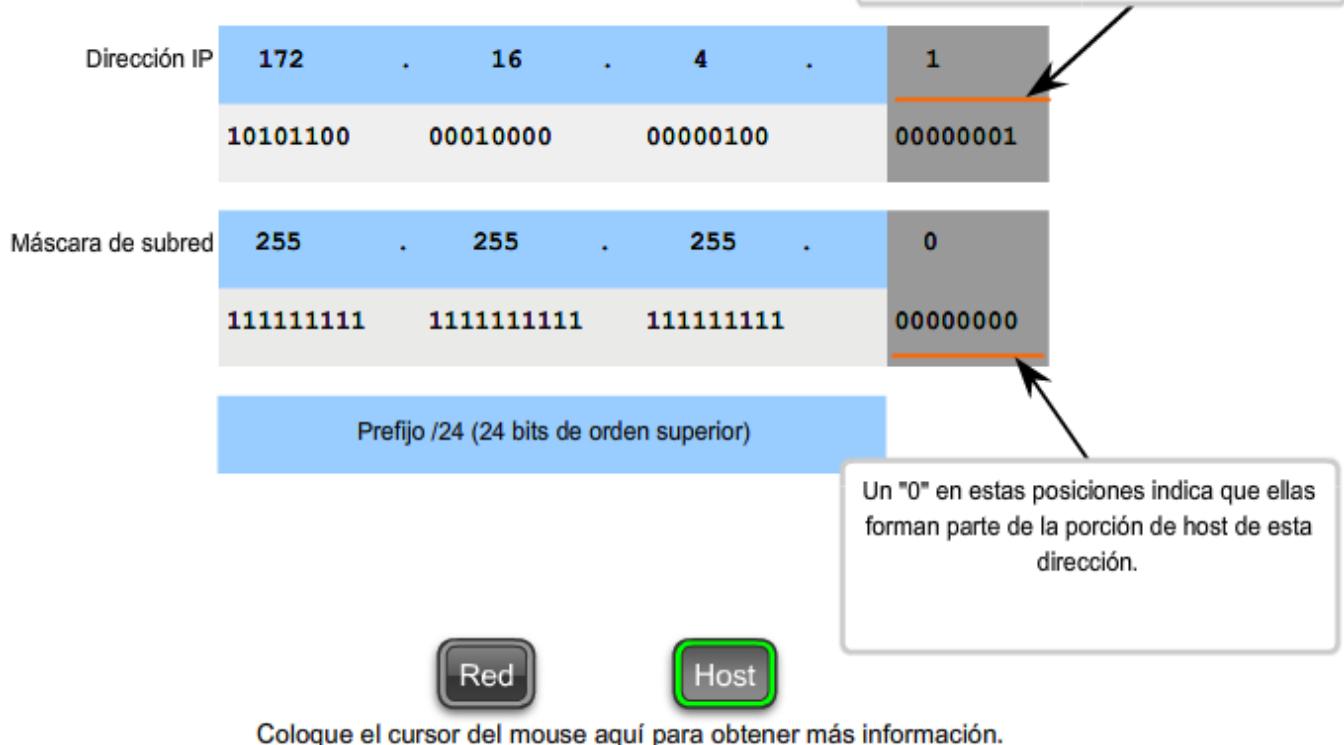
Un "1" en estas posiciones indica que ellas forman parte de la porción de red de esta dirección.

Red

Host

Coloque el cursor del mouse aquí para obtener más información.

Porciones de red y de hosts de una dirección IP



6.4.2 Lógica AND ¿Qué hay en nuestra red?

Dentro de los dispositivos de redes de datos, se aplica la lógica digital para interpretar las direcciones. Cuando se crea o envía un paquete Ipv4, la dirección de red de destino debe obtenerse de la dirección de destino. Esto se hace por medio de una lógica llamada AND.

Se aplica la lógica AND a la dirección host Ipv4 y a su máscara de subred para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND a la dirección y a la máscara de subred, el resultado que se produce es la dirección de red.

Operación AND

AND es una de las tres operaciones binarias básicas utilizadas 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:

$$11.. \text{ AND } 1 = 1$$

$$11.. \text{ AND } 0 = 0$$

$$0 \text{ AND } 1 = 0$$

$$0 \text{ AND } 0 = 0$$

El resultado de la aplicación de AND con 1 en cualquier caso produce un resultado que es el bit original. Es decir, 0 AND 1 es 0 y 1 AND 1 es 1. En consecuencia, la aplicación de AND con 0 en cualquier caso produce un 0. Estas propiedades de la aplicación de AND se usan 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.

De igual manera, 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 dirección originales.

Motivos para utilizar AND

La aplicación de AND a la dirección host y a la máscara de subred se realiza mediante dispositivos en una red de datos por diversos motivos.

Los routers usan AND para determinar una ruta aceptable para un paquete entrante. El router verifica la dirección de destino e intenta asociarla con un salto siguiente. Cuando llega un paquete a un router, éste realiza el procedimiento de aplicación de AND en la dirección IP de destino en el paquete entrante y con la máscara de subred de las rutas posibles. De esta forma, se obtiene una dirección de red que se compara con la ruta de la tabla de enrutamiento de la cual se usó la máscara de subred.

Un host de origen debe determinar si un paquete debe ser directamente enviado a un host en la red local o si debe ser dirigido al 219ersión. Para tomar esta determinación, un host primero debe conocer su propia dirección de red.

Un host obtiene su dirección de red al aplicar la lógica AND a la dirección con la máscara de subred. La lógica AND también es llevada a cabo por un host de origen entre la dirección de destino del paquete y la máscara de subred de este host. Esto produce la dirección de red de destino. Si esta dirección de red coincide con la dirección de red del host local, el paquete es directamente enviado al host de destino. Si las dos direcciones de red no coinciden, el paquete es enviado al 219ersión.

La importancia de AND

Si los routers y dispositivos finales calculan estos procesos sin la intervención de nadie, ¿por qué debemos aprender acerca de AND? Cuanto más comprendamos y podamos predecir sobre el funcionamiento de una red, más equipados estaremos para diseñar y administrar una.

En la verificación/resolución de problemas de una red, a menudo es necesario determinar en qué red Ipv4 se encuentra un host o si dos hosts se encuentran en la misma red IP. 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.

Además, un router puede tener diferentes rutas que pueden realizar el envío de un paquete a un determinado destino. La selección de la ruta utilizada para cualquier paquete es una operación compleja. Por ejemplo: el prefijo que forma estas rutas no se asocia directamente con las redes asignadas al host. Esto significa que una ruta de la tabla de enrutamiento puede representar muchas redes. Si se produjeron inconvenientes con los paquetes de enrutamiento, podrá ser necesario determinar cómo el router tomaría la decisión del enrutamiento.

A pesar de que se dispone de calculadoras de subredes, es útil para un administrador de red saber calcular subredes manualmente.

Nota: No se permite el uso de calculadoras de ningún tipo durante los exámenes de certificación.

Aplicación de la máscara de subred
Un dispositivo con la dirección 192.0.0.1 pertenece a la red 192.0.0.0

| | | | | | | | |
|-------------------|----------|----------|----------|----------|---|---|---|
| | 192 | . | 0 | . | 0 | . | 1 |
| Dirección de host | 11000000 | 00000000 | 00000000 | 00000001 | | | |
| Máscara de subred | 255 | 255 | 0 | 0 | | | |
| | 11111111 | 11111111 | 00000000 | 00000000 | | | |
| Dirección de red | 11000000 | 00000000 | 00000000 | 00000000 | | | |
| Red | 192 | . | 0 | . | 0 | . | 0 |

1 en el host AND 1 en la máscara indica 1 en la dirección de red.

1 y 1

0 y 1

0 y 0

1 y 0

Coloque el cursor del mouse para ver la operación AND.

| | | | | | | | |
|-------------------|----------|----------|----------|----------|---|---|---|
| | 192 | . | 0 | . | 0 | . | 1 |
| Dirección de host | 11000000 | 00000000 | 00000000 | 00000001 | | | |
| Máscara de subred | 255 | 255 | 0 | 0 | | | |
| | 11111111 | 11111111 | 00000000 | 00000000 | | | |
| Dirección de red | 11000000 | 00000000 | 00000000 | 00000000 | | | |
| Red | 192 | . | 0 | . | 0 | . | 0 |

0 en el host AND 1 en la máscara indica 0 en la dirección de red.

1 y 1

0 y 1

0 y 0

1 y 0

Coloque el cursor del mouse para ver la operación AND.

| | | | | | | | |
|-------------------|----------|----------|----------|----------|---|---|---|
| | 192 | . | 0 | . | 0 | . | 1 |
| Dirección de host | 11000000 | 00000000 | 00000000 | 00000001 | | | |
| Máscara de subred | 255 | 255 | 0 | 0 | | | |
| | 11111111 | 11111111 | 00000000 | 00000000 | | | |
| Dirección de red | 11000000 | 00000000 | 00000000 | 00000000 | | | |
| Red | 192 | . | 0 | . | 0 | . | 0 |

0 en el host AND 0 en la máscara indica 0 en la dirección de red.

1 y 1

0 y 1

0 y 0

1 y 0

Coloque el cursor del mouse para ver la operación AND.

| | | | | | | | |
|-------------------|----------|----------|----------|----------|---|---|---|
| | 192 | . | 0 | . | 0 | . | 1 |
| Dirección de host | 11000000 | 00000000 | 00000000 | 00000001 | | | |
| Máscara de subred | 255 | 255 | 0 | 0 | | | |
| | 11111111 | 11111111 | 00000000 | 00000000 | | | |
| Dirección de red | 11000000 | 00000000 | 00000000 | 00000000 | | | |
| Red | 192 | . | 0 | . | 0 | . | 0 |

1 en el host Y 0 en la máscara coloca 0 en la dirección de red.

1 y 1

0 y 1

0 y 0

1 y 0

Coloque el cursor del mouse para ver la operación AND.

6.4.3 El proceso de aplicación del AND

La operación AND se aplica a cada bit de la dirección binaria.

Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Dirección host

172

16

132

70

Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Convierta la dirección host en binaria

| | | | | |
|------------------------|----------|----------|----------|----------|
| Dirección host | 172 | 16 | 132 | 70 |
| Dirección host binaria | 10101100 | 00010000 | 10000100 | 01000110 |

Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

El bit más significativo de AND de la dirección host
con el bit más significativo de la máscara

| | | | | |
|---------------------------|----------|----------|----------|----------|
| Dirección host | 172 | 16 | 132 | 70 |
| Dirección host binaria | 10101100 | 00010000 | 10000100 | 01000110 |
| Máscara de subred binaria | 11111111 | 11111111 | 11110000 | 00000000 |

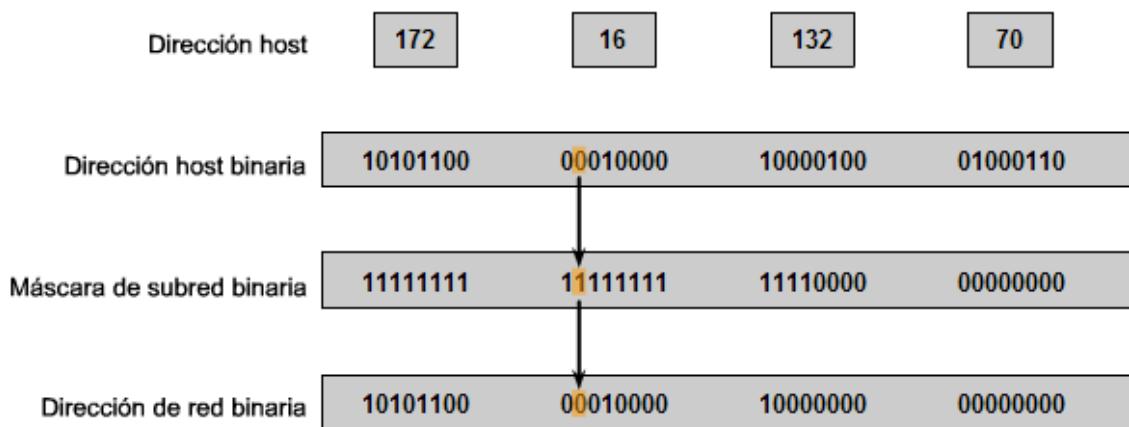
Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Convierta el prefijo /20 en una máscara de subred binaria

| | | | | |
|---------------------------|----------|----------|----------|----------|
| Dirección host | 172 | 16 | 132 | 70 |
| Dirección host binaria | 10101100 | 00010000 | 10000100 | 01000110 |
| Máscara de subred binaria | 11111111 | 11111111 | 11110000 | 00000000 |
| Dirección de red binaria | 10101100 | 00010000 | 10000000 | 00000000 |

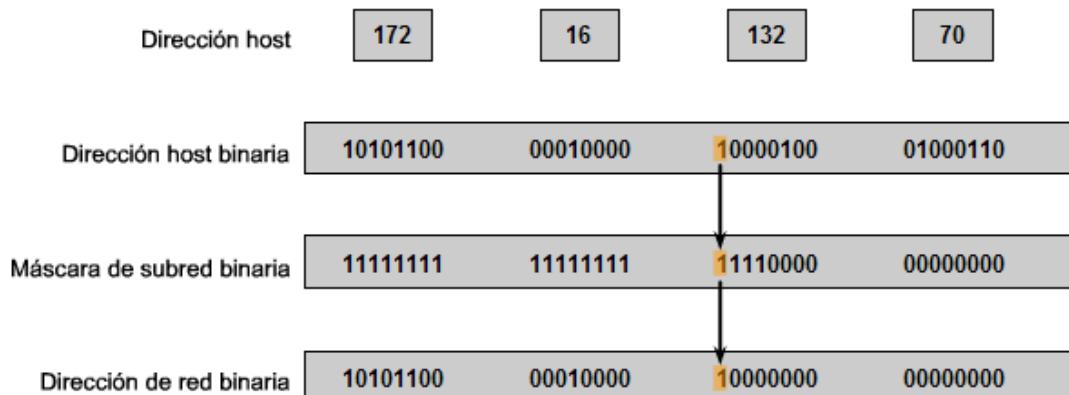
Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

El próximo bit más significativo de AND de la dirección host con el próximo bit más significativo de la máscara



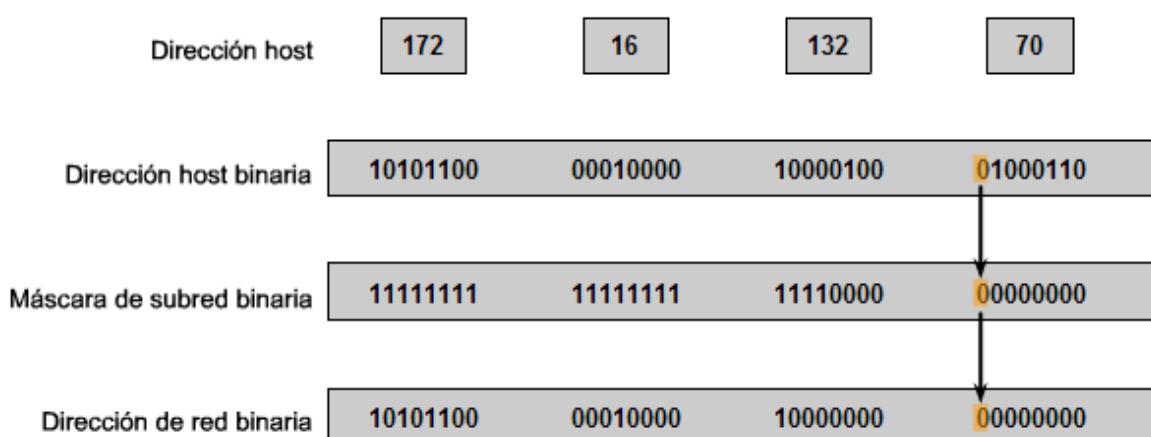
Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Continúe realizando la operación AND con cada bit de la dirección host con el bit "1" correspondiente de la máscara



Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Realice la operación AND con cada bit de la dirección host con el bit "0" correspondiente de la máscara



Utilice la máscara de subred para determinar la dirección de red para el host 172.16.132.70/20.

Convierta la dirección de red binaria en decimal

| | | | | |
|---------------------------|----------|----------|----------|----------|
| Dirección host | 172 | 16 | 132 | 70 |
| Dirección host binaria | 10101100 | 00010000 | 10000100 | 01000110 |
| Máscara de subred binaria | 11111111 | 11111111 | 11110000 | 00000000 |
| Dirección de red binaria | 10101100 | 00010000 | 10000000 | 00000000 |
| Dirección de red | 172 | 16 | 128 | 0 |

6.5 CÁLCULO DE DIRECCIONES

6.5.1 Principios de división en subredes

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Creamos las subredes utilizando uno o más de los bits del host como bits de la 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. Cuanto más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

El router A en la figura posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es “0” y para la otra subred, este bit es “1”.

Fórmula para calcular subredes

Use esta fórmula para calcular la cantidad de subredes:

2^n donde n = la cantidad de bits que se tomaron prestados

En este ejemplo, el cálculo es así:

$2^1 = 2$ subredes

La cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula $2^n - 2$ donde n = la cantidad de bits para hosts.

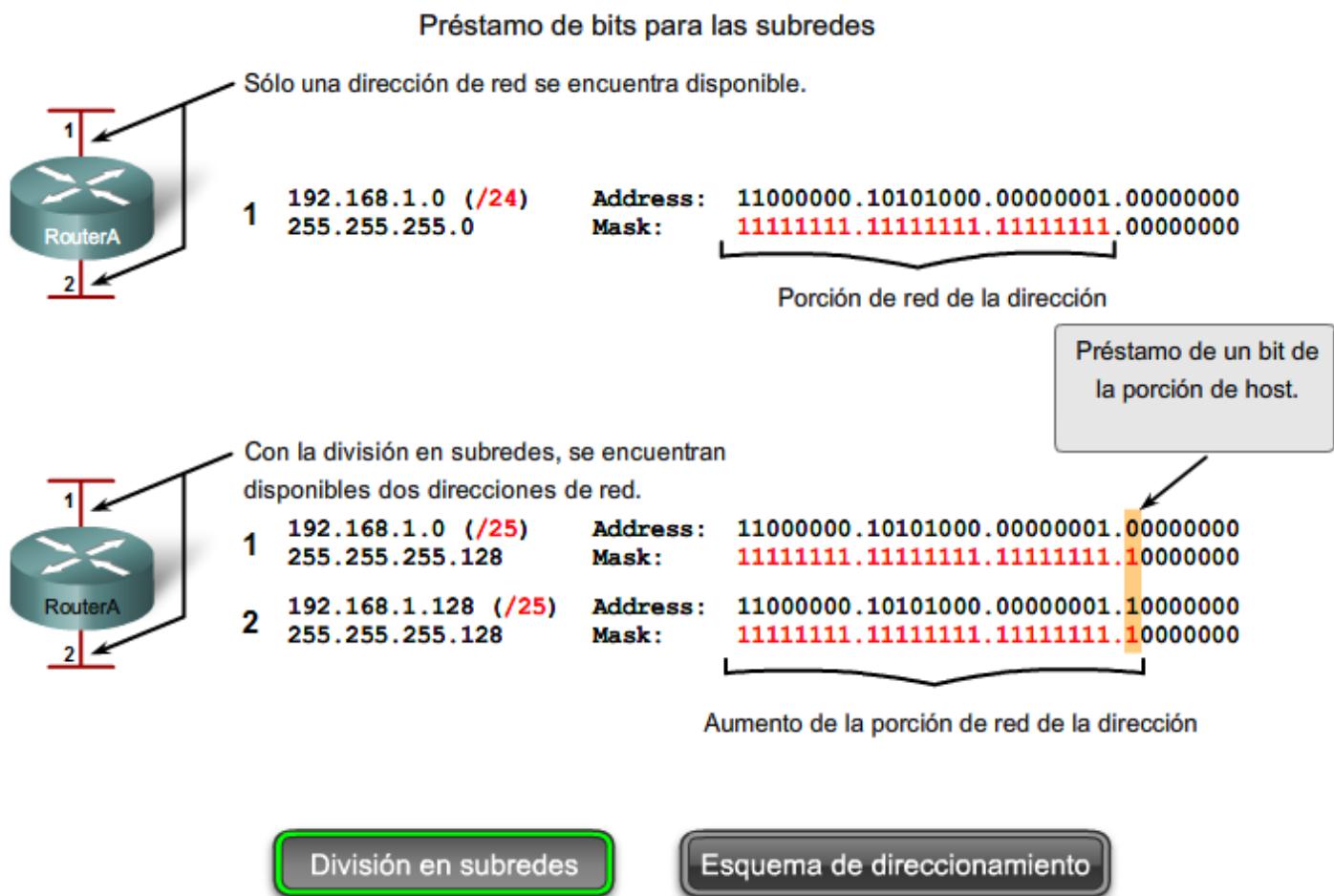
La aplicación de esta fórmula, ($2^7 - 2 = 126$) muestra que cada una de estas subredes puede tener 126 hosts.

En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: 00000000 = 0

Subred 2: 10000000 = 128

Vea la figura para conocer el esquema de direccionamiento para estas redes.



Esquema de direccionamiento: Ejemplo de 2 redes

| Subred | Dirección de red | Rango de host | Dirección de broadcast |
|--------|------------------|-------------------------------|------------------------|
| 0 | 192.168.1.0/25 | 192.168.1.1 – 192.168.1.126 | 192.168.1.127 |
| 1 | 192.168.1.128/25 | 192.168.1.129 – 192.168.1.254 | 192.168.1.255 |

Ejemplo con 3 subredes

A continuación, piense en una internetwork que requiere tres subredes. Vea la figura.

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24. Tomar prestado un solo bit proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits. Esto proveerá cuatro subredes.

Calcule la subred con esta fórmula:

$2^2 = 4$ subredes

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

Subred 0: 0 = **00000000**

Subred 1: 64 = **01000000**

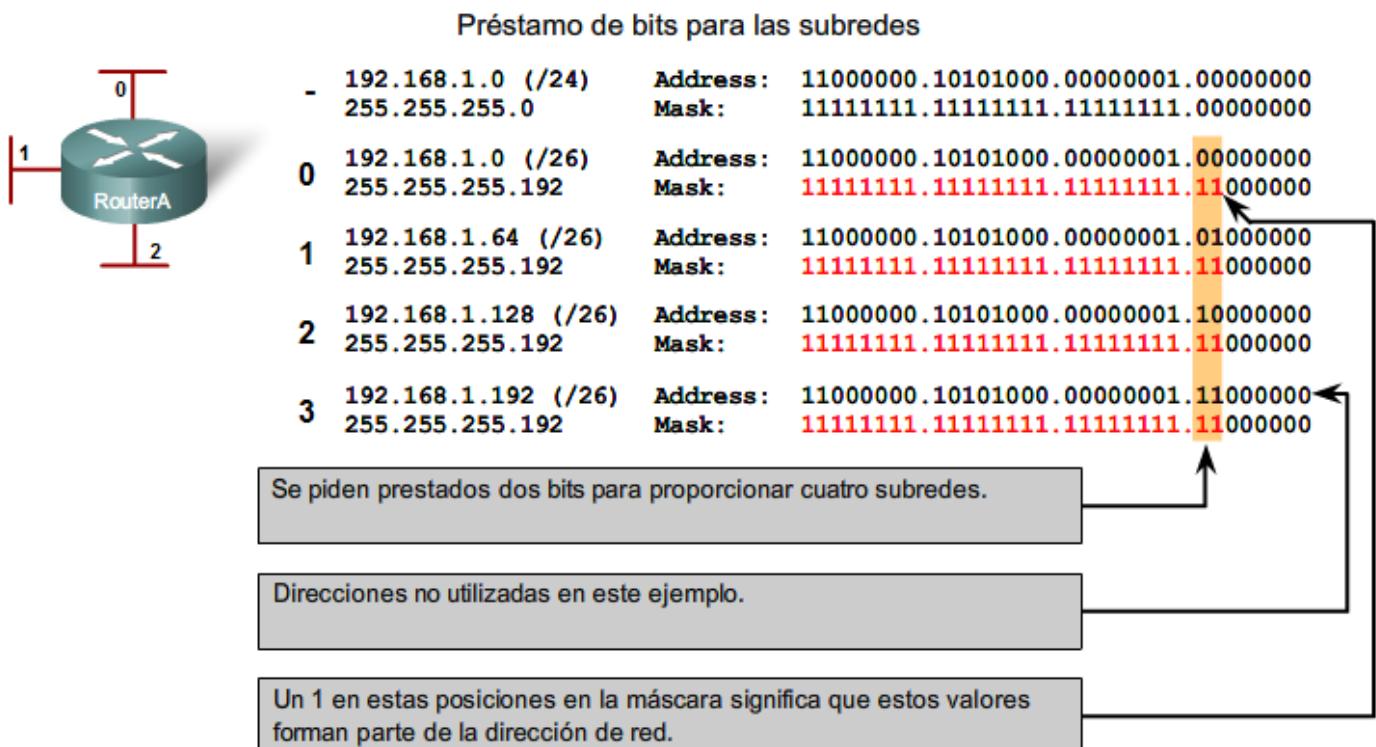
Subred 2: 128 = **10000000**

Subred 3: 192 = **11000000**

Aplique la fórmula de cálculo de host.

$2^6 - 2 = 62$ hosts por subred

Observe la figura del esquema de direccionamiento para estas redes.



Se encuentran disponibles más subredes, pero menos direcciones se encuentran disponibles por subred.

[División en subredes](#)

[Esquema de direccionamiento](#)

Esquema de direccionamiento: Ejemplo de 4 redes

| Subred | Dirección de red | Rango de host | Dirección de broadcast |
|--------|------------------|-------------------------------|------------------------|
| 0 | 192.168.1.0/26 | 192.168.1.1 – 192.168.1.62 | 192.168.1.63 |
| 1 | 192.168.1.64/26 | 192.168.1.65 – 192.168.1.126 | 192.168.1.127 |
| 2 | 192.168.1.128/26 | 192.168.1.129 – 192.168.1.190 | 192.168.1.191 |
| 3 | 192.168.1.192/26 | 192.168.1.193 – 192.168.1.254 | 192.168.1.255 |

Ejemplo con 6 subredes

Considere este ejemplo con cinco LAN y una WAN para un total de 6 redes. Observe la figura.

Para incluir 6 redes, coloque la subred 192.168.1.0 /24 en bloques de direcciones mediante la fórmula:

$$2^3 = 8$$

Para obtener al menos 6 subredes, pida prestados tres bits de host. Una máscara de subred 255.255.255.224 proporciona los tres bits de red adicionales.

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

$$0 = \textbf{000}00000$$

$$32 = \textbf{001}00000$$

$$64 = \textbf{010}00000$$

$$96 = \textbf{011}00000$$

$$128 = \textbf{100}00000$$

$$160 = \textbf{101}00000$$

$$192 = \textbf{110}00000$$

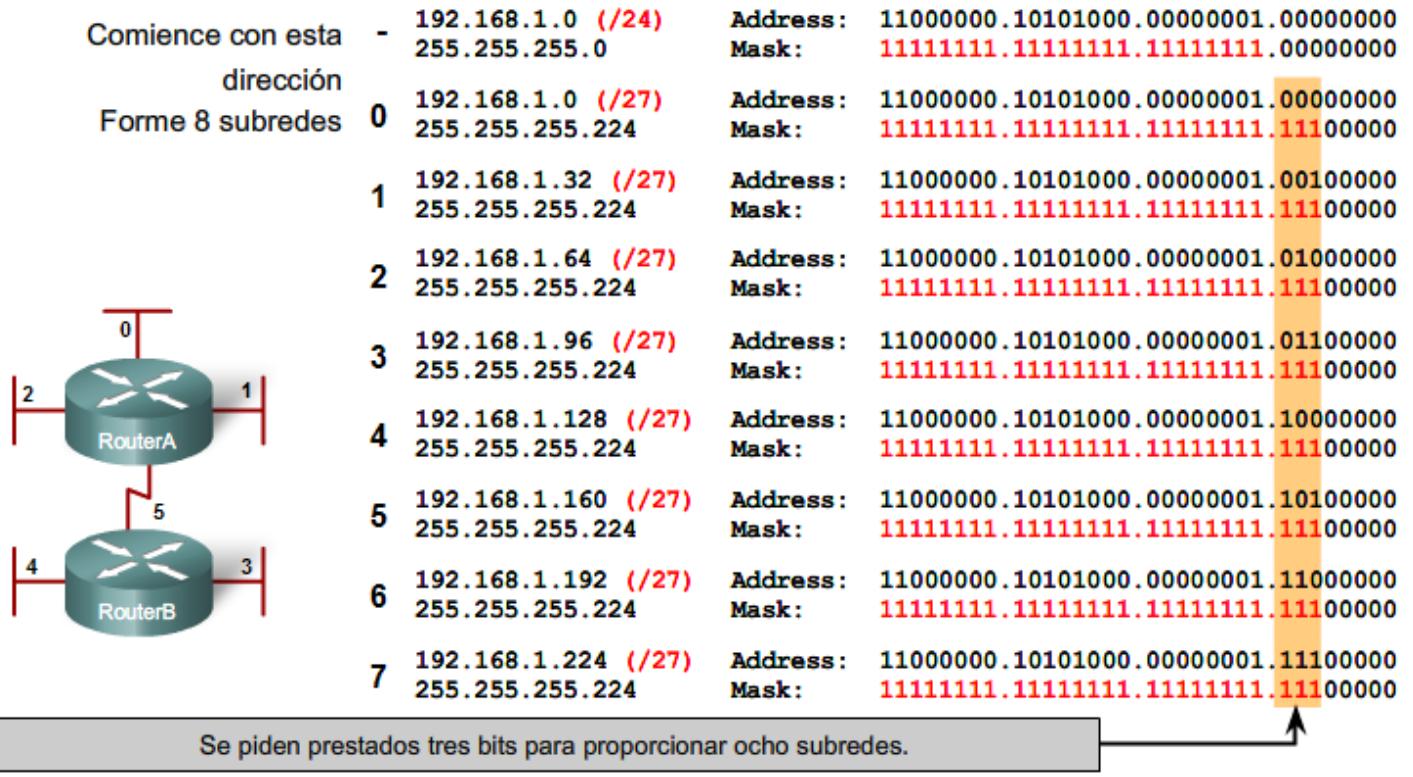
$$224 = \textbf{111}00000$$

Aplique la fórmula de cálculo de host:

$$2^5 - 2 = 30 \text{ hosts por subred.}$$

Observe la figura del esquema de direccionamiento para estas redes.

Préstamo de bits para las subredes



División en subredes

Esquema de direccionamiento

Esquema de direccionamiento: Ejemplo de 6 redes

| Subred | Dirección de red | Rango de host | Dirección de broadcast |
|--------|------------------|-------------------------------|------------------------|
| 0 | 192.168.1.0/27 | 192.168.1.1 – 192.168.1.30 | 192.168.1.31 |
| 1 | 192.168.1.32/27 | 192.168.1.33 – 192.168.1.62 | 192.168.1.63 |
| 2 | 192.168.1.64/27 | 192.168.1.65 – 192.168.1.94 | 192.168.1.95 |
| 3 | 192.168.1.96/27 | 192.168.1.97 – 192.168.1.126 | 192.168.1.127 |
| 4 | 192.168.1.128/27 | 192.168.1.129 – 192.168.1.158 | 192.168.1.159 |
| 5 | 192.168.1.160/27 | 192.168.1.161 – 192.168.1.190 | 192.168.1.191 |
| 6 | 192.168.1.192/27 | 192.168.1.193 – 192.168.1.222 | 192.168.1.223 |
| 7 | 192.168.1.224/27 | 192.168.1.225 – 192.168.1.254 | 192.168.1.255 |

6.5.2 División en Subredes: División en redes del tamaño adecuado

Cada red dentro de la internetwork de una empresa u organización está diseñada para incluir una cantidad limitada de hosts.

Algunas redes, como enlaces WAN punto a punto, sólo requieren un máximo de 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 incluir la cantidad máxima de hosts para 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 necesarios por toda la internetwork corporativa. Se debe usar un bloque de direcciones lo suficientemente amplio como para incluir todos los dispositivos en todas las redes corporativas. Esto incluye dispositivos de usuarios finales, servidores, dispositivos intermediarios e interfaces de routers.

Vea el Paso 1 de la figura.

Considere el ejemplo de una internetwork corporativa que necesita incluir 800 hosts en sus cuatro ubicaciones.

Determine la cantidad y el tamaño de las redes

A continuación, considere la cantidad de redes y el tamaño de cada una requeridas de acuerdo con los grupos comunes de hosts.

Vea el Paso 2 de la figura.

Se dividen las subredes de la red para superar problemas de ubicación, tamaño y control. Al diseñar el direccionamiento, se tienen en cuenta los factores para agrupar los hosts antes tratados:

- Agrupar basándonos en una ubicación geográfica común
- Agrupar hosts usados para propósitos específicos
- Agrupar basándonos en la propiedad

Cada enlace WAN es una red. Se crean subredes para la WAN que interconecta diferentes ubicaciones geográficas. Al conectar diferentes ubicaciones, se usa un router para dar cuenta de las diferencias de hardware entre las LAN y la WAN.

A pesar de que los hosts de una ubicación geográfica en común típicamente comprenden un solo bloque de direcciones, puede ser necesario realizar la división en subredes de este bloque para formar redes adicionales en cada ubicación. Es necesario crear subredes en diferentes ubicaciones que tengan hosts para las necesidades comunes de los usuarios. También puede suceder que otros grupos de usuarios requieran muchos recursos de red o que muchos usuarios requieran su propia subred. Además, es posible tener subredes para hosts especiales, como servidores. Es necesario tener en cuenta cada uno de estos factores para determinar la cantidad de redes.

También se deben tener en cuenta las necesidades de propiedad especiales de seguridad o administrativas que requieran redes adicionales.

Una herramienta útil para este proceso de planificación de direcciones es un diagrama de red. Un diagrama permite ver las redes y hacer una cuenta más precisa.

A fin de incluir 800 hosts en las cuatro ubicaciones de la compañía, se usa la aritmética binaria para asignar un bloque /22 ($2^{10-2}=1022$).

Asignación de direcciones

Ahora que se conoce la cantidad de redes y la cantidad de hosts para cada red, es necesario comenzar a asignar direcciones a partir del bloque general de direcciones.

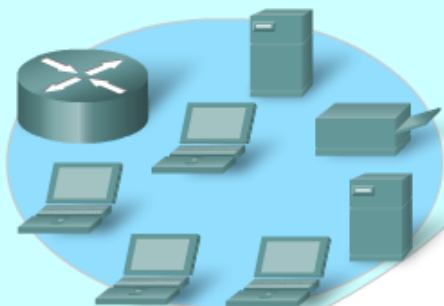
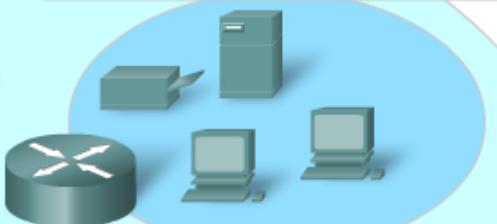
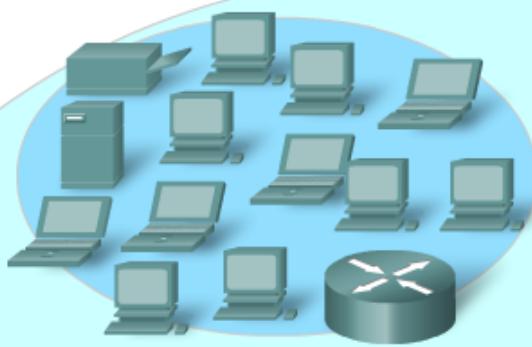
Vea el Paso 3 en la figura.

Este proceso comienza al asignar direcciones de red para ubicaciones de redes especiales. Se comienza por las ubicaciones que requieren la mayoría de los hosts y se continúa hasta los enlaces punto a punto. Este proceso asegura que se disponga de bloques de direcciones lo suficientemente amplios para incluir los hosts y las redes para estas ubicaciones.

Al hacer las divisiones y asignar las subredes disponibles, es necesario asegurarse de que haya direcciones del tamaño adecuado para mayores demandas. Además, se debe realizar una cuidadosa planificación para asegurar que los bloques de direcciones asignados a la subred no se superpongan.

División en subredes

En este ejemplo, la cantidad total de hosts en la red corporativa = 800 hosts.

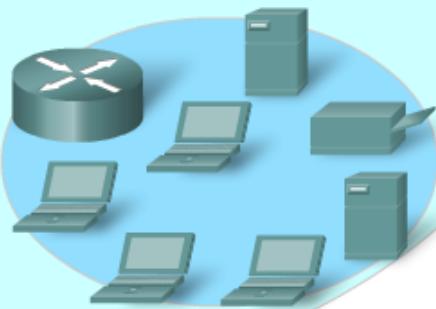
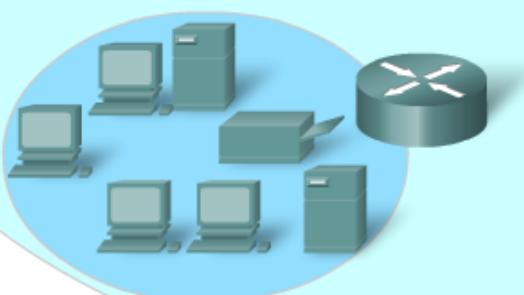
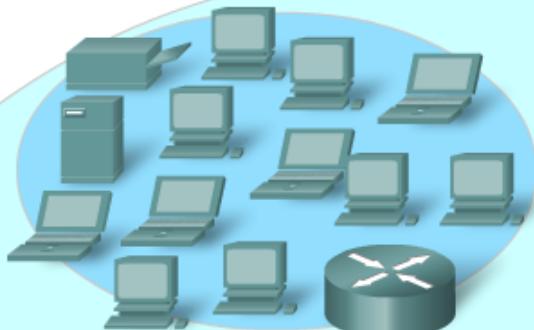


- 1 2 3

Haga clic para ver un paso.

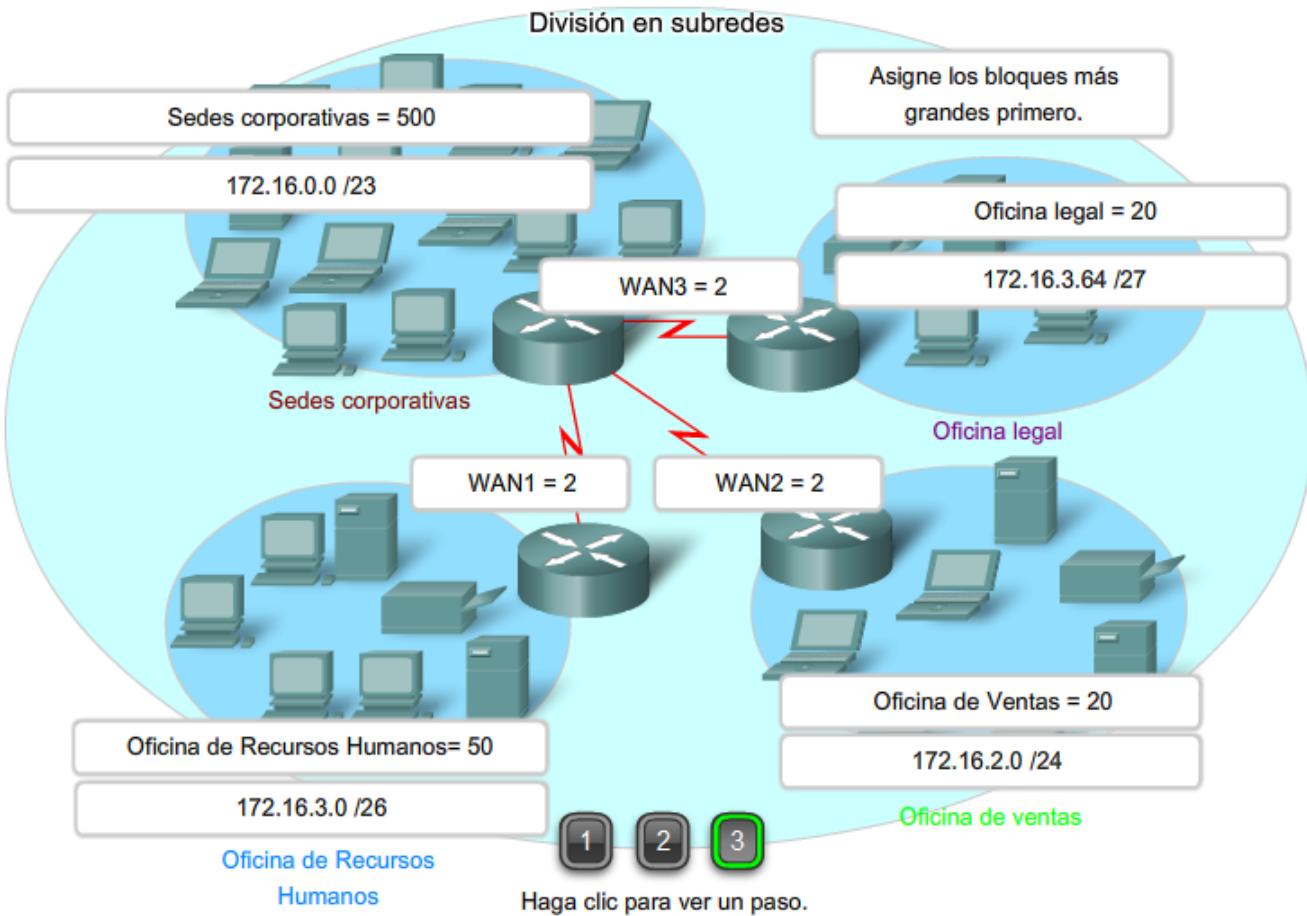
División en subredes

Elija un bloque de direcciones para alojar los hosts. $172.16.0.0 /22 = 1022$ direcciones host.



- 1 2 3

Haga clic para ver un paso.



Otra herramienta útil para este proceso de planificación es una hoja de cálculo. Es posible colocar las direcciones en columnas para visualizar la asignación de direcciones.

Vea el Paso 1 de la figura.

En el ejemplo, se asignan bloques de direcciones a las cuatro ubicaciones, así como enlaces WAN.

Con los principales bloques asignados, se continúa realizando la división en subredes de cualquiera de las ubicaciones que requiera dicha división. En el ejemplo, se divide la sede corporativa en dos redes.

Vea el Paso 2 en la figura.

Esta división adicional de las direcciones a menudo se llama división en subredes. Al igual que con la división en subredes, es necesario planificar detenidamente la asignación de direcciones de manera que se disponga de bloques de direcciones.

La creación de nuevas redes más pequeñas de un bloque de direcciones determinado se hace ampliando la longitud del prefijo; es decir, agregando números 1 a la máscara de subred. De esta forma se asignan más bits a la porción de red de la dirección para brindar más patrones para la nueva subred. Para cada bit que se pide prestado, se duplica la cantidad de redes. Por ejemplo: si se usa 1 bit, existe la posibilidad de dividir ese bloque en dos redes más pequeñas. Con un solo patrón de bit podemos producir dos patrones únicos de bit, 1 y 0. Si pedimos prestados 2 bits podemos proveer 4 patrones únicos para representar redes 00, 01, 10 y 11. Los 3 bits permitirían 8 bloques y así sucesivamente.

Número total de Hosts utilizables

Recuerde de la sección anterior que al dividir el rango de dirección en subredes perdemos dos direcciones de host para cada red nueva. Éstas son la dirección de red y la dirección de broadcast.

La fórmula para calcular el número de hosts en una red es:

$$\text{Hosts utilizables} = 2^n - 2$$

Donde n es el número de bits remanentes a ser utilizados por los hosts.

Enlaces:

Calculador de subred: <http://vlsm-calc.net>

| Red empresarial | HQ | Ventas | RECURSOS HUMANOS | DEPARTAMENTO LEGAL |
|-----------------|---------------|---------------|------------------|--------------------|
| 172.16.0.0/22 | 172.16.0.0/23 | 172.16.2.0/24 | 172.16.3.0/26 | 172.16.3.64/27 |
| 172.16.0.1 | 172.16.0.1 | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | 172.16.1.225 | | 172.16.2.0 | |
| | | | | |
| | | | | |
| | | | | |
| | | 172.16.2.225 | | |
| | | | | |

Paso 1

Paso 2

| HQ | HQ1 | HQ2 |
|---------------|--------------|--------------|
| 172.16.0.0/23 | | |
| 172.16.0.1 | 172.16.0.1 | |
| | | |
| | 172.16.0.255 | 172.16.1.0 |
| | | |
| 172.16.1.255 | | 172.16.1.255 |

6.5.3 División en subredes: subdivisión de una subred

La subdivisión en subredes, o el uso de una Máscara de subred de longitud variable (VLSM), fue diseñada para maximizar la eficiencia del direccionamiento. Al identificar la cantidad total de hosts que utiliza la división tradicional en subredes, se asigna la misma cantidad de direcciones para 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 eficientes. Sin embargo, esto no es lo que suele suceder.

Por ejemplo: la topología en la Figura 1 muestra los requisitos de subred de siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres WAN. Con la dirección 192.168.20.0, es necesario pedir prestados 3 bits de los bits del host en el último octeto para satisfacer los requisitos de subred de siete subredes.

Estos bits son bits que se toman prestados al cambiar la máscara de subred correspondiente por números “1” para indicar que estos bits ahora se usan como bits de red. Entonces, el último octeto de la máscara se representa en binario con 11100000, que es 224. La nueva máscara 255.255.255.224 se representa mediante la notación /27 para representar un total de 27 bits para la máscara.

En binario, esta máscara de subred se representa como: 11111111.11111111.11111111.11100000

Luego de tomar prestados tres de los bits de host para usar como bits de red, quedan cinco bits de host. Estos cinco bits permitirán más de 30 hosts por subred.

A pesar de que se ha cumplido la tarea de dividir la red en una cantidad adecuada de redes, esto se hizo mediante la pérdida significativa de direcciones no utilizadas. Por ejemplo: sólo se necesitan dos direcciones en cada subred para los enlaces WAN. Hay 28 direcciones no utilizadas en cada una de las tres subredes WAN que han sido bloqueadas en estos bloques de direcciones. Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de direcciones es característico del direccionamiento con clase.

Aplicar un esquema de división en subredes estándar al escenario no es muy eficiente y puede causar desperdicio. De hecho, este ejemplo es un modelo satisfactorio para mostrar cómo la división en subredes de una subred puede utilizarse para maximizar el uso de la dirección.

Obtención de más subredes para menos hosts

Como se mostró en ejemplos anteriores, se comenzó con las subredes originales y se obtuvieron subredes adicionales más pequeñas para usar en los enlaces WAN. Creando subredes más pequeñas, cada subred puede soportar 2 hosts, dejando libres las subredes originales para ser asignadas a otros dispositivos y evitando que muchas direcciones puedan ser desperdiciadas.

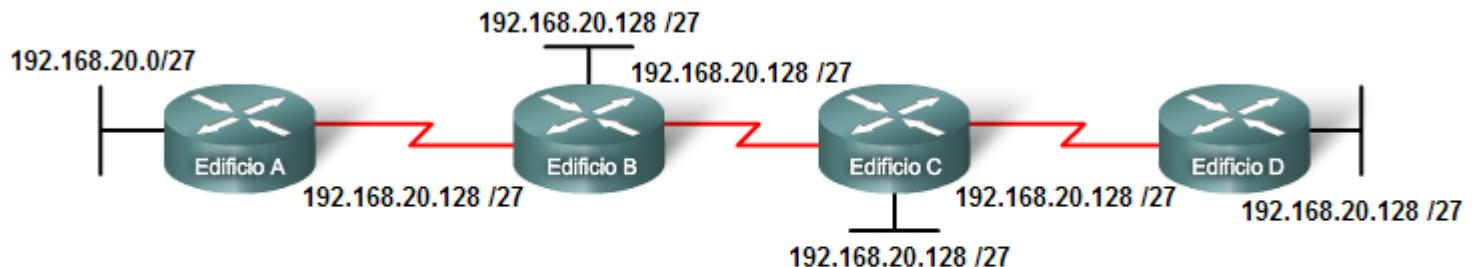
Para crear estas subredes más pequeñas para los enlaces WAN, comience con 192.168.20.192. Podemos dividir esta subred en subredes más pequeñas. Para suministrar bloques de direcciones para las WAN con dos direcciones cada una, se tomarán prestados tres bits de host adicionales para usar como bits de red.

Dirección: 192.168.20.192 En binario: 11000000.10101000.00010100.11000000

Máscara: 255.255.255.252 30 bits en binario: 11111111.11111111.11111111.11111100

La topología en la figura 2 muestra un plan de direccionamiento que divide las subredes 192.168.20.192 /27 en subredes más pequeñas para suministrar direcciones para las WAN. De esta forma se reduce la cantidad de direcciones por subred a un tamaño apropiado para las WAN. Con este direccionamiento, se obtienen subredes 4, 5 y 7 disponibles para futuras redes, así como varias subredes disponibles para las WAN.

División en subredes de un bloque de subred

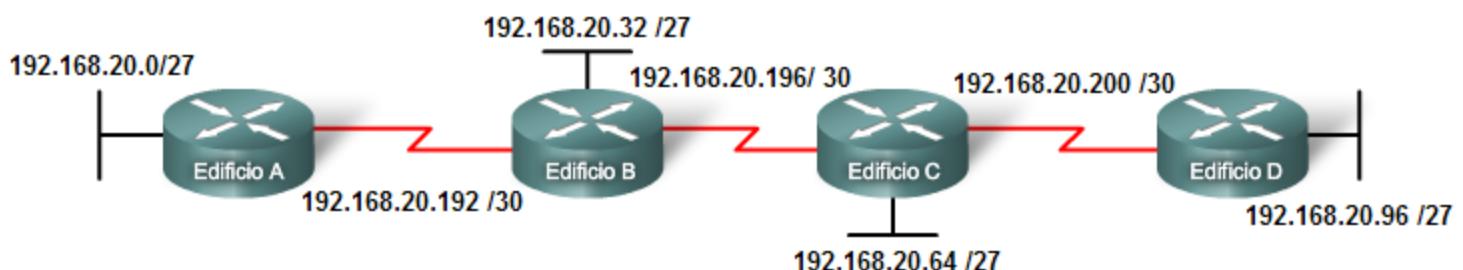


| Número de subred | Dirección de subred |
|------------------|---------------------|
| Subred 0 | 192.168.20.0/27 |
| Subred 1 | 192.168.20.32/27 |
| Subred 2 | 192.168.20.64/27 |
| Subred 3 | 192.168.20.96/27 |
| Subred 4 | 192.168.20.128/27 |
| Subred 5 | 192.168.20.160/27 |
| Subred 6 | 192.168.20.192/27 |
| Subred 7 | 192.168.20.224/27 |

1

2

División en subredes de un bloque de subred



| Número de subred | Dirección de subred |
|------------------|---------------------|
| Subred 0 | 192.168.20.0/27 |
| Subred 1 | 192.168.20.32/27 |
| Subred 2 | 192.168.20.64/27 |
| Subred 3 | 192.168.20.96/27 |
| Subred 4 | 192.168.20.128/27 |
| Subred 5 | 192.168.20.160/27 |
| Subred 6 | 192.168.20.192/27 |
| Subred 7 | 192.168.20.224/27 |

| Número de subred | Dirección de subred |
|------------------|---------------------|
| Subred 0 | 192.168.20.192/30 |
| Subred 1 | 192.168.20.196/30 |
| Subred 2 | 192.168.20.200/30 |
| Subred 3 | 192.168.20.204/30 |
| Subred 4 | 192.168.20.208/30 |
| Subred 5 | 192.168.20.212/30 |
| Subred 6 | 192.168.20.216/30 |
| Subred 7 | 192.168.20.220/30 |

En la Figura 1, se considerará el direccionamiento desde otra perspectiva. Se tendrá en cuenta la división en subredes de acuerdo con la cantidad de hosts, incluso las interfaces de router y las conexiones WAN. Este escenario posee los siguientes requisitos:

- AtlantaHQ 58 direcciones de host
- PerthHQ 26 direcciones de host
- SydneyHQ 10 direcciones de host
- CorpusHQ 10 direcciones de host
- Enlaces WAN 2 direcciones de host (cada una)

Queda claro que, a partir de estos requerimientos, el uso de un esquema de armado estándar de subredes sería un gran desperdicio. En esta internetwork, el armado estándar de subredes bloquearía cada subred en bloques de 62 hosts, lo que llevaría a un significativo desperdicio de direcciones potenciales. Este desperdicio es especialmente evidente en la figura 2, donde se ve que la LAN PerthHQ admite 26 usuarios y que los routers de LAN SydneyHQ y CorpusHQ admiten 10 usuarios cada uno.

Por lo tanto, con el bloque de direcciones 192.168.15.0 /24 se comenzará a diseñar un esquema de direccionamiento que cumpla los requisitos y guarde posibles direcciones.

Obtención de más direcciones

Al crear un esquema de direccionamiento adecuado, siempre se comienza con la mayor demanda. En este caso, AtlantaHQ, con 58 usuarios, tiene la mayor demanda. A partir de 192.168.15.0, se precisarán 6 bits de host para incluir la demanda de 58 hosts; esto deja 2 bits adicionales para la porción de red. El prefijo para esta red sería /26 y la máscara de subred 255.255.255.192.

Comencemos por dividir en subredes el bloque original de direcciones 192.168.15.0 /24. Al usar la fórmula de hosts utilizables = $2^n - 2$, se calcula que 6 bits de host permiten 62 hosts en la subred. Los 62 hosts satisfarían los 58 hosts requeridos del router de la compañía AtlantaHQ.

Dirección: 192.168.15.0

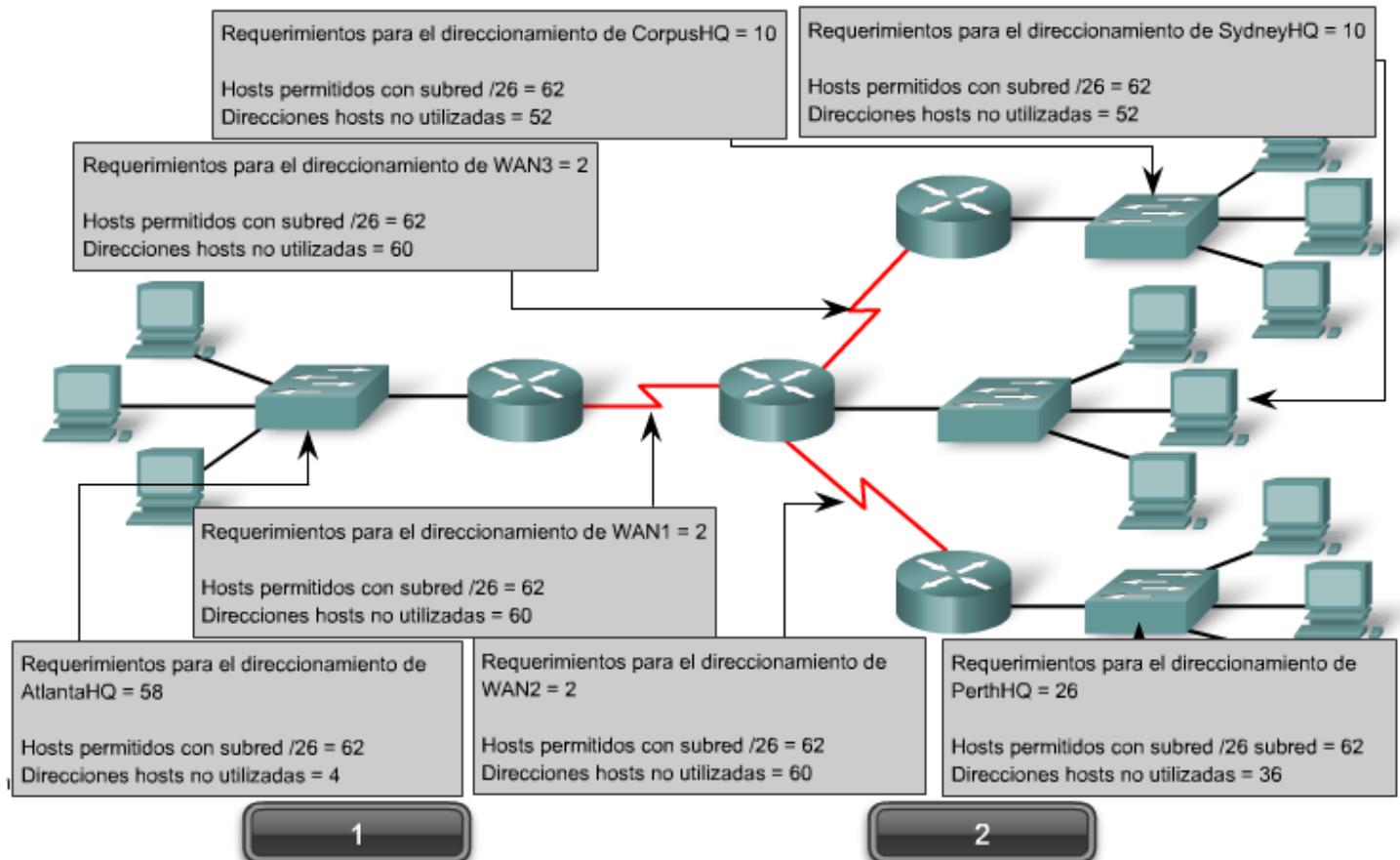
En binario: 11000000.10101000.00001111.00000000

Máscara: 255.255.255.192

26 bits en binario: 1111111.1111111.1111111.11000000

La página siguiente muestra el proceso de identificación de la próxima secuencia de pasos.

Requisitos de red: El uso de la división en subredes estándar sería ineficiente.



Aquí se describen los pasos para implementar este esquema de armado de subredes.

Asignar la LAN de AtlantaHQ

Vea los pasos 1 y 2 en la figura.

El primer paso muestra un gráfico de planificación de red. El segundo paso en la figura muestra la entrada para AtlantaHQ. Esta entrada es el resultado del cálculo de una subred a partir del bloque original 192.168.15.0 /24 a fin de incluir la LAN más grande, la LAN AtlantaHQ con 58 hosts. Para realizar esta acción fue necesario pedir prestados 2 bits de host adicionales, para usar una máscara de bits /26.

Al compararlo, el siguiente esquema muestra cómo 192.168.15.0 se dividiría en subredes mediante el bloque de direccionamiento fijo para brindar bloques de direcciones lo suficientemente amplios:

Subred 0: 192.168.15.0 /26 rango de direcciones host de 1 a 62

Subred 1: 192.168.15.64 /26 rango de direcciones host de 65 a 126

Subred 2: 192.168.15.128 /26 rango de direcciones host de 129 a 190

Subred 3: 192.168.15.192 /26 rango de direcciones host de 193 a 254

Los bloques fijos permitirían sólo cuatro subredes y, por lo tanto, no dejarían suficientes bloques de direcciones para la mayoría de las subredes de esta internetwork. En lugar de continuar utilizando la siguiente subred disponible, es necesario asegurarse de que el tamaño de cada subred sea consecuente con los requisitos de host. Para usar un esquema de direccionamiento que se relacione directamente con los requisitos de host se debe usar un método diferente de división en subredes.

Asignación de la LAN PerthHQ

Vea al Paso 3 en la figura.

En el tercer paso, se observan los requisitos de la siguiente subred más grande. Ésta es la LAN PerthHQ, que requiere 28 direcciones de host, incluida la interfaz de router. Se debe comenzar con la siguiente dirección disponible 192.168.15.64 para crear un bloque de direcciones para esta subred. Al pedir prestado otro bit, se pueden satisfacer las necesidades de PerthHQ al tiempo que se limita el desperdicio de direcciones. El bit tomado deja una máscara /27 con el siguiente intervalo de direcciones:

192.168.15.64 /27 intervalo de direcciones de host 65 a 94

Este bloque de direcciones suministra 30 direcciones, lo cual satisface la necesidad de 28 hosts y deja espacio para el crecimiento de esta subred.

Asignación de las LAN SydneyHQ y CorpusHQ

Vea los Pasos 4 y 5 en la figura.

Los pasos cuatro y cinco proporcionan direccionamiento para las siguientes subredes más grandes: Las LAN SydneyHQ y CorpusHQ. En estos dos pasos, cada LAN tiene la misma necesidad de 10 direcciones host. Esta división en subredes requiere tomar prestado otro bit, a fin de ampliar la máscara a /28. A partir de la dirección 192.168.15.96, se obtienen los siguientes bloques de direcciones:

Subred 0: 192.168.15.96 /28 rango de direcciones host de 97 a 110

Subred 1: 192.168.15.112 /28 rango de direcciones host de 113 a 126

Estos bloques proporcionan 14 direcciones para los hosts y las interfaces del router para cada LAN.

Asignación de las WAN

Vea los Pasos 6, 7 y 8 en la figura.

Los últimos tres pasos muestran la división en subredes para los enlaces WAN. Con estos enlaces WAN punto a punto, sólo se necesitan dos direcciones. Con el objetivo de satisfacer los requisitos, se toman 2 bits más para usar una máscara /30. Al utilizar las próximas direcciones disponibles, se obtienen los siguientes bloques de direcciones:

Subred 0: 192.168.15.128 /30 rango de direcciones host de 129 a 130

Subred 1: 192.168.15.132 /30 rango de direcciones host de 133 a 134

Subred 2: 192.168.15.136 /30 rango de direcciones host de 137 a 138

| Nombre - dirección requerida | Dirección de subred | Rango de dirección | Dirección de broadcast | Red/prefijo |
|------------------------------|---------------------|--------------------|------------------------|--------------------|
| AtlantaHQ - 58 | 192.168.15.0 | .1 - .62 | .63 | 192.168.15.0 /26 |
| PerthHQ - 28 | 192.168.15.64 | .65 - .94 | .95 | 192.168.15.64 /27 |
| SydneyHQ - 10 | 192.168.15.96 | .97 - .110 | .111 | 192.168.15.96 /28 |
| CorpusHQ - 10 | 192.168.15.112 | .113 - .126 | .127 | 192.168.15.112 /28 |
| WAN1 - 2 | 192.168.15.128 | .129 - .130 | .131 | 192.168.15.128 /30 |
| WAN2 - 2 | 192.168.15.132 | .133 - 134 | .135 | 192.168.15.132 /30 |
| WAN3 - 2 | 192.168.15.136 | .137 - .138 | .139 | 192.168.15.136 /30 |

Los resultados muestran en nuestro esquema de direccionamiento, usando visualizaciones VLSM, una amplia gama de bloques de direcciones correctamente asignados. Como una mejor práctica, se comenzó por documentar los requisitos, de mayor a menor. Al comenzar por el requisito mayor, fue posible determinar que un esquema de bloque de direccionamiento fijo no permitiría un uso eficiente de las direcciones Ipv4 y, como se muestra en este ejemplo, no suministraría suficientes direcciones.

Se tomaron prestados bits del bloque de direcciones asignado para crear los intervalos de direcciones que se ajusten a la topología. La figura 1 muestra los intervalos asignados. La figura 2 muestra la topología con la información de direccionamiento.

El uso de VLSM para asignar las direcciones permitió aplicar las guías de división en subredes para agrupar hosts según:

- Agrupación basada en ubicación geográfica común
- Agrupación de hosts utilizados para propósitos específicos
- Agrupación basada en propiedad

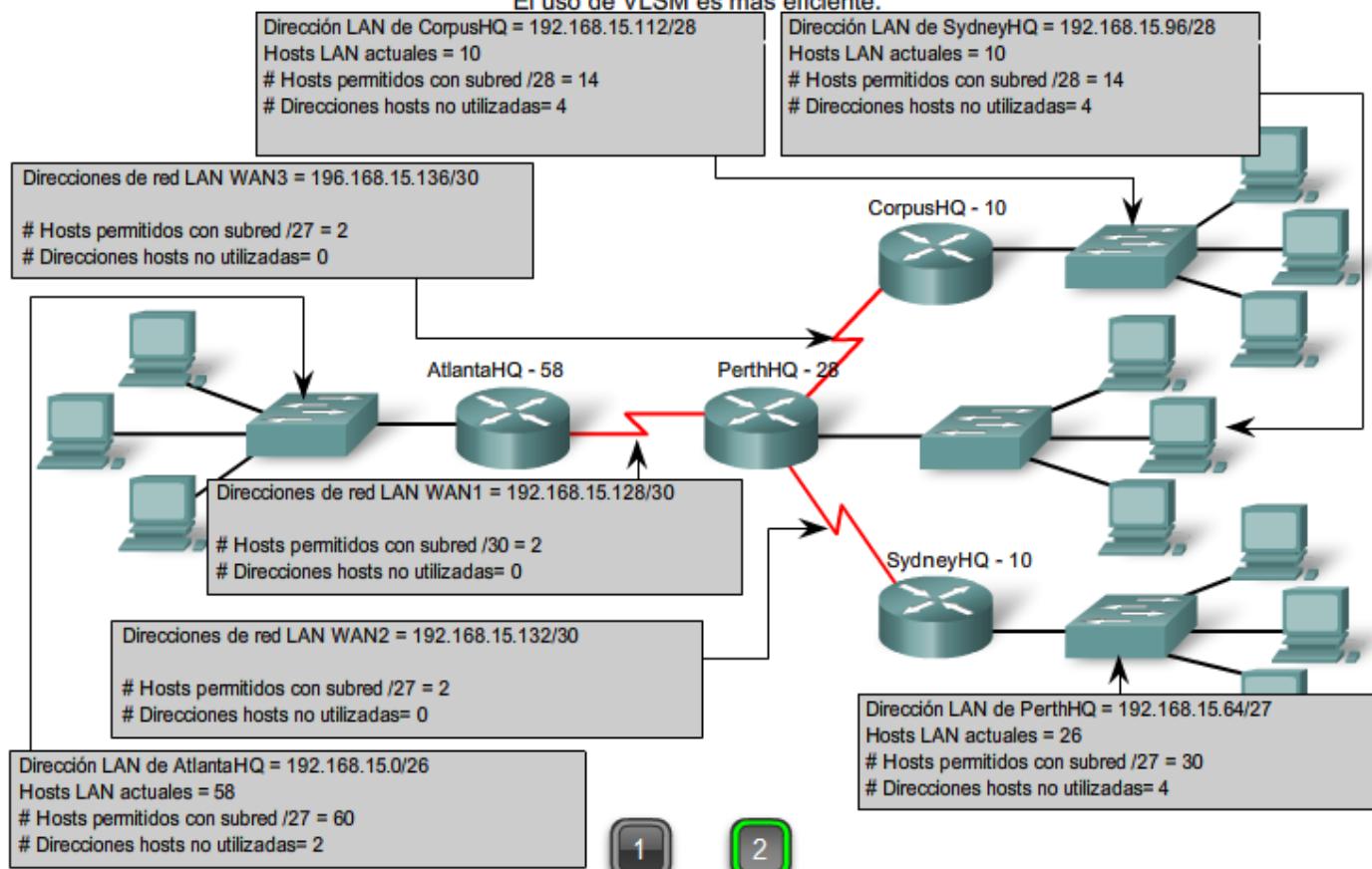
En nuestro ejemplo, basamos la agrupación en el número de hosts dentro de una ubicación geográfica común.

Requisitos de la red
El uso de VLSM es más eficiente.

| Nombre - dirección requerida | Dirección de subred | Rango de dirección | Dirección de broadcast | Red/prefijo |
|------------------------------|---------------------|--------------------|------------------------|-------------------|
| AtlantaHQ - 58 | 192.168.15.0 | .1-.62 | .63 | 192.168.15.0/26 |
| PerthHQ - 28 | 192.168.15.64 | .65-.94 | .95 | 192.168.15.64/27 |
| SydneyHQ - 10 | 192.168.15.96 | .97-.110 | .111 | 192.168.15.96/28 |
| CorpusHQ - 10 | 192.168.15.112 | .113-.126 | .127 | 192.168.15.112/28 |
| WAN1 - 2 | 192.168.15.128 | .129-.130 | .131 | 192.168.15.128/30 |
| WAN2 - 2 | 192.168.15.132 | .133-.134 | .135 | 192.168.15.132/30 |
| WAN3 - 2 | 192.168.15.136 | .137-.138 | .139 | 192.168.15.136/30 |

Requisitos de la red

El uso de VLSM es más eficiente.



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, es posible inspeccionar la planificación de direcciones usando el cuadro de VLSM para ver su uso.

El primer gráfico muestra la porción superior del cuadro. Un cuadro completo para su uso está disponible utilizando el enlace a continuación.

VLSM_Subnetting_Chart.pdf

Este cuadro se puede usar para planificar direcciones para redes con prefijos en el rango de /25 - /30. Éstos son los rangos de red de uso más frecuente para la división en subredes.

Igual que antes, se comienza con la subred que tiene la mayor cantidad de hosts. En este caso, es AtlantaHQ con 58 hosts.

Elección de un bloque de la LAN AtlantaHQ

Al observar el encabezado del cuadro de izquierda a derecha, se encuentra el encabezado que indica que el tamaño del bloque es suficiente para los 58 hosts. Ésta es la columna /26. En esta columna, se observan cuatro bloques de este tamaño:

.0 /26 rango de direcciones host de 1 a 62

.64 /26 rango de direcciones host de 65 a 126

.128 /26 rango de direcciones host de 129 a 190

.192 /26 rango de direcciones host de 193 a 254

Dado que no se han asignado direcciones, es posible elegir cualquiera de estos bloques. A pesar de que pueden existir motivos para usar un bloque diferente, comúnmente se usa el primer bloque disponible, el .0 /26. Esta asignación se muestra en la Figura 2.

Una vez que se asigna el bloque de direcciones, estas direcciones se consideran usadas. Asegúrese de marcar este bloque, al igual que cualquier otro bloque mayor que contenga estas direcciones. Al marcarlo, se pueden ver las direcciones que no pueden ser usadas y las que todavía están disponibles. Al observar la Figura 3, cuando se asigna el bloque .0 /26 a AtlantaHQ, se marcan todos los bloques que contienen estas direcciones.

Elección de un bloque para la LAN PerthHQ

A continuación, se necesita un bloque de direcciones para la LAN PerthHQ de 26 hosts. Al desplazarse por el encabezado del cuadro, se encuentra la columna con subredes de tamaño suficiente para esta LAN. Despues, es necesario desplazarse hacia abajo en el cuadro hasta el primer bloque disponible. En la Figura 3, se resalta la sección del cuadro disponible para PerthHQ. El bit que se tomó prestado hace que el bloque de direcciones esté disponible para esta LAN. Aunque podríamos haber elegido cualquiera de los bloques disponibles, generalmente procedemos con el primer bloque disponible que satisface la necesidad.

El rango de dirección para este bloque es:

.64 /27 rango de dirección host 65 a 94

Elección de bloques para la LAN de SydneyHQ y la LAN de CorpusHQ

Como se muestra en la Figura 4, continuamos marcando los bloques de dirección para evitar la superposición de asignaciones de dirección. Para satisfacer las necesidades de las LAN SydneyHQ y CorpusHQ, se asignan nuevamente los próximos bloques disponibles. Esta vez se realiza un desplazamiento hasta la columna /28 y hacia abajo a los bloques .96 y .112. Note que la sección del cuadro disponible para SydneyHQ y CorpusHQ está resaltada.

Estos bloques son:

.96 /28 rango de dirección host 97 a 110

.112 /28 rango de dirección host 113 a 126

Elección de bloques para las WAN

El último requerimiento para el direccionamiento es para las conexiones WAN entre las redes. Al observar la Figura 5, se realiza un desplazamiento hacia la columna de la derecha hasta el prefijo /30. A continuación, debe desplazarse hacia abajo y resaltar tres bloques disponibles. Estos bloques suministrarán las 2 direcciones por WAN.

Estos tres bloques son:

.128 /30 rango de direcciones host de 129 a 130

.132 /30 rango de direcciones host de 133 a 134

.136 /30 rango de direcciones host de 137 a 138

Al observar la Figura 6, las direcciones asignadas a la WAN están marcadas para indicar que los bloques que las contienen ya no pueden ser asignados. Observe en la asignación de estos intervalos de WAN que se han marcado varios bloques más grandes que no pueden ser asignados. Éstos son:

.128 /25

.128 /26

.128 /27

.128 /28

.128 /29

.136 /29

Debido a que estas direcciones son parte de estos bloques más grandes, la asignación de estos bloques se superpondría con el uso de estas direcciones.

Como se ha podido observar, el uso de VLSM permite maximizar el direccionamiento y minimizar el desperdicio. El método del cuadro que se mostró es apenas otra herramienta que los administradores y técnicos de red pueden usar para crear un esquema de direccionamiento que ocasione menos desperdicio que el enfoque de bloques de tamaño fijo.

| | /25 (1 subnet bit) 1 subnet126 hosts | /26 (2 subnet bits) 3 subnets62 hosts | /27 (3 subnet bits) 7 subnets30 hosts | /28 (4 subnet bits) 15 subnets14 hosts | /29 (5 subnet bits) 31 subnets6 hosts | /30 (6 subnet bits) 63 subnets2 hosts |
|----|---|---------------------------------------|---------------------------------------|--|---------------------------------------|---------------------------------------|
| .0 | .0 | .0 (.1-.62) | .0 .1.30) | .0 (.1.14) | .0 (.1.6) | .0 (.1.2) |
| .4 | | | | | | .4(5.6) |
| .8 | | | | | | .8(9.10) |
| .1 | | | | | .8(.9.14) | .12(13.14) |
| 2 | | | | | | |
| .1 | | | | .16(.17.30) | .16(.17.22) | .16(.17.18) |
| 6 | | | | | | .20(.21.22) |
| .2 | | | | | | .24(.25.26) |
| 0 | | | | | .24(.25.30) | .28(.29.30) |
| .2 | | | | | | |
| 4 | | | | .32(.33.46) | .32(.33.38) | .32(.33.34) |
| .2 | | | | | | .36(.37.38) |
| 8 | | | | | .40(.41.46) | .40(.41.42) |
| .4 | | | | | | .44(.45.46) |
| 0 | | | | .48(.49.62) | .48(.49.54) | .48(.49.50) |
| .4 | | | | | | .52(.53.54) |
| 4 | | | | | .56(.57.62) | .56(.57.58) |
| .4 | | | | | | .60(.61.62) |
| 8 | | | | .64(.65.78) | .64(.65.70) | .64(.65.66) |
| .6 | | | | | | .68(.69.70) |
| 8 | | | | | .72(.73.78) | .72(.73.74) |
| .7 | | | | .80(.81.94) | .76(.77.78) | |
| 2 | | | | | | .80(.81.82) |
| .7 | | | | | .84(.85.86) | |
| 6 | | | | .88(.89.94) | .88(.89.90) | |
| .8 | | | | | | .92(.93.94) |
| 0 | | | | | .96(.97.102) | .96(.97.98) |
| .9 | .64 .126)(.65 | .64(.65.94) | .96(.97.110) | .104(.105.110) | .100(.101.102) | .100(.101.102) |
| 6 | | | | | | .104(.105.106) |
| .1 | | | | | .108(.109.110) | |
| 00 | | | .96(.97.126) | .112(.113.118) | .112(.113.114) | |
| .1 | | | | | | .116(.117.118) |
| 04 | | | | | .120(.121.122) | |
| .1 | | | .112(.113.126) | .120(.121.126) | .124(.125.126) | |
| 08 | | | | | | |
| .1 | | | | | .128(.129.134) | .128(.129.130) |
| 12 | | | .128(.129.142) | .136(.137.142) | | .132(.133.134) |
| .1 | | | | | .136(.137.138) | |
| 16 | | | | | | .140(.141.142) |
| .1 | .128 | .128.190)(.129 | .128(.129.158) | .144(.145.150) | .144(.145.146) | |
| 20 | | | | | | .148(.149.150) |
| .1 | | | | | .152(.153.158) | .152(.153.154) |
| 24 | | | .144(.145.158) | .160(.161.166) | | .156(.157.158) |
| .1 | | | | | .160(.161.162) | |
| 28 | | | | | | .164(.165.166) |
| .1 | | | .160(.161.190) | .160(.161.174) | .160(.161.166) | |
| 32 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 36 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 40 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 44 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 48 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 52 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 56 | | | | | | |
| .1 | | | | | .164(.165.166) | |
| 60 | | | | | | |
| .1 | | | | | .164(.165.166) | |

| | | | | | |
|---|---------------------------------------|---------------------------------------|--|---------------------------------------|---------------------------------------|
| .64 | | | | | |
| .1 68 | | | | .168(.169.174) | .168(.169.170) |
| .1 72 | | | | | .172(.173.174) |
| .1 76 | | | | | .176(.177.178) |
| .1 80 | | | | | .180(.181.182) |
| .1 84 | | | | | .184(.185.186) |
| .1 88 | | | | | .188(.189.190) |
| .1 92 | | | | | .192(.193.194) |
| .1 96 | | | | | .196(.197.198) |
| .2 00 | | | | | .200(.201.202) |
| .2 04 | | | | | .204(.205.206) |
| .2 08 | | | | | .208(.209.210) |
| .2 12 | | | | | .212(.213.214) |
| .2 16 | | | | | .216(.217.218) |
| .2 20 | | | | | .220(.221.222) |
| .2 24 | | | | | .224(.225.226) |
| .2 28 | | | | | .228(.229.230) |
| .2 32 | | | | | .232(.233.234) |
| .2 36 | | | | | .236(.237.238) |
| .2 40 | | | | | .240(.241.242) |
| .2 44 | | | | | .244(.245.246) |
| .2 48 | | | | | .248(.249.250) |
| .2 52 | | | | | .252(.253.254) |
| /25 (1 subnet bit) 1 subnet126 hosts | /26 (2 subnet bits) 3 subnets62 hosts | /27 (3 subnet bits) 7 subnets30 hosts | /28 (4 subnet bits) 15 subnets14 hosts | /29 (5 subnet bits) 31 subnets6 hosts | /30 (6 subnet bits) 63 subnets2 hosts |

6.6 PRUEBA DE LA CAPA DE RED

6.6.1 Ping 127.0.0.1 – Prueba del Stack local

Ping es una utilidad para probar la conectividad IP entre hosts. Ping envía solicitudes de respuestas desde una dirección host específica. Ping usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control Message Protocol (Protocolo de mensajes de control de Internet, ICMP). Ping usa un datagrama de solicitud de eco ICMP.

Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. Ping posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen 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 del IP en el host local. Para hacer esta prueba, se realiza el ping de la dirección reservada especial del loopback local (127.0.0.1), como se muestra en la figura.

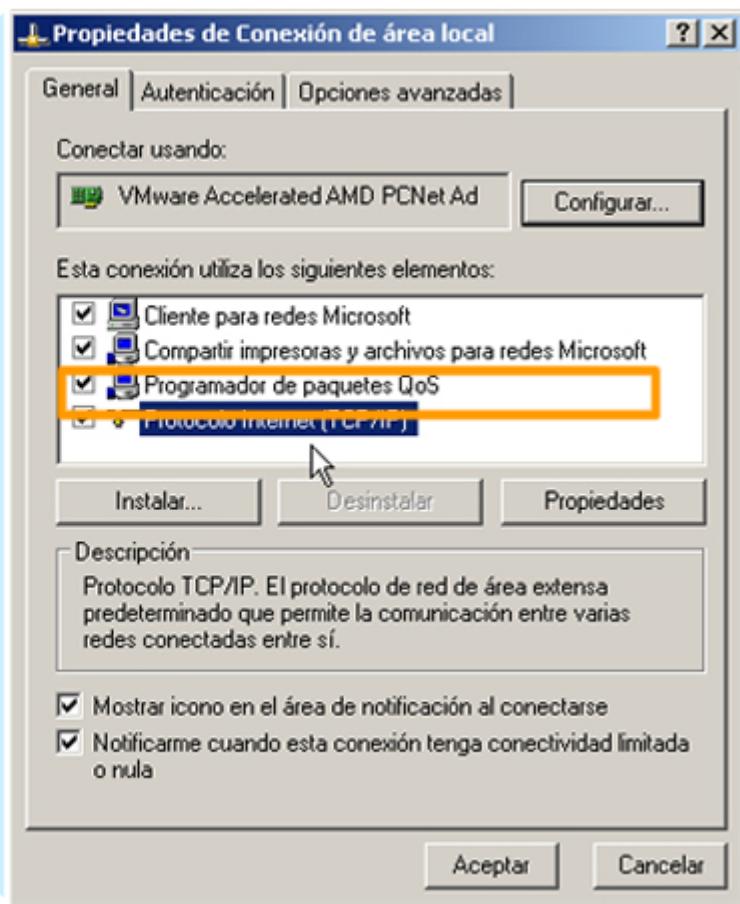
Una respuesta de 127.0.0.1 indica que el IP está correctamente instalado en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior 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.

Prueba del stack TCP/IP local

Hacer ping en el host local confirma que TCP/IP se encuentra instalado en el host y funciona.



Hacer ping a 127.0.0.1 hace que un dispositivo haga ping desde él mismo.



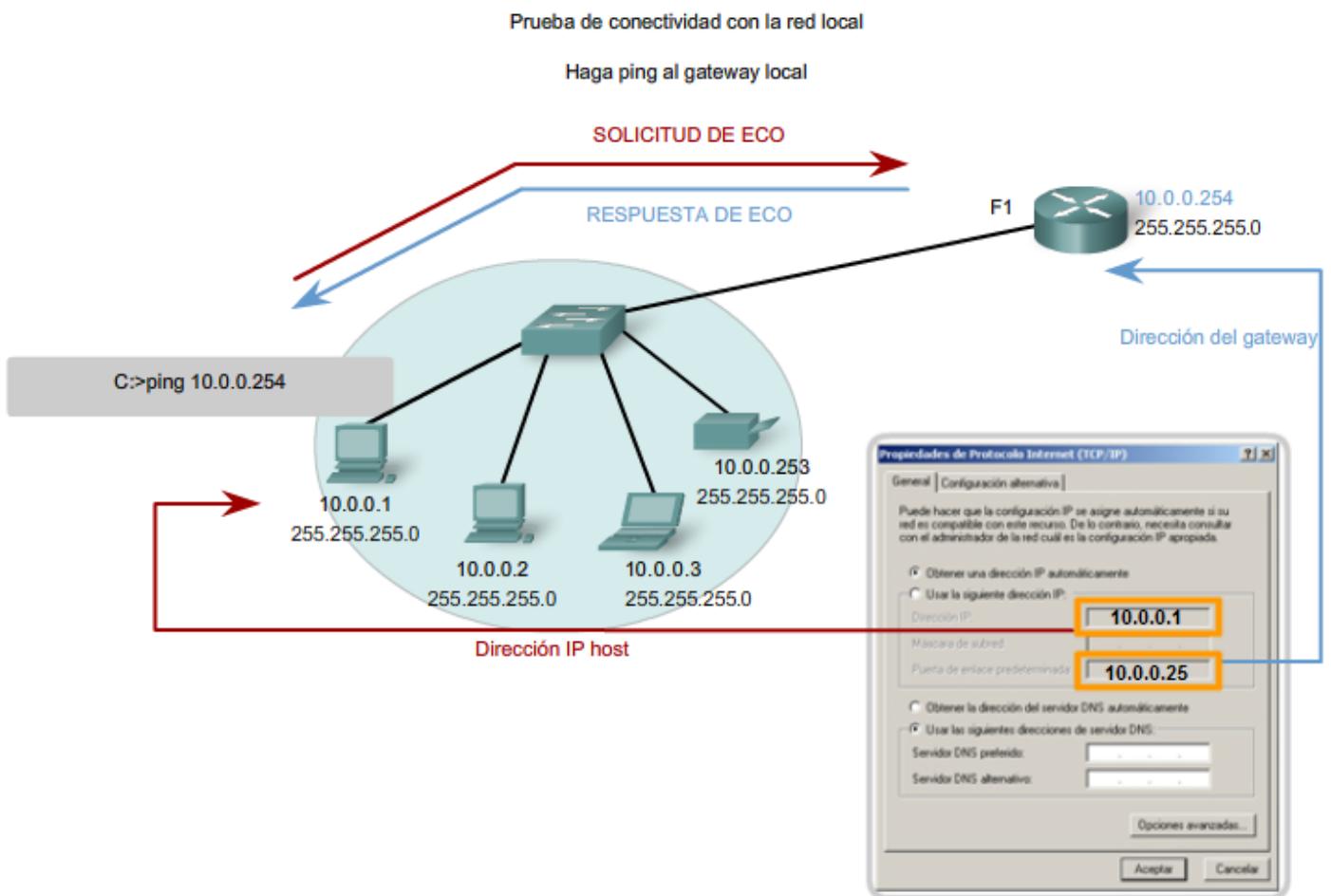
6.6.2 Ping de Gateway – Prueba de la conectividad de la LAN local

También es posible utilizar el ping para probar la capacidad de comunicación del host en la red local. Generalmente, esto se hace haciendo ping a la dirección IP del router del host, como se muestra en la figura. Un ping en el router indica que la interfaz del host y del router que funcionan como router funcionan en la red local.

Para esta prueba, se usa la dirección de router con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de router no responde, se puede intentar con la dirección IP de otro host que sepa que funciona en la red local.

Si el router u otro host responden, entonces los hosts locales pueden comunicarse con éxito en la red local. Si el router no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como router.

Una posibilidad es que se tiene la dirección equivocada para el 246ersión. 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. También puede suceder que otros hosts tengan la misma restricción de seguridad aplicada.



6.6.3 Ping de host remoto: Prueba de conectividad con una LAN remota

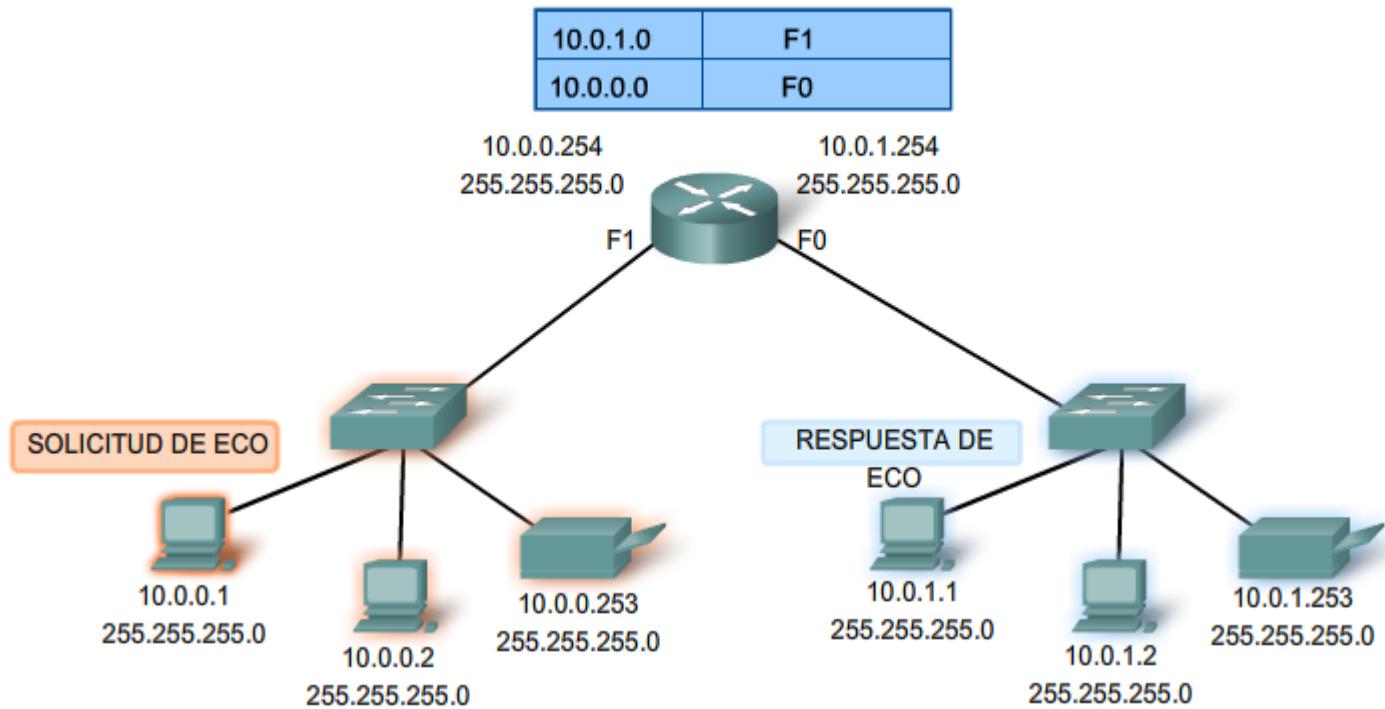
También se puede utilizar el ping para probar la capacidad de comunicación del host IP local en una internetwork. El host local puede hacer ping a un host que funciona en una red remota, como se muestra en la figura.

Si el ping se realiza con éxito, se habrá verificado la operación de una porción amplia de la internetwork. Esto significa que se ha verificado la comunicación del host en la red local, el funcionamiento del router que se usa como 246ersión y los demás routers que puedan encontrarse en la ruta entre la red y la red del host remoto.

Además, se ha verificado el mismo funcionamiento en el host remoto. Si, por algún motivo, el host remoto no pudo usar su red local para comunicarse fuera de la red, entonces no se habría producido una respuesta.

Recuerde: muchos administradores de red limitan o prohíben la entrada de datagramas ICMP en la red corporativa. Por lo tanto, la ausencia de una respuesta de ping podría deberse a restricciones de seguridad y no a elementos que no funcionan en las redes.

Prueba de conectividad con LAN remota
Haga ping en un host remoto



6.6.4 Traceroute (tracert) – Prueba de ruta

El ping se usa para indicar la conectividad entre dos hosts. Traceroute (tracert) es una utilidad que permite observar la ruta entre estos hosts. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallas. Si los datos llegan a destino, entonces el rastreador menciona la interfaz en cada router que aparece en el camino.

Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo. Esto indica el lugar donde 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 (RTT) para cada salto a lo largo del camino e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Se usa un asterisco (*) para indicar la pérdida de un paquete.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si tenemos altos tiempos de respuesta o pérdidas de datos de un salto particular, ésta es una indicación de que los recursos del router o sus conexiones pueden estar estresados.

Tiempo de vida (TTL)

Traceroute hace uso de una función del campo Tiempo de vida (TTL) en el encabezado de Capa 3 y Mensaje excedido en tiempo ICMP. El campo TTL se usa para limitar la cantidad de saltos que un paquete puede cruzar. Cuando un paquete ingresa a un router, el campo TTL disminuye en 1. Cuando el TTL llega a cero, el router no envía el paquete y éste es descartado.

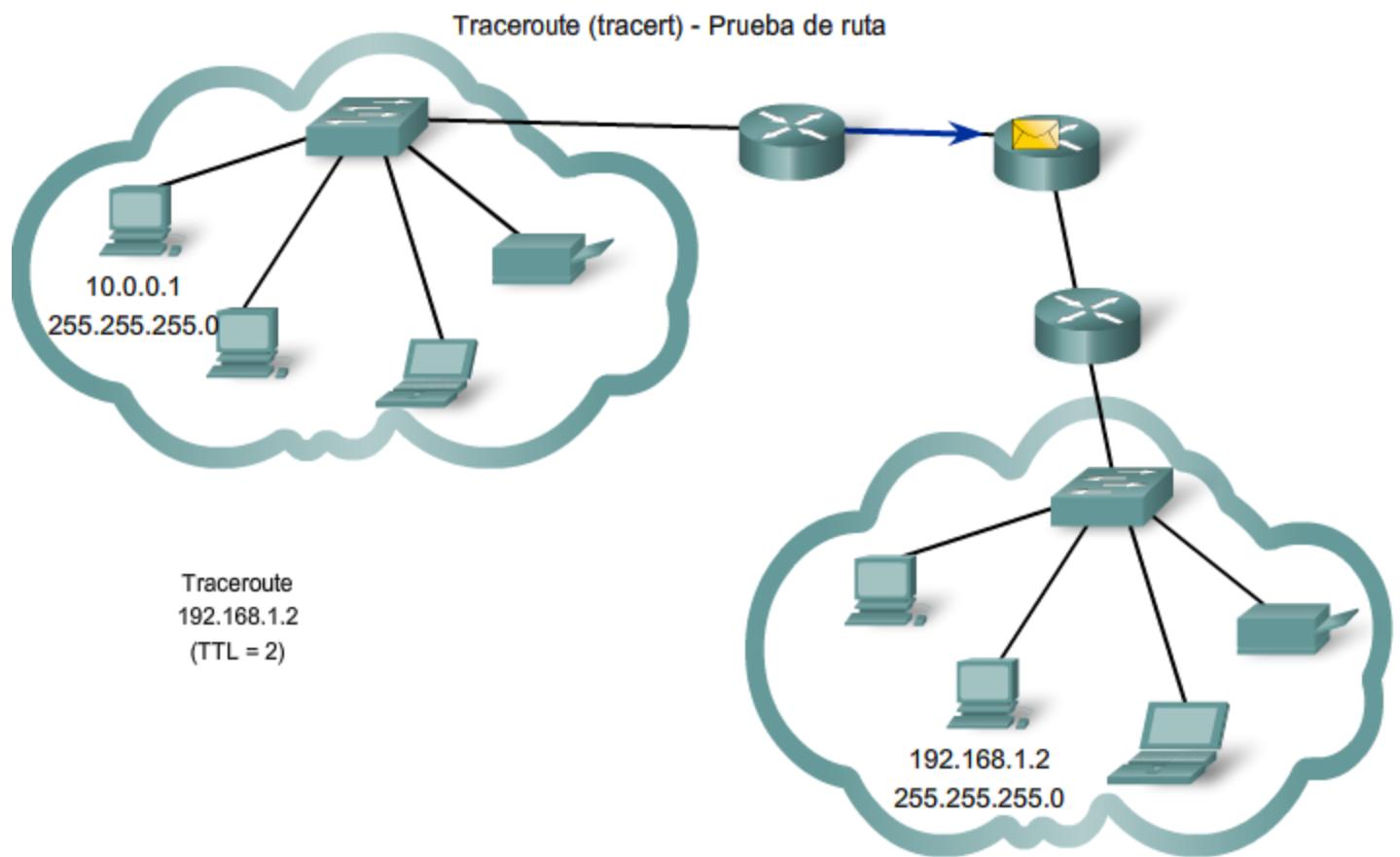
Además de descartar el paquete, el router normalmente envía un mensaje de tiempo superado de ICMP dirigido al host de origen. Este mensaje de ICMP estará conformado por la dirección IP del router que respondió.

Reproduzca la animación en la figura para ver cómo Traceroute aprovecha el TTL.

La primera secuencia de mensajes enviados desde traceroute tendrá un campo de TTL de uno. Esto hace que el TTL expire el límite de tiempo del paquete en el primer router. Este router luego responde con un mensaje de ICMP. 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 exigen 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 del mensaje de tiempo superado de ICMP.



6.6.5 ICMPv4. Protocolo que admite pruebas y mensajería

A pesar de que Ipv4 no es un protocolo confiable, ofrece el envío de mensajes en caso de determinados errores. Estos mensajes se envían mediante servicios del Control Messaging Protocol (Protocolo de mensajes de control de Internet, ICMPv4). 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 por razones de seguridad.

ICMP es el protocolo de mensajería para el conjunto de aplicaciones TCP/IP. ICMP proporciona mensajes de control y error y se usa mediante las utilidades ping y traceroute. A pesar de que ICMP usa el soporte básico de IP como si fuera un protocolo ICMP de mayor nivel, en realidad es una capa 3 separada del conjunto de aplicaciones TCP/IP.

Los tipos de mensajes ICMP, y los motivos por los que se envían, son vastos. Se tratarán algunos de los mensajes más comunes.

Los mensajes ICMP que se pueden enviar incluyen:

- Confirmación de host
- Destino o servicio inalcanzable
- Tiempo excedido
- Redirección de ruta
- Disminución de velocidad en origen

Confirmación de host

Se puede utilizar un Mensaje de eco del ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. El host que recibe el mensaje de eco responde mediante la respuesta de eco de ICMP, como se muestra en la figura. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

Destino o servicio inalcanzable

Se puede usar el destino inalcanzable de ICMP para notificar a un host que el destino o servicio es inalcanzable. Cuando un host o router recibe un paquete que no puede enviar, puede enviar un paquete de destino inalcanzable de ICMP al host que origina el paquete. El paquete de destino inalcanzable tendrá códigos que indican el motivo por el cual el paquete no pudo ser enviado.

Entre los códigos de destino inalcanzable se encuentran:

0 = red inalcanzable

- 11.. = host inalcanzable
11.. = protocolo inalcanzable
11.. = puerto inalcanzable

Los códigos para las respuestas red inalcanzable y host inalcanzable son respuestas de un router que no puede enviar un paquete. Si un router recibe un paquete para el cual no posee una ruta, puede responder con un código de destino inalcanzable de ICMP = 0, que indica que la red es inalcanzable. Si un router recibe un paquete para el cual posee una ruta conectada pero no puede enviar el paquete al host en la red conectada, el router puede responder con un código de destino inalcanzable de ICMP = 1, que indica que se conoce la red pero que el host es inalcanzable.

Los códigos 2 y 3 (protocolo inalcanzable y puerto inalcanzable) son utilizados por un host final para indicar que el segmento TCP o el datagrama UDP en un paquete no pudo ser enviado al servicio de capa superior.

Cuando el host final recibe un paquete con una PDU de capa 4 que se enviará a un servicio no disponible, el host puede responder al host de origen con un código de destino inalcanzable de ICMP = 2 o con un código = 3, que indica que el servicio no está disponible. Es posible que el servicio no esté disponible debido a que no hay un daemon en funcionamiento que proporcione el servicio o porque la seguridad del host no permite el acceso al servicio.

Tiempo superado

Un router utiliza un mensaje de tiempo superado de ICMP para indicar que no se puede enviar un paquete debido a que el campo TTL del paquete ha expirado. Si un router recibe un paquete y disminuye el campo TTL del paquete a cero, éste descarta el paquete. El router también puede enviar un mensaje de tiempo superado de ICMP al host de origen para informar al host el motivo por el que se descartó el paquete.

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. Si un router recibe un paquete para el cual tiene una ruta y para el próximo salto se conecta con la misma interfaz del paquete recibido, el router puede enviar un mensaje de redireccionamiento de ICMP al host de origen. Este mensaje informará al host de origen acerca del próximo salto en una ruta de la tabla de enrutamiento.

Disminución de velocidad en origen

El mensaje de disminución de velocidad en origen de ICMP puede usarse para informar al origen que deje de enviar paquetes por un tiempo. Si un router no posee suficiente espacio en búfer para recibir paquetes entrantes, un router descartará los paquetes. Si debe hacerlo, también puede enviar un mensaje de disminución de velocidad en origen de ICMP a los hosts de origen por cada mensaje que descarta.

Un host de destino también puede enviar un mensaje de disminución de velocidad en origen si los datagramas llegan demasiado rápido para ser procesados.

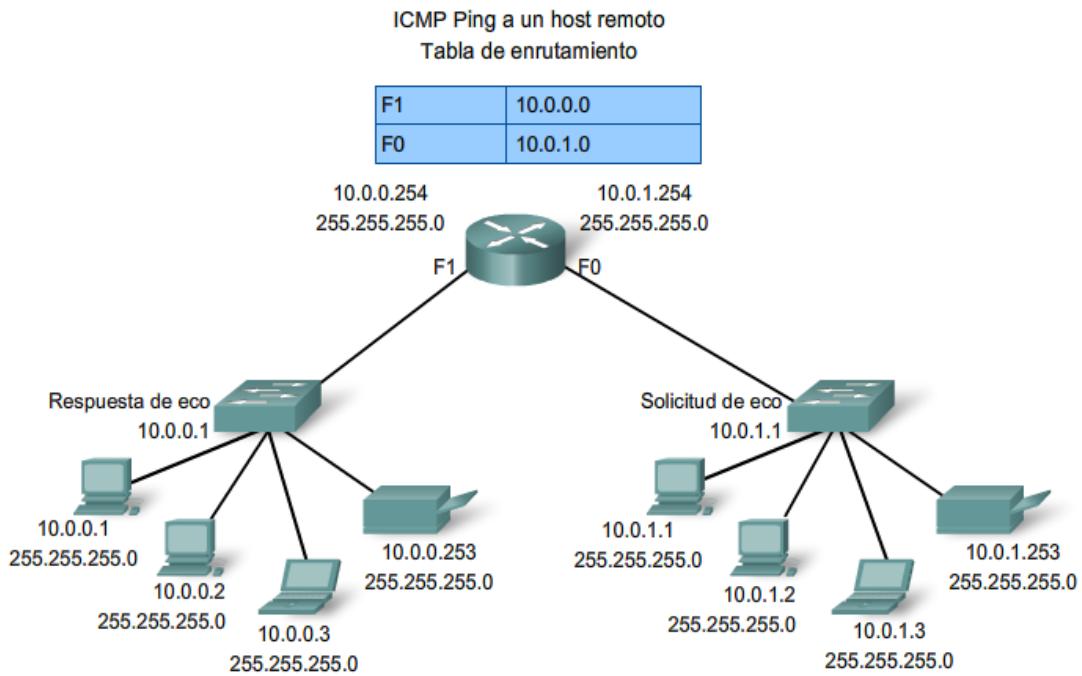
Cuando un host recibe un mensaje de disminución de velocidad en origen de ICMP, lo informa a la capa de transporte. El host de origen puede utilizar el mecanismo de control de flujo de TCP para adaptar la transmisión.

Enlaces:

RFC 792 <http://www.ietf.org/rfc/rfc0792.txt?number=792>

RFC 1122 <http://www.ietf.org/rfc/rfc1122.txt?number=1122>

RFC 2003 <http://www.ietf.org/rfc/rfc2003.txt?number=2003>



6.8 RESUMEN DEL CAPÍTULO

6.8.1 Resumen y revisión

Las direcciones Ipv4 son jerárquicas y tienen porciones de red, subred y host. Una dirección Ipv4 puede representar una red completa, un host específico o la dirección de broadcast de la red.

Se usan diferentes direcciones para comunicaciones de datos unicast, multicast y broadcast.

Las autoridades de direccionamiento y los ISP asignan intervalos de direcciones a los usuarios, que a su vez pueden asignar estas direcciones a sus dispositivos de red de manera estática o dinámica. El intervalo de direcciones asignado puede dividirse en subredes calculando y aplicando máscaras de subred.

Se requiere una planificación de direccionamiento cuidadosa para hacer buen uso del espacio de red disponible. Los requisitos de tamaño, ubicación, uso y acceso son consideraciones a tener en cuenta en el proceso de planificación de direcciones.

Una vez implementada, una red IP debe ser probada para verificar su conectividad y rendimiento operativo.

En este capítulo, aprendió a:

- Explicar la estructura del direccionamiento IP y demostrar la capacidad para convertir números decimales y binarios de 8 bits.
- Dada una dirección IPv4, clasificarla por tipo y describir cómo se utiliza en la red.
- Explicar cómo se asignan las direcciones a redes mediante ISP y dentro de redes a través de administradores.
- Determinar la porción de la red de la dirección host y explicar el rol de la máscara de subred en la división de redes.
- Seguir un IPv4, direccionar información y diseñar criterios, calcular los componentes de direccionamiento adecuados.
- Utilizar utilidades de prueba comunes para verificar y probar la conectividad de la red y el estado operativo del stack del protocolo IP en un host.

7- CAPA DE ENLACE DE DATOS

7.0 INTRODUCCIÓN DEL CAPÍTULO

7.0.1 Introducción del capítulo

Para sostener nuestras comunicaciones, el modelo OSI divide las funciones de una red de datos en capas.

Para resumir:

- La capa de aplicación provee la interfaz al usuario.
- La capa de transporte es responsable de dividir y manejar las comunicaciones entre los procesos que funcionan en los dos sistemas finales.
- Los protocolos de capa de red organizan nuestros datos de comunicación para que puedan viajar a través de internetworks desde el host que los origina hasta el host destino.

Para que los paquetes de capa de red sean transportados desde el host origen al host destino deben recorrer diferentes redes físicas. Estas redes físicas pueden componerse de diferentes tipos de medios físicos, tales como alambres de cobre, microondas, fibras ópticas y enlaces satelitales. Los paquetes de capas de red no tienen una manera de acceder directamente a estos diferentes medios.

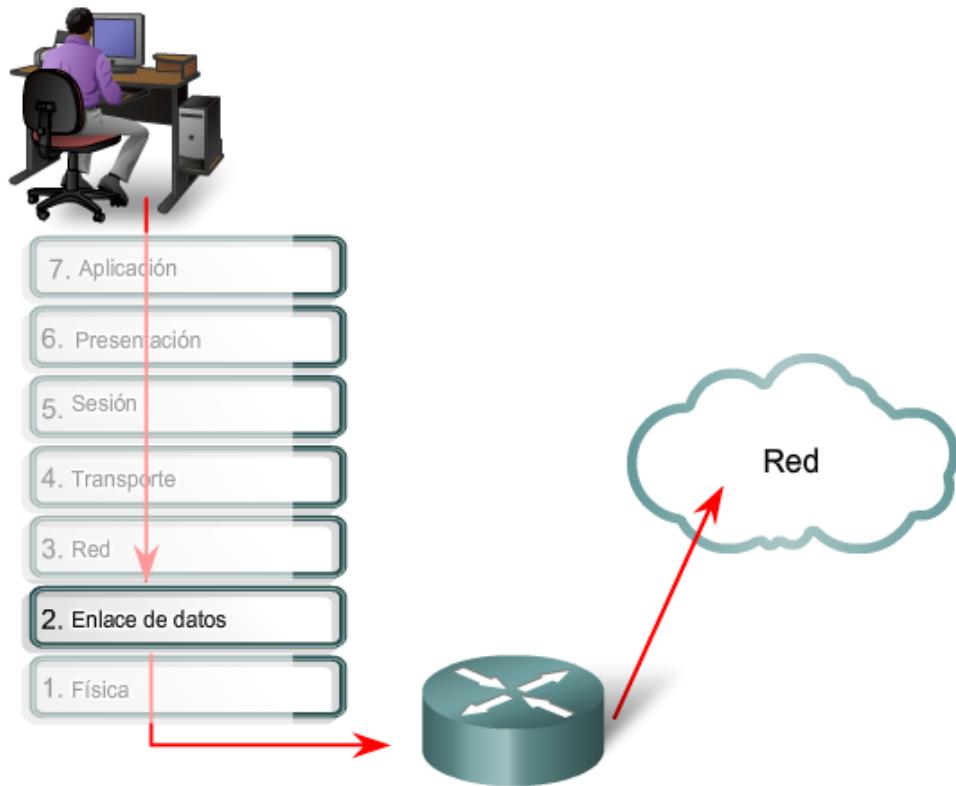
La función de la capa de enlace de datos de OSI es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos.

Este capítulo presenta las funciones generales de la capa de enlace de datos y de los protocolos asociados con ella.

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

- Explicar el papel de los protocolos de capa de enlace de datos en la transmisión de datos.
- Describir cómo la capa de enlace de datos prepara los datos para transmitirlos sobre los medios de red.
- Describir los diferentes tipos de métodos de control de acceso a los medios.
- Identificar varias topologías comunes de red lógica y describir cómo la topología lógica determina el método de control de acceso a los medios para esa red.
- Explicar el propósito de encapsular paquetes en tramas para facilitar el acceso a los medios.
- Describir la estructura de trama de la Capa 2 e identificar campos genéricos.
- Explicar el papel de los campos clave de encabezado de trama y tráiler, lo que incluye direccionamiento, calidad de servicio, tipo de protocolo y secuencia de verificación de trama.



La capa de enlace de datos prepara datos de red para la red física.

7.1 CAPA DE ENLACE DE DATOS: ACCESO AL MEDIO

7.1.1 Capa de enlace de datos: soporte y conexión a servicios de capa superior

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes.

La capa de enlace de datos realiza dos servicios básicos:

Permite a las capas superiores acceder a los medios usando técnicas, como tramas.

Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

Como con cada una de las capas OSI, existen términos específicos para esta capa:

Trama: el PDU de la capa de enlace de datos.

Nodo: la notación de la Capa 2 para dispositivos de red conectados a un medio común.

Medios/medio (físico)*: los medios físicos para la transferencia de información entre dos nodos.

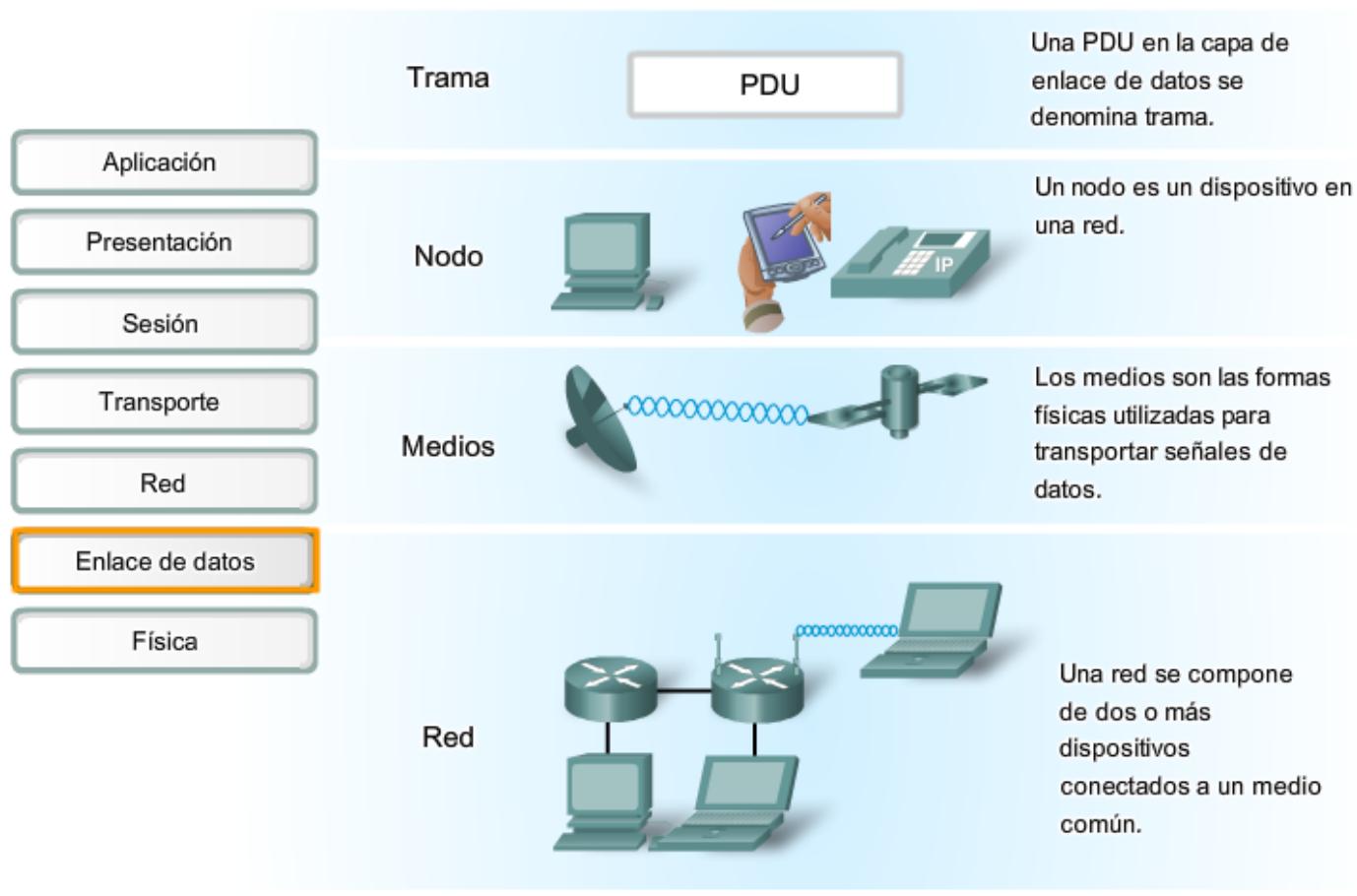
Red (física)**: dos o más nodos conectados a un medio común.

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de una red física.

*Es importante comprender el significado de las palabras medio y medios en el contexto de este capítulo. Aquí, estas palabras se refieren al material que realmente transporta las señales que representan los datos transmitidos. Los medios son el cable de cobre, la fibra óptica físicos o el entorno a través de los cuales la señal viaja. En este capítulo, medios no se refiere a programación de contenido tal como audio, animación, televisión y video, como se utiliza al referirse a contenidos digitales y multimedia.

**Una red física es diferente de una red lógica. Las redes lógicas se definen en la capa de red mediante la configuración del esquema de direccionamiento jerárquico. Las redes físicas representan la interconexión de dispositivos de medios comunes. Algunas veces, una red física también es llamada segmento de red.

Términos de la capa de enlace de datos



Acceso al medio de la capa superior

Como hemos mencionado, un modelo de red permite que cada capa funcione con un mínimo interés por los papeles de las otras capas. La capa de enlace de datos releva a las capas superiores de la responsabilidad de colocar datos en la red y de recibir datos de la red. Esta capa proporciona servicios para soportar los procesos de comunicación para cada medio por el cual se transmitirán los datos.

En cualquier intercambio de paquetes de capas de red, puede haber muchas transiciones de medios y capa de enlace de datos. En cada salto a lo largo de la ruta, un dispositivo intermediario, generalmente un router, acepta las tramas de un medio, desencapsula la trama y luego envía el paquete a una nueva trama apropiada para los medios de tal segmento de la red física.

Imagine una conversación de datos entre dos hosts distantes, como una PC en París con un servidor de Internet en Japón. Aunque los dos hosts puedan comunicarse con sus Protocolos de capa de red par (por ejemplo, IP) es probable que numerosos Protocolos de capa de enlace de datos se estén usando para transportar paquetes IP a través de varios tipos de LAN y WAN. Este intercambio de paquetes entre dos hosts requiere una diversidad de protocolos que debe existir en la capa de enlace de datos. Cada transición a un router puede requerir un protocolo de capa de enlace de datos diferente para el transporte a un medio nuevo.

Observe en la figura que cada enlace entre dispositivos utiliza un medio diferente. Entre la PC y el router puede haber un enlace Ethernet. Los routers están conectados a través de un enlace satelital y la computadora portátil está conectada a través de un enlace inalámbrico al último router. En este ejemplo, como un paquete IP viaja desde la PC hasta la computadora portátil, será encapsulado en la trama Ethernet, desencapsulado, procesado y luego encapsulado en una nueva trama de enlace de datos para cruzar el enlace satelital. Para el enlace final, el paquete utilizará una trama de enlace de datos inalámbrica desde el router a la computadora portátil.

La capa de enlace de datos aísla de manera efectiva los procesos de comunicación en las capas superiores desde las transiciones de medios que pueden producirse de extremo a extremo. Un paquete se recibe de un protocolo de capa superior y se dirige a éste, en este caso Ipv4 o Ipv6, que no necesita saber qué medio de comunicación utilizará.

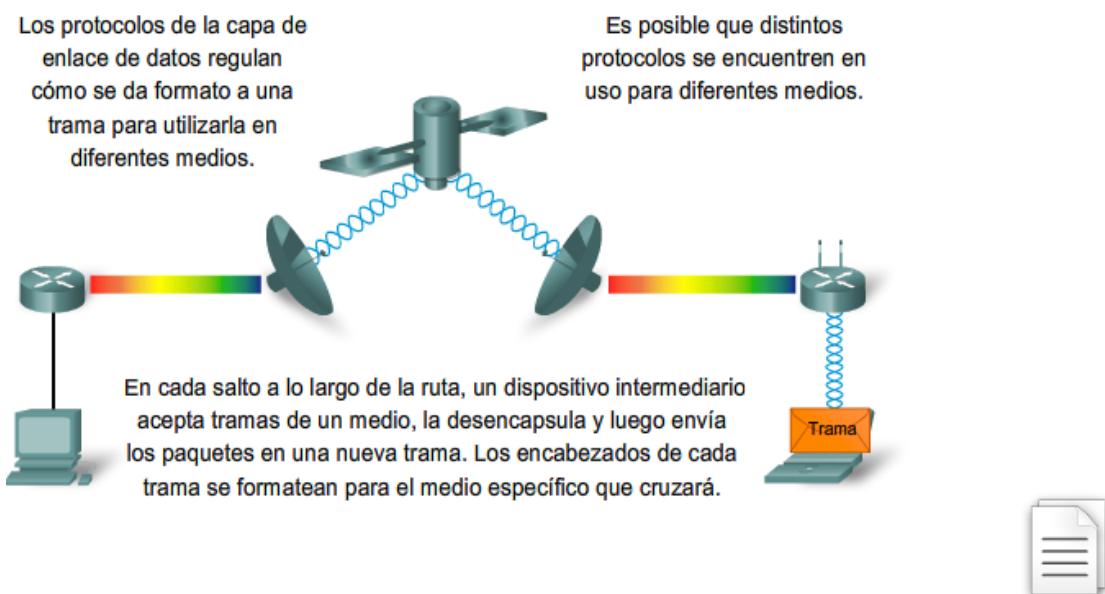
Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso 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.

El rango de los servicios de la capa de enlace de datos tiene que incluir todos los tipos de medios actualmente utilizados y los métodos para acceder a ellos. Debido a la cantidad de servicios de comunicación provistos por la capa de enlace de datos, es difícil generalizar su papel y proporcionar ejemplos de un conjunto de servicios genéricos. Por esa razón, note que cualquier protocolo dado puede o no puede soportar todos estos servicios de capa de enlace de datos.

ISO 7498 – http://www.sigcomm.org/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-1.TXT

Internetworking Basics – http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#wp1020777

MTU – http://www.tcpipguide.com/free/t_IPDatagramSizeMaximumTransmissionUnitMTUFragmentat.htm
Capa de enlace de datos



7.1.2 Capa de enlace de datos: control de la transferencia a través de medios locales

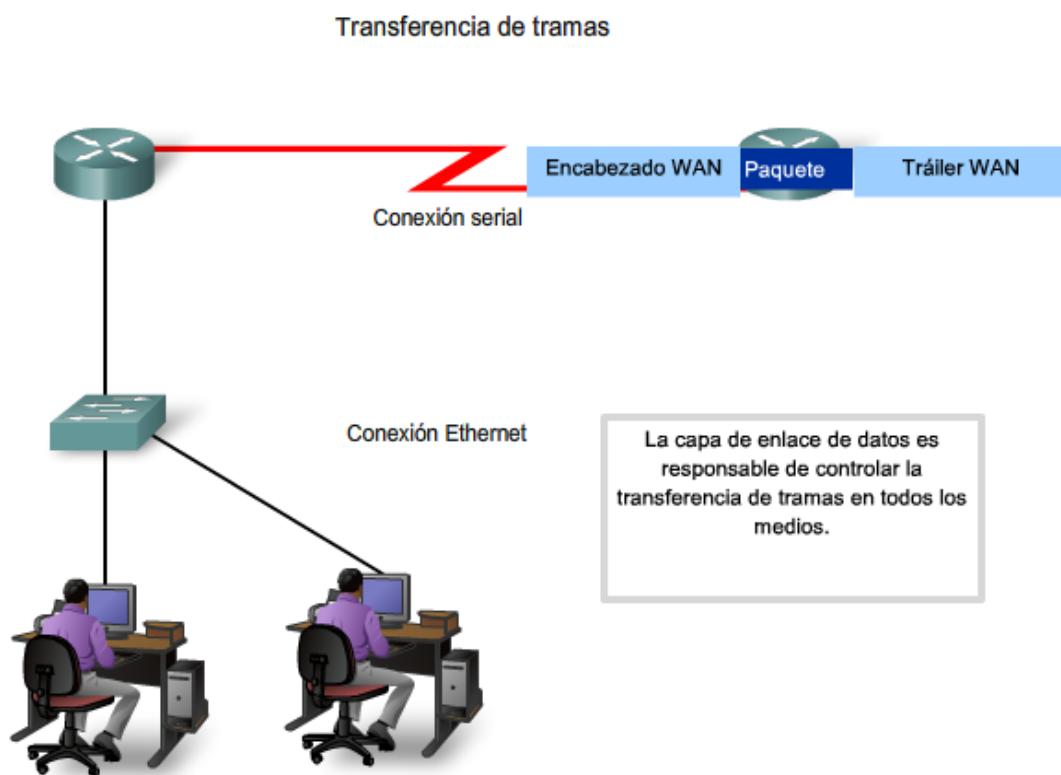
Los protocolos de la Capa 2 especifican la encapsulación de un paquete en una trama y las técnicas para colocar y sacar el paquete encapsulado de cada medio. La técnica utilizada para colocar y sacar la trama de los medios se llama método de control de acceso al medio. Para que los datos se transfieran a lo largo de una cantidad de medios diferentes, puede que se requieran diferentes métodos de control de acceso al medio durante el curso de una única comunicación.

Cada entorno de red que los paquetes encuentran cuando viajan desde un host local hasta un host remoto puede tener características diferentes. Por ejemplo: un entorno de red puede componerse de muchos hosts disputando el acceso a un medio de red de forma ad hoc. Otro entorno puede componerse de una conexión directa entre sólo dos dispositivos sobre los cuales fluyen los datos de manera secuencial como bits de manera ordenada.

Los métodos de control de acceso al medio descritos en los protocolos de capa de enlace de datos definen los procesos por los cuales los dispositivos de red pueden acceder a los medios de red y transmitir marcos en diferentes entornos de red.

Un nodo que es un dispositivo final utiliza un adaptador para hacer la conexión a la red. Por ejemplo: para conectarse a una LAN, el dispositivo usaría la tarjeta de interfaz de red (NIC) para conectarse a los medios LAN. El adaptador administra la trama y el control de acceso a los medios.

En dispositivos intermediarios, tales como un router donde los tipos de medios pueden cambiar para cada red conectada, se utilizan diferentes interfaces físicas en el router para encapsular el paquete en la trama apropiada y se utiliza un método de control de acceso a los medios adecuado para acceder a cada enlace. 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 tramas, utilizará los servicios de la capa de enlace de datos para recibir la trama desde un medio, desencapsularlo en la PDU de la Capa 3, reencapsular la PDU en una trama nueva y colocar la trama en el medio del siguiente enlace de la red.



7.1.3 Capa de enlace de datos: creación de 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. La información de control puede indicar:

- Qué nodos están en comunicación con otros
- Cuándo comienza y cuándo termina la comunicación entre nodos individuales
- Qué errores se producen mientras los nodos se comunican
- Qué nodos se comunicarán luego

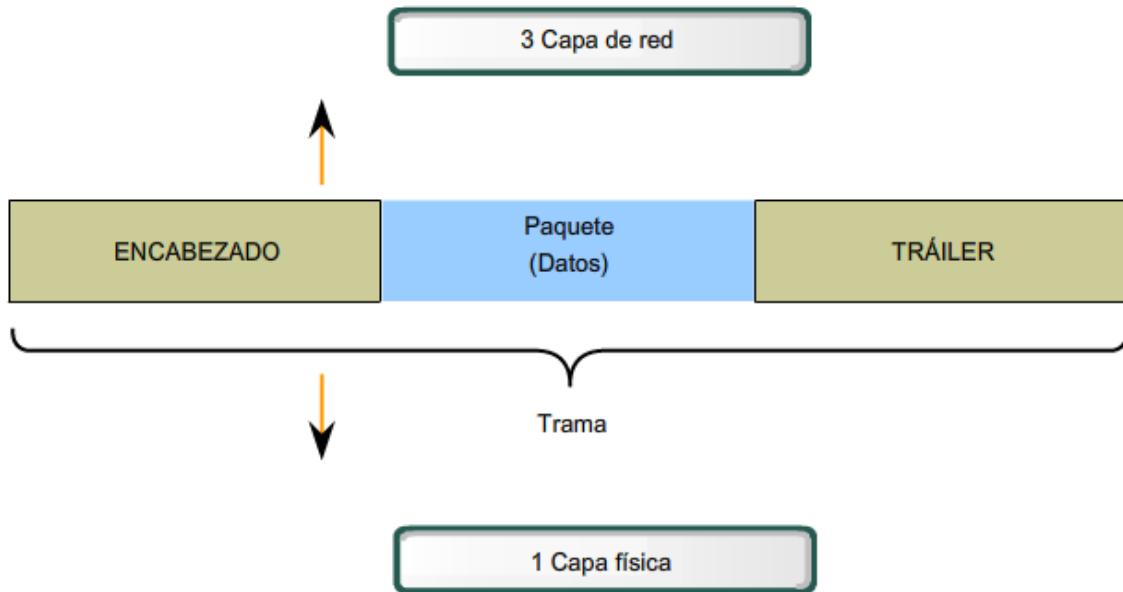
La Capa de enlace de datos prepara un paquete para transportar a través de los medios locales encapsulándolo con un encabezado y un tráiler para crear una trama.

A diferencia de otros PDU que han sido analizados en este curso, la trama de la capa de enlace de datos incluye:

- Datos: El paquete desde la Capa de red
- Encabezado: contiene información de control como direccionamiento y está ubicado al comienzo del PDU
- Tráiler: contiene información de control agregada al final del PDU

Estos elementos de trama se analizarán detalladamente más adelante en este capítulo.

Servicios de la capa de enlace de datos



Formato de datos para la transmisión

Cuando los datos viajan por los medios, se convierten en un stream de bits, o en 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 puede ser recibida por los nodos y decodificada en paquetes en el destino.

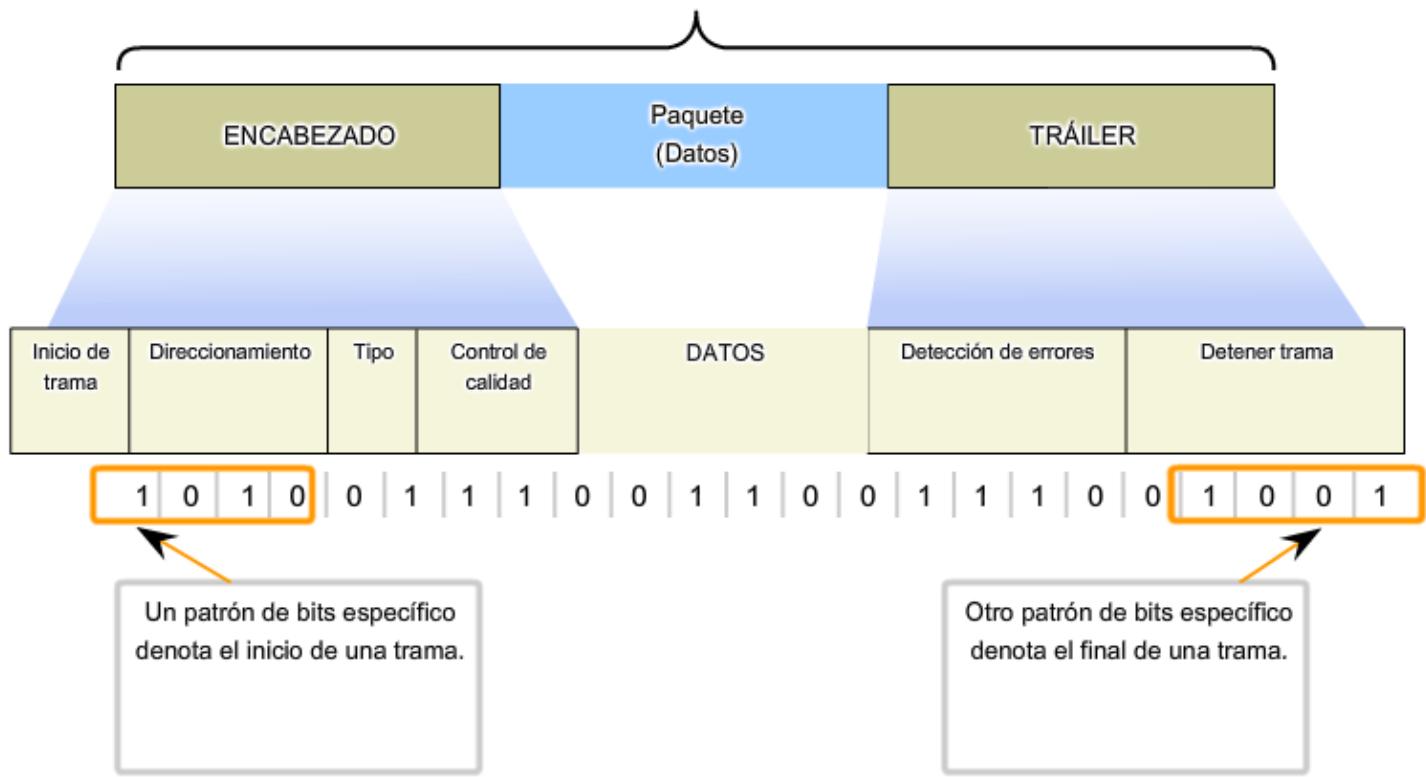
Los tipos de campos típicos incluyen:

- Campos indicadores de comienzo y detención: Límites de comienzo y finalización de la trama
- Nombrar o direccionar campos
- Campo tipo: El tipo de PDU contenido en la trama
- Calidad: campos de control
- Campo de datos: Carga de tramas (Paquete de capa de red)

Campos en el extremo final de la trama desde el tráiler. Estos campos se utilizan para la detección de errores y marcan el final de la trama.

No todos los protocolos incluyen todos estos campos. Los estándares para un protocolo de enlace de datos definen el formato real de la trama. Los ejemplos de formatos de tramas se analizarán al final de este capítulo.

Formateo de datos para la transmisión



7.1.4 Capa de enlace de datos: conexión de servicios de capa superior a los medios

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos o medios inalámbricos.

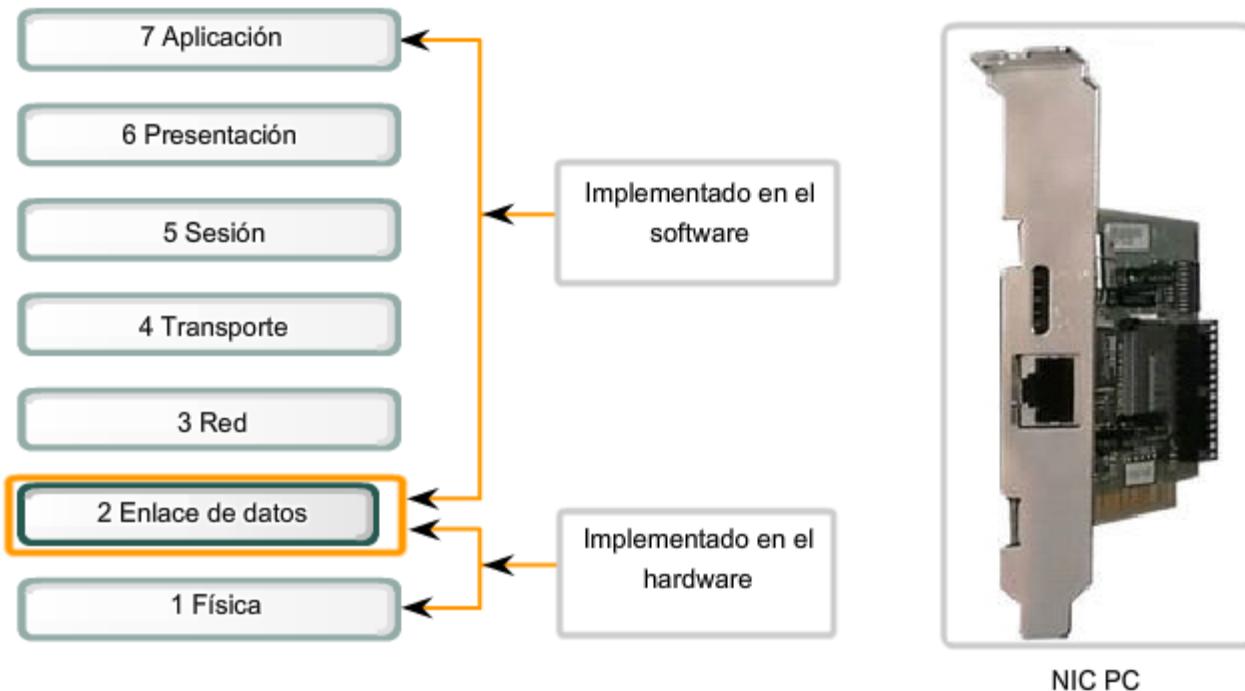
En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de una computadora y hace la conexión entre los procesos de software que se ejecutan en la computadora y los medios físicos. Sin embargo, la NIC no es solamente una entidad física.

El software asociado con la NIC permite que la NIC realice sus funciones de intermediaria preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados.

Conexión de los servicios de la capa superior con los medios

La capa de enlace de datos conecta las capas del software y del hardware.

Los dispositivos físicos dedicados a la capa de enlace de datos tienen los componentes de hardware y software.



Subcapas de enlace de datos

Para sostener una gran variedad de funciones de red, la capa de enlace de datos a menudo se divide en dos subcapas: una subcapa superior y una subcapa inferior.

- La subcapa superior define los procesos de software que proveen servicios a los Protocolos de capa de red.
- La subcapa inferior define los procesos de acceso a los medios realizados por el hardware.

Separar la Capa de enlace de datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior. Tal es el caso en muchas tecnologías LAN, incluida Ethernet.

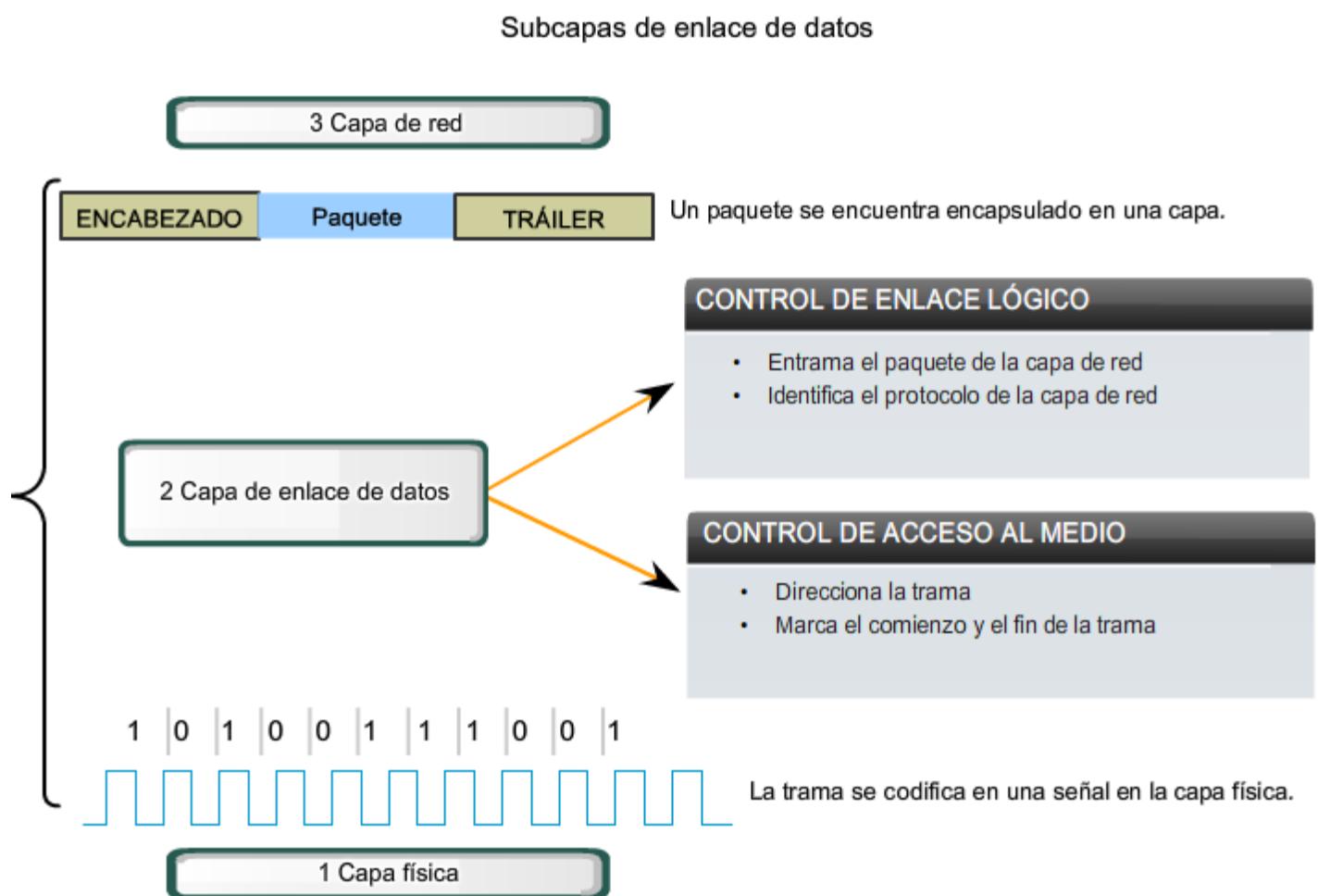
Las dos subcapas comunes de LAN son:

Control de enlace lógico

El control de enlace lógico (LLC) coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

Control de acceso al medio

El control de acceso al medio (MAC) proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.



7.1.5 Capa de enlace de datos: Estándares

A diferencia de los protocolos de las capas superiores del conjunto TCP/IP, los protocolos de capa de enlace de datos generalmente no están definidos por solicitudes de comentarios (RFC). A pesar de que el Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, la IETF no define las funciones ni la operación de esa capa de acceso a la red del modelo. La capa de acceso de red TCP/IP es el equivalente de las capas de enlace de datos OSI y la física. Estas dos capas se verán en capítulos separados para un análisis más detallado.

Los protocolos y servicios funcionales en la Capa de enlace de datos son descriptos por organizaciones de ingeniería (como IEEE, ANSI y ITU) y compañías en comunicaciones. Las organizaciones de ingeniería establecen estándares y protocolos públicos y abiertos. Las compañías de comunicaciones pueden establecer y utilizar protocolos propios para aprovechar los nuevos avances en tecnología u oportunidades de mercado.

Los servicios y especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en una variedad de 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.

Las organizaciones de ingeniería que definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos incluyen:

- Organización Internacional para la Estandarización (ISO)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Instituto Nacional Estadounidense de Estándares (ANSI)
- Unión Internacional de Telecomunicaciones (ITU)

A diferencia de los protocolos de la capa superior que están implementados principalmente en el software como el sistema operativo de host o aplicaciones específicas, los procesos de la Capa de enlace de datos se producen tanto en el software como en el hardware. Los protocolos en esta capa se implementan dentro de la electrónica de los adaptadores de red con los que el dispositivo se conecta a la red física.

Por ejemplo: un dispositivo que implementa la capa de enlace de datos en una computadora sería la tarjeta de interfaz de red (NIC). En una computadora portátil, se utiliza comúnmente un adaptador PCMCIA inalámbrico. Cada uno de estos adaptadores es el hardware que cumple con los estándares y protocolos de la Capa 2.

<http://www.iso.org>

<http://www.ieee.org>

<http://www.ansi.org>

<http://www.itu.int>

Estándares para la capa de enlace de datos

| ISO: | HDLC (Control de enlace de datos de alto nivel) |
|-------|--|
| IEEE: | 802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN [LAN inalámbrico]) |
| ITU: | Q.922 (Estándar de Frame Relay) Q.921 (Estándar de enlace de datos ISDN) HDLC (Control de enlace de datos de alto nivel) |
| ANSI: | 3T9.5 ADCCP (Protocolo de control de comunicación avanzada de datos) |

7.2 TECNICAS DE CONTROL DE ACCESO AL MEDIO

7.2.1 Colocar tramas en los medios

La regulación de la colocación de tramas de datos en los medios es conocida como control de acceso al medio. Entre las diferentes implementaciones de los protocolos de la capa de enlace de datos, hay diferentes métodos de control de acceso a los medios. Estas técnicas de control de acceso al medio definen si los nodos comparten los medios y de qué manera lo hacen.

El control de acceso al medio es el equivalente a las reglas de tráfico que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso al medio sería el equivalente a vehículos ignorando el resto del tráfico e ingresando al camino sin tener en cuenta a los otros vehículos.

Sin embargo, no todos los caminos y entradas son iguales. El tráfico puede ingresar a un camino confluendo, 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.

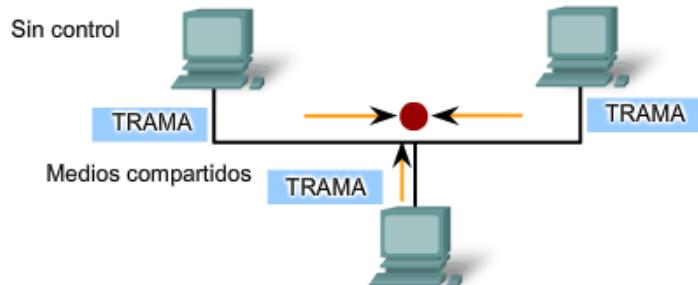
De la misma manera, hay diferentes formas de regular la colocación de tramas en los medios. Los protocolos en la capa de enlace de datos definen las reglas de acceso a los diferentes medios. Algunos métodos de control de acceso al medio utilizan procesos altamente controlados para asegurar que las tramas se coloquen con seguridad en los medios. Estos métodos se definen mediante protocolos sofisticados, que requieren mecanismos que introducen sobrecargas a la red.

El método de control de acceso al medio utilizado depende de:

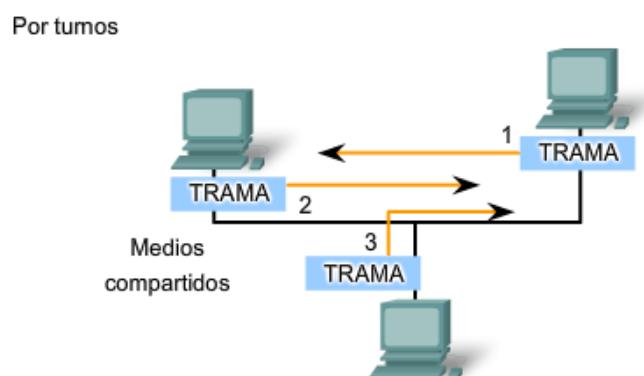
- Compartir medios: si y cómo los nodos comparten los medios.
- Topología: cómo la conexión entre los nodos se muestra a la capa de enlace de datos.

Métodos de control de acceso al medio

Si no se realiza ningún control, se producirían muchas colisiones. Las colisiones producen tramas corruptas que deben volver a enviarse.



Los métodos que cumplen con un alto grado de control impiden las colisiones, pero el proceso tiene muchas sobrecargas.



Los métodos que cumplen con un bajo nivel de control tienen pocas sobrecargas, pero hay colisiones con mayor frecuencia.

7.2.2 Control de acceso al medio para medios compartidos

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:

- Controlado: Cada nodo tiene su propio tiempo para utilizar el medio
- Basado en la contención: Todos los nodos compiten por el uso del medio

Haga clic en las fichas de la figura para ver las diferencias en los dos métodos.

Acceso controlado para medios compartidos

Al utilizar el método de acceso controlado, los dispositivos de red toman turnos, en secuencia, para acceder al medio. A este método se lo conoce como acceso programado o determinístico. Si un dispositivo no necesita acceder al medio, la oportunidad de utilizar el medio pasa al siguiente dispositivo en línea. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino.

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.

Acceso por contención para medios compartidos

Estos métodos por contención, también llamados no deterministas, permiten que cualquier dispositivo intente acceder al medio siempre que haya 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 CSMA falle si dos dispositivos transmiten al mismo tiempo. A esto se lo 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 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 requeridos para corregir errores debidos a esas colisiones disminuyen aún más el throughput.

CSMA es generalmente implementado junto con un método para resolver la contención del medio. Los dos métodos comúnmente utilizados son:

CSMA/Detección de colisión

En CSMA/Detección de colisión (CSMA/CD), el dispositivo monitorea 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

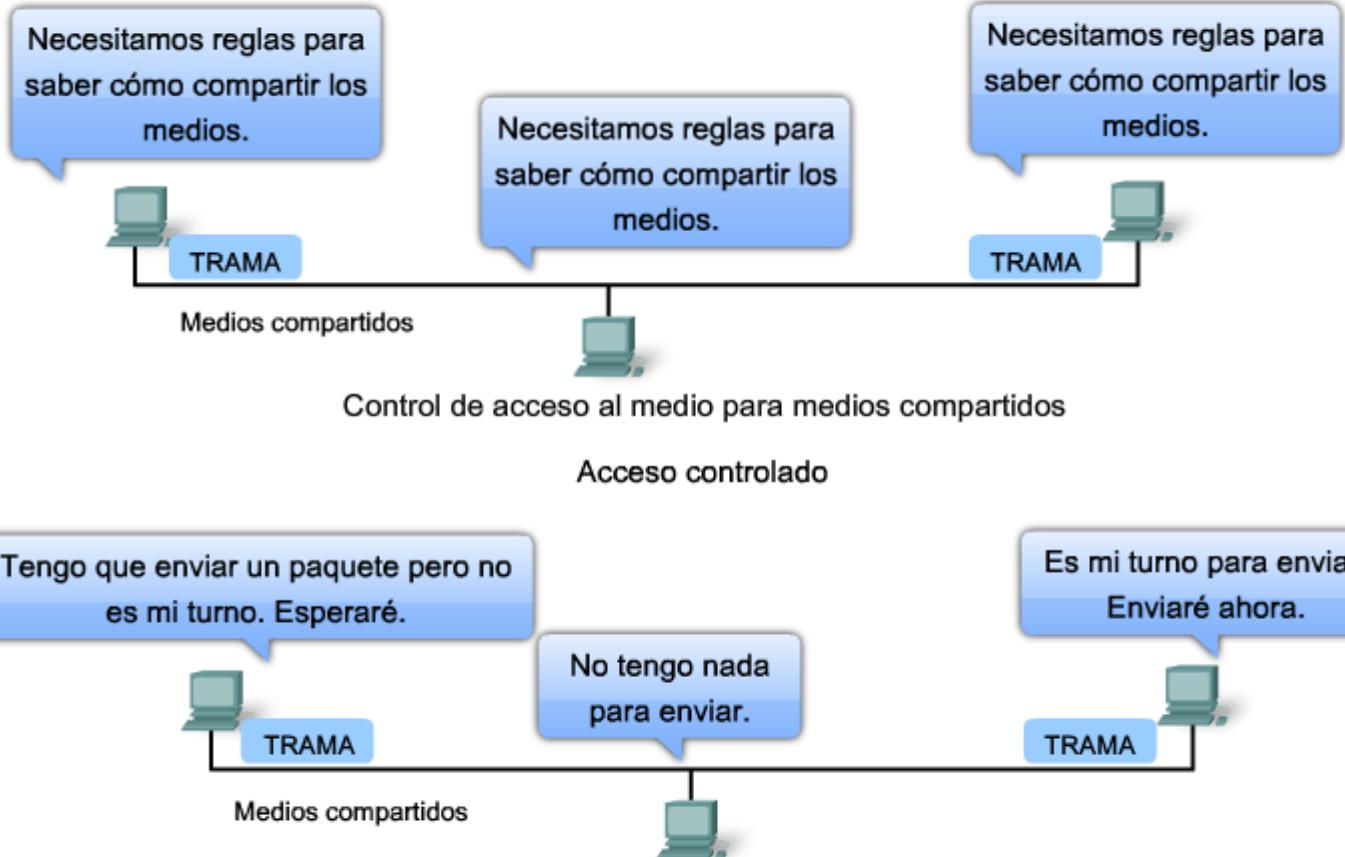
detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet usan este método.

CSMA/Prevención de colisiones

En CSMA/Prevención de colisiones (CSMA/CA), el dispositivo 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. El dispositivo luego envía los datos. Este método es utilizado por las tecnologías de redes inalámbricas 802.11.

Nota: CSMA/CD será explicado más detalladamente en el Capítulo 9.

Control de acceso al medio para medios compartidos



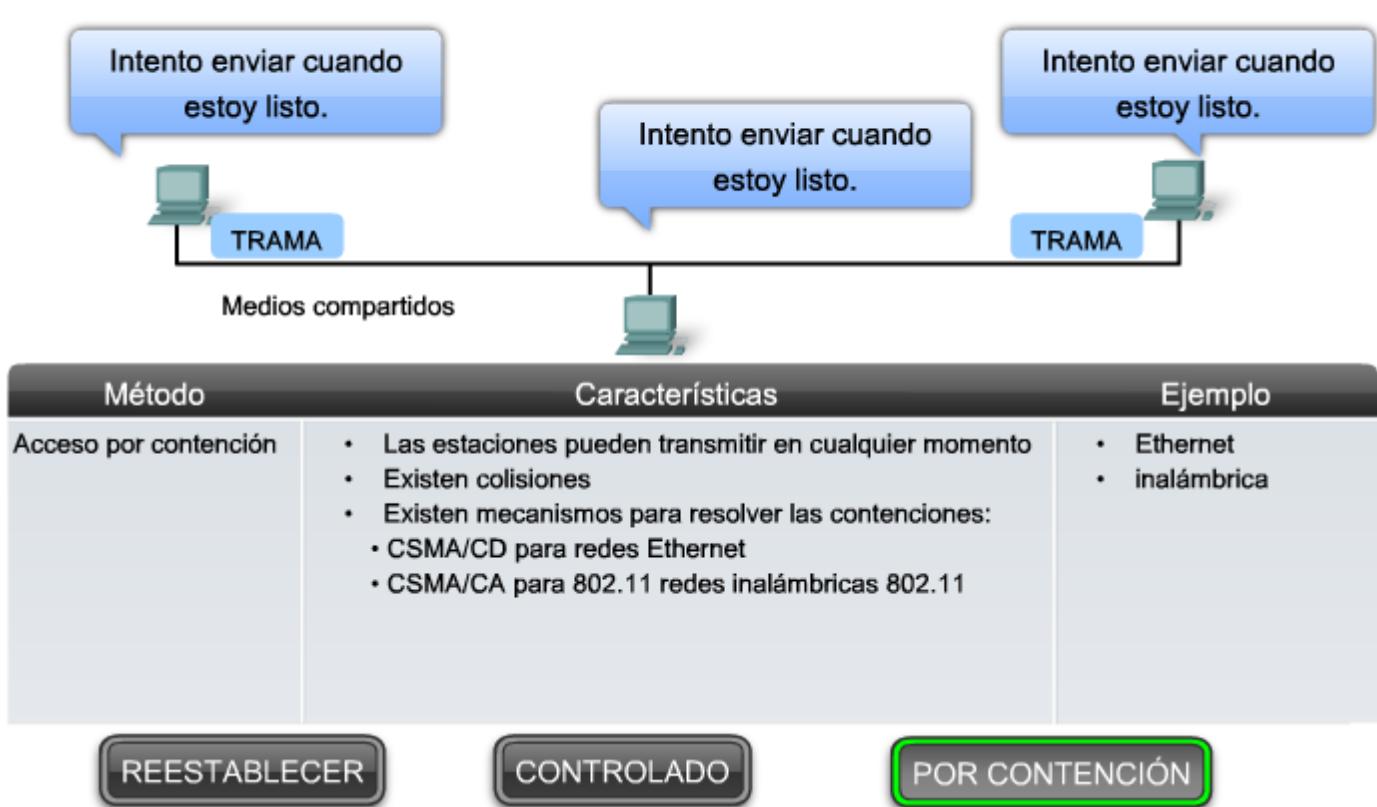
| Método | Características | Ejemplo |
|-------------------|---|---|
| Acceso controlado | <ul style="list-style-type: none">Sólo transmite una estación a la vezLos dispositivos que desean transmitir deben esperar su turnoNo hay colisionesAlgunas redes deterministas utilizan el paso de tokens | <ul style="list-style-type: none">Token RingFDDI |

REESTABLECER

CONTROLADO

POR CONTENCIÓN

Control de acceso al medio para medios compartidos



7.2.3 Control de acceso al medio para medios no compartidos

Los protocolos de control de acceso al medio para medios no compartidos requieren poco o ningún control antes de colocar tramas en los medios. Estos protocolos tienen reglas y procedimientos más simples para el control de acceso al medio. Tal es el caso de las topologías punto a punto.

En las topologías punto a punto, los medios interconectan sólo dos nodos. En esta configuración, los nodos no necesitan compartir los medios con otros hosts ni determinar si una trama está destinada para ese nodo. Por lo tanto, los protocolos de capa de enlace de datos hacen poco para controlar el acceso a medios no compartidos.

Full Duplex y Half Duplex

En conexiones punto a punto, la Capa de enlace de datos tiene que considerar si la comunicación es half-duplex o full-duplex.

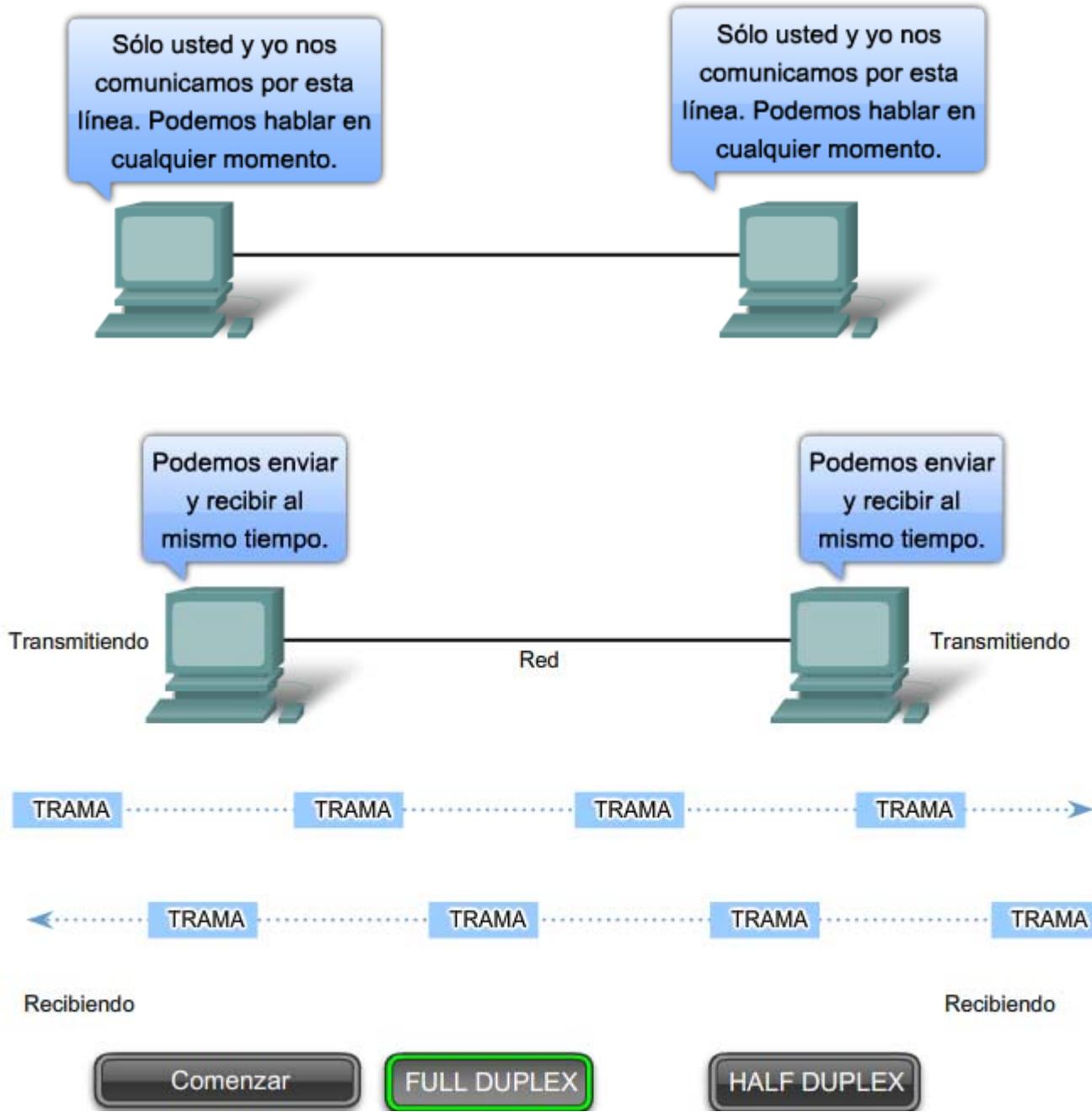
Haga clic en las fichas de la figura para ver las diferencias entre los dos métodos.

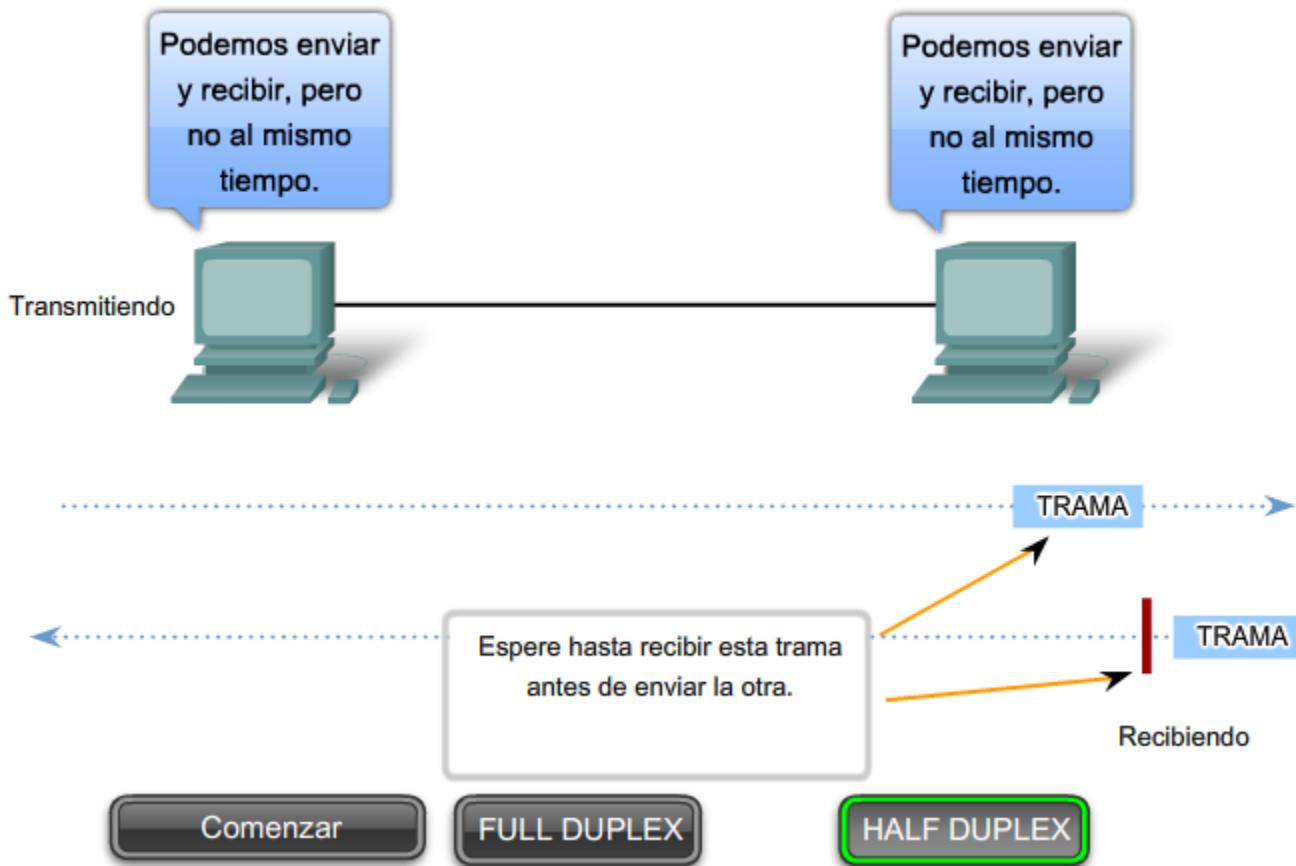
Comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo.

En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.

Los detalles de una técnica de control de acceso al medio específica sólo pueden examinarse estudiando un protocolo específico. Dentro de este curso, estudiaremos Ethernet tradicional, que utiliza CSMA/CD. Otras técnicas se abarcarán en cursos posteriores.

Control de acceso al medio para medios no compartidos





7.2.4 Comparación entre la topología lógica y la topología física

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías de red pueden verse en el nivel físico y el nivel lógico.

La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física. Ésta se abordará en capítulos posteriores de este curso.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La capa de enlace de datos "ve" la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a medios utilizados.

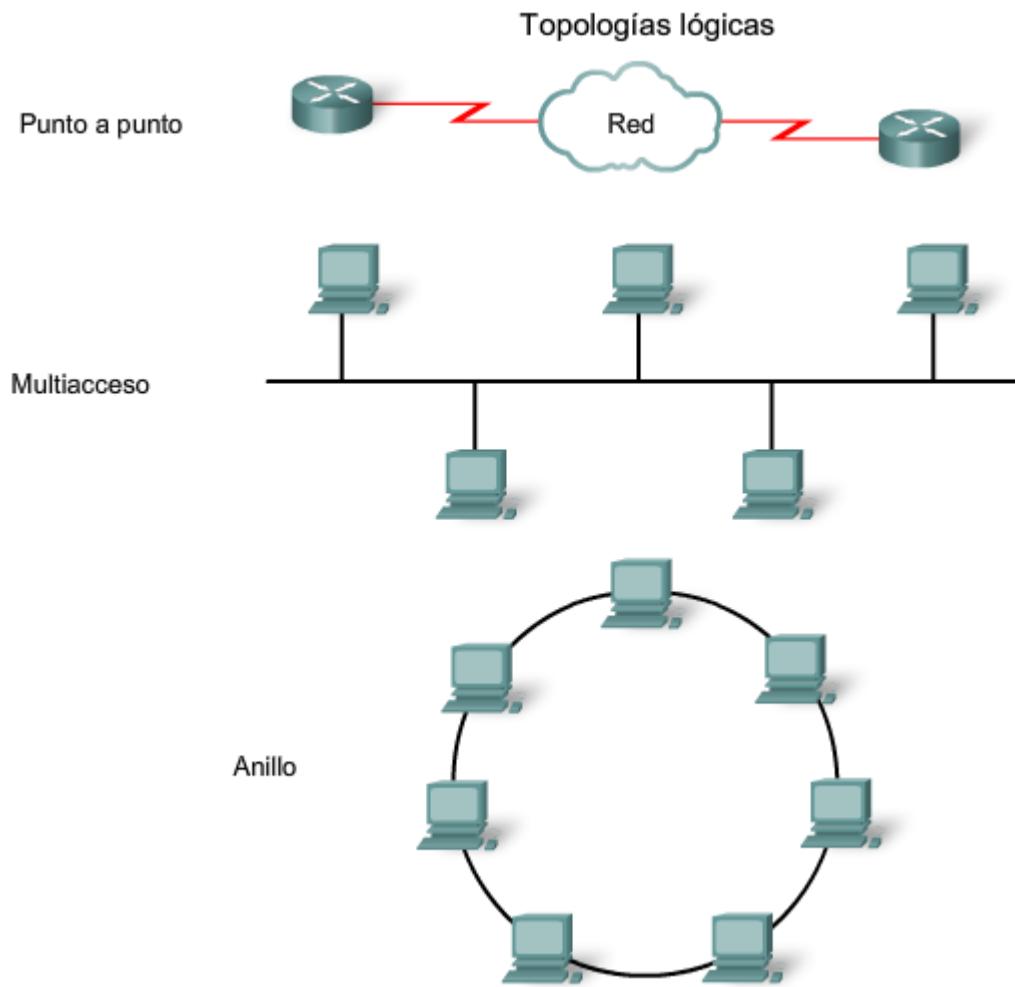
La topología física o cableada de una red probablemente no sea la misma que la topología lógica.

La topología lógica de una red está estrechamente relacionada con el mecanismo utilizado 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 son aplicados a las redes para regular este acceso a los medios. Los métodos de acceso se analizarán con más detalle más adelante.

Las topologías lógica y física generalmente utilizadas en redes son:

- Punto a Punto
- Multi-Acceso
- Anillo

Las implementaciones lógicas de estas topologías y sus métodos asociados de control de acceso a los medios son abordadas en las siguientes secciones.

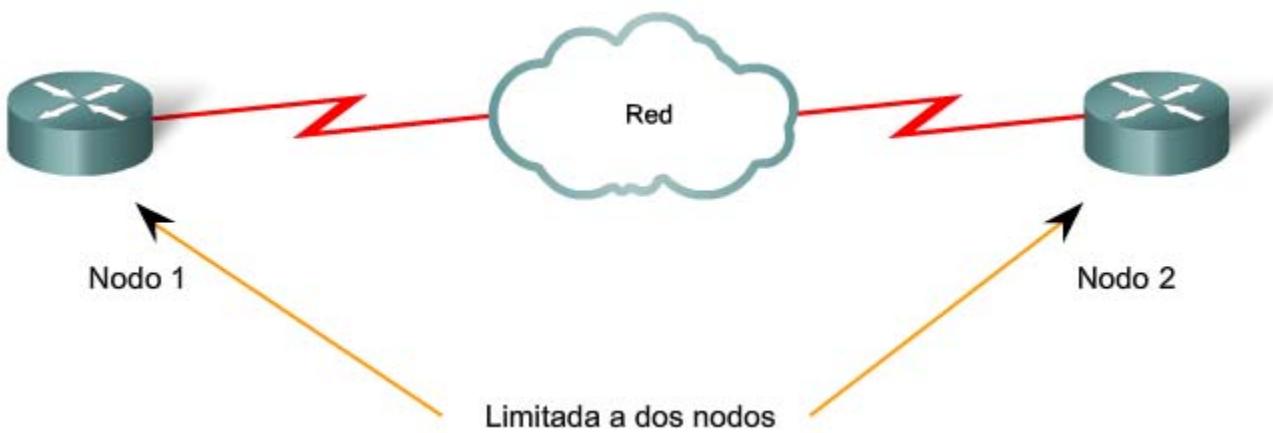


7.2.5 Topología punto a punto

Una topología punto a punto conecta dos nodos directamente entre sí, como se muestra en la figura. En redes de datos con topologías punto a punto, el protocolo de control de acceso al medio puede ser muy simple. Todas las tramas en los medios sólo pueden viajar a los dos nodos o desde éstos. 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.

En redes punto a punto, si los datos sólo pueden fluir en una dirección a la vez, está operando como un enlace half-duplex. Si los datos pueden fluir con éxito a través del enlace desde cada nodo simultáneamente, es un enlace dúplex.

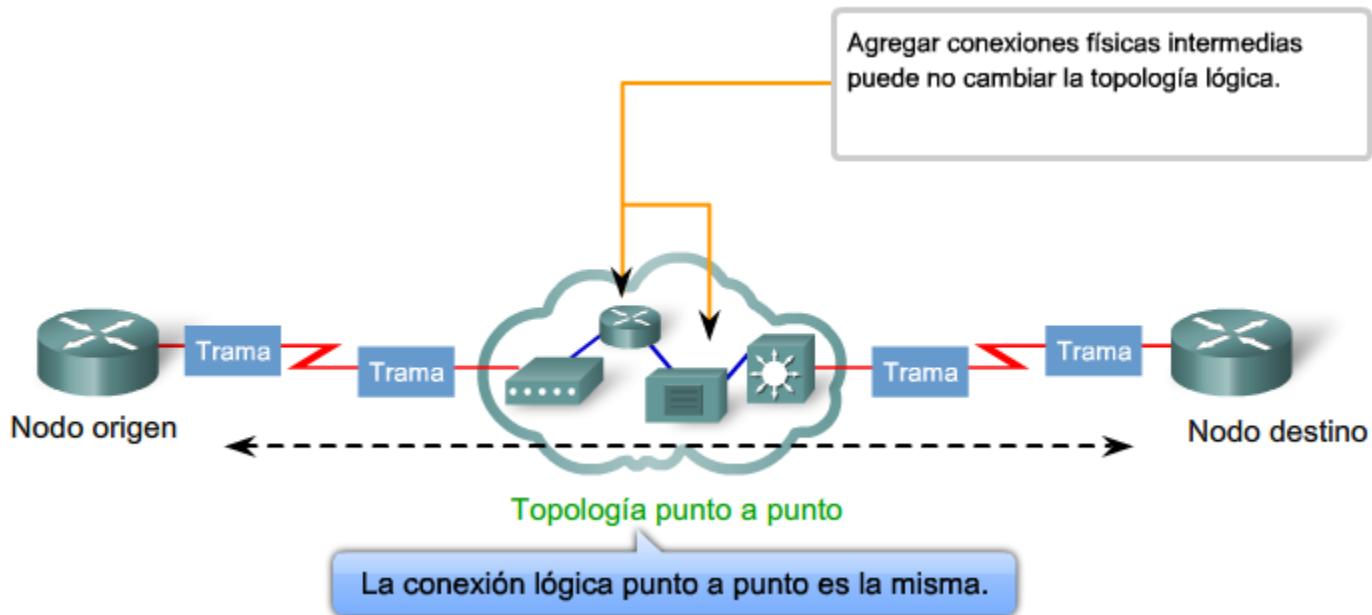
Los Protocolos de capa de enlace podrían proveer procesos más sofisticados de control de acceso a los medios para las topologías lógicas punto a punto, pero esto agregaría un gasto innecesario al protocolo.



Redes punto a punto lógicas

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 intermedios. Sin embargo, el uso de dispositivos físicos en la red no afecta la topología lógica. Como se muestra en la figura, 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 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 se determina por la topología lógica punto a punto, no 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.



7.2.6 Topología multiacceso

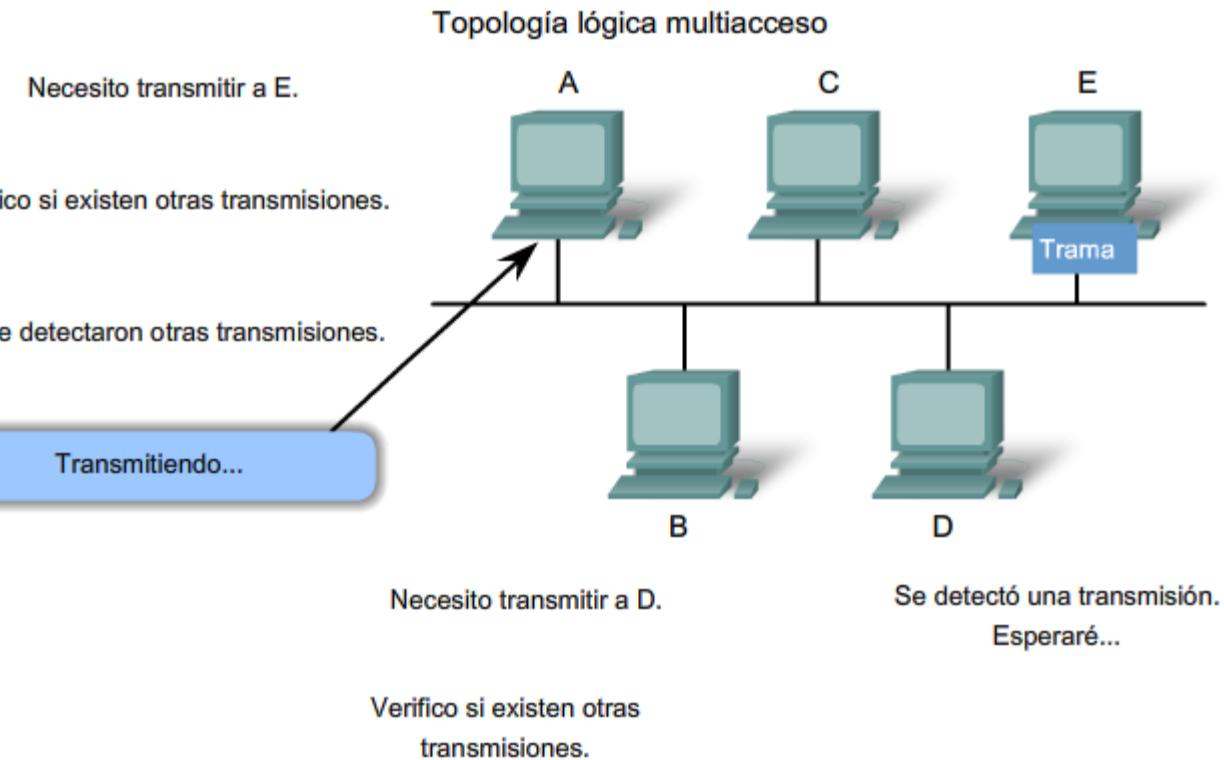
Una topología lógica multiacceso permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos. Los datos desde un sólo nodo pueden colocarse en el medio en cualquier momento. Todos los nodos ven

todas las tramas que están en el medio, pero sólo el nodo al cual la trama está direccionalmente procesa los contenidos de la trama.

Hacer que varios nodos comparten el acceso a un medio requiere un método de control de acceso al medio de enlace de datos que regule la transmisión de datos y, por lo tanto, reduzca las colisiones entre las diferentes señales.

Los métodos de control de acceso al medio utilizado por las topologías multiacceso son generalmente CSMA/CD o CSMA/CA. Sin embargo, métodos de paso de token pueden también utilizarse.

Un número de técnicas de control de acceso a los medios está disponible para este tipo de topología lógica. El protocolo de capa de enlace de datos especifica el método de control de acceso al medio que proporcionará el balance apropiado entre el control de trama, la protección de trama y la sobrecarga de red.



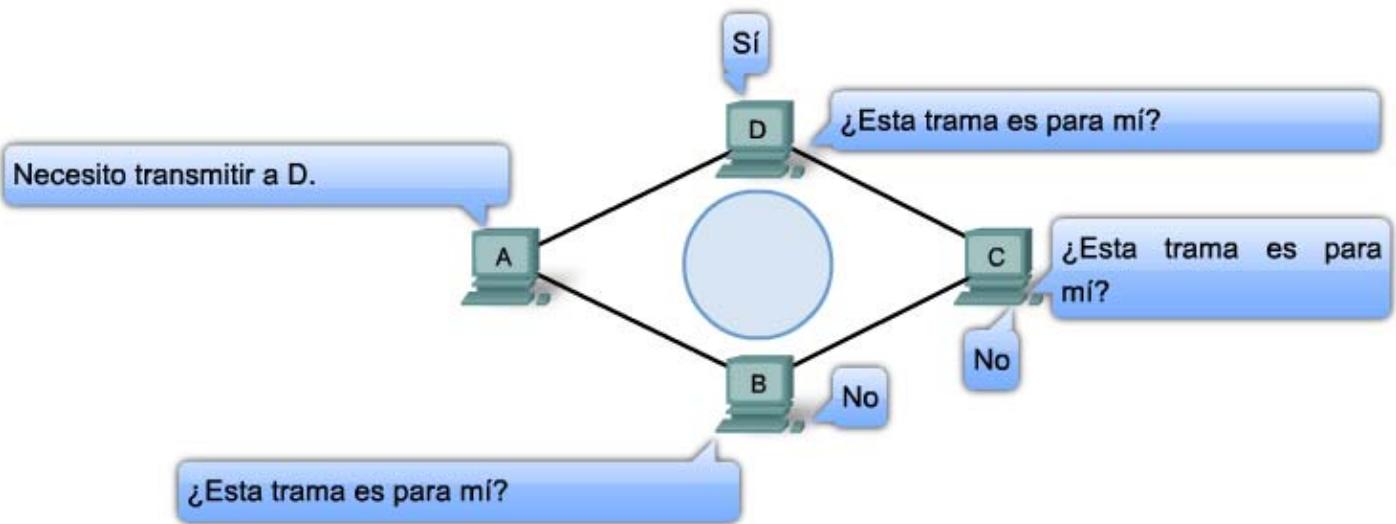
7.2.7 Topología de anillo

En una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionalmente dirigida al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso al medio llamada 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 de destino examinan la trama.

Existen múltiples técnicas de control de acceso a los medios que podrían usarse con un anillo lógico, dependiendo del 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.



7.3 DIRECCIONAMIENTO DEL CONTROL DE ACCESO AL MEDIO Y TRAMADO DE DATOS

7.3.1 Protocolos de la capa de enlace de datos: Trama

Recuerde que a pesar de que hay 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, y
- 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.

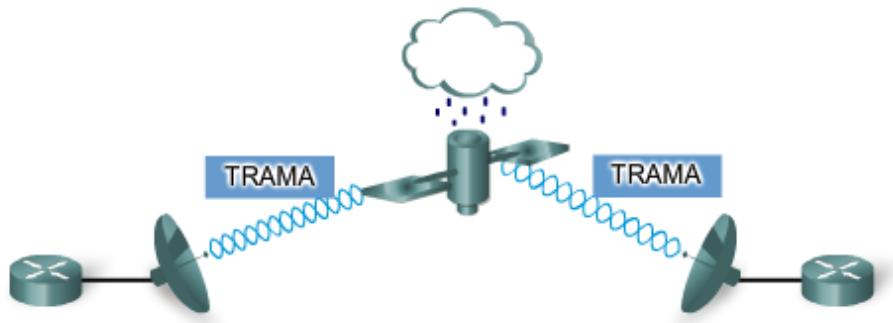
El protocolo de capa de enlace de datos describe las características requeridas para el transporte de paquetes a través de diferentes medios. Estas características del protocolo están integradas en la encapsulación de la trama. Cuando la trama llega a su destino y el protocolo de capa de enlace de datos saca la trama del medio, la información de tramo es leída y descartada.

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. Como se muestra en la figura, según el entorno, la cantidad de información de control que se necesita en la trama varía para coincidir con los requisitos de control de acceso al medio de los medios y de la topología lógica.

Protocolos de la capa de enlace de datos: la trama

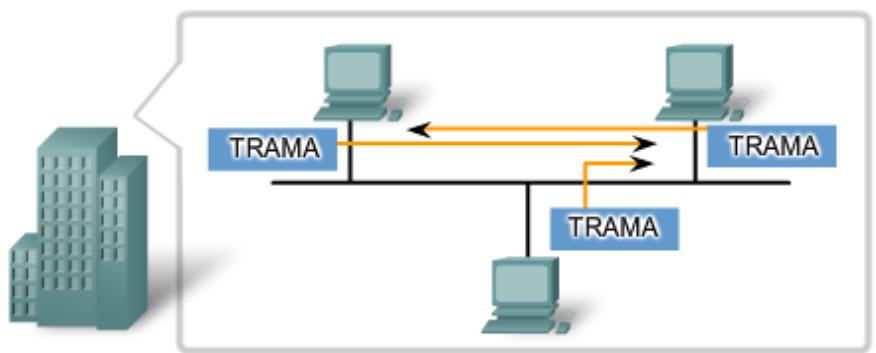
En un ambiente frágil, se necesita mayor control para asegurar la entrega. Los campos del encabezado y del tráiler son más grandes porque se necesita más información de control.

Es necesario un mayor esfuerzo para asegurar la entrega = mayor sobrecarga = velocidades de transmisión más lentas



En un ambiente protegido, podemos confiar en que la trama llegue a su destino. Se necesitan menores controles, lo que produce campos y tramas más pequeños.

Es necesario un menor esfuerzo para asegurar la entrega = menor sobrecarga = velocidades de transmisión más rápidas



7.3.2 Tramado: función del encabezado

Como se muestra en la figura, el encabezado de trama contiene la información de control especificada por el protocolo de capa de enlace de datos para la topología lógica específica y los medios utilizados.

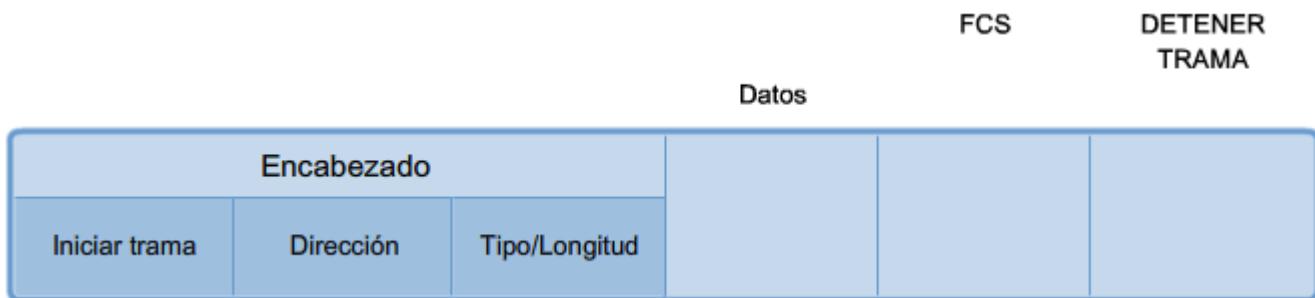
La información de control de trama es única para cada tipo de protocolo. Es utilizada por el protocolo de la Capa 2 para proporcionar las características demandadas por el entorno de comunicación.

Los campos típicos del encabezado de trama incluyen:

- Campo inicio de trama: indica el comienzo de la trama
- Campos de dirección de origen y destino: indica los nodos de origen y destino en los medios
- Prioridad/Calidad del Campo de servicio: indica un tipo particular de servicio de comunicación para el procesamiento
- Campo tipo: indica el servicio de la capa superior contenida en la trama
- Campo de control de conexión lógica: utilizada para establecer la conexión lógica entre nodos
- Campo de control de enlace físico: utilizado para establecer el enlace a los medios
- Campo de control de flujo: utilizado para iniciar y detener el tráfico a través de los medios
- Campo de control de congestión: indica la congestión en los medios

Los nombres de los campos mencionados son campos no específicos enumerados como ejemplos. Diferentes protocolos de capa de enlace de datos pueden utilizar diferentes campos de los mencionados. Debido a que los fines y funciones de

los protocolos de capa de enlace de datos están relacionados a las topologías específicas y a los medios, cada protocolo debe examinarse para tener una comprensión detallada de su estructura de trama. Como los protocolos se analizan en este curso, se explicará más información acerca de la estructura de la trama.



El campo **Iniciar trama** indica a los otros dispositivos de la red que está llegando una trama a través del medio.

El campo **Dirección** almacena las direcciones de enlace de datos de destino y de origen

El campo **Tipo/Longitud** es un campo opcional utilizado por algunos protocolos para establecer qué tipo de datos está ingresando o posiblemente la longitud de la trama.

7.3.3 Direccionamiento: hacia dónde se dirige la trama

La capa de enlace de datos proporciona direccionamiento que es utilizado para transportar la 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 está contenido 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 la Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo. Si el dispositivo es transportado a otra red o subred, aún funcionará con la misma dirección física de la Capa 2.

Debido a que la trama sólo se utiliza para transportar datos entre nodos a través del medio local, la dirección de la capa de enlace de datos sólo 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, donde las direcciones en el encabezado del paquete son transportadas desde el host de origen al host de destino sin importar la cantidad de saltos de la red a lo largo de la ruta.

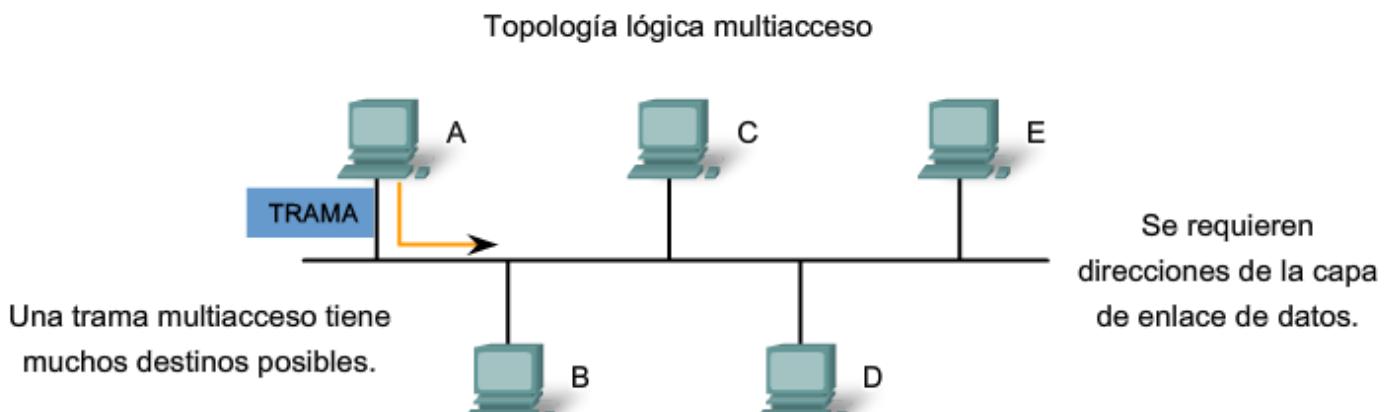
Si el paquete en la trama debe pasar a otro segmento de la red, el dispositivo intermediario, un router, desencapsulará la trama original, creará una nueva trama para el paquete y la enviará al nuevo segmento. La nueva trama usará el direccionamiento de origen y de destino según sea necesario para transportar el paquete a través del nuevo medio.

Requisitos de direccionamiento

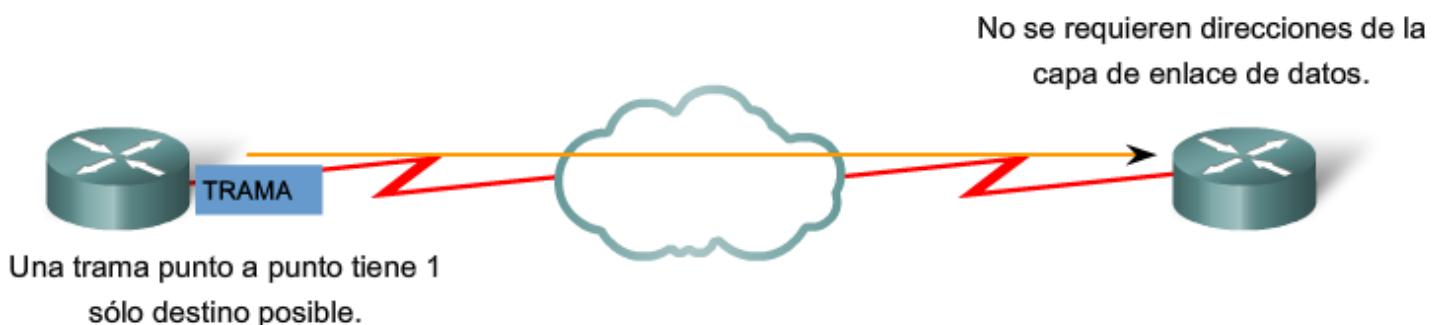
La necesidad de direccionamiento de la capa de enlace de datos en esta capa depende de la topología lógica.

Las topologías punto a punto, con sólo dos nodos interconectados, no requieren direccionamiento. Una vez en el medio, la trama sólo tiene un lugar al cual puede ir.

Debido a que las topologías de anillo y multiacceso pueden conectar muchos nodos en un medio común, se requiere direccionamiento para esas tipologías. Cuando una trama alcanza cada nodo en la topología, el nodo examina la dirección de destino en el encabezado para determinar si es el destino de la trama.



Topología lógica punto a punto



7.3.4 Tramado: función del Tráiler

Los protocolos de la capa de enlace de datos agregan un tráiler en el extremo de cada trama. El tráiler se utiliza para determinar si la trama llegó sin errores. Este proceso se denomina detección de errores. Observe que es diferente de la corrección de errores. La detección de errores se logra colocando un resumen lógico o matemático de los bits que comprenden la trama en el tráiler.

Secuencia de verificación de trama

El campo secuencia de verificación de trama (FCS) se utiliza para determinar si ocurrieron errores de transmisión y recepción de la trama. La detección de errores se agrega a la capa de enlace de datos porque es ahí donde se transfieren los datos a través de los medios. Los medios son un entorno potencialmente inseguro para los datos. Las señales en los medios pueden estar sujetas a interferencia, distorsión o pérdida que podría cambiar sustancialmente los valores de los bits que dichas señales representan. El mecanismo de detección de errores provisto por el uso del campo FCS descubre la mayoría de los errores causados en los medios.

Para asegurarse de que el contenido de la trama recibida en el destino combine con la trama que salió del nodo origen, un nodo de transmisión crea un resumen lógico del contenido de la trama. A esto se lo 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.

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.

Existe siempre la pequeña posibilidad de que una trama con un buen resultado de CRC esté realmente corrupta. 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.

El protocolo utilizado en la capa de enlace de datos determinará si se realiza la corrección del error. La FCS se utiliza para detectar el error, pero no todos los protocolos admiten la corrección del error.



Se utiliza el campo **Secuencia de verificación de trama** para controlar los errores. El origen calcula un número en función de los datos de la trama y coloca ese número en el campo FCS. El destino, entonces, recalculará los datos para determinar si FCS coincide. Si no coinciden, el destino elimina la trama.

El campo **Detener trama**, también llamado Tráiler de la trama, es un campo opcional que se utiliza cuando la longitud de la trama no se encuentra especificada en el campo Tipo/Longitud. Indica el final de una trama cuando ya se transmitió.

7.3.5 Protocolos de capa de enlace de datos: Trama

En una red TCP/IP, todos los protocolos de la Capa 2 OSI trabajan con el protocolo de Internet en la Capa 3. Sin embargo, el protocolo de la Capa 2 real utilizado depende de la topología lógica de la red y de 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.

Los protocolos que se cubrirán en los cursos CCNA incluyen:

- Ethernet
- Protocolo Punto a Punto (PPP)
- Control de enlace de datos de alto nivel (HDLC)
- Frame Relay
- Modo de transferencia asincrónico (ATM)

Cada protocolo realiza control de acceso a los medios para las topologías lógicas especificadas de Capa 2. Esto significa que una cantidad de diferentes dispositivos de red puede actuar como nodos que operan en la capa de enlace de datos al implementar estos protocolos. Estos dispositivos incluyen el adaptador de red o tarjetas de interfaz de red (NIC) en computadoras, así como las interfaces en routers y switches de la Capa 2.

El protocolo de la Capa 2 utilizado 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.

Tecnología LAN

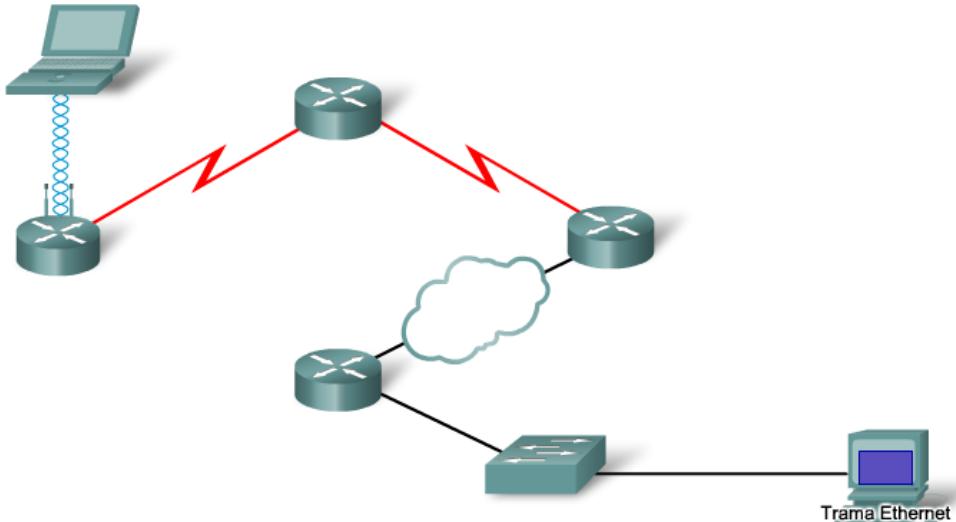
Una Red de área local generalmente utiliza una tecnología de ancho de banda alto que es capaz de sostener gran cantidad de hosts. El área geográfica relativamente pequeña de una LAN (un único edificio o un campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

Tecnología WAN

Sin embargo, utilizar una tecnología de ancho de banda alto no es generalmente rentable para redes de área extensa que cubren 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.

Ejemplos de protocolos de la Capa 2



Protocolo Ethernet para LAN

Ethernet es una familia de tecnologías de interconexión de redes que se define en los estándares 802.2 y 802.3. Los estándares de Ethernet definen los protocolos de la Capa 2 y las tecnologías de la Capa 1. Ethernet es la tecnología LAN más ampliamente utilizada y soporta anchos de banda de datos de 10, 100, 1000, o 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. El medio compartido requiere que el encabezado del paquete de Ethernet utilice la 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.

La trama de Ethernet tiene muchos campos, como se muestra en la figura. En la capa de enlace de datos, la estructura de trama es casi idéntica para todas las velocidades de Ethernet. Sin embargo, en la capa física, las diferentes versiones de Ethernet colocan los bits sobre el medio de forma diferente.

Ethernet II es el formato de trama de Ethernet utilizado en las redes TCP/IP.

Ethernet es una parte tan importante de la interconexión de redes de datos, que hemos dedicado un capítulo a ella. También la utilizamos en ejemplos a lo largo de esta serie de cursos.

Protocolo Ethernet

Un protocolo de capa de enlace de datos común para las WAN

| Trama | | | | | | |
|------------------|-----------|---------|---------|---------|------------------|------------------------------------|
| Nombre del campo | Preámbulo | Destino | Origen | Tipo | Datos | Secuencia de verificación de trama |
| Tamaño | 8 bytes | 6 bytes | 6 bytes | 2 bytes | 46 - 1.500 bytes | 4 bytes |

Preámbulo: se utiliza para la sincronización; también contiene un delimitador para marcar el final de la información de tiempo.

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 que indica qué protocolo de la capa superior recibirá los datos después de que el proceso Ethernet se haya completado.

Datos o contenido: es la PDU, por lo general un paquete IPv4, que se transporta a través de los medios..

Secuencia de verificación de trama (FCS): valor que se utiliza para controlar las tramas dañadas.

Protocolo punto a punto para WAN

El protocolo punto a punto (PPP) es un protocolo utilizado para entregar tramas entre dos nodos. A diferencia de muchos protocolos de capa de enlace de datos, definidos por las organizaciones de ingeniería eléctrica, el estándar PPP está definida por RFC. PPP fue desarrollado como un protocolo WAN y sigue siendo el protocolo elegido para implementar muchas WAN serie. PPP se puede utilizar en diversos medios físicos, lo que incluye cable de par trenzado, líneas de fibra óptica o transmisión satelital.

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 figura para ver los campos básicos de una trama PPP.

Point-to-Point Protocol

Un protocolo de capa de enlace de datos común para las WAN

| Trama | | | | | | |
|------------------|-------------|---------|---------|-----------|----------|-------------|
| Nombre del campo | Señalizador | Destino | Control | Protocolo | Datos | FCS |
| Tamaño en bytes | 1 byte | 1 byte | 1 byte | 2 bytes | variable | 2 o 4 bytes |

Señalización: un único byte que indica el comienzo y la finalización de una trama. El campo Señalización está formado por la secuencia binaria 01111110.

Dirección: un único byte que contiene la dirección de broadcast PPP estándar. PPP no asigna direcciones a estaciones individuales.

Control: un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos del 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 con números asignados (RFC) 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 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.

Protocolo inalámbrico para LAN

802.11 es una extensión de los estándares IEEE 802. Utiliza el mismo 802.2 LLC y esquema de direccionamiento de 48 bits como otras LAN 802. Sin embargo, hay 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.

El estándar IEEE 802.11, comúnmente llamada Wi-Fi, es un sistema por contención que utiliza un proceso de acceso al medio de Acceso múltiple con detección de portadora y prevención de colisiones (CSMA/CA). CSMA/CA especifica un procedimiento Postergación aleatorio 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 usan Acuse de recibo de enlace de datos para confirmar que una trama se recibió con éxito. 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).

Una trama 802.11 se muestra en la figura. Contiene estos campos:

Campo de versión del protocolo: la versión de la trama 802.11 en uso

Campos tipo y subtipo: identifica una de las tres funciones y subfunciones de la trama: control, datos y administración

Campo A DS: establecido en 1 en las tramas de datos destinadas al sistema de distribución (dispositivos en la estructura inalámbrica)

Campo Desde DS: establecido en 1 en tramas de datos que salen del sistema de distribución

Campo Más fragmentos: establecido en 1 para tramas que tienen otro fragmento

Campo Reintentar: establecido en 1 si la trama es una retransmisión de una trama anterior

Campo Administración de energía: establecido en 1 para indicar que un nodo estará en el modo ahorro de energía

Campo Más datos: establecido en 1 para indicar a un nodo en el modo ahorro de energía que más tramas se guardan en la memoria del búfer de ese nodo

Campo Privacidad equivalente por cable (WEP): establecido en 1 si la trama contiene información encriptada WEP por seguridad

Campo Orden: establecido en 1 en una trama de tipo datos que utiliza la clase de servicio Estrictamente ordenada (no requiere reordenamiento)

Campo Duración/ID: según el tipo de trama, representa el tiempo, en microsegundos, requerido para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió la trama

Campo Dirección de destino (DA): la dirección MAC del nodo de destino final en la red

Campo Dirección de origen (SA): la dirección MAC del nodo que inició la trama

Campo Dirección del receptor (RA): la dirección MAC que identifica al dispositivo inalámbrico que es el receptor inmediato de la trama

Campo Dirección del transmisor (TA): la dirección MAC que identifica al dispositivo inalámbrico que transmitió la trama

Campo Número de secuencia: indica el número de secuencia asignado a la trama; las tramas retransmitidas se identifican por números de secuencia duplicados

Campo Número de fragmento: indica el número de cada fragmento de la trama

Campo Cuerpo de la trama: contiene la información que se está transportando; para tramas de datos, generalmente un paquete IP

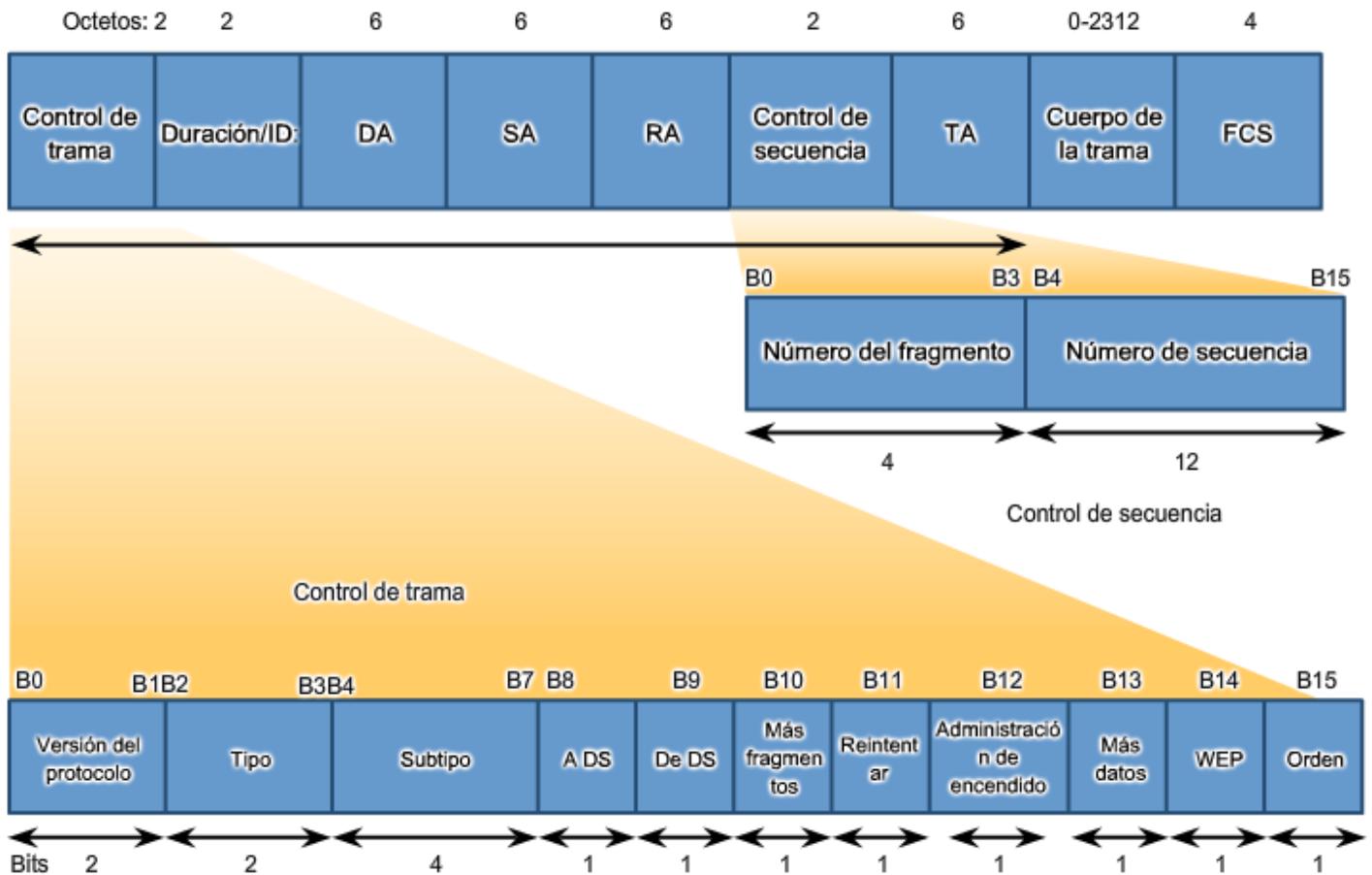
Campo FCS: contiene una verificación por redundancia cíclica (CRC) de 32 bits de la trama

Protocolo PPP:

<http://www.ietf.org/rfc/rfc1661.txt?number=1661>

Extensiones PPP del fabricante: <http://www.ietf.org/rfc/rfc2153.txt?number=2153>

Protocolo LAN inalámbrico de 802.11



7.4 INTEGRACION

7.4.1 Seguimiento de datos a través de internetwork

La figura en la siguiente página presenta una transferencia de datos simple entre dos hosts a través de una internetwork. Destacamos la función de cada capa durante la comunicación. Para este ejemplo mostraremos una solicitud HTTP entre un cliente y un servidor.

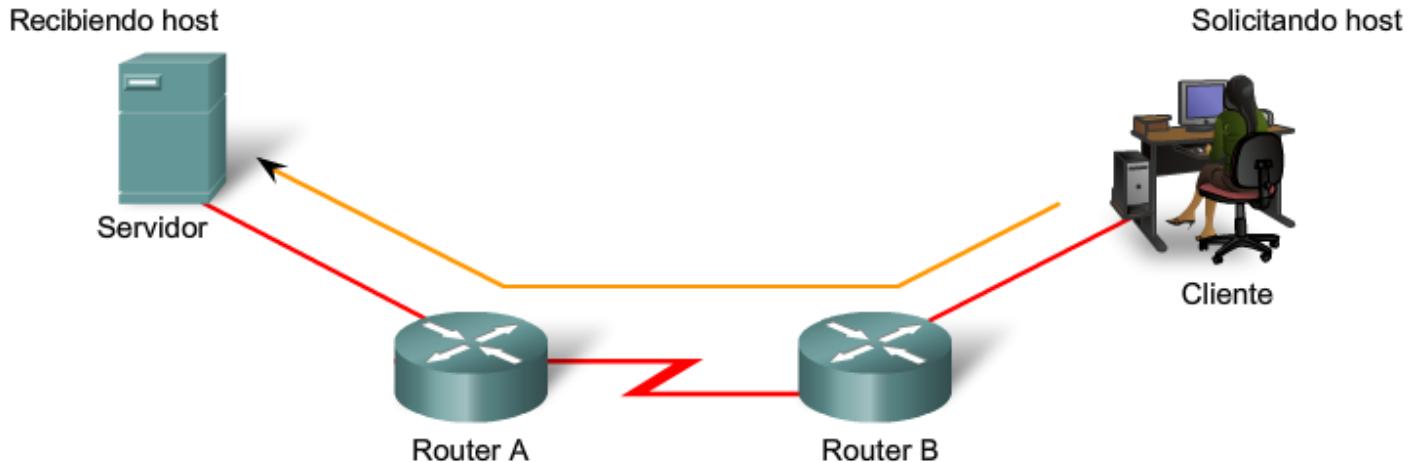
Para centrarnos en el proceso de transferencia de datos, omitimos muchos elementos que pueden producirse en una transacción real. En cada paso sólo estamos llamando la atención a los elementos principales. Por ejemplo: muchas partes de los encabezados se ignoran.

Estamos asumiendo que todas las tablas de enrutamiento son convergentes y las tablas ARP están completas. Además, suponemos que ya está establecida una sesión TCP entre el cliente y el servidor. También supondremos que la búsqueda de DNS para el servidor WWW ya está en la caché del cliente.

En la conexión WAN entre los dos routers, suponemos que PPP ya ha establecido un circuito físico y ha establecido una sesión PPP.

En la página siguiente se puede seguir paso a paso esta comunicación. Le alentamos a leer cada explicación atentamente y a estudiar la operación de las capas de cada dispositivo.

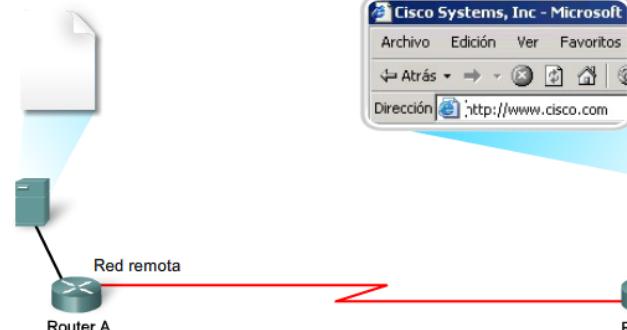
Una transferencia de datos simple entre dos hosts a través de una internetwork.



Un usuario en una red LAN quiere acceder a una página Web almacenada en un servidor que se encuentra ubicado en una red remota. El usuario comienza activando un enlace en una página Web.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

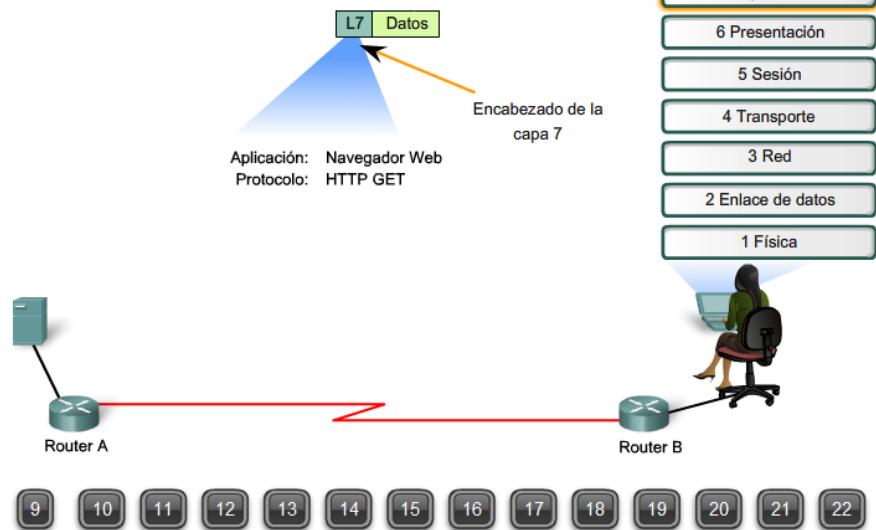
Un cliente solicita datos de un servidor



El explorador inicia una solicitud HTTP Get (Obtener HTTP). La capa de aplicación agrega el encabezado de la capa 7 para identificar la aplicación y el tipo de datos.

1 2 3 4 5 6 7

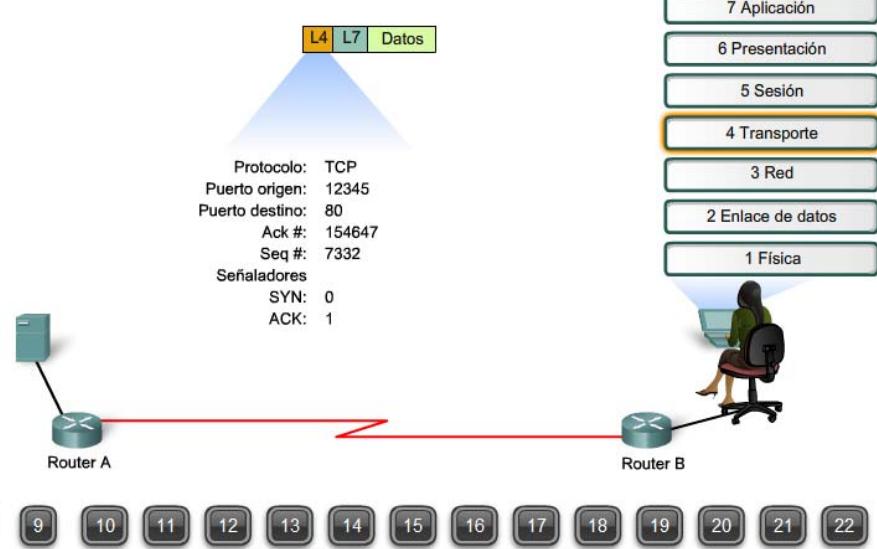
La capa de aplicación de origen inicia la transferencia de datos



La capa de transporte identifica el servicio de la capa superior como un cliente World Wide Web (WWW). La capa de transporte luego asocia este servicio con el protocolo TCP y asigna los números de puerto. Utiliza un puerto de origen seleccionado aleatoriamente que se encuentre asociado con esta sesión establecida (12345). El puerto de destino (80) se encuentra asociado con el servicio WWW.

1 2 3 4 5 6 7

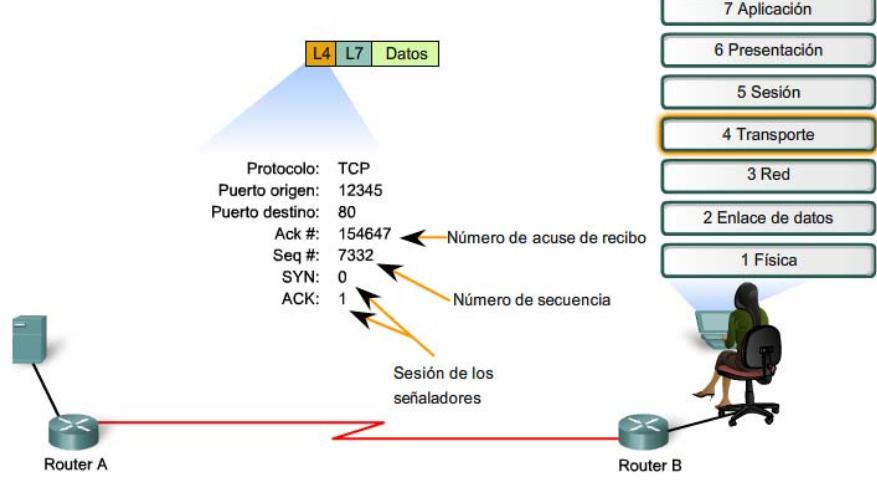
La capa de transporte de origen dirige la sesión



TCP también envía un número de reconocimiento que le indica al servidor WWW el número de secuencia del próximo segmento TCP que espera recibir. El número de secuencia indicará dónde se encuentra este segmento en las series de los segmentos relacionados. Las señalizaciones también se configuran como adecuadas para establecer una sesión.

1 2 3 4 5 6 7

La capa de transporte de origen dirige la sesión

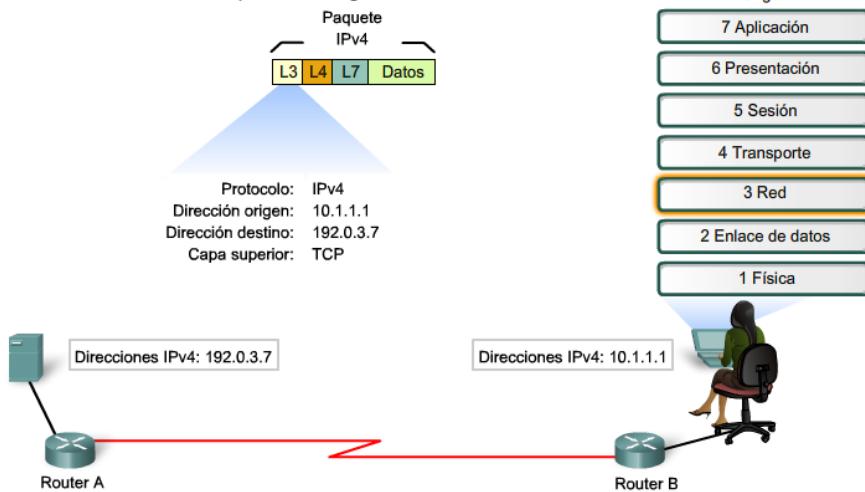


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

En la capa de red, se construye un paquete IP para identificar los hosts de origen y de destino. Para la dirección de destino, el host del cliente utiliza la dirección IP asociada con el nombre host del servidor WWW que estará en caché en la tabla del host. Utiliza su propia dirección IPv4 como dirección de origen. La capa de red también identifica el protocolo de la capa superior encapsulado en este paquete como un segmento TCP.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

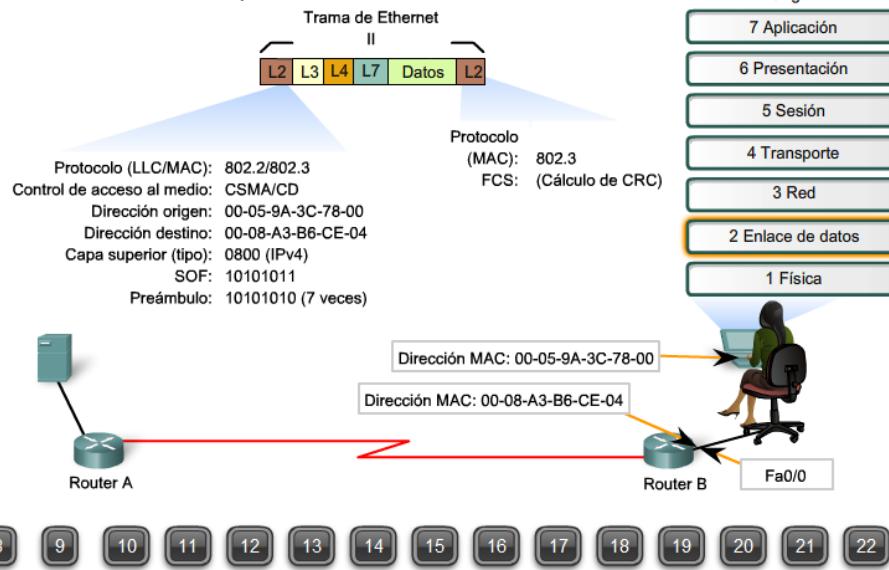
La capa de red dirige los datos al host de destino



La capa de enlace de datos hace referencia al caché del Address Resolution Protocol (Protocolo de resolución de direcciones, ARP) para determinar la dirección MAC que se encuentra asociada con la interfaz del RouterB, que se encuentra especificada como gateway por defecto. Luego, utiliza esta dirección para construir una trama de Ethernet II para transportar el paquete IPv4 a través de los medios locales. La dirección MAC de la computadora portátil se utiliza como la dirección MAC de origen, y la dirección MAC de la interfaz Fa0/0 del RouterB se utiliza como la dirección MAC de destino en la trama.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

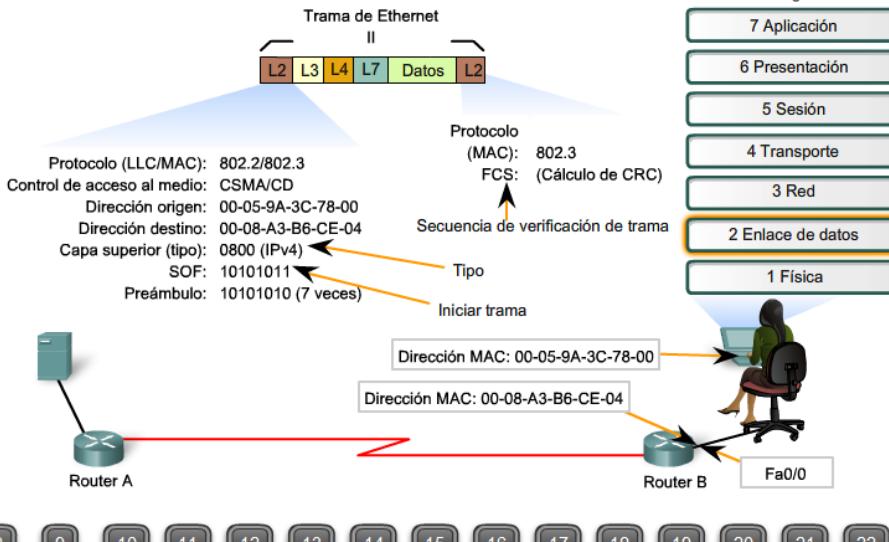
La capa de enlace de datos coloca datos en los medios



La trama también indica el protocolo de la capa superior de IPv4 con un valor de 0800 en el campo Tipo. La trama comienza con un indicador SOF, Preámbulo e inicio de trama (SOF) y termina con una comprobación cíclica de redundancia (CRC) en la Secuencia de verificación de trama al final de la trama para la detección de errores. Luego, utiliza CSMA/CD para verificar la colocación de la trama en los medios.

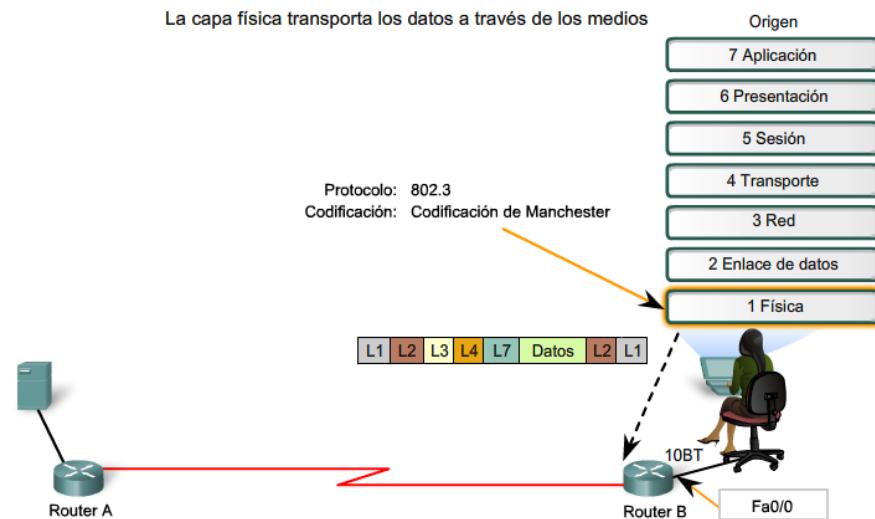
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

La capa de enlace de datos coloca datos en los medios



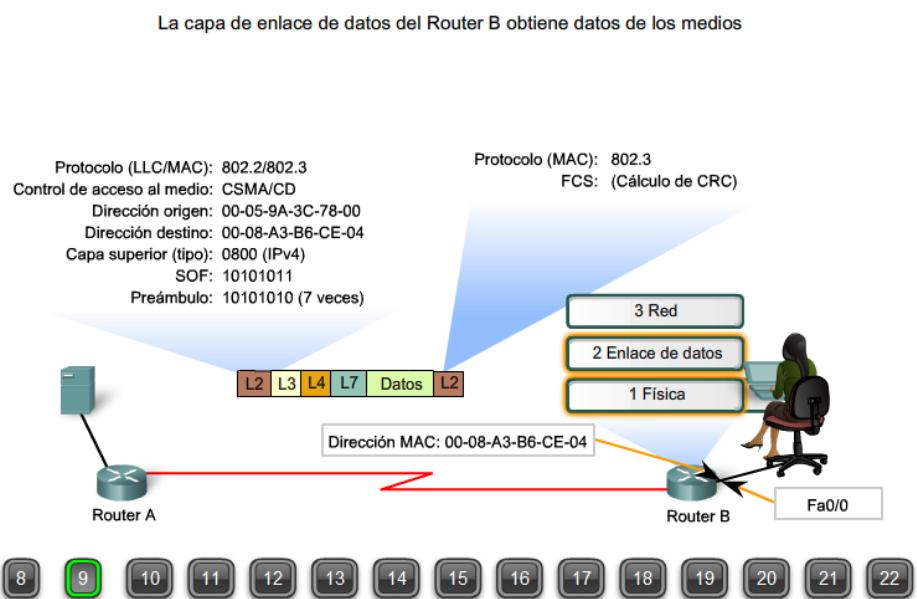
La capa física comienza a codificar la trama en los medios, bit por bit. El segmento entre el RouterA y el servidor es un segmento 10Base-T, por lo tanto, los bits se codifican mediante la codificación diferencial Manchester. El RouterB almacena los bits a medida que los recibe.

1 2 3 4 5 6 7



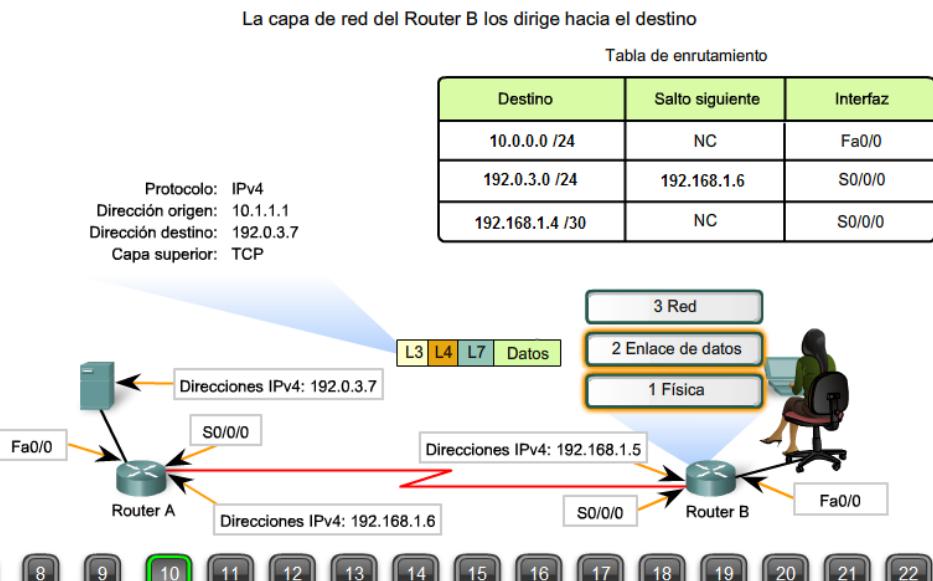
El RouterB examina los bits en el preámbulo y en SOF, y busca dos bits 1 consecutivos que indiquen el comienzo de una trama. El RouterB luego, comienza a almacenar los bits como parte de la trama reconstruida. Cuando se recibe toda la trama, el RouterB genera una CRC de ella. Luego, lo compara con la FCS al final de la trama para determinar que se haya recibido intacta. Cuando la trama se confirma como buena, la dirección MAC de destino en la trama se compara con la dirección MAC de la interfaz (Fa0/0). Como concuerda, los encabezados se retiran y el paquete se empuja hacia la capa de red.

1 2 3 4 5 6 7



En la capa de red, la dirección IPv4 de destino del paquete se compara con las rutas en la tabla de enrutamiento. Se encuentra una coincidencia que se asocia con una próxima interfaz S0/0/0 de salto. Luego, el paquete dentro del RouterB se pasa al circuito para la interfaz S0/0/0.

1 2 3 4 5 6 7

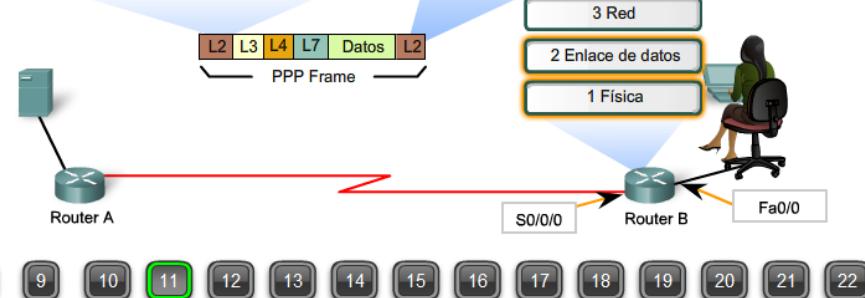


El RouterB crea una trama PPP para transportar el paquete a través de WAN. En el encabezado PPP, se agrega una señalización binaria 01111110 para indicar el comienzo de una trama. Luego, se agrega un campo de dirección de 11111111, que es equivalente a un broadcast (lo que quiere decir "enviar a todas las estaciones"). Debido a que PPP es punto a punto y se utiliza como enlace directo entre dos nodos, este campo no tiene un significado real.

1 2 3 4 5 6 7

La capa de enlace de datos coloca datos en los medios

Protocolo: PPP
Control de acceso al medio: NA
Señalizador: 01111110
Dirección (todos los nodos): 11111111
Capa superior (Protocolo): 0021 (hex) (IPv4)



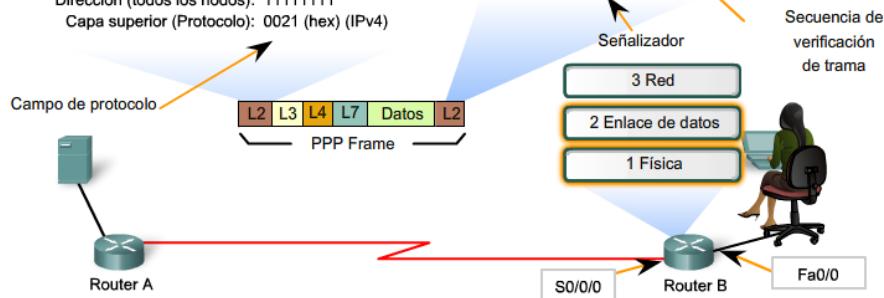
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

También está incluido un campo de protocolo con un valor de 0021 (hex.) para indicar que un paquete IPv4 se encuentra encapsulado. El tráiler de la trama termina con una verificación cíclica de redundancia en la Secuencia de verificación de trama para la detección de errores. Un valor de señalización de 01111110 binarios indica el fin de una trama PPP.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

La capa de enlace de datos coloca datos en los medios

Protocolo: PPP
Control de acceso al medio: NA
Señalizador: 01111110
Dirección (todos los nodos): 11111111
Capa superior (Protocolo): 0021 (hex) (IPv4)



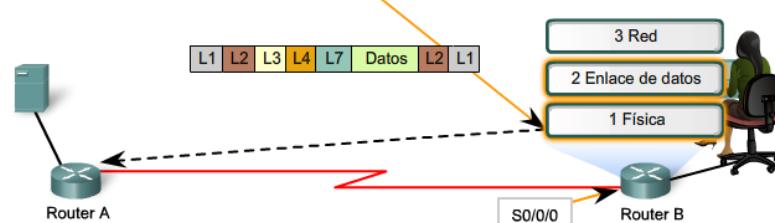
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

Con el circuito y con la sesión PPP ya establecida entre los routers, la capa física comienza a codificar la trama en los medios WAN, bit por bit. El router que recibe (RouterA) almacena los bits a medida que los recibe. El tipo de representación de bit y codificación depende del tipo de tecnología WAN que se utiliza.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

La capa física transporta los datos a través de los medios

Protocolo: ????
Codificación: ?????



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

El RouterA examina los bits en la señalización para identificar el comienzo de la trama. El RouterA luego, comienza a almacenar los bits como parte de la trama reconstruida. Cuando se recibe toda la trama, como se indica en la señalización en el tráiler, el RouterA genera un CRC de ella. Luego, lo compara con la FCS al final de la trama para determinar que se haya recibido intacta. Cuando la trama se confirma como buena, los encabezados se retiran y el paquete se empuja hacia la capa de red del RouterA.

1 2 3 4 5 6 7

En la capa de red, la dirección IPv4 de destino del paquete se compara con las rutas en la tabla de enrutamiento. Se encuentra una coincidencia que está directamente conectada a la interfaz Fa0/0. Luego el paquete dentro del RouterA se pasa al circuito de la interfaz Fa0/0.

1 2 3 4 5 6 7

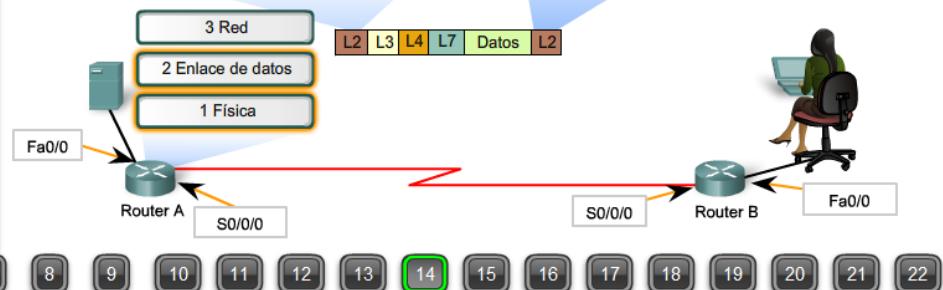
La capa de enlace de datos hace referencia al caché ARP del RouterA para determinar la dirección MAC que se encuentra asociada a la interfaz del servidor Web. Luego, utiliza esta dirección MAC para construir una trama de Ethernet II para transportar el paquete IPv4 a través de los medios locales al servidor. La dirección MAC de la interfaz fa0/0 del RouterA se utiliza como la dirección MAC de origen, y la dirección MAC del servidor se utiliza como la dirección MAC de destino en la trama. La trama también indica el protocolo de la capa superior de IPv4 con un valor de 0800 en el campo Tipo. La trama comienza con un indicador SOF, Preámbulo e inicio de trama (SOF) y

1 2 3 4 5 6 7

La capa de enlace de datos del RouterB obtiene datos de los medios

Protocolo: PPP
Control de acceso al medio: NA
Señalizador: 01111110
Dirección (todos los nodos): 11111111
Capa superior (Protocolo): 0021 (hex) (IPv4)

Protocolo: PPP
FCS: (Cálculo de CRC)
Señalizador: 01111110

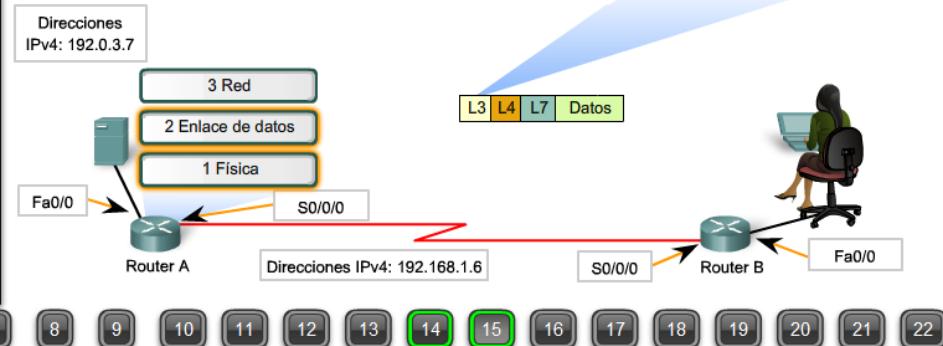


La capa de red del RouterB los dirige hacia el destino

Tabla de enrutamiento

| Destino | Salto siguiente | Interfaz |
|-----------------|-----------------|----------|
| 10.0.0.0 /24 | 192.168.1.5 | S0/0/0 |
| 192.0.3.0 /24 | NC | Fa0/0 |
| 192.168.1.4 /30 | NC | S0/0/0 |

Protocolo: IPv4
Dirección origen: 10.1.1.1
Dirección destino: 192.0.3.7
Capa superior: TCP



La capa de enlace de datos coloca datos en los medios

Protocolo (LLC/MAC): 802.2/802.3
Control de acceso al medio: CSMA/CD
Dirección origen: 00-08-A3-79-FF-23
Dirección destino: 00-1D-17-67-45-FC
Capa superior (tipo): 0800 (IPv4)
SOF: 10101011
Preámbulo: 10101010 (7 veces)

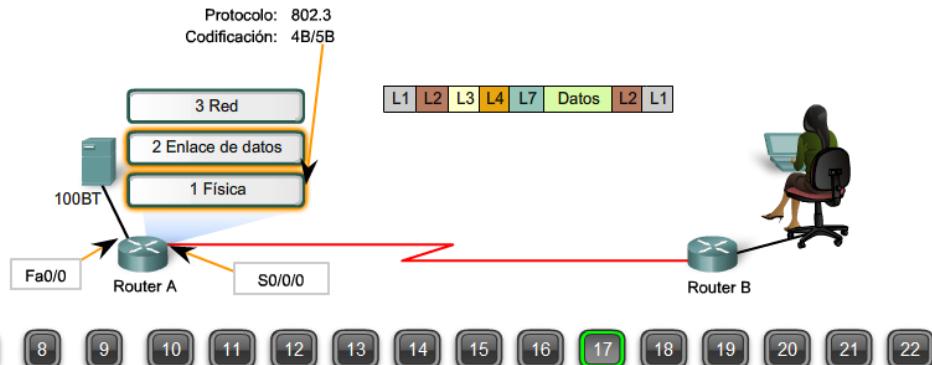
Protocolo (MAC): 802.3
FCS: (Cálculo de CRC)



La capa física comienza a codificar la trama en los medios, bit por bit. El segmento entre el RouterA y el servidor es un segmento 100Base-T, por lo tanto, los bits se codifican mediante la codificación 4B/5B. El servidor almacena los bits a medida que los recibe.

1 2 3 4 5 6 7

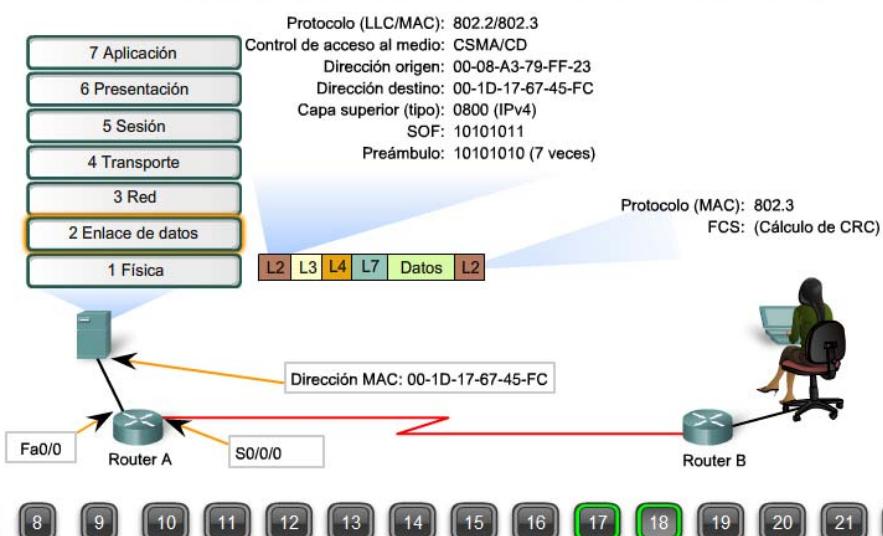
La capa física transporta los datos a través de los medios



El servidor web examina los bits en el preámbulo y en SOF, y busca dos bits 1 consecutivos que indiquen el comienzo de una trama. El servidor luego comienza a almacenar los bits como parte de la trama reconstruida. Cuando ya recibió toda la trama, el servidor genera una CRC de la trama. Luego, lo compara con la FCS al final de la trama para determinar que se haya recibido intacta.

1 2 3 4 5 6 7

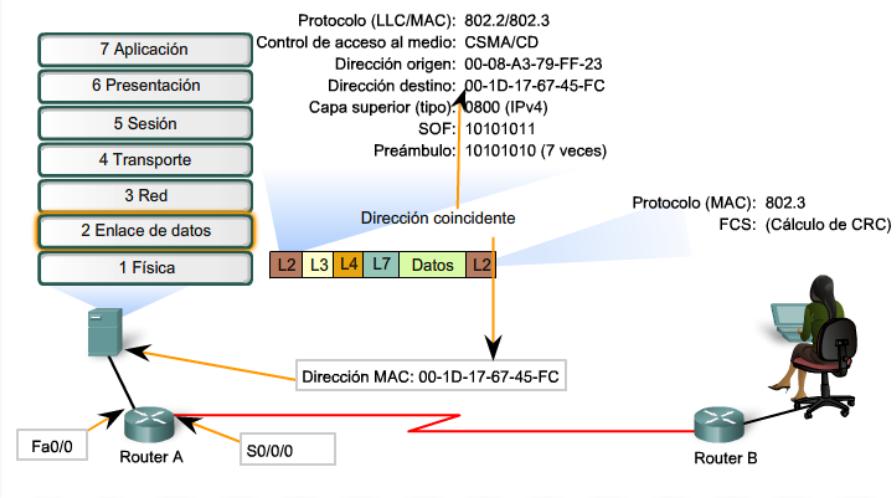
La capa de destino de enlace de datos del servidor obtiene datos de los medios



Cuando se confirma que la trama es buena, la dirección MAC de destino en la trama se compara con la dirección MAC del NIC en el servidor. Como concuerda, los encabezados se retiran y el paquete se empuja hacia la capa de red.

1 2 3 4 5 6 7

La capa de destino de enlace de datos del servidor obtiene datos de los medios



En la capa de red, la dirección IPv4 de destino del paquete se examina para identificar el host de destino. Como esta dirección coincide con su propia dirección IPv4, el servidor procesa el paquete. La capa de red identifica el protocolo de la capa superior como TCP y dirige el segmento contenido al servidor TCP en la capa de transporte.

1 2 3 4 5 6 7

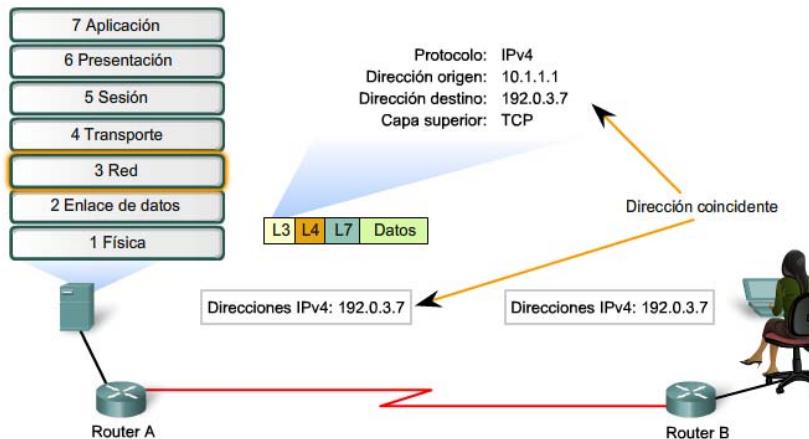
En la capa de transporte del servidor, el segmento TCP se examina para determinar la sesión a la cual pertenecen los datos contenidos en el segmento. Esto se realiza examinando los puertos de origen y de destino. El puerto único de origen y destino identifica una sesión existente en el servicio del servidor Web. Se utiliza el número de secuencia para colocar este segmento en el orden correcto para que pueda ser enviado hacia arriba a la capa de aplicación.

1 2 3 4 5 6 7

En la capa de aplicación, la solicitud HTTP Get (Obtener HTTP) se entrega al servicio del servidor web (httpd). El servicio luego puede formular una respuesta.

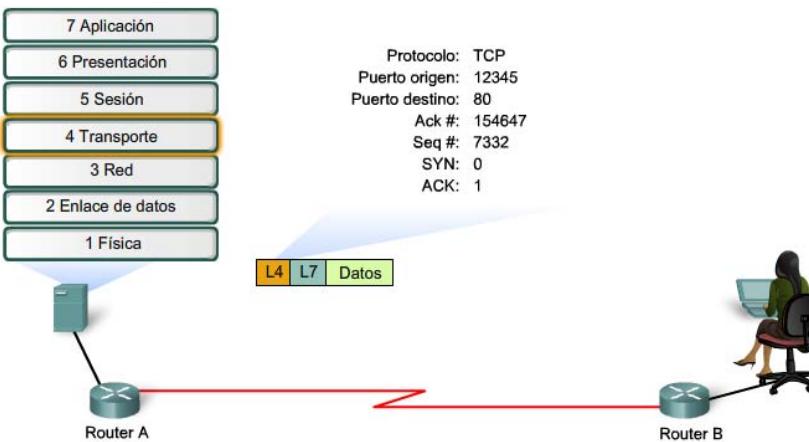
1 2 3 4 5 6 7

La capa de red de destino del servidor distingue que el paquete es para el host



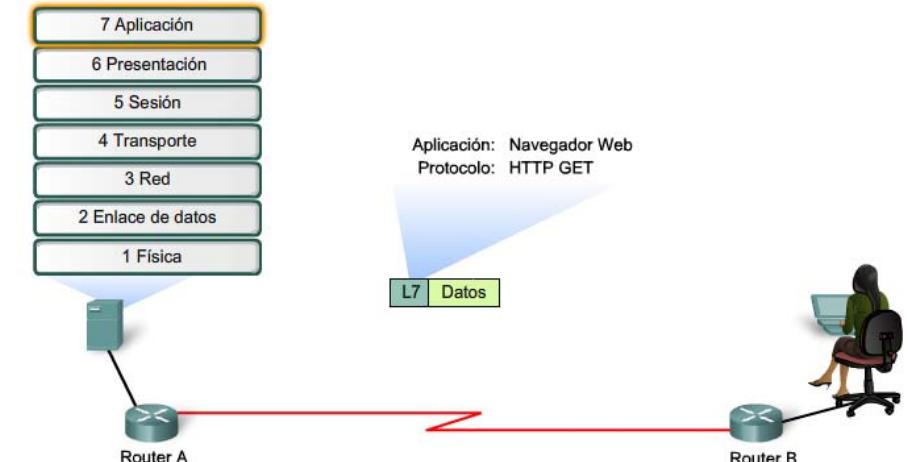
1 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

La capa de transporte de destino del servidor identifica la sesión



1 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

El servidor de la capa de aplicación de destino entrega los datos



1 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

7.6 RESUMEN DEL CAPITULO

7.6.1 Resumen y revisión

La capa de enlace de datos OSI prepara los paquetes de capa de red para ser colocados en el medio físico que transporta los datos.

El amplio intervalo de medios de comunicación requiere, de forma correspondiente, un amplio intervalo de protocolos de enlace de datos para controlar el acceso a los datos de estos medios.

El acceso a los medios puede ser ordenado y controlado o puede ser por contención. La topología lógica y el medio físico ayudan a determinar el método de acceso al medio.

La capa de enlace de datos prepara los datos para ser colocados en el medio encapsulando el paquete de la Capa 3 en una trama.

Una trama tiene un encabezado y una información final que incluye las direcciones del enlace de datos de origen y de destino, calidad de servicio, tipo de protocolo y valores de secuencia de verificación de tramas.

En este capítulo, aprendió que:

- Explicar la función de los protocolos de la capa de Enlace de datos en la transmisión de datos.
- Describir la forma en que la capa de Enlace de datos prepara los datos para ser transmitidos en los medios de red.
- Describir los distintos tipos de métodos de control de acceso a los medios.
- Identificar varias topologías de red lógicas comunes y describir la forma en que la topología lógica determina el método de control de acceso a medios para esa red.
- Explicar el objetivo de encapsular los paquetes en tramas para facilitar el acceso a los medios.
- Describir la estructura de trama de la Capa 2 e identificar campos genéricos.
- Explicar la función del encabezado de trama principal y campos de tráiler, calidad de servicio, tipo de protocolo y Secuencia de verificación de trama.

8 – CAPA FISICA DEL MODELO OSI

8.0 INTRODUCCION DEL CAPITULO

8.0.1 Introducción del capítulo

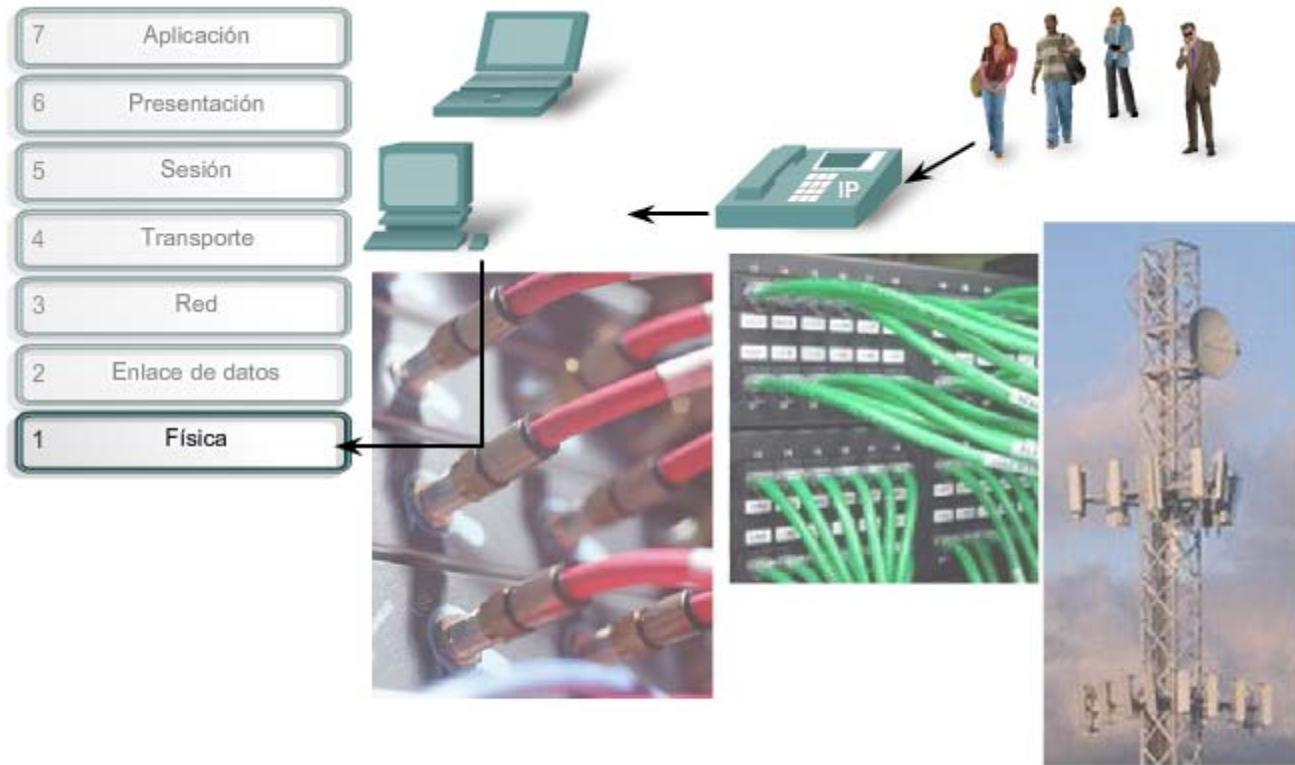
Los protocolos de la capa superior de OSI preparan los datos desde la red humana para realizar la transmisión hacia su destino. La capa física controla de qué manera se ubican los datos en los medios de comunicación.

La función de la capa física de OSI es la de codificar en señales los dígitos binarios que representan las tramas de la capa de Enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos (alambres de cobre, fibra óptica o medio inalámbrico) que conectan los dispositivos de la red.

Este capítulo presenta las funciones generales de la capa física al igual que los estándares y protocolos que administran la transmisión de datos a través de medios locales.

En este capítulo, usted aprenderá a:

- Explicar la función de los servicios y protocolos de capa física en la admisión de comunicaciones a través de las redes de datos.
- Describir el propósito de la codificación y señalización de la capa física, según estos métodos se utilizan en las redes.
- Describir la función de las señales que se utilizan para representar bits mientras se transporta una trama a través de los medios locales.
- Identificar las características básicas de los medios de cobre, de fibra y de red inalámbrica.
- Describir los usos comunes de los medios de cobre, de fibra y de red inalámbrica.



La capa Física interconecta nuestras redes de datos.

8.1 CAPA FISICA DEL MODELO OSI

8.1.1 Capa física: objetivo

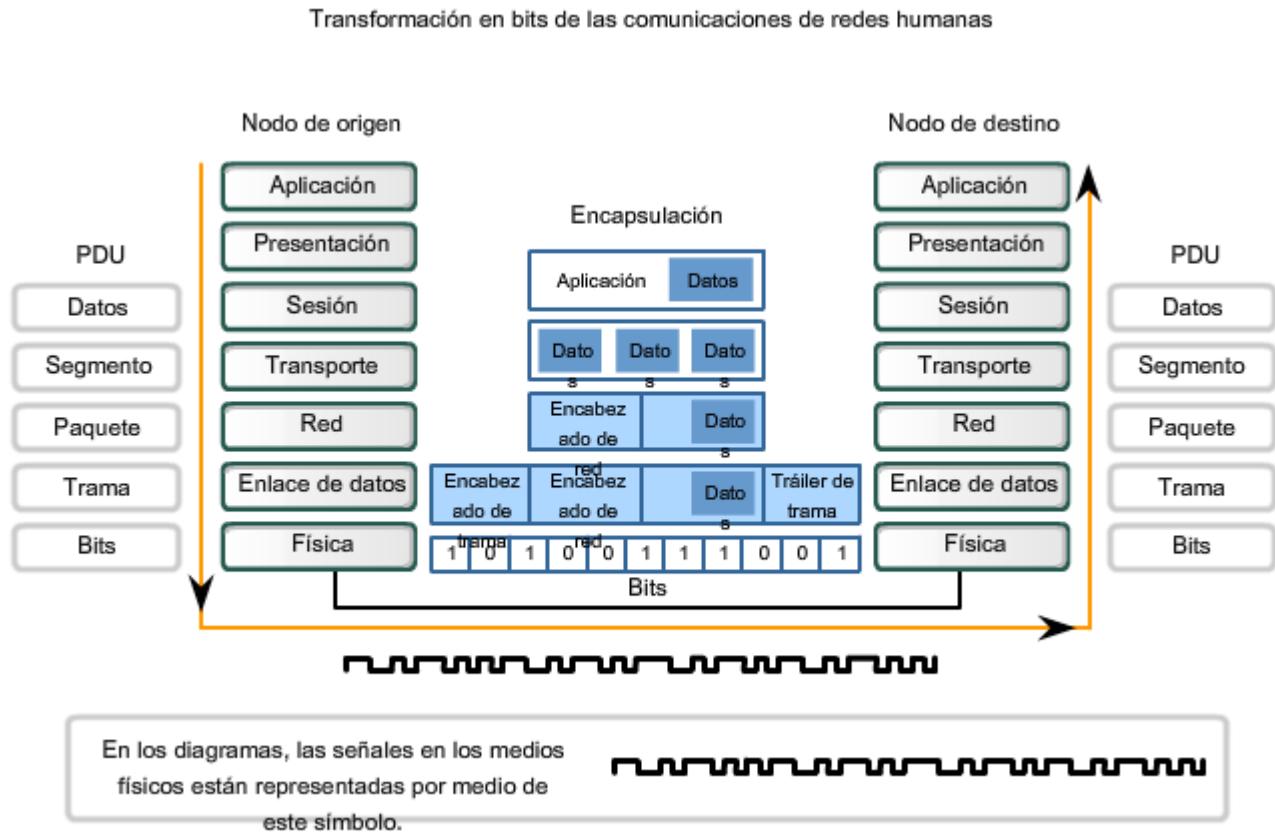
La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio recibe los bits codificados que componen una trama.

El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.
- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

En este momento del proceso de comunicación, la capa de transporte ha segmentado los datos del usuario, la capa de red los ha colocado en paquetes y luego la capa de enlace de datos los ha encapsulado como tramas. **El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama.** Luego, estas señales se envían por los medios una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa.



8.1.2 Capa física: Funcionamiento

Los medios no transportan la trama como una única entidad. Los medios transportan señales, una por vez, para representar los bits que conforman la trama.

Existen tres tipos básicos de medios de red en los cuales se representan los datos:

- Cable de cobre
- Fibra
- Inalámbrico

La presentación de los bits –es decir, el tipo de señal- depende del tipo de medio. Para los medios de cable de cobre, las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz. Para los medios inalámbricos, las señales son patrones de transmisiones de radio.

Identificación de una trama

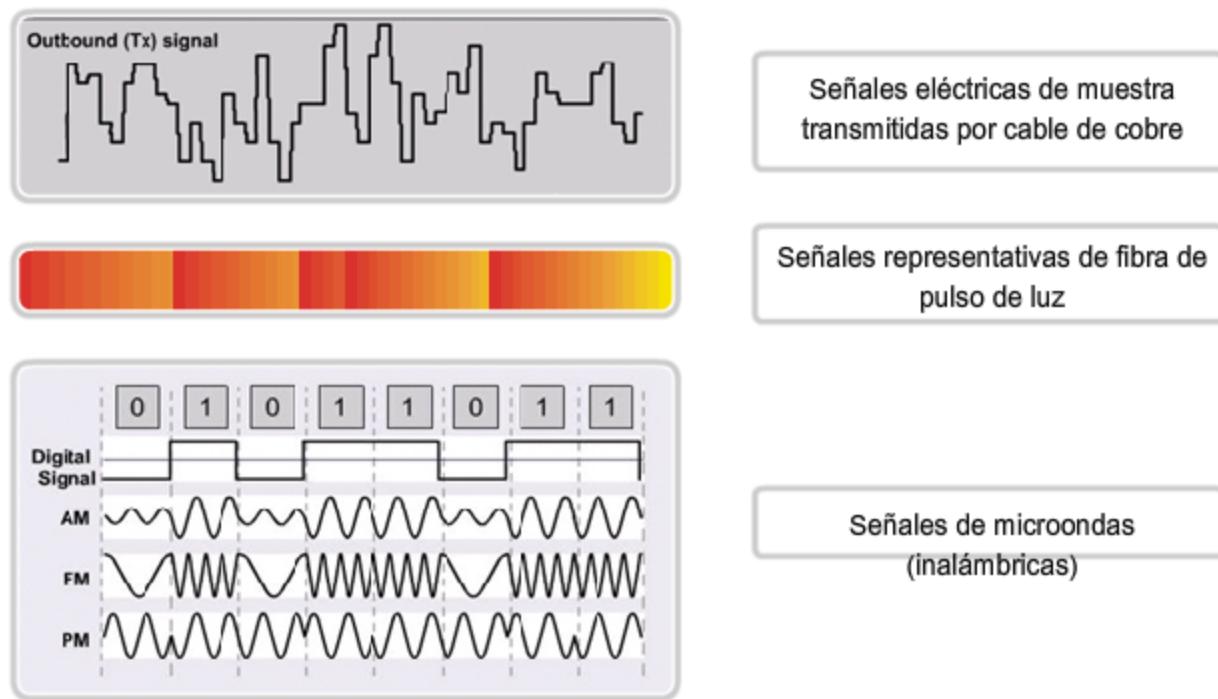
Cuando la capa física codifica los bits en señales para un medio específico, también debe distinguir dónde termina una trama y dónde se inicia la próxima. De lo contrario, los dispositivos de los medios no reconocerían cuándo se ha recibido

exitosamente una trama. En tal caso, el dispositivo de destino sólo recibiría una secuencia de señales y no sería capaz de reconstruir la trama correctamente. Como se describió en el capítulo anterior, indicar el comienzo de la trama es a menudo una función de la capa de Enlace de datos. Sin embargo, en muchas tecnologías, la capa física puede agregar sus propias señales para indicar el comienzo y el final de la trama.

Para habilitar un dispositivo receptor a fin de reconocer de manera clara el límite de una trama, el dispositivo transmisor agrega señales para designar el comienzo y el final de una trama. Estas señales representan patrones específicos de bits que sólo se utilizan para indicar el comienzo y el final de una trama.

En las siguientes secciones de este capítulo, se analizarán detalladamente el proceso de codificación de una trama de datos de bits lógicos a señales físicas en los medios y las características de los medios físicos específicos.

Representaciones de señales en los medios físicos



8.1.3 Capa física: Estándares

La capa física consiste en un hardware creado por ingenieros en forma de conectores, medios y circuitos electrónicos. Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

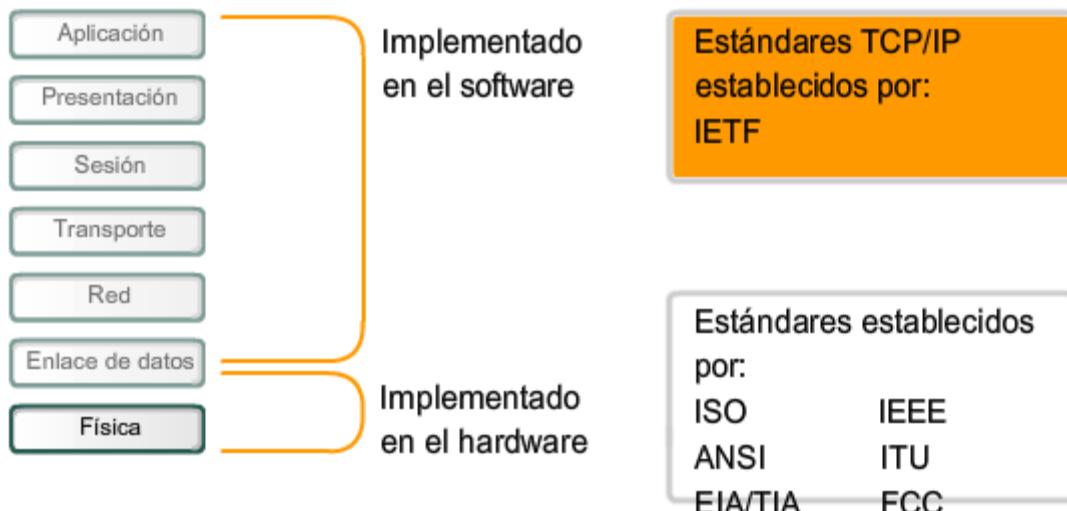
Por el contrario, las operaciones y los protocolos de las capas superiores de OSI se llevan a cabo mediante un software y están diseñados por especialistas informáticos e ingenieros de software. Como vimos en el capítulo anterior, el grupo de trabajo de ingeniería de Internet (IETF) define los servicios y protocolos del conjunto TCP/IP en las RFC.

Al igual que otras tecnologías asociadas con la capa de Enlace de datos, las tecnologías de la capa física se definen por diferentes organizaciones, tales como:

- La Organización Internacional para la Estandarización (ISO)
- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- El Instituto Nacional Estadounidense de Estándares (ANSI)

- La Unión Internacional de Telecomunicaciones (ITU)
- La Asociación de Industrias Electrónicas/Asociación de la Industria de las Telecomunicaciones (EIA/TIA)
- Autoridades de las telecomunicaciones nacionales, como la Comisión Federal de Comunicaciones (FCC) en EE.UU.

Comparación entre los estándares de capa física y los estándares de capa superior



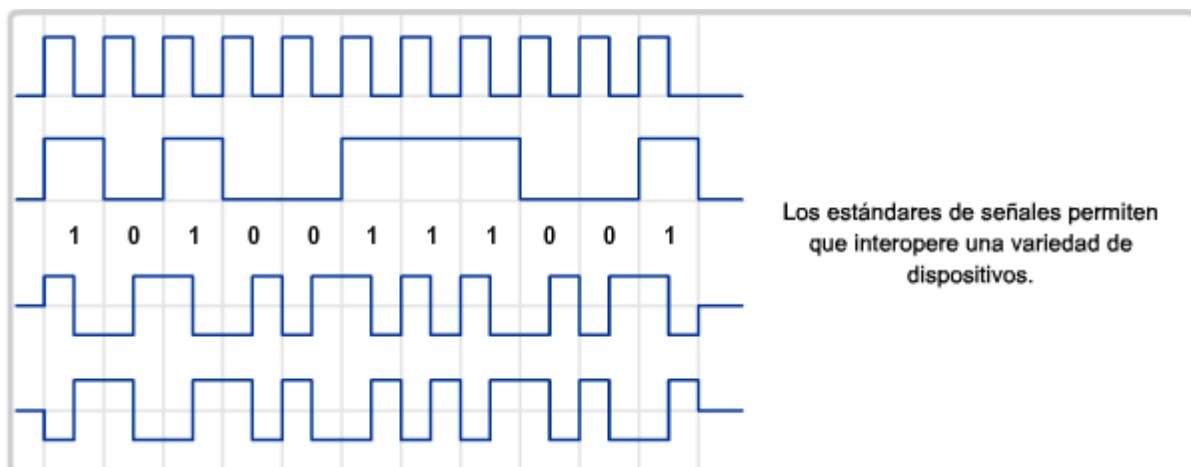
Hardware y tecnologías de la Capa física

Las tecnologías definidas por estas organizaciones incluyen cuatro áreas de estándares de la capa física:

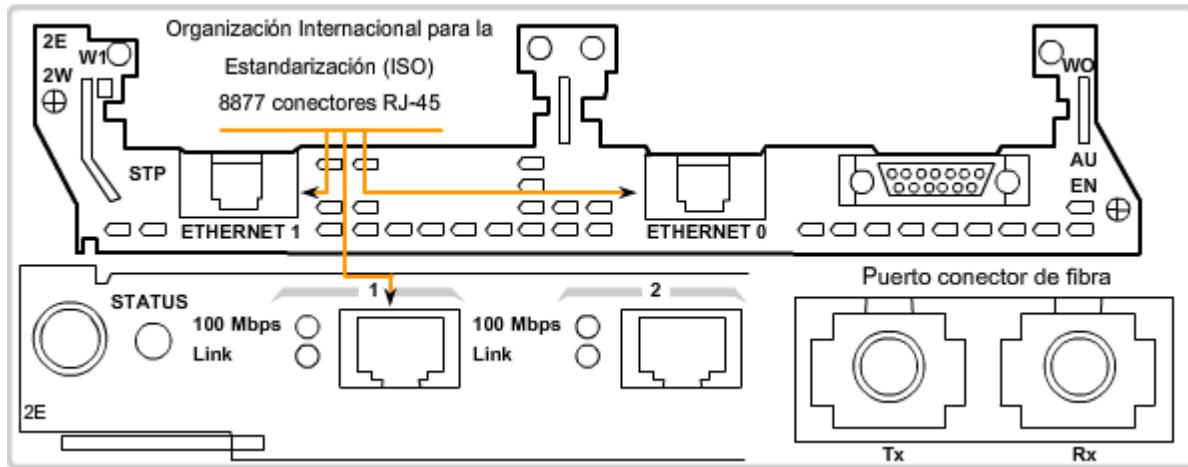
- Propiedades físicas y eléctricas de los medios
- Propiedades mecánicas (materiales, dimensiones, diagrama de pines) de los conectores
- Representación de los bits por medio de las señales (codificación)
- Definición de las señales de la información de control

Todos los componentes de hardware, como adaptadores de red (NIC, Tarjeta de interfaz de red), interfaces y conectores, material y diseño de los cables, se especifican en los estándares asociados con la capa física.

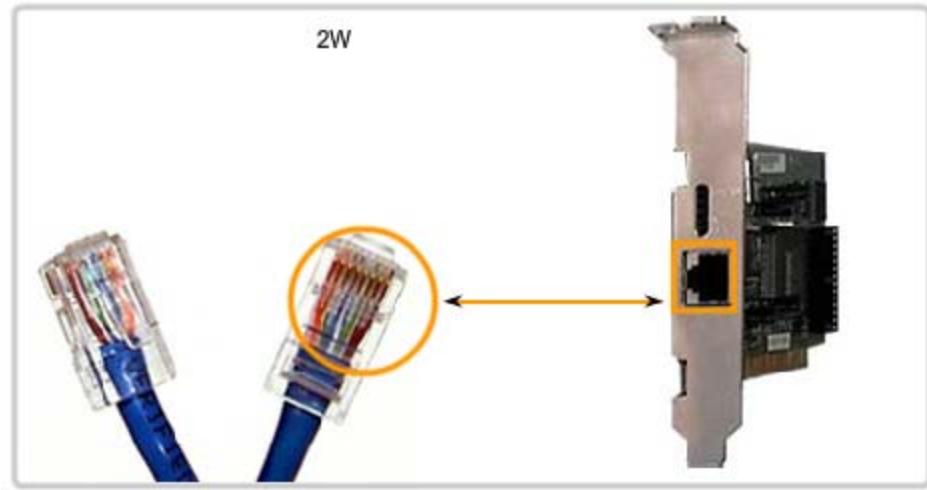
SEÑALES



CONECTORES



CABLES



8.1.4 Principios fundamentales de la capa física

Las tres funciones esenciales de la capa física son:

- Los componentes físicos
- Codificación de datos
- Señalización

Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.

Codificación

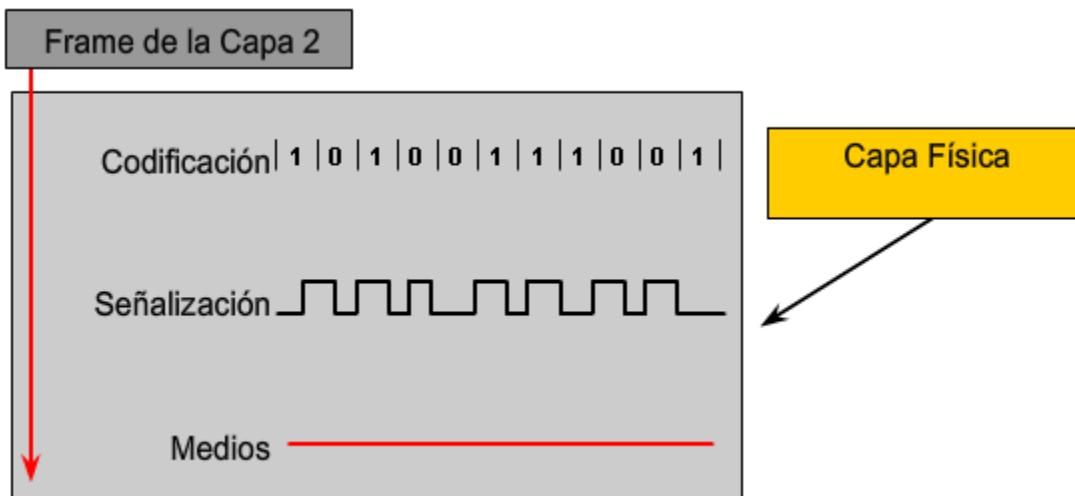
La codificación es un método utilizado para convertir un stream de bits de datos en un código predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. La utilización de patrones predecibles permite distinguir los bits de datos de los bits de control y ofrece una mejor detección de errores en los medios.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proporcionar códigos para control, como la identificación del comienzo y el final de una trama. El host que realiza la transmisión transmitirá el patrón específico de bits o un código para identificar el comienzo y el final de la trama.

Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan el “1” y el “0” en los medios. El método de representación de bits se denomina método de señalización. Los estándares de capa física deben definir qué tipo de señal representa un “1” y un “0”. Esto puede ser tan sencillo como un cambio en el nivel de una señal eléctrica, un impulso óptico o un método de señalización más complejo.

En las siguientes secciones, se examinarán diferentes métodos de señalización y codificación.



8.2 SEÑALIZACION Y CODIFICACION FISICA: REPRESENTACION DE BITS

8.2.1 Señalización de bits para los medios

Eventualmente, todas las comunicaciones desde la red humana se convierten en dígitos binarios que se transportan individualmente a través de los medios físicos.

Si bien todos los bits que conforman una trama se presentan ante la capa física como una unidad, la transmisión de la trama a través de los medios se realiza mediante un stream de bits enviados uno por vez. La capa física representa cada uno de los bits de la trama como una señal. Cada señal ubicada en los medios cuenta con un plazo específico de tiempo para ocupar los medios. Esto se denomina tiempo de bit. Las señales se procesan mediante el dispositivo receptor y se vuelven a enviar para representarlas como bits.

En la capa física del nodo receptor, las señales se vuelven a convertir en bits. Luego se examinan los bits para los patrones de bits del comienzo y el final de la trama con el objetivo de determinar si se ha recibido una trama completa. Luego la capa física envía todos los bits de una trama a la capa de Enlace de datos.

El envío exitoso de bits requiere de algún método de sincronización entre el transmisor y el receptor. Se deben examinar las señales que representan bits en momentos específicos durante el tiempo de bit, para determinar correctamente si la señal representa un “1” o un “0”. La sincronización se logra mediante el uso de un reloj. En las LAN, cada extremo de la transmisión mantiene su propio reloj. Muchos métodos de señalización utilizan transiciones predecibles en la señal para proporcionar sincronización entre los relojes de los dispositivos receptores y transmisores.

Métodos de señalización

Los bits se representan en el medio al cambiar una o más de las siguientes características de una señal:

- Amplitud
- Frecuencia
- Fase

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.

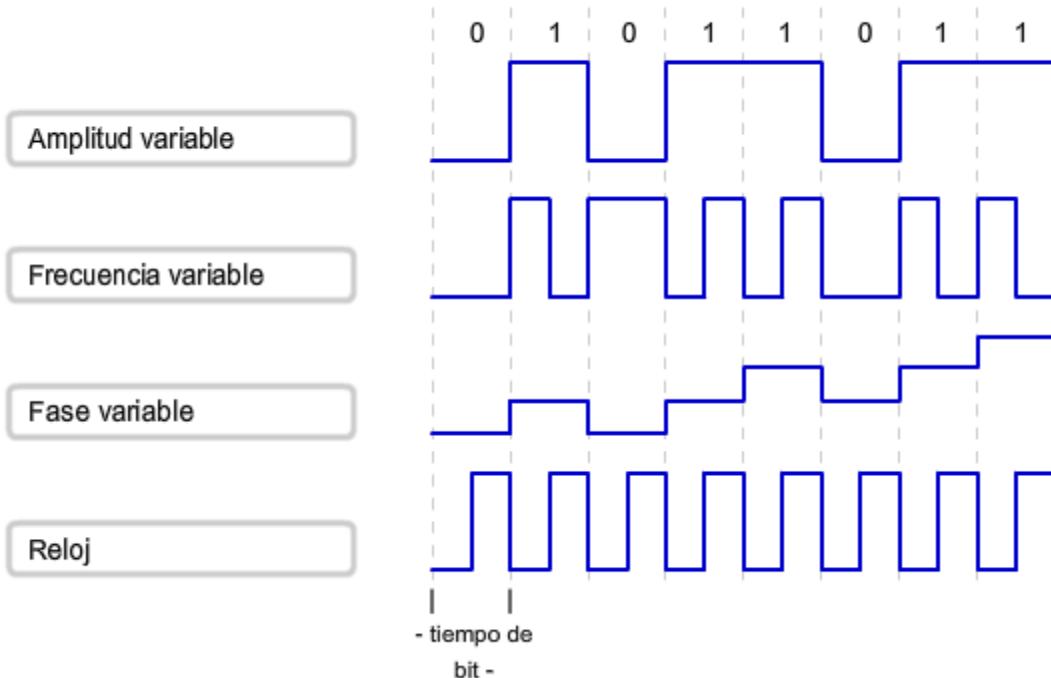
Por ejemplo, con el método sin retorno a cero (NRZ), un 0 puede representarse mediante un nivel de voltaje en los medios durante el tiempo de bit y un 1 puede representarse mediante un voltaje diferente en los medios durante el tiempo de bit.

También existen métodos de señalización que utilizan transiciones, o la ausencia de las mismas, para indicar un nivel lógico. Por ejemplo, la codificación Manchester indica un 0 mediante una transición de alto a bajo voltaje en el medio del tiempo de bit. Para un 1, existe una transición de bajo a alto voltaje en el medio del tiempo de bit.

El método de señalización utilizado debe ser compatible con un estándar para que el receptor pueda detectar las señales y decodificarlas. El estándar incluye un acuerdo entre el transmisor y el receptor sobre cómo representar los 1 y los 0. Si no existe un acuerdo de señalización, es decir, si se utilizan diferentes estándares en cada extremo de la transmisión, la comunicación a través del medio físico no se podrá llevar a cabo.

Los métodos de señalización para representar bits en los medios pueden ser complejos. Observaremos dos de las técnicas más simples para exemplificar el concepto.

Formas de representar una señal en el medio



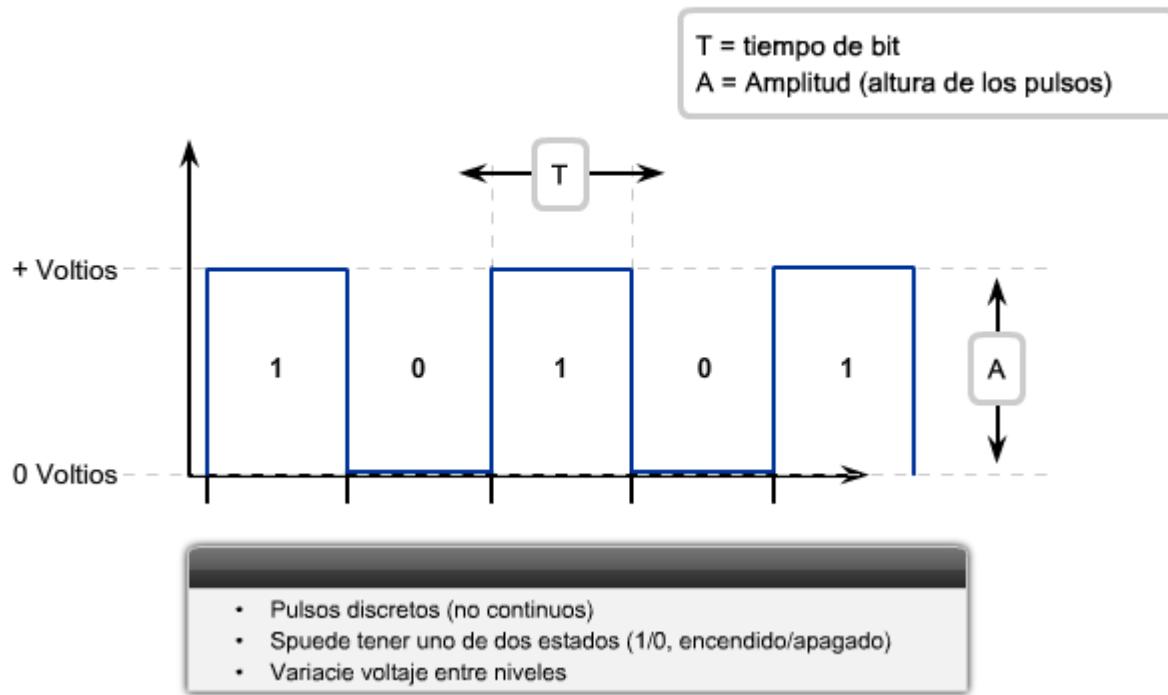
Señalización NRZ

Como primer ejemplo, examinaremos un método simple de señalización: sin retorno a cero (NRZ). En NRZ, el stream de bits se transmite como una secuencia de valores de voltaje, tal como se muestra en la figura.

Un valor de bajo voltaje representa un 0 lógico y un valor de alto voltaje representa un 1 lógico. El intervalo de voltaje depende del estándar específico de capa física utilizado.

Este método simple de señalización sólo es adecuado para enlaces de datos de velocidad lenta. La señalización NRZ no utiliza el ancho de banda de manera eficiente y es susceptible a la interferencia electromagnética. Además, los límites entre bits individuales pueden perderse al transmitir en forma consecutiva secuencias largas de 1 ó 0. En dicho caso, no se detectan transiciones de voltaje en los medios. Por lo tanto, los nodos receptores no tienen una transición para utilizar al resincronizar tiempos de bit con el nodo transmisor.

Bits de señalizacióSin retorno a cero (NRZ)



Codificación Manchester

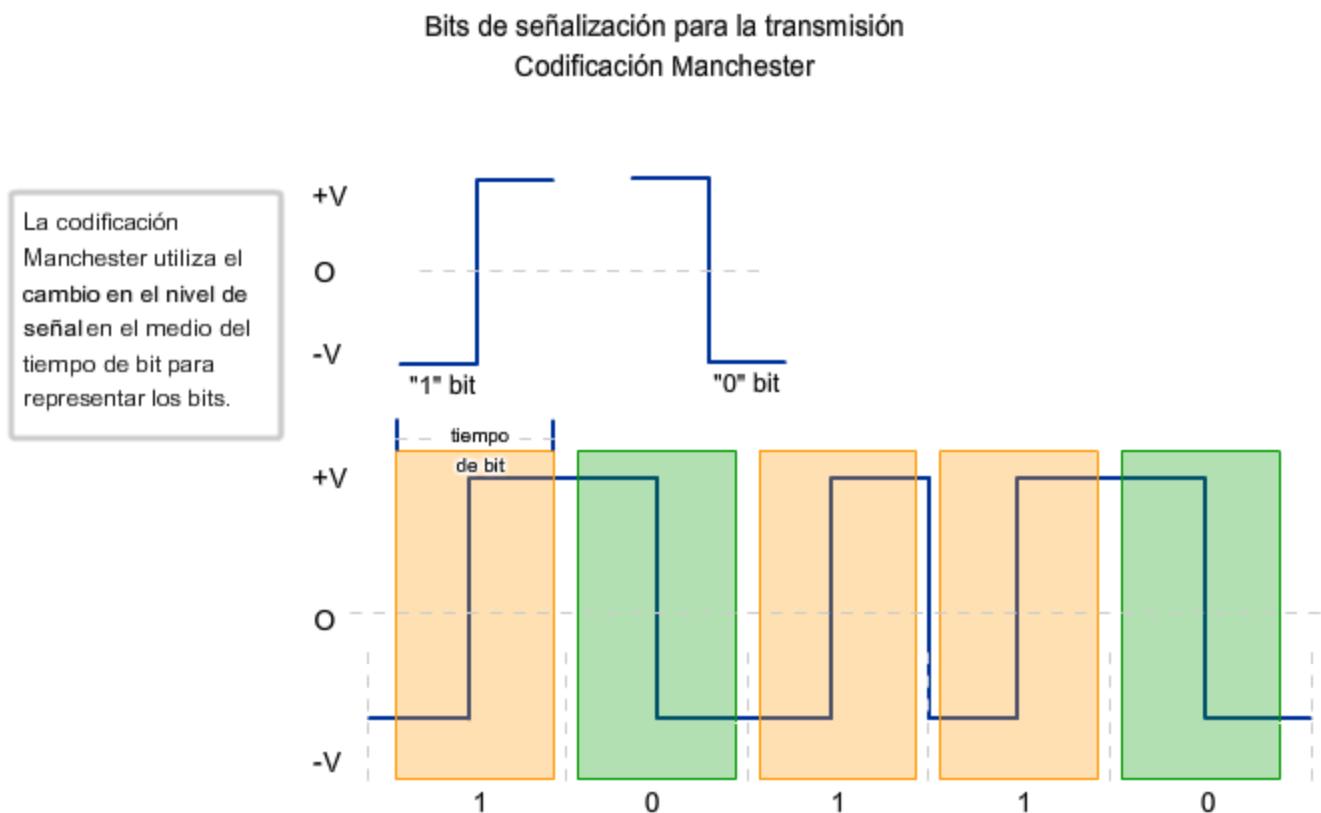
En lugar de representar bits como impulsos de valores simples de voltaje, en el esquema de codificación Manchester, los valores de bit se representan como transiciones de voltaje.

Por ejemplo, una transición desde un voltaje bajo a un voltaje alto representa un valor de bit de 1. Una transición desde un voltaje alto a un voltaje bajo representa un valor de bit de 0.

Como se muestra en la figura, se debe realizar una transición de voltaje en el medio de cada tiempo de bit. Esta transición puede utilizarse para asegurar que los tiempos de bit en los nodos receptores se encuentren sincronizados con el nodo transmisor.

La transición a la mitad del tiempo de bit será en dirección ascendente o descendente para cada unidad de tiempo en la cual se transmite un bit. Para los valores de bit consecutivos, una transición en el límite del bit "configura" la transición adecuada de tiempo medio de bit que representa el valor del bit.

Si bien no es lo suficientemente eficiente como para ser utilizada en velocidades de señalización superiores, la codificación Manchester constituye el método de señalización empleado por Ethernet 10BaseT (Ethernet se ejecuta a 10 megabits por segundo).



8.2.2 Codificación: Agrupación de bits

En la sección anterior, describimos el proceso de señalización según la forma en la que se representan los bits en los medios físicos. En esta sección, utilizamos la palabra codificación para representar una agrupación simbólica de bits antes de ser presentados a los medios. Al utilizar el paso de codificación antes de ubicar las señales en los medios, mejoramos la eficiencia mediante una transmisión de datos de mayor velocidad.

A medida que utilizamos mayores velocidades en los medios, existe la posibilidad de que se corrompan los datos. Al utilizar los grupos de codificación, podemos detectar errores de manera más eficiente. Además, a medida que aumenta la demanda de velocidades de datos, buscamos formas de representar más datos a través de los medios mediante la transmisión de menos bits. Los grupos de codificación proporcionan un método para realizar esta representación de datos.

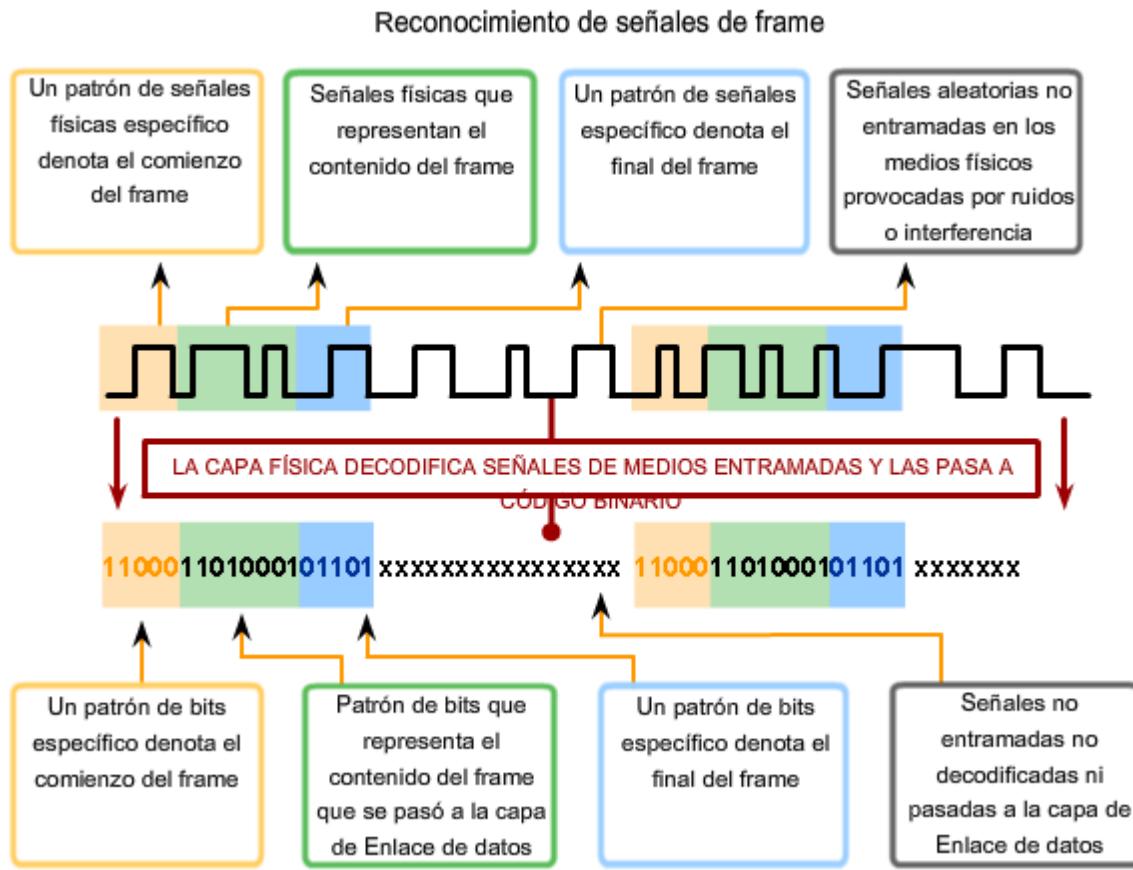
La capa física del dispositivo de red debe ser capaz de detectar señales legítimas de datos e ignorar señales aleatorias sin datos que también pueden encontrarse en el medio físico. El stream de señales que se transmite necesita iniciarse de tal forma que el receptor reconozca el comienzo y el final de la trama.

Patrones de señales

Una forma de detectar tramas es iniciar cada trama con un patrón de señales que represente los bits que la capa física reconoce como indicador del comienzo de una trama. Otro patrón de bits señalizará el final de la trama. Los bits de señales que no se entran de esta manera son ignorados por la capa física estándar que se utiliza.

Los bits de datos válidos deben agruparse en una trama. De lo contrario, los bits de datos se recibirán sin ningún contexto para darle significado a las capas superiores del modelo de red. La capa de Enlace de datos, la capa física o ambas pueden proporcionar este método de tramado.

La figura describe algunos de los objetivos de la señalización de patrones. Los patrones de señales pueden indicar: el comienzo, el final o el contenido de una trama. Estos patrones de señales pueden codificarse en bits. Los bits se interpretan como códigos. Los códigos indican la ubicación donde comienzan y finalizan las tramas.



Grupos de códigos

Las técnicas de codificación utilizan patrones de bits denominados símbolos. Es posible que la capa física utilice un conjunto de símbolos codificados, denominado grupos de códigos, para representar la información de control o datos codificados. **Un grupo de códigos es una secuencia consecutiva de bits de código que se interpretan y asignan como patrones de bits de datos.** Por ejemplo, los bits de código 10101 pueden representar los bits de datos 0011.

Como se muestra en la figura, los grupos de códigos a menudo se utilizan como una técnica de codificación intermedia para tecnologías LAN de mayor velocidad. Este paso se realiza en la capa física antes de generar señales de voltaje, impulsos de luz o radiofrecuencias. La transmisión de símbolos mejora la capacidad para detectar errores y la sincronización de los tiempos entre los dispositivos receptores y transmisores. Estas consideraciones son importantes al admitir una transmisión de velocidad alta a través de los medios.

Si bien la utilización de grupos de códigos genera sobrecarga debido a los bits adicionales que se transmiten, se logra mejorar la solidez de un enlace de comunicaciones. Esta característica se aplica especialmente a la transmisión de datos de mayor velocidad.

Entre las ventajas de utilizar grupos de códigos se incluyen:

- Reducción del nivel de error en los bits
- Limitación de la energía efectiva transmitida a los medios
- Ayuda para distinguir los bits de datos de los bits de control
- Mejoras en la detección de errores en los medios

Reducción de los errores en el nivel de bits

Para detectar correctamente un bit individual como un 0 o un 1, el receptor debe saber cómo y cuándo probar la señal en los medios. Este paso requiere la sincronización de los tiempos entre el receptor y el transmisor. En muchas tecnologías de la capa física, las transiciones en los medios se utilizan para esta sincronización. Si los patrones de bit que se transmiten en los medios no crean transiciones frecuentes, esta sincronización puede perderse y ocasionar un error binario individual. Los grupos de códigos se diseñan para que los símbolos obliguen la introducción de un amplio número de transacciones de bits en los medios para sincronizar estos tiempos. Esto se logra utilizando símbolos para asegurar que no se utilicen demasiados 1 ó 0 en forma consecutiva.

Limitación de la energía transmitida

En muchos grupos de códigos, los símbolos garantizan el equilibrio entre la cantidad de 1 y 0 en una secuencia de símbolos. El proceso de equilibrar la cantidad de números 1 y 0 transmitidos se denomina equilibrio DC. Este método evita que se incluyan cantidades excesivas de energía en los medios durante una transmisión. De esta manera, se reduce la interferencia generada desde los medios. En muchos métodos de señalización de medios, un nivel lógico, por ejemplo un 1, se representa mediante la presencia de energía que se envía a los medios, mientras que el nivel lógico opuesto, un 0, se representa como la ausencia de esta energía. La transmisión de una secuencia larga de números 1 podría recalentar el láser transmisor y los fotodiodos en el receptor, lo que podría causar elevados índices de error.

Distinción entre datos y control

Los grupos de códigos incluyen tres tipos de símbolos:

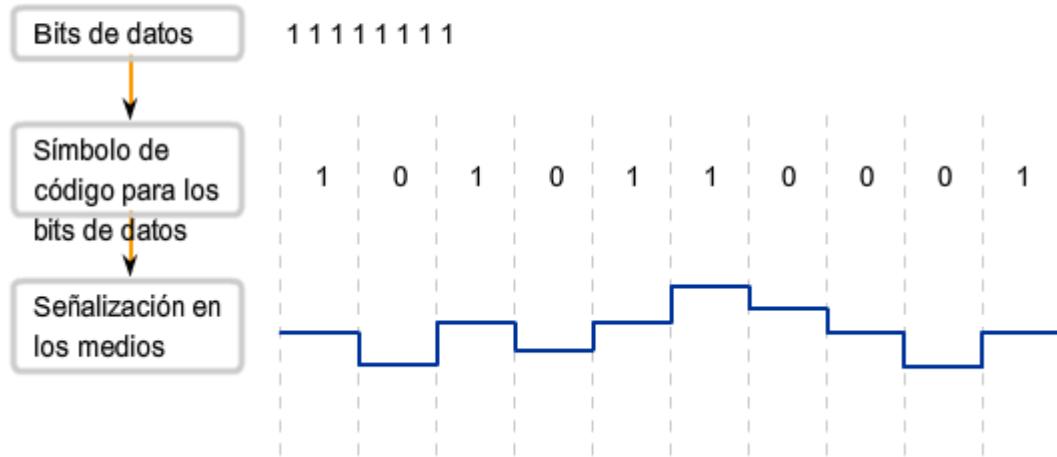
- Símbolos de datos: Símbolos que representan los datos de la trama cuando ésta se transmite a la capa física.
- Símbolos de control: Códigos especiales introducidos por la capa física que se utiliza para controlar la transmisión. Entre ellos se incluyen los símbolos de fin de la trama y de medios inactivos.
- Símbolos no válidos: Símbolos cuyos patrones no están permitidos en los medios. El receptor de un símbolo no válido indica un error de trama.

Todos los símbolos codificados en los medios son exclusivos. Los símbolos que representan datos que se envían a través de la red tienen diferentes patrones de bit de los símbolos utilizados para control. Estas diferencias permiten que la capa física en el nodo receptor identifique inmediatamente datos desde la información de control.

Mejoras en la detección de errores en los medios

Además de los símbolos de datos y de control, los grupos de códigos incluyen símbolos inválidos. Éstos son los símbolos que pueden crear secuencias largas de 1 ó 0 en los medios. Por lo tanto, no son utilizados por el nodo transmisor. Si un nodo receptor recibe uno de estos patrones, la capa física puede determinar que se ha producido un error en la recepción de datos.

Grupos de códigos



4B/5B

Como ejemplo, examinaremos un grupo de códigos simple denominado 4B/5B. Los grupos de códigos que se utilizan actualmente en las redes modernas son, por lo general, más complejos.

En esta técnica, 4 bits de datos se convierten en símbolos de un código de 5 bits para la transmisión a través del sistema de medios. En 4B/5B, cada byte que se transmitirá se divide en parte de cuatro bits o cuartetos y se codifica como valores de cinco bits denominados símbolos. Estos símbolos representan los datos que deben transmitirse al igual que el conjunto de códigos que permite controlar la transmisión en los medios. Los códigos incluyen símbolos que indican el comienzo y el final de la transmisión de una trama. Si bien este proceso genera una sobrecarga en las transmisiones de bits, también incorpora características que ayudan a la transmisión de datos a velocidades superiores.

4B/5B garantiza la aplicación de al menos un cambio de nivel por código para proporcionar sincronización. La mayoría de los códigos utilizados en 4B/5B equilibran la cantidad de números 1 y 0 utilizados en cada símbolo.

Como se muestra en la figura, se asignan 16 de las 32 combinaciones posibles de grupos de códigos para los bits de datos. Los grupos de códigos restantes se utilizan para los símbolos inválidos y los símbolos de control. Seis de los símbolos se utilizan para ejecutar funciones especiales que identifican la transición desde datos de espera a datos de trama y el delimitador de final del stream. Los 10 símbolos restantes indican códigos inválidos.

Símbolos de código 4B/5B

Códigos de datos

| Código 4B | Símbolo 5B |
|-----------|------------|
| 0000 | 11110 |
| 0001 | 01001 |
| 0010 | 10100 |
| 0011 | 10101 |
| 0100 | 01010 |
| 0101 | 01011 |
| 0110 | 01110 |
| 0111 | 01111 |
| 1000 | 10010 |
| 1001 | 10011 |
| 1010 | 10110 |
| 1011 | 10111 |
| 1100 | 11010 |
| 1101 | 11011 |
| 1110 | 11100 |
| 1111 | 11101 |

Códigos no válidos y de control

| Código 4B | Símbolo 5B |
|----------------------|------------|
| inactivo | 11111 |
| comienzo del stream | 11000 |
| comienzo del stream | 10001 |
| final del stream | 01101 |
| final del stream | 00111 |
| error de transmisión | 00111 |
| inválido | 00000 |
| inválido | 00001 |
| inválido | 00010 |
| inválido | 00011 |
| inválido | 00100 |
| inválido | 00101 |
| inválido | 00110 |
| inválido | 01000 |
| inválido | 10000 |
| inválido | 11001 |

8.2.3 Capacidad de transportar datos

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. La transferencia de datos puede medirse de tres formas:

- Ancho de banda
- Rendimiento
- Capacidad de transferencia útil

Ancho de banda

La capacidad que posee un medio de transportar datos se describe como el **ancho de banda** de los datos sin procesar de los medios. **El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado.** El ancho de banda generalmente se mide en kilobits por segundo (303ers) o megabits por segundo (Mbps).

El ancho de banda práctico de una red se determina mediante una combinación de factores: las propiedades de las tecnologías y los medios físicos elegidos para señalizar y detectar 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.

La figura muestra las unidades de ancho de banda de uso más frecuente.

Unidades de ancho de banda, velocidad de transmisión (throughput) y capacidad de transferencia útil

| Unidad de ancho de banda | Abreviatura | Equivalencia |
|--------------------------|-------------|--|
| Bits por segundo | bps | 1 bps = fundamental unit of bandwidth |
| Kilobits por segundo | kbps | 1 kbps = 1,000 bps = 10^3 bps |
| Megabits por segundo | Mbps | 1 Mbps = 1,000,000 bps = 10^6 bps |
| Gigabits por segundo | Gbps | 1 Gbps = 1,000,000,000 bps = 10^9 bps |
| Terabits por segundo | Tbps | 1 Tbps = 1,000,000,000,000 bps = 10^{12} bps |

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 generalmente no coincide con el ancho de banda especificado en las implementaciones de la capa física, como Ethernet.

Muchos factores influyen en el rendimiento. Entre estos factores se incluye la cantidad y el tipo de tráfico además de la cantidad de dispositivos de red que se encuentran en la red que se está midiendo. En una topología multiacceso como Ethernet, los nodos compiten por el acceso y la utilización de medios. Por lo tanto, el rendimiento de cada nodo se degrada a medida que aumenta el uso de los medios.

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.

Capacidad de transferencia útil

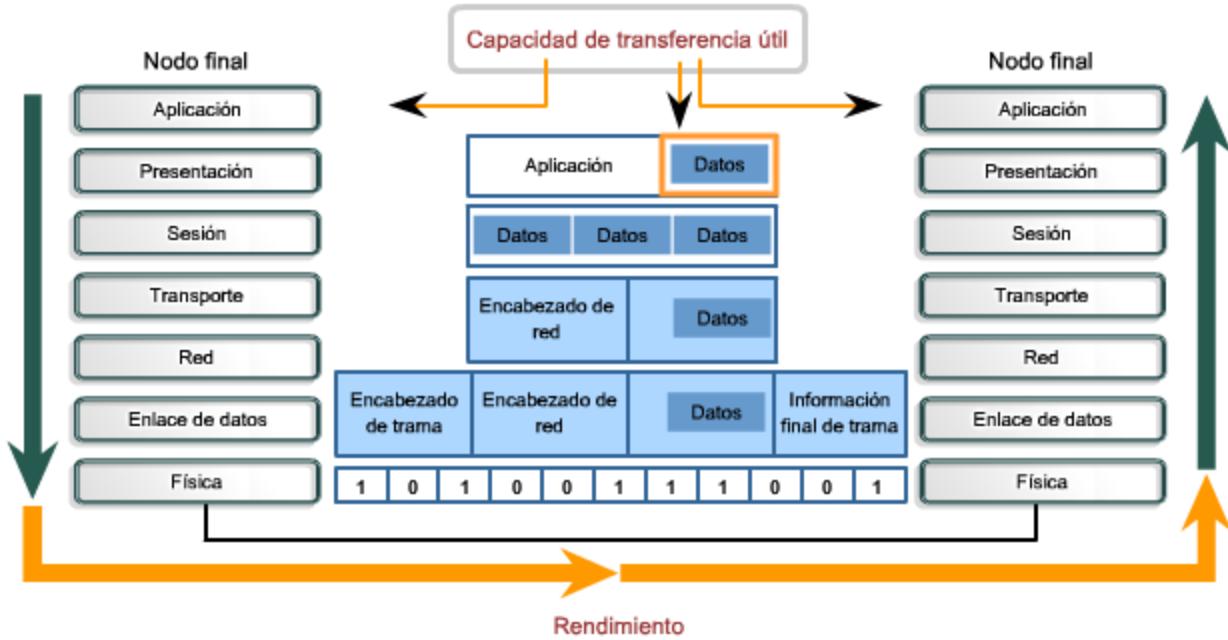
Se ha creado una tercera medida para evaluar la transferencia de datos utilizables. Dicha medición se denomina capacidad de transferencia útil. **La capacidad de transferencia útil es la medida de datos utilizables transferidos durante un período de tiempo determinado. Por lo tanto, es la medida de mayor interés para los usuarios de la red.**

Como se muestra en la figura, la capacidad de transferencia útil mide la transferencia efectiva de los datos del usuario entre las entidades de la capa de aplicación, por ejemplo entre el proceso de un servidor Web de origen y un dispositivo con explorador Web de destino.

A diferencia del rendimiento, que mide la transferencia de bits y no la transferencia de datos utilizables, la capacidad de transferencia útil considera los bits que generan la sobrecarga del protocolo. Esta capacidad representa el rendimiento sin la sobrecarga de tráfico para establecer sesiones, acuses de recibo y encapsulaciones.

Por ejemplo, considere dos hosts en una LAN que transfiere un archivo. El ancho de banda de la LAN es de 100 Mbps. Debido al uso compartido y al encabezado de los medios, el rendimiento entre los equipos es solamente de 60 mbps. Con una sobrecarga del proceso de encapsulación de stack TCP/IP, la velocidad real de los datos recibidos por la computadora de destino, es decir la capacidad de transferencia útil, es sólo de 40 Mbps.

El rendimiento de los datos y la capacidad de transferencia



La **velocidad de transferencia de datos** es el rendimiento real de la red. La **capacidad de transferencia útil** es una medida de la transferencia de datos utilizables una vez que se ha eliminado el tráfico de encabezado de protocolo.

8.3 MEDIOS FÍSICOS: CONEXIÓN DE LA COMUNICACIÓN

8.3.1 Tipos de medios físicos

La capa física se ocupa de la señalización y los medios de red. Esta capa produce la representación y agrupación de bits en voltajes, radiofrecuencia e impulsos 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 conectores funcionen según lo previsto mediante diferentes implementaciones de la 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.

La figura muestra algunas de las características de los medios de networking.

Esta sección también describirá algunas de las características importantes de los medios inalámbricos, ópticos y de cobre comúnmente utilizados.

Medios de Ethernet

| | 10BASE-T | 100BASE-TX | 100BASE-FX | 1000BASE-CX | 1000BASE-T | 1000BASE-SX | 1000BA |
|-----------------------------|---|------------------------------------|---------------------------|------------------|---|---|---|
| Medios | UTP Categoría EIA/TIA 3, 4, 5, cuatro pares | UTP Categoría 5 EIA/TIA, dos pares | 50/62.5 m fibra multimodo | STP | UTP Categoría 5 (o mayor) EIA/TIA, cuatro pares | fibra multimodo de 50/62.5 micrones | fibra mi de 50/6 microne fibra monorr 9 micro |
| Longitud de segmento máxima | 100m (328 pies) | 100m (328 pies) | 2 km (6562 pies) | 25 m (82 pies) | 100 m (328 pies) | Hasta 550m (1804 pies) según la fibra utilizada | 550 m (MMF) (SMF) |
| Topología | Estrella | Estrella | Estrella | Estrella | Estrella | Estrella | Estrella |
| Conector | ISO 8877 (RJ-45) | ISO 8877 (RJ-45) | | ISO 8877 (RJ-45) | | | |

Medios inalámbricos

| | | | | |
|--------------|---------------------------------------|-----------------------------|---------------------------|--|
| Estándares | Bluetooth 802.15 | 802.11(a,b,g,n), HiperLAN 2 | 802.11, MMDS, LMDS | GSM, GPRS, CDMA, 2.5- 3G |
| Velocidad | <1 Mbps | 1 - 54+ Mbps | 22 Mbps+ | De 10 a 384 Kbps |
| Intervalo | Cortocircuito | Medio | Medio - largo | Largo |
| Aplicaciones | Dispositivo a dispositivo entre pares | Red empresarial | Fijo, acceso última milla | Acceso para PDA, teléfonos móviles y celulares |

8.3.2 Medios de cobre

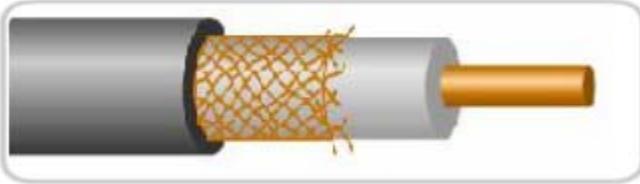
El medio más utilizado para las comunicaciones de datos es el cableado que utiliza alambres de cobre para señalizar bits de control y datos entre los dispositivos de red. El cableado utilizado para las comunicaciones de datos generalmente consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización.

Otros tipos de cableado de cobre, conocidos como cables coaxiales, tienen un conductor simple que circula por el centro del cable envuelto por el otro blindaje, pero está aislado de éste. El tipo de medio de cobre elegido se especifica mediante el estándar de la capa física necesario para enlazar las capas de Enlace de datos de dos o más dispositivos de red.

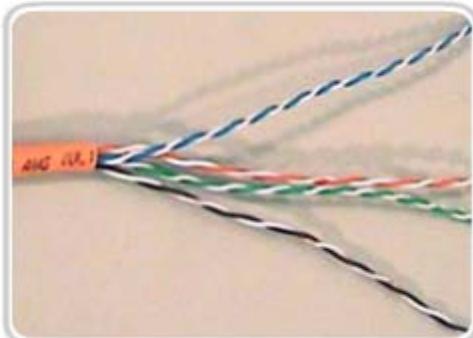
Estos cables pueden utilizarse para conectar los nodos de una LAN a los dispositivos intermedios, como routers o switches. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos, como una compañía telefónica. Cada tipo de conexión y sus dispositivos complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física.

Los medios de red generalmente utilizan conectores y tomas. Estos elementos ofrecen conexión y desconexión sencillas. 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.

La figura muestra algunos conectores y medios de cobre de uso común.



Cable coaxial



Cable de par trenzado no blindado



Conexiones RJ-45

Interferencia de señal externa

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.

Los valores de voltaje y sincronización en estas señales son susceptibles a la interferencia o “ruido” generado fuera del sistema de comunicaciones. Estas señales no deseadas pueden distorsionar y corromper las señales de datos que se transportan a través de los medios de cobre. Las ondas de radio y los dispositivos electromagnéticos como luces fluorescentes, motores eléctricos y otros dispositivos representan una posible fuente de ruido.

Los tipos de cable con blindaje o trenzado de pares de alambre están diseñados para minimizar la degradación de señales debido al ruido electrónico.

La susceptibilidad de los cables de cobre al ruido electrónico también puede estar limitada por:

- Selección del tipo o categoría de cable más adecuado para proteger las señales de datos en un entorno de networking determinado
- Diseño de una infraestructura de cables para evitar las fuentes de interferencia posibles y conocidas en la estructura del edificio
- Utilización de técnicas de cableado que incluyen el manejo y la terminación apropiados de los cables

La figura muestra algunas fuentes de interferencia.

Interferencia externa con los medios de cobre



Fuentes de interferencia con las señales de datos en los medios de cobre



Iluminación fluorescente



Motores eléctricos



Ondas de radio

8.3.3 Cable de par trenzado no blindado (UTP)

El cableado de par trenzado no blindado (UTP), como se utiliza en las LAN Ethernet, consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible. Como se muestra en la figura, los códigos de color identifican los pares individuales con sus alambres y sirven de ayuda para la terminación de cables.

El trenzado cancela las señales no deseadas. Cuando dos alambres de un circuito eléctrico se colocan uno cerca del otro, los campos electromagnéticos externos crean la misma interferencia en cada alambre. Los pares se trenzan para mantener los alambres lo más cerca posible. Cuando esta interferencia común se encuentra en los alambres del par trenzado, el receptor los procesa de la misma manera pero en forma opuesta. Como resultado, las señales provocadas por la interferencia electromagnética desde fuentes externas se cancelan de manera efectiva.

Este efecto de cancelación ayuda además a evitar la interferencia proveniente de fuentes internas denominada crosstalk. Crosstalk es la interferencia ocasionada por campos magnéticos alrededor de los pares adyacentes de alambres en un cable. Cuando la corriente eléctrica fluye a través de un alambre, se crea un campo magnético circular a su alrededor. Cuando la corriente fluye en direcciones opuestas en los dos alambres de un par, los campos magnéticos, como fuerzas equivalentes pero opuestas, producen un efecto de cancelación mutua. Además, los distintos pares de cables que se trenzan en el cable utilizan una cantidad diferente de vueltas por metro para ayudar a proteger el cable de la crosstalk entre los pares.

Estándares de cableado UTP

El cableado UTP que se encuentra comúnmente en el trabajo, las escuelas y los hogares cumple con los estándares estipulados en conjunto por la Asociación de las Industrias de las Telecomunicaciones (TIA) y la Asociación de Industrias

Electrónicas (EIA). TIA/EIA-568^a estipula los estándares comerciales de cableado para las instalaciones LAN y es el estándar de mayor uso en entornos de cableado LAN. Algunos de los elementos definidos son:

- Tipos de cables
- Longitudes de los cables
- Conectores
- Terminación de los cables
- Métodos para realizar pruebas de cable

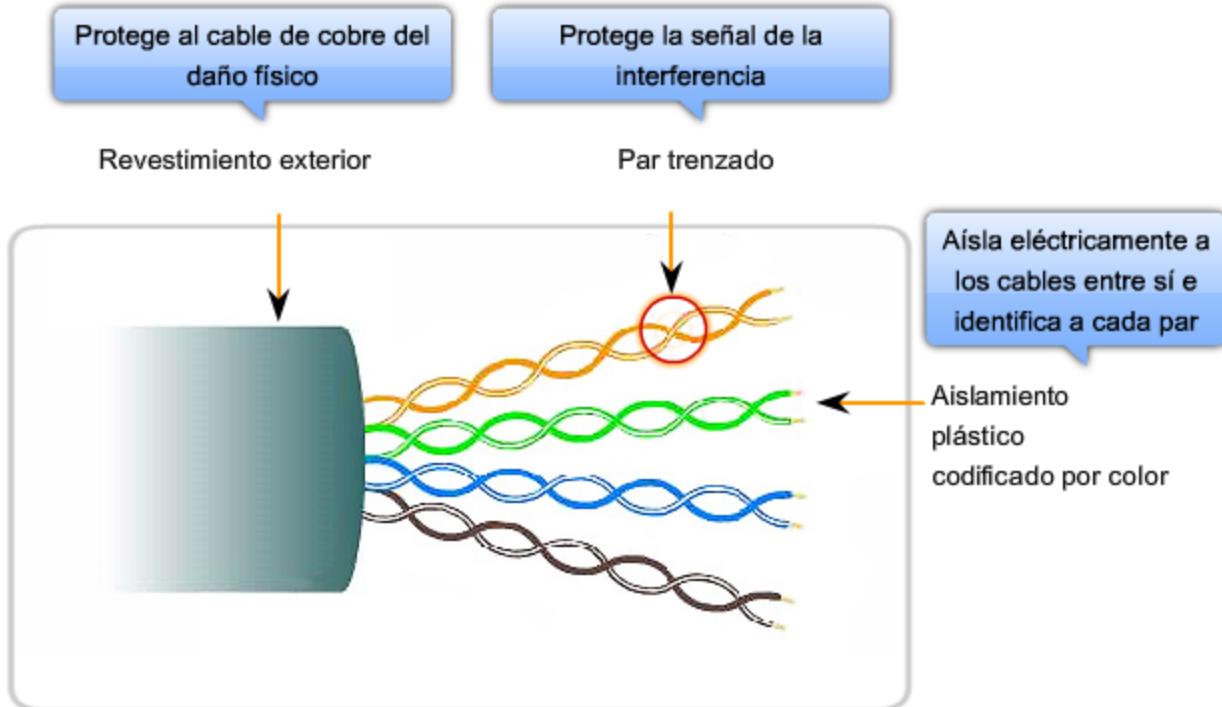
El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define las características eléctricas del cableado de cobre. IEEE califica el cableado UTP según su rendimiento. Los cables se dividen en categorías según su capacidad para transportar datos de ancho de banda a velocidades mayores. Por ejemplo, el cable de Categoría 5 (Cat5) se utiliza comúnmente en las instalaciones de FastEthernet 100BASE-TX. Otras categorías incluyen el cable de Categoría 5 mejorado (Cat5e) y el de Categoría 6 (Cat6).

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.

Algunas personas conectan redes de datos utilizando los sistemas telefónicos existentes. Generalmente, el cableado de estos sistemas es algún tipo de UTP de categoría inferior en comparación con los estándares actuales de Cat5+.

La instalación de cableado menos costoso pero de calificación inferior resulta poco útil y limitada. Si se decide adoptar posteriormente una tecnología LAN más rápida, es posible que se requiera el reemplazo total de la infraestructura del cableado instalado.

Cable de par trenzado no blindado (UTP)



Tipos de cable UTP

El cableado UTP, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red, como computadoras, y dispositivos intermedios, como routers y switches de red.

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los alambres individuales del cable deben conectarse en diferentes órdenes para distintos grupos de pins en los conectores RJ-45. A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

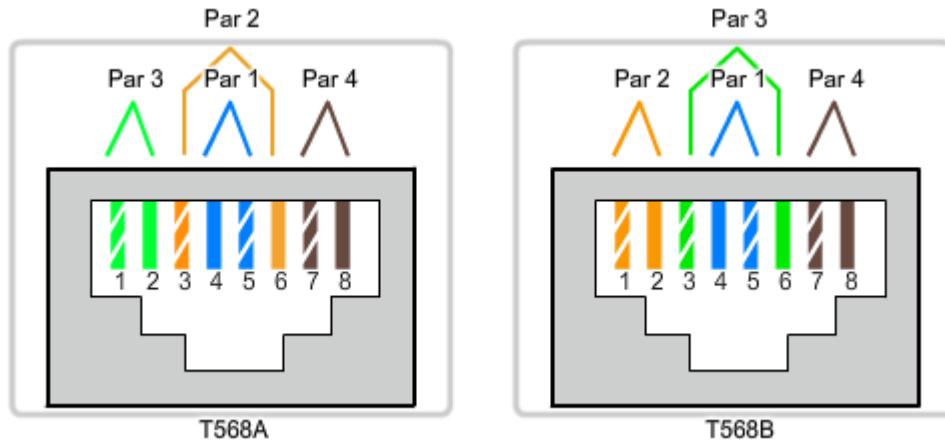
- Cable directo de Ethernet
- Cruzado de Ethernet
- Consola

La figura muestra la aplicación típica de estos cables, como así también una comparación de estos tres tipos de cable.

Es posible que la utilización 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.

Tipos de cables directo, de conexión cruzada y transpuesto

| Tipo de cable | Estándar | Aplicación |
|---------------------------|--------------------------------------|---|
| Cable directo de Ethernet | Un extremo T568A, otro extremo T568B | Conexión de un host de red a un dispositivo de red como un switch o hub. |
| Cruzado Ethernet | Un extremo T568A, otro extremo T568B | Conexión de dos hosts de red. Conexión de dos dispositivos intermedios de red (switch a switch o router a router). |
| Transpuesto | Propietario de Cisco | Conecte el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador. |



8.3.4 Otros cables de cobre

Se utilizan otros dos tipos de cable de cobre:

1. Coaxial

2. Par trenzado blindado (STP)

Cable coaxial

El cable coaxial consiste en un conductor de cobre rodeado de una capa de aislante flexible, como se muestra en la figura.

Sobre este material aislante hay una malla de cobre tejida o una hoja metálica que actúa como segundo alambre del circuito y como blindaje para el conductor interno. La segunda capa o blindaje reduce la cantidad de interferencia electromagnética externa. La envoltura del cable recubre el blindaje.

Todos los elementos del cable coaxial rodean el conductor central. Esta construcción se denomina coaxial (o coax como abreviatura) ya que todos comparten el mismo eje.

Usos del cable coaxial

El diseño del cable coaxial ha sido adaptado para diferentes necesidades. El coaxial es un tipo de cable importante que se utiliza en tecnologías de acceso inalámbrico o por cable. Estos cables se utilizan para colocar antenas en los dispositivos inalámbricos. También transportan energía de radiofrecuencia (RF) entre las antenas y el equipo de radio.

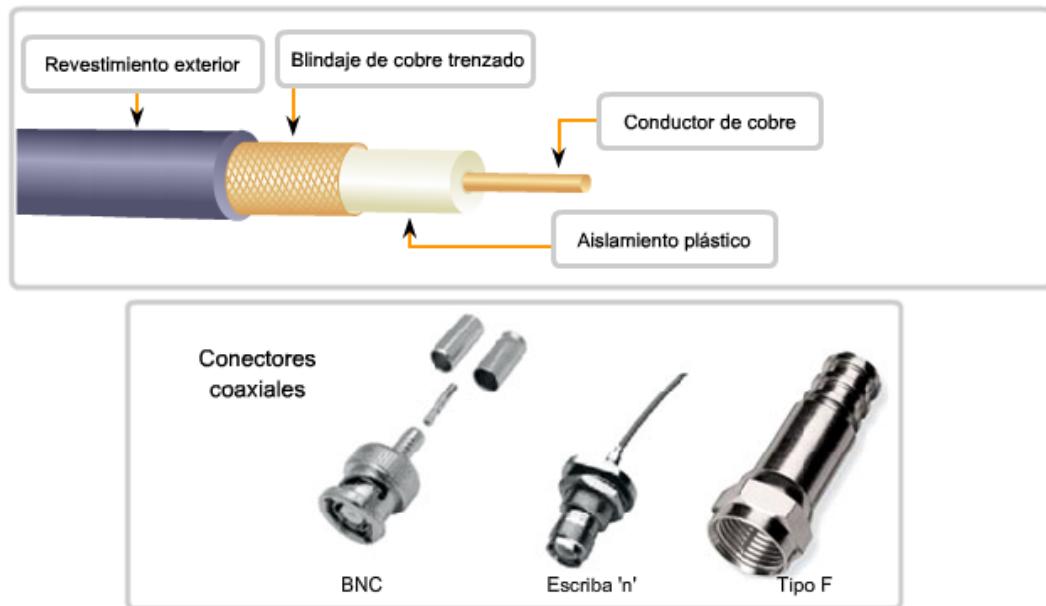
Es el medio de uso más frecuente para transportar señales elevadas de radiofrecuencia mediante cableado, especialmente señales de televisión por cable. La televisión por cable tradicional, con transmisión exclusiva en una dirección, estaba totalmente compuesta por cable coaxial.

Actualmente, los proveedores de servicio de cable están convirtiendo sistemas de una a dos vías para suministrar conectividad de Internet a sus clientes. Para ofrecer estos servicios, las partes de cable coaxial y los elementos de amplificación compatibles se reemplazan por cables de fibra óptica multimodo. 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).

En el pasado, el cable coaxial se utilizaba para las instalaciones Ethernet. Hoy en día, el UTP (Par trenzado no blindado) ofrece costos más bajos y un ancho de banda mayor que el coaxial y lo ha reemplazado como estándar para todas las instalaciones Ethernet.

Existen diferentes tipos de conectores con cable coaxial. La figura muestra algunos de estos tipos de conectores.

Diseño de cable coaxial



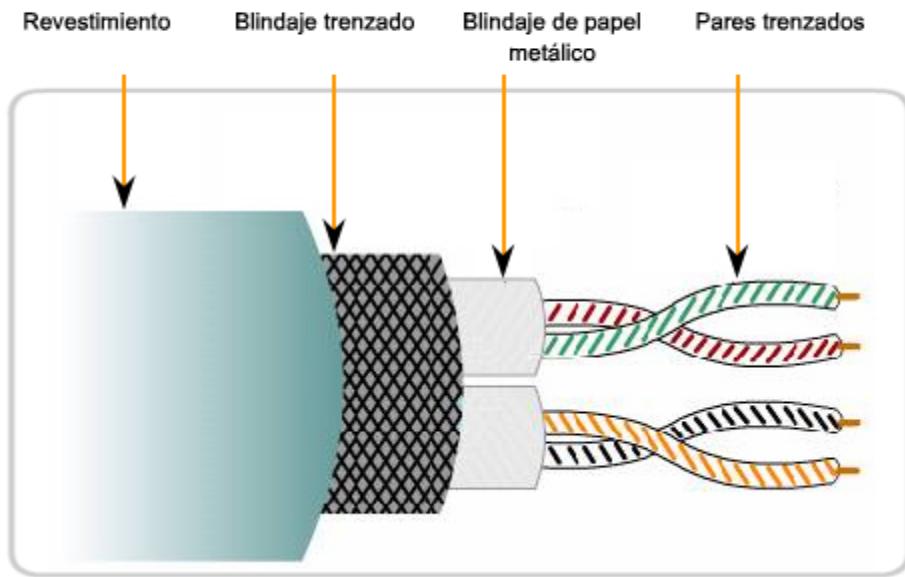
Cable de par trenzado blindado (STP)

Otro tipo de cableado utilizado en las redes es el par trenzado blindado (STP). Como se muestra en la figura, STP utiliza dos pares de alambres que se envuelven en una malla de cobre tejida o una hoja metálica.

El cable STP cubre todo el grupo de alambres dentro del cable al igual que los pares de alambres individuales. STP ofrece una mejor protección contra el ruido que el cableado UTP pero a un precio considerablemente superior.

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. El nuevo estándar de 10 GB para Ethernet incluye una disposición para el uso del cableado STP. Esta medida vuelve a generar interés en el cableado de par trenzado blindado.

Cable de par trenzado blindado (STP)



8.3.5 Seguridad de los medios de cobre

Peligro por electricidad

Uno de los posibles problemas de los medios de cobre es que los alambres de cobre pueden conducir la electricidad de manera no deseada. Debido a este problema, el personal y el equipo podrían estar sujetos a diferentes peligros por electricidad.

Un dispositivo de red defectuoso podría conducir la corriente al chasis 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. Por último, el cableado de cobre puede conducir voltajes provocados por descargas eléctricas a los dispositivos de red.

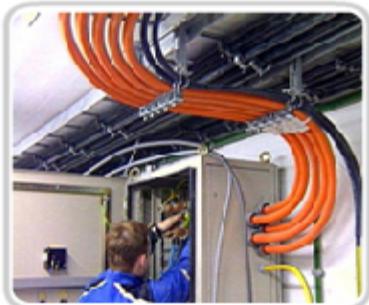
Como consecuencia, las corrientes y los voltajes no deseados pueden generar un daño a los dispositivos de red y a las computadoras conectadas o bien provocar lesiones al personal. Para prevenir situaciones potencialmente peligrosas y

perjudiciales, es importante instalar correctamente el cableado de cobre según las especificaciones relevantes y los códigos de edificación.

Peligros de incendio

El revestimiento y 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.

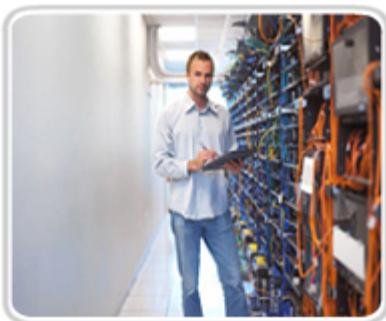
Seguridad de los medios de cobre



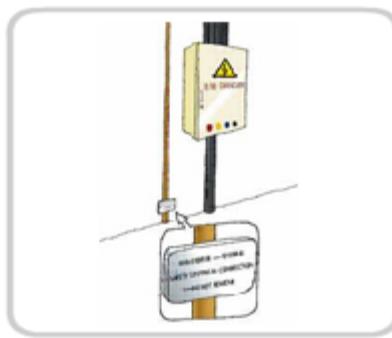
La separación entre el cableado de datos y el de energía eléctrica debe cumplir con los códigos de seguridad.



Los cables deben estar conectados correctamente.



Se deben verificar las instalaciones para detectar cualquier daño.



El equipo debe estar correctamente conectado a tierra.

8.3.6 Medios de fibra

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar. La mayoría de los estándares actuales de transmisión aún necesitan analizar el ancho de banda potencial de este medio.

Comparación entre cableado de cobre y de fibra óptica

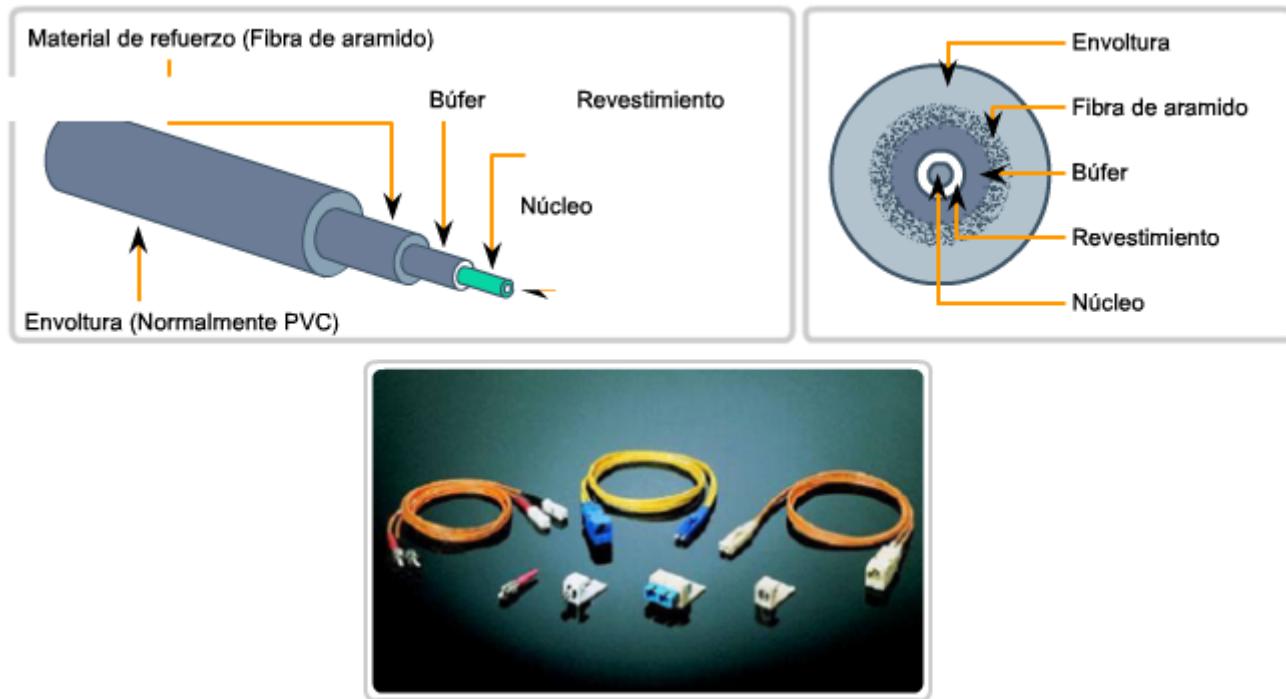
Teniendo en cuenta que las fibras utilizadas en los medios de fibra óptica no son conductores eléctricos, este medio es inmune a la interferencia electromagnética y no conduce corriente eléctrica no deseada cuando existe un problema de conexión a tierra. Las fibras ópticas pueden utilizarse en longitudes 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 en la misma distancia (pero para una capacidad mayor)
- Se necesitan diferentes habilidades y equipamiento 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.

Diseño de cable de los medios de fibra



Connectores de fibra

Fabricación del cable

Los cables de fibra óptica consisten en un revestimiento exterior de PVC y un conjunto de materiales de refuerzo que rodean la fibra óptica y su revestimiento. El revestimiento rodea la fibra de plástico o de vidrio y está diseñado para prevenir la pérdida de luz de la fibra. 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. Los patch cables de la fibra óptica agrupan dos cables de fibra óptica y su terminación incluye un par de conectores de fibra únicos y estándares. Algunos conectores de fibra aceptan fibras receptoras y transmisoras en un único conector.

Diseño de cables de medios de fibra

La fibra proporciona comunicaciones full duplex con un cable dedicado para cada dirección.



Producción y detección de señales ópticas

Los láseres o diodos de emisión de luz (LED) generan impulsos de luz que se utilizan para representar los datos transmitidos como bits en los medios. 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 del 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.

Fibra multimodo y monomodo

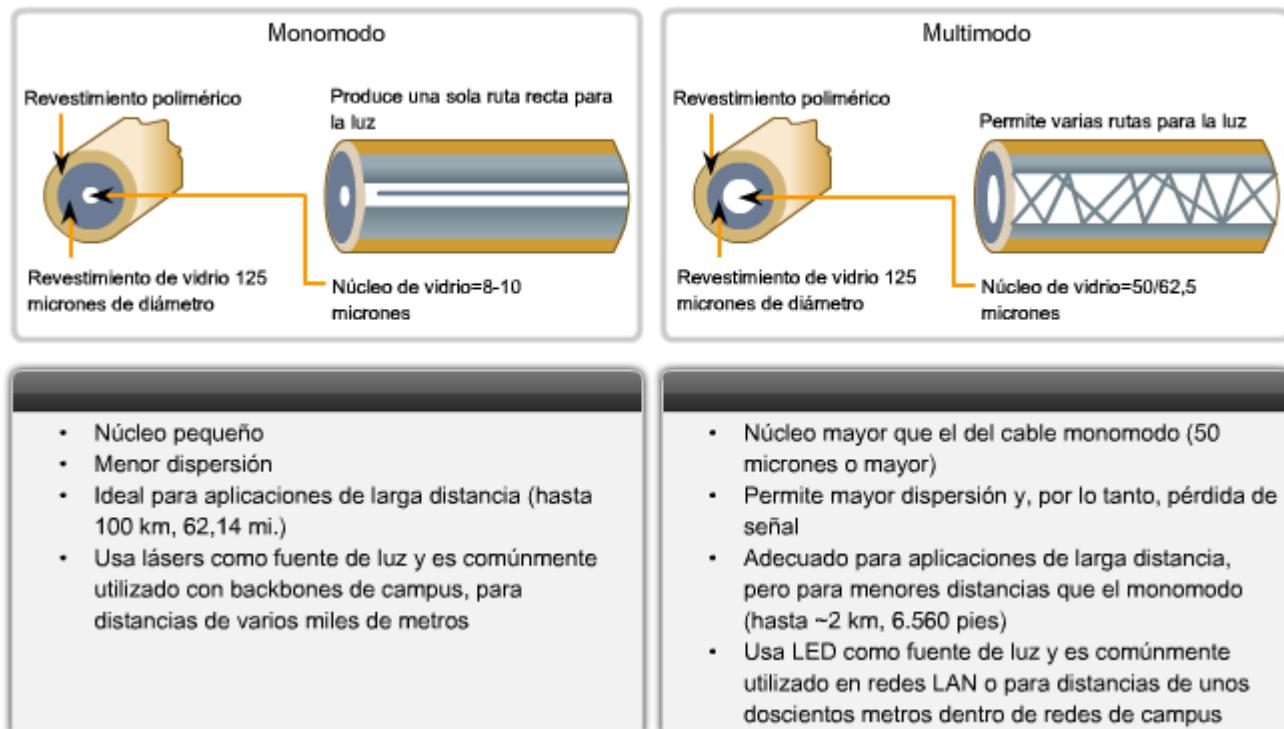
En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos: monomodo y multimodo.

La fibra óptica monomodo transporta un sólo rayo de luz, generalmente emitido desde un láser. Este tipo de fibra puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

La fibra óptica multimodo a menudo utiliza emisores LED que no generan una única ola de luz coherente. En cambio, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos. Los tendidos extensos de fibra pueden generar impulsos poco claros al recibirlos en el extremo receptor ya que la luz que ingresa a la fibra en diferentes ángulos requiere de distintos períodos de tiempo para viajar a través de la fibra. Este efecto, denominado dispersión modal, limita la longitud de los segmentos de fibra multimodo.

La fibra multimodo y la fuente de luz del LED que utiliza resultan más económicas que la fibra monomodo y su tecnología del emisor basada en láser.

Modos de medios de fibra



8.3.7 Medios inalámbricos

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Como medio de red, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre.

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. El medio inalámbrico también es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

Los dispositivos y usuarios que no están autorizados a ingresar a la red pueden obtener acceso a la transmisión, ya que la cobertura de la comunicación inalámbrica no requiere el acceso a una conexión física de los medios. Por lo tanto, la seguridad de la red es el componente principal de la administración de redes inalámbricas.

Seguridad y señales de medios inalámbricos



Tipos de redes inalámbricas

Los estándares de IEEE y de la industria de las telecomunicaciones sobre las comunicaciones inalámbricas de datos abarcan la capas física y de Enlace de datos. Los cuatro estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

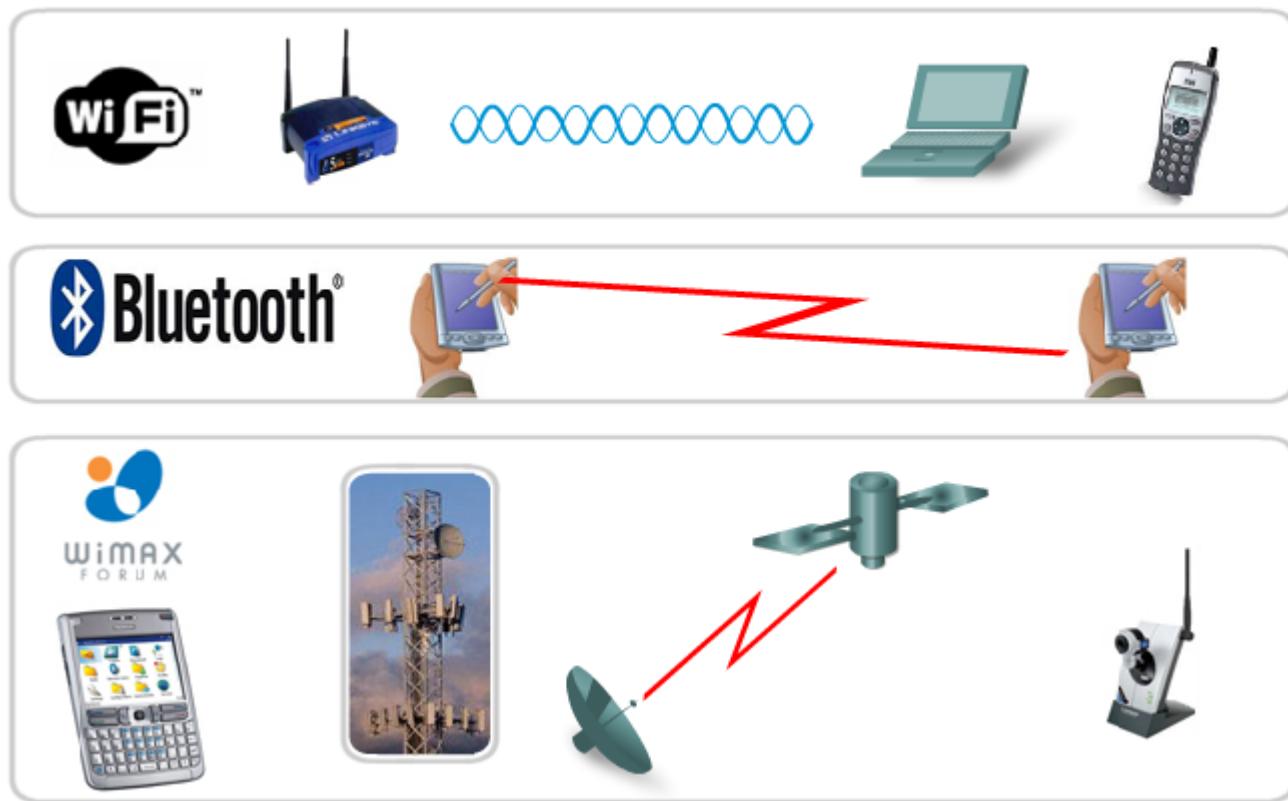
- IEEE estándar 802.11: Comúnmente denominada Wi-Fi, se trata de una tecnología LAN inalámbrica (Red de área local inalámbrica, WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de Acceso múltiple con detección de portadora/Prevención de colisiones (CSMA/CA).

- IEEE estándar 802.15: Red de área personal inalámbrica (WPAN) estándar, comúnmente denominada “Bluetooth”, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.
- IEEE estándar 802.16: Comúnmente conocida como WiMAX (Interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.
- Sistema global para comunicaciones móviles (GSM): Incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

Otros tipos de tecnologías inalámbricas, como las comunicaciones satelitales, ofrecen una conectividad de red de datos para ubicaciones sin contar con otros medios de conexión. Los protocolos, incluso GPRS, permiten la transferencia de datos entre estaciones terrestres y enlaces satelitales.

En cada uno de los ejemplos anteriores, las especificaciones de la capa física se aplican a áreas que incluyen: datos para la codificación de señales de radio, frecuencia y poder de transmisión, recepción de señales y requisitos decodificación y diseño y construcción de la antena.

Tipos y estándares de medios inalámbricos



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 (AP): 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 cobre, como Ethernet.

- Adaptadores NIC inalámbricos: Proporcionan capacidad de comunicación inalámbrica a cada host de la red.

A medida que la tecnología ha evolucionado, ha surgido una gran cantidad de estándares WLAN basados en Ethernet. Se debe tener precaución al comprar dispositivos inalámbricos para garantizar compatibilidad e interoperabilidad.

Los estándares incluyen:

IEEE 802.11a: opera en una banda de frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbps. Posee un área de cobertura menor y es menos efectivo al penetrar estructuras edilicias ya que opera en frecuencias superiores. Los dispositivos que operan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g descritos a continuación.

IEEE 802.11b: opera en una banda de frecuencia de 2.4 GHz y ofrece velocidades de hasta 11 Mbps. 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 una frecuencia de banda de 2.4 GHz y ofrece 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: el estándar IEEE 802.11n se encuentra actualmente en desarrollo. El estándar propuesto define la frecuencia de 2.4 Ghz o 5 GHz. La velocidad típica de transmisión de datos que se espera es de 100 Mbps a 210 Mbps con un alcance de distancia de hasta 70 metros.

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.

Estos estándares e implementaciones para las LAN inalámbricas se analizarán con más detalle en el curso Redes inalámbricas y comutación LAN.

Adaptadores y puntos de acceso de una WLAN



Punto de acceso
inalámbrico



Adaptadores
inalámbricos

8.3.8 Conectores de medios

Conectores comunes de medios de cobre

Los diferentes estándares de la capa física especifican el uso de distintos conectores. Estos estándares establecen las dimensiones mecánicas de los conectores y las propiedades eléctricas aceptables de cada tipo de implementación diferente en el cual se implementan.

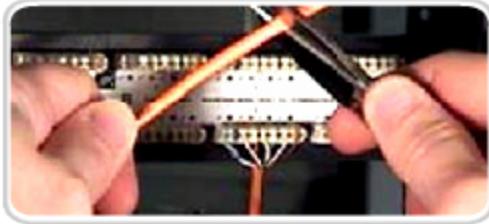
Si bien algunos conectores pueden parecer idénticos, éstos pueden conectarse de manera diferente según la especificación de la capa física para la cual fueron diseñados. El conector RJ-45 definido por ISO 8877 se utiliza para diferentes especificaciones de la capa física en las que se incluye Ethernet. Otra especificación, EIA-TIA 568, describe los códigos de color de los cables para colocar pines a las asignaciones (diagrama de pines) para el cable directo de Ethernet y para los cables de conexión cruzada.

Si bien muchos tipos de cables de cobre pueden comprarse prefabricados, en algunas situaciones, especialmente en instalaciones LAN, la terminación de los medios de cobre pueden realizarse en sitio. Estas terminaciones incluyen conexiones engarzadas para la terminación de medios Cat5 con tomas RJ-45 para fabricar patch cables y el uso de conexiones insertadas a presión en patch panels 110 y conectores RJ-45. La figura muestra algunos de los componentes de cableado de Ethernet.

Conectores de medios de cobre



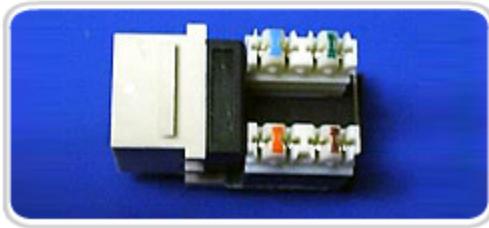
Bloque de inserción a presión 110



Conectores UTP RJ-45



Socket UTP RJ-45



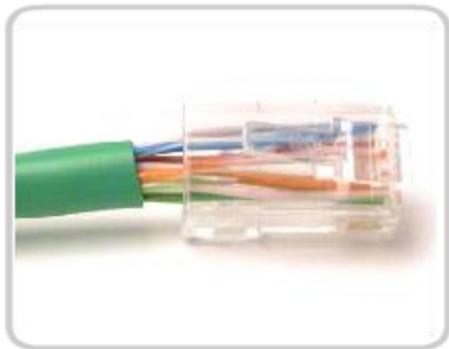
Terminación correcta del conector

Cada vez que se realiza la terminación de un cableado de cobre, existe la posibilidad de que se pierda la señal y de que se genere ruido en el circuito de comunicación. Las especificaciones de cableado de Ethernet en los lugares de trabajo establecen cuáles son los cables necesarios para conectar una computadora a un dispositivo intermedio de red activa. Cuando se realizan las terminaciones de manera incorrecta, cada cable representa una posible fuente de degradación

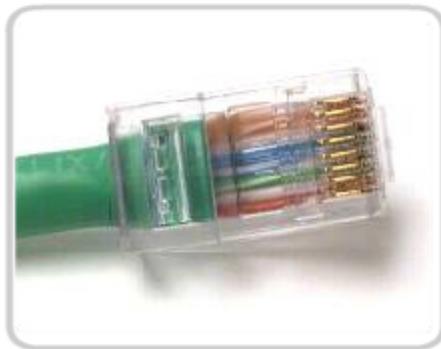
del funcionamiento de la capa física. **Es fundamental que todas las terminaciones de medios de cobre sean de calidad superior para garantizar un funcionamiento óptimo con tecnologías de red actuales y futuras.**

En algunos casos, como por ejemplo en las tecnologías WAN, si se utiliza un cable de terminación RJ-45-instalado incorrectamente, pueden producirse daños en los niveles de voltaje entre los dispositivos interconectados. Este tipo de daño generalmente ocurre cuando un cable se conecta para una tecnología de capa física y se utiliza con otra tecnología diferente.

Conectores de medios de cobre Terminación RJ-45



Conejor defectuoso: Los hilos están sin trenzar en un trecho demasiado largo.



Conejor correcto: Los hilos están sin trenzar sólo en el trecho necesario para unir el conector.

Conejores comunes de fibra óptica

Los conectores de fibra óptica incluyen varios tipos. La figura muestra algunos de los tipos más comunes:

Punta Recta (ST) (comercializado por AT&T): un conector muy común estilo Bayonet, ampliamente utilizado con fibra multimodo.

Conejor suscriptor (SC): conector que utiliza un mecanismo de doble efecto para asegurar la inserción positiva. Este tipo de conector se utiliza ampliamente con fibra monomodo.

Conejor Lucent (LC): un conector pequeño que está adquiriendo popularidad en su uso con fibra monomodo; también admite la fibra multimodo.

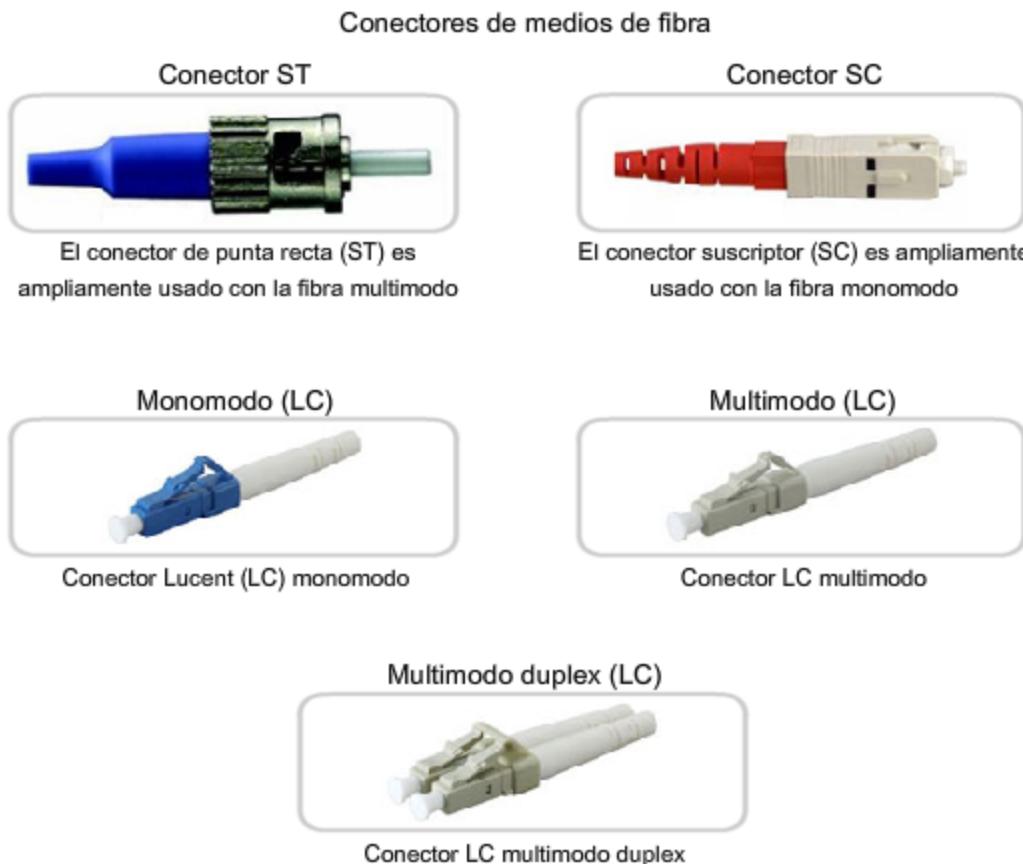
La terminación y el empalme del cableado de fibra óptica requiere de equipo y capacitación especiales. La terminación incorrecta de los medios de fibra óptica producen una disminución en las distancias de señalización o una falla total en la transmisión.

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 final: los extremos de los medios no se encuentran bien pulidos o puede verse suciedad en la terminación.

Se recomienda el uso de 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.

Se puede realizar una prueba de campo al emitir una luz brillante en un extremo de la fibra 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.



8.5 RESUMENES DEL CAPITULO

8.5.1 Resumen y revisión

La Capa 1 del modelo OSI es responsable de la interconexión física de los dispositivos. Los estándares de esta capa definen las características de la representación en frecuencias eléctricas, ópticas y radiofrecuencias de los bits que componen las tramas de la capa de Enlace de datos que se transmiten. Los valores de bit pueden representarse mediante impulsos electrónicos, impulsos de luz o cambios en las ondas de radio. Los protocolos de la capa física codifican los bits para la transmisión y los decodifican en el destino.

Los estándares de esta capa también son responsables de describir las características físicas, mecánicas y eléctricas de los conectores y medios físicos que interconectan los dispositivos de red.

Los diversos protocolos de la capa física y los medios poseen distintas capacidades para transportar datos. El ancho de banda de datos sin procesar es el límite máximo teórico de transmisión de bits. El rendimiento y la capacidad de transferencia útil son diferentes medidas de una transferencia de datos observada durante un período de tiempo determinado.

En este capítulo, aprendió que:

- Explicar la función que cumplen los servicios y protocolos de la capa Física al admitir la comunicación a través de redes de datos.
- Describir el objetivo de la codificación y señalización de la capa Física de la manera en que se utilizan en las redes.
- Describir la función de las señales utilizadas para representar bits a medida que se transporta un frame a través de medios locales.
- Identificar las características básicas de los medios de red inalámbricos, de fibra y de cobre.
- Describir los usos comunes de los medios de red inalámbricos, de fibra y de cobre.

9 – ETHERNET

9.0 INTRODUCCION DEL CAPITULO

9.0.1 Introducción del capítulo

Hasta este punto del curso, cada capítulo se concentró en las diferentes funciones de cada una de las capas de los modelos OSI y de protocolo TCP/IP, y en cómo se utilizan los protocolos para lograr la comunicación de red. Estos análisis hacen referencia constantemente a diversos protocolos clave (TCP, UDP e IP), ya que brindan las bases sobre cómo funcionan actualmente desde la red más pequeña hasta la red más grande, la Internet. Estos protocolos comprenden el stack de protocolos TCP/IP y, dado que la Internet se creó utilizando dichos protocolos, Ethernet es en la actualidad la tecnología LAN preponderante a nivel mundial.

El grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP de las capas superiores. Sin embargo, diversas organizaciones especializadas en ingeniería (IEEE, ANSI, ITU) o empresas privadas (protocolos propietarios) describen los protocolos y servicios funcionales de la capa de Enlace de datos y la capa física del modelo OSI. Dado que Ethernet se compone de estándares en estas capas inferiores, puede decirse que en términos generales se entiende mejor con referencia al modelo OSI. El modelo OSI separa las funcionalidades de la capa de Enlace de datos de direccionamiento, entrampado y acceso a los medios desde 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.

Objetivos de aprendizaje

Al completar este capítulo, podrá realizar lo siguiente:

- Describir la evolución de Ethernet.
- Explicar los campos de la trama de Ethernet.
- Describir la función y las características del método de control de acceso a los medios utilizado por el protocolo Ethernet.
- Describir las funciones de la capa física y de la capa de enlace de datos de Ethernet.
- Comparar y contrastar los hubs y switches de Ethernet.
- Explicar el Protocolo de resolución de direcciones (ARP).



Ethernet es la tecnología LAN predominante en uso hoy en día.

9.1 DESCRIPCION GENERAL DE ETHERNET

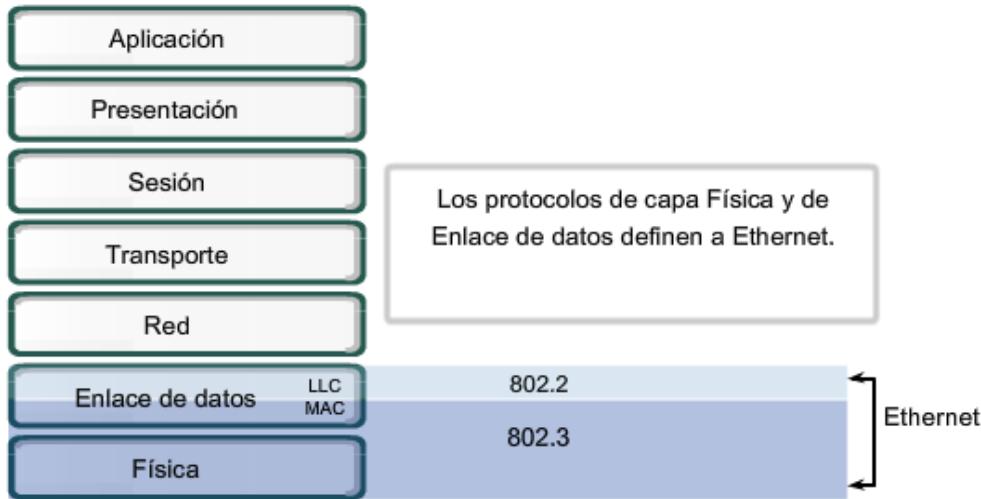
9.1.1 Ethernet: Estándares e implementación

Estándares de IEEE

La primera LAN (Red de área local) del mundo fue la versión original de Ethernet. Robert Metcalfe y sus compañeros de Xerox la diseñaron hace más de treinta años. El primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Corporation, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto. Los primeros productos que se desarrollaron a partir del estándar de Ethernet se vendieron a principios de la década de 1980.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO). Para garantizar la compatibilidad, los estándares IEEE 802.3 debían cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Ethernet opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos y la capa física.



9.1.2 Ethernet: Capa 1 y Capa 2

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Tal como lo muestra la figura, Ethernet en la Capa 2 se ocupa de estas limitaciones. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

Direcciones de la Capa 2 Limitaciones de la Capa 1

| Limitaciones de la Capa 1 | Funciones de la Capa 2 |
|--|--|
| No se puede comunicar con capas superiores | Se conecta con las capas superiores mediante control de enlace lógico (LLC) |
| No pueden identificar dispositivos | Utiliza esquemas de direccionamiento para identificar dispositivos |
| Sólo reconoce streams de bits | Utiliza tramas para organizar los bits en grupos |
| No puede determinar la fuente de la transmisión cuando transmiten múltiples dispositivos | Utiliza control de acceso al medio (MAC) para identificar fuentes de transmisión |

9.1.3 Control de enlace lógico: Conexión con las capas superiores

Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. 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. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

<http://standards.ieee.org/getieee802/download/802.2-1998.pdf>

<http://standards.ieee.org/regauth/llc/llctutorial.html>

http://www.wildpackets.com/support/compendium/reference/sap_numbers

Control de enlace lógico (LLC)

- Establece la conexión con las capas superiores
- Entrama el paquete de la capa de Red
- Identifica el protocolo de capa de Red
- Permanece relativamente independiente del equipo físico

Subcapa de control de enlace lógico

Control de acceso al medio 802.3

| Subcapa de señalización física | 10BASE5 (500m) 50 Ohm Coax N Style | 10BASE2 (185m) 50 Ohm Coax BNC | 10BASE-T (100m) 100 Ohm UTP RJ-45 | 100BASE-TX (100m) 100 Ohm UTP RJ-45 | 1000BASE-CX (25m) 150 Ohm STP mini-DB-9 | 1000BASE-T (100m) 100 Ohm UTP RJ-45 | 1000BASE-SX (220-550m) MM Fiber SC | 1000BASE-LX (550-5000m) MM or SM Fiber SC |
|--------------------------------|------------------------------------|--------------------------------|-----------------------------------|-------------------------------------|---|-------------------------------------|------------------------------------|---|
| Medio físico | | | | | | | | |

9.1.4 MAC: Envío de datos a los medios

El Control de acceso al medio (MAC) es la subcapa de Ethernet inferior de la capa de Enlace de datos. El hardware implementa el Control de acceso al medio, generalmente en la Tarjeta de interfaz de red (NIC).

La subcapa MAC de Ethernet tiene dos responsabilidades principales:

- Encapsulación de datos
- Control de Acceso al medio

Encapsulación de datos

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de trama
- Direccionamiento
- Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir una trama. Cuando forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de Capa 3. 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.

El proceso de entramado ofrece 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.

El proceso de encapsulación también posibilita el 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.

Una función adicional de la encapsulación de datos es la detección de errores. Cada trama de Ethernet contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos 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.

Control de acceso al medio

La subcapa MAC controla la colocación de tramas en los medios y el retiro de tramas de los medios. Como su nombre lo indica, se encarga de administrar el control de acceso al medio. Esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

Topología lógica

La topología lógica subyacente de Ethernet es un bus de multiacceso. Esto significa que todos los nodos (dispositivos) en ese segmento de la red comparten el medio. Esto significa además que todos los nodos de ese segmento reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Debido a que todos los nodos reciben todas las tramas, cada nodo debe determinar si debe aceptar y procesar una determinada trama. Esto requiere analizar el direccionamiento en la trama provisto por la dirección MAC.

Ethernet ofrece un método para determinar cómo comparten los nodos el acceso al medio. El método de control de acceso a los medios para Ethernet clásica es el Acceso múltiple con detección de portadora con detección de colisiones (CSMA/CD). Este método se describe más adelante en este capítulo.

<http://standards.ieee.org/regauth/groupmac/tutorial.html>

MAC—Llevar datos a los medios



9.1.5 Implementaciones físicas de Ethernet

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet. Desde su inicio en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. Cuando se introdujo el medio de fibra óptica, Ethernet se adaptó a esta nueva tecnología para aprovechar el mayor ancho de banda y el menor índice de error que ofrece la fibra. Actualmente, el mismo protocolo que transportaba datos a 3 Mbps puede transportar datos a 10 Gbps.

El éxito de Ethernet se debe a los siguientes factores:

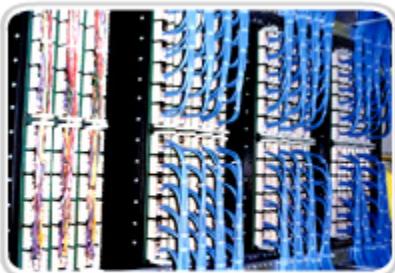
- Simplicidad y facilidad de mantenimiento
- Capacidad para incorporar nuevas tecnologías
- Confiabilidad
- Bajo costo de instalación y de actualización

La introducción de Gigabit Ethernet ha extendido la tecnología LAN original a distancias tales que convierten a Ethernet en un estándar de Red de área metropolitana (MAN) y de WAN (Red de área extensa).

Ya que se trata de una tecnología asociada con la capa física, Ethernet especifica e implementa los esquemas de codificación y decodificación que permiten el transporte de los bits de trama como señales a través de los medios. Los dispositivos Ethernet utilizan una gran variedad de especificaciones de cableado y conectores.

En las redes actuales, la Ethernet utiliza cables de cobre UTP y fibra óptica para interconectar dispositivos de red a través de dispositivos intermedios como hubs y switches. Dada la diversidad de tipos de medios que Ethernet admite, la estructura de la trama de Ethernet permanece constante a través de todas sus implementaciones físicas. Es por esta razón que puede evolucionar hasta cumplir con los requisitos de red actuales.

Dispositivos físicos que implementan Ethernet



Patch panels UTP en un bastidor



Switches Ethernet



Conectores de fibra Ethernet



Switch Ethernet

9.2 ETHERNET: COMUNICACIÓN A TRAVES DE LAN

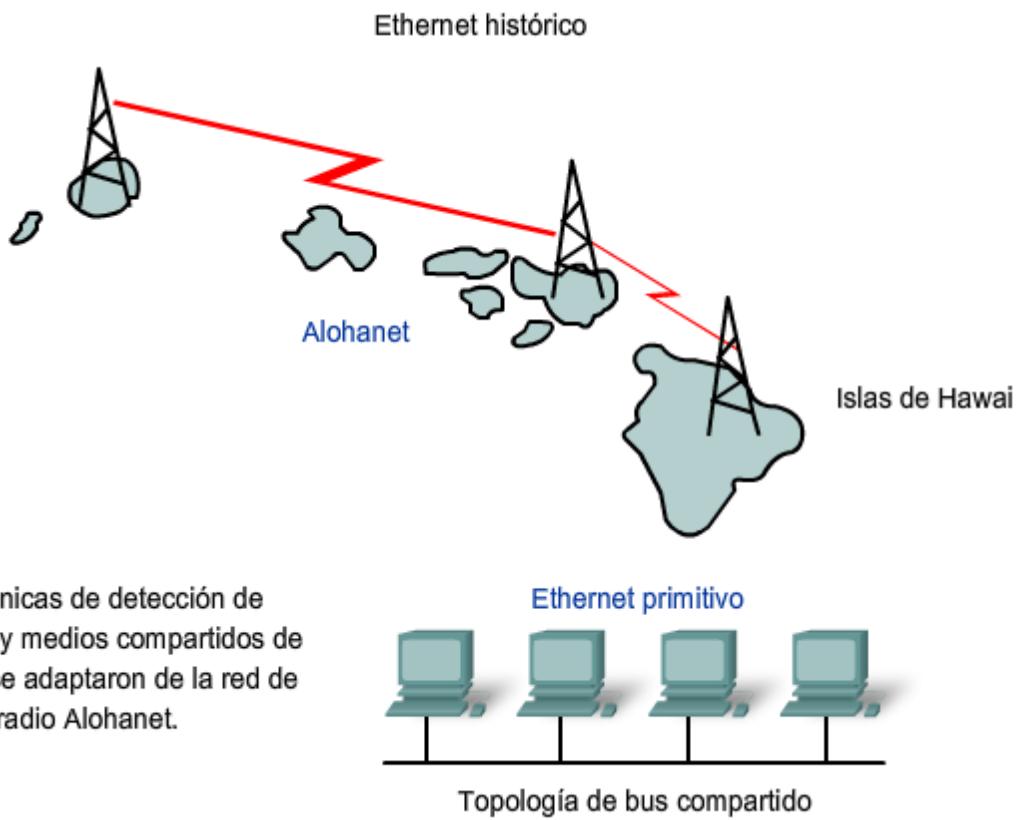
9.2.1 Ethernet histórica

Los cimientos de la tecnología Ethernet se fijaron por primera vez en 1970 mediante un programa llamado Alohanet. Alohanet era una red de radio digital diseñada para transmitir información por una frecuencia de radio compartida entre las Islas de Hawái.

Alohanet obligaba a todas las estaciones a seguir un protocolo según el cual una transmisión no reconocida requería una retransmisión después de un período de espera breve. Las técnicas para utilizar un medio compartido de esta manera se aplicaron posteriormente a la tecnología cableada en forma de Ethernet.

La Ethernet se diseñó para aceptar múltiples computadoras que se interconectaban en una topología de bus compartida.

La primera versión de Ethernet incorporaba un método de acceso al medio conocido como Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD). El CSMA/CD administraba los problemas que se originaban cuando múltiples dispositivos intentaban comunicarse en un medio físico compartido.



Primeros medios Ethernet

Las primeras versiones de Ethernet utilizaban cable coaxial para conectar computadoras en una topología de bus. Cada computadora se conectaba directamente al backbone. Estas primeras versiones de Ethernet se conocían como Thicknet (10BASE5) y Thinnet (10BASE2).

La 10BASE5, o Thicknet, utilizaba un cable coaxial grueso que permitía lograr distancias de cableado de hasta 500 metros antes de que la señal requiriera un repetidor. La 10BASE2, o Thinnet, utilizaba un cable coaxial fino que tenía un diámetro menor y era más flexible que la Thicknet y permitía alcanzar distancias de cableado de 185 metros.

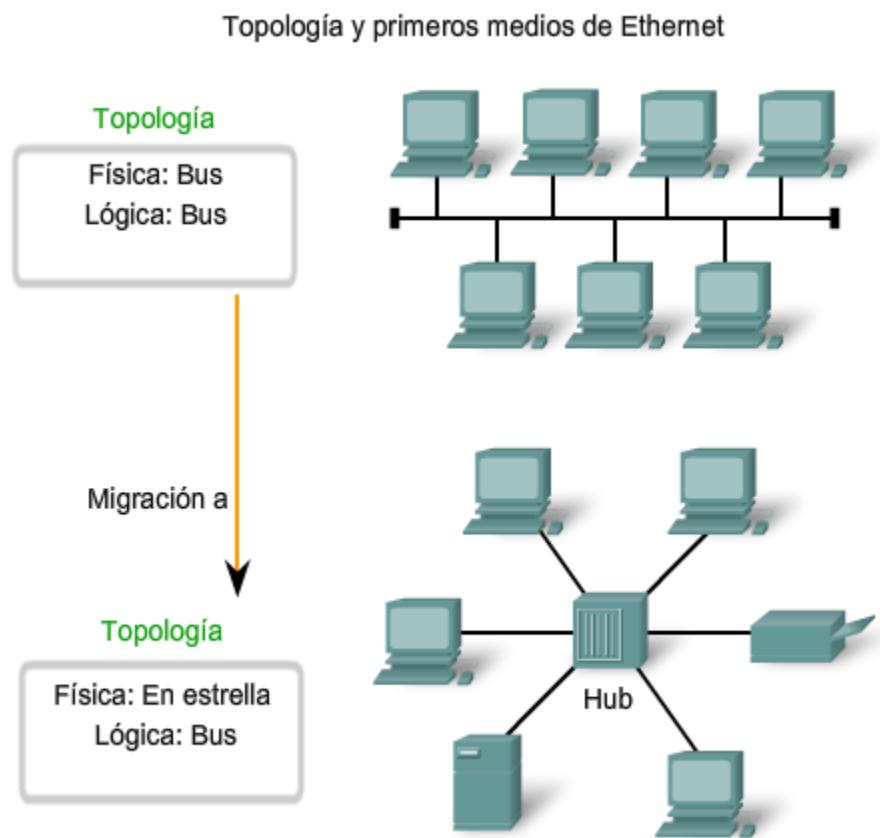
La capacidad de migrar la implementación original de Ethernet a las implementaciones de Ethernet actuales y futuras se basa en la estructura de la trama de Capa 2, que prácticamente no ha cambiado. Los medios físicos, el acceso al medio y el control del medio han evolucionado y continúan haciéndolo. Pero el encabezado y el tráiler de la trama de Ethernet han permanecido constantes en términos generales.

Las primeras implementaciones de Ethernet se utilizaron en entornos LAN de bajo ancho de banda en los que el acceso a los medios compartidos se administraba mediante CSMA y, posteriormente, mediante CSMA/CD. Además de ser una topología de bus lógica de la capa de Enlace de datos, Ethernet también utilizaba una topología de bus física. Esta topología se volvió más problemática a medida que las LAN crecieron y que los servicios LAN demandaron más infraestructura.

Los medios físicos originales de cable coaxial grueso y fino se reemplazaron por categorías iniciales de cables UTP. En comparación con los cables coaxiales, los cables UTP eran más fáciles de utilizar, más livianos y menos costosos.

La topología física también se cambió por una topología en estrella utilizando hubs. Los hubs concentran las conexiones. En otras palabras, toman un grupo de nodos y permiten que la red los trate como una sola unidad. Cuando una trama llega a un puerto, se lo copia a los demás puertos para que todos los segmentos de la LAN reciban la trama. La utilización

del hub en esta topología de bus aumentó la confiabilidad de la red, ya que permite que cualquier cable falle sin provocar una interrupción en toda la red. Sin embargo, la repetición de la trama a los demás puertos no solucionó el problema de las colisiones. Más adelante en este capítulo se verá cómo se manejaron las cuestiones relacionadas con colisiones en Ethernet mediante la introducción de switches en la red.



9.2.2 Administración de colisiones en Ethernet

Ethernet antigua

En redes 10BASE-T, el punto central del segmento de red era generalmente un hub. Esto creaba un medio compartido. Debido a que el medio era compartido, sólo una estación a la vez podía realizar una transmisión de manera exitosa. Este tipo de conexión se describe como comunicación half-duplex.

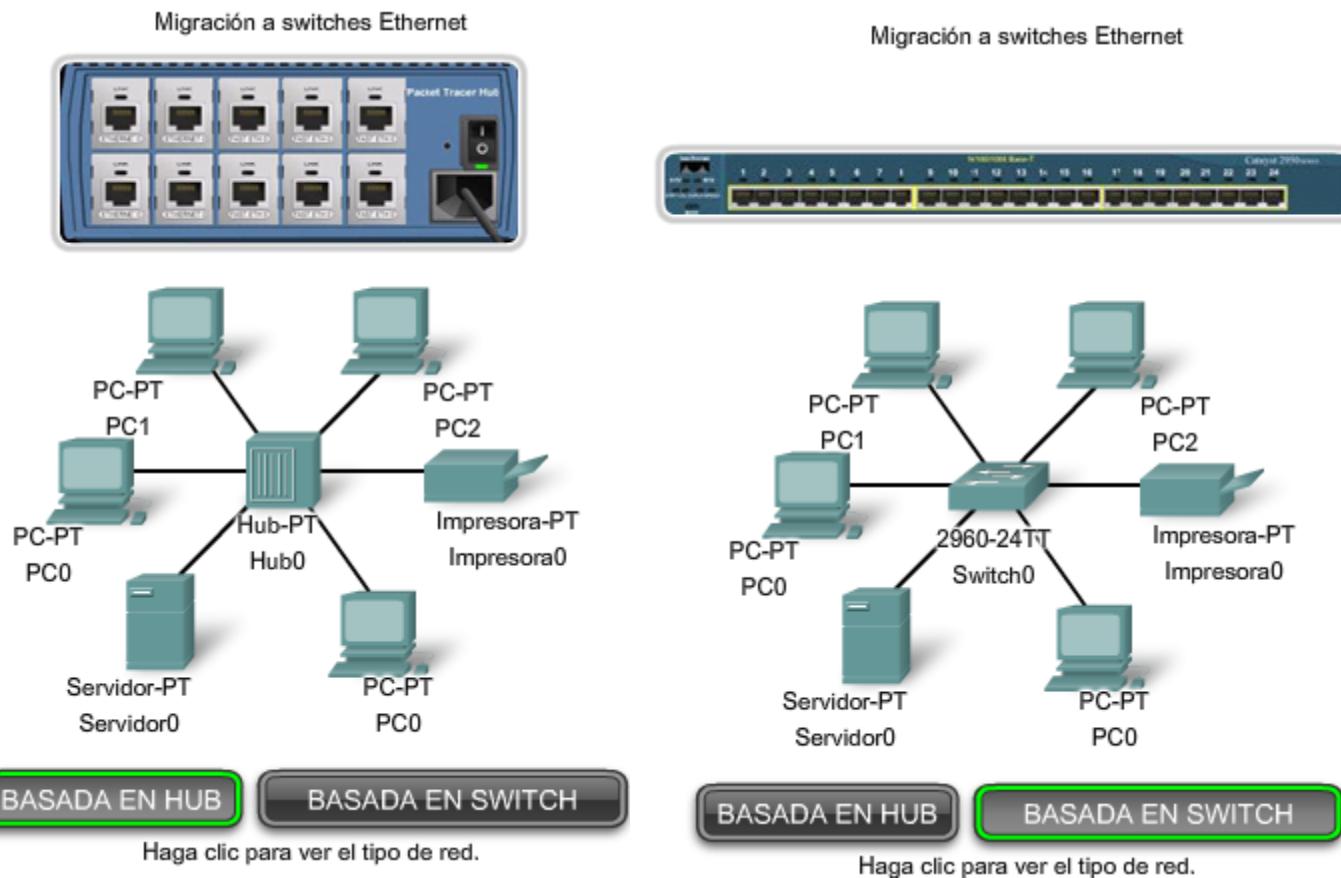
A medida que se agregaban más dispositivos a una red Ethernet, la cantidad de colisiones de tramas aumentaba notablemente. Durante los períodos de poca actividad de comunicación, las pocas colisiones que se producían se administraban mediante el CSMA/CD, con muy poco impacto en el rendimiento, en caso de que lo hubiera. Sin embargo, a medida que la cantidad de dispositivos y el consiguiente tráfico de datos aumenta, el incremento de las colisiones puede producir un impacto significativo en la experiencia del usuario.

A modo de analogía, sería similar a cuando salimos a trabajar o vamos a la escuela a la mañana temprano y las calles están relativamente vacías. Más tarde, cuando hay más automóviles en las calles, pueden producirse colisiones y generar demoras en el tráfico.

Ethernet actual

Un desarrollo importante que mejoró el rendimiento de la LAN fue la introducción de los switches para reemplazar los hubs en redes basadas en Ethernet. Este desarrollo estaba estrechamente relacionado con el desarrollo de Ethernet 100BASE-TX. Los switches pueden controlar el flujo de datos mediante el aislamiento de cada uno de los puertos y el envío de una trama sólo al destino correspondiente (en caso de que se lo conozca) en vez del envío de todas las tramas a todos los dispositivos.

El switch reduce la cantidad de dispositivos que recibe cada trama, lo que a su vez disminuye o minimiza la posibilidad de colisiones. Esto, junto con la posterior introducción de las comunicaciones full-duplex (que tienen una conexión que puede transportar señales transmitidas y recibidas al mismo tiempo), permitió el desarrollo de Ethernet de 1 Gbps y más.



9.3.2 Cambio a 1Gbps y más

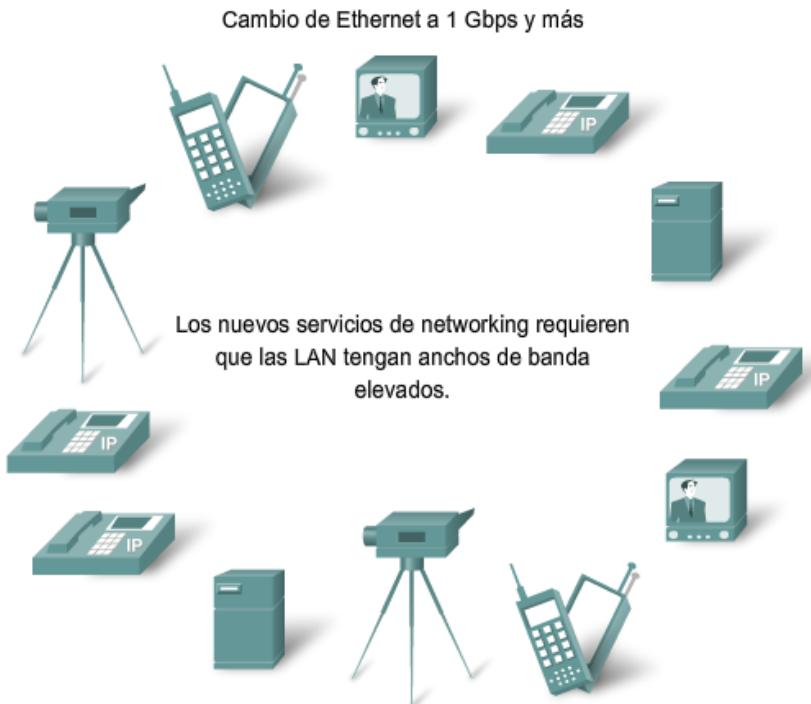
Las aplicaciones que atraviesan enlaces de red a diario ponen a prueba incluso a las redes más sólidas. Por ejemplo, el uso cada vez mayor de servicios de Voz sobre IP (VoIP) y multimedia requiere conexiones más rápidas que Ethernet de 100 Mbps.

Gigabit Ethernet se utiliza para describir las implementaciones de Ethernet que ofrecen un ancho de banda de 1000 Mbps (1 Gbps) o más. Esta capacidad se creó sobre la base de la capacidad full-duplex y las tecnologías de medios UTP y de fibra óptica de versiones anteriores de Ethernet.

El aumento del rendimiento de la red es significativo cuando la velocidad de transmisión (throughput) potencial aumenta de 100 Mbps a 1 Gbps y más.

La actualización a Ethernet de 1 Gbps no siempre implica que la infraestructura de red de cables y switches existente debe reemplazarse por completo. Algunos equipos y cableados de redes modernas bien diseñadas e instaladas podrían

trabajar a mayores velocidades con sólo una actualización mínima. Esta capacidad tiene el beneficio de reducir el costo total de propiedad de la red.

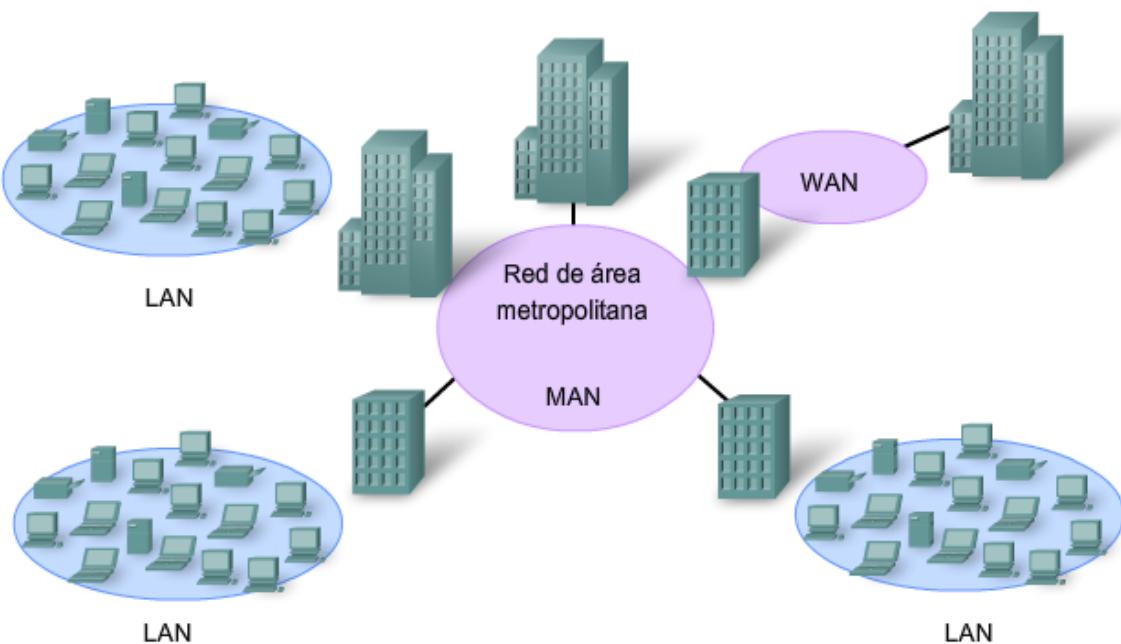


Ethernet más allá de la LAN

Las mayores distancias de cableado habilitadas por el uso de cables de fibra óptica en redes basadas en Ethernet disminuyeron las diferencias entre las LAN y las WAN. La Ethernet se limitaba originalmente a sistemas de cableado LAN dentro de un mismo edificio y después se extendió a sistemas entre edificios. Actualmente, puede aplicarse a través de toda una ciudad mediante lo que se conoce como Red de área metropolitana (MAN).

Ethernet Gigabit

La tecnología Ethernet Gigabit se aplica más allá de la LAN empresarial a las redes basadas en WAN y MAN.



9.3 LA TRAMA DE ETHERNET

9.3.1 La trama: Encapsulación del paquete

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 encabezado como el tráiler de Ethernet tienen varias secciones de información que el protocolo Ethernet utiliza. Cada sección de la trama se denomina campo. Hay dos estilos de tramas de Ethernet: el IEEE 802.3 (original) y el IEEE 802.3 revisado (Ethernet).

Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 (original) y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud, tal como se muestra en la figura.

Tamaño de la trama de Ethernet

El estándar Ethernet original definió 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. 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.

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.

Comparación del tamaño del campo y las estructuras de tramas de Ethernet y 802.3



Campos Preámbulo y Delimitador de inicio de trama

Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos de envío y de recepción. 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

El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. 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

El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama. Los switches también utilizan esta dirección para ampliar sus tablas de búsqueda. El rol de los switches se analizará más adelante en este capítulo.

Campo Longitud/Tipo

El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. En este campo debe ingresarse una longitud o un tipo. Sin embargo, sólo uno u otro podrá utilizarse en una determinada implementación. Si el objetivo del campo es designar un tipo, el campo Tipo describe qué protocolo se implementa.

El campo denominado Longitud/Tipo sólo aparecía como Longitud en las versiones anteriores del IEEE y sólo como Tipo en la versión DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que ambos usos eran comunes. El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. La Ethernet II es el formato de trama de Ethernet que se utiliza en redes TCP/IP. Cuando un nodo recibe una trama, debe analizar el campo Longitud/Tipo para determinar qué protocolo de capa superior está presente. Si el valor de los dos octetos es equivalente a 0x0600 hexadecimal o 1536 decimal o mayor que éstos, los contenidos del campo Datos se codifican según el protocolo indicado.

Campos Datos y Relleno

Los campos Datos y Relleno (de 46 a 1500 bytes) contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica o, con mayor frecuencia, un paquete Ipv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para aumentar el tamaño de la trama hasta alcanzar este tamaño mínimo.

Campos de trama Ethernet

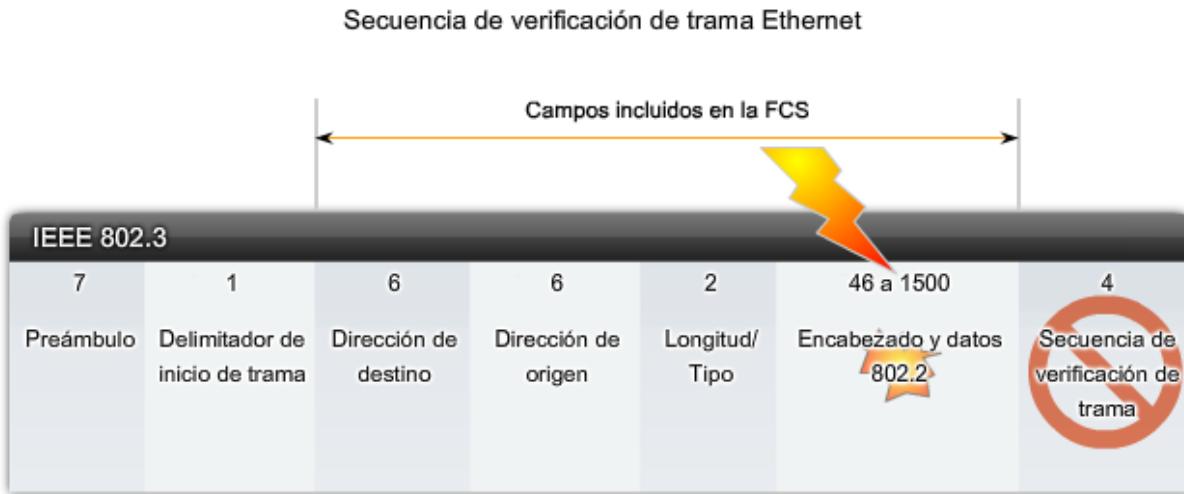
| IEEE 802.3 | | | | | | | |
|------------|--------------------------------|----------------------|---------------------|----------------|--------------------------|------------------------------------|--|
| 7 | 1 | 6 | 6 | 2 | 46 a 1500 | 4 | |
| Preámbulo | Delimitador de inicio de trama | Dirección de destino | Dirección de origen | Longitud/ Tipo | Encabezado y datos 802.2 | Secuencia de verificación de trama | |

| | |
|--|---|
| Preámbulo | Delimitador de inicio de trama |
| Preámbulo de trama de 7 bytes | Delimitador de inicio de trama de 1 byte |
| Dirección de destino | Dirección de origen |
| Dirección MAC de destino de 6 bytes | Dirección MAC de origen de 6 bytes |
| Longitud/Tipo | Encabezado y datos 802.2 |
| Tipo de protocolo encapsulado o longitud de trama de 2 bytes | Datos de 46 a 1500 bytes (paquete encapsulado) más relleno, de ser necesario. |
| Secuencia de verificación de trama | |
| Secuencia de verificación de trama de 4 bytes (checksum CRC) | |

Campo Secuencia de verificación de trama

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (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 detectar 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.



Si la FCS calculada por el receptor (basada en los contenidos de la trama recibida) no es igual a la FCS calculada por el origen (la cual está incluida en la trama), la trama se considera inválida y se la descarta.

9.3.2 La dirección MAC de Ethernet

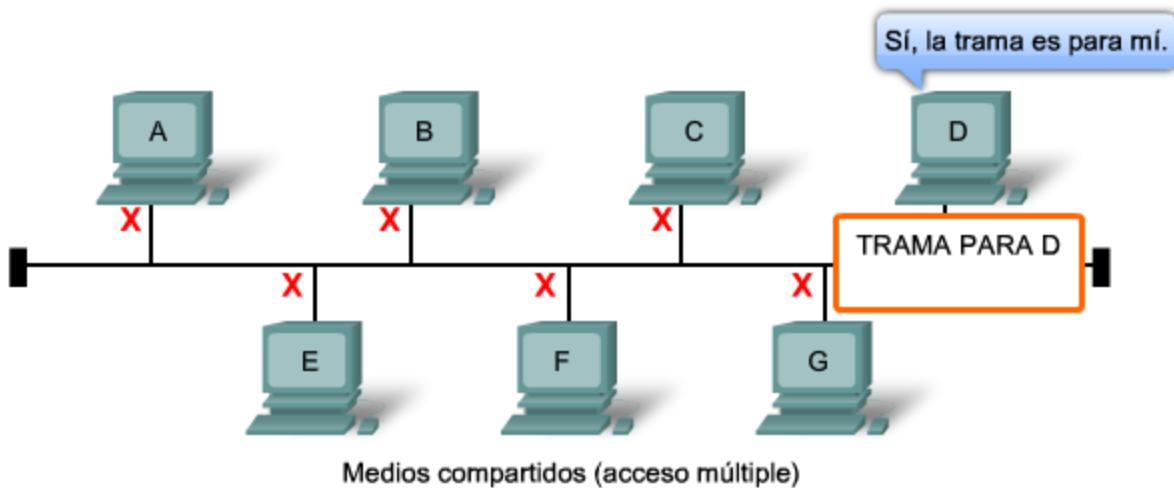
Inicialmente, la Ethernet se implementaba como parte de una topología de bus. Cada uno de los dispositivos de red se conectaba al mismo medio compartido. En redes con poco tráfico o pequeñas, ésta era una implementación aceptable. El problema más importante que debía resolverse era cómo identificar cada uno de los dispositivos. La señal podía

enviarse a todos los dispositivos, pero ¿cómo podía determinar cada uno de los dispositivos si era el receptor del mensaje?

Se creó un identificador único, denominado dirección de Control de acceso al medio (MAC), para ayudar a determinar las direcciones de origen y destino dentro de una red Ethernet. Independientemente de qué variedad de Ethernet se estaba utilizando, la convención de denominación brindó un método para identificar dispositivos en un nivel inferior del modelo OSI.

Como recordará, la dirección 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.

La dirección MAC— Direccionamiento en Ethernet



Todos los nodos Ethernet comparten los medios.

Para recibir los datos que se le enviaron, cada nodo necesita una dirección única.

Estructura de la dirección MAC

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 a cada proveedor un código de 3 bytes, denominado Identificador único organizacional (OUI).

El IEEE obliga a los proveedores a respetar dos normas simples:

- 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 a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) (código del fabricante o número de serie) en los últimos 3 bytes.

La dirección MAC se suele denominar dirección grabada (BIA) porque se encuentra grabada en la ROM (Memoria de sólo 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).

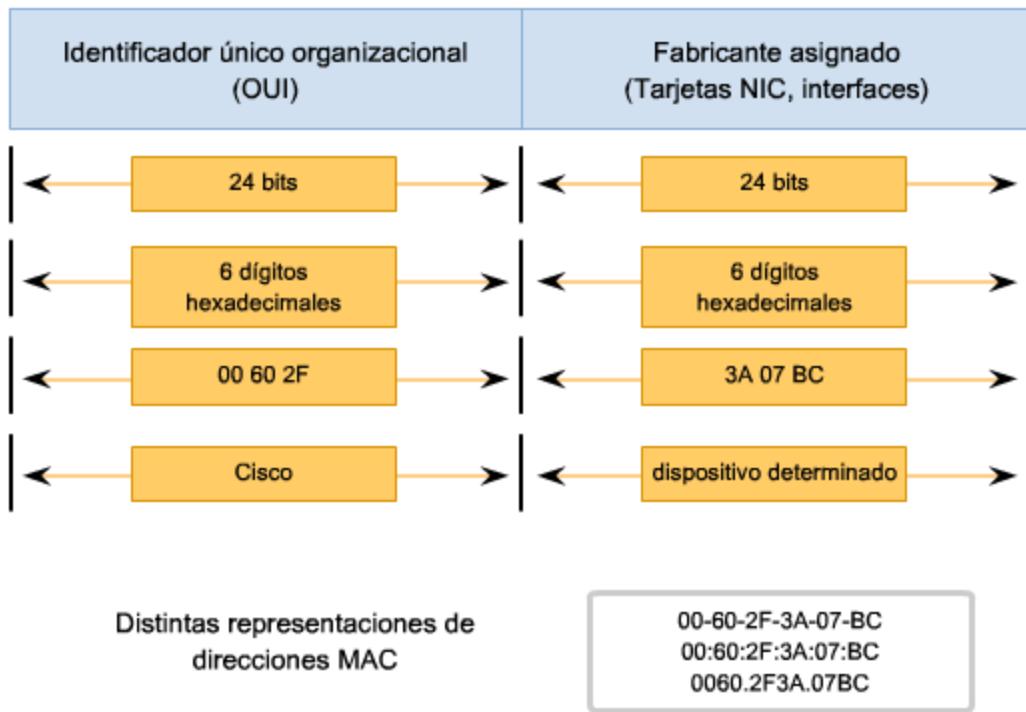
Sin embargo, cuando se inicia el equipo la NIC copia la dirección a la RAM (Memoria de acceso aleatorio). Cuando se examinan tramas se utiliza la dirección que se encuentra en la RAM como dirección de origen para compararla con la dirección de destino. La NIC utiliza la dirección MAC para determinar si un mensaje debe pasarse a las capas superiores para procesarlo.

Dispositivos de red

Cuando el dispositivo de origen reenvía el mensaje a una red Ethernet, se adjunta la información del encabezado dentro de la dirección MAC. El dispositivo de origen envía los datos a través de la red. Cada NIC de la red visualiza la información para determinar si la dirección MAC coincide con su dirección física. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino donde la MAC de la NIC coincide con la MAC de destino de la trama, la NIC pasa la trama hasta las capas OSI (Interconexión de sistema abierto), donde se lleva a cabo el proceso de desencapsulación.

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 00-05-9a-3C-78-00, 00:05:9a:3C:78:00 ó 0005.9a3C.7800. Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers (cualquier dispositivo que pueda originar o recibir datos en la red).

Estructura de la dirección MAC Ethernet



9.3.3 Numeración hexadecimal y direccionamiento

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. La figura muestra los valores decimales, binarios y hexadecimales equivalentes para los binarios 0000 hasta 1111. Nos resulta más conveniente expresar un valor como un único dígito hexadecimal que como cuatro bits.

Comprendión 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. 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.

Representación de valores hexadecimales

Nota: Es importante distinguir los valores hexadecimales de los valores decimales en cuanto a los caracteres del 0 al 9, tal como lo muestra la figura.

El valor hexadecimal se representa generalmente en texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un 16 en subíndice. Con menor frecuencia, puede estar seguido de una H, como 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. Ya hemos visto que los valores hexadecimales se utilizan en el panel Bytes de paquetes de Wireshark para representar los valores binarios dentro de tramas y paquetes.

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. La figura ilustra dichos patrones para valores seleccionados de 8 bits.

Números hexadecimales

| Equivalentes decimales y binarios del 0 al F hexadecimal | | | Equivalentes decimales, binarios y hexadecimales escogidos | | |
|--|---------|-------------|--|-----------|-------------|
| Decimal | Binario | Hexadecimal | Decimal | Binario | Hexadecimal |
| 0 | 0000 | 0 | 0 | 0000 0000 | 00 |
| 1 | 0001 | 1 | 1 | 0000 0001 | 01 |
| 2 | 0010 | 2 | 2 | 0000 0010 | 02 |
| 3 | 0011 | 3 | 3 | 0000 0011 | 03 |
| 4 | 0100 | 4 | 4 | 0000 0100 | 04 |
| 5 | 0101 | 5 | 5 | 0000 0101 | 05 |
| 6 | 0110 | 6 | 6 | 0000 0110 | 06 |
| 7 | 0111 | 7 | 7 | 0000 0111 | 07 |
| 8 | 1000 | 8 | 8 | 0000 1000 | 08 |
| 9 | 1001 | 9 | 10 | 0000 1010 | 0A |
| 10 | 1010 | A | 15 | 0000 1111 | 0F |
| 11 | 1011 | B | 16 | 0001 0000 | 10 |
| 12 | 1100 | C | 32 | 0010 0000 | 20 |
| 13 | 1101 | D | 64 | 0100 0000 | 40 |
| 14 | 1110 | E | 128 | 1000 0000 | 80 |
| 15 | 1111 | F | 192 | 1100 0000 | C0 |
| | | | 202 | 1100 1010 | CA |
| | | | 240 | 1111 0000 | F0 |
| | | | 255 | 1111 1111 | FF |

Visualización de la MAC

Una herramienta útil para analizar la dirección MAC de nuestra computadora es ipconfig /all o ifconfig. En el gráfico, observe la dirección MAC de esta computadora. Si el usuario tiene acceso, es posible que desee intentar esto en su equipo.

Quizás quiera buscar el OUI de la dirección MAC para determinar quién es el fabricante de su NIC.

```
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:\>
```

9.3.4 Otra Capa de direccionamiento

Capa de Enlace de datos

El direccionamiento físico de la capa de Enlace de datos (Capa 2) de OSI, implementado como dirección MAC de Ethernet, se utiliza para transportar la trama a través de los medios locales. Si bien brindan una dirección host única, las direcciones físicas no son jerárquicas. Estas direcciones se asocian a un dispositivo en particular, independientemente de su ubicación o de la red a la que esté conectado.

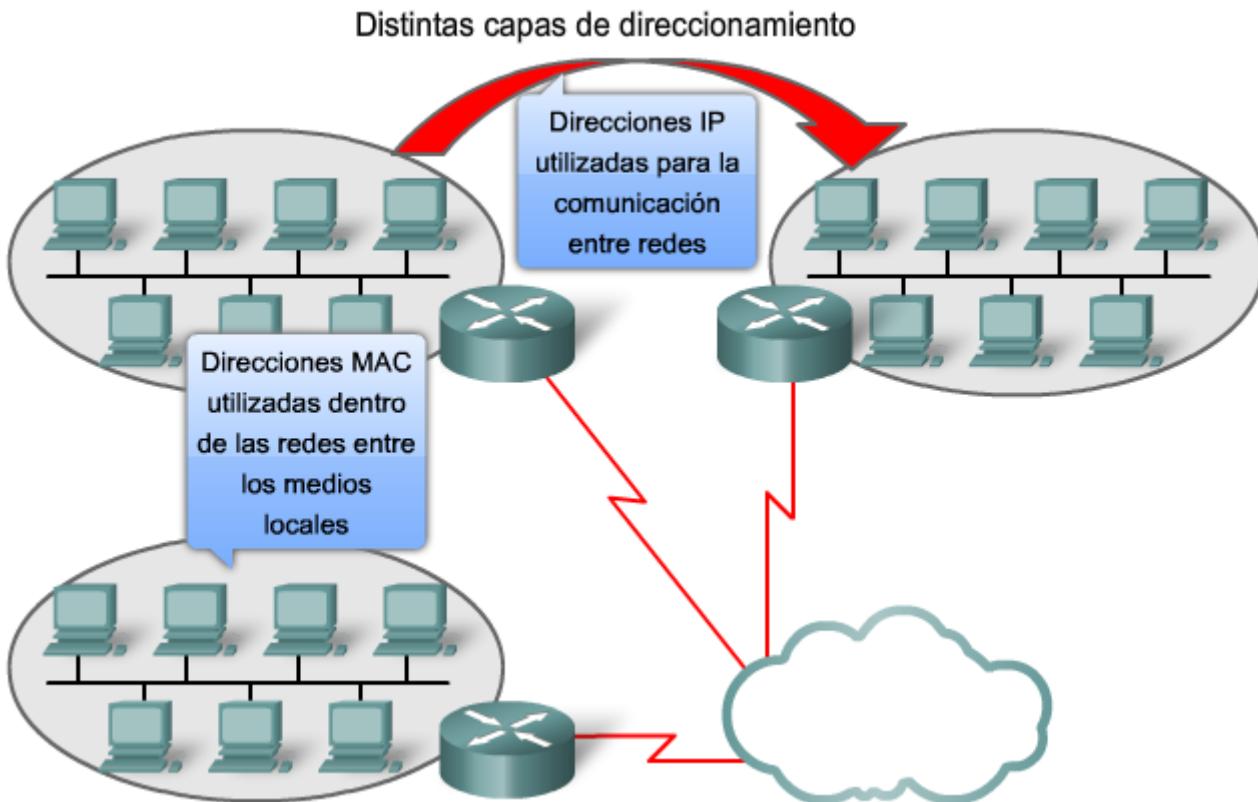
Estas direcciones de Capa 2 no tienen ningún significado fuera de los medios de la red local. Es posible que un paquete deba atravesar una serie de tecnologías de conexión de datos diferentes en redes locales y de área amplia antes de llegar a su destino. Por lo tanto, un dispositivo de origen no tiene conocimiento de la tecnología utilizada en redes intermedias y de destino o de sus direcciones de Capa 2 y estructuras de trama.

Capa de Red

Las direcciones de capa de Red (Capa 3), como por ejemplo, las direcciones Ipv4, brindan el direccionamiento general y local que se comprende tanto en el origen como en el destino. Para llegar a su último destino, un paquete transporta la dirección de destino de Capa 3 desde su origen. Sin embargo, debido a que diferentes protocolos de la capa de Enlace de datos la traman durante el trayecto, la dirección de Capa 2 que recibe cada vez se aplica sólo a esa porción local del trayecto y sus medios.

En resumen:

- La dirección de capa de red permite el envío del paquete a su destino.
- La dirección de capa de enlace de datos permite el transporte del paquete utilizando los medios locales a través de cada segmento.



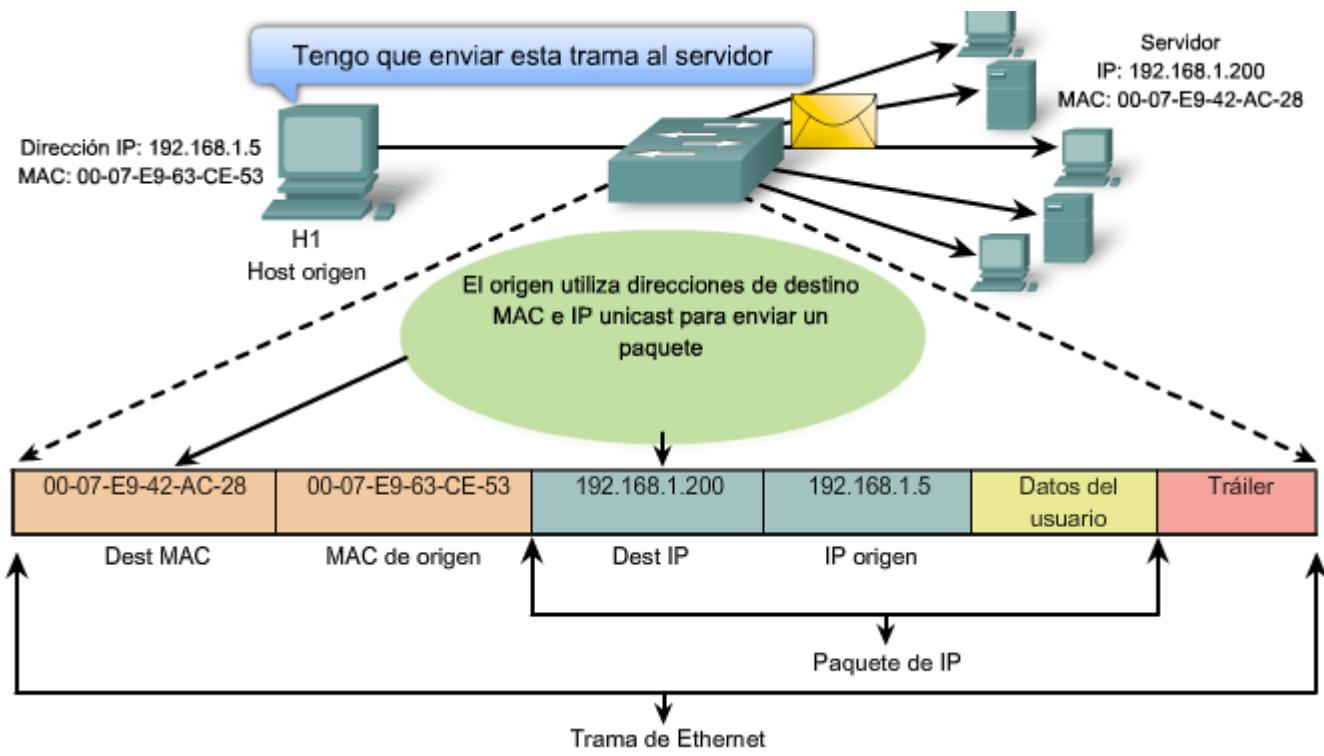
9.3.5 Ethernet unicast, multicast y broadcast

En Ethernet se utilizan distintas direcciones MAC para la capa 2: comunicaciones **unicast**, **multicast** y **broadcast**.

Unicast

Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.

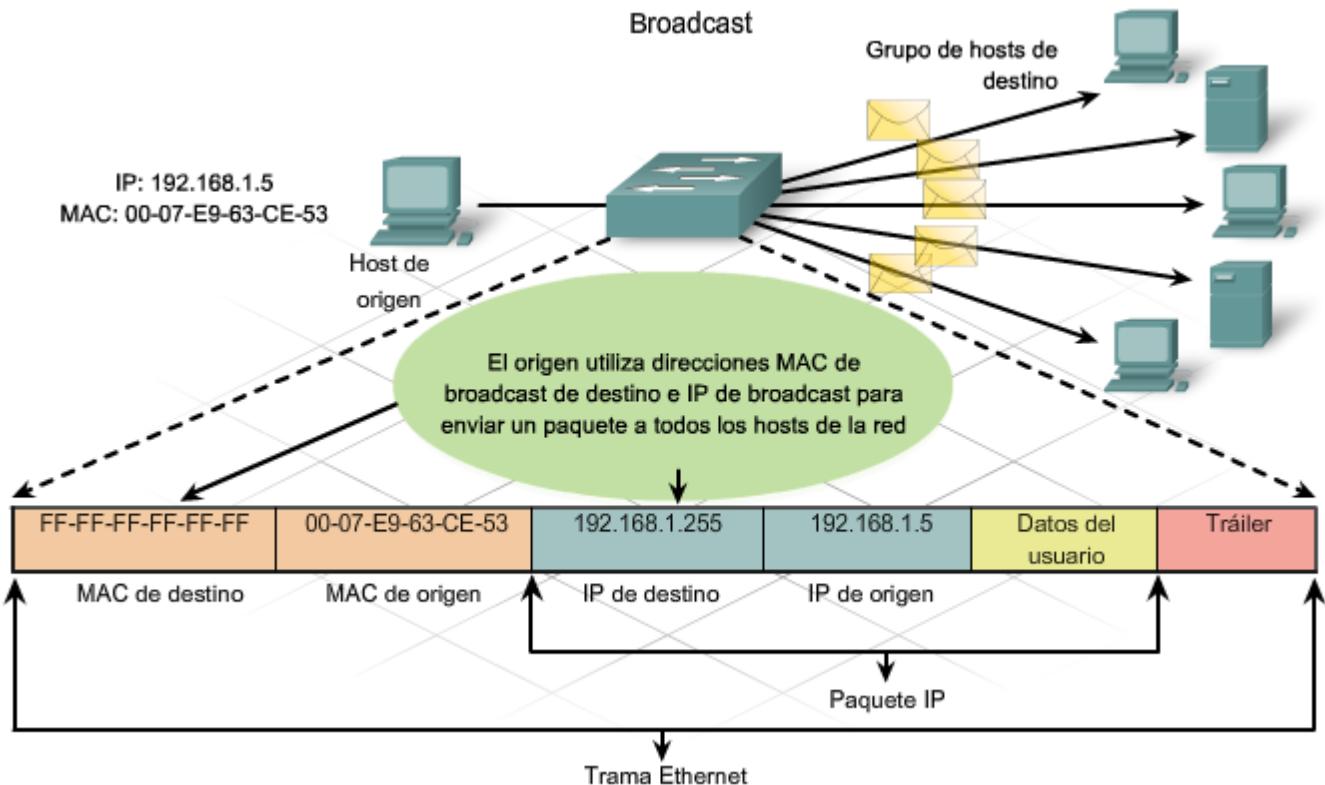
En el ejemplo que se muestra en la figura, un host con una dirección IP 192.168.1.5 (origen) solicita una página Web del servidor en la dirección IP 192.168.1.200. Para que se pueda enviar y recibir un paquete unicast, el encabezado del paquete IP debe contener una dirección IP de destino. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. La dirección IP y la dirección MAC se combinan para enviar datos a un host de destino específico.



Broadcast

Con broadcast, el paquete contiene una dirección IP de destino con todos unos (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. Una gran cantidad de protocolos de red utilizan broadcast, como el Protocolo de configuración dinámica de host (DHCP) y el Protocolo de resolución de direcciones (ARP). Más adelante en este capítulo se analizará cómo el ARP utiliza los broadcasts para asignar direcciones de Capa 2 a direcciones de Capa 3.

Tal como se muestra en la figura, una dirección IP de broadcast para una red necesita un dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.



Multicast

Recuerde que 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 intervalo de direcciones multicast es 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.

Ejemplos de dónde se utilizarían las direcciones multicast serían el juego remoto, en el que varios jugadores se conectan de manera remota pero juegan el mismo juego, y el aprendizaje a distancia a través de videoconferencia, en el que varios estudiantes se conectan a la misma clase.

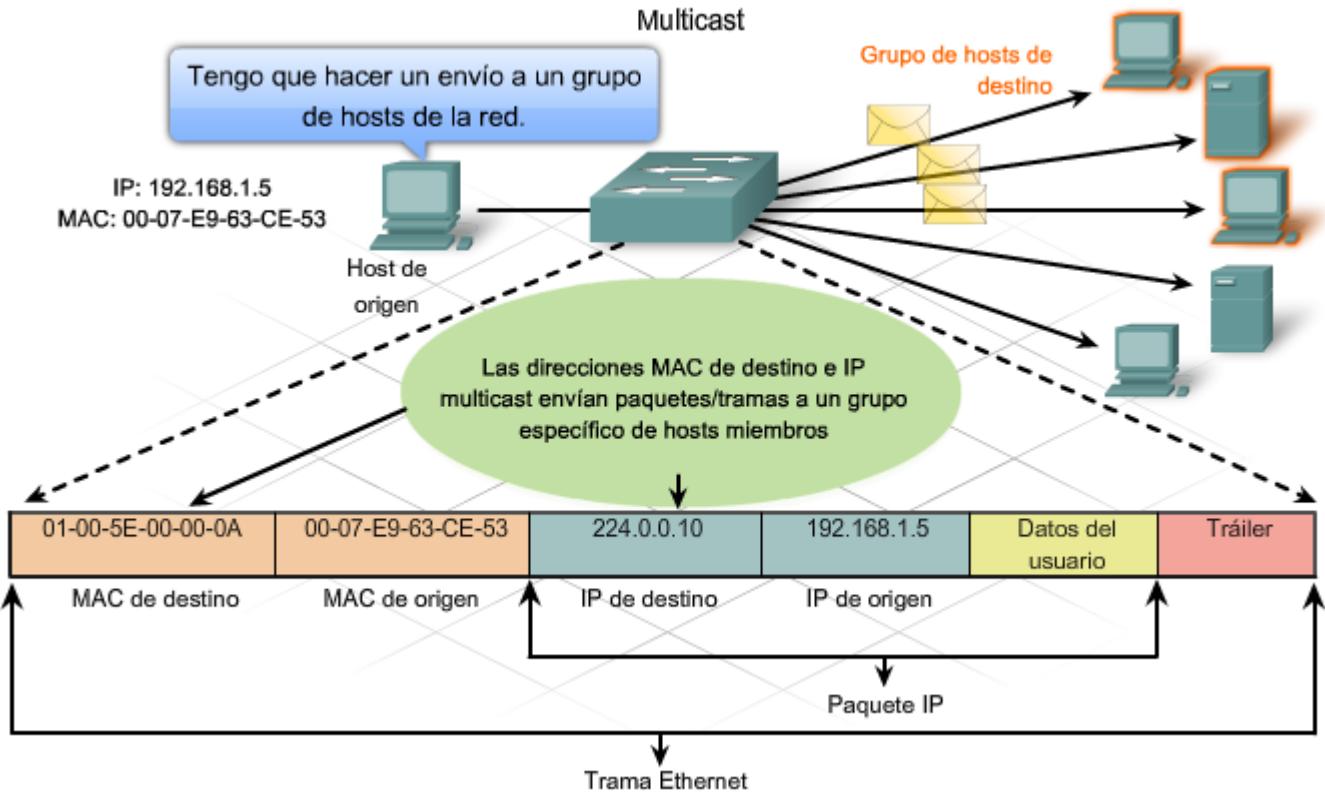
Al igual que con las direcciones unicast y de broadcast, la dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor termina con la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección de Ethernet. El bit restante en la dirección MAC es siempre “0”.

Un ejemplo, tal como se muestra en el gráfico, es el hexadecimal 01-00-5E-00-00-0A. Cada versión 342 hexadecimal es 4 bits binarios.

<http://www.iana.org/assignments/ethernet-numbers>

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v51/configuration/central/guide/51ipmul.html

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm



9.4 CONTROL DE ACCESO AL MEDIO EN ETHERNET

9.4.1 Control de acceso al medio en Ethernet

En un entorno de medios compartidos, todos los dispositivos tienen acceso garantizado al medio, pero no tienen ninguna prioridad en dicho medio. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse para que pueda continuar la comunicación.

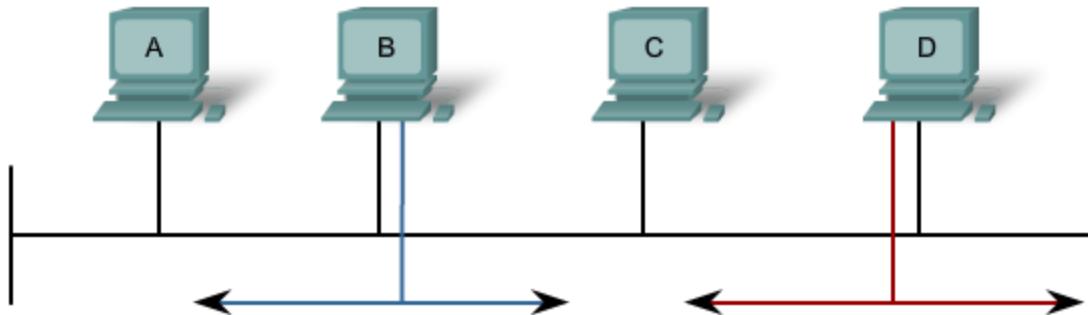
Las colisiones representan el precio que debe pagar la Ethernet para obtener el bajo gasto relacionado con cada transmisión.

La Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones y para administrar la reanudación de las comunicaciones.

Debido a que todas las computadoras que utilizan Ethernet envían sus mensajes en el mismo medio, se utiliza un esquema de coordinación distribuida (CSMA) para detectar la actividad eléctrica en el cable. Entonces, un dispositivo puede determinar cuándo puede transmitir. Cuando un dispositivo detecta que ninguna otra computadora está enviando una trama o una señal portadora, el dispositivo transmitirá en caso de que tenga algo para enviar.

Control de acceso al medio en Ethernet

Acceso múltiple por detección de portadora y
detección de colisiones (CSMA/CD)



CSMA/CD controla el acceso a los medios compartidos. Si hay una colisión, se detecta y las tramas se retransmiten.

9.4.2 CSMA/CD: El proceso

Detección de portadora

En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir.

Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN. Una vez que se envía el mensaje, el dispositivo regresa a su modo de escucha predeterminado.

Multiacceso

Si la distancia existente entre los dispositivos es tal que la latencia de las señales de un dispositivo denota que un segundo dispositivo no detecta las señales, el segundo dispositivo puede comenzar también a transmitir. Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren. En ese punto, las señales se mezclan y el mensaje se destruye. Si bien los mensajes se corrompen, la mezcla de señales restantes continúa propagándose a través de los medios.

Detección de colisiones

Cuando un dispositivo está en modo de escucha, puede detectar una colisión en el medio compartido. La detección de una colisión es posible porque todos los dispositivos pueden detectar un aumento de la amplitud de la señal por encima del nivel normal.

Una vez que se produce una colisión, los demás dispositivos que se encuentren en modo de escucha (como así también todos los dispositivos transmisores) detectarán el aumento de la amplitud de la señal. Una vez detectada la colisión,

todos los dispositivos transmisores continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.

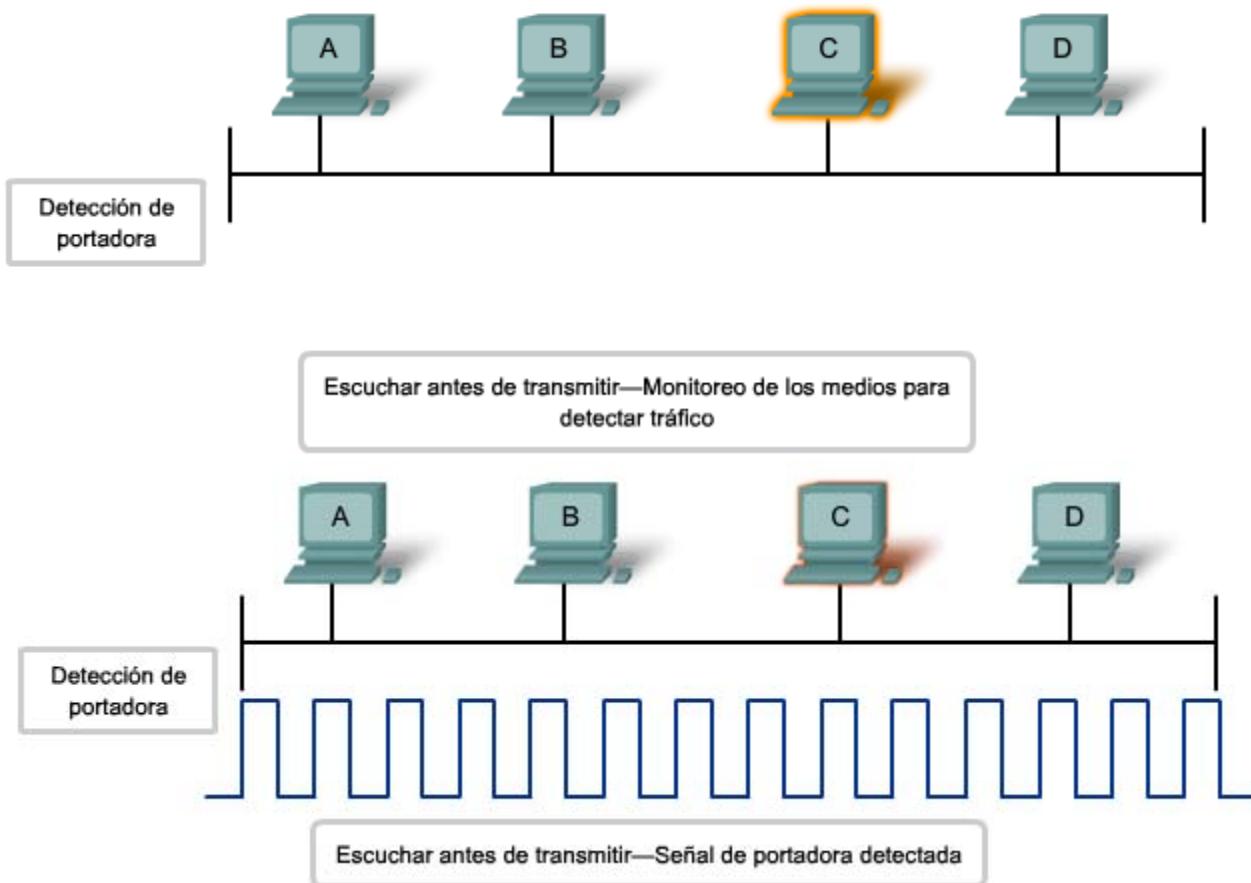
Señal de congestión y postergación aleatoria

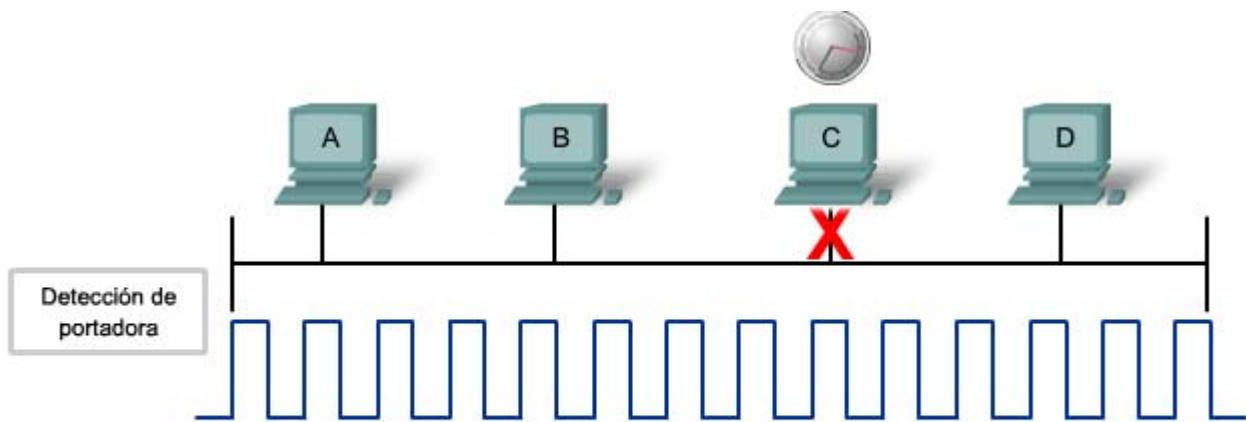
Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal interferente se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que éstos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo “escuchar antes de transmitir”. El período de postergación aleatoria garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, esto también significa que un tercer dispositivo puede transmitir antes de que cualquiera de los dos dispositivos involucrados en la colisión original tenga la oportunidad de volver a transmitir.

Control de acceso al medio en Ethernet

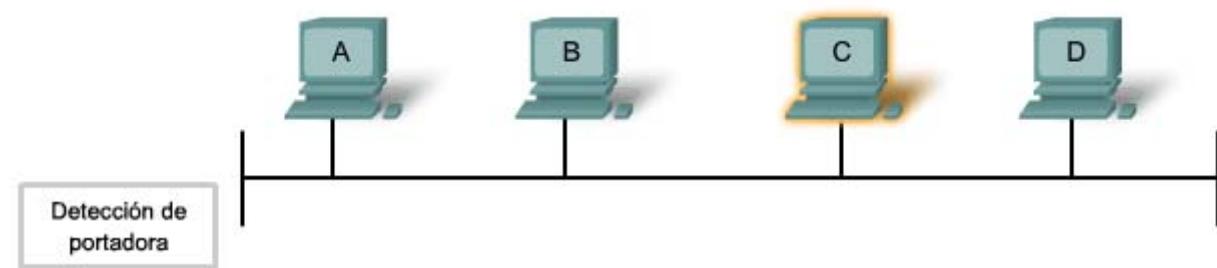
Acceso múltiple con detección de portadora con detección de portadora y detección de colisiones
(CSMA/CD)



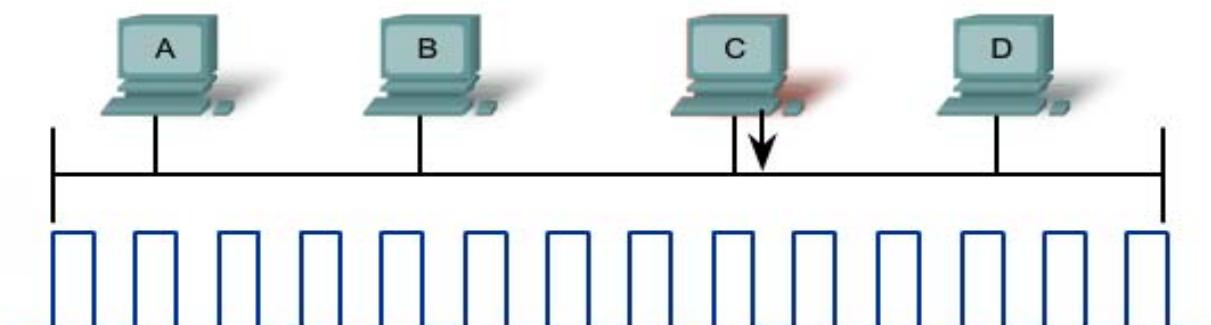


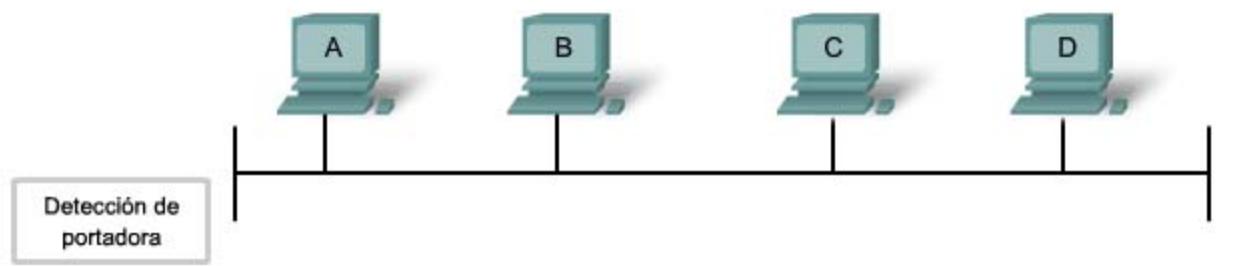
Espera durante un tiempo especificado luego de la señal pasa.

Intente de nuevo más tarde.

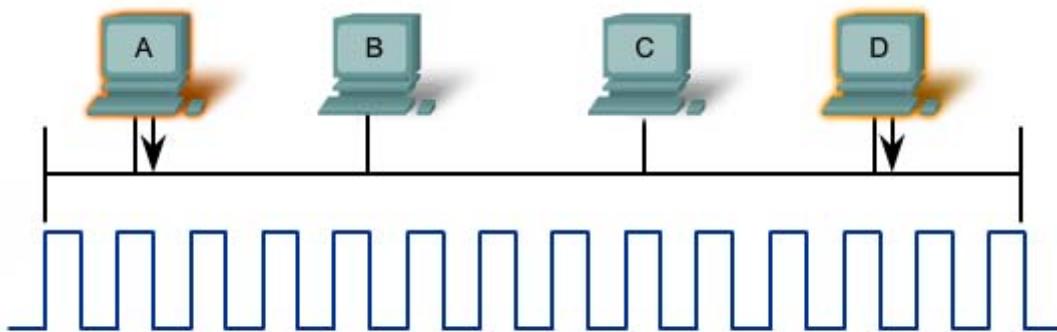


Escuchar antes de transmitir—Monitoreo de los medios para detectar tráfico





Escuchar antes de transmitir—Monitoreo de los medios para detectar tráfico



Colisión

Colisión

Se produce una colisión.

Detección de portadora

Temporizador de postergación—Intente de nuevo más tarde.

Hubs y dominios de colisiones

Dado que las colisiones se producirán ocasionalmente en cualquier topología de medios compartidos (incluso cuando se emplea CSMA/CD), debemos prestar atención a las condiciones que pueden originar un aumento de las colisiones.

Debido al rápido crecimiento de la Internet:

- Se conectan más dispositivos a la red.
- Los dispositivos acceden a los medios de la red con una mayor frecuencia.
- Aumentan las distancias entre los dispositivos.

Recuerde que los hubs fueron creados como dispositivos de red intermediarios que permiten a una mayor cantidad de nodos conectarse a los medios compartidos. Los hubs, que también se conocen como repetidores multipuerto, retransmiten las señales de datos recibidas a todos los dispositivos conectados, excepto a aquél desde el cual se reciben las señales. Los hubs no desempeñan funciones de red tales como dirigir los datos según las direcciones.

Los hubs y los repetidores son dispositivos intermediarios que extienden la distancia que pueden alcanzar los cables de Ethernet. Debido a que los hubs operan en la capa física, ocupándose únicamente de las señales en los medios, pueden producirse colisiones entre los dispositivos que conectan y dentro de los mismos hubs.

Además, la utilización de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones.

Tal como se muestra en la figura, la interconexión de los hubs forma una topología física que se denomina estrella extendida. La estrella extendida puede crear un dominio de colisiones notablemente expandido.

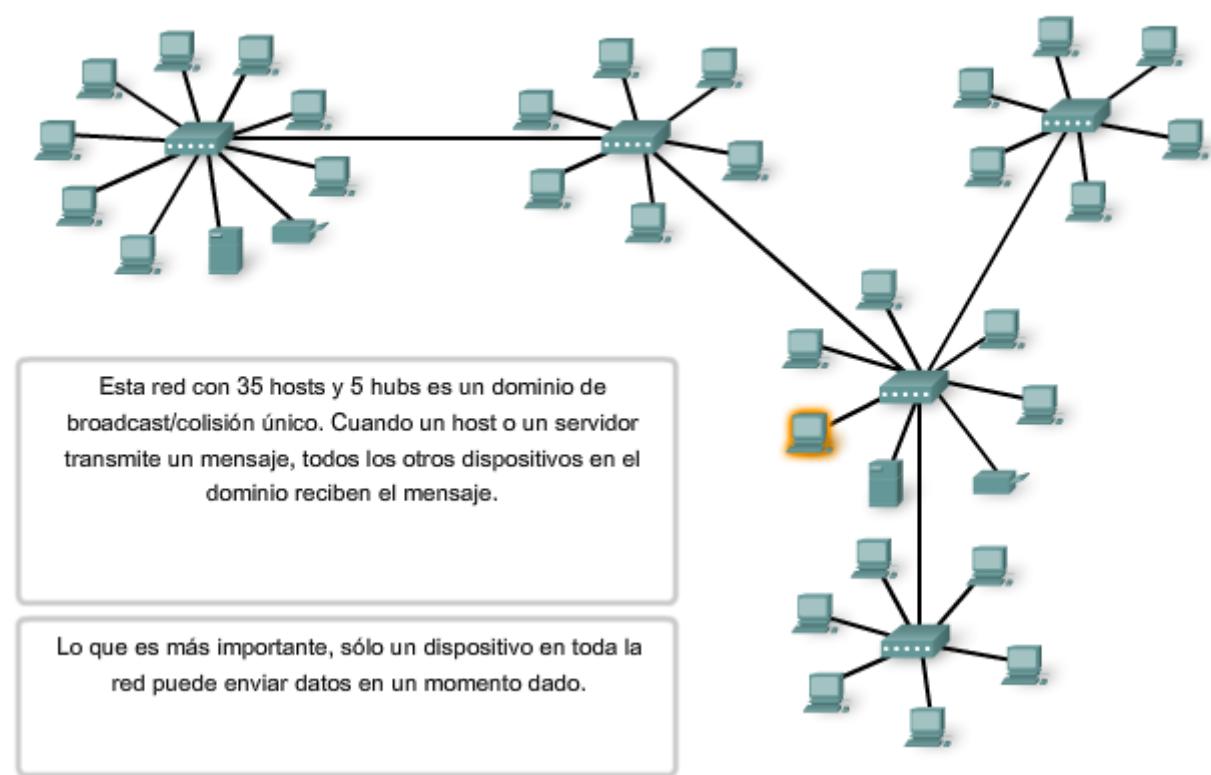
Un mayor número de colisiones reduce la eficiencia y la efectividad de la red hasta que las colisiones se convierten en una molestia para el usuario.

Si bien el CSMA/CD es un sistema de administración de colisiones de tramas, dicho sistema se diseñó para administrar colisiones sólo para una cantidad limitada de dispositivos y en redes con poco uso de red. Por lo tanto, se requiere de otros mecanismos cuando existen grandes cantidades de usuarios que quieren tener acceso y cuando se necesita un acceso a la red más activo.

Comprobaremos que la utilización de switches en lugar de hubs puede ser un comienzo para reducir este problema.

<http://standards.ieee.org/getieee802/802.3.html>

La utilización de hubs en topologías en estrella extendidas puede crear grandes dominios de colisión



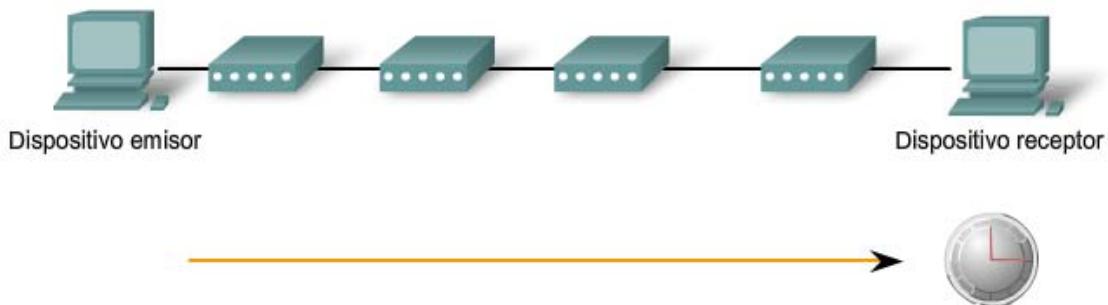
9.4.3 Temporización de Ethernet

Las implementaciones más rápidas de la capa física de Ethernet introducen complejidades en la administración de colisiones.

Latencia

Tal como se analizó anteriormente, cada dispositivo que deseé transmitir debe “escuchar” primero el medio para verificar la presencia de tráfico. Si no hay tráfico, la estación comenzará a transmitir de inmediato. La señal eléctrica que se transmite requiere una cantidad determinada de tiempo (latencia) para propagarse (viajar) a través del cable. Cada hub o repetidor en la ruta de la señal agrega latencia a medida que envía los bits desde un puerto al siguiente.

Este retardo acumulado aumenta la probabilidad de que se produzcan colisiones, porque un nodo de escucha puede transformarse en señales de transmisión mientras el hub o repetidor procesa el mensaje. Debido a que la señal no había alcanzado este nodo mientras estaba escuchando, dicho nodo pensó que el medio estaba disponible. Esta condición produce generalmente colisiones.



A una trama Ethernet le lleva un tiempo considerable trasladarse desde el dispositivo emisor hasta el receptor. Cada dispositivo intermedio contribuye a la latencia general.

Temporización y sincronización

En modo half-duplex, si no se produce una colisión, el dispositivo emisor transmitirá 64 bits de información de sincronización de temporización, lo que se conoce como el Preámbulo.

El dispositivo emisor transmitirá a continuación la trama completa.

La Ethernet con velocidades de transmisión (throughput) de 10 Mbps y menos es asíncrona. Una comunicación asíncrona en este contexto significa que cada dispositivo receptor utilizará los 8 bytes de información de temporización para sincronizar el circuito receptor con los datos entrantes y a continuación descartará los 8 bytes.

Las implementaciones de Ethernet con velocidades de transmisión (throughput) de 100 Mbps y más son síncronas. La comunicación síncrona en este contexto significa que la información de temporización no es necesaria. Sin embargo, por razones de compatibilidad, los campos Preámbulo y Delimitador de inicio de trama (SFD) todavía están presentes.

Sincronización de tramas para comunicaciones asíncronas

| Nombres de los campos | | | | |
|--------------------------|--------------------|---------------------|----------------|-----------|
| A | B | C | D | E |
| Campo de inicio de trama | Campo de dirección | Campo tipo/longitud | Campo de datos | Campo FCS |

Ethernet de 10 Mbps y más lenta usa los primeros 64 bits del preámbulo de la trama para sincronizar el receptor.

Tiempo de bit

Para cada velocidad de medios diferente se requiere un período de tiempo determinado para que un bit pueda colocarse y detectarse en el medio. Dicho período de tiempo se denomina tiempo de bit. En Ethernet de 10 Mbps, un bit en la capa MAC requiere de 100 nanosegundos (ns) para ser transmitido. A 100 Mbps, ese mismo bit requiere de 10 ns para ser transmitido. Y a 1000 Mbps, sólo se requiere 1 ns para transmitir un bit. A menudo, se utiliza una estimación aproximada de 20,3 centímetros (8 pulgadas) por nanosegundo para calcular el retardo de propagación en un cable UTP. El resultado es que para 100 metros de cable UTP se requiere un poco menos de 5 tiempos de bit para que una señal 10BASE-T recorra la longitud del cable.

Para que el CSMA/CD de Ethernet funcione, el dispositivo emisor debe detectar la colisión antes de que se haya completado la transmisión de una trama del tamaño mínimo. A 100 Mbps, la temporización del dispositivo apenas es capaz de funcionar con cables de 100 metros. A 1000 Mbps, ajustes especiales son necesarios porque se suele transmitir una trama completa del tamaño mínimo antes de que el primer bit alcance el extremo de los primeros 100 metros de cable UTP. Por este motivo, no se permite el modo half-duplex en la Ethernet de 10 Gigabits.

Estas consideraciones de temporización deben aplicarse al espacio entre las tramas y a los tiempos de postergación (ambos temas se analizan en la próxima sección) para asegurar que cuando un dispositivo transmite su próxima trama, se ha reducido al mínimo el riesgo de que se produzca una colisión.

Intervalo de tiempo

En Ethernet half-duplex, donde los datos sólo pueden viajar en una dirección a la vez, el intervalo de tiempo se convierte en un parámetro importante para determinar cuántos dispositivos pueden compartir una red. Para todas las velocidades de transmisión de Ethernet de o por debajo de 1000 Mbps, el estándar describe cómo una transmisión individual no puede ser menor que el intervalo de tiempo.

La determinación del intervalo de tiempo es una compensación entre la necesidad de reducir el impacto de la recuperación en caso de colisión (tiempos de postergación y retransmisión) y la necesidad de que las distancias de red sean lo suficientemente grandes como para adaptarse a tamaños razonables de red. El compromiso fue elegir un diámetro de red máximo (2500 metros aproximadamente) para después establecer la longitud mínima de una trama que fuera suficiente como para garantizar la detección de todas las peores colisiones.

El intervalo de tiempo para Ethernet de 10 y 100 Mbps es de 512 tiempos de bit o 64 octetos. El intervalo de tiempo para Ethernet de 1000 Mbps es de 4096 tiempos de bit o 512 octetos.

El intervalo de tiempo garantiza que si está por producirse una colisión, se detectará dentro de los primeros 512 bits (4096 para Gigabit Ethernet) de la transmisión de la trama. Esto simplifica el manejo de las retransmisiones de tramas posteriores a una colisión.

El intervalo de tiempo es un parámetro importante por las siguientes razones:

- El intervalo de tiempo de 512 bits establece el tamaño mínimo de una trama de Ethernet en 64 bytes. 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 intervalo de tiempo determina un límite para el tamaño máximo de los segmentos de una red. Si la red crece demasiado, pueden producirse colisiones tardías. La colisiones tardías se consideran una falla en la red, porque un dispositivo detecta la colisión demasiado tarde durante la transmisión de tramas y será manejada automáticamente mediante CSMA/CD.

El intervalo de tiempo se calcula teniendo en cuenta las longitudes máximas de cables en la arquitectura de red legal de mayor tamaño. Todos los tiempos de retardo de propagación del hardware se encuentran al máximo permisible y se utiliza una señal de congestión de 32 bits cuando se detectan colisiones.

El intervalo de tiempo real calculado es apenas mayor que la cantidad de tiempo teórica necesaria para realizar una transmisión entre los puntos de máxima separación de un dominio de colisión, colisionar con otra transmisión en el último instante posible y luego permitir que los fragmentos de la colisión regresen a la estación transmisora y sean detectados. Ver la figura.

Para que el sistema funcione correctamente, el primer dispositivo debe estar al tanto de la colisión antes de que termine de enviar la trama legal de menor tamaño.

Para que una Ethernet de 1000 Mbps pueda operar en modo half-duplex, se agregó a la trama el campo de extensión cuando se envían tramas pequeñas, con el sólo fin de mantener ocupado al transmisor durante el tiempo que sea necesario para que vuelva un fragmento de colisión. Este campo sólo se incluye en los enlaces en half-duplex de 1000 Mbps y permite que las tramas de menor tamaño duren el tiempo suficiente para satisfacer los requisitos del intervalo de tiempo. El dispositivo receptor descarta los bits de extensión.

9.4.4 Espacio entre tramas y postergación

Espacio entre tramas

Los estándares de Ethernet requieren un espacio mínimo entre dos tramas que no hayan sufrido una colisión. Esto le otorga al medio tiempo para estabilizarse antes de la transmisión de la trama anterior y tiempo a los dispositivos para que procesen la trama. Este tiempo, llamado espacio entre tramas, se mide desde el último bit del campo FCS de una trama hasta el primer bit del Preámbulo de la próxima trama.

Una vez enviada la trama, todos los dispositivos de una red Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier dispositivo pueda transmitir la siguiente trama. En versiones de Ethernet más veloces, el espacio sigue siendo el mismo, 96 tiempos de bit, pero el tiempo del espacio entre tramas se vuelve proporcionalmente más corto.

Los retardos de sincronización entre dispositivos pueden ocasionar la pérdida de algunos de los bits del preámbulo de la trama. A su vez, esto puede producir una reducción mínima del espacio entre tramas cuando los hubs y repetidores regeneran los 64 bits completos de la información de temporización (el Preámbulo y el SFD) al comienzo de cada trama que se reenvía. En Ethernet de mayor velocidad, algunos dispositivos sensibles al tiempo podrían eventualmente no reconocer las tramas individuales lo que originaría una falla de comunicación.

Separación entre tramas Ethernet

| Velocidad | Separación entre tramas | Tiempo necesario |
|-----------|-------------------------|------------------|
| 10 Mbps | 96 tiempo de bit | 9,6 µs |
| 100 Mbps | 96 tiempo de bit | 0,96 µs |
| 1 Gbps | 96 tiempo de bit | 0,096 µs |
| 10 Gbps | 96 tiempo de bit | 0,0096 µs |

El tiempo entre tramas se reduce a medida que aumenta la velocidad de Ethernet



Señal de congestión

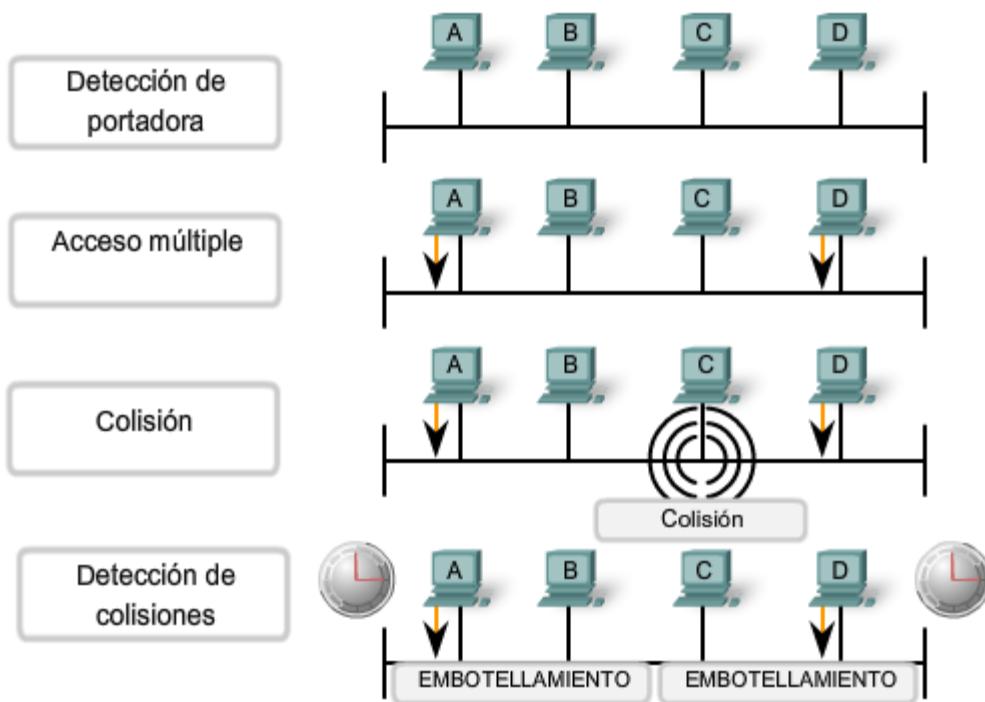
Como recordará, la Ethernet permite que los dispositivos compitan para el tiempo de transmisión. En caso de que dos dispositivos transmitan simultáneamente, el CSMA/CD de la red intenta resolver el problema. Sin embargo, recuerde que cuando se agrega un mayor número de dispositivos a la red, es posible que las colisiones sean cada vez más difíciles de resolver.

Tan pronto como se detecta una colisión, los dispositivos transmisores envían una señal de congestión de 32 bits que la impone. Esto garantiza que todos los dispositivos de la LAN detectarán la colisión.

Es importante que la señal de congestión no se detecte como una trama válida; de lo contrario, no podría identificarse la colisión. El patrón de datos que se observa con mayor frecuencia para una señal de congestión es simplemente un patrón de 1, 0, 1, 0 que se repite, al igual que el Preámbulo.

Los mensajes corrompidos, transmitidos de forma parcial, generalmente se conocen como fragmentos de colisión o runts. Las colisiones normales tienen menos de 64 octetos de longitud y, por lo tanto, reproban tanto la prueba de longitud mínima como la FCS, lo que facilita su identificación.

Las estaciones que detectan una colisión envían una señal de embotellamiento.



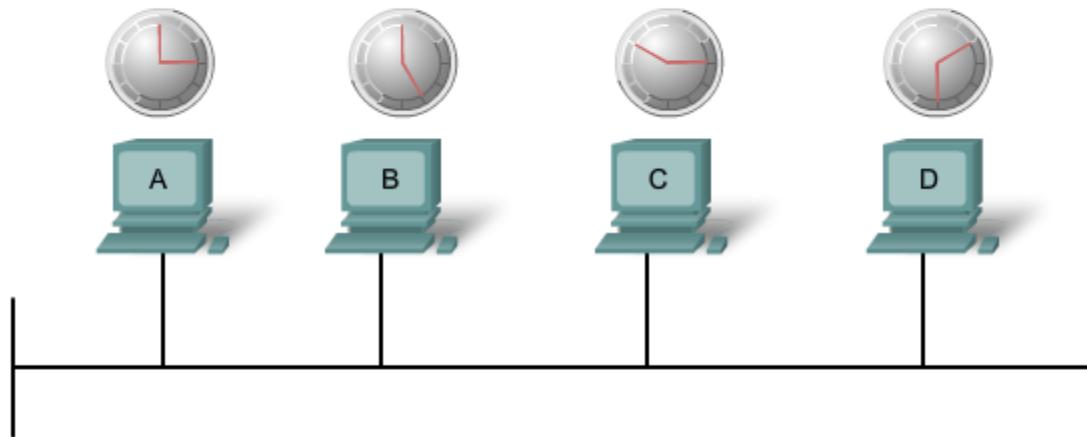
Temporización de postergación

Una vez producida la colisión y que todos los dispositivos permitan que el cable quede inactivo (cada uno espera que se cumpla el espacio completo entre tramas), los dispositivos cuyas transmisiones sufrieron la colisión deben esperar un período adicional, y cada vez potencialmente mayor, antes de intentar la retransmisión de la trama que sufrió la colisión. El período de espera está intencionalmente diseñado para que sea aleatorio de modo que dos estaciones no demoren la misma cantidad de tiempo antes de efectuar la retransmisión, lo que causaría colisiones adicionales. Esto se logra en parte al aumentar el intervalo a partir del cual se selecciona el tiempo de retransmisión aleatorio cada vez que se efectúa un intento de retransmisión. El período de espera se mide en incrementos del intervalo de tiempo del parámetro.

Si la congestión en los medios provoca que la capa MAC no pueda enviar la trama después de 16 intentos, abandona el intento y genera un error en la capa de Red. Este tipo de sucesos es raro en una red que funciona correctamente y sólo sucedería en el caso de cargas de red extremadamente pesadas o cuando se produce un problema físico en la red.

Los métodos descriptos en esta sección permitían a Ethernet proporcionar un servicio superior en una topología de medios compartidos basándose en el uso de hubs. En la sección de switches que aparece a continuación, veremos cómo, mediante el uso de switches, la necesidad de utilizar el CSMA/CD comienza a disminuir o, en algunos casos, a desaparecer por completo.

Temporización de postergación



Una vez que se recibe una señal de embottellamiento, todas las estaciones dejan de transmitir y cada una espera un periodo de tiempo aleatorio—establecido por el temporizador de postergación—antes de intentar enviar otra trama.

9.5 CAPA FÍSICA DE ETHERNET

9.5.1 Descripción general de la capa física de Ethernet

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física, generalmente denominada Ethernet PHY.

La Ethernet se rige por los estándares IEEE 802.3. Actualmente, se definen cuatro velocidades de datos para el funcionamiento con cables de fibra óptica y de par trenzado:

- 10 Mbps – Ethernet 10Base-T
- 100 Mbps – Fast Ethernet
- 1000 Mbps – Gigabit Ethernet
- 10 Gbps – 10 Gigabit Ethernet

Si bien existe una gran cantidad de implementaciones de Ethernet diferentes para estas diversas velocidades de transmisión de datos, aquí sólo se presentarán las más comunes. La figura muestra algunas de las características de la Ethernet PHY.

En esta sección se analizará la porción de Ethernet que opera en la capa física, comenzando por 10Base-T y continuando con las variedades de 10 Gbps.

Tipos de Ethernet

| Tipo de Ethernet | Ancho de banda | Tipo de cable | Duplex | Distancia máxima |
|------------------|----------------|------------------|--------|------------------|
| 10Base-5 | 10 Mbps | Coaxial thicknet | Half | 500 m |
| 10Base-2 | 10 Mbps | Coaxial thinnet | Half | 185 m |
| 100Base-TX | 10 Mbps | UTP Cat3/Cat5 | Half | 100 m |
| 100Base-TX | 100 Mbps | UTP Cat5 | Half | 100 m |
| 100Base-TX | 200 Mbps | UTP Cat5 | Full | 100 m |
| 100Base-TX | 100 Mbps | Fibra multimodo | Half | 400 m |
| 1000Base-T | 200 Mbps | Fibra multimodo | Full | 2 km |
| 1000Base-TX | 1 Gbps | UTP Cat5e | Full | 100 m |
| 1000Base-SX | 1 Gbps | UTP Cat6 | Full | 100 m |
| 1000Base-LX | 1 Gbps | Fibra multimodo | Full | 550 m |
| 10GBase-CX4 | 1 Gbps | Fibra monomodo | Full | 2 km |
| 10GBase-T | 10 Gbps | Twinaxial | Full | 100 m |
| 10GBase-LX4 | 10 Gbps | UTP Cat6a/Cat7 | Full | 100 m |
| 10GBase-LX4 | 10 Gbps | Fibra multimodo | Full | 300 m |
| 10 Mbps | 10 Gbps | Fibra monomodo | Full | 10 km |

9.5.2 Ethernet de 10 y 100 Mbps

Las principales implementaciones de 10 Mbps de Ethernet incluyen:

- 10BASE5 con cable coaxial Thicknet
- 10BASE2 con cable coaxial Thinnet
- 10BASE-T con cable de par trenzado no blindado Cat3/Cat5

Las primeras implementaciones de Ethernet, 10BASE5 y 10BASE2 utilizaban cable coaxial en un bus físico. Dichas implementaciones ya no se utilizan y los más recientes estándares 802.3 no las admiten.

Ethernet de 10 Mbps – 10BASE-T

La 10BASE-T utiliza la codificación Manchester para dos cables de par trenzado no blindado. Las primeras implementaciones de la 10BASE-T utilizaban cableado Cat3. Sin embargo, el cableado Cat5 o superior es el que se utiliza generalmente en la actualidad.

La Ethernet de 10 Mbps se considera como la Ethernet clásica y utiliza una topología en estrella física. Los enlaces de Ethernet 10BASE-T pueden tener hasta 100 metros de longitud antes de que requieran un hub o repetidor.

La 10BASE-T utiliza dos pares de cables de cuatro pares y finaliza en cada extremo con un conector RJ-45 de 8 pins. El par conectado a los pins 1 y 2 se utiliza para transmitir y el par conectado a los pins 3 y 6 se utiliza para recibir. La figura muestra la salida de pins RJ45 utilizada con Ethernet 10BASE-T.

La 10BASE-T generalmente no se elige para instalaciones de LAN nuevas. Sin embargo, todavía existen actualmente muchas redes Ethernet 10BASE-T. El reemplazo de los hubs por los switches en redes 10BASE-T aumentó notablemente

la velocidad de transmisión (throughput) disponible para estas redes y le otorgó a la Ethernet antigua una mayor longevidad. Los enlaces de 10BASE-T conectados a un switch pueden admitir el funcionamiento tanto half-duplex como full-duplex.

Salidas 10Base-T Ethernet RJ-45



| Número de Pin | Señal |
|---------------|--|
| 1 | TD+ (Transmitir datos, señal diferencial positiva) |
| 2 | TD- (Transmitir datos, señal diferencial negativa) |
| 3 | RD+ (Recibir datos, señal diferencial positiva) |
| 4 | No se utiliza |
| 5 | No se utiliza |
| 6 | RD- (Recibir datos, señal diferencial negativa) |
| 7 | No se utiliza |
| 8 | No se utiliza |

100 Mbps – Fast Ethernet

Entre mediados y fines de la década de 1990 se establecieron varios estándares 802.3 nuevos para describir los métodos de transmisión de datos en medios Ethernet a 100 Mbps. Estos estándares utilizaban requisitos de codificación diferentes para lograr estas velocidades más altas de transmisión de datos.

La Ethernet de 100 Mbps, también denominada Fast Ethernet, puede implementarse utilizando medios de fibra o de cable de cobre de par trenzado. Las implementaciones más conocidas de la Ethernet de 100 Mbps son:

- 100BASE-TX con UTP Cat5 o mayor
- 100BASE-FX con cable de fibra óptica

Ya que las señales de mayor frecuencia que se utilizan en Fast Ethernet son más susceptibles al ruido, Ethernet de 100 Mbps utiliza dos pasos de codificación por separado para mejorar la integridad de la señal.

100BASE-TX

100BASE-TX fue diseñada para admitir la transmisión a través de dos hilos de fibra óptica o de dos pares de cable de cobre UTP de Categoría 5. La implementación 100BASE-TX utiliza los mismos dos pares y salidas de pares de UTP que la 10BASE-T. Sin embargo, la 100BASE-TX requiere UTP de Categoría 5 o superior. La codificación 4B/5B se utiliza para la Ethernet 100BASE-T.

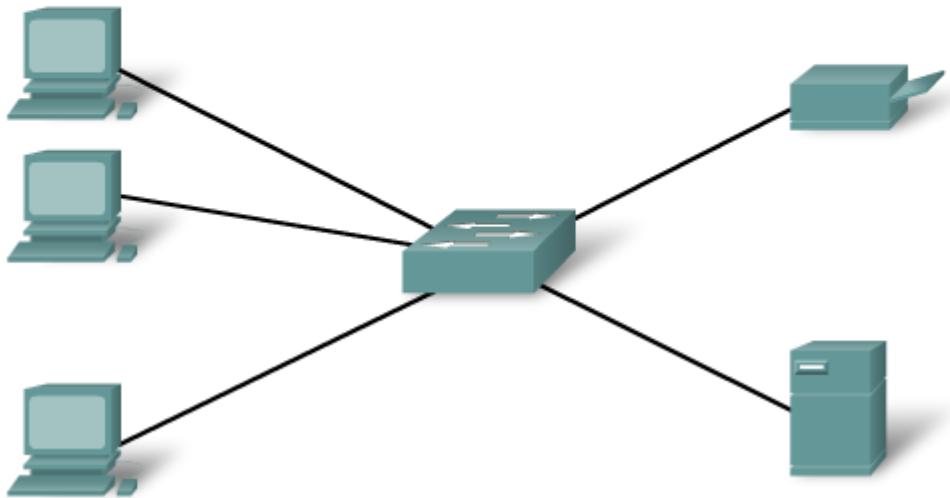
Al igual que con la 10BASE-TX, la 100BASE-TX se conecta como estrella física. La figura muestra un ejemplo de una topología en estrella física. Sin embargo, a diferencia de la 10Baset, las redes 100BASE-TX utilizan generalmente un switch en el centro de la estrella en vez de un hub. Aproximadamente al mismo tiempo que las tecnologías 100BASE-TX se convirtieron en la norma, los switches LAN también comenzaron a implementarse con frecuencia. Estos desarrollos simultáneos llevaron a su combinación natural en el diseño de las redes 100BASE-TX.

100BASE-FX

El estándar 100BASE-FX utiliza el mismo procedimiento de señalización que la 100BASE-TX, pero lo hace en medios de fibra óptica en vez de cobre UTP. Si bien los procedimientos de codificación, decodificación y recuperación de reloj son los mismos para ambos medios, la transmisión de señales es diferente: pulsos eléctricos en cobre y pulsos de luz en fibra óptica. La 100BASE-FX utiliza conectores de interfaz de fibra de bajo costo (generalmente llamados conectores SC 358ersió).

Las implementaciones de fibra son conexiones punto a punto, es decir, se utilizan para interconectar dos dispositivos. Estas conexiones pueden ser entre dos computadoras, entre una computadora y un switch o entre dos switches.

Topología en estrella utilizada con Ethernet 10BASE-T y 100BASE-TX



9.5.3 Ethernet de 1000 Mbps

1000 Mbps – Gigabit Ethernet

El desarrollo de los estándares de Gigabit Ethernet dio como resultado especificaciones para cobre UTP, fibra monomodo y fibra multimodo. En redes de Gigabit Ethernet, los bits se producen en una fracción del tiempo que requieren en redes de 100 Mbps y redes de 10 Mbps. Gracias a que las señales se producen en menor tiempo, los bits se vuelven más susceptibles al ruido y, por lo tanto, la temporización tiene una importancia decisiva. La cuestión del rendimiento se basa en la velocidad con la que el adaptador o la interfaz de red puedan cambiar los niveles de voltaje y en la manera en que dicho cambio de voltaje pueda detectarse de un modo confiable a 100 metros de distancia en la NIC o la interfaz de recepción.

A estas mayores velocidades, la codificación y decodificación de datos es más compleja. La Gigabit Ethernet utiliza dos distintos pasos de codificación. La transmisión de datos es más eficiente cuando se utilizan códigos para representar el stream binario de bits. La codificación de datos permite la sincronización, el uso eficiente del ancho de banda y características mejoradas de relación entre señal y ruido.

Ethernet 1000BASE-T

La Ethernet 1000BASE-T brinda una transmisión full-duplex utilizando los cuatro pares de cable UTP Categoría 5 o superior. La Gigabit Ethernet por cables de cobre permite un aumento de 100 Mbps por par de cable a 125 Mbps por par de cable o 500 Mbps para los cuatro pares. Cada par de cable origina señales en full-duplex, lo que duplica los 500 Mbps a 1000 Mbps.

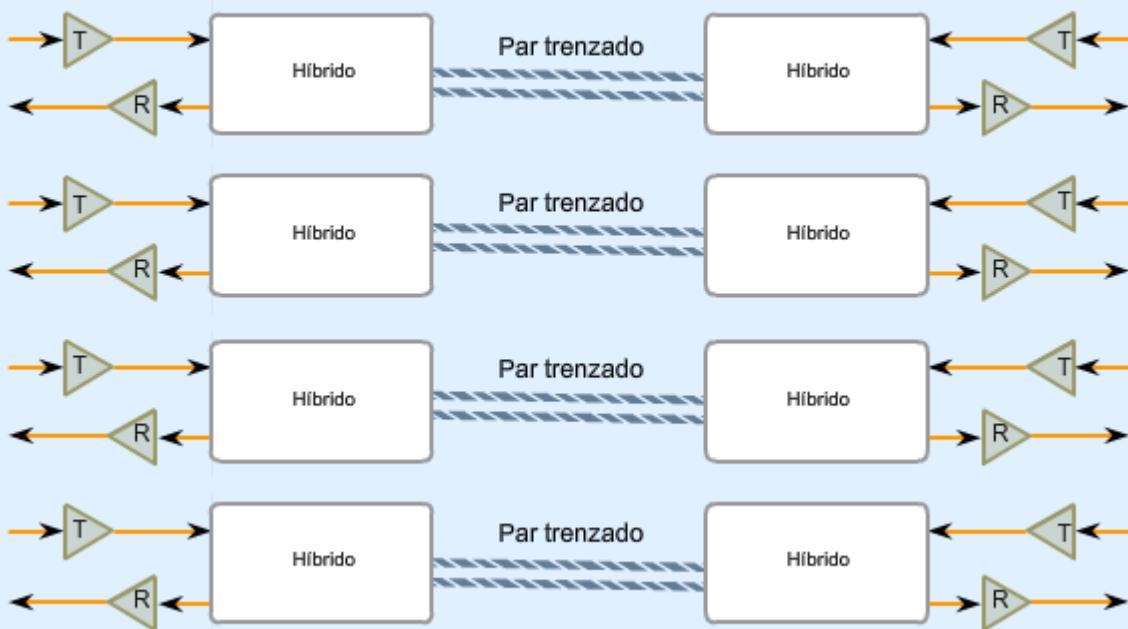
La 1000BASE-T utiliza codificación de línea 4D-PAM5 para obtener un throughput de datos de 1 Gbps. Este esquema de codificación permite señales de transmisión en cuatro pares de cables simultáneamente. Traduce un byte de 8 bits de datos en una transmisión simultánea de cuatro símbolos de código que se envían por los medios, uno en cada par, como señales de Modulación de amplitud de pulsos de 5 niveles (PAM5). Esto significa que cada símbolo se corresponde con dos bits de datos. Debido a que la información viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor. La figura muestra una representación del sistema de circuitos que utiliza la Ethernet 1000BASE-T.

La 1000BASE-T permite la transmisión y recepción de datos en ambas direcciones (en el mismo cable y al mismo tiempo). Este flujo de tráfico crea colisiones permanentes en los pares de cables. Estas colisiones generan patrones de voltaje complejos. Los circuitos híbridos que detectan las señales utilizan técnicas sofisticadas tales como la cancelación de eco, la corrección del error de envío de Capa 1 (FEC) y una prudente selección de los niveles de voltaje. Al utilizar dichas técnicas, el sistema alcanza un throughput de 1 Gigabit.

Para contribuir a la sincronización, la capa física encapsula cada trama con delimitadores de inicio y finalización de stream. La temporización de loops se mantiene mediante streams continuos de símbolos INACTIVOS que se envían en cada par de cables durante el espacio entre tramas.

A diferencia de la mayoría de las señales digitales, en las que generalmente se encuentra un par de niveles de voltaje discretos, la 1000BASE-T utiliza muchos niveles de voltaje. En períodos inactivos, se encuentran nueve niveles de voltaje en el cable. Durante los períodos de transmisión de datos, se encuentran hasta 17 niveles de voltaje en el cable. Con este gran número de estados, combinado con los efectos del ruido, la señal en el cable parece más analógica que digital. Como en el caso del analógico, el sistema es más susceptible al ruido debido a los problemas de cable y terminación.

Circuitos 1000BASE-T



Ethernet 1000BASE-SX y 1000BASE-LX por fibra óptica

Las versiones de fibra óptica de la Gigabit Ethernet (1000BASE-SX y 1000BASE-LX) ofrecen las siguientes ventajas sobre el UTP: inmunidad al ruido, tamaño físico pequeño y distancias y ancho de banda aumentados y sin repeticiones.

Todas las versiones de 1000BASE-SX y 1000BASE-LX admiten la transmisión binaria full-duplex a 1250 Mbps en dos hebras de fibra óptica. La codificación de la transmisión se basa en el esquema de codificación 8B/10B. Debido al gasto de esta codificación, la velocidad de transferencia de datos sigue siendo 1000 Mbps.

Cada trama de datos se encapsula en la capa física antes de la transmisión y la sincronización de los enlaces se mantiene enviando un stream continuo de grupos de códigos INACTIVOS durante el espacio entre tramas.

Las principales diferencias entre las versiones de fibra de 1000BASE-SX y 1000BASE-LX son los medios de enlace, los conectores y la longitud de onda de la señal óptica. Estas diferencias se ilustran en la figura.

| Soporte de enlace de fibra 1000Base-X | | |
|---------------------------------------|--|---|
| Configuración del enlace | 1000Base-SX (850 nm de longitud de onda) | 1000Base-LX (1300 nm de longitud de onda) |
| 125/62.5 µm fibra óptica multimodo | Compatible | Compatible |
| fibra óptica multimodo de 125/50 µm | Compatible | Compatible |
| fibra óptica monomodo de 125/10 µm | No compatible | Compatible |

9.5.4 Ethernet: Opciones futuras

Se adaptó el estándar IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. El estándar 802.3ae y los estándares 802.3 para la Ethernet original son muy similares. La Ethernet de 10 Gigabits (10GbE) está evolucionando para poder utilizarse no sólo en LAN sino también en WAN y MAN.

Debido a que el formato de trama y otras especificaciones de Ethernet de Capa 2 son compatibles con estándares anteriores, la 10GbE puede brindar un mayor ancho de banda para redes individuales que sea interoperable con la infraestructura de red existente.

10Gbps se puede comparar con otras variedades de Ethernet de este modo:

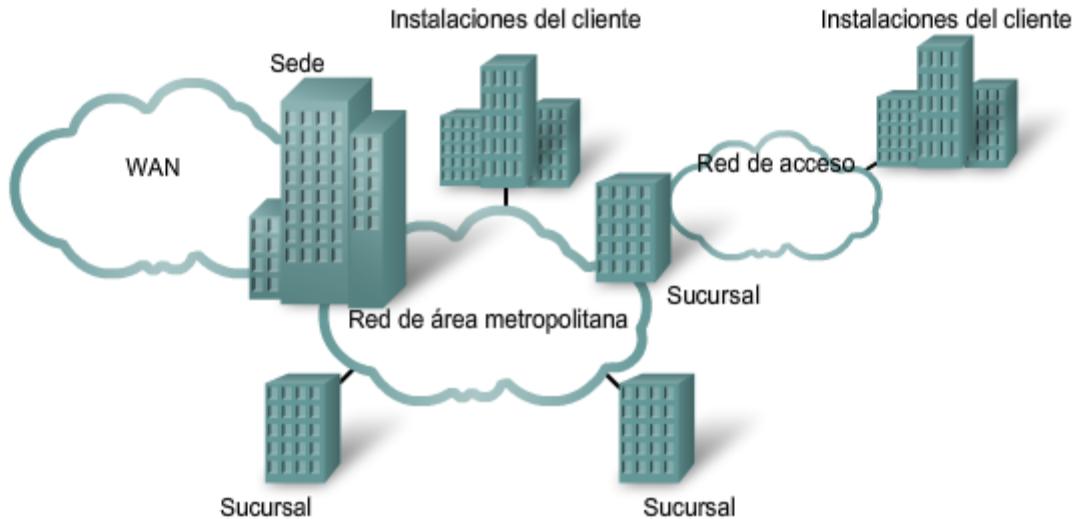
- El formato de trama es el mismo, permitiendo así la interoperabilidad entre todos los tipos de tecnologías antiguas, fast, gigabit y 10 Gigabit Ethernet, sin la necesidad de retramado o conversiones de protocolo.
- El tiempo de bit ahora es de 0,1 nanosegundos. Todas las demás variables de tiempo caen en su correspondiente lugar en la escala.
- Ya que sólo se utilizan conexiones de fibra óptica full-duplex, no hay ningún tipo de contención de medios ni se necesita el CSMA/CD.
- Se preserva la mayoría de las subcapas de 802.3 de IEEE dentro de las Capas OSI 1 y 2, con algunos pocos agregados para que se adapten a enlaces de fibra de 40 km y la posibilidad de interoperabilidad con otras tecnologías en fibra.

Con 10Gbps Ethernet es posible crear redes de Ethernet flexibles, eficientes, confiables, a un costo punto a punto relativamente bajo.

Futuras velocidades de Ethernet

Si bien la Ethernet de 1 Gigabit es muy fácil de hallar en el mercado y cada vez es más fácil conseguir los productos de 10 Gigabits, el IEEE y la Alianza de Ethernet de 10 Gigabits trabajan actualmente en estándares para 40, 100 e inclusive 160 Gbps. Las tecnologías que se adopten dependerán de un número de factores que incluyen la velocidad de maduración de las tecnologías y de los estándares, la velocidad de adopción por parte del mercado y el costo de los productos emergentes.

La trama común Ethernet se puede aplicar a diferentes tipos de red



| Ethernet | | | | | |
|-----------|----------------------|---------------------|------|-----------|------------------------------------|
| 8 | 6 | 6 | 2 | 46 a 1500 | 4 |
| Preámbulo | Dirección de destino | Dirección de origen | Tipo | Datos | Secuencia de verificación de trama |

9.6 HUBS Y SWITCHES

9.6.1 Ethernet antigua: Utilización de hubs

En secciones anteriores, vimos cómo la Ethernet clásica utiliza medios compartidos y control de acceso al medio basado en contenciones. La Ethernet clásica utiliza hubs para interconectar los nodos del segmento de LAN. Los hubs no realizan ningún tipo de filtro de tráfico. En cambio, el hub reenvía todos los bits a todos los dispositivos conectados al hub. Esto obliga a todos los dispositivos de la LAN a compartir el ancho de banda de los medios.

Además, esta implementación de Ethernet clásica origina a menudo grandes niveles de colisiones en la LAN. Debido a estos problemas de rendimiento, este tipo de LAN Ethernet tiene un uso limitado en las redes actuales. Las implementaciones de Ethernet con hubs se utilizan generalmente en la actualidad en LAN pequeñas o LAN con pocos requisitos de ancho de banda.

El hecho de que los dispositivos compartan medios crea problemas significativos a medida que la red crece. La figura ilustra algunas de los problemas que aquí se presentan.

Escalabilidad

En una red con hubs, existe un límite para la cantidad de ancho de banda que los dispositivos pueden compartir. Con cada dispositivo que se agrega al medio compartido, el ancho de banda promedio disponible para cada dispositivo disminuye. Con cada aumento de la cantidad de dispositivos en los medios, el rendimiento se ve degradado.

Latencia

La latencia de la red es la cantidad de tiempo que le lleva a una señal llegar a todos los destinos del medio. Cada nodo de una red basada en hubs debe esperar una oportunidad de transmisión para evitar colisiones. La latencia puede aumentar notablemente a medida que la distancia entre los nodos se extiende. La latencia también se ve afectada por un retardo de la señal en los medios, como así también por el retardo añadido por el procesamiento de las señales mediante hubs y repetidores. El aumento de la longitud de los medios o de la cantidad de hubs y repetidores conectados a un segmento origina una mayor latencia. A mayor latencia, mayor probabilidad de que los nodos no reciban las señales iniciales, lo que aumenta las colisiones presentes en la red.

Falla de red

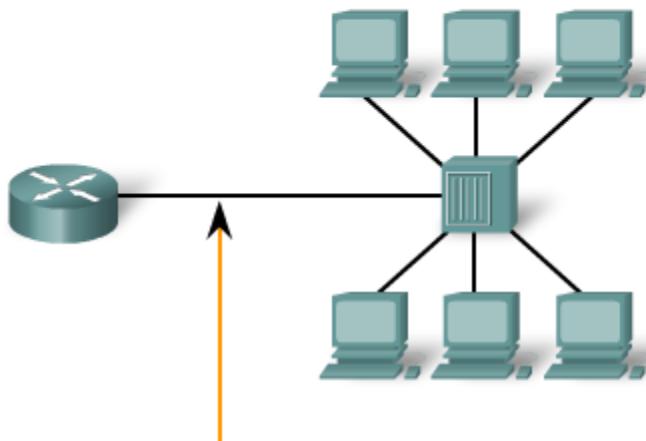
Debido a que la Ethernet clásica comparte los medios, cualquier dispositivo de la red puede potencialmente ocasionar problemas para otros dispositivos. Si cualquier dispositivo conectado al hub genera tráfico perjudicial, puede verse impedida la comunicación de todos los dispositivos del medio. Este tráfico perjudicial puede deberse a una velocidad incorrecta o a los ajustes de full-duplex de la NIC.

Colisiones

Según el CSMA/CD, un nodo no debería enviar un paquete a menos que la red esté libre de tráfico. Si dos nodos envían paquetes al mismo tiempo, se produce una colisión y los paquetes se pierden. Entonces, ambos nodos envían una señal de congestión, esperan una cantidad de tiempo aleatoria y retransmiten sus paquetes. Cualquier parte de la red en donde los paquetes de dos o más nodos puedan interferir entre ellos se considera como un dominio de colisiones. Una red con una gran cantidad de nodos en el mismo segmento tiene un dominio de colisiones mayor y, generalmente, más tráfico. A medida que aumenta la cantidad de tráfico en la red, aumentan las posibilidades de colisión.

Los switches brindan una alternativa para el entorno basado en contenciones de la Ethernet clásica.

Rendimiento deficiente de las LAN basadas en hubs



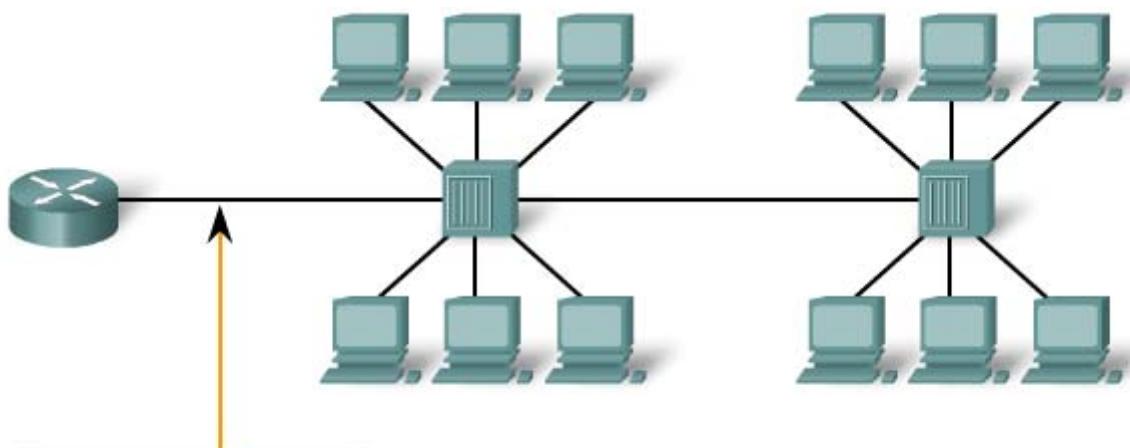
Ancho de banda de red
compartido por 6 hosts

Redefinir

Falta de escalabilidad

Mayor latencia

Más colisiones



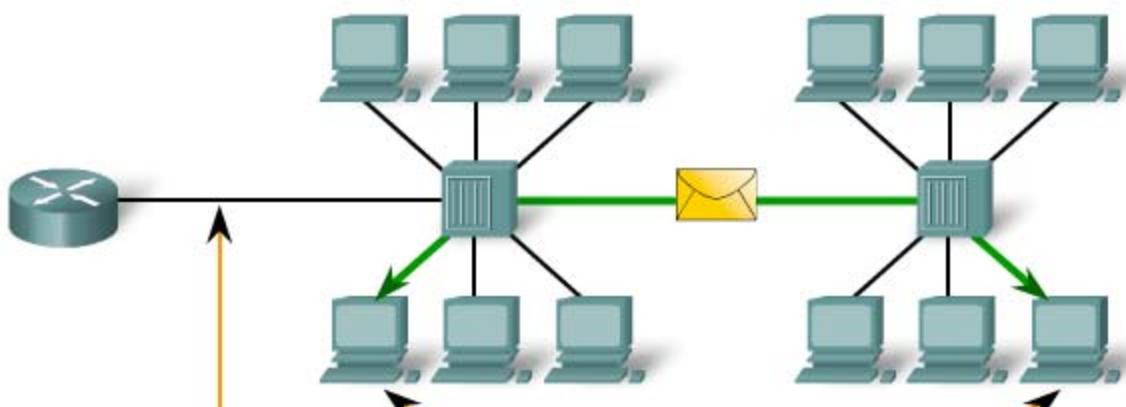
Igual ancho de banda de red
compartido por 12 hosts

Redefinir

Falta de escalabilidad

Mayor latencia

Más colisiones



Igual ancho de banda de red
compartido por 12 hosts

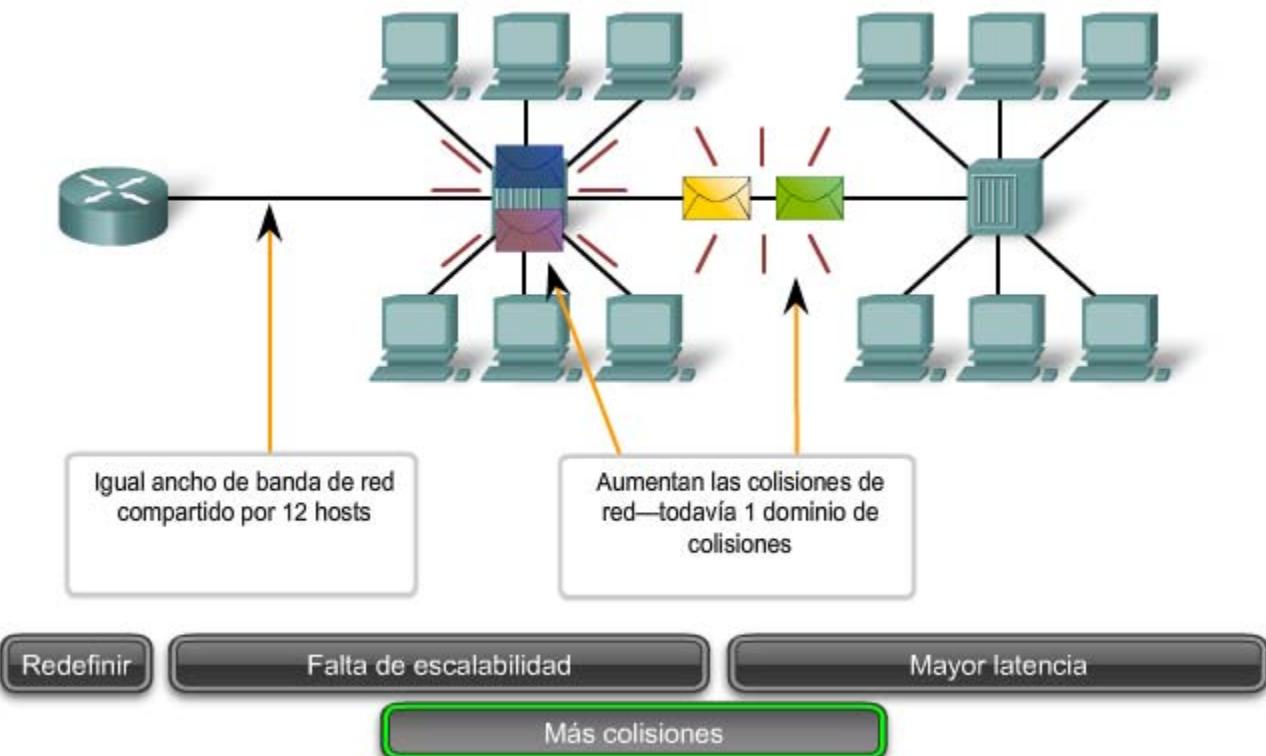
Aumenta la latencia de la
red

Redefinir

Falta de escalabilidad

Mayor latencia

Más colisiones



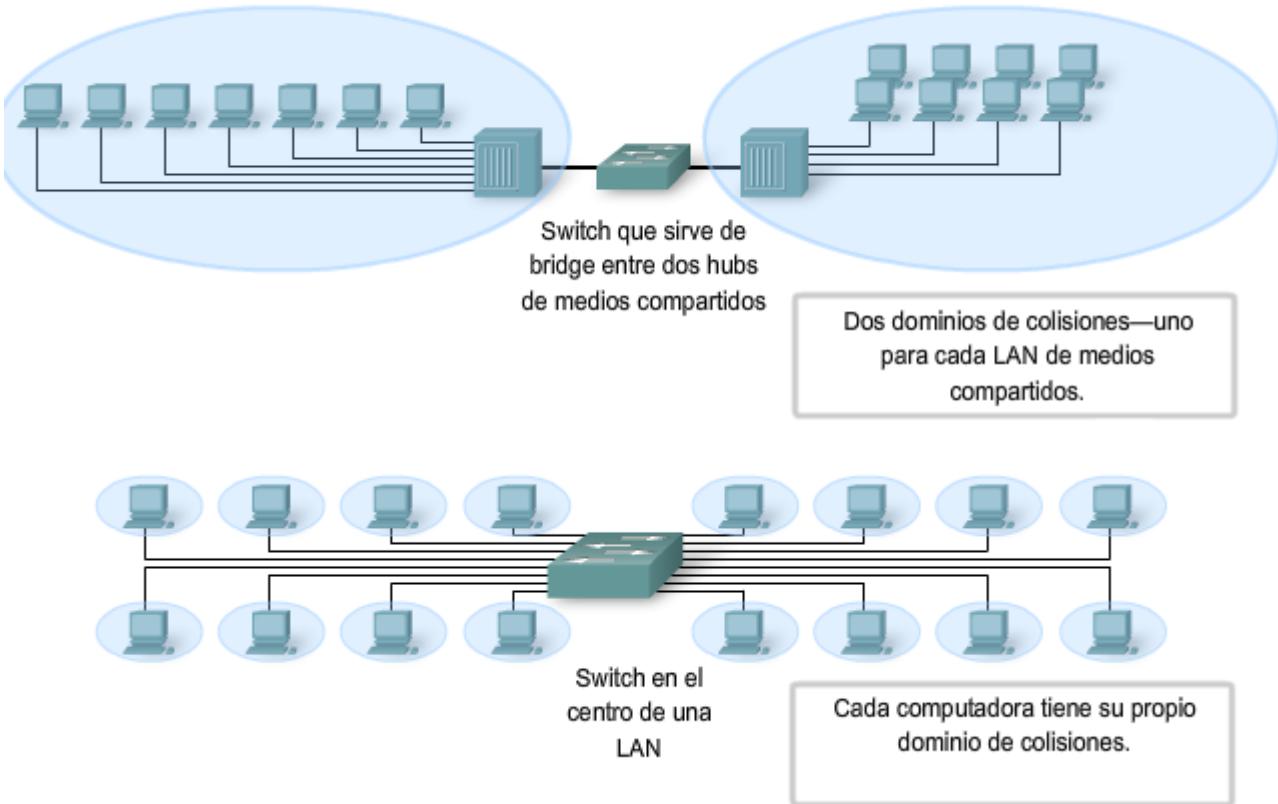
9.6.2 Ethernet: Utilización de switches

En los últimos años, los switches se convirtieron rápidamente en una parte fundamental de la mayoría de las redes. **Los switches permiten la segmentación de la LAN en distintos dominios de colisiones.** Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

Una LAN puede tener un switch centralizado que conecta a hubs que todavía brindan conectividad a los nodos. O bien, una LAN puede tener todos los nodos conectados directamente a un switch. Estas topologías se ilustran en la figura.

En una LAN en la que se conecta un hub a un puerto de un switch, todavía existe un ancho de banda compartido, lo que puede producir colisiones dentro del entorno compartido del hub. Sin embargo, el switch aislará el segmento y limitará las colisiones para el tráfico entre los puertos del hub.

Usos del switch



Los nodos se conectan directamente

En una LAN en la que todos los nodos están conectados directamente al switch, el throughput de la red aumenta notablemente. Las tres principales razones de este aumento son:

- Ancho de banda dedicado a cada puerto
- Entorno libre de colisiones
- Operación full-duplex

Estas topologías físicas en estrella son esencialmente enlaces punto a punto.

Ancho de banda dedicado

Cada nodo dispone del ancho de banda de los medios completo en la conexión entre el nodo y el switch. Debido a que un hub replica las señales que recibe y las envía a todos los demás puertos, los hubs de Ethernet clásica forman un bus lógico. Esto significa que todos los nodos deben compartir el mismo ancho de banda para este bus. Con los switches, cada dispositivo tiene una conexión punto a punto dedicada entre el dispositivo y el switch, sin contención de medios.

A modo de ejemplo, pueden compararse dos LAN de 100 Mbps, cada una de ellas con 10 nodos. En el segmento de red A, los 10 nodos se conectan a un hub. Cada nodo comparte el ancho de banda de 100 Mbps disponible. Esto ofrece un promedio de 10 Mbps para cada nodo. En el segmento de red B, los 10 nodos se conectan a un switch. En este segmento, los 10 nodos tienen el ancho de banda completo de 100 Mbps disponible.

Incluso en este ejemplo de red pequeña, el aumento del ancho de banda es significativo. A medida que la cantidad de nodos aumenta, la discrepancia entre el ancho de banda disponible para las dos implementaciones aumenta significativamente.

Entorno libre de colisiones

Una conexión punto a punto dedicada a un switch también evita contenciones de medios entre dispositivos, lo que permite que un nodo funcione con pocas colisiones o ninguna colisión. En una red Ethernet clásica de tamaño moderado que utiliza hubs, aproximadamente entre el 40% y el 50% del ancho de banda se consume en la recuperación por colisiones. En una red Ethernet con switch, en la que prácticamente no hay colisiones, el gasto destinado a la recuperación por colisiones se elimina casi por completo. Esto le ofrece a la red con switches tasas de throughput significativamente mejoradas.

Funcionamiento full-duplex

La utilización de switches también le permite a una red funcionar como entorno de Ethernet full-duplex. Antes de que existieran los switches, la Ethernet sólo era half-duplex. Esto implicaba que en un momento dado un nodo podía transmitir o recibir. Con la característica full-duplex habilitada en una red Ethernet con switches, los dispositivos conectados directamente a los puertos del switch pueden transmitir y recibir simultáneamente con el ancho de banda completo de los medios.

La conexión entre el dispositivo y el switch está libre de colisiones. Esta disposición efectivamente duplica la velocidad de transmisión cuando se la compara con la half-duplex. Por ejemplo, si la velocidad de la red es de 100 Mbps, cada nodo puede transmitir una trama a 100 Mbps y, al mismo tiempo, recibir una trama a 100 Mbps.

Utilización de switches en lugar de hubs

Gran parte de la Ethernet moderna utiliza switches para los dispositivos finales y opera en full 367ersió. Debido a que los switches brindan mucho más throughput que los hubs y aumentan el rendimiento tan notablemente, es justo preguntarse: ¿por qué no utilizamos switches en todas las LAN Ethernet? Existen tres razones por las que los hubs siguen utilizándose:

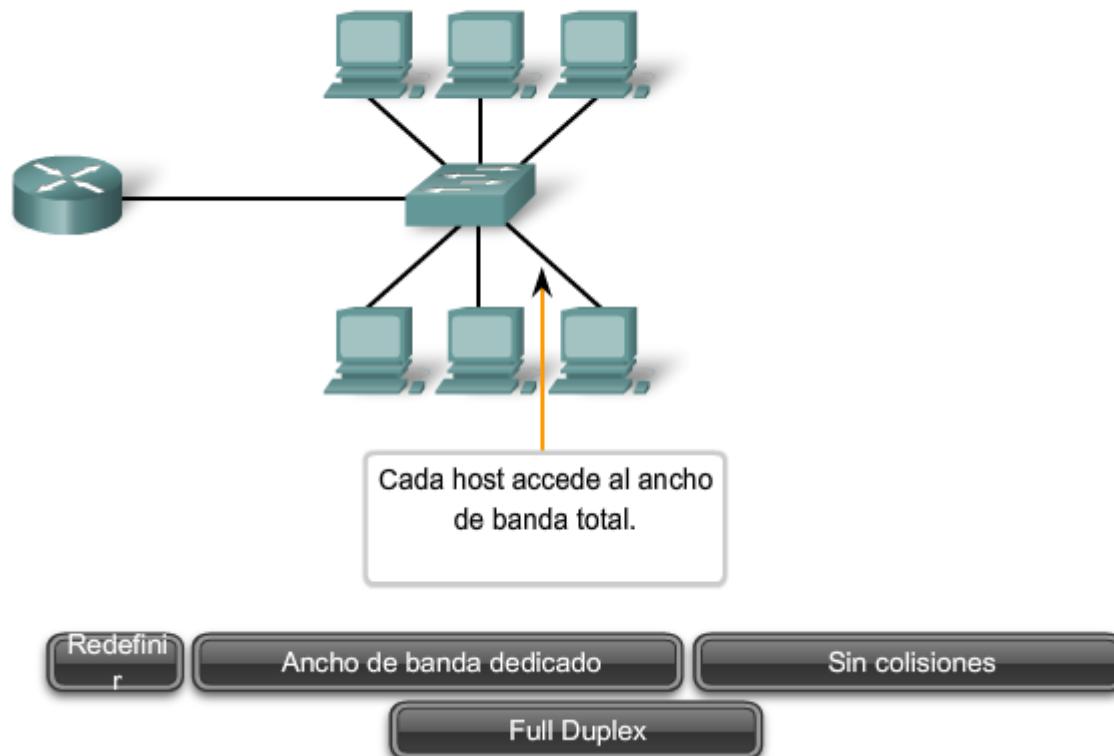
Disponibilidad: los switches de LAN no se desarrollaron hasta comienzos de la década de 1990 y no estuvieron disponibles hasta mediados de dicha década. Las primeras redes Ethernet utilizaban hubs de UTP y muchas de ellas continúan funcionando hasta el día de hoy.

Económicas. En un principio, los switches resultaban bastante costosos. A medida que el precio de los switches se redujo, la utilización de hubs disminuyó y el costo es cada vez menos un factor al momento de tomar decisiones de implementación.

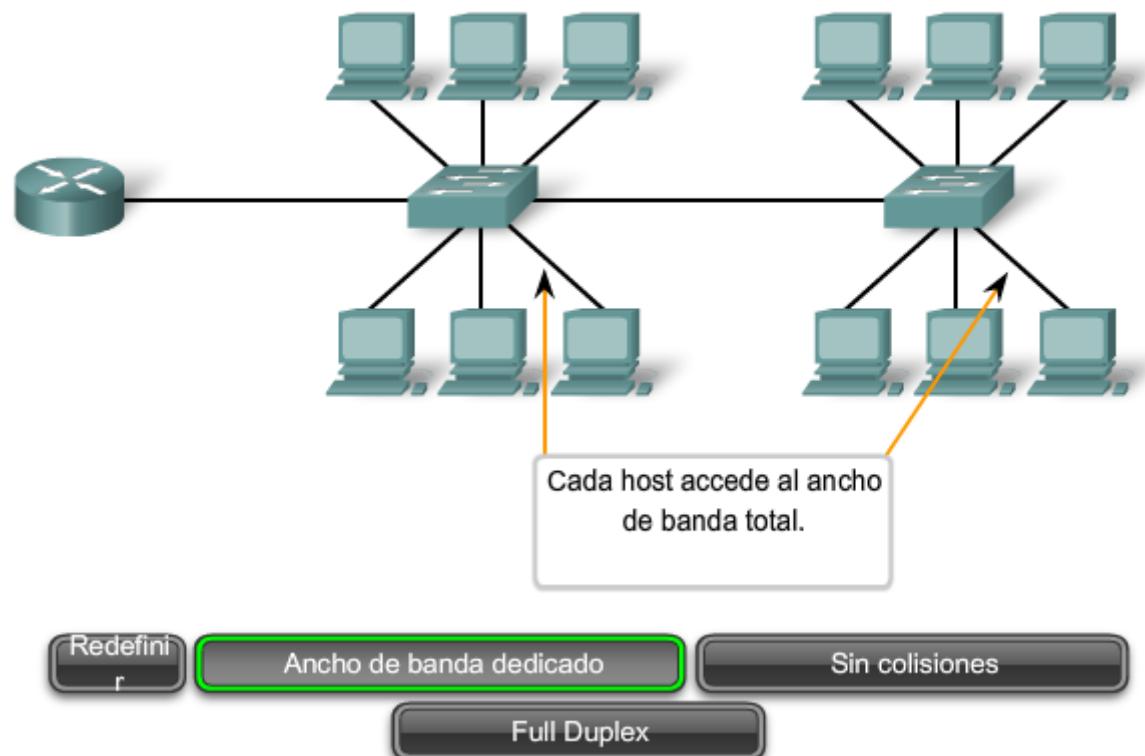
Requisitos: Las primeras redes LAN eran redes simples diseñadas para intercambiar archivos y compartir impresoras. Para muchas ubicaciones, las primeras redes evolucionaron hasta convertirse en las redes convergentes de la actualidad, lo que originó una necesidad imperante de un mayor ancho de banda disponible para los usuarios individuales. En algunos casos, sin embargo, será suficiente con un hub de medios compartidos y estos productos permanecen en el mercado.

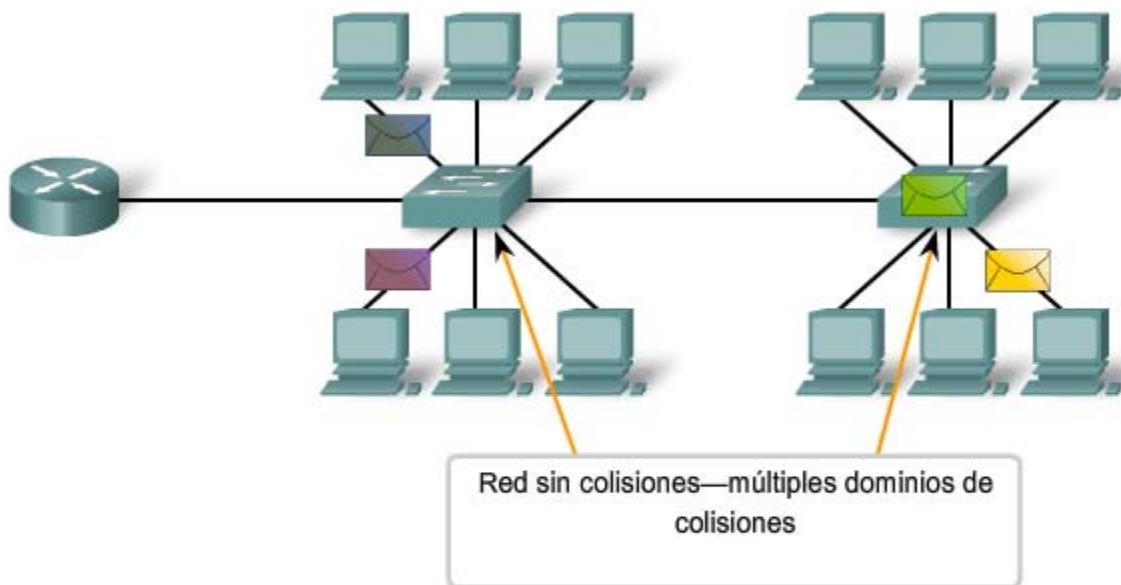
La siguiente sección estudia la operación básica de los switches y cómo un switch logra el rendimiento mejorado del que ahora dependen nuestras redes. En un curso posterior se presentarán más detalles y tecnologías adicionales relacionadas con la conmutación.

Características de las LAN basadas en switches

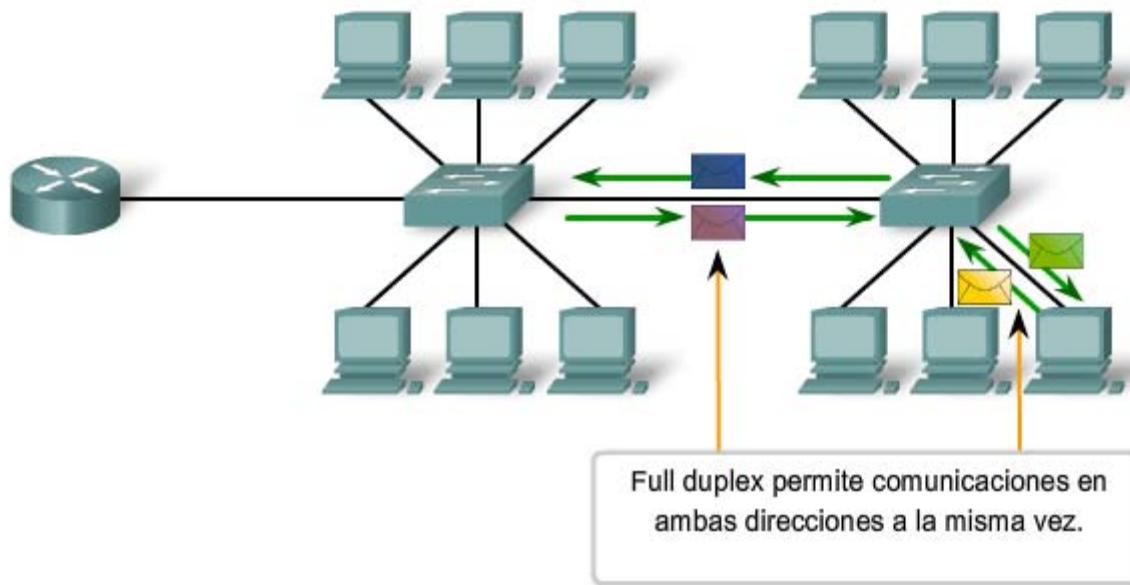


Características de las LAN basadas en switches





Redefinir **Ancho de banda dedicado** **Sin colisiones**
Full Duplex



Redefinir **Ancho de banda dedicado** **Sin colisiones**
Full Duplex

6.6.3 Switches: Reenvío selectivo

Los switches Ethernet reenvían selectivamente tramas individuales desde un puerto receptor hasta el puerto en el que esté conectado el nodo de destino. Este proceso de reenvío selectivo puede pensarse como la posibilidad de establecer una conexión punto a punto momentánea entre los nodos de transmisión y recepción. La conexión se establece sólo

durante el tiempo suficiente como para enviar una sola trama. Durante este instante, los dos nodos tienen una conexión de ancho de banda completa entre ellos y representan una conexión lógica punto a punto.

Para ser más precisos en términos técnicos, esta conexión temporal no se establece entre los dos nodos de manera simultánea. Básicamente, esto hace que la conexión entre los hosts sea una conexión punto a punto. De hecho, cualquier nodo que funcione en modo full-duplex puede transmitir en cualquier momento que tenga una trama, independientemente de la disponibilidad del nodo receptor. Esto sucede porque un switch LAN almacena una trama entrante en la memoria búfer y después la envía al puerto correspondiente cuando dicho puerto está inactivo. Este proceso se denomina almacenar y enviar.

Con la conmutación almacenar y enviar, el switch recibe la trama completa, controla el FCS en busca de errores y reenvía la trama al puerto indicado para el nodo de destino. Debido a que los nodos no deben esperar a que el medio esté inactivo, los nodos pueden enviar y recibir a la velocidad completa del medio sin pérdidas ocasionadas por colisiones o el gasto asociado con la administración de colisiones.

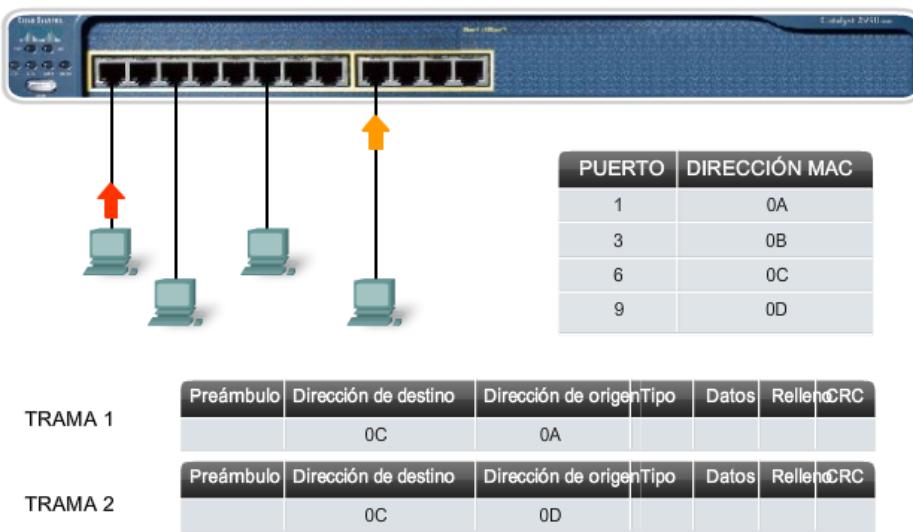
El reenvío se basa en la MAC de destino

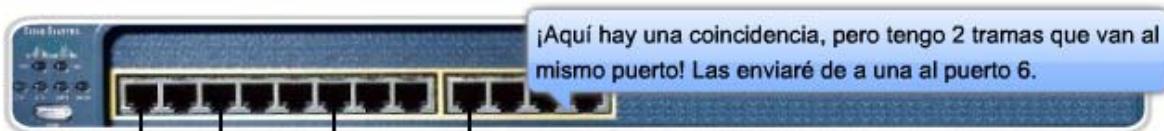
El switch mantiene una tabla, denominada tabla MAC que hace coincidir una dirección MAC de destino con el puerto utilizado para conectarse a un nodo. Para cada trama entrante, la dirección MAC de destino en el encabezado de la trama se compara con la lista de direcciones de la tabla MAC. Si se produce una coincidencia, el número de puerto de la tabla que se asoció con la dirección MAC se utiliza como puerto de salida para la trama.

La tabla MAC puede denominarse de diferentes maneras. Generalmente, se la llama tabla de switch. Debido a que la conmutación deriva de una tecnología más antigua denominada bridging transparente, la tabla suele denominarse tabla del puente. Por esta razón, muchos de los procesos que realizan los switches LAN pueden contener las palabras bridge o bridging en su nombre.

Un bridge es un dispositivo que se utilizaba con mayor frecuencia en los inicios de la LAN para conectar dos segmentos de red física. Los switches pueden utilizarse para realizar esta operación, a la vez que permiten la conectividad del dispositivo final con la LAN. Muchas otras tecnologías se desarrollaron en torno a los switches LAN. Muchas de estas tecnologías se presentarán en otro curso. Un entorno en el que prevalecen los bridges son las redes inalámbricas. Utilizamos bridges inalámbricos para interconectar dos segmentos de red inalámbrica. Por lo tanto, encontrará que la industria de redes utiliza ambos términos, conmutación y bridging.

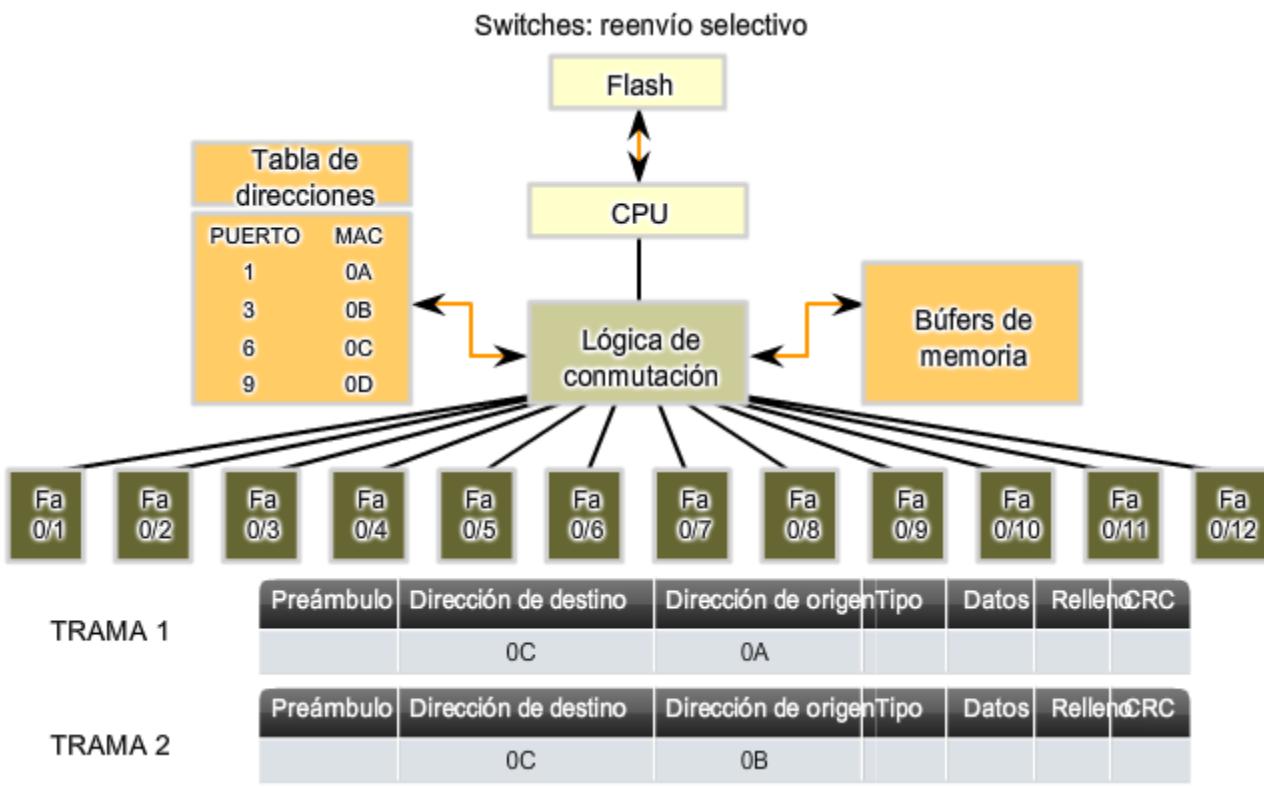
Switches: reenvío selectivo





| PUERTO | DIRECCIÓN MAC |
|--------|---------------|
| 1 | 0A |
| 3 | 0B |
| 6 | 0C |
| 9 | 0D |

| | | | | | | | |
|---------|-----------|----------------------|---------------------|------|-------|---------|-----|
| TRAMA 1 | Preámbulo | Dirección de destino | Dirección de origen | Tipo | Datos | Relleno | CRC |
| | | 0C | 0A | | | | |
| TRAMA 2 | Preámbulo | Dirección de destino | Dirección de origen | Tipo | Datos | Relleno | CRC |
| | | 0C | 0D | | | | |



Funcionamiento del switch

Para lograr su fin, los switches LAN Ethernet realizan cinco operaciones básicas:

- Aprendizaje
- Actualización
- Inundación
- Reenvío selectivo
- Filtrado

Aprendizaje

La tabla MAC debe llenarse con las direcciones MAC y sus puertos correspondientes. El proceso de aprendizaje permite que estos mapeos se adquieran dinámicamente durante el funcionamiento normal.

A medida que cada trama ingresa al switch, el switch analiza la dirección MAC de origen. Mediante un proceso de búsqueda, el switch determina si la tabla ya contiene una entrada para esa dirección MAC. Si no existe ninguna entrada, el switch crea una nueva entrada en la tabla MAC utilizando la dirección MAC de origen y asocia la dirección con el puerto en el que llegó la entrada. Ahora, el switch puede utilizar este mapeo para reenviar tramas a este nodo.

Actualización

Las entradas de la tabla MAC que se adquirieron mediante el proceso de Aprendizaje reciben una marca horaria. La marca horaria se utiliza como instrumento para eliminar las entradas antiguas de la tabla MAC. Después de que se crea una entrada en la tabla MAC, un proceso comienza una cuenta regresiva utilizando la marca horaria como el valor inicial. Una vez que el valor alcanza 0, la entrada de la tabla se actualizará la próxima vez que el switch reciba una trama de ese nodo en el mismo puerto.

Flooding

Si el switch no sabe a qué puerto enviar una trama porque la dirección MAC de destino no se encuentra en la tabla MAC, el switch envía la trama a todos los puertos, excepto al puerto en el que llegó la trama. El proceso que consiste en enviar una trama a todos los segmentos se denomina inundación. El switch no reenvía la trama al puerto en el que llegó la trama porque cualquier destino de ese segmento ya habrá recibido la trama. La inundación también se utiliza para tramas que se envían a la dirección MAC de broadcast.

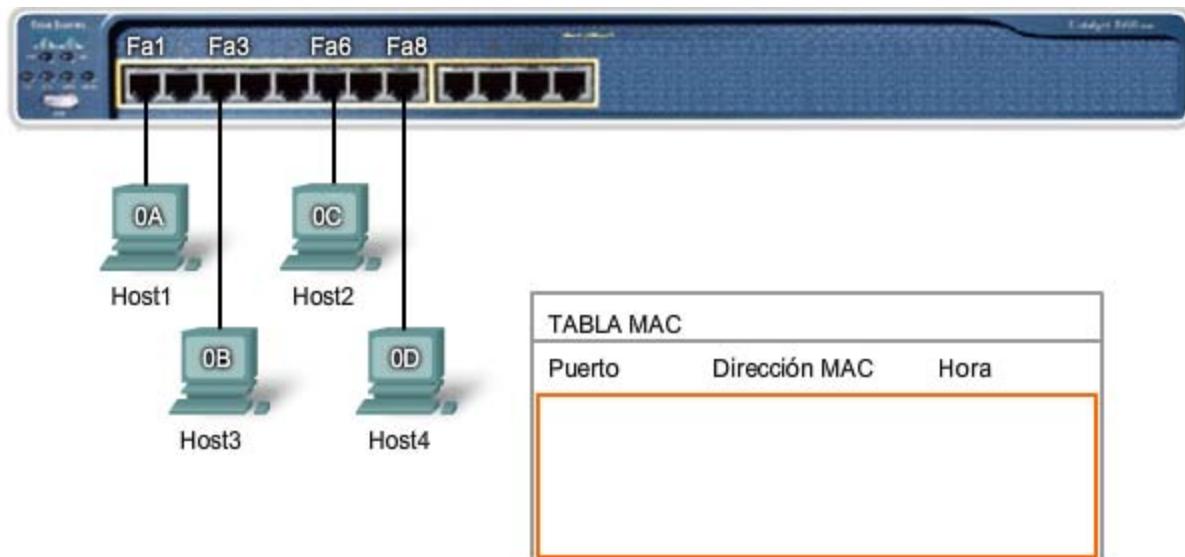
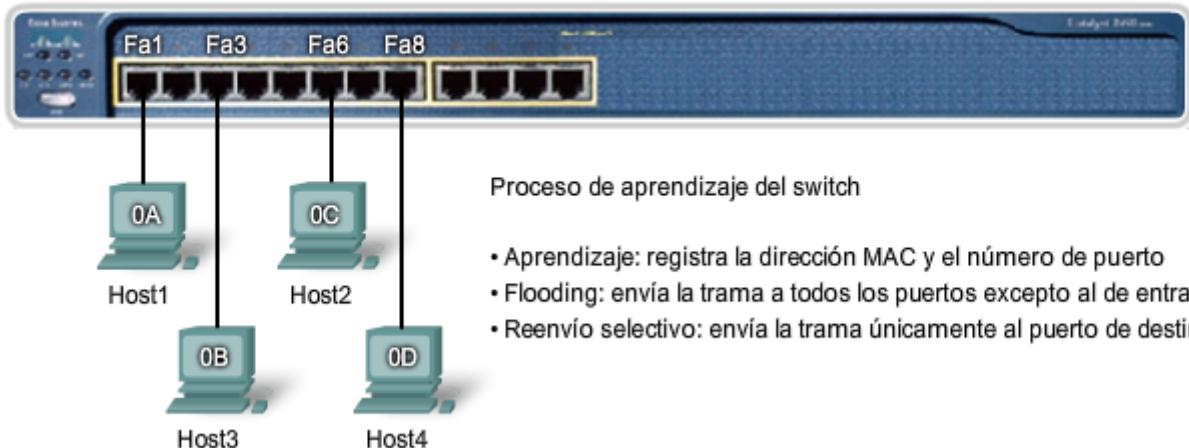
Reenvío selectivo

El reenvío selectivo es el proceso por el cual se analiza la dirección MAC de destino de una trama y se la reenvía al puerto correspondiente. Ésta es la función principal del switch. Cuando una trama de un nodo llega al switch y el switch ya aprendió su dirección MAC, dicha dirección se hace coincidir con una entrada de la tabla MAC y la trama se reenvía al puerto correspondiente. En lugar de saturar la trama hacia todos los puertos, el switch envía la trama al nodo de destino a través del puerto indicado. Esta acción se denomina reenvío..

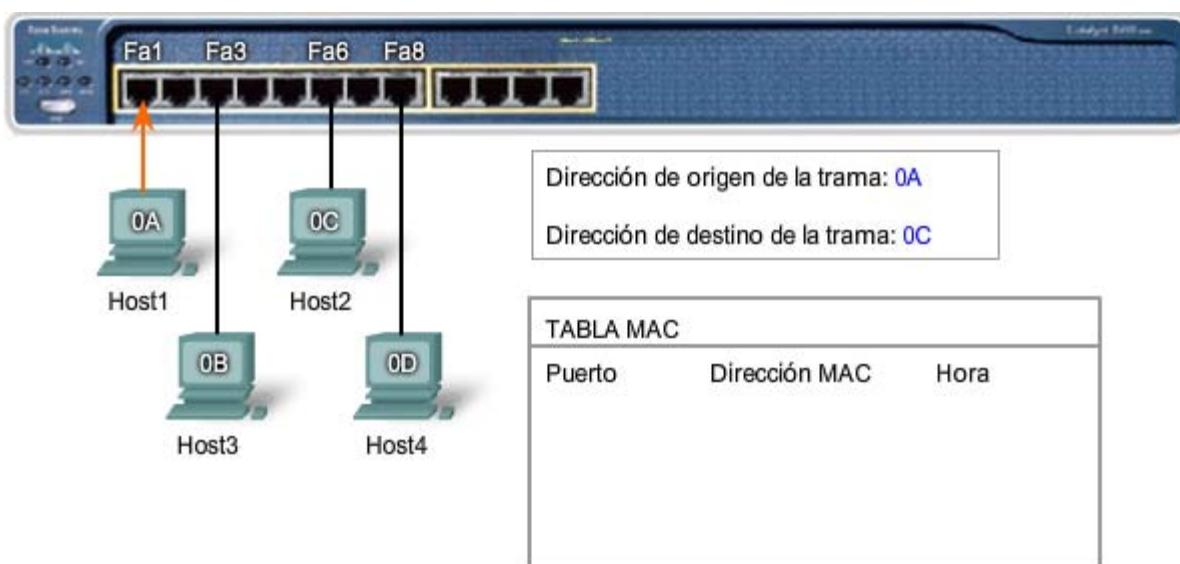
Filtrado

En algunos casos, la trama no se reenvía. Este proceso se denomina filtrado de la trama. Uno de los usos del filtrado ya se describió: un switch no reenvía una trama al mismo puerto en el que llega. El switch también descartará una trama corrupta. Si una trama no aprueba la verificación CRC, dicha trama se descarta. Otra razón por la que una trama se filtra es por motivos de seguridad. Un switch tiene configuraciones de seguridad para bloquear tramas hacia o desde direcciones MAC selectivas o puertos específicos.

Funcionamiento del switch



Al iniciar el switch, la tabla de direcciones MAC está vacía.



El Host1 envía datos al Host2. La trama enviada contiene una dirección MAC de origen y una dirección MAC de destino.



Dirección de origen de la trama: 0A

Dirección de destino de la trama: 0C

TABLA MAC

| Puerto | Dirección MAC | Hora |
|--------|---------------|----------|
| Fa1 | 0A | 11:25:11 |

Aprendizaje

El switch lee la dirección MAC de origen, 0A, de la trama recibida en el puerto Fa1 y la almacena en la tabla de direcciones MAC para utilizarla en el reenvío de tramas al Host1.



Dirección de origen de la trama: 0A

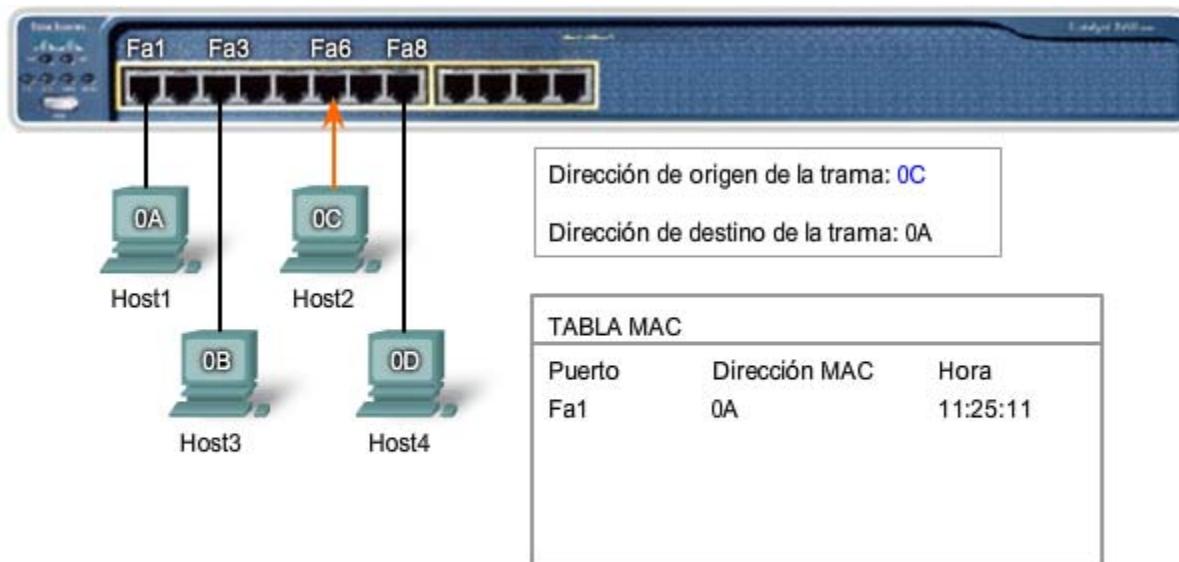
Dirección de destino de la trama: 0C

TABLA MAC

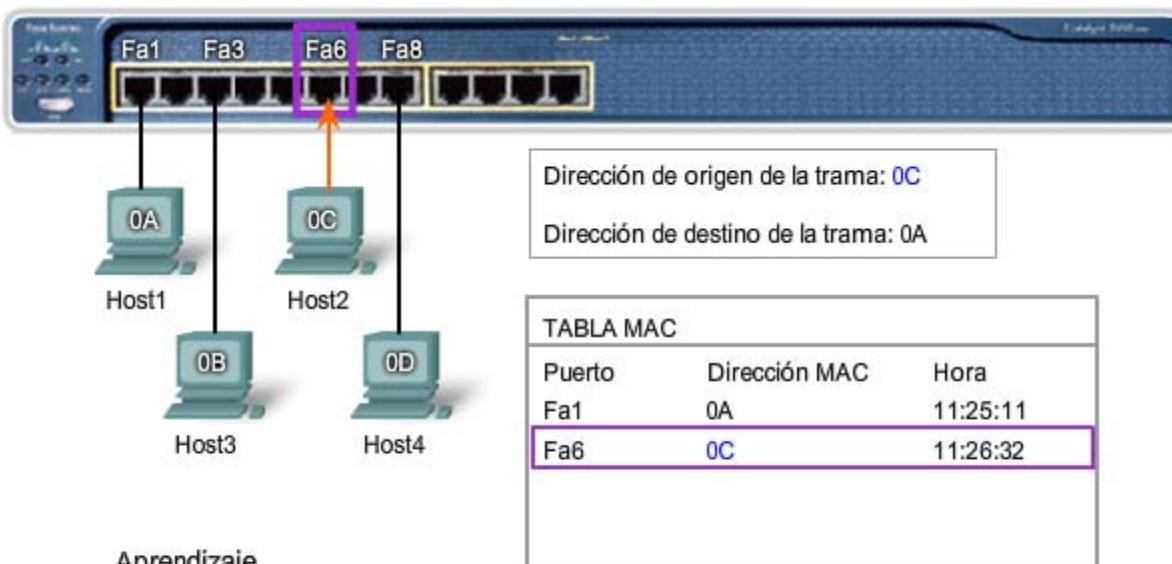
| Puerto | Dirección MAC | Hora |
|--------|---------------|----------|
| Fa1 | 0A | 11:25:11 |
| Fa3 | 0C | ? |

Flooding

La dirección MAC de destino, 0C, no está en la tabla MAC. El switch inunda la trama desde todos los puertos excepto Fa1, el puerto del emisor. Host3 y Host4 la reciben, pero la dirección que está en la trama no coincide con sus direcciones MAC. Descartan la trama. La dirección MAC de destino en la trama coincide con Host2 y éste acepta la trama.

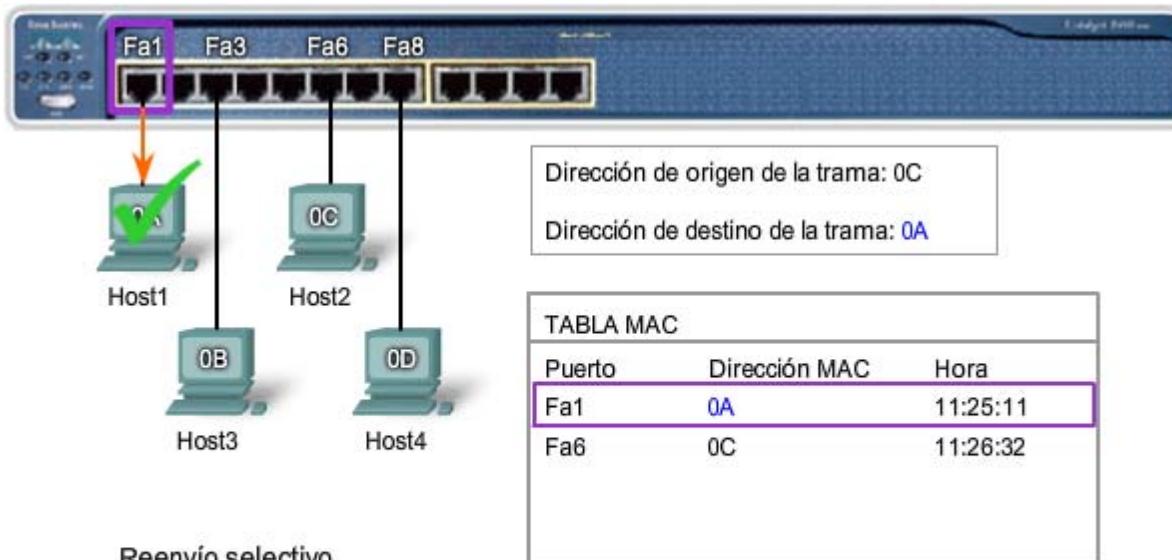


Host2 le envía a Host1 una trama que contiene una respuesta. La dirección de origen en la trama es la dirección MAC de Host2. La dirección de destino en la trama coincide con la dirección MAC de Host1.



Aprendizaje

El switch lee la dirección MAC de origen, 0C, de la trama recibida en el puerto Fa6 y la almacena en la tabla de direcciones MAC para utilizarla en el reenvío de tramas a Host2.



La dirección MAC de destino, 0A, está en la tabla de direcciones MAC. El switch envía selectivamente la trama sólo desde el puerto Fa1. La dirección MAC de destino en la trama coincide con la dirección MAC de Host1. Host 1 acepta la trama.

9.7 ADDRESS RESOLUTION PROTOCOL (ARP)

9.7.1 El proceso ARP: Mapeo de direcciones IP a direcciones MAC

El protocolo ARP ofrece dos funciones básicas:

- Resolución de direcciones Ipv4 a direcciones MAC.
- Mantenimiento de una caché de las asignaciones.

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 lo encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de Enlace de datos que se mapea 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 tiene un par de valores: una dirección IP y 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. La tabla ARP almacena el mapeo de los dispositivos de la LAN local en la memoria caché.

Para comenzar el proceso, un nodo transmisor intenta localizar en la tabla ARP la dirección MAC mapeada a un destino Ipv4. Si este mapa está almacenado en la tabla, el nodo utiliza la dirección MAC como la MAC de destino en la trama que encapsula el paquete Ipv4. La trama se codifica entonces en los medios de la red.

Mantenimiento de una 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.

Otra manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud de ARP. El ARP envía un broadcast de Capa 2 a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud de ARP con la dirección IP del host de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya responde enviando un paquete de respuesta de ARP al emisor como una trama unicast. Esta respuesta se utiliza entonces para crear una entrada nueva en la tabla ARP.

Estas entradas dinámicas de la tabla MAC tienen una marca horaria similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un determinado dispositivo antes de que venza la marca horaria, la entrada para este dispositivo se elimina de la tabla ARP.

Además, pueden ingresarse entradas estáticas de mapas en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP caducan cuando pasa el tiempo y deben eliminarse en forma manual.

Creación de la trama

¿Qué hace un nodo cuando debe crear una trama y la caché ARP no contiene un mapa de una dirección IP hacia una dirección MAC de destino? 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.

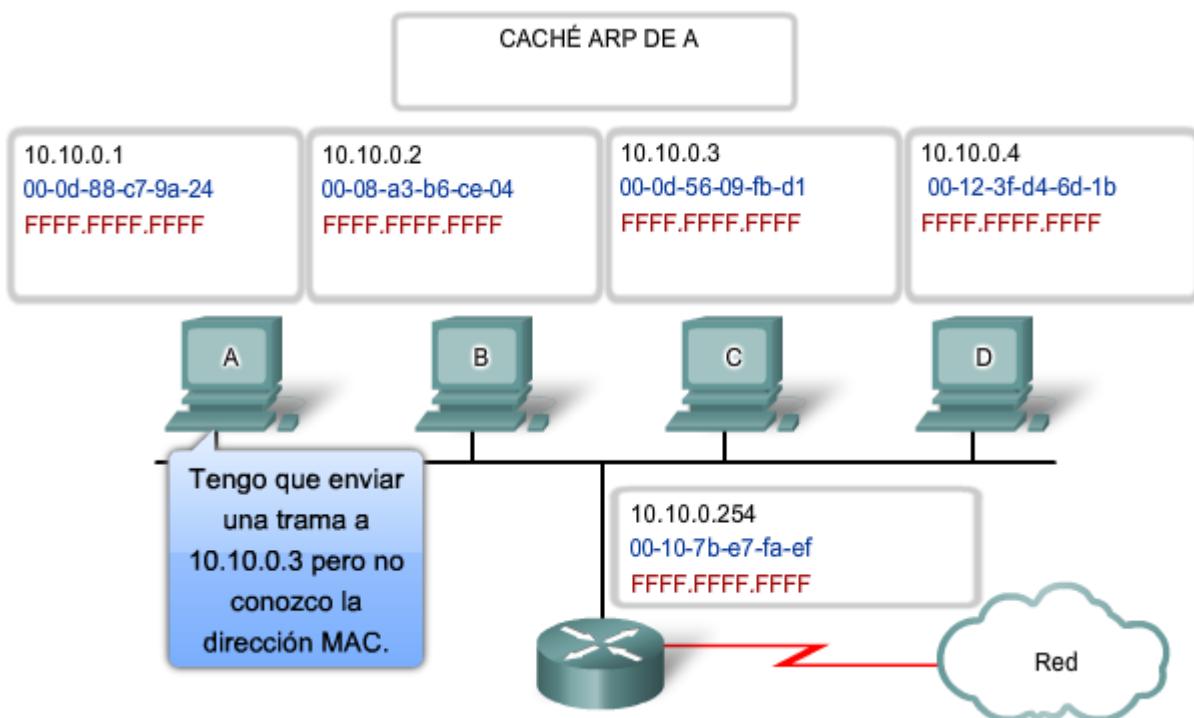
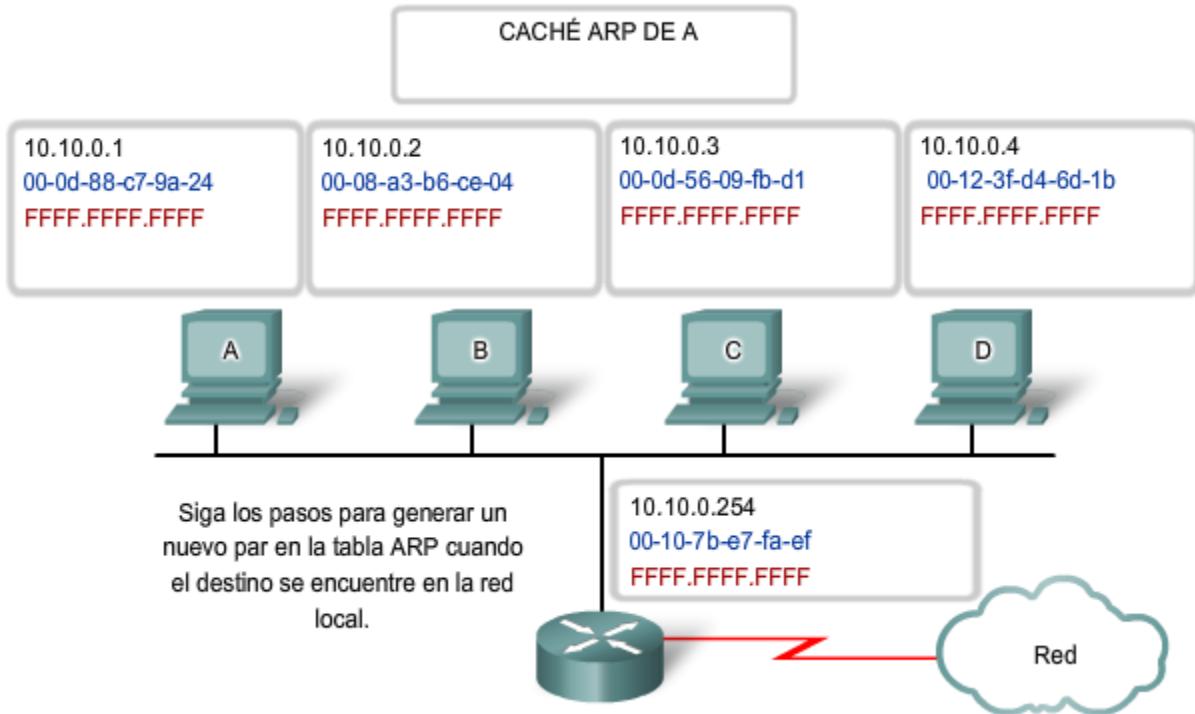
Los procesos ARP envían entonces un paquete de solicitud de ARP para descubrir la dirección MAC del dispositivo de destino de la red local. Si un dispositivo que recibe la solicitud tiene la dirección IP de destino, responde con una respuesta ARP. Se crea un mapa en la tabla ARP. Los paquetes para esa dirección Ipv4 pueden ahora encapsularse en tramas.

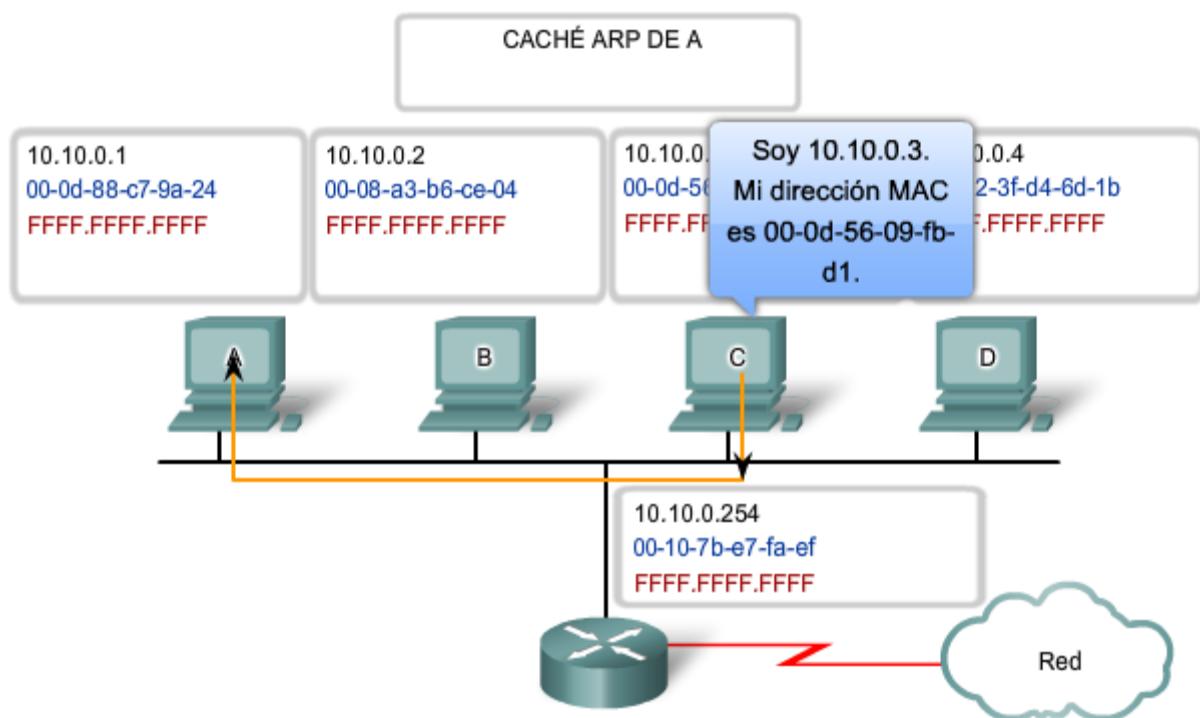
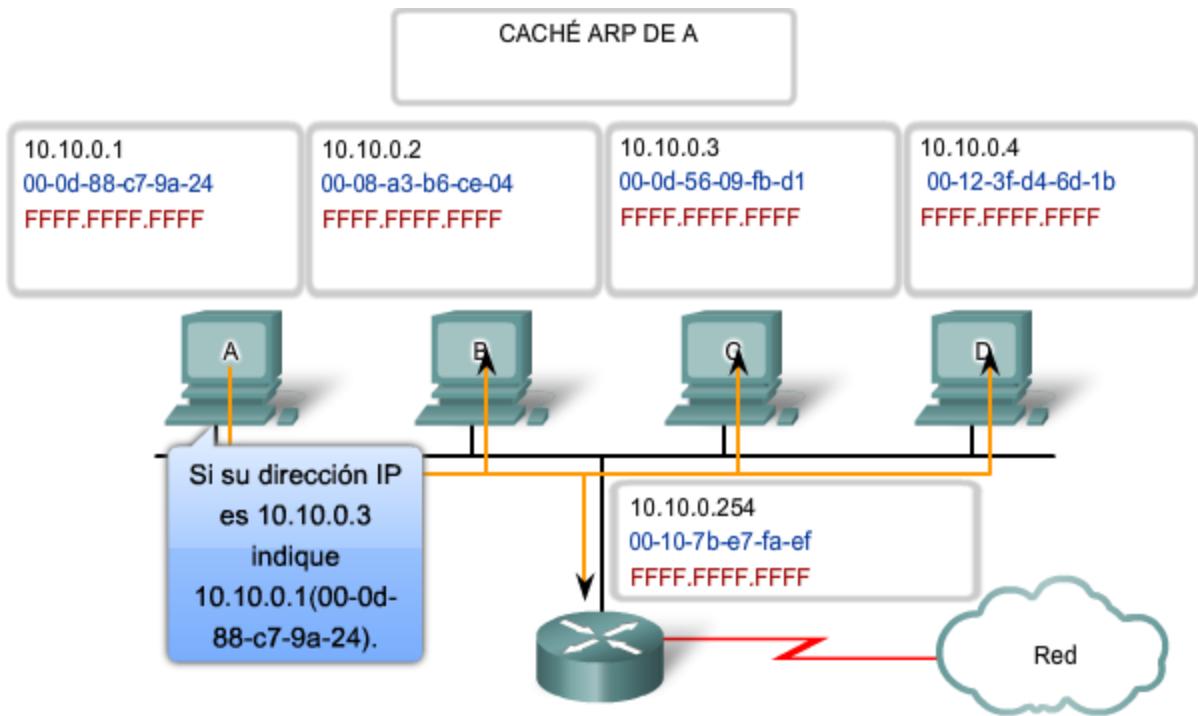
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no puede crearse una trama. Esta falla de encapsulación se informa a las capas superiores del dispositivo. Si el dispositivo es un dispositivo intermediario, como por ejemplo, un router, las capas superiores pueden optar por responder al host de origen con un error en un paquete ICMPv4.

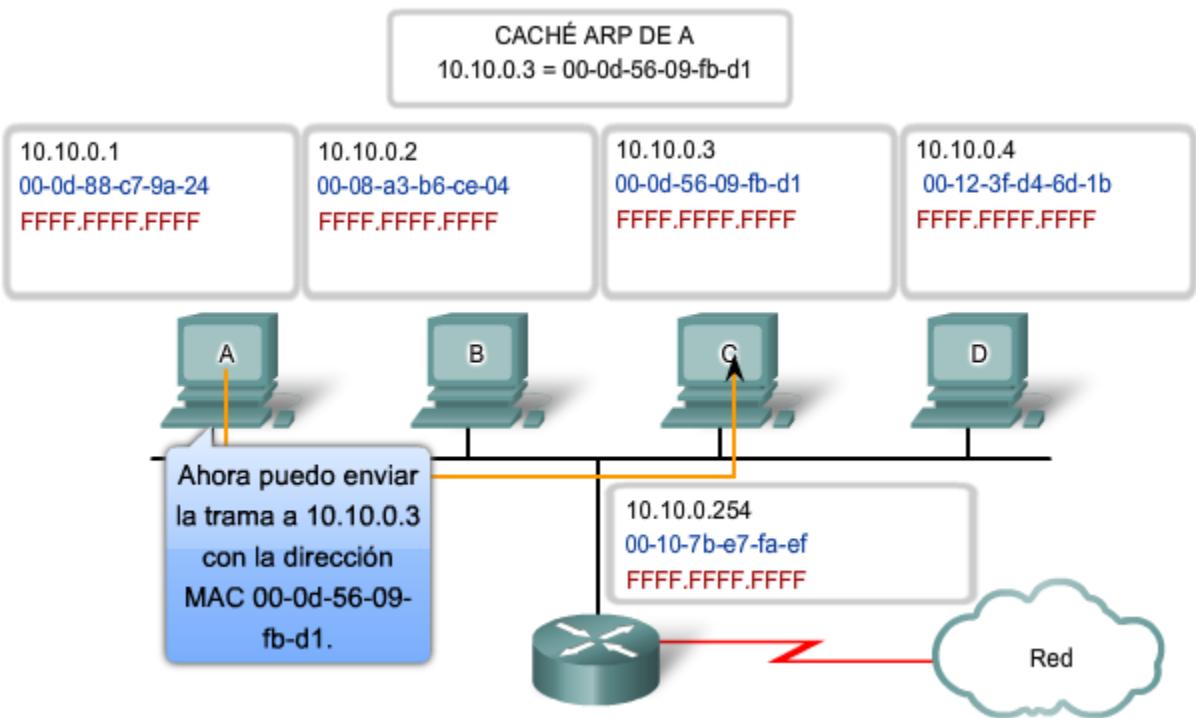
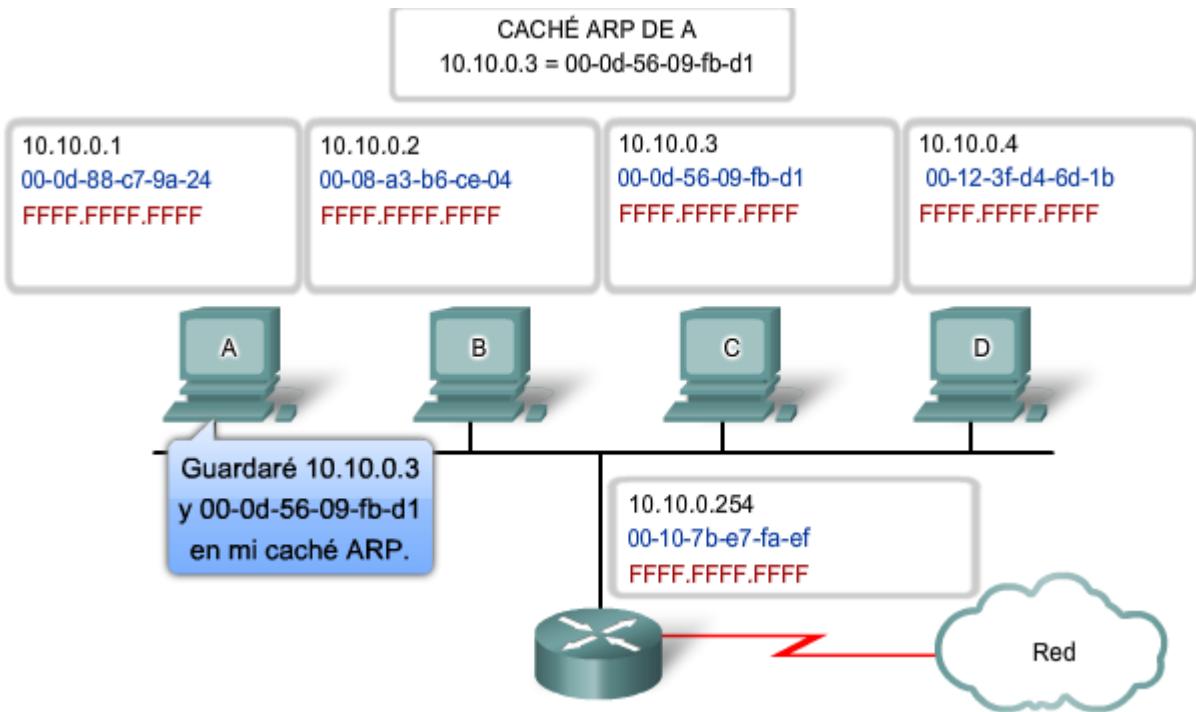
Haga clic en los números de los pasos que aparecen en la figura para ver el proceso que se utiliza para obtener la dirección MAC de un nodo de la red física local.

En la práctica de laboratorio, utilizará Wireshark para observar las solicitudes y respuestas de ARP en toda una red.

Proceso ARP — Asignación de direcciones







9.7.2 El proceso ARP: Destinos fuera de la red local

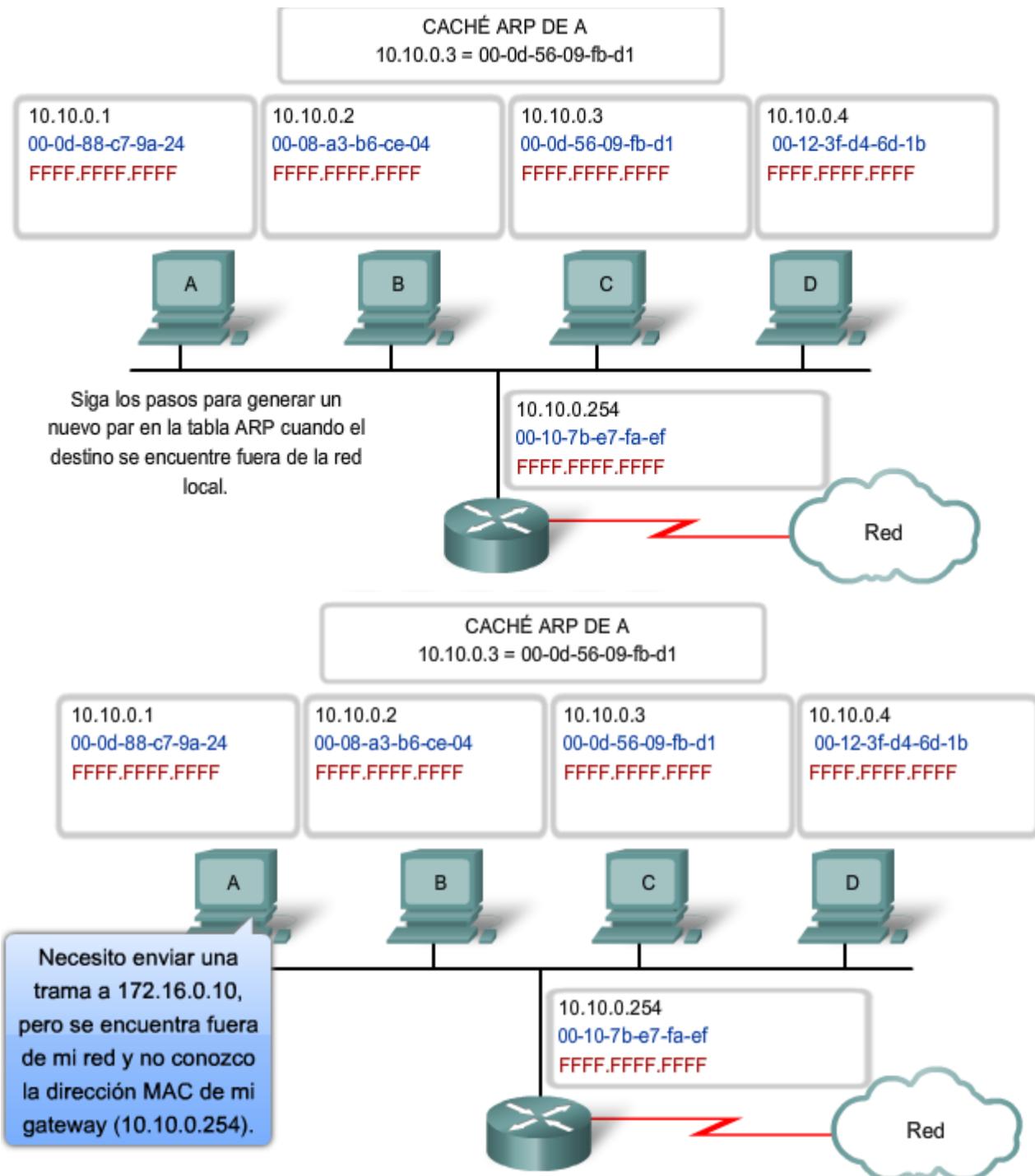
Todas las tramas deben enviarse a un nodo de un segmento de la red local. Si el host Ipv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

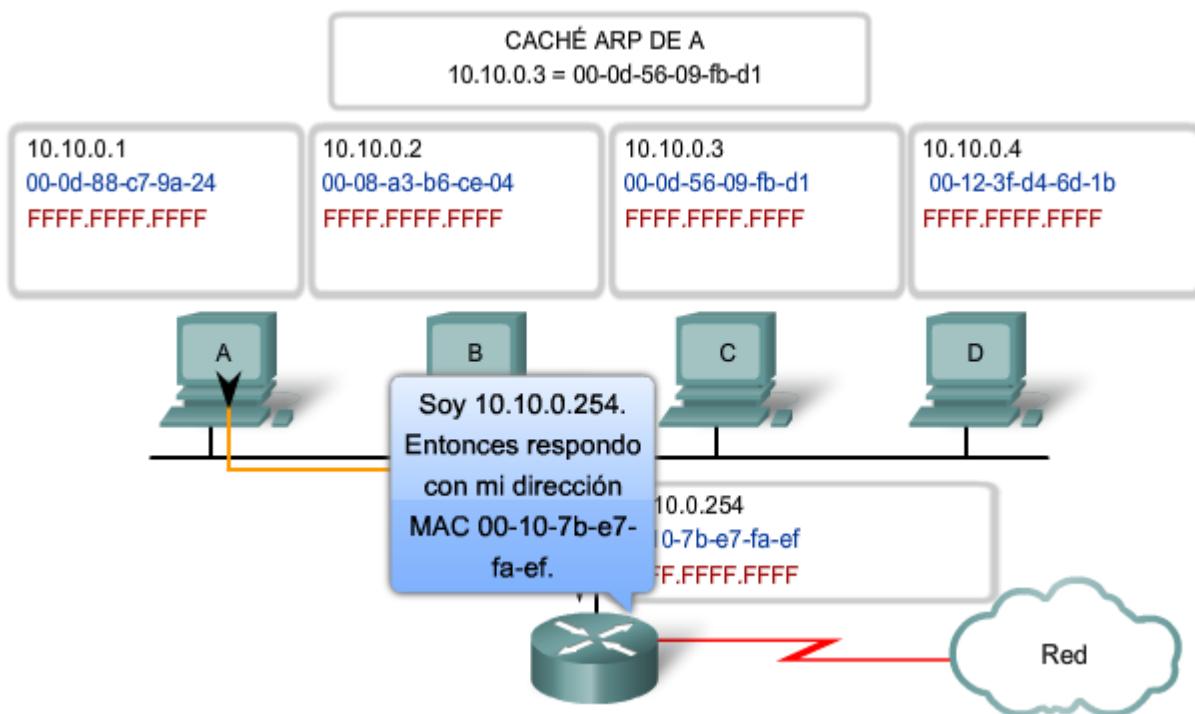
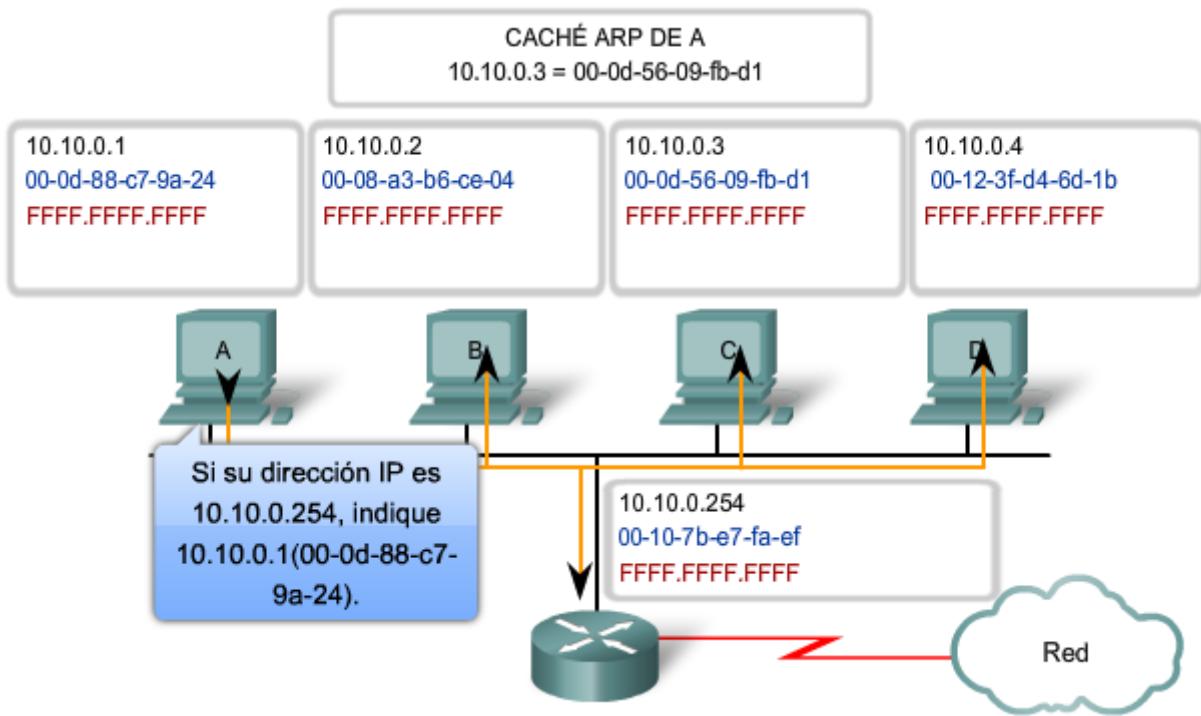
Si el host Ipv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router que es el 380ersión o el siguiente salto que se utiliza para llegar a dicho destino. El nodo de origen utilizará la dirección MAC del 380ersión como dirección de destino para las tramas que contengan un paquete Ipv4 dirigido a hosts que se encuentren en otras redes.

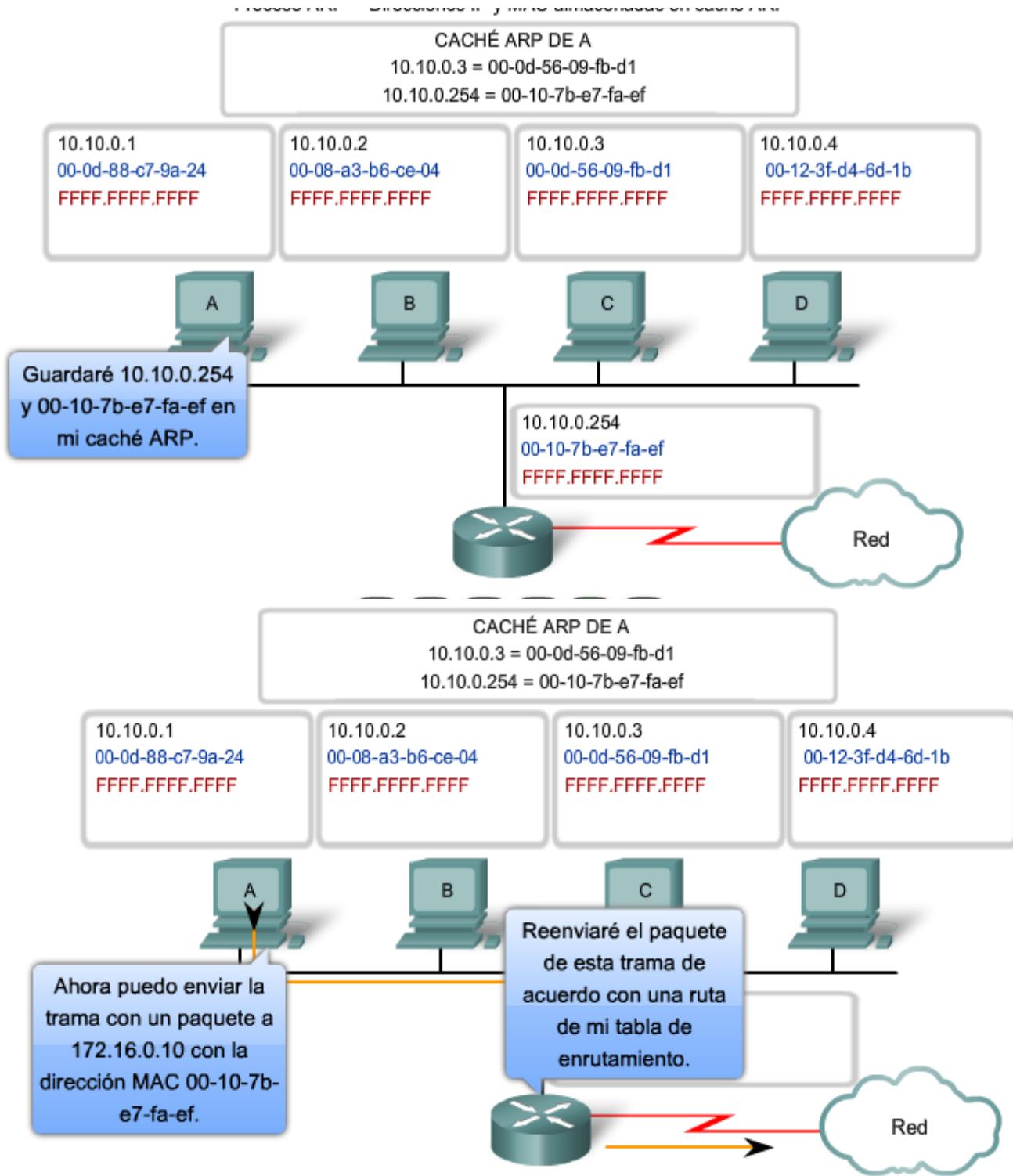
La dirección de 381ersión de la interfaz del router se almacena en la configuración Ipv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de Capa 3. Si el 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 381ersión.

En caso de que la entrada de 381ersión 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.

Haga clic en los números de pasos que aparecen en la figura para ver el proceso que se utiliza para obtener la dirección MAC del 381ersión.







ARP proxy

Hay ocasiones en las que un host puede enviar una solicitud de ARP con el objetivo de mapear una dirección IPv4 fuera del alcance de la red local. En estos casos, el dispositivo envía solicitudes de ARP para direcciones IPv4 que no se encuentran en la red local en vez de solicitar la dirección MAC asociada a la dirección IPv4 del destinatario. Para proporcionar una dirección MAC para estos hosts, una interfaz de router puede utilizar un ARP proxy para responder en nombre de estos hosts remotos. Esto significa que la caché de ARP del dispositivo solicitante contendrá la dirección MAC del destinatario mapeada a cualquier dirección IP que no se encuentre en la red local. Con el proxy ARP, una interfaz de

router actúa como si fuera el host con la dirección Ipv4 solicitada por la solicitud de ARP. Al “simular” su identidad, el router acepta la responsabilidad de enrutar paquetes al destino “real”.

Uno de los usos que se le da a dicho proceso es cuando una implementación más antigua de Ipv4 no puede determinar si el host de destino se encuentra en la misma red lógica que el origen. En estas implementaciones, el ARP siempre envía solicitudes de ARP para la dirección Ipv4 de destino. Si el ARP proxy se desactiva en la interfaz del router, estos hosts no pueden comunicarse fuera de la red local.

Otro caso en el que se utiliza el ARP proxy es cuando un host cree que está directamente conectado a la misma red lógica que el host de destino. Esto ocurre generalmente cuando un host se configura con una máscara inapropiada.

Tal como se muestra en la figura, el Host A se configuró inapropiadamente con una máscara de subred /16. Este host cree que está directamente conectado a la red 172.16.0.0 /16 en vez de a la subred 172.16.10.0 /24.

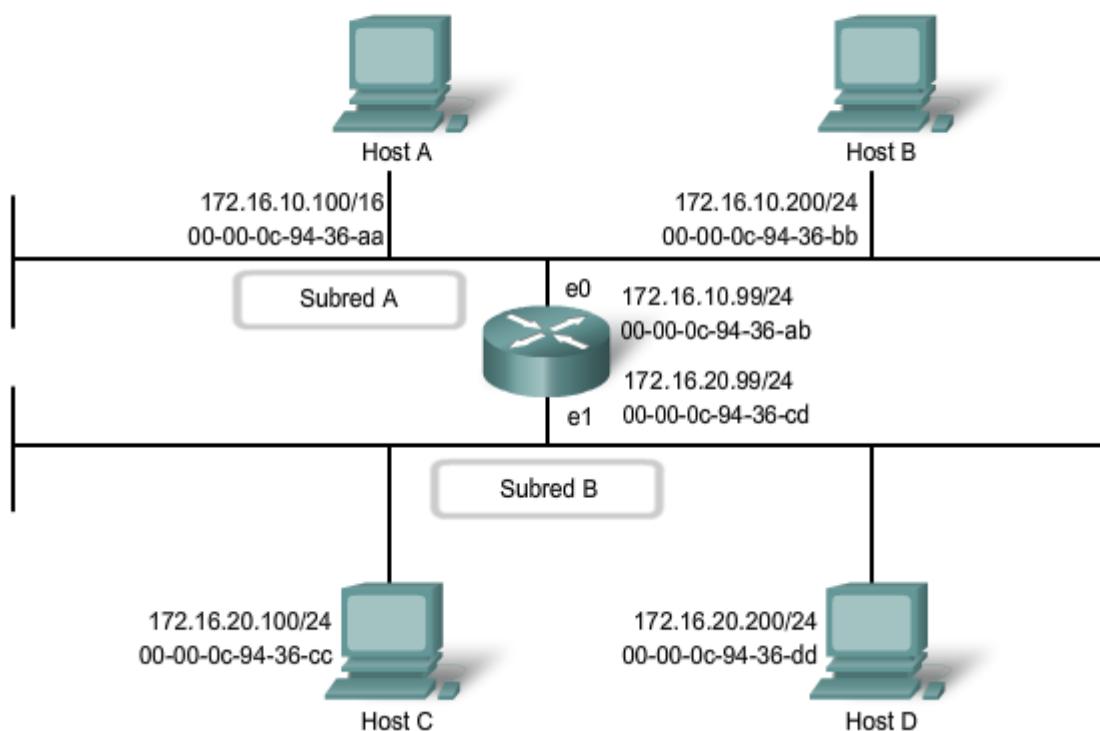
Cuando se intenta comunicar con cualquier host Ipv4 en el intervalo de 172.16.0.1 a 172.16.255.254, el Host A enviará una solicitud de ARP para esa dirección Ipv4. El router puede utilizar un ARP proxy para responder a las solicitudes de dirección Ipv4 del Host C (172.16.20.100) y el Host D (172.16.20.200). Como resultado, el Host A tendrá entradas para estas direcciones mapeadas a la dirección MAC de la interfaz e0 del router (00-00-0c-94-36-ab).

Otro uso que se le puede dar al ARP proxy es cuando un host no está configurado con una máscara de subred /24 por defecto. El ARP proxy puede ayudar a que los dispositivos de una red alcancen subredes remotas sin la necesidad de configurar el enrutamiento o una máscara de subred /24 por defecto.

Por defecto, los routers Cisco poseen un proxy ARP habilitado en las interfaces LAN.

<http://www.cisco.com/warp/public/105/5.html>

ARP proxy permite que el router responda por el host remoto

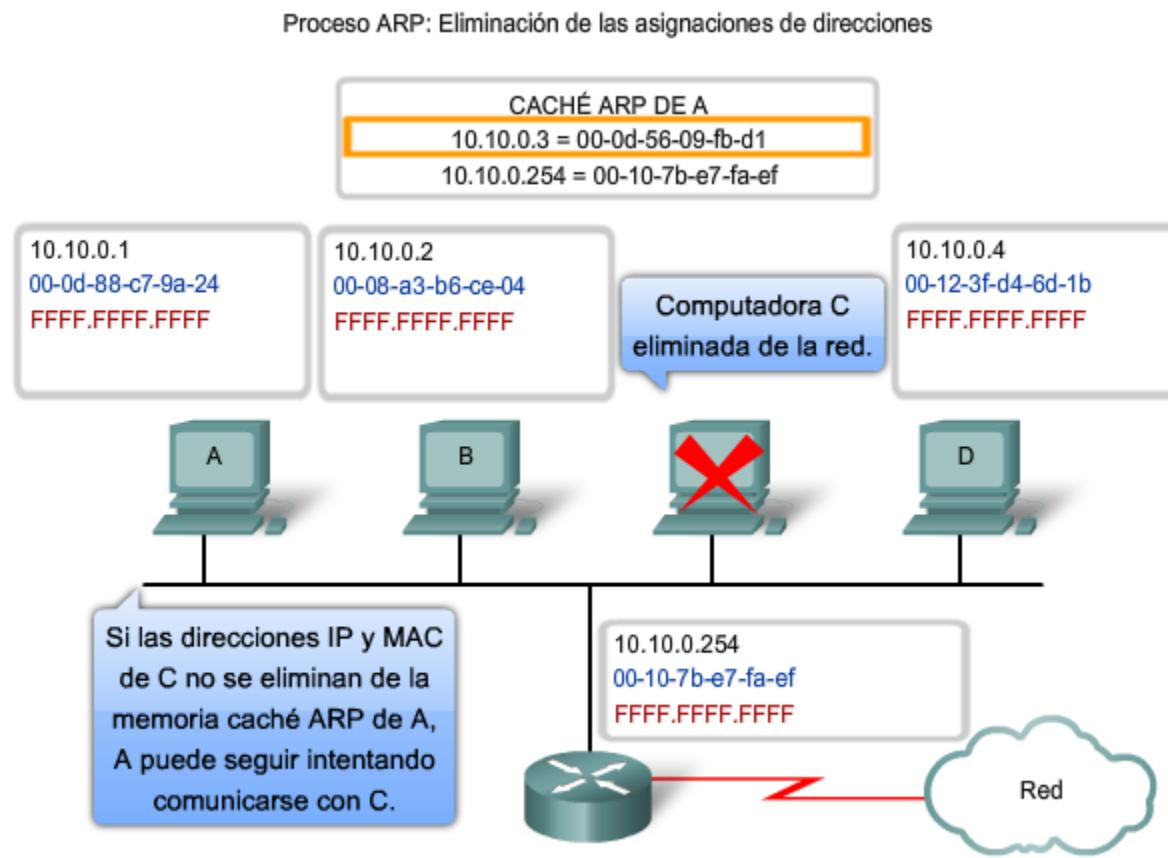


9.7.3 El proceso ARP: Eliminación de mapeo de direcciones

Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo específico. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. Por ejemplo, algunos sistemas operativos de Windows almacenan las entradas de caché de ARP durante 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 ARP debe ocurrir nuevamente para ingresar el mapa en la tabla ARP.

En la práctica de laboratorio para esta sección, utilizará el comando arp para visualizar y borrar los contenidos de la caché de ARP de una computadora. Observe que este comando, a pesar de su nombre, no invoca en absoluto la ejecución del Protocolo de resolución de direcciones. Sólo se utiliza para mostrar, agregar o eliminar 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.



9.3.4 Broadcasts de ARP: Problemas

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

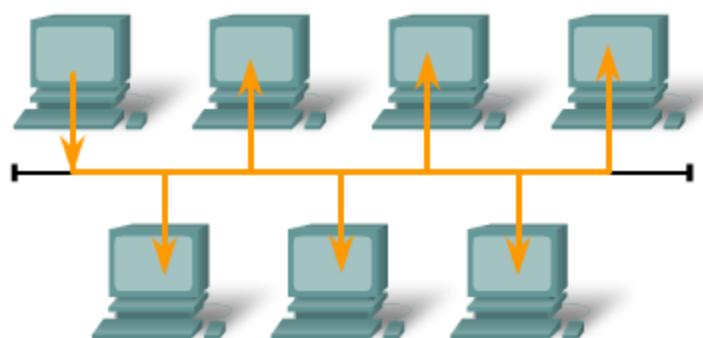
En algunos casos, la utilización del ARP puede ocasionar un riesgo potencial de seguridad. La suplantación ARP o el envenenamiento ARP es una técnica que utiliza un atacante para introducir una asociación de direcciones MAC incorrecta en una red emitiendo solicitudes de ARP falsas. Un atacante falsifica la dirección MAC de un dispositivo y a continuación pueden enviarse tramas al destino equivocado.

La configuración manual de asociaciones ARP estáticas es una manera de evitar el ARP spoofing. Las direcciones MAC autorizadas pueden configurarse en algunos dispositivos de red para que limiten el acceso a la red para sólo los dispositivos indicados.

Problemas de ARP:

- Broadcasts, sobrecarga en la
- seguridad de los medios

Medios compartidos (acceso múltiple)



Un mensaje ARP falso puede proporcionar una dirección MAC incorrecta que luego robará las tramas que utilicen esa dirección (denominado suplantación de identidad).

| Ethernet | | | | | |
|-----------|----------------------|---------------------|------|-----------|------------------------------------|
| 8 | 6 | 6 | 2 | 46 a 1500 | 4 |
| Preámbulo | Dirección de destino | Dirección de origen | Tipo | Datos | Secuencia de verificación de trama |

9.9 RESUMEN DEL CAPITULO

9.9.1 Resumen y revisión

Ethernet es un protocolo de acceso de red TCP/IP efectivo y ampliamente utilizado. Su estructura de trama común se implementó a través de una variedad de tecnologías de medios, tanto de cobre como de fibra, lo que la convierten en el protocolo LAN que más se utiliza en la actualidad.

Como implementación de los estándares IEEE 802.2/3, la trama de Ethernet brinda direccionamiento MAC y verificación de errores. Dado que era una tecnología de medios compartidos, la Ethernet inicial debía aplicar un mecanismo CSMA/CD para administrar la utilización de los medios por parte de dispositivos múltiples. El reemplazo de hubs por switches en la red local redujo las probabilidades de colisiones de tramas en enlaces half-duplex. Sin embargo, las versiones actuales y futuras funcionan inherentemente como enlaces de comunicaciones full-duplex y no necesitan administrar la contención de medios con tanta precisión.

El direccionamiento de Capa 2 provisto por Ethernet admite comunicaciones unicast, multicast y broadcast. La Ethernet utiliza el Protocolo de resolución de direcciones para determinar las direcciones MAC de los destinos y mapearlas con direcciones de capa de Red conocidas.

En este capítulo, aprendió a:

- Identificar las características básicas de los medios de red utilizados en Ethernet.
- Describir las características de la capa Física y la capa de Enlace de datos de Ethernet.
- Describir el funcionamiento y las características del método de control de acceso al medio utilizado por el protocolo Ethernet.
- Explicar la importancia del direccionamiento de Capa 2 utilizado para la transmisión de datos y determinar cómo los diferentes tipos de direccionamiento afectan el funcionamiento y rendimiento de la red.
- Comparar y contrastar la aplicación y los beneficios de la utilización de switches Ethernet en una LAN con la utilización de hubs.
- Explicar el proceso de ARP.

10 – PLANIFICACION Y CABLEADO DE REDES

10.0 INTRODUCCION DEL CAPITULO

10.0.1 Introducción del capítulo

Antes de utilizar un teléfono IP, acceder a mensajería instantánea o realizar otras interacciones a través de una red de datos, debemos conectar dispositivos intermediarios y finales mediante conexiones inalámbricas o de cable para formar una red que funcione. Esta red será la que soporte nuestra comunicación en la red humana.

Hasta esta etapa del curso, hemos considerado los servicios que una red de datos puede proporcionar a la red humana, examinando las características de cada capa del modelo OSI y las operaciones de los protocolos TCP/IP, observado en detalle a Ethernet, una tecnología LAN universal. El siguiente paso es aprender cómo reunir todos estos elementos para formar una red que funcione.

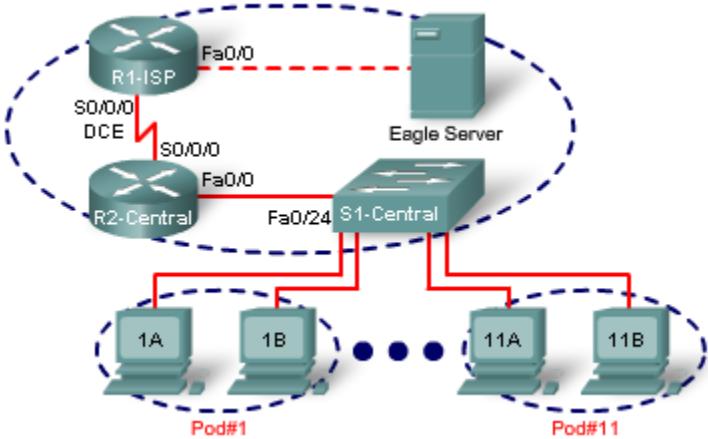
En este capítulo, examinaremos diferentes medios y los distintos roles que desempeñan en torno a los dispositivos que conectan. Identificará los cables necesarios para lograr conexiones LAN y WAN exitosas y aprenderá a utilizar conexiones de administración de dispositivos.

Se presentará la selección de dispositivos y el diseño de un esquema de direccionamiento de red, y luego se aplicarán en los laboratorios de red.

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

- Identificar los medios de red básicos que se requieren para realizar una conexión LAN (Red de área local).
- Identificar los tipos de conexiones para conexiones de dispositivos finales e intermedios en una LAN.
- Identificar las configuraciones de los diagramas de pines para cables de conexión directa y de conexión cruzada.
- Identificar los diferentes tipos de cableado, estándares y puertos utilizados para las conexiones WAN (Red de área extensa).
- Definir la función de las conexiones para la administración de dispositivos cuando se utiliza un equipo de Cisco.
- Diseñar un esquema de direccionamiento para una internetwork y asignar rangos para los hosts, los dispositivos de red y la interfaz del router.
- Indicar las similitudes y diferencias de la importancia de los diseños de red.



Planificación y cableado de una red

10.1 LAN: REALIZACION DE LA CONEXIÓN FISICA

10.1.1 Selección de un dispositivo LAN adecuado

En este curso, las interfaces Ethernet que coincidan con la tecnología de los switches en el centro de la LAN determinan la selección del router que se debe utilizar. Es importante destacar que los routers ofrecen varios servicios y características para la LAN. Estos servicios y características se tratan en los cursos más avanzados.

Cada LAN contará con un router que servirá de conexión para conectar la LAN a otras redes. Dentro de la LAN habrá uno o más hubs o switches para conectar los dispositivos finales a la LAN.

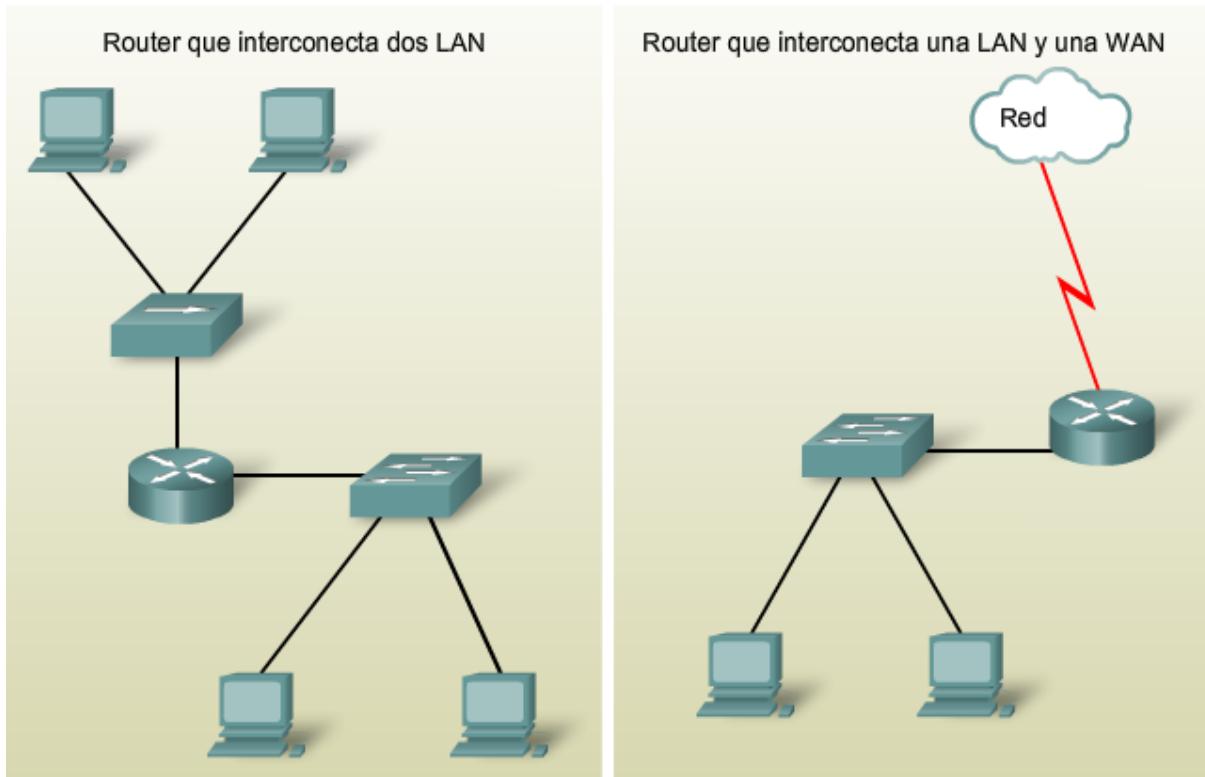
Dispositivos de internetwork

Los routers son los dispositivos principales utilizados para interconectar redes. Cada puerto de un router se conecta a una red diferente y realiza el enrutamiento de los paquetes entre las redes. Los routers tienen la capacidad de dividir dominios de broadcast y dominios de colisiones.

También pueden utilizarse para interconectar redes que utilizan diferentes tecnologías. Los routers pueden tener interfaces LAN y WAN.

Las interfaces LAN del router permiten a los routers conectarse a los medios LAN. Para esto generalmente se utiliza un cableado de UTP (Par trenzado no blindado), pero se pueden agregar módulos con fibra óptica. Según la serie o el modelo del router, puede haber diferentes tipos de interfaces para la conexión del cableado WAN y LAN.

Conexión de internetwork con un router



Dispositivos de intranetwork

Para crear una LAN, necesitamos seleccionar los dispositivos adecuados para conectar el dispositivo final a la red. Los dos dispositivos más comúnmente utilizados son los hubs y los switches.

Hub

Un hub recibe una señal, la regenera y la envía a todos los puertos. El uso de hubs crea un bus lógico. Esto significa que la LAN utiliza medios de acceso múltiple. Los puertos utilizan un método de ancho de banda compartido y a menudo disminuyen su rendimiento en la LAN debido a las colisiones y a la recuperación. Si bien se pueden interconectar múltiples hubs, éstos permanecen como un único dominio de colisiones.

Los hubs son más económicos que los switches. Un hub generalmente se elige como dispositivo intermediario dentro de una LAN muy pequeña que requiera requisitos de velocidad de transmisión (throughput) lenta o cuando los recursos

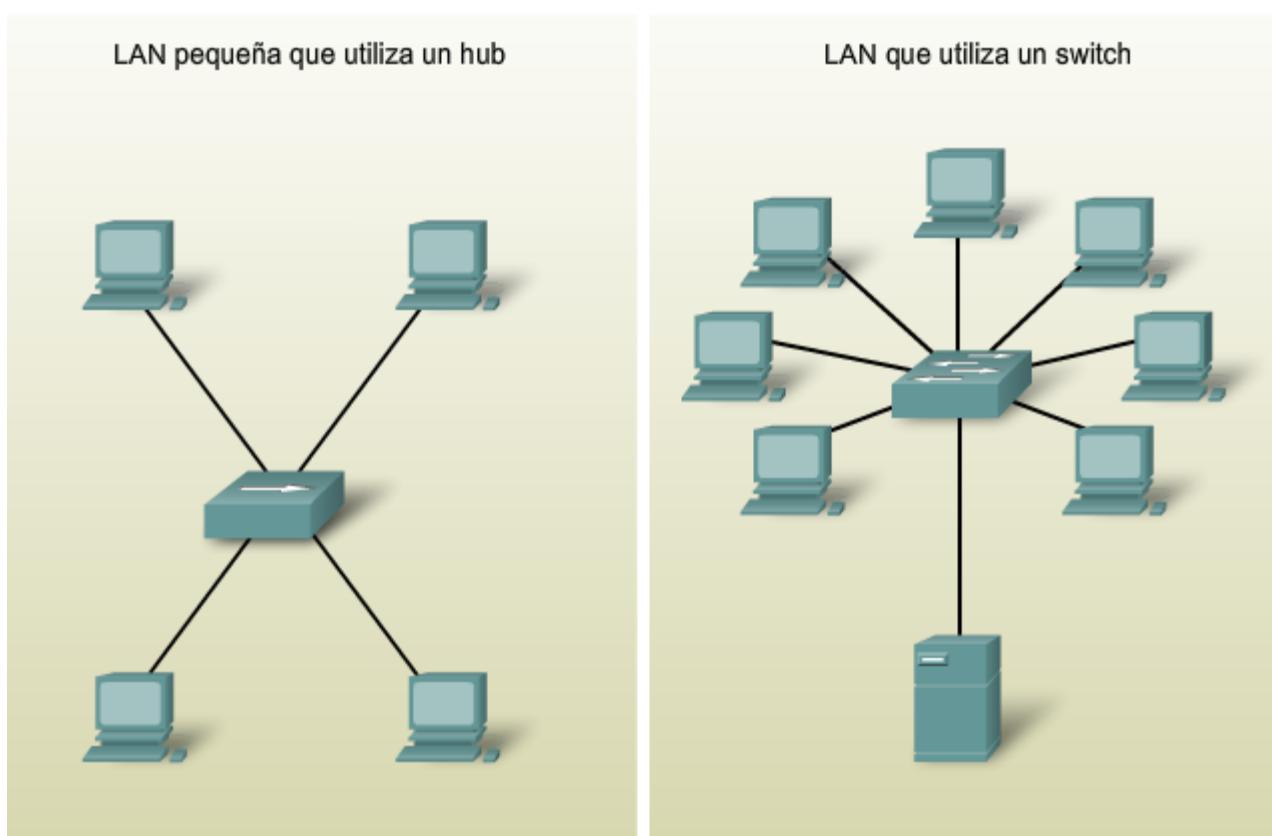
económicos sean limitados.

Switch

Un switch recibe una trama y regenera cada bit de la trama en el puerto de destino adecuado. Este dispositivo se utiliza para segmentar una red en múltiples dominios de colisiones. A diferencia del hub, un switch reduce las colisiones en una LAN. Cada puerto del switch crea un dominio de colisiones individual. Esto crea una topología lógica punto a punto en el dispositivo de cada puerto. Además, un switch proporciona ancho de banda dedicado en cada puerto y así aumenta el rendimiento de una LAN. El switch de una LAN también puede utilizarse para interconectar segmentos de red de diferentes velocidades.

Generalmente, los switches se eligen para conectar dispositivos a una LAN. Si bien un switch es más costoso que un hub, resulta económico al considerar su confiabilidad y rendimiento mejorados.

Existe una variedad de switches disponibles con distintas características que permiten la interconexión de múltiples computadoras en el entorno empresarial típico de una LAN.



10.1.2 Factores de selección de dispositivos

Para cumplir con los requisitos de usuario, se debe planificar y diseñar una LAN. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación.

Se deben considerar varios factores al seleccionar un dispositivo para una LAN particular. Estos factores incluyen, entre otros:

- Costo

- Velocidad y tipos de puertos/interfaces
- Posibilidad de expansión
- Facilidad de administración
- Características y servicios adicionales

Factores que se deben tener en cuenta al momento de elegir un dispositivo



Factores que se deben considerar en la elección de un switch

Si bien existen varios factores que deben considerarse al seleccionar un switch, el próximo tema analizará dos de ellos: las características de la interfaz y el costo.

Costo

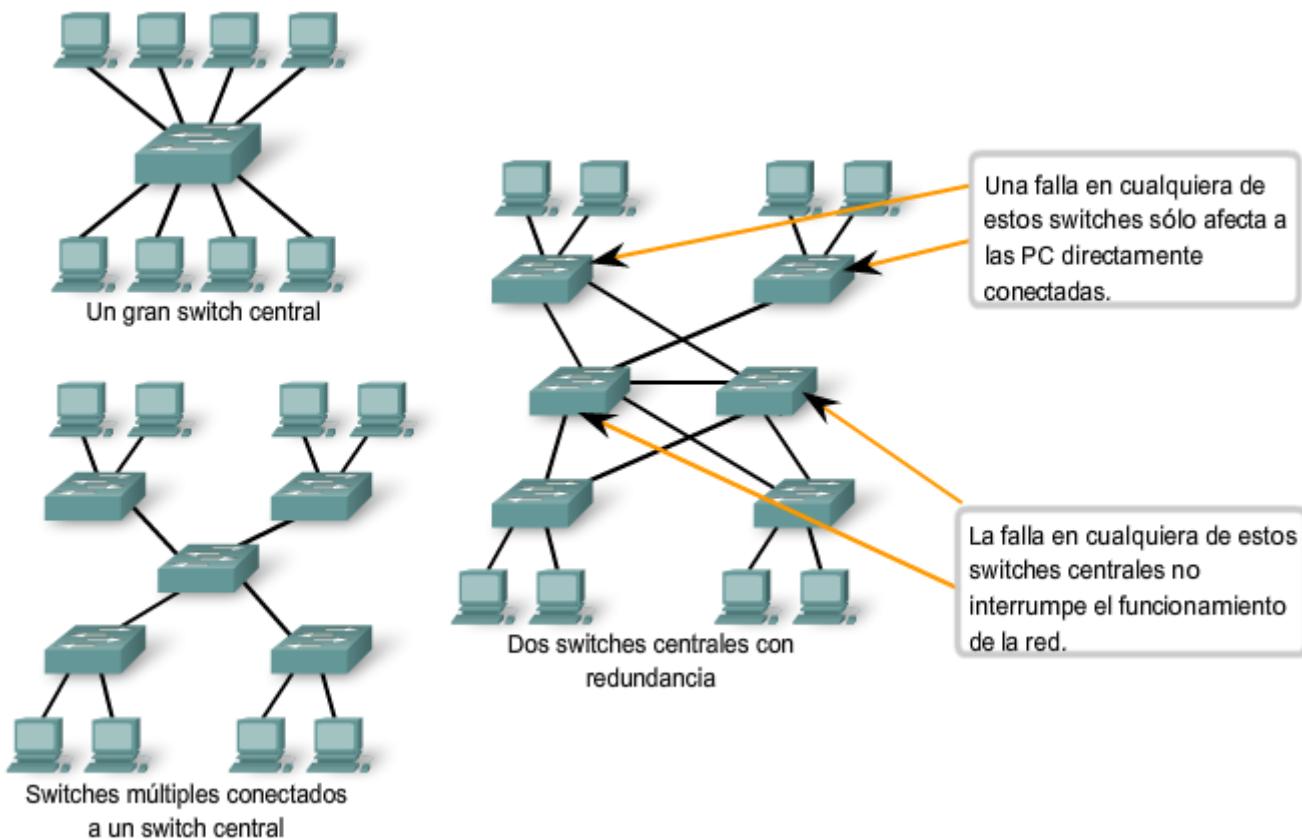
El costo de un switch se determina según sus capacidades y características. La capacidad del switch incluye el número y los tipos de puertos disponibles además de la velocidad de conmutación. Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y las tecnologías opcionales de conmutación avanzadas.

Al utilizar un simple cálculo de “costo por puerto”, en principio puede parecer que la mejor opción es implementar un switch grande en una ubicación central. Sin embargo, este aparente ahorro en los costos puede contrarrestarse por el gasto generado por las longitudes de cable más extensas que se necesitan para conectar cada dispositivo de la LAN a un switch. Esta opción debe compararse con el costo generado al implementar una cantidad de switches más pequeños conectados a un switch central con una cantidad menor de cables largos.

Otra consideración en los costos es cuánto invertir en redundancia. El funcionamiento de toda la red física se ve afectada si existen problemas con un switch central único.

Existen varias formas de proporcionar redundancia. Podemos ofrecer un switch central secundario para que funcione simultáneamente con el switch central primario. También podemos proporcionar cableado adicional para suministrar múltiples interconexiones entre los switches. El objetivo de los sistemas redundantes es permitir que la red física continúe con su funcionamiento incluso si falla uno de los dispositivos.

Factores que determinan la elección del switch LAN



Velocidad y tipos de puertos e interfaces

La necesidad de velocidad está siempre presente en un entorno LAN. Se encuentran disponibles computadoras más nuevas con NIC incorporadas de 10/100/1000 Mbps. La selección de dispositivos de Capa 2 que puedan ajustarse a mayores velocidades permite a la red evolucionar sin reemplazar los dispositivos centrales.

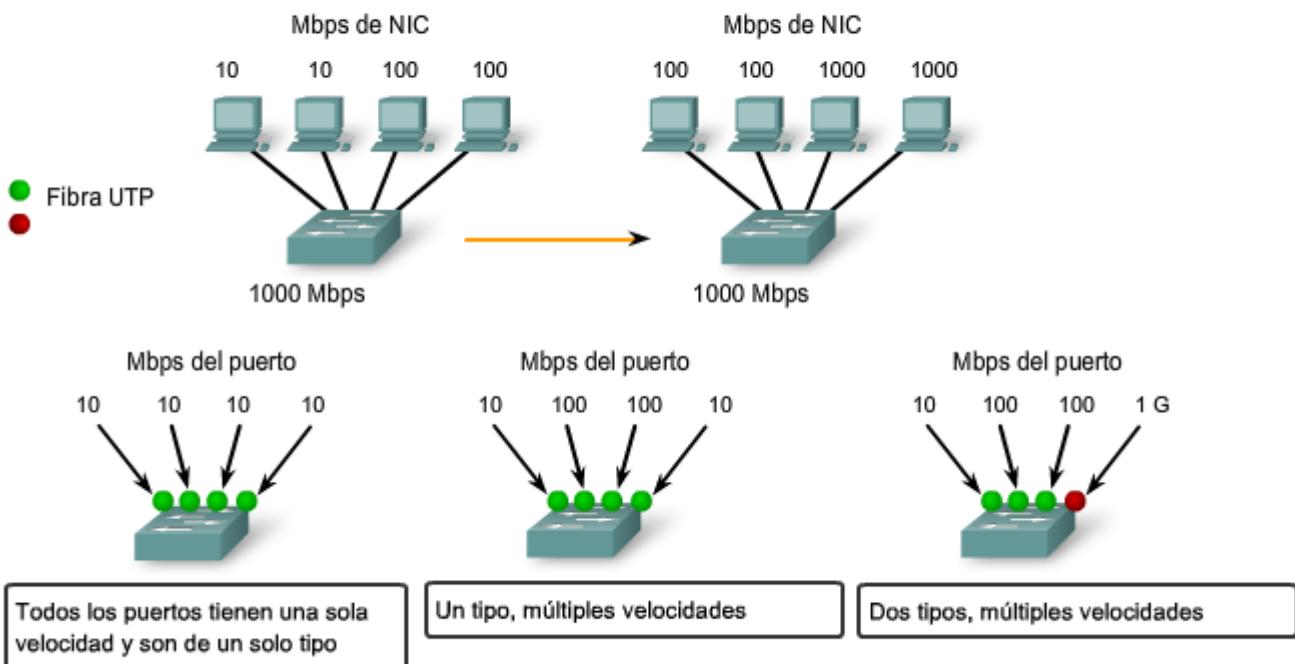
Al seleccionar un switch, es fundamental la elección del número y tipo de puerto. Hágase las siguientes preguntas: ¿Usted compraría un switch con:

- Sólo los puertos suficientes para las necesidades actuales?
- Una combinación de velocidades UTP?
- Dos tipos de puerto, de UTP y de fibra?

Considere cuidadosamente cuántos puertos UTP se necesitarán y cuántos puertos de fibra se necesitarán. Del mismo modo, considere cuántos puertos necesitarán una capacidad de 1 Gbps y cuántos requerirán sólo anchos de banda de 10/100 Mbps. Tenga en cuenta además cuándo necesitará más puertos.

Factores que determinan la elección del switch LAN

Velocidades, tipos y capacidad de expansión de los puertos



Algunos switches se pueden expandir con módulos adicionales para cumplir nuevos requisitos.

Factores para tener en cuenta al elegir un router

Cuando se selecciona un router, deben coincidir las características del mismo con su propósito. Al igual que el switch, también deben considerarse las velocidades, los tipos de interfaz y el costo. Los factores adicionales para elegir un router incluyen:

- Posibilidad de expansión
- Medios
- Características del sistema operativo

Posibilidad de expansión

Los dispositivos de red, como los routers y switches, forman parte tanto de las configuraciones físicas modulares como de las 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. Se debe tener precaución al seleccionar las interfaces y los módulos adecuados para los medios específicos ya que los routers pueden utilizarse para conectar diferentes cantidades y tipos de red.

Características del sistema operativo

Según la versión del sistema operativo, el router puede admitir determinadas características y servicios, como por ejemplo:

- Seguridad
- Calidad de servicio (QoS)

- Voz sobre IP (VoIP)
- Enrutamiento de varios protocolos de capa 3
- Servicios especiales como Traducción de direcciones de red (NAT) y Protocolo de configuración dinámica de host (DHCP)

Para la selección de dispositivos, el presupuesto es un detalle importante a tener en cuenta. Los routers pueden ser costosos según las interfaces y las características necesarias. Los módulos adicionales, como la fibra óptica, pueden aumentar los costos. Los medios utilizados para conectar el router deben admitirse sin necesidad de comprar módulos adicionales. Esto puede mantener los costos en un nivel mínimo.

Routers Cisco



Cada serie de router Cisco brinda capacidad de expansión, admite múltiples tipos de medios y ofrece diversos servicios y funciones de sistema.

10.2 INTERCONEXIONES ENTRE DISPOSITIVOS

10.2.1 LAN y WAN: Conexión

Al planificar la instalación del cableado LAN, existen cuatro áreas físicas que se deben considerar:

- Área de trabajo.
- Cuarto de telecomunicaciones, también denominado servicio de distribución.
- Cableado backbone, también denominado cableado vertical.
- Cableado de distribución, también denominado cableado horizontal.

Longitud total del cable

Para las instalaciones UTP, el estándar ANSI/TIA/EIA-568-B especifica que la longitud combinada total del cable que abarca las cuatro áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por canal. Este estándar establece que se pueden utilizar hasta 5 metros de patch cable para interconectar los patch panels. Pueden

utilizarse hasta 5 metros de cable desde el punto de terminación del cableado en la pared hasta el teléfono o la computadora.

Áreas de trabajo

Las áreas de trabajo son las ubicaciones destinadas para los dispositivos finales utilizados por los usuarios individuales. Cada área de trabajo tiene un mínimo de dos conectores que pueden utilizarse para conectar un dispositivo individual a la red. Utilizamos patch cables para conectar dispositivos individuales a estos conectores de pared. El estándar EIA/TIA establece que los patch cords de UTP utilizados para conectar dispositivos a los conectores de pared tienen una longitud máxima de 10 metros.

El cable de conexión directa es el patch cable de uso más común en el área de trabajo. Este tipo de cable se utiliza para conectar dispositivos finales, como computadoras, a una red. Cuando se coloca un hub o switch en el área de trabajo, generalmente se utiliza un cable de conexión cruzada para conectar el dispositivo al jack de pared.

Cuarto de telecomunicaciones

El cuarto de telecomunicaciones es el lugar donde se realizan las conexiones a los dispositivos intermediarios. Estos cuartos contienen dispositivos intermediarios (hubs, switches, routers y unidades de servicio de datos [DSU]) que conectan la red. Estos dispositivos proporcionan transiciones entre el cableado backbone y el cableado horizontal.

Dentro del cuarto de telecomunicaciones, los patch cords realizan conexiones entre los patch panels, donde terminan los cables horizontales, y los dispositivos intermediarios. Los patch cables también interconectan estos dispositivos intermediarios.

Los estándares de la Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen dos tipos diferentes de patch cables de UTP. Uno de los tipos es el patch cord, con una longitud de hasta 5 metros y se utiliza para interconectar el equipo y los patch panels en el cuarto de telecomunicaciones. Otro tipo de patch cable puede ser de hasta 5 metros de longitud y se utiliza para conectar dispositivos a un punto de terminación en la pared.

Estos cuartos a menudo tienen una doble finalidad. En muchas organizaciones, el cuarto de telecomunicaciones también incluye los servidores utilizados por la red.

Cableado horizontal

El cableado horizontal se refiere a los cables que conectan los cuartos de telecomunicaciones con las áreas de trabajo. La longitud máxima de cable desde el punto de terminación en el cuarto de telecomunicaciones hasta la terminación en la toma del área de trabajo no puede superar los 90 metros. Esta distancia máxima de cableado horizontal de 90 metros se denomina enlace permanente porque está instalada en la estructura del edificio. Los medios horizontales se ejecutan desde un patch panel en el cuarto de telecomunicaciones a un jack de pared en cada área de trabajo. Las conexiones a los dispositivos se realizan con patch cables.

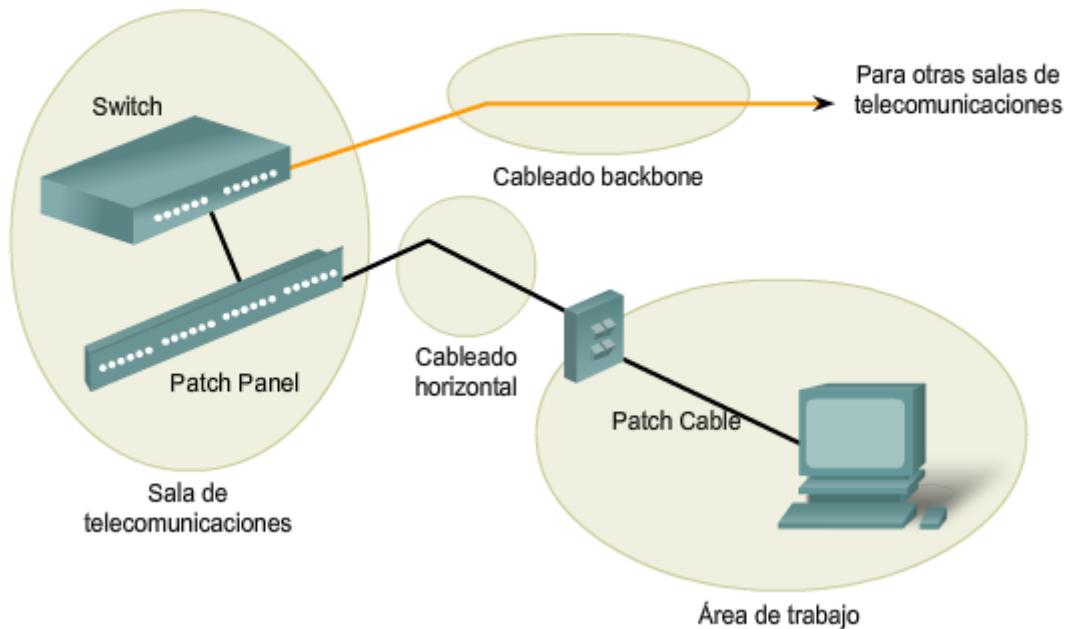
Cableado backbone

El cableado backbone se refiere al cableado utilizado para conectar los cuartos de telecomunicaciones a las salas de equipamiento donde suelen ubicarse los servidores. El cableado backbone también interconecta múltiples cuartos de telecomunicaciones en toda la instalación. A menudo, estos cables se enrutan fuera del edificio a la conexión WAN o ISP.

Los backbones, o cableado vertical, se utilizan para el tráfico agregado, como el tráfico de entrada o de salida de Internet, y para el acceso a los recursos corporativos en una ubicación remota. Gran parte del tráfico desde varias áreas

de trabajo utilizará el cableado backbone para acceder a los recursos externos del área o la instalación. Por lo tanto, los backbones generalmente requieren de medios de ancho de banda superiores como el cableado de fibra óptica.

Áreas de cableado LAN



Tipos de medios

Se deben considerar los diferentes tipos de medios al elegir los cables necesarios para realizar una conexión WAN o LAN exitosa. Como ya mencionamos, existen diferentes implementaciones de la capa Física que admiten múltiples tipos de medios:

- UTP (Categorías 5, 5e, 6 y 7).
- Fibra óptica.
- Inalámbrico.

Cada tipo de medios tiene ventajas y desventajas. Algunos de los factores que se deben considerar son los siguientes:

- Longitud del cable: ¿El cable debe atravesar una habitación o extenderse desde un edificio hasta otro?
- Costo: ¿El presupuesto permite que se utilice un tipo de medios más costoso?
- Ancho de banda: ¿La tecnología utilizada con los medios ofrece un ancho de banda apropiado?
- Facilidad de instalación: ¿Tiene el equipo de implementación la capacidad de instalar el cable o es necesario contratar a un proveedor?
- Susceptibilidad a EMI/RFI: ¿Interferirá con la señal el entorno en el que estamos instalando el cable?

Tipos de interconexión de dispositivos



Fibra



UTP



Inalámbrica

Longitud del cable

La longitud total del cable que se requiere para conectar un dispositivo incluye todos los cables desde los dispositivos finales del área de trabajo hasta el dispositivo intermediario en el cuarto de telecomunicaciones (generalmente un switch). Esto incluye el cable desde los dispositivos hasta el enchufe de pared, el cable a través el edificio desde el enchufe de pared hasta el punto de conexión cruzada, o patch panel, y el cable desde el patch panel hasta el switch. Si el switch se ubica en los cuartos de telecomunicaciones en diferentes pisos de un edificio o en diferentes edificios, el cable entre estos puntos debe incluirse en la longitud total.

La atenuación es la reducción de la potencia de una señal a medida que se transmite a través de un medio. Cuanto más extensos sean los medios, más la atenuación afectará la señal. En algún punto, la señal no será detectable. **La distancia del cableado es un factor esencial en el rendimiento de la señal de datos. La atenuación de la señal y la exposición a una posible interferencia aumenta con la longitud del cable.**

Por ejemplo, cuando se utiliza un cableado UTP para Ethernet, la longitud del cableado horizontal (o fijo) necesita mantenerse a una distancia máxima recomendada de 90 metros para evitar la atenuación de la señal. Los cables de fibra óptica pueden proporcionar una distancia de cableado mayor de hasta 500 metros o algunos kilómetros, según el tipo de tecnología. Sin embargo, el cable de fibra óptica también puede sufrir una atenuación cuando se alcanzan estos límites.

Costo

El costo asociado con el cableado de una LAN puede variar según el tipo de medio y es posible que el personal no pueda darse cuenta del impacto sobre el presupuesto. En un entorno ideal, el presupuesto permitiría instalar un cableado de fibra óptica para cada dispositivo de la LAN. Si bien la fibra proporciona un ancho de banda superior que el UTP, los

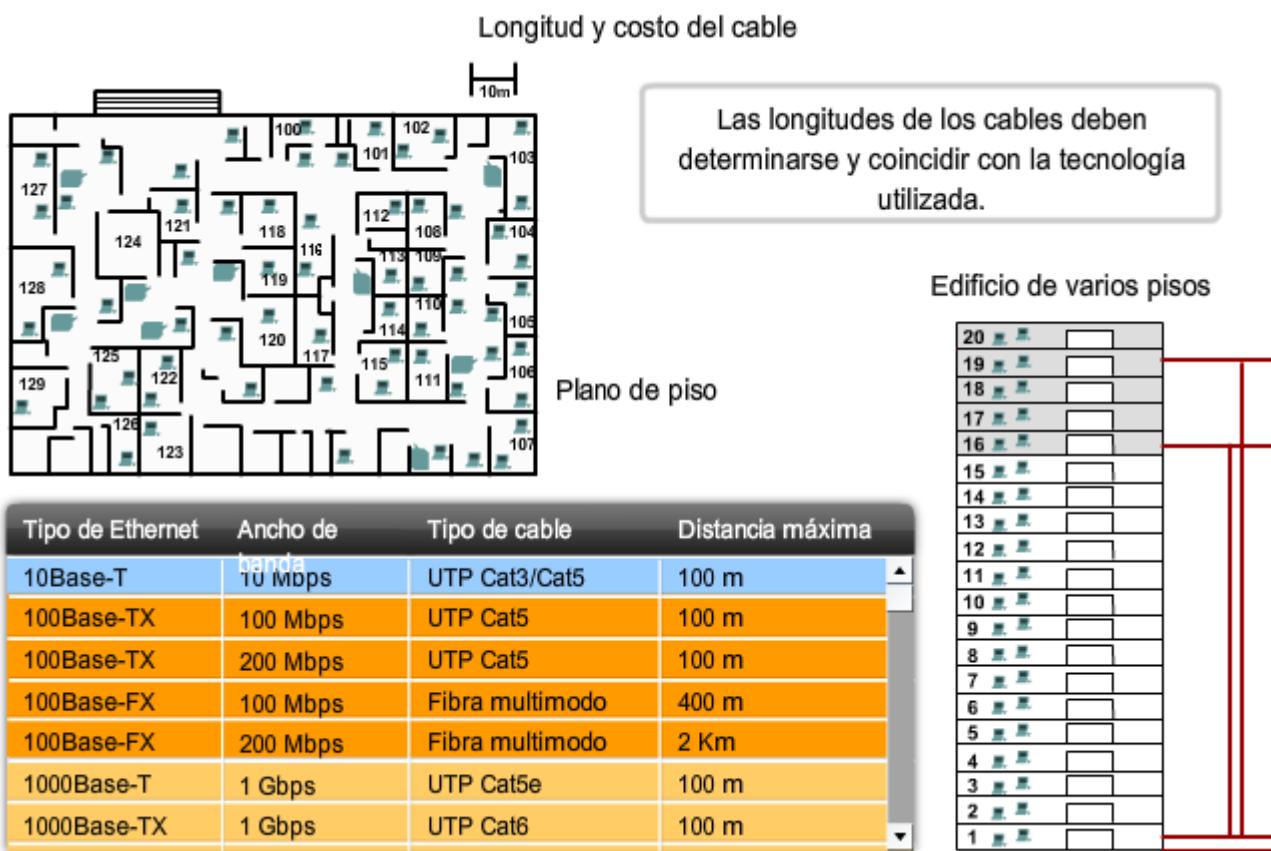
costos de la instalación y el material son considerablemente mayores. En la práctica, generalmente no se requiere este nivel de rendimiento y no constituye una expectativa razonable en la mayoría de los entornos. Los diseñadores de redes deben lograr que coincidan las necesidades de rendimiento por parte de los usuarios con el costo de equipo y cableado para obtener la mejor relación costo/rendimiento.

Ancho de banda

Los dispositivos de una red presentan requisitos de ancho de banda diferentes. Al seleccionar los medios para las conexiones individuales, considere cuidadosamente los requisitos de ancho de banda.

Por ejemplo, un servidor generalmente necesita mayor ancho de banda que una computadora dedicada a un único usuario. Para la conexión del servidor, considere aquellos medios que proporcionarán un ancho de banda superior y que podrán desarrollarse para cumplir con mayores requisitos de ancho de banda y utilizar las tecnologías más nuevas. Un cable de fibra puede ser una elección lógica para la conexión de un servidor.

Actualmente, la tecnología utilizada en los medios de fibra óptica ofrece el mayor ancho de banda disponible entre las opciones para los medios LAN. Teniendo en cuenta el ancho de banda aparentemente ilimitado disponible en los cables de fibra, se esperan velocidades mayores para las LAN. El medio inalámbrico también admite aumentos considerables en el ancho de banda, pero tiene limitaciones en cuanto al consumo de la potencia y la distancia.



Facilidad de instalación

La facilidad al instalar un cableado varía según los tipos de cables y la estructura del edificio. El acceso al piso y a sus espacios, además de las propiedades y el tamaño físico del cable, influyen en la facilidad de instalación de un cable en distintos edificios. Los cables de los edificios generalmente se instalan en canales para conductores eléctricos.

Como se muestra en la figura, un canal para conductores eléctricos es un recinto o tubo que se adjunta al cable y lo protege. Un canal también mantiene la prolijidad del cableado y facilita el paso de los cables.

El cable UTP es relativamente liviano, flexible y tiene un diámetro pequeño, lo que permite introducirlo en espacios pequeños. Los conectores, enchufes RJ-45, son relativamente fáciles de instalar y representan un estándar para todos los dispositivos Ethernet.

Muchos cables de fibra óptica contienen una fibra de vidrio delgada. Esta característica genera problemas para el radio de curvatura del cable. La fibra puede romperse al enroscarla o doblarla fuertemente. La terminación de los conectores del cable (ST, SC, MT-RJ) son mucho más difíciles de instalar y requieren de un equipo especial.

En algún punto, las redes inalámbricas requieren de cableado para conectar dispositivos, como puntos de acceso, a la LAN instalada. Los medios inalámbricos a menudo son más fáciles de instalar que un cable de fibra o UTP, ya que se necesitan menos cables en una red inalámbrica. Sin embargo, una LAN inalámbrica requiere de una prueba y planificación más detalladas. Además, varios factores externos, como otros dispositivos de radiofrecuencia o las construcciones edilicias, pueden afectar su funcionamiento.

Interferencia electromagnética/Interferencia de radiofrecuencia

La Interferencia electromagnética (EMI) y la Interferencia de radiofrecuencia (RFI) deben tenerse en cuenta al elegir un tipo de medios para una LAN. La EMI/RFI en un entorno industrial puede producir un impacto significativo sobre las comunicaciones de datos si se utiliza un cable incorrecto.

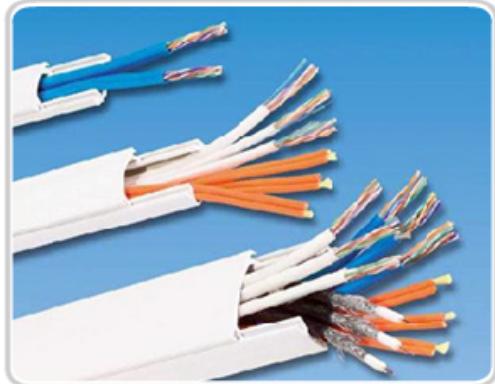
La interferencia puede provenir de máquinas eléctricas, rayos y otros dispositivos de comunicación, incluyendo computadoras y equipos de radio.

A modo de ejemplo, piense en una instalación donde los dispositivos de dos edificios distintos se encuentran interconectados. Los medios utilizados para interconectar estos edificios estarán expuestos a la posible descarga de los rayos. Además, es posible que exista una gran distancia entre estos dos edificios. La fibra óptica es la mejor elección para esta instalación.

Los medios inalámbricos son los más susceptibles a la RFI. Antes de utilizar una tecnología inalámbrica, se deben identificar las posibles fuentes de interferencia y reducirlas en lo posible.

Facilidad de instalación

El UTP y la fibra tienen distintos requisitos de instalación.



Canal para cable UTP

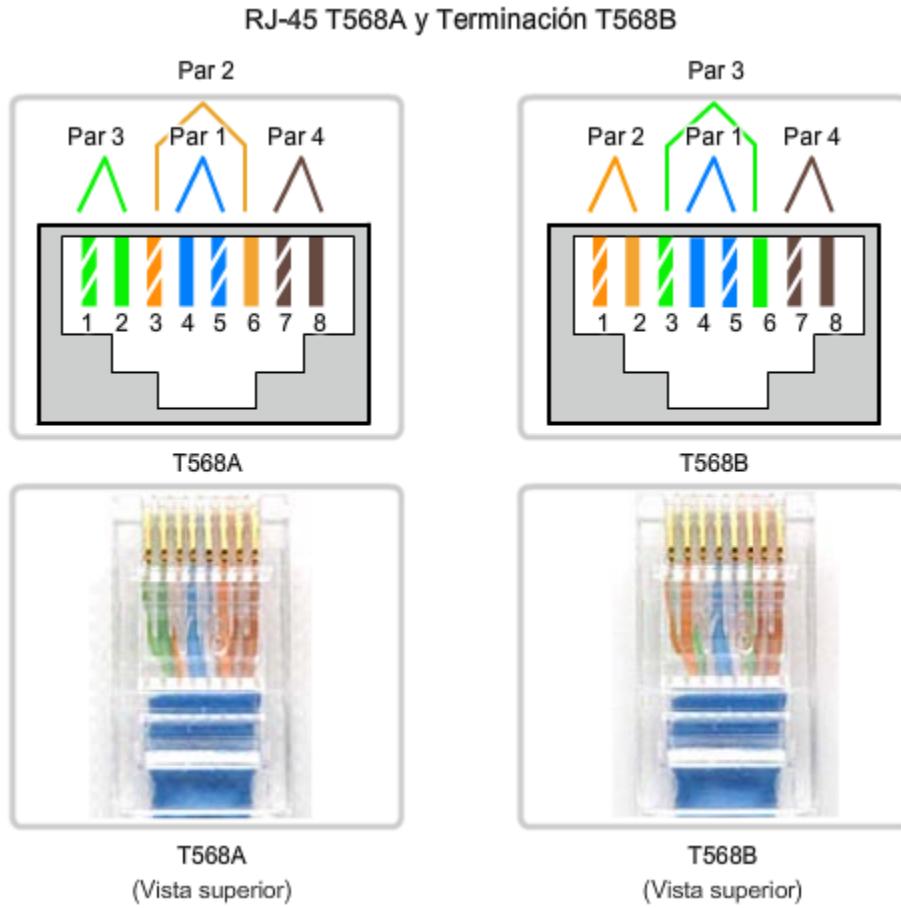


Canal para cable de fibra

10.2.2 Realización de conexiones LAN

La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen las conexiones del cableado UTP.

El conector RJ-45 es el componente macho engarzado al extremo del cable. Cuando se observan desde el frente, los pins se numeran del 8 al 1. Cuando se observan desde arriba con la entrada de apertura frente a usted, los pins se enumeran del 1 al 8, de izquierda a derecha. Es importante recordar esta orientación al identificar un cable.



Tipos de interfaces

En una LAN Ethernet, los dispositivos utilizan uno de los dos tipos de interfaces UTP: MDI o MDIX.

La MDI (interfaz dependiente del medio) utiliza un diagrama de pines normal de Ethernet. Los pins 1 y 2 se utilizan como transmisores y los pins 3 y 6 como receptores. Dispositivos como computadoras, servidores o routers tendrán conexiones MDI.

Los dispositivos que proporcionan la conectividad a la LAN (por lo general, hubs o switches) habitualmente utilizan conexiones MDIX (Interfaz cruzada dependiente del medio). Los cables MDIX intercambian los pares transmisores internamente. Este intercambio permite que los dispositivos finales se encuentren conectados a un hub o switch utilizando un cable de conexión directa.

En general, cuando conecte diferentes tipos de dispositivos, utilice un cable de conexión directa. Cuando conecte el mismo tipo de dispositivo, utilice un cable de conexión directa.

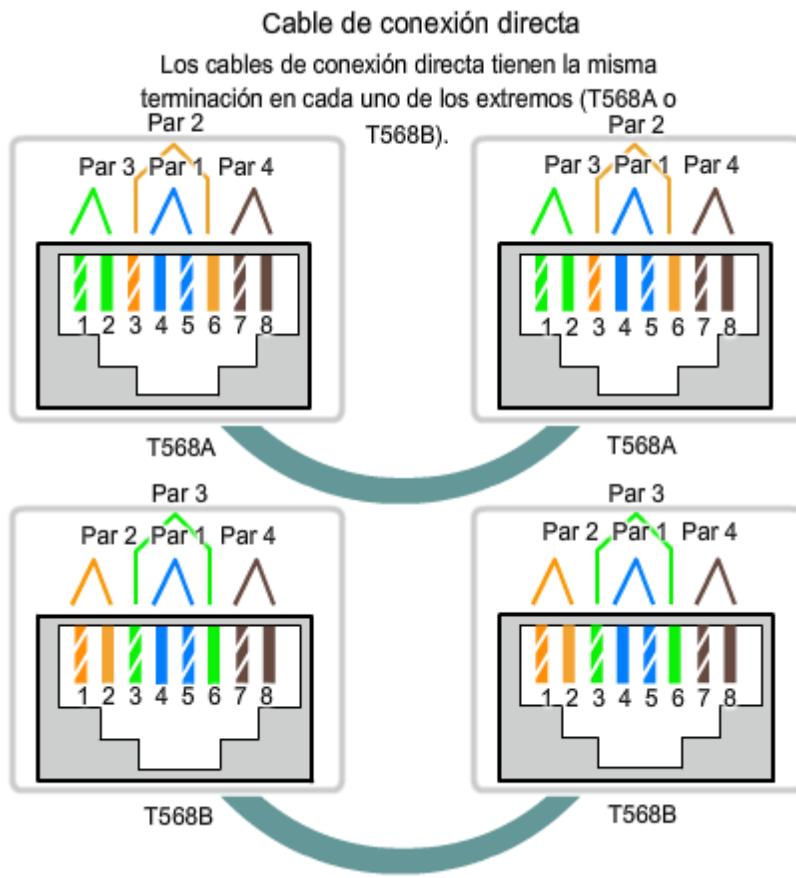
Cables UTP de conexión directa

Un cable de conexión directa tiene conectores en cada extremo y su terminación es idéntica conforme a los estándares T568A o T568B.

La identificación del estándar del cable utilizado le permite determinar si cuenta con el cable correcto para un determinado trabajo. Más importante aún, es normal utilizar los mismos códigos de color en toda la LAN para lograr consistencia en la documentación.

Utilice cables directos para las siguientes conexiones:

- Switch a puerto Ethernet del router
- Equipo a switch
- Equipo a hub



Cables UTP de conexión cruzada

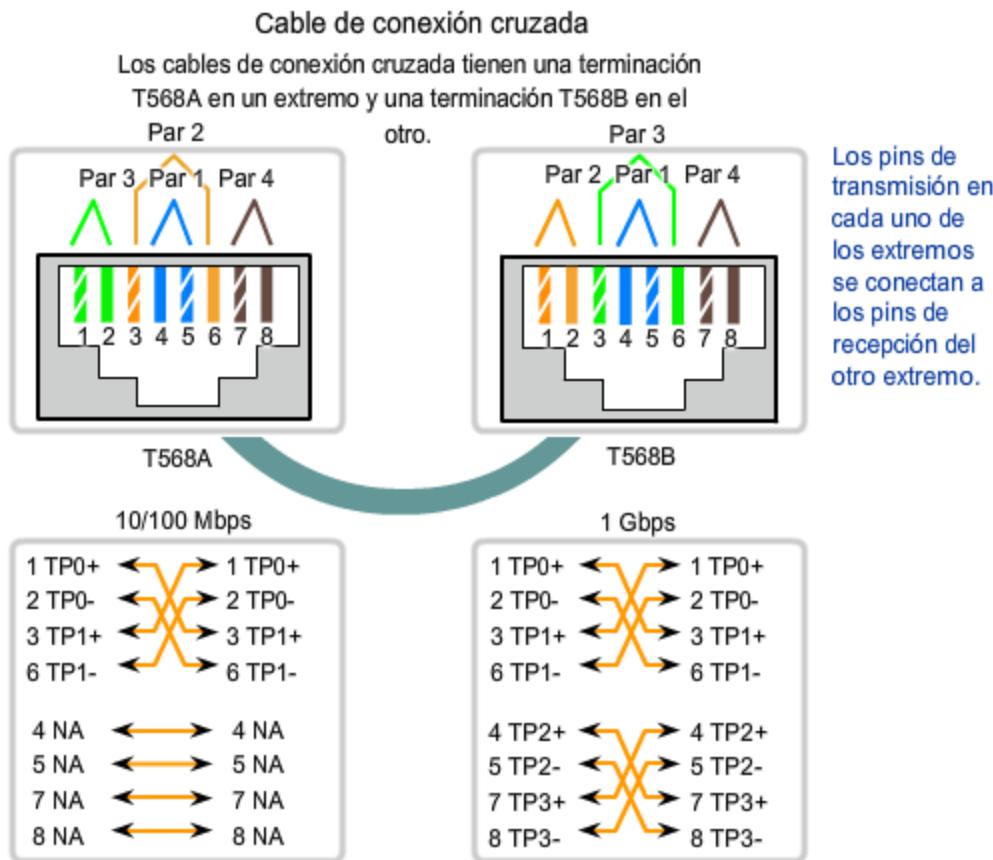
Para que los dos dispositivos se comuniquen a través de un cable directamente conectado entre los dos, el terminal transmisor de uno de los dispositivos necesita conectarse al terminal receptor del otro dispositivo.

El cable debe tener una terminación para que el pin transmisor, Tx, que toma la señal desde el dispositivo A en un extremo, se conecte al pin receptor, Rx, en el dispositivo B. De manera similar, el pin Tx del dispositivo B debe estar conectado al pin Rx del dispositivo A. Si el pin Tx de un dispositivo tiene el número 1 y el pin Rx tiene el número 2, el cable conecta el pin 1 en un extremo con el pin 2 en el otro extremo. Este tipo de cable se denomina “de conexión cruzada” por estas conexiones de pin cruzadas.

Para alcanzar este tipo de conexión con un cable UTP, un extremo debe tener una terminación como diagrama de pin EIA/TIA T568A y el otro, como T568B.

En resumen, los cables de conexión cruzada conectan directamente los siguientes dispositivos en una LAN:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a conexión del puerto Ethernet del router
- Equipo a equipo
- Equipo a puerto Ethernet del router



En la figura, identifique el tipo de cable utilizado según los dispositivos conectados.

A modo de recordatorio, nuevamente se enumeran los usos comunes:

Utilice cables de conexión directa para conectar:

- Switch a router
- Equipo a switch
- Equipo a hub

Utilice cables de conexión cruzada para conectar:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a router
- Equipo a equipo

- Equipo a router

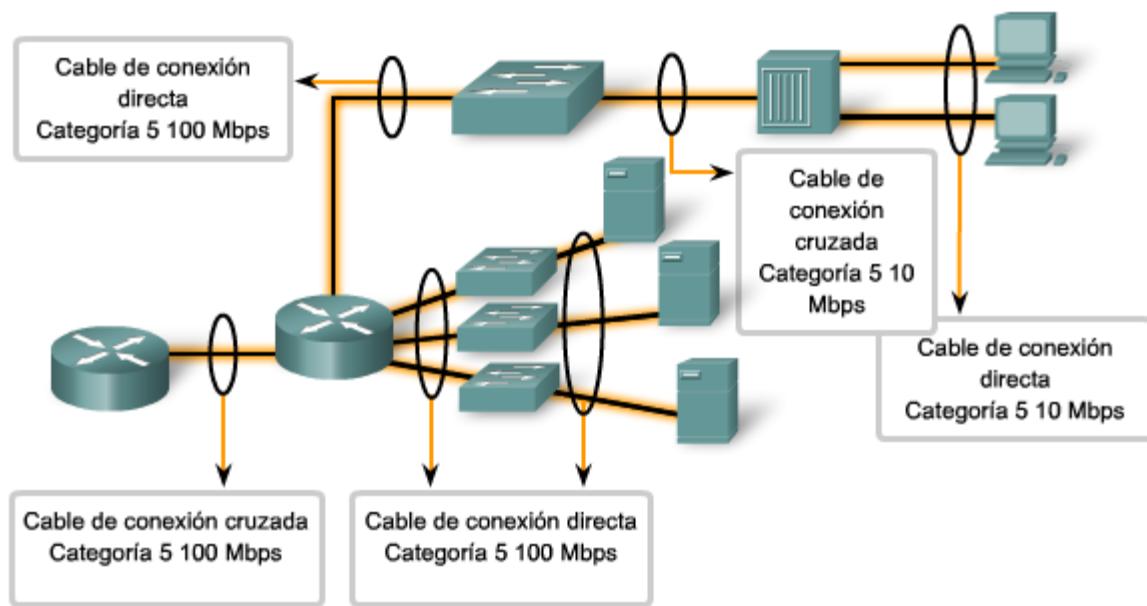
Selección de MDI/MDIX

Una gran cantidad de dispositivos permite que el puerto Ethernet UTP se establezca en MDI o en MDIX. Esta configuración puede realizarse en una de tres formas, según las características del dispositivo:

1. En algunos dispositivos, los puertos pueden incluir un mecanismo que intercambia de manera eléctrica los pares receptores y transmisores. El puerto puede cambiarse de MDI a MDIX al activar el mecanismo.
2. Como parte de la configuración, algunos dispositivos permiten seleccionar la función del puerto como MDI o MDIX.
3. Muchos de los dispositivos más nuevos incluyen una característica de conexión cruzada automática. Esta característica permite al dispositivo detectar el tipo de cable requerido y configura las interfaces según corresponda. En algunos dispositivos, esta detección automática se realiza en forma predeterminada. Otros dispositivos que requieren un comando de configuración de interfaz para habilitar la detección automática de MDIX.

Realización de conexiones LAN

Identifique el tipo de cable UTP apropiado y la posible categoría para conectar diferentes dispositivos intermedios y finales en una LAN.



10.2.3 Realización de conexiones WAN

Por naturaleza, los enlaces WAN pueden abarcar distancias sumamente extensas. Estas distancias pueden variar en todo el mundo ya que proporcionan los enlaces de comunicación que utilizamos para administrar cuentas de e-mail, visualizar páginas Web o realizar una sesión de teleconferencia con un cliente.

Las conexiones de área amplia en las redes adquieren diferentes formas, entre ellas:

- Conectores de la línea telefónica RJ11 para dial-up o conexiones de la Línea de suscriptor digital (DSL)
- Conexiones serial de 60 pins

En las prácticas de laboratorio del curso, el usuario puede utilizar routers Cisco con uno de los dos tipos de cable serial físico. Ambos cables utilizan un conector Winchester grande de 15 pines en el extremo de la red. Este extremo del cable

se utiliza como una conexión V.35 a un dispositivo de capa física como CSU/DSU (Unidad de servicio de canal/Unidad de servicio de datos).

El primer tipo de cable tiene un conector macho DB-60 en el extremo de Cisco y un conector Winchester macho en el extremo de la red. El segundo tipo es una versión más compacta de este cable y tiene un conector serial inteligente en el extremo del dispositivo Cisco. Es necesario poder identificar los dos tipos diferentes a fin de conectar el router de manera exitosa.

Tipos de conexiones WAN

| HDLC de Cisco | PPP | Frame Relay | Módem DSL | Cable módem |
|--|-----|-------------|--|---|
| EIA/TIA-232 EIA/TIA-449 X.21V.24 V.35 Interfaz serial de alta velocidad (HSSI) | | | RJ-11 Nota: Funciona sobre línea telefónica | F Nota: Funciona sobre línea de televisión por cable |

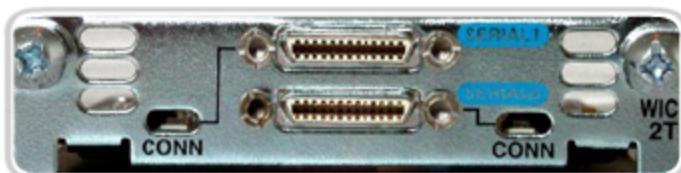


Router: Serial inteligente macho



Red: Tipo de bloque Winchester macho

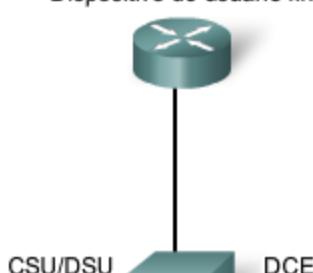
Tipos de conexiones WAN: Serial



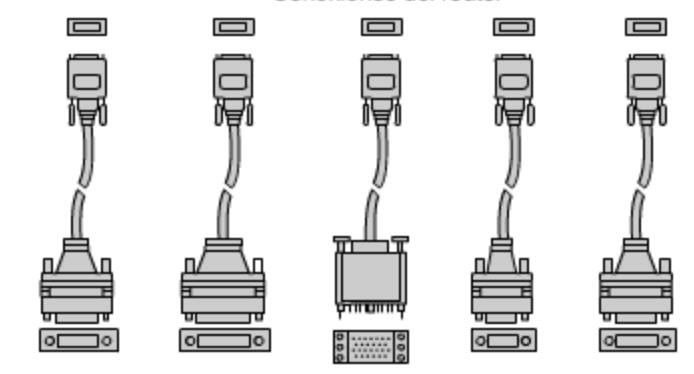
Dispositivo de usuario final



Conexiones del router

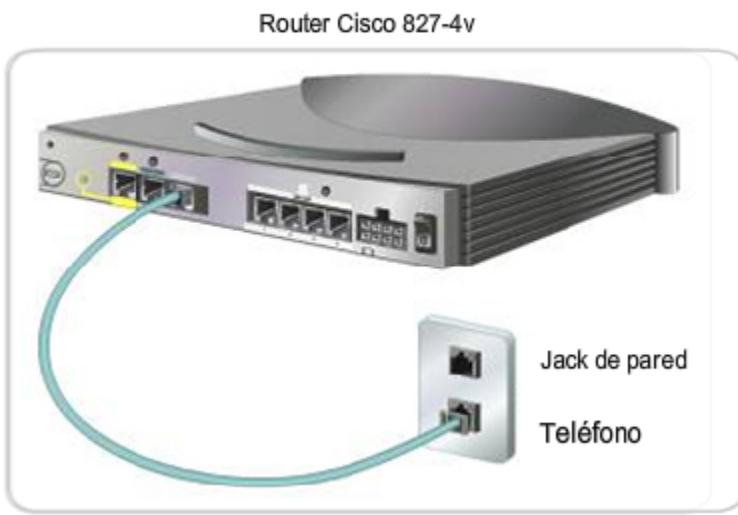


Proveedor del servicio



Conexiones de red en la CSU/DSU

Tipos de conexiones WAN: DSL



Equipo de comunicación de datos y Equipo terminal de datos

Los siguientes términos describen los tipos de dispositivos que mantienen el enlace entre un dispositivo de envío y uno de recepción:

Equipo de comunicación de datos (DCE): Un dispositivo que suministra los servicios de temporización a otro dispositivo. Habitualmente, este dispositivo se encuentra en el extremo del enlace que proporciona el acceso WAN.

Equipo terminal de datos (DTE): Un dispositivo que recibe los servicios de temporización desde otro dispositivo y se ajusta en consecuencia. Habitualmente, este dispositivo se encuentra en el extremo del enlace del cliente WAN o del usuario.

Si se establece una conexión serial directa con un proveedor de servicios o con un dispositivo que proporcione la temporización de la señal, como una unidad de servicio de canal/unidad de servicio de datos (CSU/DSU), se considera que el router es un equipo terminal de datos (DTE) y utilizará un cable serial DTE.

Tenga en cuenta que habrá situaciones, especialmente en nuestros laboratorios, en las que se requerirá que el router local brinde la frecuencia de reloj y entonces utilizará un cable para equipo de comunicación de datos (DCE).

Los DCE y DTE se utilizan en conexiones WAN. La comunicación mediante una conexión WAN se mantiene al proporcionar una frecuencia de reloj aceptable tanto para el dispositivo receptor como el emisor. En la mayoría de los casos, la compañía telefónica o ISP proporciona el servicio de temporización que sincroniza la señal transmitida.

Por ejemplo, si un dispositivo conectado mediante un enlace WAN envía su señal a 1.544 Mbps, cada dispositivo receptor debe utilizar un reloj, enviando una señal de muestra cada $1/1,544,000$ de segundo. La temporización en este caso es sumamente breve. Los dispositivos deben ser capaces de sincronizarse a la señal que se envía y recibe rápidamente.

Al asignar al router una frecuencia de reloj, se configura la temporización. Esto permite al router ajustar la velocidad de sus operaciones de comunicación. De esta manera, se sincroniza con los dispositivos conectados a él.

Conexiones WAN seriales para DCE y DTE



Equipo terminal de datos:

- Extremo del dispositivo del usuario en el enlace de WAN

Equipo de comunicación de datos:

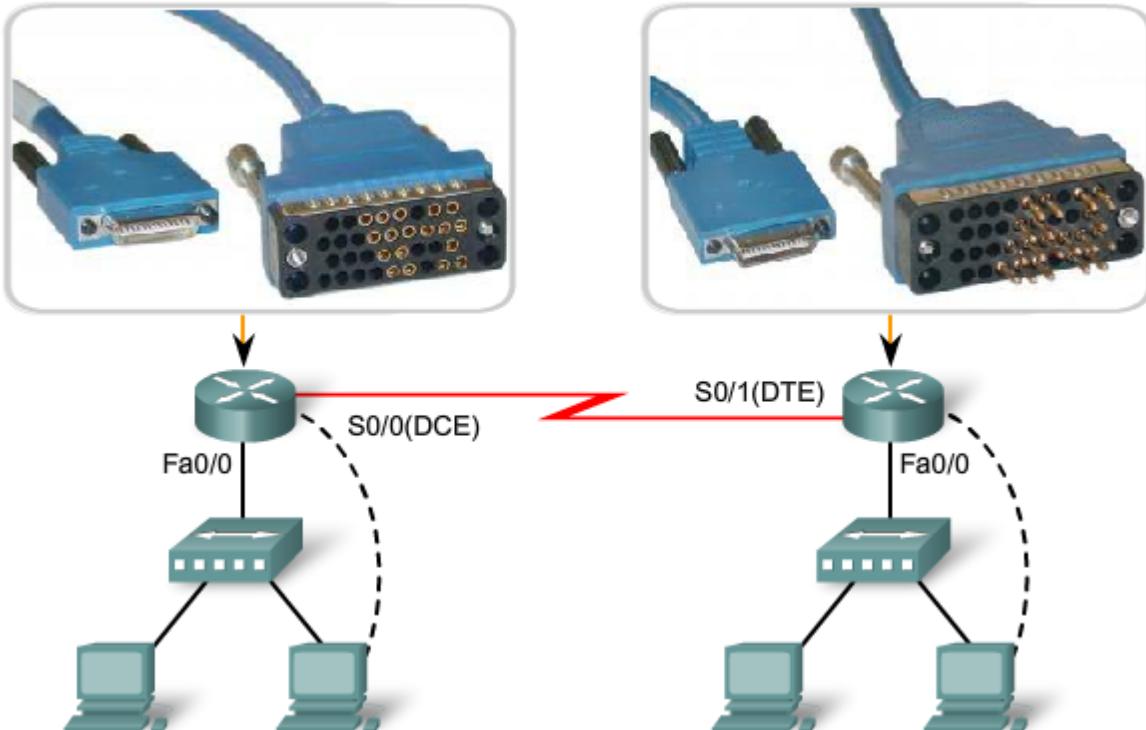
- Extremo del lado del proveedor de la WAN de la instalación de comunicaciones
- Responsable de proveer la señal de temporización.

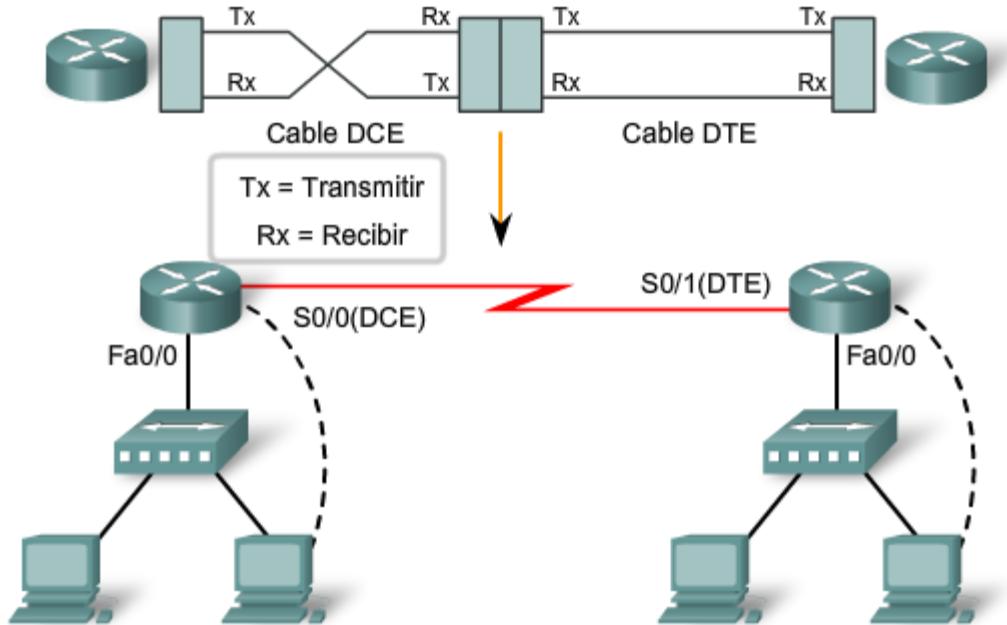
En el laboratorio

Cuando se realizan conexiones WAN entre dos routers en un entorno de práctica de laboratorio, conecte dos routers con un cable serial para simular un enlace WAN punto a punto. En este caso, decida qué router tendrá el control de la temporización. Por defecto, los Router son dispositivos DTE, pero se los puede configurar de manera tal que actúen como dispositivos DCE.

Los cables que cumplen con el estándar V35 se encuentran disponibles en versiones DTE y DCE. Para crear una conexión serial punto a punto entre dos routers, una un cable DTE con uno DCE. Cada cable incluye un conector que se combina con su tipo complementario. Estos conectores están configurados de modo que no pueda unir dos cables DCE o dos cables DTE juntos por error.

Conexiones WAN seriales en el laboratorio





10.3 DESARROLLO DE UN ESQUEMA DE DIRECCIONAMIENTO

10.3.1 ¿Cuántos host hay en la red?

Para desarrollar un esquema de direccionamiento para una red, comience por definir la cantidad total de hosts. Considere cada dispositivo que requerirá una dirección IP, ahora y en el futuro.

Algunos dispositivos finales que requieren una dirección IP son:

- Equipos de usuarios.
- Equipos de administradores.
- Servidores.
- Otros dispositivos finales, como impresoras, teléfonos IP y cámaras IP.

Entre los dispositivos de red que requieren una dirección IP se incluyen:

- Interfaces LAN del Router.
- Interfaces (serial) WAN del Router.

Entre los dispositivos de red que requieren una dirección IP para la administración se incluyen:

- Switches.
- Puntos de acceso inalámbrico.

Es posible que existan otros dispositivos en una red que requieran una dirección IP. Agréguelos a esta lista y calcule cuántas direcciones se necesitará tener en cuenta para el crecimiento de la red a medida que se agregan más dispositivos.

Una vez que se ha establecido la cantidad total de hosts (actuales y a futuro), considere el rango de direcciones disponibles y dónde encajan en la dirección de red determinada.

Luego, determine si todos los hosts formarán parte de la misma red o si toda la red se dividirá en subredes independientes.

Recuerde que la cantidad de hosts en una red o subred se calcula mediante la fórmula $2^n - 2$, donde n es la cantidad de bits disponibles como bits de host. Recuerde también que sustraemos dos direcciones (la dirección de red y la dirección de broadcast de la red) y no pueden asignarse a los hosts.

Cómo determinar de la cantidad de hosts en una red

Incluya estos dispositivos en la cuenta:



Interfaces de routers

Cuento la cantidad de interfaces y no la cantidad de routers



Impresoras



Teléfonos IP

Cuento también cualquier otro dispositivo IP especial



Direcciones de administración de switches



Usuarios de administración



Usuarios generales



Servidores

10.3.2 ¿Cuántas redes?

Existen muchas razones para dividir una red en subredes:

- Administrar el tráfico de broadcast: Los broadcasts pueden controlarse porque un gran dominio de broadcast se divide en una gran cantidad de dominios más pequeños. No todos los hosts del sistema reciben todos los broadcasts.
- Diferentes requisitos de red: Si los diferentes grupos de usuarios requieren servicios informáticos o de red específicos, resulta más sencillo administrar estos requisitos si aquellos usuarios que comparten requisitos se encuentran todos juntos en una subred.
- Seguridad: Se pueden implementar diferentes niveles de seguridad en la red basándose en las direcciones de red. Esto permite la administración del acceso a diferentes servicios de red y de datos.

Número de subredes

Cada subred, como segmento físico de la red, requiere una interfaz de Router que funcione como 408ersión para tal subred.

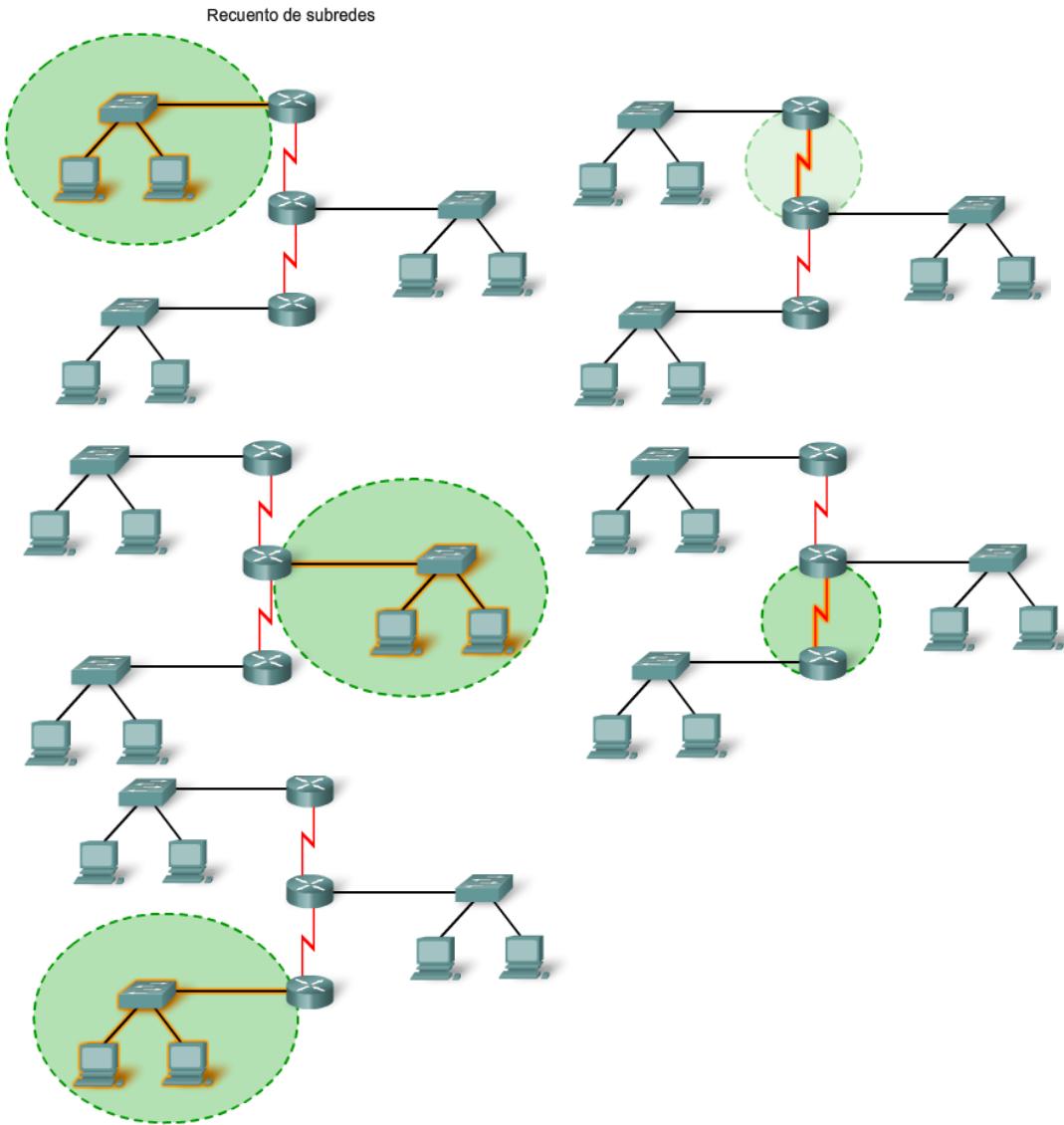
Además, cada conexión entre los routers constituye una red independiente.

La cantidad de subredes en una red también se calcula mediante la fórmula 2^n , donde n es la cantidad de bits "prestados" por la dirección de red IP determinada disponible para crear las subredes.

Máscaras de subredes

Después de establecer la cantidad requerida de hosts y subredes, el siguiente paso es aplicar una máscara de subred a toda la red y luego calcular los siguientes valores:

- Una subred y máscara de subred exclusivas para cada segmento físico
- Un rango de direcciones host utilizables para cada subred



10.3.3 Diseño del estándar de dirección para nuestra networking

Para contribuir a la resolución de problemas y acelerar la incorporación de nuevos hosts a la red, utilice direcciones que se ajusten a un patrón común en todas las subredes. Cada uno de estos diferentes tipos de dispositivos debería asignarse a un bloque lógico de direcciones dentro del rango de direcciones de la red.

Algunas de las diferentes categorías para hosts son:

- Usuarios generales

- Usuarios especiales
- Recursos de red
- Interfaces LAN del Router
- Enlaces WAN del router
- Acceso de la administración

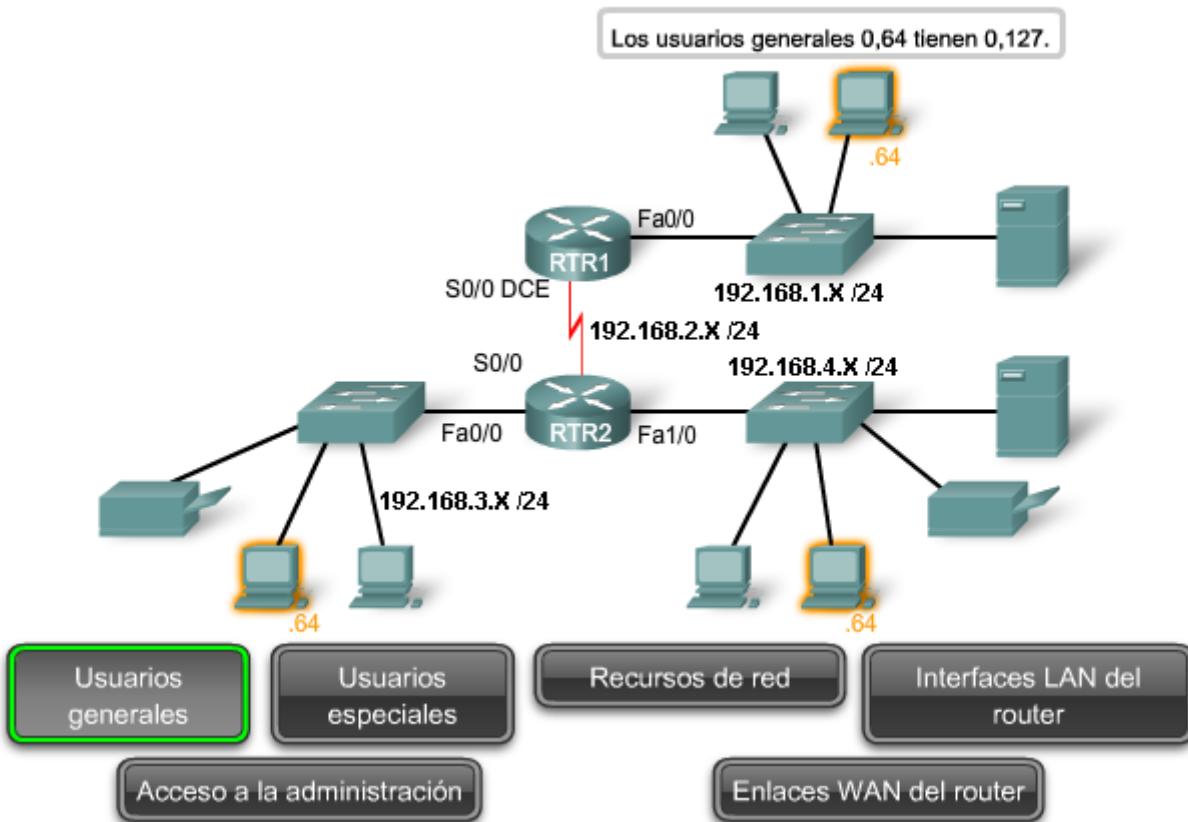
Por ejemplo, al asignar una dirección IP a una interfaz del Router que es la 410ersión para una LAN, es una práctica común utilizar la primera (más baja) o última (más alta) dirección dentro del rango de la subred. El enfoque constante contribuye a la configuración y a la resolución de problemas.

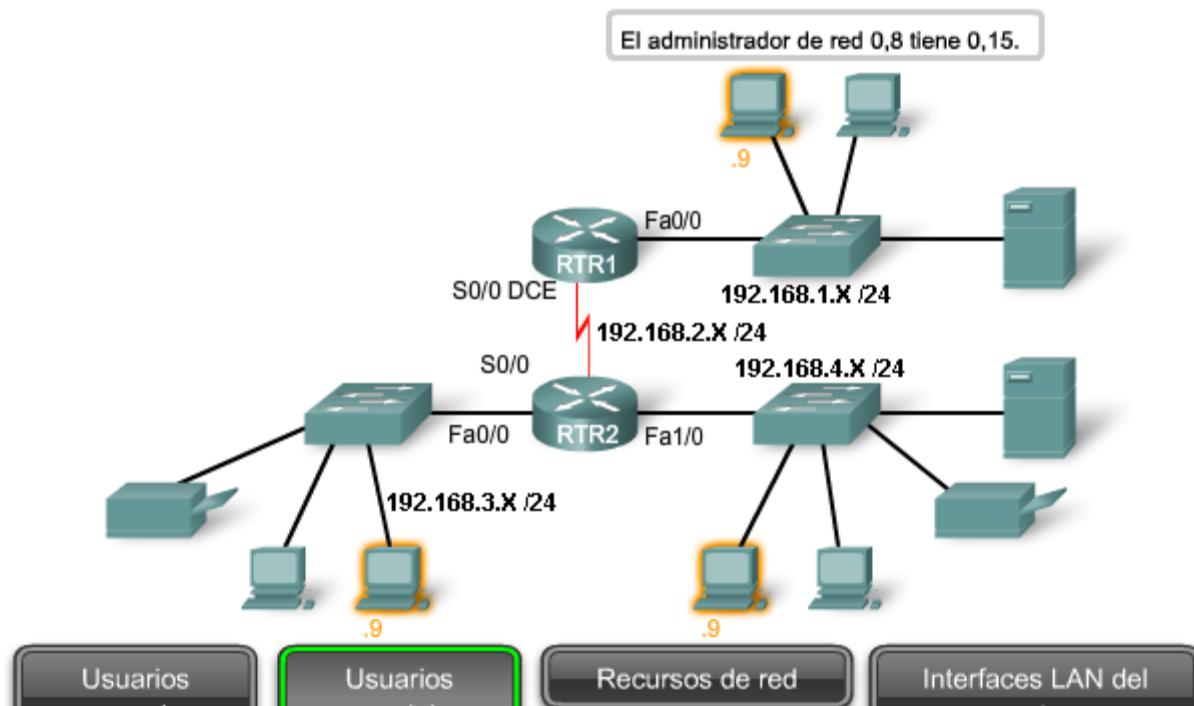
De manera similar, cuando se asignan direcciones a dispositivos que administran otros dispositivos, la utilización de un patrón constante dentro de la subred permite reconocer estas direcciones con mayor facilidad. Por ejemplo, en la figura, las direcciones con 64 – 127 en los octetos siempre representan a los usuarios generales. Un administrador de red puede controlar o incorporar seguridad a todas las direcciones que terminan con estos valores.

Pase el cursor del mouse sobre los grupos de dispositivos en la figura para ver un ejemplo de cómo asignar direcciones basadas en las categorías de dispositivos.

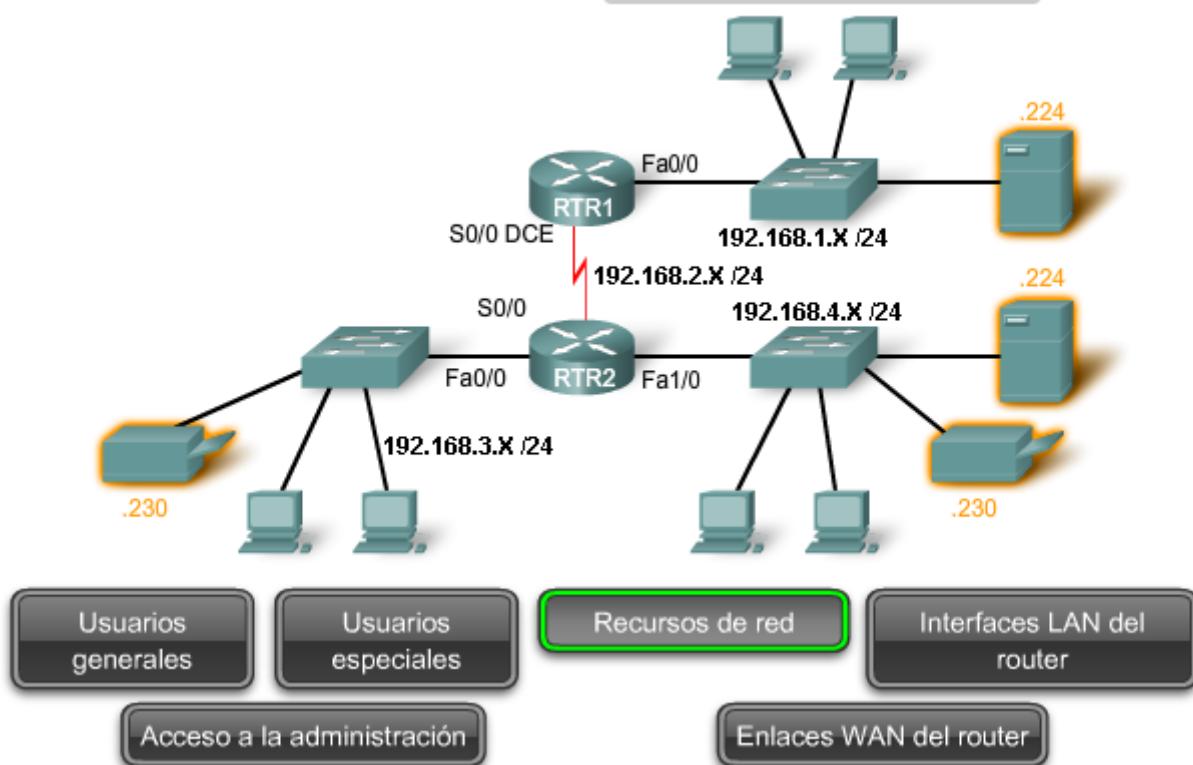
Además, recuerde documentar su esquema de direccionamiento IP por escrito. Este paso será de gran ayuda en la resolución de problemas y la evolución de la red.

Diseño de un estándar de dirección de internetwork

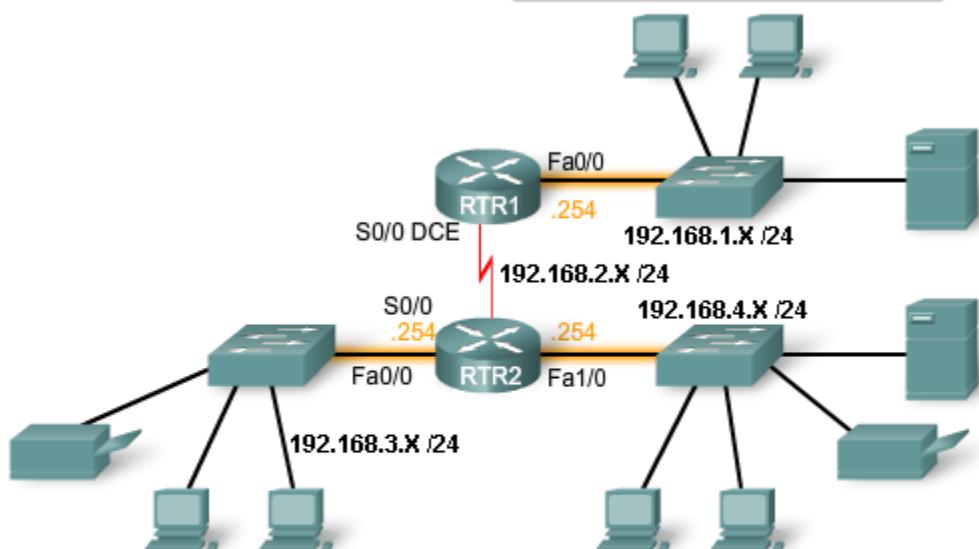




Los recursos de red 0,224 tienen 0,239.



El router 0,250 tiene 0,254 interfaces.



Usuarios generales

Usuarios especiales

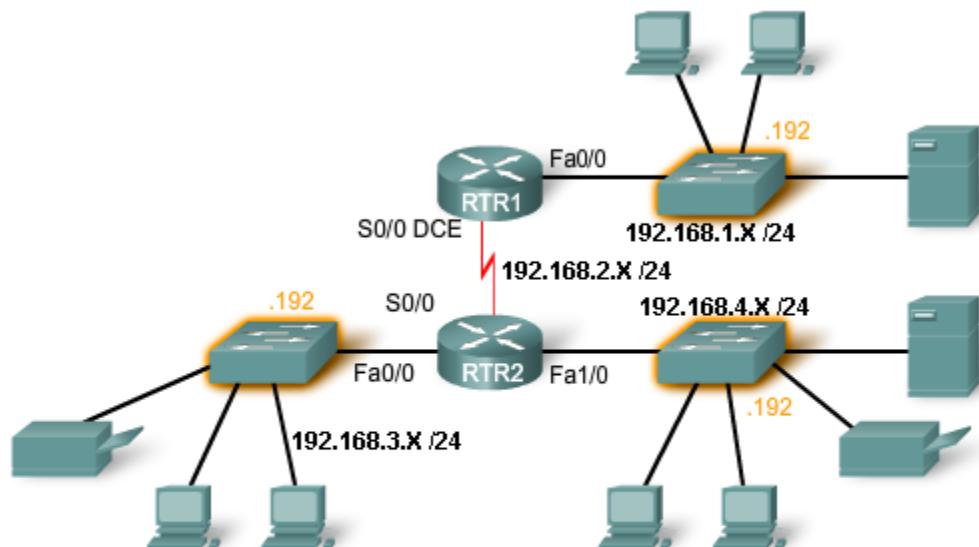
Recursos de red

Interfaces LAN del router

Acceso a la administración

Enlaces WAN del router

Los dispositivos de red 0,192 tiene 0,207.



Usuarios generales

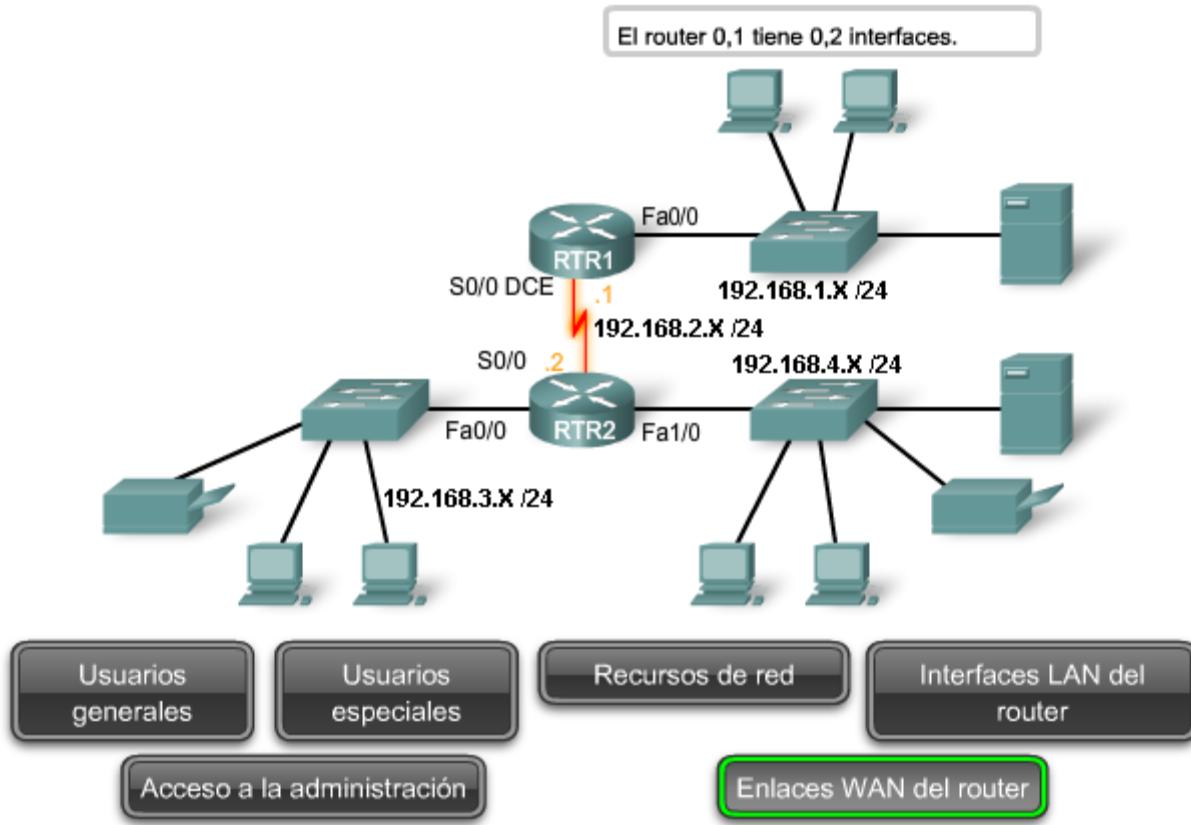
Usuarios especiales

Recursos de red

Interfaces LAN del router

Acceso a la administración

Enlaces WAN del router



10.4 CALCULO DE SUBREDES

10.4.1 Cálculo de direcciones: caso 1

En esta sección, utilizaremos una topología de muestra para practicar la asignación de direcciones a los hosts.

La figura muestra la topología de la red para este ejemplo. Al comenzar con un determinado prefijo (máscara de subred) y dirección IP asignados por el administrador de red, podemos empezar creando nuestra documentación de red.

La cantidad y grupo de hosts es:

LAN de estudiantes

Computadoras de estudiantes: 460

Router (LAN Gateway): 1

Switches (administración): 20

Total por subred de estudiante: 481

LAN de instructores

Computadoras de instructores: 64

Router (LAN Gateway): 1

Switches (administración): 4

Total por subred de instructores: 69

LAN de administradores

Computadoras de administradores: 20

Servidor: 1

Router (LAN Gateway): 1

Switch (administración): 1

Total por subred de administración: 23

WAN

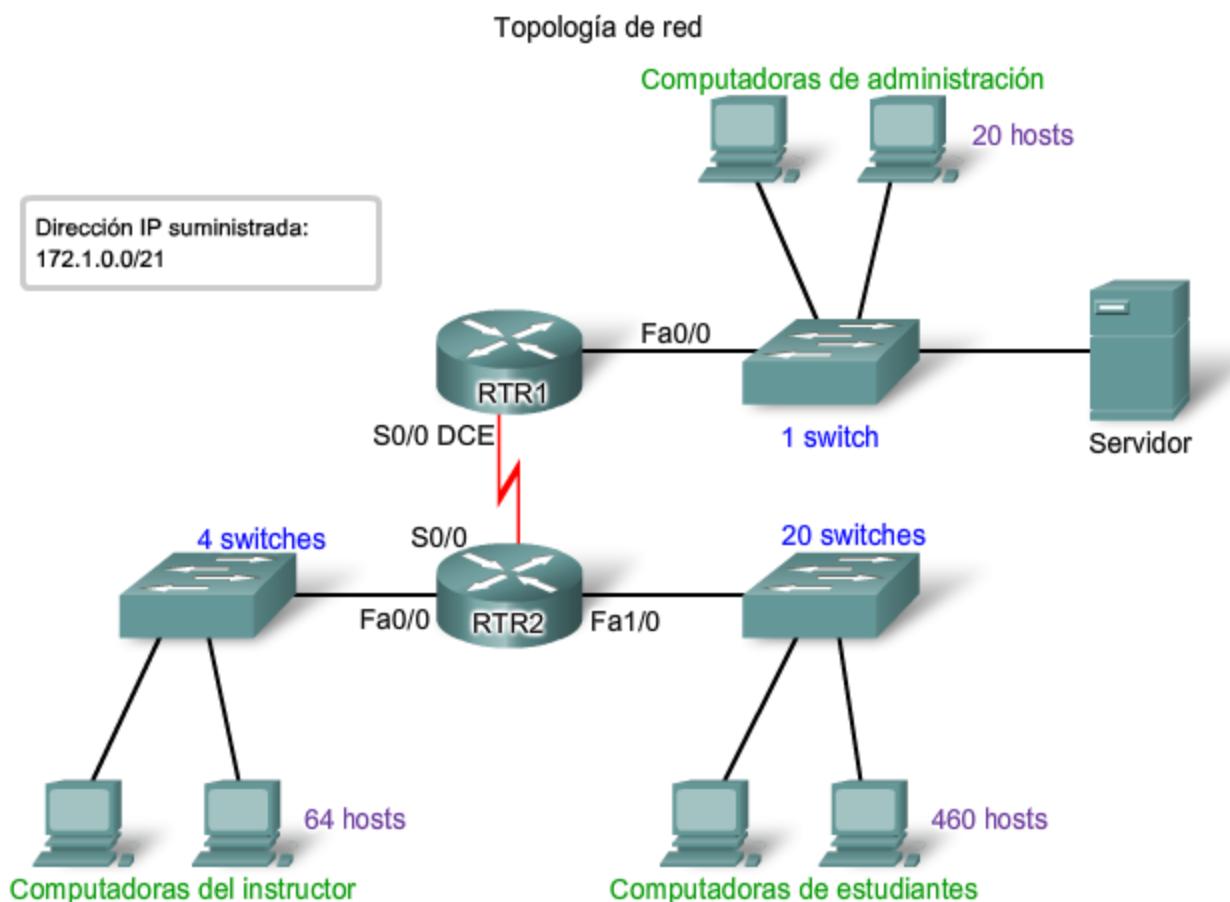
Router – Router WAN: 2

Total por WAN: 2

Métodos de asignación

Existen dos métodos disponibles para asignar direcciones a una internetwork. Se puede utilizar una Máscara de subred de longitud variable (VLSM), donde se asignan el prefijo y los bits de host a cada red basándose en la cantidad de host de esa red. O bien podemos utilizar un enfoque distinto a VLSM, en donde todas las subredes utilizan la misma longitud de prefijo y la misma cantidad de bits del host.

Para el ejemplo de nuestra red, demostraremos los dos enfoques.



Cálculo y asignación de direcciones: sin VLSM

Al utilizar un método de asignación de direcciones distinto a VLSM, todas las subredes tienen la misma cantidad de direcciones asignadas a ellas. A fin de proporcionar a cada red una cantidad adecuada de direcciones, basamos la cantidad de direcciones para todas las redes en los requisitos de direccionamiento para la red más extensa.

En el Caso 1, la LAN de estudiantes es la red más extensa que requiere 481 direcciones.

Utilizaremos esta fórmula para calcular la cantidad de hosts:

$$\text{Hosts utilizables} = 2^n - 2$$

Utilizamos 9 como valor para n ya que es la primera potencia de 2 superior a 481.

Al pedir prestado 9 bits para la porción de host se produce este cálculo:

$$2^9 = 512$$

$$512 - 2 = 510 \text{ direcciones host utilizables}$$

Este cálculo cumple con el requisito actual para al menos 481 direcciones, con una asignación pequeña para el crecimiento. Esto también da como resultado 23 bits de red (32 bits totales, 9 bits de host).

Necesitaremos cuatro bloques de 512 direcciones cada uno por un total de 2048 direcciones ya que existen cuatro redes en nuestra internetwork. Utilizaremos el bloque de direcciones 172.16.0.0 /23. Esto proporciona a las direcciones un rango de 172.16.0.0 a 172.16.7.255.

Examinemos los cálculos de dirección para las redes:

Dirección: 172.16.0.0

En números binarios:

10101100.00010000.00000000.00000000

Máscara: 255.255.254.0

23 bits en números binarios:

11111111.11111111.11111110.00000000

Esta máscara proporcionará los cuatro rangos de direcciones que se muestran en la figura.

LAN estudiante

Para el bloque de red estudiante, los valores serían:

172.16.0.1 a 172.16.1.254 con una dirección broadcast de 172.16.1.255.

LAN administradora

La red administradora requiere un total de 66 direcciones. No se utilizarán las direcciones restantes en este bloque de 512 direcciones. Los valores para la red del administrador son:

de 172.16.2.1 a 172.16.3.254 con una dirección de broadcast de 172.16.3.255.

LAN de instructores

La asignación de un bloque 172.16.4.0 /23. A la LAN de instructores asigna un rango de dirección de:

172.16.4.1 a 172.16.5.254 con una dirección de broadcast de 172.16.5.255.

En realidad, sólo se utilizarán 23 de las 512 direcciones en la LAN de instructores.

WAN

En la WAN, se incluye una conexión punto a punto entre dos routers. Esta red sólo requiere de dos direcciones Ipv4 para los routers en este enlace serial. Como se muestra en la figura, la asignación de este bloque de direcciones al enlace WAN desperdicia 508 direcciones.

Podemos utilizar VLSM en esta internetwork para ahorrar espacio de dirección, pero la utilización de VLSM requiere de mayor planificación. La siguiente sección demuestra la planificación asociada con el uso de VLSM.

Cálculo de direcciones **sin** rangos de direcciones VLSM para subredes

Caso 1

| Red | Direccie subred | Rango de direccie host | Direccie broadcast |
|----------------|-----------------|------------------------|--------------------|
| Estudiante | 172.16.0.0/23 | 172.16.0.1 | 172.16.1.254 |
| Instructor | 172.16.2.0/23 | 172.16.2.1 | 172.16.3.254 |
| Administracib> | 172.16.4.0/23 | 172.16.4.1 | 172.16.5.254 |
| WAN | 172.16.6.0/23 | 172.16.6.1 | 172.16.7.254 |

172.16.0.0 - 172.16.1.255

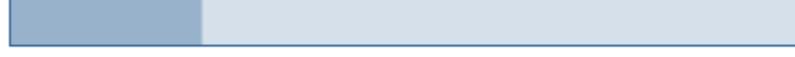
510 direcciones host disponibles en cada subred

481 direcciones utilizadas



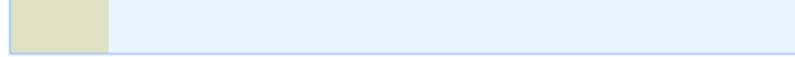
172.16.2.0 - 172.16.3.255

69 direcciones utilizadas



172.16.4.0 - 172.16.5.255

23 direcciones utilizadas



172.16.6.0 - 172.16.7.255

2 direcciones utilizadas



Cálculo y asignación de direcciones: con VLSM

Para la asignación VLSM, podemos asignar un bloque de direcciones mucho menor para cada red, según sea adecuado.

Se ha asignado el bloque de direcciones 172.16.0.0/22 (máscara de subred 255.255.252.0) a esta internetwork en su totalidad. Se utilizarán diez bits para definir direcciones host y subredes. Esto produce un total de 1024 direcciones locales Ipv4 en el rango de 172.16.0.0 a 172.16.3.0.

LAN de estudiantes

La subred más extensa es la LAN de estudiantes que requiere de 460 direcciones.

La utilización de la fórmula hosts utilizables = $2^n - 2$, al pedir prestado 9 bits para la porción del host, da como resultado $512 - 2 = 510$ direcciones host utilizables. Este cálculo cumple con el requisito actual con una asignación pequeña para el crecimiento.

Utilizar 9 bits para los hosts da como resultado 1 bit que puede utilizarse localmente para definir las direcciones de subred. La utilización de la dirección disponible más baja da como resultado una dirección de subred de 172.16.0.0 /23.

El cálculo de la máscara de subred de estudiantes es:

Dirección: 172.16.0.0

En números binarios:

10101100.00010000.00000000.00000000

Máscara: 255.255.254.0

23 bits en números binarios:

11111111.11111111.11111110.00000000

En la red de estudiantes, el rango de host Ipv4 sería de:

172.16.0.1 a 172.16.1.254 con direcciones de broadcast de 172.16.1.255.

Ya que estas direcciones han sido asignadas para la LAN de estudiantes, no se encuentran disponibles para la asignación de las subredes restantes: LAN de instructores, LAN de administradores y WAN. Las direcciones que aún deben asignarse se encuentran en el rango de 172.16.2.0 a 172.16.3.255.

LAN de instructores

La siguiente red más extensa es la LAN de instructores. Esta red requiere de al menos 66 direcciones. La utilización del 6 en la potencia de la fórmula $2^6 - 2$, sólo proporciona 62 direcciones utilizables. Debemos utilizar un bloque de dirección utilizando 7 bits del host. El cálculo $2^7 - 2$ producirá un bloque de 126 direcciones. Esto da como resultado 25 bits para asignar a una dirección de red. El siguiente bloque disponible de este tamaño es la red 172.16.2.0 /25.

Dirección: 172.16.2.0

En números binarios:

10101100.00010000.0000010.00000000

Máscara: 255.255.255.128

25 bits en números binarios:

11111111.11111111.1111111.10000000

Esto provee un rango de host Ipv4 de:

172.16.2.1 a 172.16.2.126 con una dirección de broadcast de 172.16.2.127.

Desde nuestro bloque de direcciones original de 172.16.0.0 /22, asignamos direcciones de 172.16.0.0 a 172.16.2.127. Las direcciones restantes que deben asignarse son de 172.16.2.128 a 172.16.3.255.

LAN de administradores

Para la LAN de administradores, necesitamos adaptar 23 hosts. Esta medida requerirá del uso de 6 bits del host utilizando el cálculo: $2^6 - 2$.

El siguiente bloque disponible de direcciones que puede adaptar estos hosts es el bloque 172.16.2.128 /26.

Dirección: 172.16.2.128

En números binarios:

10101100.00010000.0000010.10000000

Máscara: 255.255.255.192

26 bits en números binarios:

11111111.11111111.1111111.11000000

Esto provee un rango de host Ipv4 de:

172.16.2.129 a 172.16.2.190 con una dirección de broadcast de 172.16.2.191.

Esto produce 62 direcciones Ipv4 únicas para la LAN de administradores.

WAN

El último segmento es la conexión WAN que requiere de 2 direcciones host. Sólo 2 bits del host adaptarán los enlaces WAN. $2^2 - 2 = 2$.

Esto da como resultado 8 bits para definir las direcciones locales de subred. El siguiente bloque de direcciones disponible es 172.16.2.192 /30.

Dirección: 172.16.2.192

En números binarios:

10101100.00010000.0000010.11000000

Máscara: 255.255.255.252

30 bits en números binarios:

11111111.11111111.1111111.11111100

Esto provee un rango de host Ipv4 de:

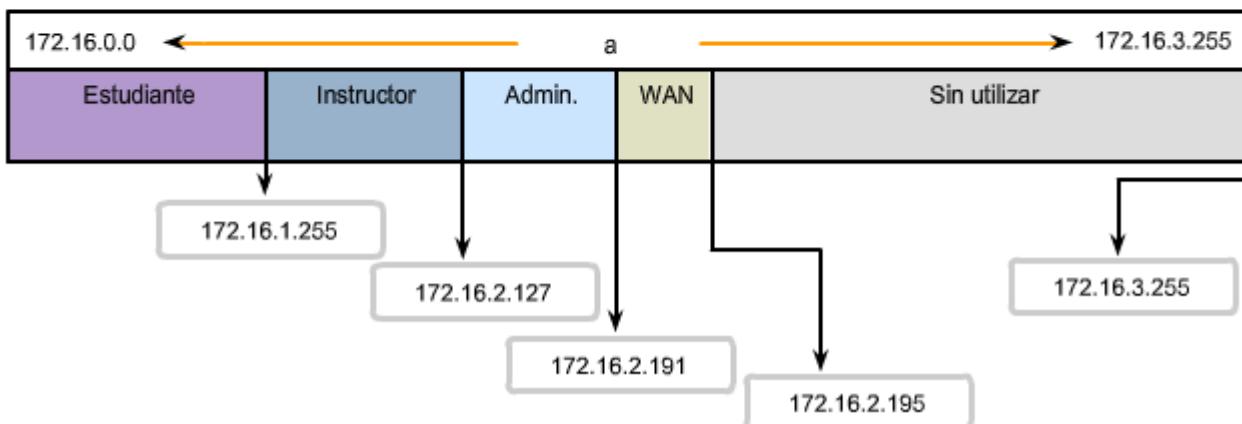
172.16.2.193 a 172.16.2.194 con una dirección de broadcast de 172.16.2.195.

Esto completa la asignación de direcciones utilizando VLSM para el Caso 1. Si es necesario realizar un ajuste para adaptar el crecimiento futuro, aún se encuentran disponibles las direcciones en el rango de 172.16.2.196 a 172.16.3.255.

Cálculo de direcciones con rangos de direcciones VLSM para subredes

Caso 1

| Red | Dirección de subred | Rango de dirección de host | Dirección de broadcast | |
|----------------|---------------------|----------------------------|------------------------|--------------|
| Estudiante | 172.16.0.0/23 | 172.16.0.1 | 172.16.1.254 | 172.16.1.255 |
| Instructor | 172.16.2.0/25 | 172.16.2.1 | 172.16.2.126 | 172.16.2.127 |
| Administración | 172.16.2.128/26 | 172.16.2.129 | 172.16.2.190 | 172.16.2.191 |
| WAN | 172.16.2.192/30 | 172.16.2.193 | 172.16.2.194 | 172.16.2.195 |
| Sin utilizar | na | 172.16.2.197 | 172.16.3.254 | na |



10.4.2 Calculo de direcciones: Caso 2

En el Caso 2, el desafío es dividir esta internetwork en subredes mientras se limita la cantidad de subredes y hosts desperdiciadas.

La figura muestra 5 subredes diferentes, cada una con diferentes requisitos de host. La dirección IP otorgada es 192.168.1.0/24.

Los requisitos de host son:

- Red A: 14 hosts
- Red B: 28 hosts
- Red C: 2 hosts
- Red D: 7 hosts
- Red E: 28 hosts

Como en el Caso 1, se comienza el proceso dividiendo primero en subredes el mayor requisito de host. En este caso, los requisitos más grandes son para la Red B y la Red E, cada una con 28 hosts.

Aplicamos la fórmula: hosts utilizables = $2^n - 2$. Para las redes B y E, se piden prestados 5 bits a la porción de Host y el cálculo es $2^5 = 32 - 2$. Sólo se disponen de 30 direcciones host utilizables debido a las 2 direcciones reservadas. Al pedir prestado 5 bits se cumple con el requisito pero deja poco margen para el crecimiento.

Por lo tanto, se puede considerar pedir prestado 3 bits para las subredes que dará un resultado de 5 bits para los hosts. Esto permite 8 subredes con 30 hosts cada una.

Primero asignamos direcciones para las redes B y E:

La Red B utilizará la Subred 0: 192.168.1.0/27

la dirección host incluye un rango de 1 a 30

La Red E utilizará la Subred 1: 192.168.1.32/27

rango de direcciones host 33 a 62

El mayor requisito de host siguiente es la RedA, seguida de la RedD.

Si se pide prestado otro bit y se divide en subredes la dirección de red 192.168.1.64, se produce un rango de hosts de:

La Red A utilizará la Subred 0: 192.168.1.64/28

la dirección host incluye un rango de 65 a 78

La Red D utilizará la Subred 1: 192.168.1.80/28

rango de direcciones host 81 a 94

Esta asignación admite 14 hosts en cada subred y satisface el requisito.

La Red C tiene sólo dos hosts. Se piden prestado dos bits para cumplir con este requisito.

Si se comienza por 192.168.1.96 y se piden prestados 2 bits más, el resultado es la subred 192.168.1.96/30.

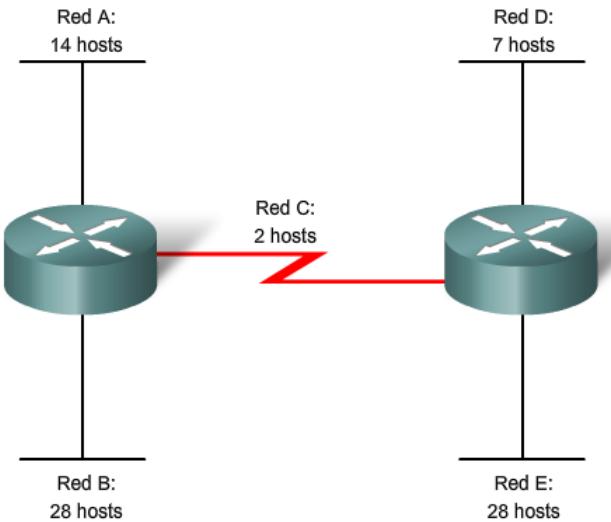
La Red C utilizará la Subred 1: 192.168.1.96/30

la dirección host incluye un rango de 97 a 98

En el Caso 2, hemos cumplido con todos los requisitos sin desperdiciar muchas subredes potenciales y direcciones disponibles.

En este caso, se pidieron prestados los bits de las direcciones que ya habían sido divididas en subredes. Como podrá recordar de la sección anterior, este método se conoce como Máscara de subred de longitud variable o VLSM.

Cálculo de direcciones para requisitos de host



10.5 INTERCONEXION DE DISPOSITIVOS

10.5.1 Interfaces del dispositivo

Es importante comprender que los dispositivos, routers y switches Cisco incluyen varios tipos de interfaces relacionadas con los mismos. Usted ha trabajado con estas interfaces en los laboratorios. En estas interfaces, comúnmente denominadas puertos, los cables se conectan al dispositivo. Consulte la figura para obtener algunos ejemplos de interfaces.

Interfaces LAN – Ethernet

La interfaz Ethernet se utiliza para conectar cables que terminan con dispositivos LAN, como equipos y switches. La interfaz también puede utilizarse para conectar routers entre sí. Este uso se analizará con mayor detalle en cursos futuros.

Son comunes las diversas convenciones para denominar las interfaces Ethernet, que incluyen AUI (dispositivos Cisco antiguos que utilizan un transceptor), Ethernet, FastEthernet y Fa 0/0. El nombre que se utiliza depende del tipo y modelo del dispositivo.

Interfaces WAN: seriales

Las interfaces WAN seriales se utilizan para conectar los dispositivos WAN a la CSU/DSU. CSU/DSU es un dispositivo que se utiliza para realizar una conexión física entre las redes de datos y los circuitos de proveedores de WAN.

También se utilizarán interfaces seriales entre los routers en nuestros laboratorios como parte de diferentes cursos. Para cumplir con el objetivo de esta práctica de laboratorio, haremos una conexión interconectada entre dos routers utilizando cables seriales y estableceremos la frecuencia de reloj en una de las interfaces.

Posiblemente también necesite configurar otros parámetros de la capa Física y de Enlace de datos en un router. Para establecer una comunicación con un router mediante una consola en una WAN remota, se asigna una dirección de Capa 3 (dirección Ipv4) a la interfaz WAN.

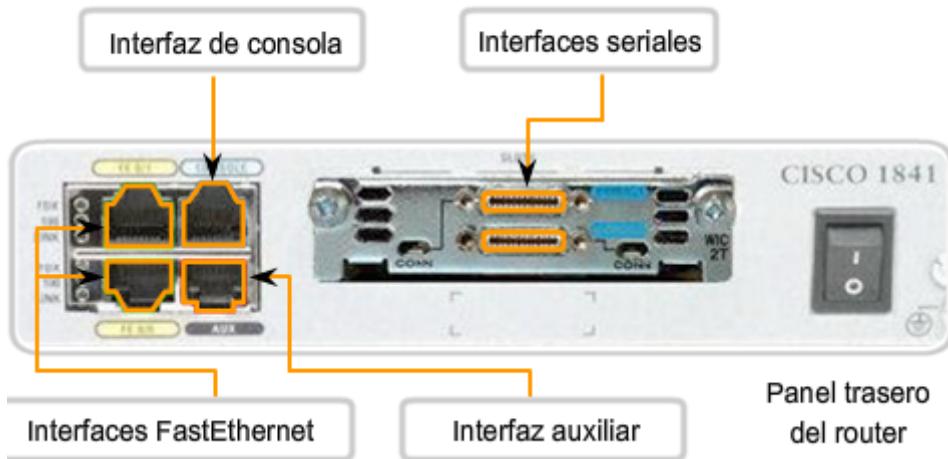
Interfaz de consola

La interfaz de consola es la interfaz principal para la configuración inicial de un switch o router Cisco. Es además un medio importante para la resolución de problemas. Es importante observar que, mediante el acceso físico a la interfaz de consola del router, una persona no autorizada puede interrumpir o comprometer el tráfico de la red. **Es extremadamente importante la seguridad física de los dispositivos de red.**

Interfaz Auxiliar (AUX)

Esta interfaz se utiliza para la administración remota del router. Generalmente, se conecta un módem a la interfaz AUX para obtener acceso telefónico. Desde el punto de vista de la seguridad, habilitar la opción para conectarse en forma remota a un dispositivo de red implica la responsabilidad de mantener una administración de dispositivos alerta.

Ejemplo de interfaces de dispositivos



10.5.2 Conexión de administración de dispositivos

Generalmente, los dispositivos de red no tienen sus propias pantallas, teclados o dispositivos de entrada como un trackball o un mouse. El acceso a un dispositivo de red para la configuración, verificación o resolución de problemas se realiza mediante una conexión entre el dispositivo y una computadora. Para lograr esta conexión, la computadora ejecuta un programa denominado emulador de terminal.

Un emulador de terminal es un programa de software que permite a una computadora acceder a las funciones en otro dispositivo. Este programa permite a una persona utilizar la pantalla y el teclado de una computadora para operar otro dispositivo, como si el teclado y la pantalla estuvieran directamente conectados a otro dispositivo. La conexión de cables entre la computadora que ejecuta el programa de emulación de terminal y el dispositivo a menudo se realiza mediante la interfaz serial.

Si desea conectarse a un router o switch para administrar un dispositivo utilizando una emulación de terminal, cumpla con los siguientes pasos:

Paso 1:

Conecte un equipo al puerto de consola mediante el cable de la consola que suministra Cisco. El cable de consola, suministrado con un router y un switch, incluye un conector DB-9 en un extremo y un conector RJ-45 en el otro. (Los dispositivos Cisco antiguos incluían un adaptador RJ-45 a DB-9. Este adaptador se utiliza con un cable de consola que tiene un conector RJ-45 en cada extremo).

La conexión a la consola se realiza al enchufar el conector DB-9 en un puerto serial EIA/TIA 232 disponible en la computadora. Es importante recordar que si existe más de un puerto serial, deberá observar qué número de puerto se utiliza para la conexión a la consola. Una vez que se realiza la conexión serial a la computadora, conecte el extremo del cable RJ-45 directamente en la interfaz de la consola en el router.

Muchas de las computadoras más nuevas no cuentan con una interfaz serial EIA/TIA 232. Si su computadora sólo tiene una interfaz USB, utilice un cable de conversión serial a USB para acceder al puerto de consola. Conecte el cable de conversión a un puerto USB en la computadora y luego conecte el cable de consola o el adaptador RJ-45 a DB-9 a este cable.

Paso 2:

En el caso de los dispositivos conectados directamente a través de un cable, configure un emulador de terminal con las configuraciones correspondientes. Las instrucciones exactas para configurar un emulador de terminal dependerán del emulador específico. Para cumplir con el objetivo de este curso, generalmente utilizamos HyperTerminal, ya que se incluye en la mayoría de los tipos de Windows. Este programa puede encontrarse en Todos los programas > Accesorios > Comunicaciones. Seleccionar HyperTerminal.

Abra HyperTerminal, confirme el número de puerto serial elegido y luego configure el puerto con las siguientes configuraciones:

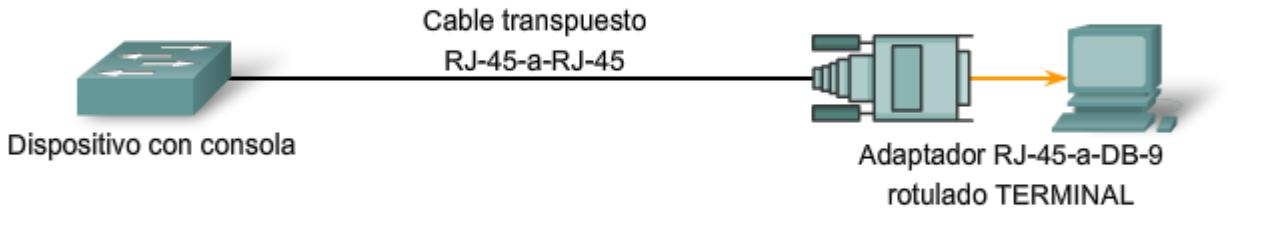
- Bits por segundo: 9600 bps
- Bits de datos: 8
- Paridad: Ninguna
- Bits de parada: 1
- Control de flujo: Ninguno

Paso 3:

Inicie sesión en el router mediante el software emulador de terminal. Si se realizan correctamente todas las configuraciones y conexiones de cables, podrá acceder al router al presionar la tecla Intro del teclado.

Durante la práctica de laboratorio, usted tendrá la oportunidad de utilizar varios tipos de emuladores de terminal. Pueden tener aspecto diferente pero sus funciones son las mismas.

La conexión de administración de dispositivos



- Las PC requieren un adaptador RJ-45 a DB-9 o RJ-45 a DB-25.
- Las configuraciones del puerto COM son 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada, sin control del flujo.
- Esto proporciona acceso de consola fuera de banda.
- El puerto auxiliar del switch se puede usar para una consola conectada por módem.

10.7 RESUMEN DEL CAPITULO

10.7.1 Resumen y revisión

En este capítulo se analizaron los procesos de diseño y planificación que contribuyen a la instalación de una red operativa exitosa.

Se consideraron los diferentes tipos de medios LAN y WAN, además de sus cables y conectores relacionados, para poder tomar las decisiones más adecuadas sobre interconexión.

Al determinar la cantidad de hosts y subredes en una red requerida en la actualidad (y al planificarla de manera simultánea para el crecimiento futuro), se garantiza la disponibilidad de las comunicaciones de datos combinando de la mejor manera el costo y el rendimiento.

De manera similar, un esquema de direccionamiento planificado e implementado de manera constante es un factor importante al garantizar el funcionamiento adecuado de las redes con adaptación a las disposiciones según sea necesario. Dichos esquemas de direccionamiento también facilitan la configuración y resolución de problemas.

El acceso de terminal a los routers y switches es un medio para configurar direcciones y características de red en estos dispositivos.

En este capítulo, aprendió a:

- Identificar los medios de red básicos necesarios para realizar una conexión LAN.
- Identificar los tipos de conexiones para conexiones de dispositivos intermedios y finales en una LAN.
- Identificar las configuraciones de diagrama de pines para cables de conexión directa y conexión cruzada.
- Identificar los tipos de cableado, estándares y puertos utilizados para conexiones WAN.
- Definir el rol de las conexiones de administración de dispositivos cuando se utilizan equipos Cisco.
- Diseñar un esquema de direccionamiento para una internetwork y asignar rangos para los hosts, los dispositivos de red y la interfaz del router.
- Comparar y contrastar la importancia de los diseños de redes.

11 - CONFIGURACION Y VERIFICACION DE SU RED

11.0 CONFIGURACION Y VERIFICACION DE SU RED

11.0.1 Introducción del capítulo

En este capítulo analizaremos el proceso para conectar y configurar equipos, switches y routers en una LAN Ethernet.

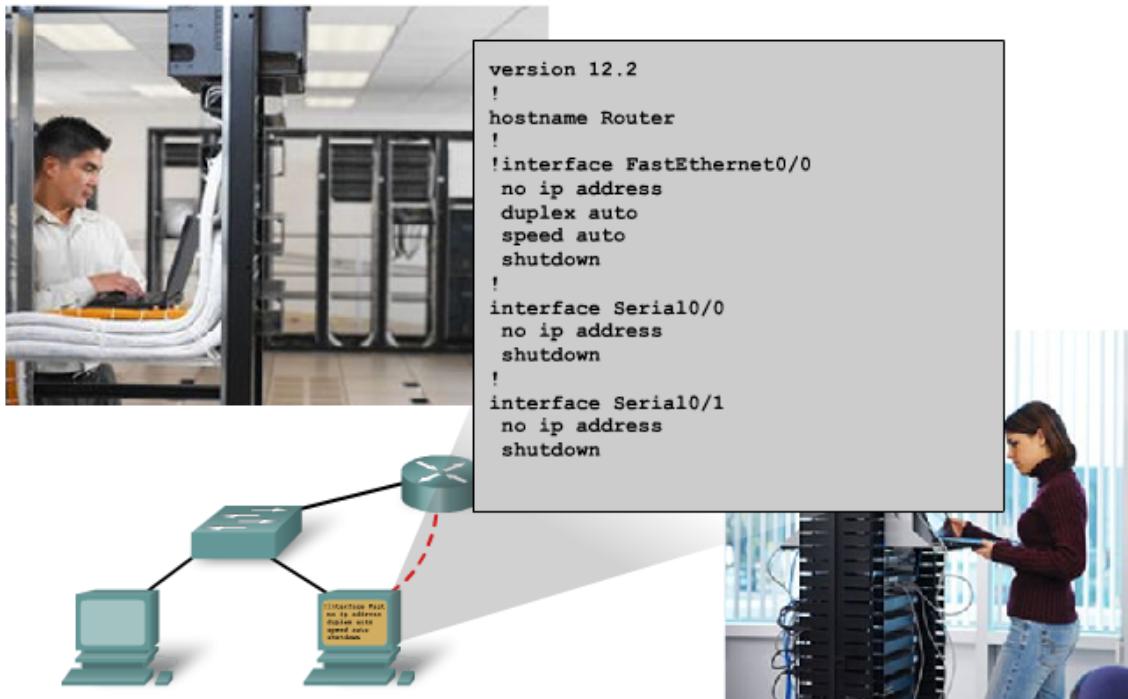
Presentaremos los procedimientos básicos de configuración para dispositivos de red Cisco. Estos procedimientos requieren la utilización del Sistema operativo Internetwork (IOS) de Cisco y de los archivos de configuración relacionados para los dispositivos intermedios.

Resulta esencial la comprensión del proceso de configuración con IOS por parte de los administradores de red y de los técnicos de red. Las prácticas de laboratorio permitirán la familiarización con las prácticas comunes utilizadas para configurar y monitorear los dispositivos Cisco.

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

- Definir la función del Sistema operativo Internetwork (IOS).
- Definir el propósito de un archivo de configuración.
- Identificar las diversas clases de dispositivos que tienen IOS incorporado.
- Identificar los factores que contribuyen al conjunto de comandos IOS disponible para un dispositivo.
- Identificar los modos de operación de IOS.
- Identificar los comandos básicos de IOS.
- Comparar y contrastar los comandos show básicos.



Configuración y prueba de la red

11.1 CONFIGURACION DE DISPOSITIVOS CISCO – PRINCIPIOS BASICOS DE IOS

11.1.1 Cisco IOS

Al igual que una computadora personal, un router o switch no puede funcionar sin un sistema operativo. Sin un sistema operativo, el hardware no puede realizar ninguna función. El sistema operativo Internetwork (IOS) de Cisco es el software del sistema en dispositivos Cisco. Es la tecnología principal de Cisco y está presente en casi todos sus productos. El Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbricos, grandes routers con decenas de interfaces y muchos otros dispositivos.

El Cisco IOS provee a los dispositivos los siguientes servicios de red:

- Funciones básicas de enrutamiento y conmutación.
- Acceso confiable y seguro a recursos en red.
- Escalabilidad de la red.

Los detalles operativos de IOS varían de acuerdo con los diferentes dispositivos de internetworking, según el propósito y el conjunto de características del dispositivo.

Por lo general, se tiene acceso a los servicios que proporciona el IOS de Cisco mediante una Interfaz de línea de comandos (CLI). Las funciones accesibles a través de la CLI varían según la versión de IOS y el tipo de dispositivo.

El archivo IOS en sí tiene un tamaño de varios megabytes y se encuentra en un área de memoria semipermanente llamada flash. La memoria flash provee almacenamiento no volátil. Esto significa que los contenidos de la memoria no se pierden cuando el dispositivo se apaga. Aunque los contenidos no se pierden, pueden modificarse o sobreescibirse si es necesario.

El uso de memoria flash permite que se actualice el IOS a versiones más nuevas o que se incorporen nuevas funciones. En muchas arquitecturas de router, el IOS se copia en la RAM cuando se enciende el dispositivo y el IOS se ejecuta desde la RAM cuando el dispositivo está funcionando. Esta función mejora el rendimiento del dispositivo.

Cisco IOS



Sistema operativo de Internetwork para dispositivos de networking de Cisco



Métodos de acceso

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

- Consola
- Telnet o SSH
- Puerto auxiliar

Consola

Se puede tener acceso a la CLI a través de una sesión de consola, también denominada línea CTY. La consola usa una conexión serial de baja velocidad para conectar directamente un equipo o un terminal al puerto de consola en el router o switch.

El puerto de consola es un puerto de administración que provee acceso al router fuera de banda. Es posible acceder al puerto de consola aunque no se hayan configurado servicios de networking en el dispositivo. **El puerto de consola se suele utilizar para tener acceso a un dispositivo cuando no se han iniciado o han fallado los servicios de networking.**

Ejemplos del uso de la consola son:

- La configuración de inicio del dispositivo de red.
- Procedimientos de recuperación de desastres y resolución de problemas donde no es posible el acceso remoto.
- Procedimientos de recuperación de contraseña.

Cuando un router se pone en funcionamiento por primera vez, no se han configurado los parámetros de networking. Por lo tanto, el router no puede comunicarse a través de una red. Para preparar la puesta en marcha y configuración iniciales, se conecta un equipo que ejecuta un software de emulación de terminal al puerto de consola del dispositivo. En el equipo conectado pueden ingresarse los comandos de configuración para iniciar el router.

Durante el funcionamiento, si no se puede acceder a un router en forma remota, una conexión a la consola puede permitir a un equipo determinar el estado del dispositivo. En forma predeterminada, la consola comunica el inicio del dispositivo, la depuración y los mensajes de error.

Para muchos dispositivos Cisco, 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. **Debe colocarse el dispositivo en un cuarto cerrado con llave o en un bastidor de equipos para impedir el acceso físico.**

Telnet y SSH

Un método que sirve para acceder en forma remota a la sesión CLI es hacer telnet al router. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de networking activos en el dispositivo. El dispositivo de red debe tener configurada por lo menos una interfaz activa con una dirección de Capa 3, como por ejemplo una dirección Ipv4. Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que se activa cuando se inicia el dispositivo. El IOS también contiene un cliente Telnet.

Un host con un cliente Telnet puede acceder a las sesiones vty que se ejecutan en el dispositivo Cisco. Por razones de seguridad, el IOS requiere que la sesión Telnet use una contraseña, como método mínimo de autenticación. Los métodos para establecer las conexiones y contraseñas se analizarán en una sección posterior.

El Secure Shell protocol (SSH) es un método que ofrece más seguridad en el acceso al dispositivo remoto. Este protocolo provee la estructura para una conexión remota similar a Telnet, salvo 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. La sesión SSH encripta todas las comunicaciones entre el cliente y el dispositivo IOS. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. **Una mejor práctica es utilizar siempre SSH en lugar de Telnet, siempre que sea posible.**

La mayoría de las versiones más recientes de IOS contienen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren la activación del servidor SSH.

Los dispositivos IOS también incluyen un cliente SSH que puede utilizarse para establecer sesiones SSH con otros dispositivos. De manera similar, puede utilizarse un equipo remoto con un cliente SSH para iniciar una sesión de CLI

segura. No se provee el software de cliente SSH de manera predeterminada en los sistemas operativos de todos los equipos. Es posible que deba adquirir, instalar y configurar el software de cliente SSH en su equipo.

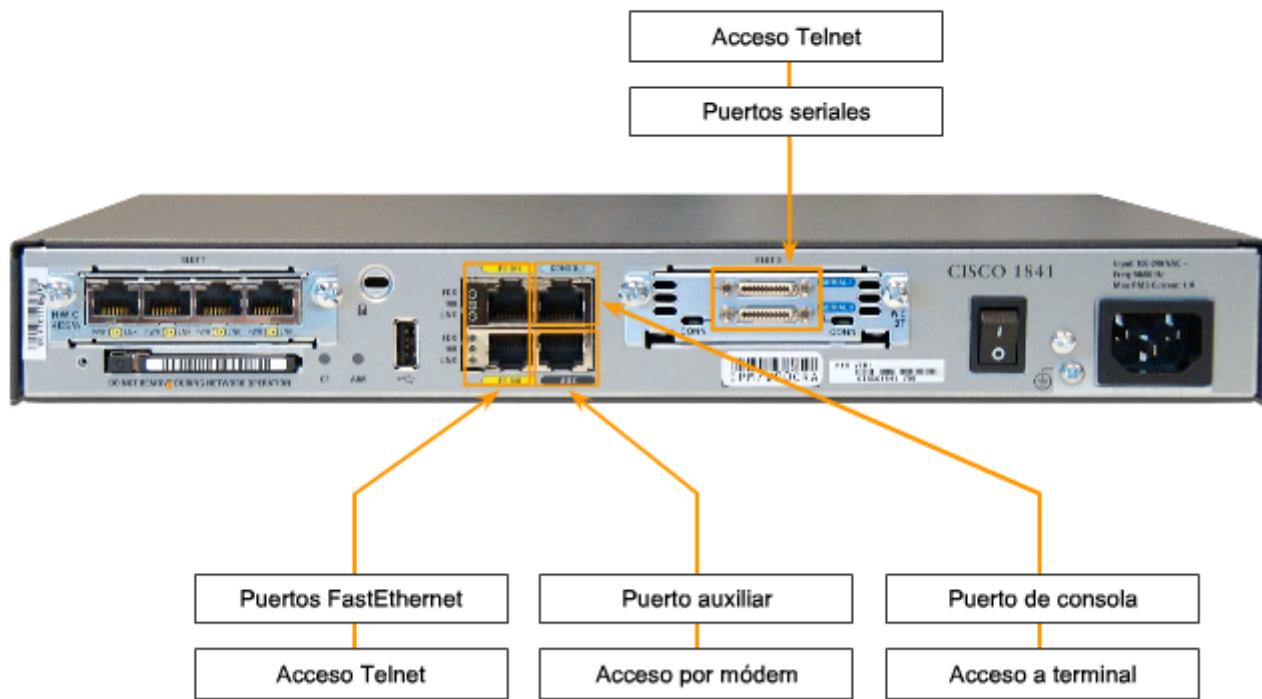
Auxiliar

Otra manera de establecer una sesión CLI en forma remota es a través de una conexión de marcado telefónico mediante un módem conectado al puerto auxiliar del router. De manera similar a la conexión de consola, este método no requiere ningún servicio de networking para configurarlo o activarlo en el dispositivo.

El puerto auxiliar también puede usarse en forma local, como el puerto de consola, con una conexión directa a un equipo que ejecute un programa de emulación de terminal. El puerto de consola es necesario para la configuración del router, pero no todos los routers tienen un puerto auxiliar. También se prefiere el puerto de consola antes que el puerto auxiliar para la resolución de problemas, ya que muestra de manera predeterminada la puesta en marcha del router, la depuración y los mensajes de error.

Generalmente, en la única oportunidad que el puerto auxiliar se usa en forma local en lugar del puerto de consola es cuando surgen problemas en el uso del puerto de consola, como por ejemplo cuando no se conocen ciertos parámetros de consola.

Acceso a Cisco IOS en un dispositivo



11.1.2 Archivo de configuración

Los dispositivos de red dependen de dos tipos de software para su funcionamiento: el sistema operativo y la configuración. Al igual que el sistema operativo en cualquier equipo, el sistema operativo facilita la operación básica de los componentes de hardware del dispositivo.

Los archivos de configuración contienen los comandos del software IOS de Cisco utilizados para personalizar la funcionalidad de un dispositivo Cisco. Los comandos son analizados (traducidos y ejecutados) por el software IOS de

Cisco cuando inicia el sistema (desde el archivo startup-config) o cuando se ingresan los comandos en la CLI mientras está en modo configuración.

El administrador de red crea una configuración que define la funcionalidad deseada del dispositivo Cisco. El tamaño del archivo de configuración normalmente es de unos cientos a unos miles de bytes.

Tipos de archivos de configuración

- Un dispositivo de red Cisco contiene dos archivos de configuración:
- El archivo de configuración en ejecución, utilizado durante la operación actual del dispositivo
- El archivo de configuración de inicio, utilizado como la configuración de respaldo, se carga al iniciar el dispositivo

También puede almacenarse un archivo de configuración en forma remota en un servidor a modo de respaldo.

Archivo de configuración de inicio

El archivo de configuración de inicio (startup-config) se usa durante el inicio del sistema para configurar el dispositivo. El **archivo de configuración de inicio o el archivo startup-config** se almacena en la RAM no volátil (NVRAM). Como la NVRAM es no volátil, el archivo permanece intacto cuando el dispositivo Cisco se apaga. Los archivos startup-config se cargan en la RAM cada vez que se inicia o se vuelve a cargar el router. Una vez que se ha cargado el archivo de configuración en la RAM, se considera la **configuración en ejecución o running-config**.

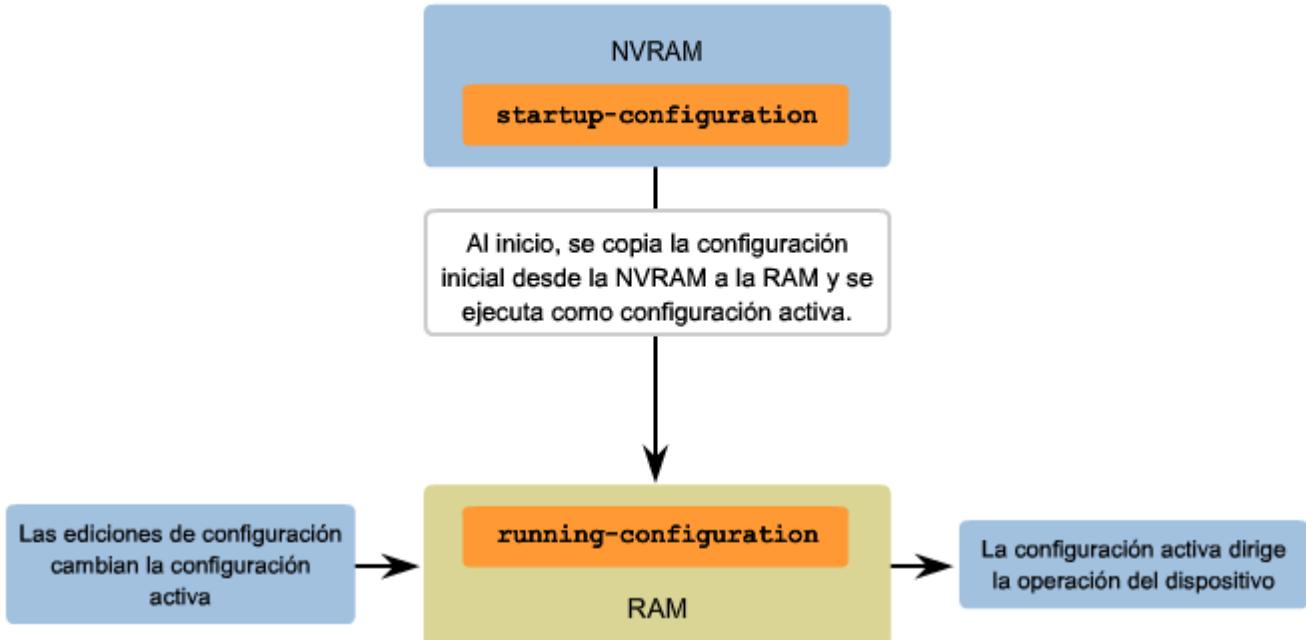
Configuración en ejecución

Una vez en la RAM, esta configuración se utiliza para operar el dispositivo de red.

La configuración en ejecución se modifica cuando el administrador de red realiza la configuración del dispositivo. **Los cambios en la configuración en ejecución afectarán la operación del dispositivo Cisco en forma inmediata**. Luego de realizar los cambios necesarios, el administrador tiene la opción de guardar tales cambios en el archivo startup-config, de manera que se utilicen la próxima vez que se reinicie el dispositivo.

Como el archivo de configuración en ejecución se encuentra en la RAM, se pierde si se apaga la energía que alimenta al dispositivo o si se reinicia el dispositivo. También se perderán los cambios realizados en el archivo running-config si no se guardan en el archivo startup-config antes de apagar el dispositivo.

Archivos de configuración



11.1.3 Modos Cisco IOS

El Cisco IOS está diseñado como un sistema operativo modal. El término modal describe un sistema en el que hay distintos modos de operación, cada uno con su propio dominio de operación. La CLI utiliza una estructura jerárquica para los modos.

En orden descendente, los principales modos son:

- Modo de ejecución usuario
- Modo de ejecución privilegiado
- Modo de configuración global
- Otros modos de configuración específicos

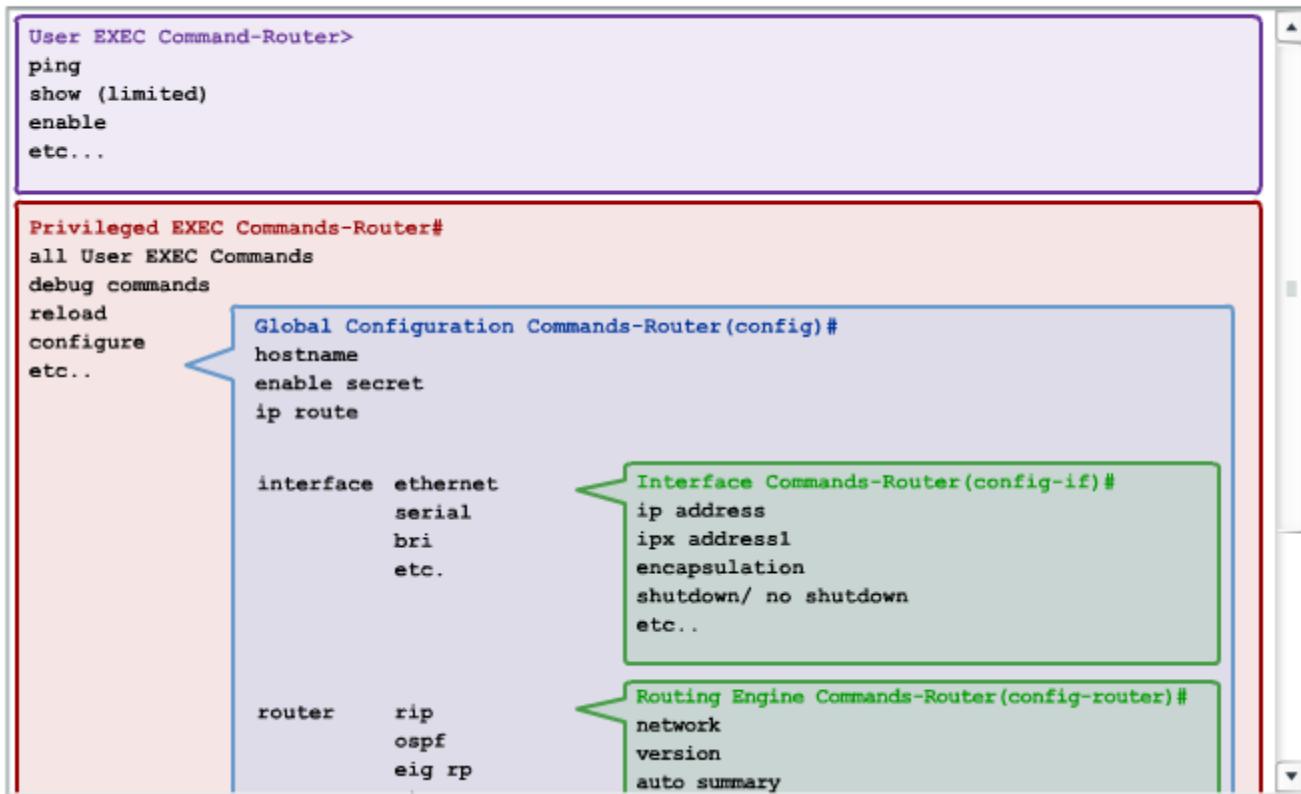
Cada modo se utiliza para cumplir determinadas tareas y tiene un conjunto específico de comandos que se encuentran disponibles cuando el modo está habilitado. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces. Todas las configuraciones que se ingresan en el modo de configuración de interfaz se aplican sólo a esa interfaz.

Algunos comandos están disponibles para todos los usuarios; otros pueden ejecutarse únicamente después de ingresar el modo en el que ese comando está disponible. Cada modo se distingue por una petición de entrada singular y sólo se permiten los comandos apropiados para ese modo.

Se puede configurar la estructura modal jerárquica a fin de 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.

La figura muestra la estructura modal de IOS con funciones y peticiones de entrada típicas.

Estructura jerárquica del modo IOS



Peticiones de entrada de comando

Cuando se usa la CLI, el modo se identifica mediante la petición de entrada de línea de comandos que es exclusiva de ese modo. La petición de entrada está compuesta por las palabras y los símbolos en la línea a la izquierda del área de entrada. Se usa la frase petición de entrada porque el sistema le solicita que ejecute una entrada.

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 por defecto para el modo de configuración global en un router sería:

Router(config)#

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

Estructura del indicador del IOS

```
Router>ping 192.168.10.5  
Router#show running-config  
  
Router(config)#Interface FastEthernet 0/0  
  
Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

El indicador cambia para indicar el modo CLI actual.

```
Switch>ping 192.168.10.9  
Switch#show running-config  
  
Switch(config)#Interface FastEthernet 0/0  
  
Switch(config-if)#Description connection to WEST LAN4
```

Modos principales

Los dos modos de operación principales son:

- EXEC del usuario
- EXEC privilegiado

Como característica de seguridad, el software IOS de Cisco divide las sesiones EXEC en dos modos de acceso. Estos dos modos de acceso principales se usan dentro de la estructura jerárquica de la CLI de Cisco.

Cada modo tiene comandos similares. Sin embargo, el modo EXEC privilegiado tiene un nivel de autoridad superior en cuanto a lo que permite que se ejecute.

Modo de ejecución usuario

El modo de ejecución usuario o, para abreviar, EXEC del usuario, tiene capacidades limitadas pero resulta útil en el caso de algunas operaciones básicas. El modo EXEC usuario se encuentra en la parte superior de la estructura jerárquica modal. Este modo es la primera entrada en la CLI de un router IOS.

El modo EXEC 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 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 usuario desde la consola. Siempre conviene asegurarse de que se configure la autenticación durante la configuración inicial.

El modo EXEC 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 comandos de configuración y administración requiere que el administrador de red use el modo EXEC privilegiado, o un modo específico que esté más abajo en la jerarquía.

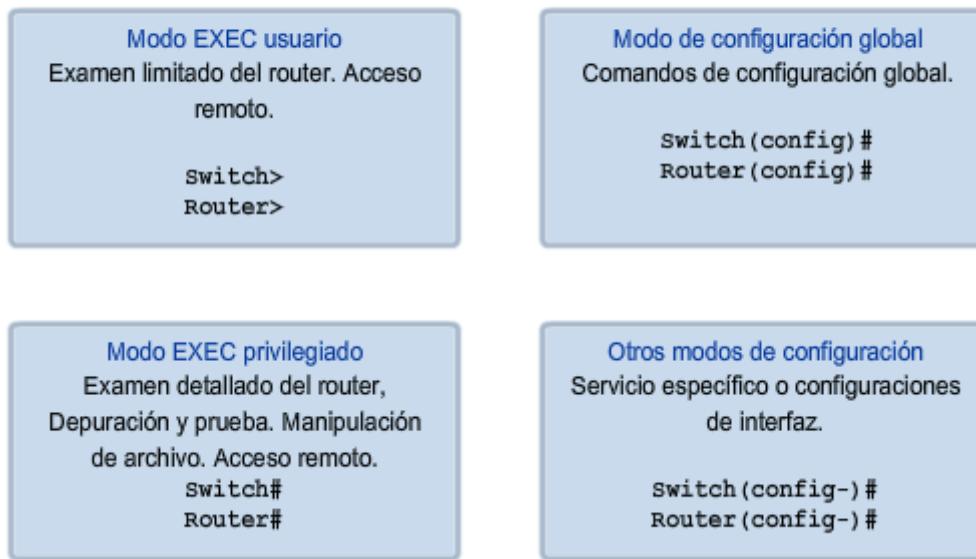
El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #.

Switch#

En forma predeterminada, 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.

Modos principales del IOS



Intercambio entre los modos EXEC usuario y EXEC privilegiado

Los comandos enable y disable se usan para cambiar la CLI entre el modo EXEC 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:

Router>enable

Este comando se ejecuta sin la necesidad de un argumento o una palabra clave. Cuando se presiona <Intro>, la petición e entrada del router cambia a:

Router#

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

Si se ha configurado la autenticación de la contraseña para el modo EXEC privilegiado, el IOS pide la contraseña.

Por ejemplo:

Router>enable

Password:

Router#

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

Por ejemplo:

Router#disable

Router>

Modos del IOS

```
Router con0 is now available.  
Press RETURN to get started.  
  
User Access Verification  
Password:  
Router>← Indicador de modo usuario  
Router>enable  
Router#← Modo privilegiado  
Password:  
Router#← Indicador de modo usuario  
Router#disable  
Router>← Indicador de modo usuario  
Router>exit
```

11.1.4 Estructura básica de comandos IOS

Cada comando de IOS tiene un formato o sintaxis específicos y se ejecuta con la petición de entrada correspondiente. 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. La figura muestra estas partes de un comando.

El comando es la palabra o las palabras iniciales ingresadas en la línea de comandos. Los comandos no distinguen mayúsculas de minúsculas. A continuación del comando siguen una o más palabras clave y argumentos.

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 pueden usarse para definir el resultado particular que se mostrará. Por ejemplo:

```
Switch#show running-config
```

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

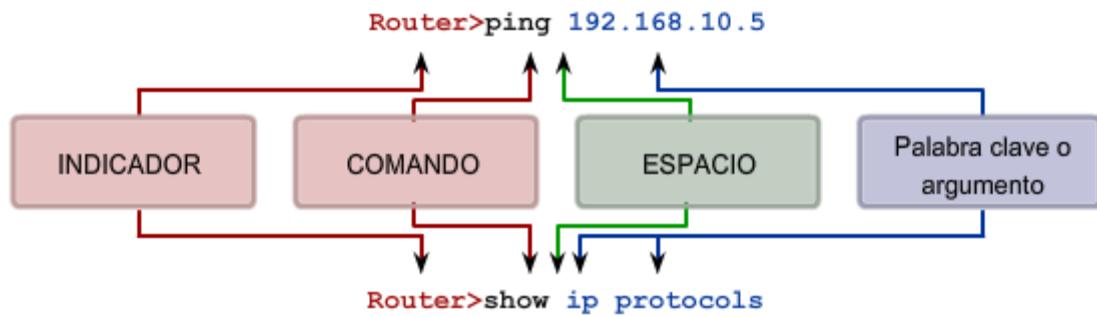
Un comando puede requerir uno o más argumentos. A diferencia de una palabra clave, generalmente un argumento no es una palabra predefinida. Un argumento es un valor o una variable definida por el usuario. Como ejemplo, cuando se solicita una descripción a una interfaz con el comando description, se debe ingresar una línea de estas características:

```
Switch(config-if)#description MainHQ Office Switch
```

El comando es: description. El argumento es: MainHQ Office Switch. El usuario define el argumento. Para este comando, el argumento puede ser cualquier cadena de texto con un máximo de 80 caracteres.

Después de ingresar cada comando completo, incluso cualquier palabra clave y argumento, presione la tecla <Intro> para enviar el comando al intérprete de comandos.

Estructura básica de comandos del IOS



Los comandos del indicador están seguidos de un espacio y luego una palabra clave o argumentos.

Convenciones de IOS

La figura y los siguientes ejemplos demuestran algunas convenciones para documentar comandos IOS.

Para el comando ping :

Formato:

```
Router>ping Dirección IP
```

Ejemplo con valores:

Router>ping 10.10.10.5

El comando es ping y el argumento es la Dirección IP.

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

Formato:

Switch>traceroute Dirección IP

Ejemplo con valores:

Switch>traceroute 192.168.254.254

El comando es traceroute y el argumento es la Dirección IP.

Los comandos se utilizan para ejecutar una acción y las palabras clave se utilizan para identificar dónde o cuándo ejecutar el comando.

Por citar otro ejemplo, vuelva a examinar el comando description .

Formato:

Router(config-if)#description cadena

Ejemplo con valores:

Switch(config-if)#description Interfaz para crear una LAN

El comando es description y el argumento aplicado a la interfaz es la cadena de texto, Interfaz para crear una LAN. Una vez que se ejecuta el comando, esa descripción se aplicará a la interfaz específica.

Convenciones de denominación del IOS

Cuando se describe el uso de comandos, generalmente utilizamos estas convenciones.

| Convención | Descripción |
|----------------|---|
| negrita | El texto en negrita indica comandos y palabras clave que se introducen literalmente como se muestra. |
| <i>cursiva</i> | El texto en cursiva indica los argumentos donde el usuario suministra valores. |
| [X] | Los corchetes encierran un elemento opcional (palabra clave o argumento). |
| | Una línea vertical indica una opción dentro de un conjunto opcional o requerido de palabras clave o argumentos. |
| [X Y] | Los corchetes encierran un elemento opcional (palabra clave o argumento). |
| {X Y} | Las llaves que encierran palabras clave o argumentos separados por una línea vertical indican una opción requerida. |

11.1.5 Uso de la ayuda de la CLI

El IOS ofrece varias formas de ayuda:

- Ayuda sensible al contexto
- Verificación de la sintaxis del comando
- Teclas de acceso rápido y accesos directos

Ayuda sensible al contexto

La ayuda sensible al contexto proporciona una lista de comandos y los argumentos asociados con esos comandos dentro del contexto del modo actual. Para acceder a la ayuda contextual, ingrese un signo de interrogación (?) ante cualquier petición de entrada. Habrá una respuesta inmediata sin necesidad de usar la tecla <Intro>.

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 usuario, ingrese un signo de interrogación ? ante la petición de entrada del router.

Otro de los usos de la ayuda contextual es para visualizar una lista de los comandos o palabras clave que empiezan con uno o varios caracteres específicos. Después de ingresar una secuencia de caracteres, si inmediatamente se ingresa un signo de interrogación, sin espacio, el IOS mostrará una lista de comandos o palabras clave para este contexto que comienzan con los caracteres ingresados.

Por ejemplo, ingrese sh? Para obtener una lista de los comandos que empiezan con la secuencia de caracteres sh.

Un último tipo de ayuda contextual se utiliza para determinar qué opciones, palabras clave o argumentos concuerdan con un comando específico. Cuando ingresa un comando, escriba un espacio seguido de ? para determinar qué puede o debe ingresarse a continuación.

Como se muestra en la figura, después de ingresar el comando clock set 19:50:00, podemos ingresar el signo ? para determinar las opciones o palabras clave adecuadas para este comando.

Ayuda contextual

Ejemplo de una secuencia de comandos usando la ayuda contextual de CLI

```
Cisco#cl?
clear clock
Cisco#clock ?
  set Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

Explicaciones de comandos

Mensajes de comandos incompletos

Mensajes de entradas no válidas

Formatos variables

```
Cisco#clock set 19:50:00 ?
<1-31> Day of the month
MONTH Month of the year
Cisco#clock set 19:50:00 25 6
^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
<1993-2035> Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Verificación de sintaxis de comando

Cuando se envía un comando al presionar la tecla <Intro>, el intérprete de la línea de comandos analiza al comando de izquierda a derecha para determinar qué acción se está solicitando. El IOS generalmente provee sólo comentarios negativos. 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.

Existen tres tipos diferentes de mensajes de error:

- Comando ambiguo
- Comando incompleto
- Comando incorrecto

Vea la figura para conocer los tipos de errores y las soluciones.

Ayuda para verificar la sintaxis de comandos

El IOS devuelve un mensaje de ayuda que indica que las palabras clave o los argumentos se omitieron del final del comando:

```
Switch#>clock set  
% Incomplete command.  
Switch#clock set 19:50:00  
% Incomplete command.
```

El IOS devuelve un mensaje de ayuda para indicar que no hay suficientes caracteres introducidos para que el intérprete de comandos reconozca el comando.

```
Switch#c  
% Ambiguous command: 'c'
```

El IOS devuelve un "^" para indicar dónde el intérprete de comandos no puede descifrar el comando:

```
Switch#clock set 19:50:00 25 ^  
% Invalid input detected at '^' marker.
```

Ayuda para verificar la sintaxis de comandos

| Mensaje de error | Significado | Ejemplos | Cómo obtener ayuda |
|--|--|---|---|
| % Ambiguous command: 'command' | no se introdujeron suficientes caracteres para que el IOS reconozca el comando | Switch# c % Ambiguous command: 'c' | Vuelva a introducir el comando seguido de un signo de interrogación (?) sin ningún espacio entre el comando y el signo de interrogación. Aparecen las posibles palabras clave que puede introducir con el comando. |
| % Incomplete command. | no se ingresaron todas las palabras clave o los argumentos requeridos | Switch#clock set % Incomplete command. | Vuelva a ingresar el comando seguido de un signo de interrogación (?) con un espacio después de la última palabra. Aparecen las palabras clave o los argumentos requeridos. |
| % Invalid input detected at '^' marker | el comando se introdujo incorrectamente. El error se produjo donde aparece la marca de acento (^). | Switch# clock set 19:50:00 25 ^ % Invalid input detected at '^' marker. | Vuelva a ingresar el comando seguido de un signo de interrogación (?) en un lugar señalado por la marca '^'. También puede ser necesario borrar las últimas palabras clave o argumentos. |

Teclas de acceso rápido y métodos abreviados

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

La figura muestra la mayoría de los métodos abreviados. La siguiente información merece una nota especial:

- Tab: Completa la parte restante del comando o palabra clave
- Ctrl-R: Vuelve a mostrar una línea
- Ctrl-Z: Sale del modo de configuración y vuelve al EXEC
- Flecha abajo: Permite al usuario desplazarse hacia adelante a través los comandos anteriores
- Flecha arriba: Permite al usuario desplazarse hacia atrás a través de los comandos anteriores
- Ctrl-Shift-6: Permite al usuario interrumpir un proceso IOS, como ping o traceroute
- Ctrl-C: Cancela el comando actual y sale del modo de configuración

Análisis con mayor profundidad:

Tab – Tab complete se utiliza para completar la parte restante de los comandos y parámetros abreviados, si la abreviatura contiene suficientes letras para diferenciarse de cualquier otro comando o parámetro actualmente disponible. Cuando se ha ingresado parte suficiente del comando o palabra clave como para que sean únicos, presione la tecla Tab y la CLI mostrará el resto del comando o palabra clave.

Ésta 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: Volver a mostrar línea actualizará la línea recientemente ingresada. 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 440ersión440o n Interface FastEthernet0/10, changed state to down
```

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

Switch#show mac

Ctrl-Z: Salir del modo de configuración. Para salir de un modo de configuración y regresar al modo EXEC privilegiado, use Ctrl-Z. Dado que el IOS tiene una estructura jerárquica de modos, el usuario puede encontrarse varios niveles hacia abajo. En lugar de salir de cada modo en forma individual, use Ctrl-Z para volver directamente a la petición de entrada de EXEC privilegiado en el nivel superior.

Flechas arriba y abajo: uso de comandos anteriores. 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 reingresar comandos sin tener que volver a escribir.

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

Ctrl-Shift-6: uso de la secuencia de escape. 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-Shift-6.

Ctrl-C: interrumpe la entrada de un comando y sale del modo de configuración. Resulta útil cuando se ingresa un comando que luego se decide cancelar y se sale del modo de configuración.

Comandos o palabras clave abreviados. Los comandos y las palabras clave pueden abreviarse a la cantidad mínima de caracteres que identifica a una selección única. Por ejemplo, el comando configure 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 puede abreviarse de esta forma:

Router#show interfaces

Router#show int

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

Router#sh int

11.1.6 Comandos de “análisis” de IOS

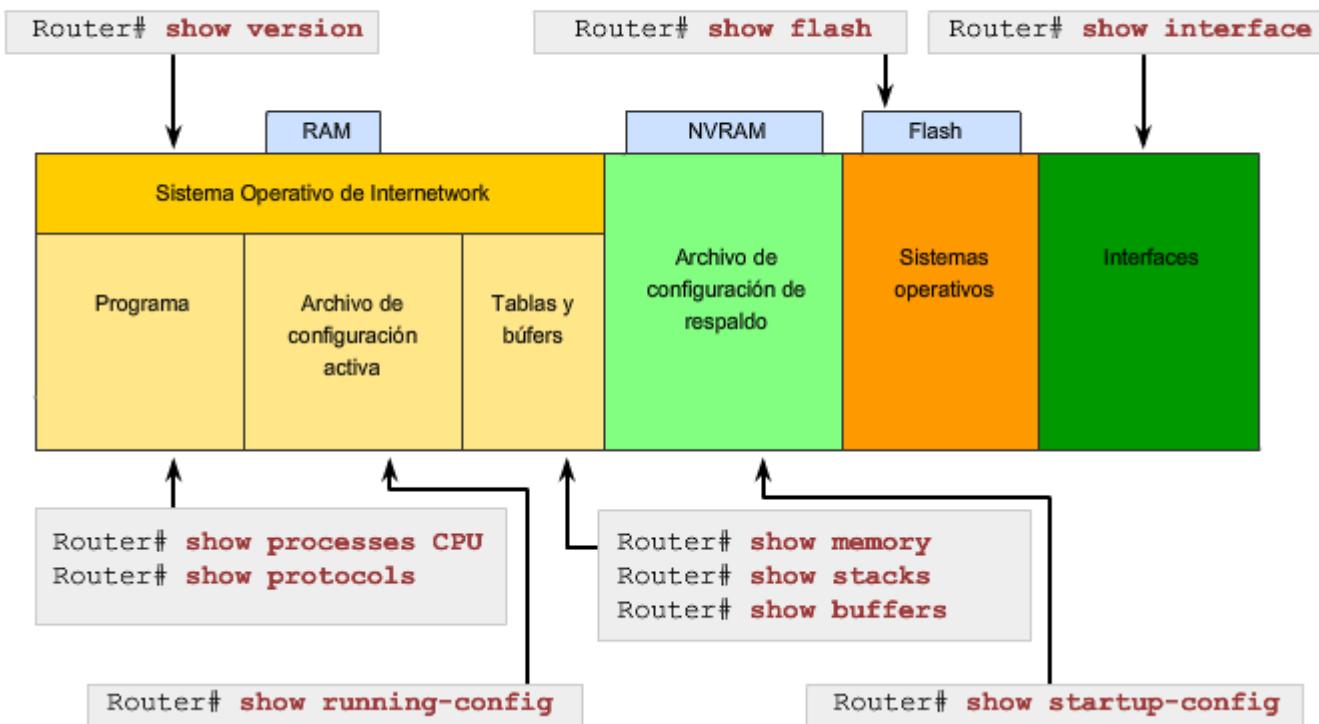
Para verificar y resolver problemas en la operación de la red, debemos examinar la operación de los dispositivos. El comando básico de examen es el comando show.

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. Use el comando show ? para obtener una lista de los comandos disponibles en un modo o contexto determinado.

La figura muestra cómo el típico comando show puede proveer información sobre la configuración, la operación y el estado de partes de un router Cisco.

En este curso, se utilizan algunos de los comandos show más básicos.

Los comandos IOS show pueden proporcionar información acerca de la configuración, operación y estado de las partes de un router de Cisco.



Algunos de los comandos usados con más frecuencia son:

show interfaces

Muestra estadísticas de todas las interfaces del dispositivo. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido del número de puerto/ranura de la interfaz específica. Por ejemplo:

Router#show interfaces serial 0/1

show 441ersión

Muestra información sobre la versión de software actualmente cargada, además de información de hardware y del dispositivo. Algunos de los datos que se obtienen a partir de este comando son:

- 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 funcionamiento del sistema: tiempo transcurrido desde la última vez que se reinició
- Información de reinicio del sistema: Método de reinicio (por ejemplo: apagar y encender, colapso)
- Nombre de la imagen del software: Nombre del archivo IOS almacenado en la flash
- Tipo de router y tipo de procesador: Número de modelo y tipo de procesador
- Tipo de memoria y asignación (Compartida/Principal): RAM del procesador principal y búfering de E/S de paquetes compartidos
- Características del software: Protocolos admitidos / conjuntos de características
- Interfaces de hardware: Interfaces disponibles en el router
- Registro de configuración: Establece especificaciones de arranque inicial, la configuración de velocidad de la consola y parámetros relacionados.

La figura muestra un ejemplo del típico resultado de show versión .

- show arp: Muestra la tabla ARP del dispositivo.
- show mac-address-table: (sólo switch) Muestra la tabla MAC de un switch.
- show startup-config: Muestra la configuración guardada que se ubica en la NVRAM.
- show running-config: Muestra el contenido del archivo de configuración actualmente en ejecución o la configuración para una interfaz específica o información de clase de mapa.
- show ip interfaces: Muestra las estadísticas Ipv4 para todas las interfaces de un router. Para ver las estadísticas de una interfaz específica, ejecute el comando show ip interfaces seguido del número de puerto/ranura de la interfaz específica. Otro formato importante de este comando es show ip interface brief. Es útil para obtener un resumen rápido de las interfaces y su estado operativo.

Por ejemplo:

Router#show ip interface brief

Interfaz Dirección IP ¿OK? Método Estado Protocolo

FastEthernet0/0 172.16.255.254 Sí manual activo activo

FastEthernet0/1 no asignada Sí no establecido inactivo inactivo

Serial0/0/0 10.10.10.5 Sí manual activo activo

Serial0/0/1 no asignada Sí no establecido inactivo inactivo

La petición de entrada Más

Cuando un comando devuelve más resultados de los que pueden mostrarse en una única pantalla, aparece la petición de entrada –Más–en la parte inferior de la pantalla. Cuando aparece la petición de entrada –More--, presione la barra espaciadora para visualizar el tramo siguiente 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.

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), version 12.4(11)T, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 18-Nov-06 15:20 by prod_rel_team

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

Router uptime is 10 weeks, 4 days, 23 hours, 36 minutes
System returned to ROM by power-on
System restarted at 16:43:31 UTC Fri Jan 26 2007
System image file is "flash:c1841-ipbasek9-mz.124-11.T.bin"

Cisco 1841 (revision 5.0) with 115712K/15360K bytes of memory.
Processor board ID FTX0932W21Y
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102

Router#
```

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE2,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh
Image text-base: 0x00003000, data-base: 0x00AA2F34

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE2/c2960-lanbase-
mz.122-25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K
bytes of memory.
Processor board ID FOC1107Z9ZN
Last reset from power-on
1 virtual Ethernet interface
```

11.1.7 Modos de configuración IOS

Modo de configuración global

El modo de configuración principal recibe el nombre de configuración global o global config. Desde configuración global, se realizan cambios en la configuración de la CLI que afectan la operación del dispositivo en su totalidad.

El modo configuración global también se usa como precursor para acceder a modos de configuración específicos.

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:

```
Router#configure terminal
```

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

```
Router(config)#
```

Modos de configuración específicos

Desde el modo de configuración global, pueden ingresarse muchos modos de configuración diferentes. 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, etc.)
- Modo de línea: para configurar una de las líneas (física o virtual) (consola, ,auxiliar, VTY, etc.).
- Modo de router: para configurar los parámetros de uno de los protocolos de enrutamiento

La figura muestra las peticiones de entrada para algunos modos. Recuerde que cuando se hacen cambios de configuración en una interfaz o proceso, los cambios sólo afectan a esa interfaz o proceso.

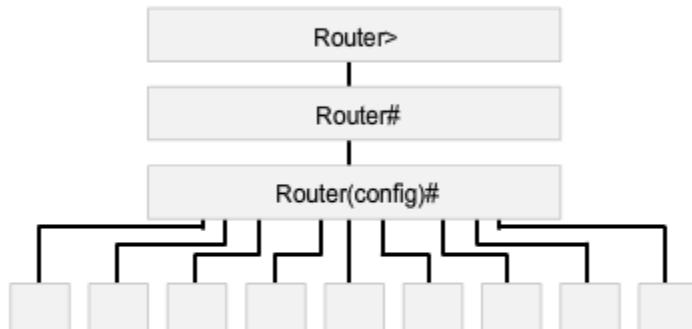
Para salir de un modo de configuración específico y volver al modo de configuración global, ingrese exit ante la petición de entrada. Para salir completamente del modo de configuración y volver al modo EXEC privilegiado, ingrese end o use la secuencia de teclas Ctrl-Z.

Cuando se ha realizado un cambio desde el modo global, conviene guardararlo en el archivo de configuración de inicio almacenado en la NVRAM. Así se evita que los cambios se pierdan por cortes de energía o un reinicio intencional. El comando para guardar la configuración en ejecución en el archivo de configuración de inicio es:

```
Router#copy running-config startup-config
```

Modos de configuración del IOS

Modo EXEC usuario
Modo EXEC privilegiado
Modo de configuración global
Modo de configuración específico



| Modo de configuración | Indicador |
|-----------------------|------------------------|
| Interfaz | Router(config-if)# |
| Línea | Router(config-line)# |
| Routers | Router(config-router)# |

11.2 APLICACIÓN DE UNA CONFIGURACION BASICA CON CISCO IOS

11.2.1 Los dispositivos necesitan nombres

El nombre de host se usa en las peticiones de entrada de la CLI. Si el nombre de host no está explícitamente configurado, el router usa el nombre de host predeterminado, asignado de fábrica, "Router". El switch tiene el nombre de host predeterminado, asignado de fábrica, "Switch". Imagine que una internetwork tiene varios routers y todos recibieron el nombre predeterminado "Router". Se crearía una importante confusión durante la configuración y el mantenimiento de la red.

Cuando se accede a un dispositivo remoto con Telnet o SSH, es importante tener la confirmación de que se ha hecho una conexión al dispositivo adecuado. Si todos los dispositivos quedaran con sus nombres predeterminados, no se podría identificar que el dispositivo correcto esté conectado.

Al elegir y documentar nombres atinadamente, resulta más fácil recordar, analizar e identificar 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. **Siempre conviene crear la convención de denominación al mismo tiempo que el esquema de direccionamiento para permitir la continuidad dentro de la organización.**

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

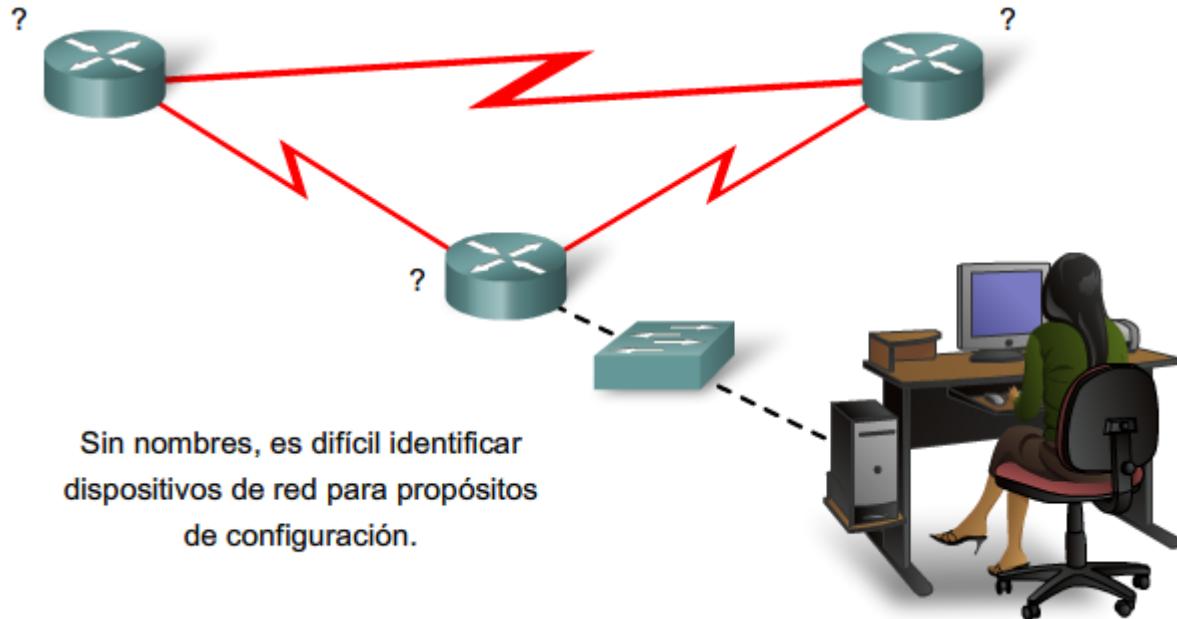
- Comenzar con una letra.
- No debe incluirse ningún espacio.
- Finalizar con una letra o dígito.
- Sólo deben incluirse caracteres que sean letras, dígitos y guiones.
- Tener 63 caracteres o menos.

Los nombres de hosts utilizados en el dispositivo IOS conservan su uso de mayúsculas y minúsculas. 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. RFC 1178 provee algunas de las reglas que pueden usarse como referencia para la denominación de dispositivos.

Como parte de la configuración del dispositivo, debe configurarse un nombre de host único para cada dispositivo.

Nota: Sólo los administradores usan los nombres de host de los dispositivos cuando usan la CLI para configurar y monitorear los dispositivos. A menos que estén configurados de esa manera, los dispositivos no usan estos nombres cuando se detectan entre sí e interoperan.

Configuración básica con Cisco IOS



Aplicación de nombres: ejemplo

Veamos un ejemplo de tres routers conectados en una red que abarca tres ciudades diferentes (Atlanta, Phoenix y Corpus) como se muestra en la figura.

Para crear una convención de denominación para los routers, se debe tener en cuenta la ubicación y el propósito de los dispositivos. Pregúntese lo siguiente: ¿Serán estos routers parte de la sede de una organización? ¿Tiene cada router un propósito diferente? Por ejemplo, ¿es el router de Atlanta un punto de unión principal en la red o es una unión en una cadena?

En este ejemplo, cada router se identificará como una sucursal de la sede para cada ciudad. Los nombres podrían ser AtlantaHQ, PhoenixHQ y CorpusHQ. Si cada router hubiera sido una unión en una cadena sucesiva, los nombres podrían haber sido AtlantaJunction1, PhoenixJunction2 y CorpusJunction3.

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 ha identificado la convención de denominación, el próximo paso es aplicar los nombres al router usando la CLI. Este ejemplo nos conducirá a través del proceso de denominación del router de Atlanta.

Configuración del nombre de host de IOS

Desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando `configure terminal` (configurar terminal):

```
Router#configure terminal
```

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

```
Router(config)#
```

En el modo global, ingrese el nombre de host:

```
Router(config)#hostname AtlantaHQ
```

Después de ejecutar ese comando, la petición de entrada cambiará a:

```
AtlantaHQ(config)#
```

Observe que el nombre de host aparece en la petición de entrada. Para salir del modo global, use 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 anular los efectos de un comando, establezca el prefacio del comando con la palabra clave no.

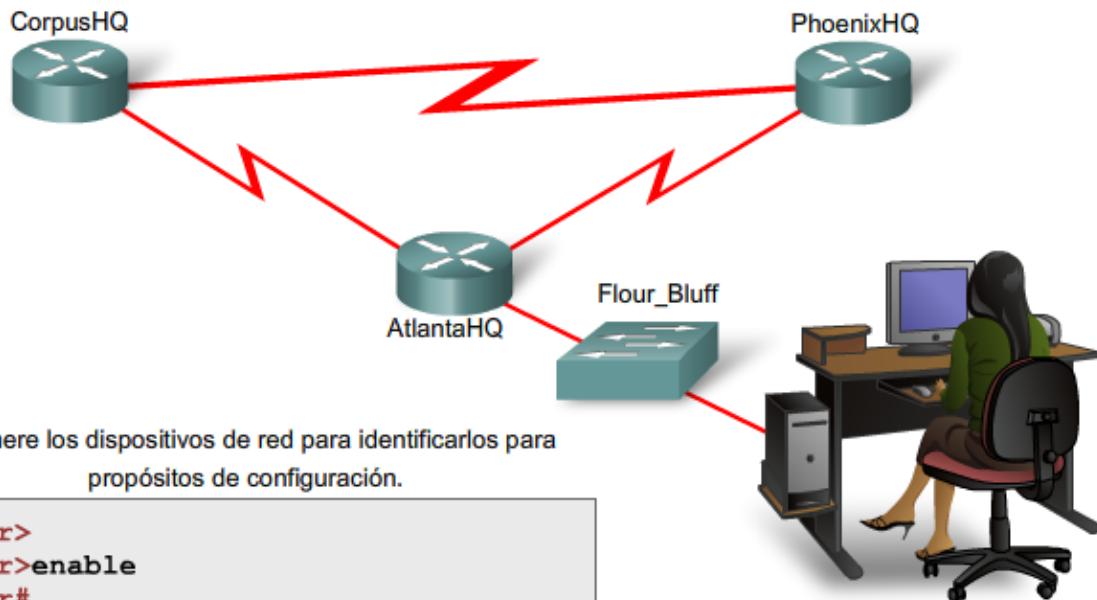
Por ejemplo: para eliminar el nombre de un dispositivo, utilice:

```
AtlantaHQ(config)# no hostname
```

```
Router(config)#
```

Nótese que el comando no hostname provoca que el router vuelva a usar el nombre de host por defecto, "Router."

Configuración de nombres de dispositivos



11.2.2 Limitar acceso a dispositivo: Configuración de contraseñas y uso de mensajes

La limitación física del acceso a los dispositivos de red con armarios o bastidores con llave resulta una buena práctica; sin embargo, las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red. Cada dispositivo debe tener contraseñas configuradas a nivel local para limitar el acceso. En un curso futuro, analizaremos cómo reforzar la seguridad al exigir una ID 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 son:

- Contraseña de consola: limita el acceso de los dispositivos mediante la conexión de consola
- Contraseña de enable: limita el acceso al modo EXEC privilegiado
- Contraseña enable secret: encriptada, limita el acceso del modo EXEC privilegiado
- Contraseña de VTY: limita el acceso de los dispositivos que utilizan 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.
- Use en las contraseñas una combinación de secuencias de letras mayúsculas y minúsculas o numéricas.
- 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, usaremos contraseñas simples como cisco o clase. Estas contraseñas se consideran simples y fáciles de adivinar, y deben evitarse en un entorno de producción. Sólo usamos estas contraseñas por comodidad en el entorno instructivo.

Como se muestra en la figura, cuando se le solicita una contraseña, el dispositivo no repetirá la contraseña mientras se ingresa. En otras palabras, los caracteres de la contraseña no aparecerán cuando el usuario los ingrese. Esto se hace por cuestiones de seguridad; muchas contraseñas se obtienen por ojos espías.

Contraseña de consola

El puerto de consola de un dispositivo Cisco IOS tiene privilegios especiales. 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 password
```

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

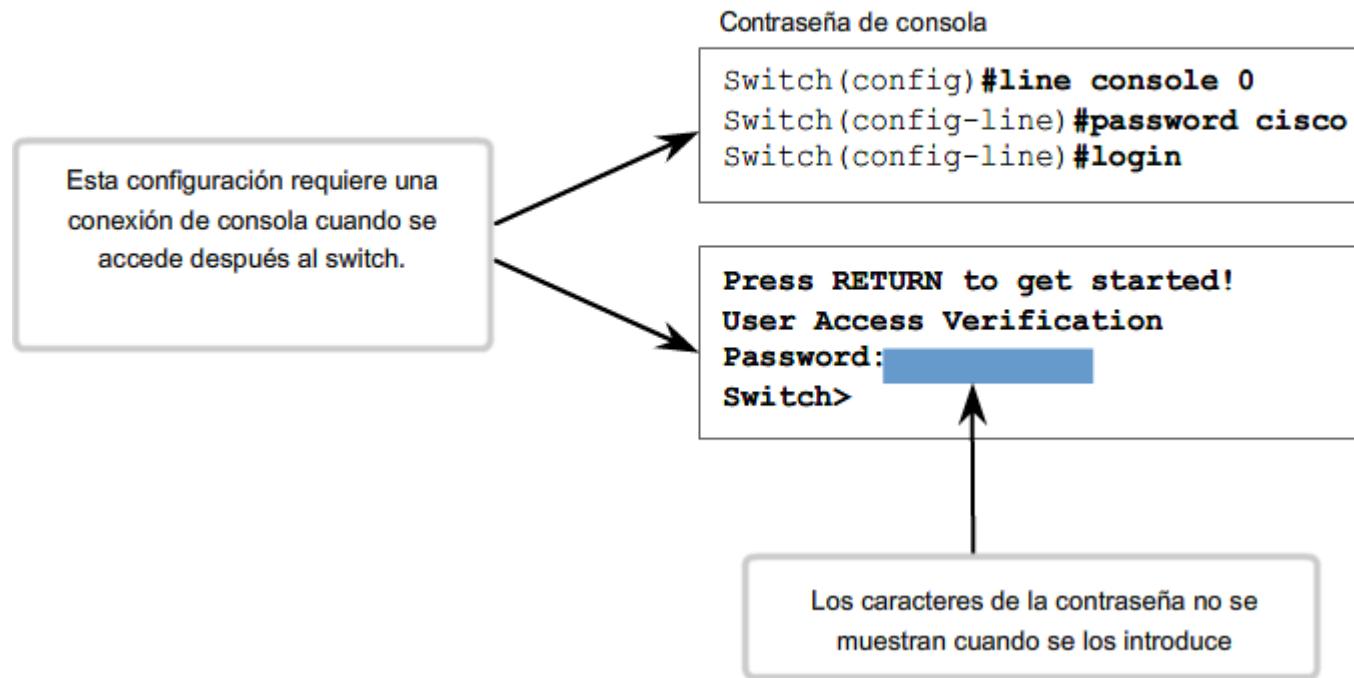
Desde el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea para la consola. El cero se utiliza para representar la primera (y, en la mayoría de los casos, la única) interfaz de consola para un router.

El segundo comando, password password especifica una contraseña en una línea.

El comando login configura al router para que pida la autenticación al iniciar sesión. Cuando el login está habilitado y se ha configurado una contraseña, habrá una petición de entrada de contraseña.

Una vez que se han ejecutado estos tres comandos, aparecerá una petición de entrada de contraseña cada vez que un usuario intente obtener acceso al puerto de consola.

Limitación de acceso a dispositivo - Configuración de contraseñas de consola



Contraseña de enable y Contraseña enable secret

Para proporcionar una mayor seguridad, utilice el comando enable password o el comando enable secret. Puede usarse cualquiera de estos comandos para establecer la autenticación antes de acceder al modo EXEC privilegiado (enable).

Si es posible, use siempre el comando enable secret, no el comando anterior enable password. El comando enable secret provee mayor seguridad porque la contraseña está encriptada. El comando enable password puede usarse sólo si enable secret no se ha configurado aún.

El comando enable password se ejecutaría si el dispositivo usa una versión anterior del software IOS de Cisco que no reconoce el comando enable secret.

Los siguientes comandos se utilizan para configurar las contraseñas:

```
Router(config)#enable password contraseña
```

```
Router(config)#enable secret contraseña
```

Nota: Si no se configura una contraseña enable password o enable secret, IOS impide el acceso EXEC privilegiado desde una sesión Telnet.

Si no se ha establecido una contraseña de enable, podría aparecer una sesión Telnet de esta forma:

```
Switch>enable
```

```
% No se ha establecido contraseña
```

```
Switch>
```

Contraseña de VTY

Las líneas vty permiten el acceso a un router a través de Telnet. En forma predeterminada, muchos dispositivos Cisco admiten cinco líneas VTY con numeración del 0 al 4. Es necesario configurar 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 proveer un recurso secundario para el ingreso administrativo al dispositivo si las demás conexiones están en uso.

Los siguientes comandos se usan para configurar una contraseña en líneas vty:

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password contraseña
```

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

Por defecto, el IOS incluye el comando login en las líneas VTY. Esto impide el acceso Telnet al dispositivo sin la previa solicitud de autenticación. Si por error, se configura el comando no login, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de Telnet. Esto representaría un gran riesgo de seguridad.

Visualización de contraseñas de encriptación

Existe otro comando de utilidad que impide que las contraseñas aparezcan como texto sin cifrar cuando se visualizan los archivos de configuración. Ese comando es el service password-encryption.

Este comando provee la encriptación de la contraseña cuando ésta se configura. El comando service password-encryption aplica una encriptación débil a todas las contraseñas no encriptadas. Esta encriptación no se aplica a las contraseñas cuando se envían a través de medios únicamente en la configuración. 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-config antes de ejecutar el comando service password-encryption, las contraseñas no encriptadas estarán 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.

Limitación de acceso a dispositivo

Configuración Telnet y encriptación de contraseña

Contraseña de terminales virtuales

```
Router(config)#line vty 0 4  
Router(config-line)#password cisco  
Router(config-line)#login
```

Habilitar contraseña

```
Router(config)#enable password san fran
```

Habilitar contraseña secreta

```
Router(config)#enable secret cisco
```

Contraseña altamente encriptada



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 aplicarán medidas legales en caso de uso no autorizado."

Ya que cualquier persona que intenta iniciar sesión puede ver los títulos, 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 usa un aviso, nunca debe invitar a un usuario al router. 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 los usuarios de la red.

El IOS provee 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 global.

Como se muestra en la figura, el comando banner motd requiere el uso de delimitadores para identificar el contenido del mensaje del 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, con frecuencia se usan símbolos tales como "#".

Para configurar un MOTD, ingrese el comando banner motd desde el modo de configuración global:

```
Switch(config)#banner motd # message #
```

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.



11.2.3 Administración de archivos de configuración

Como se analizó anteriormente, la modificación de la configuración en ejecución afecta la operación del dispositivo en forma inmediata.

Después de hacer cambios en una configuración, considere estas opciones como siguiente paso:

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

Establecer la configuración modificada como la nueva configuración de inicio

Recuerde: ya que la configuración en ejecución se almacena en la RAM, se encuentra temporalmente activa mientras se ejecuta (se encuentra encendido) el dispositivo Cisco. Si se corta la energía al router o si se reinicia el router, se perderán todos los cambios de configuración a menos que se hayan guardado.

Al guardar la configuración en ejecución en el archivo de configuración de inicio en la NVRAM se mantienen los cambios como la nueva configuración de inicio.

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

Cuando se verifica si los cambios son correctos, utilice el comando copy running-config startup-config en la petición de entrada del modo EXEC privilegiado. El siguiente ejemplo muestra el comando:

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

Una vez ejecutado, el archivo de configuración en ejecución reemplaza al archivo de configuración de inicio.

Volver a la configuración original del dispositivo

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 la tecla Intro. Si se presiona cualquier otra tecla, se cancelará el procedimiento.

Por ejemplo:

```
Router#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)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 2004 by cisco Systems, Inc.

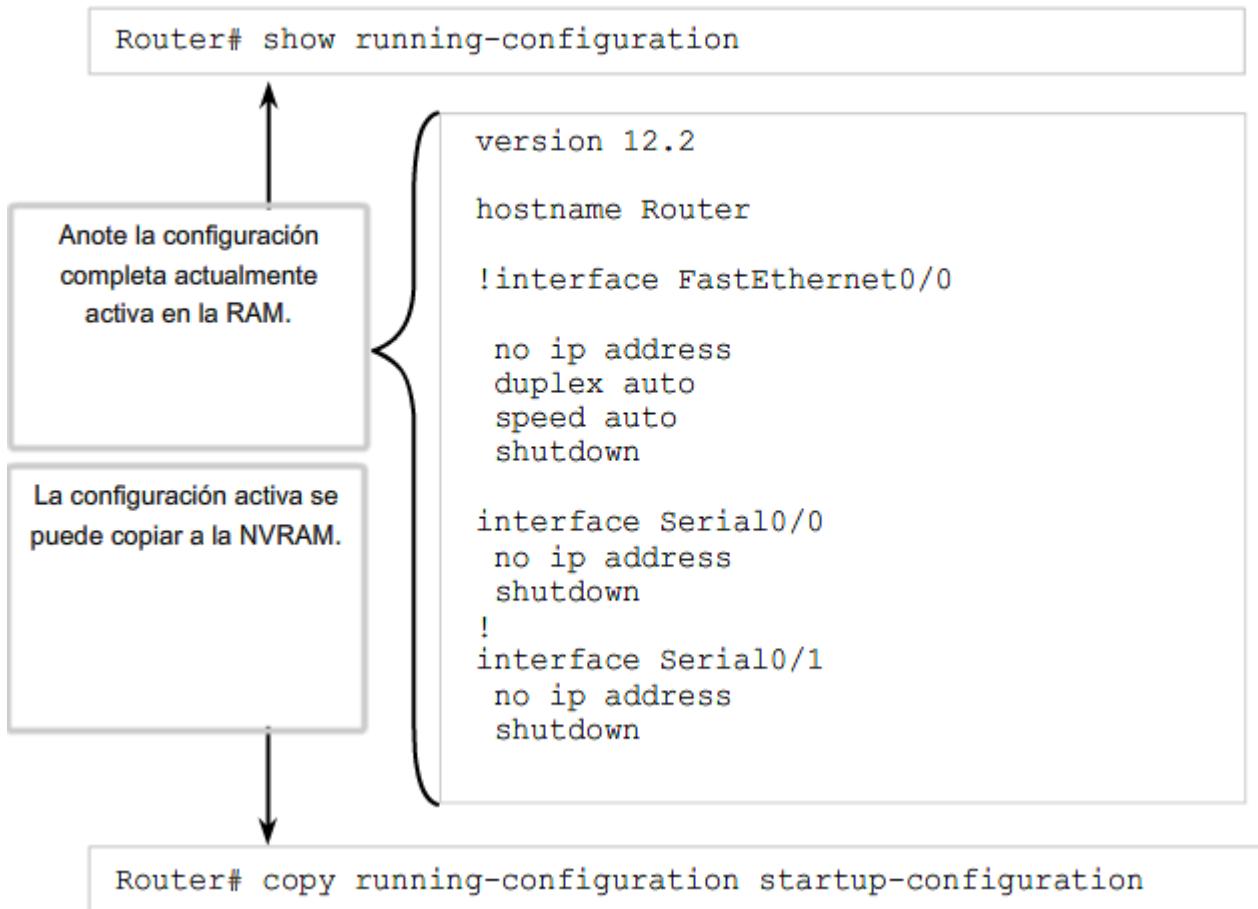
Versión PLD 0x10

Versión GIO ASIC 0x127

Procesador c1841 con 131072 KB de memoria principal

La memoria principal se encuentra configurada en modo 64 bits con la paridad deshabilitada

Verificación de archivos de configuración



Copia de respaldo de las configuraciones sin conexión

Los archivos de configuración deben guardarse como archivos de respaldo ante cualquier problema que surja. Los archivos de configuración se pueden almacenar en un servidor Trivial File Transfer Protocol (TFTP), un CD, una barra de memoria USB o un disquete almacenado en un lugar seguro. Un archivo de configuración también tendría que incluirse en la documentación de red.

Configuración de respaldo en el servidor TFTP

Como se muestra en la figura, una opción es guardar la configuración en ejecución o la configuración de inicio en un servidor TFTP. Use los comandos copy running-config tftp o copy startup-config tftp y siga estos pasos:

1. Ingrese el comando copy running-config tftp.
2. Ingrese la dirección IP del host donde se guardará el archivo de configuración.
3. Ingrese el nombre que se asignará al archivo de configuración.
4. Responda yes para confirmar cada opción.

Estudie la figura para observar este proceso.

Eliminación de todas las configuraciones

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 con el uso del 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:

```
Router#erase startup-config
```

Una vez que se ejecuta el comando, el router solicitará la 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 Intro. Si se presiona cualquier otra tecla, se cancelará el proceso.

Advertencia: Use el comando erase con cautela. Este comando puede utilizarse para borrar cualquier archivo del dispositivo. El uso incorrecto del comando puede borrar el IOS mismo u otro archivo esencial.

Después de eliminar la configuración de inicio de la NVRAM, recargue el dispositivo para eliminar el archivo de configuración actual en ejecución de la memoria RAM. El dispositivo cargará entonces la configuración de inicio predeterminada que se envió originalmente con el dispositivo en la configuración en ejecución.

```
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] y
Writing tokyo.2 !!!!!!! [OK]
```

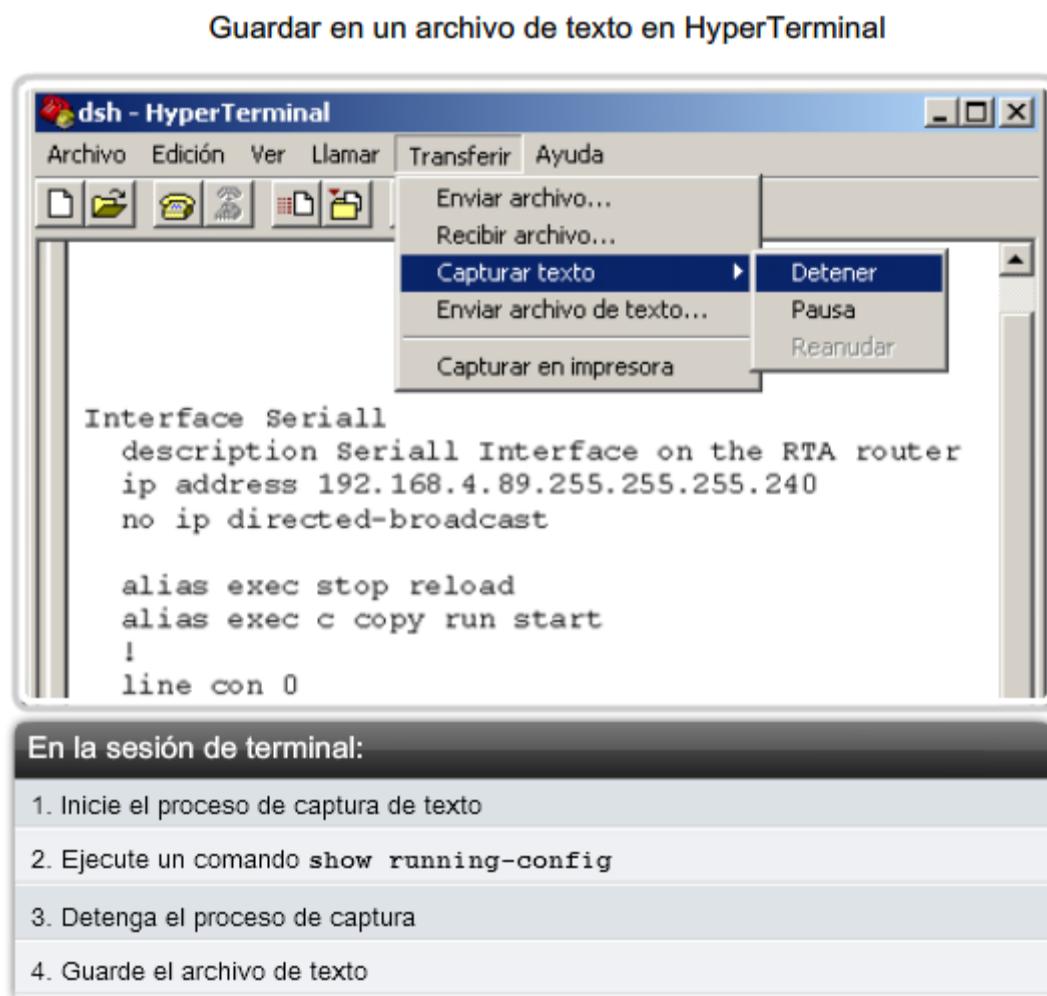
Copia de seguridad de las configuraciones con captura de texto (HyperTerminal)

Se pueden guardar/archivar los archivos de configuración en un documento de texto. Esta secuencia de pasos asegura la disponibilidad de una copia de trabajo de los archivos de configuración para su modificación o reutilización en otra oportunidad.

Cuando se use HyperTerminal, siga estos pasos:

1. En el menú Transfer, haga clic en Capture Text.
2. Elija la ubicación.
3. Haga clic en Start para comenzar la captura del texto. Una vez que la captura ha comenzado, ejecute el comando show running-config o show startup-config ante la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
5. Visualice el resultado para verificar que no esté dañado.

Observe un ejemplo en la figura.



Configuraciones de respaldo con captura de texto (TeraTerm)

Los archivos de configuración pueden guardarse o archivarse en un documento de texto a través de TeraTerm.

Como se muestra en la figura, los pasos son:

1. En el menú File, haga clic en Log.
2. Elija la ubicación. TeraTerm comenzará a capturar texto. Una vez que la captura ha comenzado, ejecute el comando show running-config o show startup-config ante la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
4. Cuando la captura haya finalizado, seleccione Close en TeraTerm: Ventana de registro.

5. Visualice el resultado para verificar que no se ha dañado.

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. 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 copia.

Cuando se usa HyperTerminal, los pasos son:

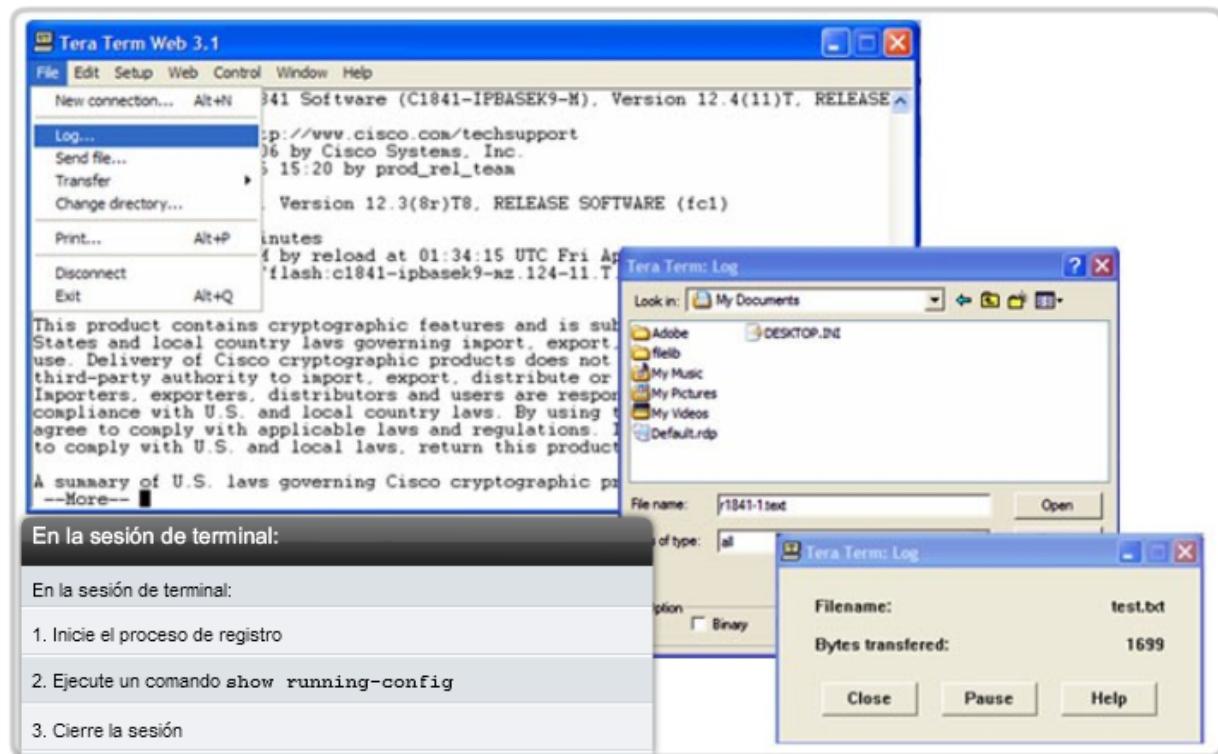
1. Ubicar el archivo que se debe copiar en el dispositivo y abrir el documento de texto.
2. Copiar el texto completo.
3. En el menú Edit, haga clic en paste to host.

Cuando se usa TeraTerm, los pasos son:

1. En el menú File, haga clic en Send archivo.
2. Ubique el archivo que debe copiar en el dispositivo y haga clic en Open.
3. TeraTerm 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.

Guardar en un archivo de texto en TeraTerm



11.2.4 Configuración de interfaces

A lo largo de este capítulo, hemos analizado los comandos que son comunes a muchos de los dispositivos IOS. Algunas configuraciones son específicas de un tipo de dispositivo. Una configuración de esta clase es la configuración de interfaces en un router.

La mayoría de los dispositivos de red intermediarios tienen una dirección IP para la administración del dispositivo. Algunos dispositivos, como los switches y los puntos de acceso inalámbricos, pueden operar sin tener una dirección IP.

Dado que el objetivo de un router es interconectar diferentes redes, cada interfaz en un router tiene su propia dirección IPv4 exclusiva. La dirección asignada a cada interfaz existe en una red separada dedicada a la interconexión de routers.

Hay muchos parámetros que pueden configurarse en las interfaces del router. Analizaremos los comandos de interfaz más básicos, que se resumen en la figura.

Configuración de las interfaces del router

Se accede a todas las interfaces ejecutando el comando `interface` en la petición de configuración global.

En los siguientes comandos, el argumento `type` incluye serial, ethernet, fastethernet y otros:

```
Router(config)#interface type port  
Router(config)#interface type slot/port  
Router(config)#interface type slot/subslot/port
```

El siguiente comando se utiliza para desactivar la interfaz de forma administrativa:

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

El siguiente comando se utiliza para activar una interfaz que se desactivó:

```
Router(config-if)#no shutdown
```

El siguiente comando se utiliza para salir del modo de configuración de interfaz actual:

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

Cuando la configuración está completa, la interfaz queda habilitada y se sale del modo de configuración de interfaz.

Configuración de Interfaz Ethernet del router

La Interfaz Ethernet del router se utiliza como gateway para los dispositivos finales en las LAN conectadas directamente al router.

Cada Interfaz Ethernet debe contar con una dirección IP y máscara de subred para enrutar los paquetes IP.

Para configurar una interfaz Ethernet, siga estos pasos:

1. Ingrese al modo de configuración global.
2. Ingrese al modo de configuración de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Active la interfaz.

Como se muestra en la figura, configure la dirección IP de Ethernet mediante los siguientes comandos:

```
Router(config)#interface FastEthernet 0/0
```

```
Router(config-if)#ip address ip_address netmask
```

```
Router(config-if)#no shutdown
```

Habilitación de la interfaz

Por defecto, las interfaces se encuentran deshabilitadas. Para habilitar una interfaz, ingrese el comando no shutdown en el modo de configuración de interfaz. Si es necesario desactivar una interfaz por cuestiones de mantenimiento o para resolver problemas, use el comando shutdown.

Configuración de interfaces seriales del router

Las interfaces seriales se usan para conectar WAN a routers en un sitio remoto o ISP.

Para configurar una interfaz serial siga estos pasos:

1. Ingrese al modo de configuración global.
2. Ingrese al modo de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Si el cable de conexión es DCE, fije la frecuencia de reloj. Omita este paso si el cable es DTE.
5. Active la interfaz.

Cada interfaz serial conectada debe tener una dirección IP y una máscara de subred para enrutar paquetes IP.

Configure la dirección IP con los siguientes comandos:

```
Router(config)#interface Serial 0/0/0
```

```
Router(config-if)#ip address ip_address netmask
```

Las interfaces seriales requieren una señal de reloj para controlar la temporización de las comunicaciones. En la mayoría de los entornos, un dispositivo DCE como por ejemplo un CSU/DSU, proporciona dicha señal. En forma predeterminada, los routers Cisco son dispositivos DTE, pero pueden configurarse como dispositivos DCE.

En los enlaces seriales interconectados directamente, como en nuestro entorno de laboratorio, un extremo debe operar como DCE para proporcionar la señal del reloj. Se activa el reloj y la velocidad se especifica con el comando clock rate. Algunas frecuencias de bit pueden no estar disponibles en ciertas interfaces seriales. Esto depende de la capacidad de cada interfaz.

En la práctica de laboratorio, si debe establecerse una frecuencia de reloj en una interfaz identificada como DCE, se debe usar la frecuencia de reloj 56000.

Como se muestra en la figura, los comandos que se utilizan para establecer una frecuencia de reloj y habilitar una interfaz serial son:

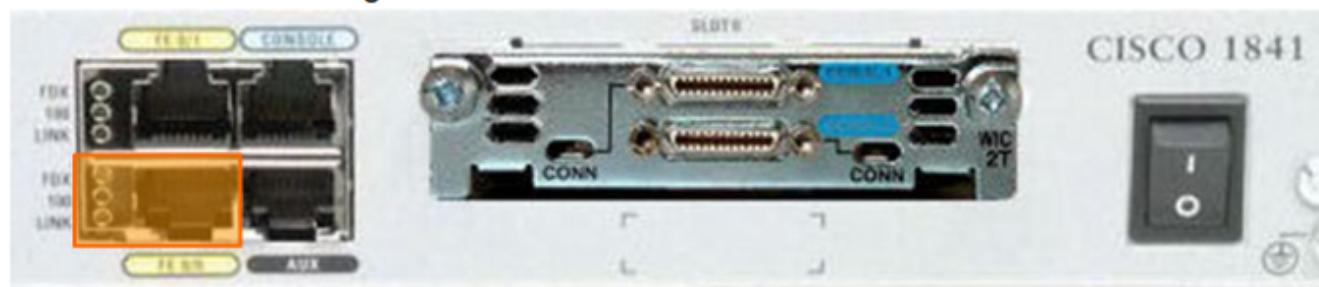
```
Router(config)#interface Serial 0/0/0
```

```
Router(config-if)#clock rate 56000
```

```
Router(config-if)#no shutdown
```

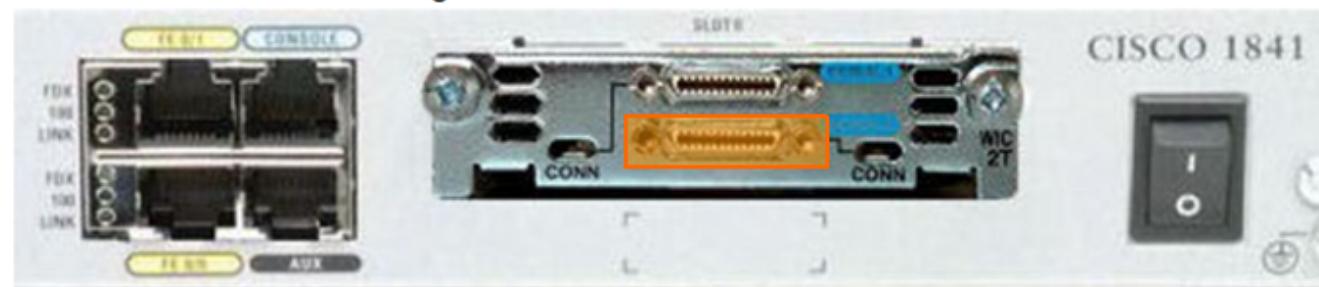
Una vez que se aplicaron los cambios de configuración en el router, recuerde utilizar los comandos show para verificar la precisión de los cambios y luego guardar la configuración modificada como configuración de inicio.

Configuración de las interfaces Ethernet del router



```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config) #
```

Configure las interfaces seriales del router



```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config) #
```

Así como el nombre del host ayuda a identificar el dispositivo en una red, una descripción de interfaz indica el propósito de la interfaz. Una descripción de lo que una interfaz hace o dónde está conectada debe ser parte de la configuración de cada interfaz. Esta descripción puede resultar útil para la resolución de problemas.

La descripción de interfaz aparecerá en el resultado de estos comandos: show startup-config, show running-config y show interfaces.

Por ejemplo, esta descripción provee información valiosa sobre el propósito de la interfaz:

Esta interfaz es el gateway para la LAN administrativa.

Una descripción puede ayudar a determinar los dispositivos o las ubicaciones conectadas a la interfaz. A continuación, se proporciona otro ejemplo:

La interfaz F0/0 está conectada al switch principal en el edificio administrativo.

Cuando el personal de soporte puede identificar con facilidad el propósito de una interfaz o de un dispositivo conectado, pueden comprender más fácilmente el alcance del problema, y esto puede conducir a la resolución del problema.

La información de contacto y de circuito también puede incorporarse en la descripción de la interfaz. La siguiente descripción de una interfaz serial proporciona la información que un administrador de red puede necesitar antes de decidir la prueba de un circuito WAN. Esta descripción indica dónde terminan los circuitos, el ID del circuito y el número de teléfono de la empresa que suministra el circuito:

FR a circuito GAD1 ID:AA.HCGN.556460 DLCI 511 - support# 555.1212

Para crear una descripción, utilice el comando descripción. Este ejemplo muestra los comandos utilizados para crear una descripción para una interfaz FastEthernet:

```
HQ-switch1#configurar terminal
```

```
HQ-switch1(config)#interfaz fa0/0
```

```
HQ-switch1(config-if)#descripción Conectarse al switch principal del Edificio A
```

Una vez que se aplica la descripción a la interfaz, utilice el comando show interfaces para verificar que la descripción sea correcta.

Vea la figura a modo de ejemplo.

Descripciones de interfaces de router



```
Router(config)#interface FastEthernet 0/0
Router(config-if)#description Building B Sales LAN
Router(config-if)#exit
```

La descripción es sólo texto después de este espacio

Descripción de la interfaz usada para documentación de red interna

```
Router(config)#interface Serial 0/0/0
Router(config-if)#description To Perth CKT-PT27834365-01
Router(config-if)#exit
```

La descripción es sólo texto después de este espacio

Configuración de una interfaz de switch

Un switch LAN es un dispositivo intermediario que interconecta segmentos dentro de una red. Por lo tanto, las interfaces físicas en el switch no tienen direcciones IP. A diferencia de un router en el que las interfaces están conectadas a diferentes redes, una interfaz física en un switch conecta dispositivos dentro de una red.

Las interfaces de switch también están habilitadas en forma predeterminada. Como se muestra en la figura del Switch 1, podemos asignar descripciones pero no es necesario activar la interfaz.

Para poder administrar un switch, asignamos direcciones al dispositivo hacia dicho switch. Con una dirección IP asignada al switch, actúa como dispositivo host. Una vez que se asigna la dirección, se accede al switch con telnet, ssh o servicios Web.

La dirección para un switch se asigna a una interfaz virtual representada como una interfaz LAN virtual (VLAN). En la mayoría de los casos, esta es la interfaz VLAN 1. En la figura del Switch 2, se asigna una dirección IP a la interfaz VLAN 1. Al igual que las interfaces físicas de un router, también se debe activar esta interfaz con el comando no shutdown.

Como cualquier otro host, el switch necesita una dirección de gateway definida para comunicarse fuera de la red local. Como se muestra en la figura del Switch 2, este gateway se asigna con el comando ip default-gateway.

Configuración del switch

```
Switch#configure terminal
Switch(config)#interface FastEthernet 0/0
Switch(config-if)#description To TAM switch
Switch(config-if)#exit
Switch(config)#hostname Flour_Bluff
Flour_Bluff(config)#exit
Flour_Bluff#
```

Configuración de la interfaz.

Switch 1

Switch 2

Configuración del switch

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#exit
Switch#
```

Observe que la petición de entrada cambia para indicar el modo IOS actual.

Switch 1

Switch 2

11.3 VERIFICACION DE LA CONECTIVIDAD

11.3.1 Prueba de stack

El comando ping

El comando ping es una manera efectiva de probar la conectividad. La prueba se denomina prueba de stack de protocolos, porque el comando ping se mueve desde la Capa 3 del Modelo OSI hasta la Capa 2 y luego hacia a la Capa 1. El ping utiliza el protocolo ICMP (Protocolo de mensajes de control de Internet) para comprobar la conectividad.

Utilización de ping en una secuencia de prueba

En esta sección se utilizará el comando ping del router IOS en una secuencia de pasos planificados para establecer conexiones válidas, comenzando por el dispositivo individual y luego extendiéndose a la LAN y, por último, a las redes remotas. Mediante el uso del comando ping en esta secuencia ordenada, los problemas pueden aislarse. El comando ping no siempre indicará con precisión la naturaleza del problema, pero puede ayudar a identificar el origen del problema, un primer paso importante en la resolución de una falla en la red.

El comando ping proporciona un método para comprobar la stack de protocolos y la configuración de la dirección IPv4 en un host. 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 de IOS cederá a una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:

! - indica la recepción de una respuesta de eco ICMP

. - indica un límite de tiempo cuando se espera una respuesta

U - se recibió un mensaje ICMP inalcanzable

El "!" (signo de exclamación) indica que el ping se completó correctamente y verifica la conectividad de la Capa 3.

El " ." (punto) puede indicar problemas en la comunicación. Puede señalar que ocurrió un problema de conectividad en algún sector de la ruta. También puede indicar que un router a lo largo de la ruta no tenía una ruta hacia el destino y no envió un mensaje ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo.

La "U" indica que un router del camino no tenía una ruta a la dirección de destino y respondió con un mensaje ICMP inalcanzable.

Prueba de loopback

A modo de primer paso en la secuencia de prueba, se utiliza el comando ping para verificar la configuración IP interna en el host local. Recuerde que esta prueba se cumple con el comando ping en una dirección reservada denominada loopback (127.0.0.1). Esto verifica la correcta operación del stack de protocolos desde la capa de Red a la capa Física, y viceversa, sin colocar realmente una señal en el medio.

Ping se ingresa en una línea de comandos.

Ingrese el comando de loopback ping con esta sintaxis:

```
C:\>ping 127.0.0.1
```

La respuesta de este comando se parecería a esta:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Mínimo = 0 ms, Máximo = 0 ms, Promedio = 0 ms

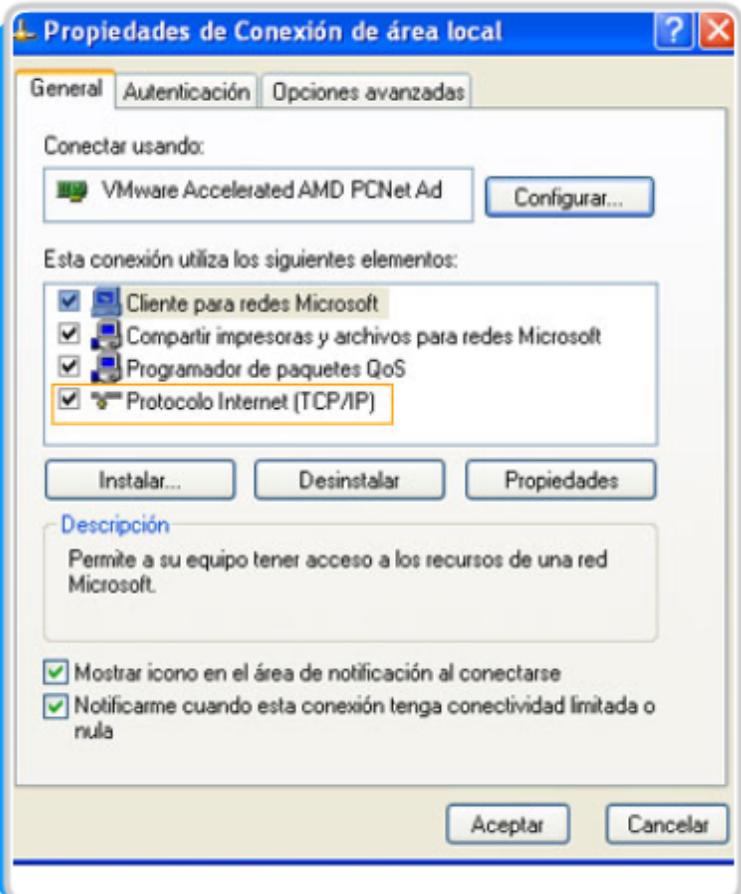
El resultado indica que se enviaron cuatro paquetes (cada uno con un tamaño de 32 bytes) y se devolvieron del host 127.0.0.1 en un tiempo menor a 1 milisegundo. TTL significa Tiempo de vida y define la cantidad de saltos que le quedan al paquete de ping antes de que se lo descarte.

Prueba del stack TCP/IP local

Hacer ping al host local confirma que los TCP/IP se instalaron y funcionan en el adaptador de red local.



Hacer ping a 127.0.0.1 hace que un dispositivo haga ping desde él mismo.



11.3.2 Prueba de la asignación de interface

Del mismo modo que se usan comandos y utilidades para verificar la configuración de un host, se deben aprender los comandos para verificar las interfaces de dispositivos intermediarios. El IOS provee comandos para verificar la operación de interfaces de router y switch.

Verificación de interfaces de router

Uno de los comandos más utilizados es el comando show ip interface brief. Este proporciona un resultado más abreviado que el comando show ip interface. Ofrece además un resumen de la información clave de todas las interfaces.

Si se observa la figura del Router 1, se puede ver que este resultado muestra todas las interfaces conectadas al router, la dirección IP, si la hay, asignada a cada interfaz y el estado operativo de la interfaz.

Si se observa la línea de la interfaz FastEthernet 0/0, se ve que la dirección IP es 192.168.254.254. Si se observan las dos últimas columnas, se advierte el estado de la interfaz de Capa 1 y Capa 2. up en la columna de estado muestra que esta interfaz está en funcionamiento en la Capa 1. up en la columna de protocolo señala que el protocolo de Capa 2 está funcionando.

En la misma figura, se observa que la interfaz serial 0/0/1 no ha sido habilitada. La indicación correspondiente es administratively down en la columna de estado. Esta interfaz puede activarse con el comando no shutdown.

Prueba de la conectividad del router

Como con un dispositivo final, es posible verificar la conectividad de Capa 3 con los comandos ping y traceroute. En la figura del Router 1 se puede ver un ejemplo de los resultados de un ping a un host en la LAN local y un trace a un host remoto a través de la WAN.

Verificación de las interfaces del switch

Al examinar la figura del Switch 1 se puede ver el uso del comando show ip interface para verificar la condición de las interfaces del switch. Como se aprendió anteriormente, la dirección IP para el switch se aplica a una interfaz VLAN (Red de área local virtual). En este caso, se asigna una dirección IP 192.168.254.250 a la interfaz Vlan1. También se puede observar que esta interfaz está activada y en funcionamiento.

Al examinar la interfaz FastEthernet0/1, se puede detectar que esta interfaz está desactivada. Esto quiere decir que no hay un dispositivo conectado a la interfaz o que la interfaz de red de los dispositivos conectada no está funcionando.

Por otro lado, los resultados de las interfaces FastEthernet0/2 y FastEthernet0/3 muestran que están en funcionamiento. Esto se indica en el Estado y en el Protocolo, cuando ambos se muestran activos.

Prueba de la conectividad del switch

Del mismo modo que otros hosts, el switch puede probar la conectividad de su Capa 3 con los comandos ping y traceroute . La figura del Switch1 también muestra un ping al host local y un trace a un host remoto.

No deben olvidarse dos cosas importantes: que no se requiere de una dirección IP para que un switch cumpla su tarea de reenvío de trama y que el switch requiere una gateway para comunicarse con el exterior de su red local.

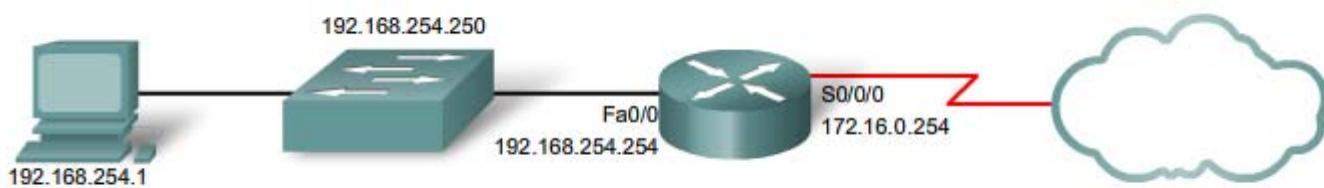
```

Router1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    192.168.254.254  YES  NVRAM   up               up
FastEthernet0/1/0  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

Router1#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

Router1#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

```



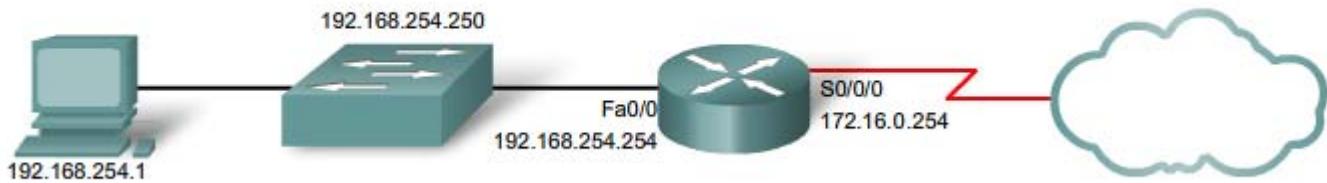
```

Switch1#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             down
FastEthernet0/2     unassigned      YES  unset   up               up
FastEthernet0/3     unassigned      YES  unset   up               up
<output omitted>

Switch1#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

Switch1#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

```



El siguiente paso en la secuencia de prueba es verificar que la dirección NIC esté unida a la dirección IPv4 y que la NIC esté lista para transmitir señales a través de los medios.

En este ejemplo, que también se muestra en la figura, asumimos que la dirección IPv4 asignada a una NIC es 10.0.0.5.

Para verificar la dirección IPv4, siga estos pasos:

En la línea de comandos, ingrese lo siguiente:

```
C:\>ping 10.0.0.5
```

A successful reply would resemble:

```
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
```

Ping statistics for 10.0.0.5:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

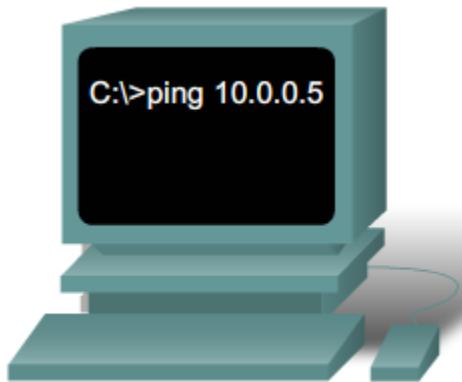
```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Esta prueba verifica que el controlador de la NIC y la mayoría del hardware de la NIC están funcionando correctamente. También verifica que la dirección IP está correctamente unida a la NIC, sin colocar verdaderamente una señal en los medios.

Si la prueba falla, es probable que existan problemas con el controlador de software y el hardware de la NIC que pueden requerir la reinstalación de uno de ellos, o de ambos. Este procedimiento depende del tipo de host y su sistema operativo.

Prueba de la asignación de NIC local

```
Dirección IP. . . . . : 10.0.0.5
Máscara de subred. . . . . :
255.255.255.0
Gateway por defecto. . . . . : 10.0.0.254
```



Verifique que la dirección NIC del host esté limitada y lista para transmitir las señales a través del medio haciendo ping en su propia dirección IP.

11.3.3 Prueba de la red local

La siguiente prueba de la secuencia corresponde a los hosts en la LAN local.

Al hacer ping a los hosts remotos satisfactoriamente se verifica que tanto el host local (en este caso, el router) como el host remoto estén configurados correctamente. Esta prueba se realiza al hacer ping a cada host en forma individual en la LAN.

Observe el ejemplo en la figura.

Si un host responde con el mensaje "Destination Unreachable" (destino inalcanzable), observe qué dirección no fue satisfactoria y continúe haciendo ping a los otros hosts de la LAN.

Otro mensaje de falla es "Request Timed Out" (la petición ha expirado). Indica que no hubo respuesta al intento del ping en el período de tiempo predeterminado, lo cual indica que el problema puede estar en la latencia de red.

Ping extendido

Para examinarlo, el IOS ofrece un modo "extendido" del comando ping. Este modo se ingresa escribiendo ping en modo EXEC privilegiado, en la petición de entrada de la CLI sin una dirección IP de destino. Luego se presenta una serie de peticiones de entrada como se muestra en este ejemplo. Al presionar Intro se aceptan los valores predeterminados indicados.

```
Router#ping
```

```
Protocol [ip]:
```

Target IP address:10.0.0.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:5

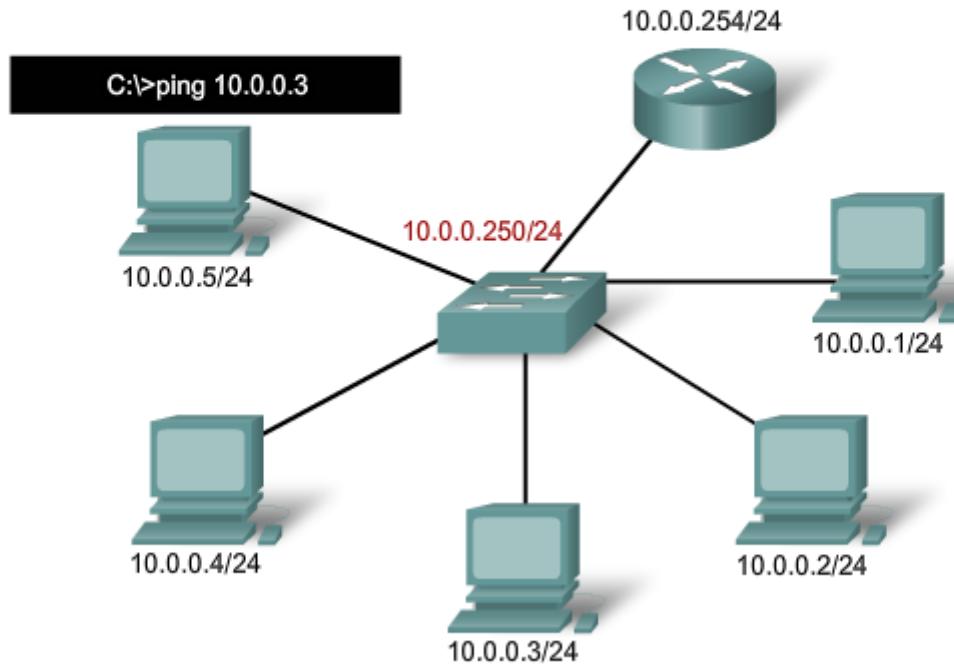
Extended commands [n]: n

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.

Observe que al ingresar "y" en la petición de entrada "Extended commands" se proporcionan más opciones provechosas para la resolución de problemas. Estas opciones se analizarán en la práctica de laboratorio y en las actividades del Packet Tracer.

Prueba de la red local

Hacer ping con éxito a las otras direcciones IPv4 del host verifica que tanto el host local como los otros hosts están configurados correctamente.



11.3.4 Prueba de Gateway t conectividad remota

El siguiente paso de la secuencia de prueba es utilizar el comando ping para verificar que un host local puede conectarse con una dirección de gateway. Esto es sumamente importante porque el gateway es la entrada y salida del host hacia la red más amplia. Si el comando ping devuelve una respuesta satisfactoria, se verifica la conectividad a la gateway.

Al comenzar, elija una estación como dispositivo de origen. En este caso, se optó por 10.0.0.1, como se indica en la figura. Utilice el comando ping para llegar a la dirección de gateway, en este caso, 10.0.0.254.

```
c:\>ping 10.0.0.254
```

La dirección IPv4 de gateway debe encontrarse disponible en la documentación de la red, pero si no se encontrara disponible, utilice el comando ipconfig para detectar la dirección IP de gateway.

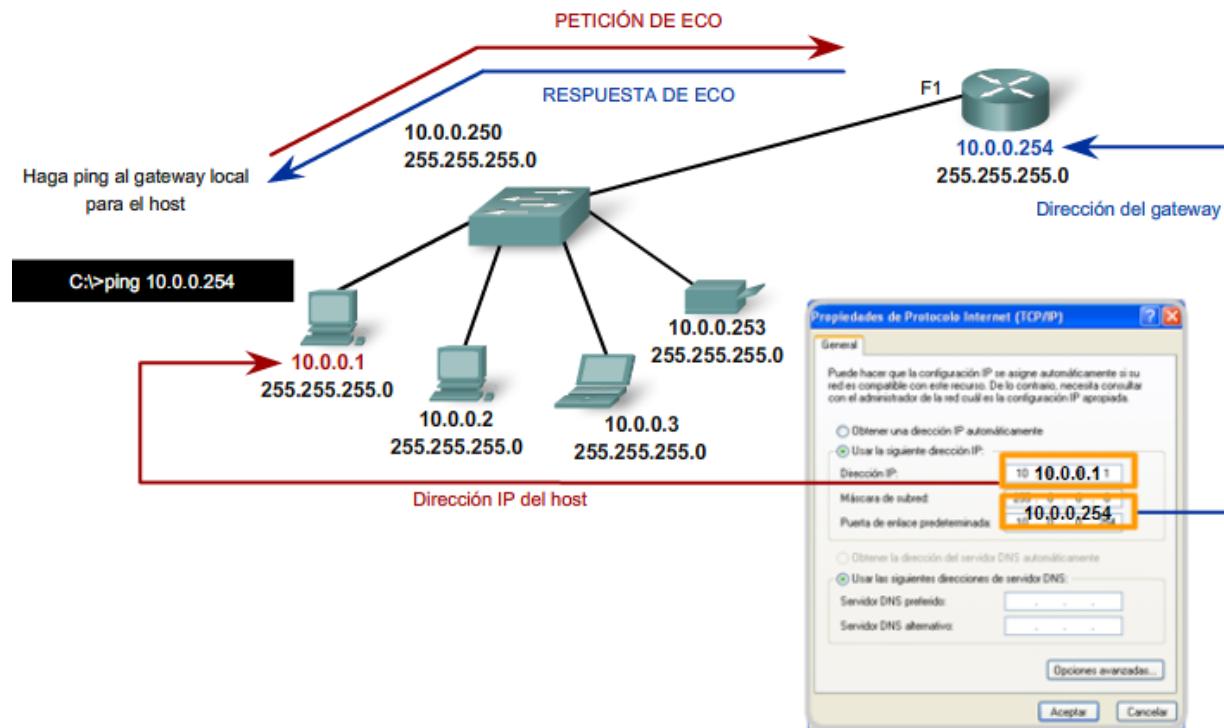
Prueba del siguiente salto en la ruta

En un router, use el IOS para probar el siguiente salto de las rutas individuales. Como se analizó anteriormente, la tabla de enrutamiento muestra el siguiente salto de cada ruta. Para determinar el siguiente salto, examine la tabla de enrutamiento desde el resultado del comando show ip route. Los paquetes que trasladan tramas y que se dirigen a la red destino indicada en la tabla de enrutamiento se envían al dispositivo que representa el siguiente salto. Si el siguiente salto es inaccesible, el paquete se descarta. Para probar el siguiente salto, determine la ruta apropiada al destino y trate de hacer ping al gateway por defecto o al siguiente salto apropiado para esa ruta en la tabla de enrutamiento. Una falla en el ping indica que puede existir un problema de configuración o de hardware. Sin embargo, el ping también puede estar prohibido por la seguridad del dispositivo.

Si la prueba de gateway falla, retroceda un paso en la secuencia y pruebe otro host en la LAN local para verificar que el problema no sea el host origen. Luego verifique la dirección de gateway con el administrador de red a fin de asegurar que se esté probando la dirección correcta.

Si todos los dispositivos están configurados en forma adecuada, controle el cableado físico para asegurar que esté firme y correctamente conectado. Mantenga un registro preciso de los intentos que se han realizado para verificar la conectividad. Esto será de ayuda para solucionar este problema y, tal vez, problemas futuros.

Prueba de conectividad del gateway



Prueba de hosts remotos

Una vez que se ha completado la verificación de la LAN local y el gateway, la prueba puede continuar con los dispositivos remotos, lo cual es el siguiente paso en la secuencia de prueba.

La figura ilustra un ejemplo de topología de red. Hay 3 hosts dentro de una LAN, un router (que actúa como gateway) que está conectado a otro router (que actúa como gateway para una LAN remota) y 3 hosts remotos. Las pruebas de verificación deben comenzar dentro de la red local y progresar externamente hacia los dispositivos remotos.

Comience con la prueba de la interfaz externa de un router que está directamente conectada a una red remota. En este caso, el comando ping prueba la conexión a 192.168.0.253, la interfaz externa del router de gateway de la red local.

Si el comando ping resulta satisfactorio, se verifica la conectividad a la interfaz externa. A continuación, haga ping a la dirección IP externa del router remoto, en este caso, 192.168.0.254. Si es satisfactorio, se verifica la conectividad del router remoto. Si se produce una falla, intente aislar el problema. Vuelva a realizar la prueba hasta que exista una conexión válida a un dispositivo y verifique dos veces cada una de las direcciones.

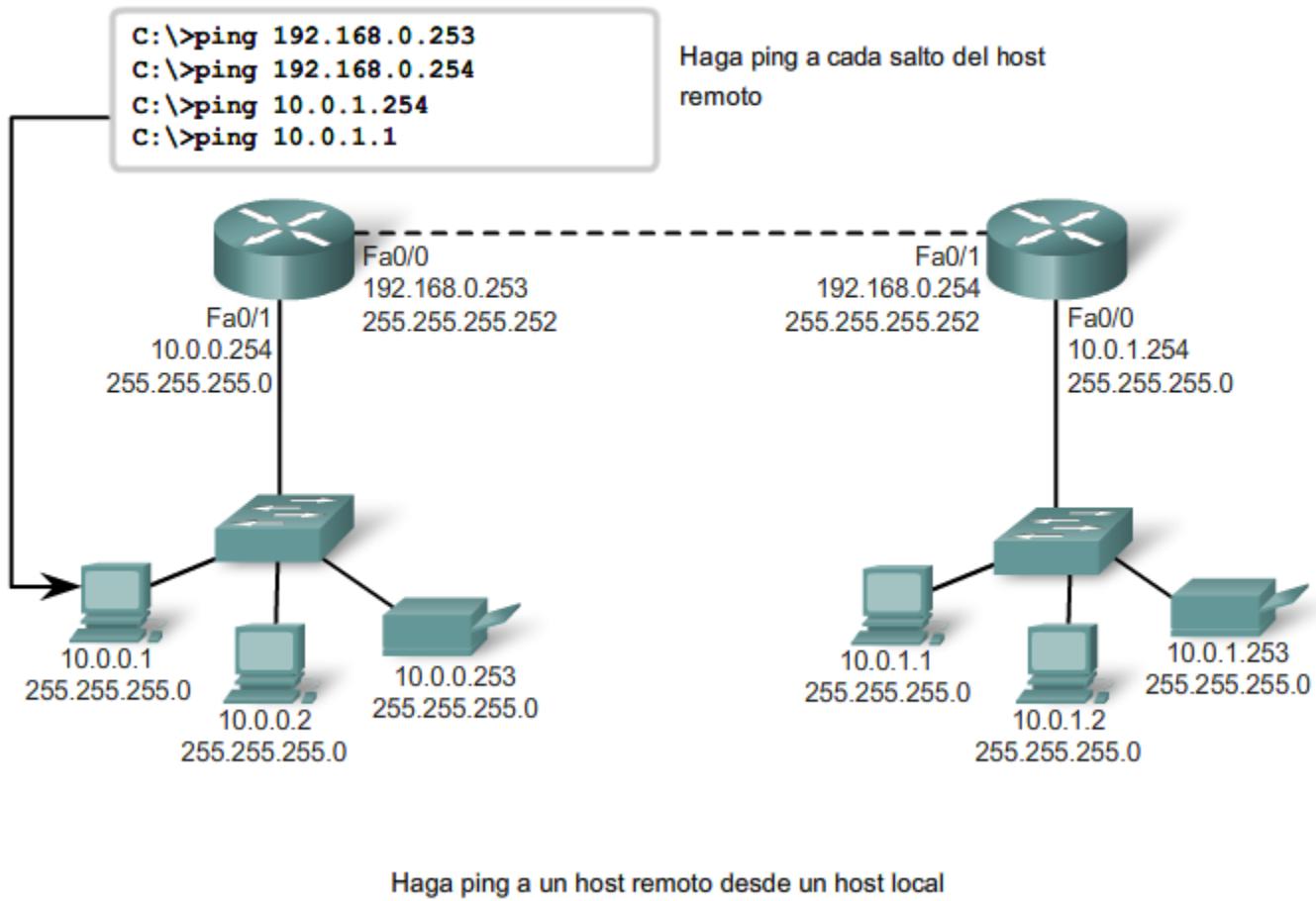
El comando ping no siempre será de ayuda para identificar el motivo subyacente de un problema, pero puede aislar los problemas y orientar el proceso de resolución de problemas. Documente cada prueba, los dispositivos involucrados y los resultados.

Verifique la conectividad remota del router

Un router establece una conexión entre ciertas redes gracias al reenvío de paquetes entre ellas. Para reenviar paquetes entre dos redes dadas, el router debe poder comunicarse tanto con la red de origen como con la red de destino. El router necesitará rutas hacia ambas redes en su tabla de enrutamiento.

Para probar la comunicación hacia la red remota, se puede hacer ping a un host conocido en esta red remota. Si no puede hacer ping correctamente en el host de la red remota desde un router, primero debe verificar la tabla de enrutamiento en busca de una ruta adecuada hacia cada red remota. Es posible que el router use la ruta predeterminada para llegar a un destino. Si no hay una ruta para llegar a esta red, será necesario determinar por qué no existe la ruta. Como siempre, también se debe descartar que el ping no esté prohibido administrativamente.

verificación de conectividad



11.3.5 Rastreo e interpretación de los resultados de rastreo

El siguiente paso en la secuencia de prueba es realizar un rastreo.

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 con Windows, utilice tracert. Cuando lleve a cabo el rastreo desde la CLI de un router, utilice traceroute.

Ping y Trace

Ping y trace pueden utilizarse en forma conjunta para diagnosticar un problema.

Supongamos que se ha establecido una conexión satisfactoria entre el Host 1 y el Router A, como se muestra en la figura.

Luego, supongamos que el Host 1 hace ping al Host 2 mediante este comando.

```
C:\>ping 10.1.0.2
```

El comando ping devuelve este resultado:

Ping 10.1.0.2 con 32 bytes de datos:

Tiempo límite de la solicitud.

Estadísticas de ping para 10.1.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

The ping test failed.

Ésta es una prueba de comunicación fuera de la red local a un dispositivo remoto. Dado que el gateway local respondió pero el host más distante no lo hizo, el problema parece estar en algún punto fuera de la red local. Un próximo paso es aislar el problema de una red en particular fuera de la red local. Los comandos trace pueden mostrar la ruta de la última comunicación satisfactoria.

Trace a un host remoto

Del mismo modo que los comandos ping , los comandos trace se ingresan en la línea de comandos y toman una dirección IP como argumento.

Suponiendo que se emitirá el comando desde un equipo con Windows, se utilizará el formato tracert :

C:\>tracert 10.1.0.2

Rastreo de la ruta a 10.1.0.2 en un máximo de 30 saltos

1 2 ms 2 ms 2 ms 10.0.0.254

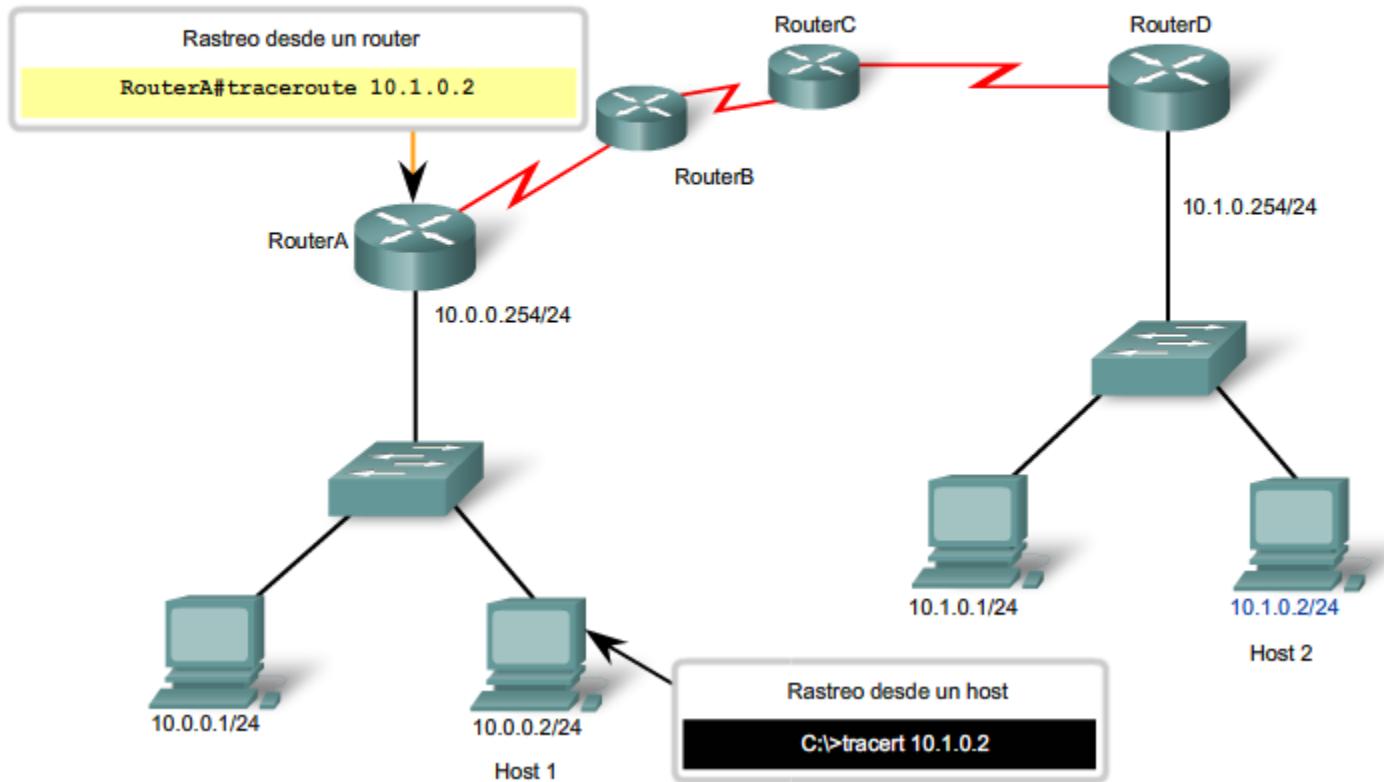
2 * * * Tiempo límite de la solicitud.

3 * * * Request timed out.

4 ^C

La única respuesta satisfactoria provino del gateway en el Router A. Las peticiones de rastreo al siguiente salto expiraron, lo cual significa que el siguiente salto no respondió. Los resultados del comando trace indican que la falla entonces se encuentra en la internetwork más allá de la LAN.

Prueba de la ruta a un host remoto



Secuencia de prueba: Unificación

A modo de revisión, recorramos la secuencia de prueba en otra situación.

Prueba 1: Loopback local: Exitoso

```
C:\>ping 127.0.0.1
```

Pinging 127.0.0.1 with 32 bytes of data:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:
```

Paquetes: Enviados = 4, Recibidos = 4, Perdidos = 0 (0% de pérdida),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 0 ms, Máximo = 0 ms, Promedio = 0 ms

El Host 1 tiene la stack de IP configurada correctamente.

Prueba 2: NIC local: Exitosa

C:\>ping 192.168.23.3

Pinging 192.168.23.3 with 32 bytes of data:

Reply from 192.168.23.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.23.3:

Paquetes: Enviados = 4, Recibidos = 4, Perdidos = 0 (0% de pérdida), Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 0 ms, Máximo = 0 ms, Promedio = 0 ms

Se asignó correctamente la dirección IP a la NIC y la electrónica de la NIC responde a la dirección IP.

Prueba 3: Ping de gateway local: Exitoso

C:\>ping 192.168.23.254

Pinging 192.168.23.254 with 32 bytes of data:

Reply from 192.168.23.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.23.254:

Paquetes: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

El gateway por defecto está en funcionamiento. De esta manera también se verifica el funcionamiento de la red local.

Prueba 4: Ping de host remoto: Falla

C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.11.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Esta es una prueba de la comunicación fuera de la red local. Ya que la gateway respondió pero el host más lejano no lo hizo, el problema parece encontrarse más allá de la red local.

Prueba 5: Traceroute al host remoto: Falla en el primer salto

C:\>tracert 192.168.11.1

Tracing route to 192.168.11.1 over a maximum of 30 hops

1 * * * Request timed out.

2 * * * Request timed out.

3 ^C

Parece haber resultados contradictorios. El gateway por defecto responde, lo cual indica que existe comunicación entre el Host1 y el gateway. Por otro lado, el gateway parece no estar respondiendo a traceroute.

Una explicación posible es que el host local no esté correctamente configurado para usar 192.168.23.254 como gateway por defecto. Para confirmarlo se analizará la configuración del Host1.

Prueba 6: Análisis de configuración de host para determinar el gateway local correcto: Incorrecto

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

IP Address : 192.168.23. 3

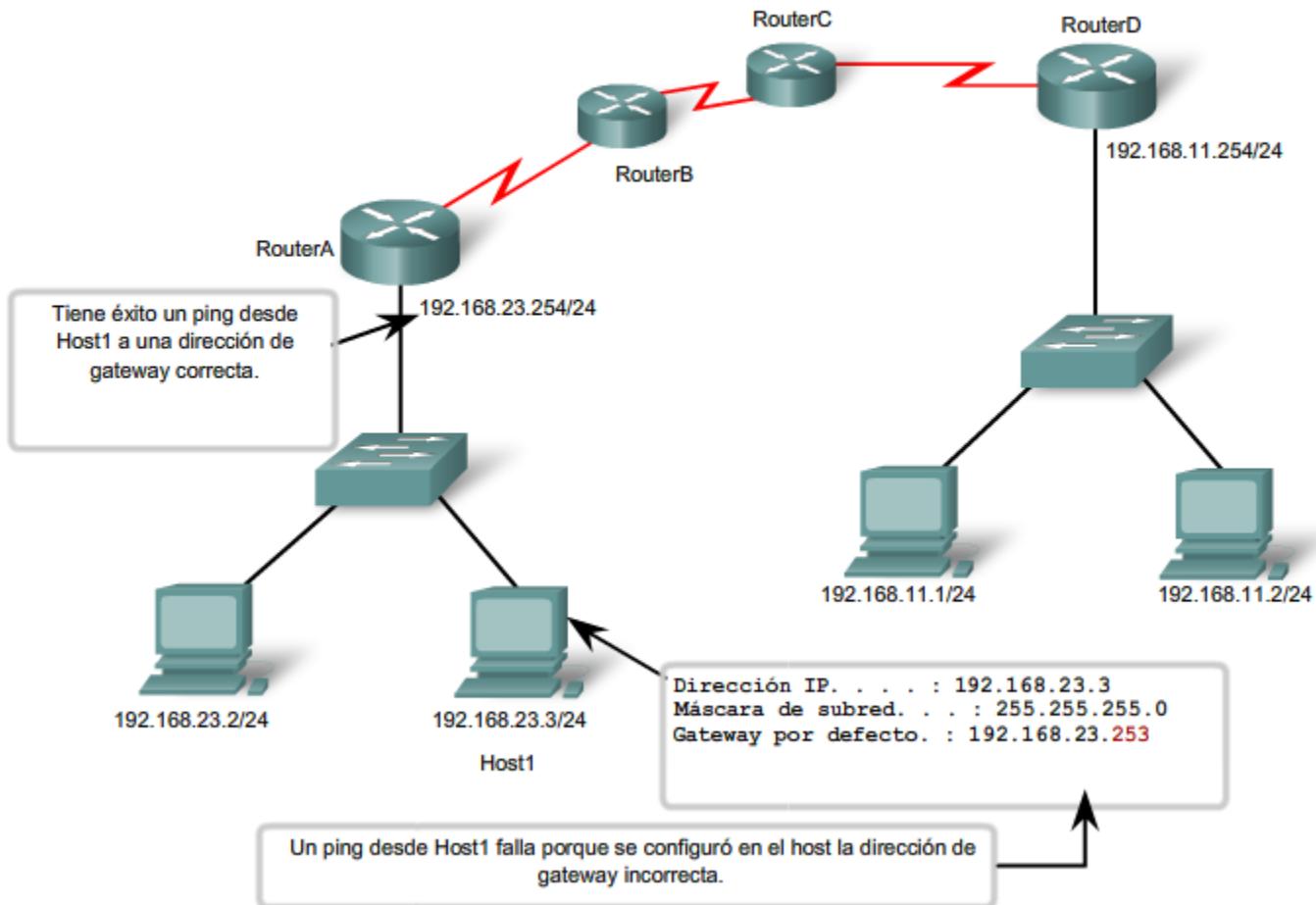
Subnet Mask : 255.255.255.0

Default Gateway : 192.168.23.253

A partir del resultado del comando ipconfig se puede determinar que la gateway no se encuentra configurada correctamente en el host. Esto explica la falsa indicación de que el problema se encontraba en la internetwork fuera de la red local. Aunque la dirección 192.168.23.254 respondía, esta no era la dirección configurada en el Host1 como gateway.

Al no poder construir una trama, el Host1 descarta el paquete. En este caso, no hay respuesta indicada desde el rastreo al host remoto.

Interpretación de los resultados de la prueba



11.4 MONITOREO Y DOCUMENTACIÓN DE REDES

11.4.1 Líneas de base de red fundamentales

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. Es más que un simple informe que detalla el estado de la red en un momento determinado. 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 y de las cargas le ayudará al usuario 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. La figura muestra la información que se debe registrar.

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 efectivo de la información guardada es comparar los resultados en el transcurso del tiempo. 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, abarcaremos algunas técnicas básicas y analizaremos el propósito de las líneas de base.

Línea de base con ping

2 DE FEB DE 2007 08:14:43

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<1ms TTL=128
```

17 DE MAR DE 2007 14:41:06

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.254.159: bytes=32 time<6ms TTL=128
```

Captura de host

Un método común para capturar información de la línea de base es copiar el resultado de la ventana de línea de comandos y pegarlo en un archivo de texto.

Para capturar los resultados del comando ping comience por ejecutar un comando en la línea de comandos similar a este. Sustituya una dirección IP válida en su red.

C:\>ping 10.66.254.159

La respuesta aparecerá debajo del comando.

Observe el ejemplo que se muestra en la figura.

Con el resultado aún visible en la ventana de comando, siga estos pasos:

1. Haga clic con el botón derecho del mouse en la ventana de petición de entrada de comando, luego haga clic en Select All.
2. Presione Ctrl-C para copiar el resultado.

3. Abra un editor de texto.

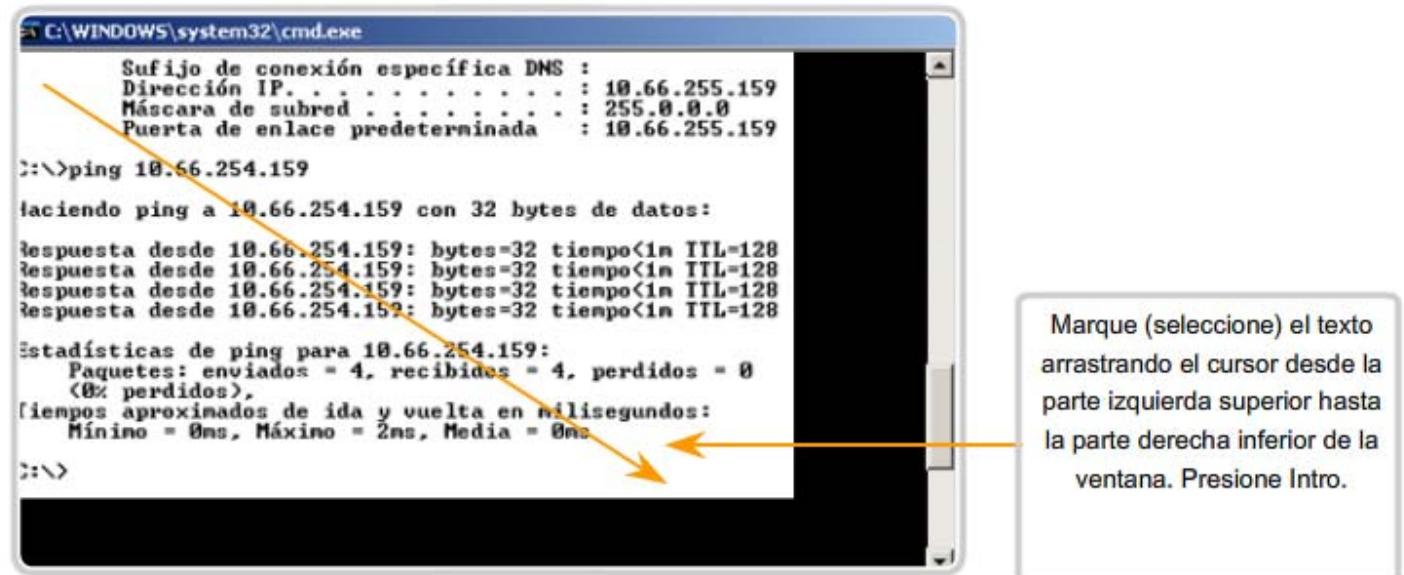
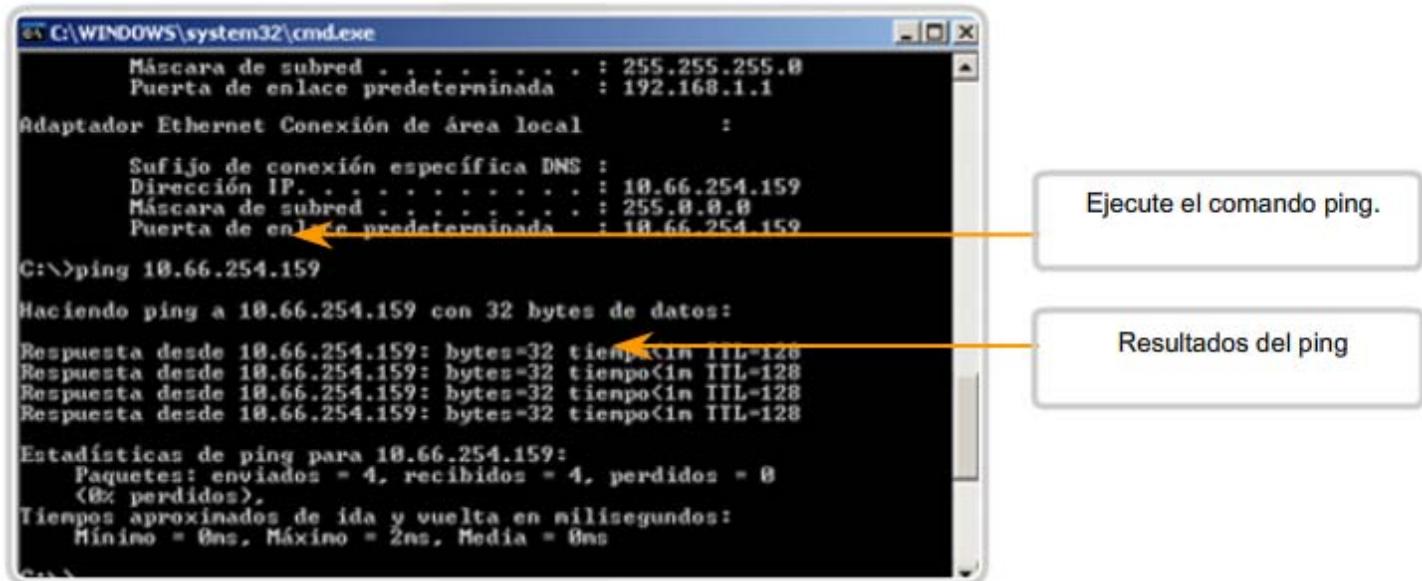
4. Presione Ctrl-V para pegar el texto.

5. Guarde el archivo de texto con la fecha y la hora como parte del nombre.

Ejecute la misma prueba durante algunos días y guarde la información en todas las oportunidades. Un análisis de los archivos comenzará a revelar patrones en el rendimiento de la red y proveerá la línea de base para la futura resolución de problemas.

Cuando seleccione texto en la ventana de comando, use el comando Select All para copiar todo el texto de la ventana. Use el comando Mark para seleccionar una parte del texto.

Consulte la figura donde encontrará instrucciones de uso con Windows XP Professional.



Captura de IOS

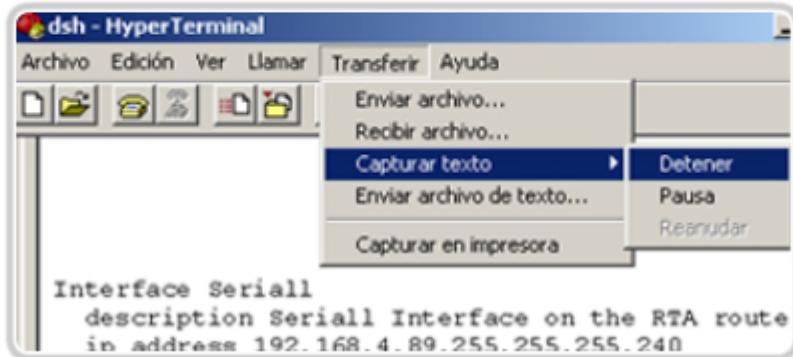
La captura del resultado del comando ping también puede realizarse desde la petición de entrada de IOS. Los siguientes pasos describen cómo capturar el resultado y guardarla en un archivo de texto.

Cuando se usa HyperTerminal para el acceso, los pasos son:

1. En el menú Transfer, haga clic en Capture Text.
2. Seleccione Browse para encontrar el archivo donde guardará o para escribir el nombre de éste.
3. Haga clic en Start para empezar a capturar texto.
4. Ejecute el comando ping en el modo EXEC del usuario o ante la petición de entrada del modo EXEC privilegiado. El router colocará el texto que se muestra en la terminal en la ubicación elegida.
5. Visualice el resultado para verificar que no esté dañado.
6. En el menú Transfer, haga clic en Capture Text, y luego haga clic en Stop Capture.

Los datos generados a través del indicador del equipo o el indicador del router pueden contribuir a la línea de base.

Captura de ping del router - Cómo guardar en archivo de texto



En la sesión de terminal:

1. Inicie el proceso de captura de texto.
2. Ejecute un comando `ping <ip address> command`.
3. Detenga el proceso de captura.
4. Guarde el archivo de texto.

11.4.2 Captura e interpretación del comando trace

Como se analizó previamente, el comando trace puede utilizarse para rastrear los pasos o saltos entre los hosts. Si la petición llega al destino deseado, el resultado muestra cada router que atraviesa el paquete. Se puede capturar este resultado y utilizarlo de la misma manera que se utiliza el resultado de ping.

A veces las configuraciones de seguridad en la red destino impedirán que el rastreo llegue al destino final. Sin embargo, aún así se puede capturar la línea de base de los saltos a lo largo de la ruta.

Recuerde que la forma de usar el comando trace desde un host Windows es tracert.

Para rastrear la ruta desde su equipo hasta cisco.com, ingrese este comando en una línea de comandos:

```
C:\>tracert www.cisco.com
```

Vea la figura para obtener un ejemplo del resultado.

Los pasos que se deben seguir para guardar el resultado de trace son idénticos a los pasos necesarios para guardar el resultado de ping: Seleccione el texto en la ventana de comando y péguelo en un archivo de texto.

Los datos del comando trace pueden agregarse a los datos de los comandos ping para obtener una perspectiva combinada del rendimiento de la red. Por ejemplo, si la velocidad de un comando ping disminuye con el tiempo, compare el resultado del comando trace en el mismo período de tiempo. El análisis de los tiempos de respuesta en una comparación de salto por salto puede revelar un punto particular de tiempo de respuesta más prolongado. La causa de este retardo puede ser una congestión en el salto que crea un cuello de botella en la red.

Otro caso podría demostrar que la ruta del salto al destino puede variar con el tiempo a medida que los routers seleccionan diferentes y mejores caminos para los paquetes de rastreo. Estas variaciones pueden mostrar patrones que podrían ser útiles en la programación de grandes transferencias entre sitios.

Captura de Traceroute

```
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

 1       1 ms      <1 ms      <1 ms  192.168.0.1
 2     20 ms      20 ms      20 ms  nexthop.wa.ii.net [203.59.14.16]
 3     20 ms      19 ms      20 ms  gi2-4.per-qv1-bdr1.ii.net [203.215.4.32]
 4    79 ms      78 ms      78 ms  gi0-14-0-0.syd-ult-core1.ii.net [203.215.20.2]
 5    79 ms      81 ms      79 ms  202.139.19.33
 6   227 ms     228 ms     227 ms  203.208.148.17
 7   227 ms     227 ms     227 ms  203.208.149.34
 8   225 ms     225 ms     226 ms  208.30.205.145
 9   236 ms     249 ms     233 ms  sl-bb23-ana-8-0-0.sprintlink.net [144.232.9.23]

10   241 ms     244 ms     240 ms  sl-bb25-sj-9-0.sprintlink.net [144.232.20.159]
11   238 ms     238 ms     239 ms  sl-gw8-sj-10-0.sprintlink.net [144.232.3.114]
12   238 ms     239 ms     240 ms  144.228.44.14
13   240 ms     242 ms     248 ms  sjce-dmzbb-gw1.cisco.com [128.107.239.89]
```

Resultado de trace de ejemplo

Captura de router

La captura del resultado de traceroute también puede realizarse desde el indicador del router. Los siguientes pasos muestran cómo capturar el resultado y guardararlo en un archivo.

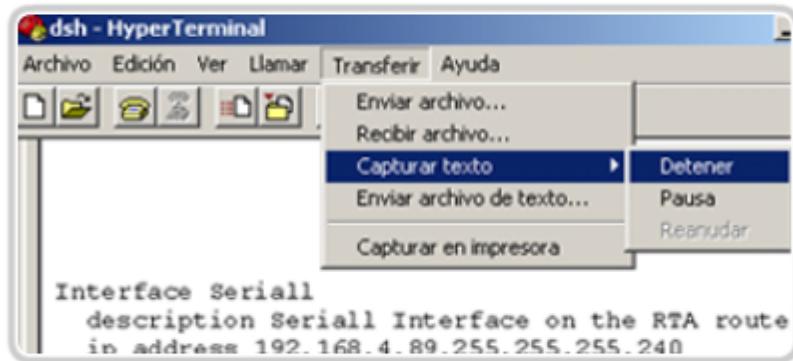
Recuerde que la forma del comando trace para la CLI del router es traceroute.

Cuando se usa HyperTerminal, los pasos que se deben seguir son:

1. En el menú Transfer, haga clic en Capture Text.
2. Seleccione un nombre para el archivo donde guardará o use Browse para localizarlo.
3. Haga clic en Start para empezar a capturar texto.
4. Ejecute el comando traceroute en el modo EXEC del usuario o ante la petición de entrada del modo EXEC privilegiado. El router colocará el texto que se muestra en la terminal en la ubicación elegida.
5. Visualice el resultado para verificar que no esté dañado.
6. En el menú Transfer, haga clic en Capture Text, y luego haga clic en Stop Capture.

Guarde los archivos de texto generados por estas pruebas en un lugar seguro, junto con el resto de la documentación de la red.

Captura de traceroute del router - Cómo guardar en archivo de texto



En la sesión de terminal:

1. Inicie el proceso de captura de texto.
2. Issue a `traceroute <ip address>` command.
3. Detenga el proceso de captura.
4. Guarde el archivo de texto.

11.4.3 Nociones sobre los nodos de la red

Si existe un esquema de direccionamiento adecuado, la identificación de direcciones IPv4 para los dispositivos de una red debería ser tarea sencilla. Sin embargo, la identificación de las direcciones físicas (MAC) puede resultar una tarea desalentadora. Necesitaría acceso a todos los dispositivos y tiempo suficiente para visualizar la información, un host por vez. Debido a que esta opción en muchos casos no resulta práctica, existe un medio alternativo para la identificación de direcciones MAC a través del comando arp.

El comando arp proporciona la asignación de direcciones físicas a direcciones IPv4 conocidas. Un método común para ejecutar el comando arp es ejecutarlo desde la petición de entrada del comando. Este método implica el envío de una solicitud de ARP. El dispositivo que necesita la información envía una solicitud de ARP broadcast a la red y sólo el dispositivo local que concuerda con la dirección IP de la solicitud envía una respuesta ARP que contiene su par IP-MAC.

Para ejecutar un comando arp, ingrese en el indicador de comando de un host:

```
C:\host1>arp -a
```

como se muestra en la figura, el comando arp enumera todos los dispositivos que se encuentran actualmente en la caché ARP, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché del router mediante el comando arp -d en caso de que el administrador de red desee volver a llenar la caché con información actualizada.

Nota: El caché ARP sólo se carga con información de dispositivos a los que se ha accedido recientemente. Para asegurar que el caché ARP esté cargado, haga ping a un dispositivo de manera tal que tenga una entrada en la tabla ARP.

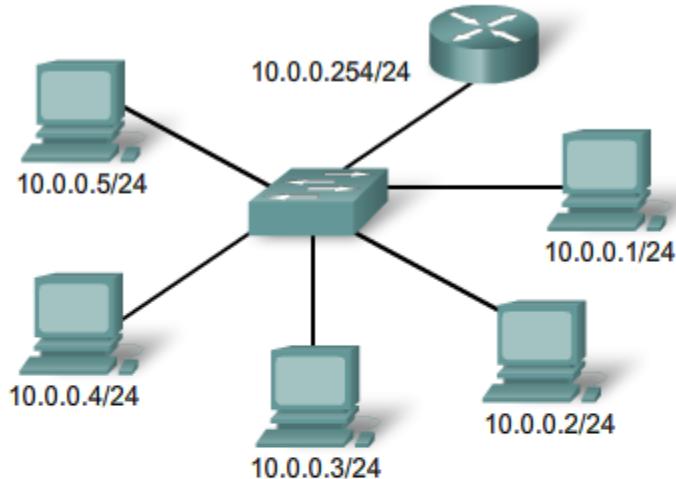
Barrido de Ping (Ping Sweep)

Otro método para reunir direcciones MAC es hacer un barrido de ping a través de un rango de direcciones IP. Un barrido de ping es un método de escaneo que puede ejecutarse en la línea de comandos o mediante el uso de herramientas de administración de red. Estas herramientas proporcionan un método para especificar un rango de hosts a los que se hará ping con un comando.

A través del barrido de ping, se pueden generar datos de red de dos maneras. En primer lugar, muchas de las herramientas de barrido de ping construyen una tabla con los hosts que responden. Estas tablas a menudo enumeran a los hosts según la dirección IP y la dirección MAC. Así se obtiene un mapa de los hosts activos en el momento del barrido.

A medida que se intenta cada ping, se realiza una solicitud de ARP para obtener la dirección IP en el caché ARP. De tal modo, se activa cada host al que se ha accedido recientemente y se garantiza que la tabla ARP esté actualizada. El comando arp puede mostrar la tabla de direcciones MAC, como se mencionó anteriormente, pero ahora se puede confiar razonablemente en que la tabla ARP está actualizada.

Aprendizaje sobre los nodos en la red



| C:\ >arp -a | Internet Address | Physical Address | Type |
|-------------|------------------|-------------------|---------|
| | 10.0.0.2 | 00-08-a3-b6-ce-04 | dynamic |
| | 10.0.0.3 | 00-0d-56-09-fb-d1 | dynamic |
| | 10.0.0.4 | 00-12-3f-d4-6d-1b | dynamic |
| | 10.0.0.254 | 00-10-7b-e7-fa-ef | dynamic |

Par de dirección MAC e IP

Conexiones del switch

Una herramienta adicional que puede resultar útil es un mapeo de cómo están conectados los hosts a un switch. Dicho mapeo se puede obtener emitiendo el comando show mac-address-table .

Por medio de una línea de comandos de un switch, ingrese el comando show con el argumento mac-address-table :

```
Sw1-2950#show mac-address-table
```

Vea la figura para obtener un ejemplo del resultado.

La tabla que aparece en la figura enumera la dirección MAC de los hosts que se encuentran conectados a este switch. Como otros resultados en la ventana de comando, esta información puede copiarse y pegarse en un archivo. Los datos también pueden pegarse en una hoja de cálculo para una manipulación más sencilla en el futuro.

El análisis de esta tabla también revela que la interfaz Fa0/23 es un segmento compartido o está conectada a otro switch. Varias direcciones MAC representan múltiples nodos. Esto indica que un puerto está conectado a otro dispositivo intermediario, como por ejemplo un hub, un punto de acceso inalámbrico u otro switch.

En cursos futuros se presentarán comandos adicionales y herramientas para recolección de datos.

Conexiones de switch

```
Sw1-2950#show mac-address-table
```

Mac Address Table

| Vlan | Mac Address | Type | Ports |
|------|----------------|---------|--------|
| All | 0014.a8a8.8780 | STATIC | CPU |
| All | 0100.0ccc.cccc | STATIC | CPU |
| All | 0100.0ccc.cccd | STATIC | CPU |
| All | 0100.0cdd.dddd | STATIC | CPU |
| 1 | 0001.e640.3b4b | DYNAMIC | Fa0/23 |
| 1 | 0002.fde1.6acb | DYNAMIC | Fa0/14 |
| 1 | 0006.5b88.dfc4 | DYNAMIC | Gi0/2 |
| 1 | 0006.5bdd.6f8e | DYNAMIC | Fa0/23 |
| 1 | 0006.5bdd.7035 | DYNAMIC | Fa0/23 |
| 1 | 0006.5bdd.72fd | DYNAMIC | Fa0/23 |
| 1 | 0006.5bdd.73b0 | DYNAMIC | Fa0/23 |
| 1 | 000e.0cb6.2b51 | DYNAMIC | Fa0/2 |
| 1 | 000f.8f28.b7b5 | DYNAMIC | Fa0/18 |
| 1 | 0011.1165.8acf | DYNAMIC | Fa0/1 |
| 1 | 0013.720b.40c3 | DYNAMIC | Fa0/19 |
| 1 | 0080.9120.1766 | DYNAMIC | Fa0/8 |
| 1 | 00a0.c949.702a | DYNAMIC | Fa0/15 |
| 1 | 00c0.b770.6c19 | DYNAMIC | Fa0/22 |
| 1 | 00c0.b770.6c8e | DYNAMIC | Fa0/21 |
| 1 | 00c0.b770.6c8f | DYNAMIC | Fa0/20 |
| 1 | 00e0.1e68.0987 | DYNAMIC | Fa0/17 |

Múltiples dispositivos conectados a Fa0/23

Tabla que muestra las direcciones MAC conectadas a las interfaces del switch

11.6 RESUMEN

11.6.1 Resumen y revisión

Este capítulo planteó las cuestiones que deben considerarse al conectar y configurar equipos, switches y routers para construir una red de área local basada en Ethernet.

Se presentó el software del Sistema operativo Internetwork (IOS) de Cisco y los archivos de configuración para routers y switches. Esto incluyó el acceso y uso de los modos de la CLI de IOS y los procesos de configuración y la comprensión de la importancia que tienen las funciones de petición de entrada y de ayuda.

La administración de los archivos de configuración de IOS y la utilización de un enfoque estructurado metódico para probar y documentar la conectividad de la red son habilidades clave que deben poseer el administrador de red y el técnico de red.

Resumen de las características y comandos de IOS:

Modo EXEC del usuario

enable - Ingresar el modo EXEC privilegiado

Modo EXEC privilegiado

copy running-config startup-config - Copiar la configuración activa a la NVRAM.

copy startup-config running-config - Copiar la configuración en la NVRAM a la RAM.

erase startup-configuration - Borrar la configuración almacenada en la NVRAM.

ping ip_address - Hacer ping a esa dirección.

traceroute ip_address - Rastrear cada salto a esa dirección.

show interfaces - Mostrar las estadísticas para todas las interfaces de un dispositivo.

show clock - Mostrar el tiempo establecido en el router.

show version - Mostrar la versión de IOS cargada actualmente, hardware e información del dispositivo.

show arp - Mostrar la tabla ARP del dispositivo.

show startup-config - Mostrar la configuración almacenada en la NVRAM.

show running-config - Mostrar el contenido del archivo de configuración actualmente en ejecución.

show ip interface - Mostrar las estadísticas de IP para la/s interfaz/ces de un router.

configure terminal - Ingresar al modo Configuración de terminal.

Modo configuración de terminal

hostname hostname - Asignar un nombre de host al dispositivo.

enable password password - Establecer una contraseña de enable no encriptada.

enable secret password - Establecer una contraseña de enable encriptada en forma segura.

service password-encryption - Encriptar la visualización de todas las contraseñas, excepto la secreta.

banner motd# message # - Establecer un título con el mensaje del día.

line console 0 - Ingresar al modo Configuración de la línea de consola.

line vty 0 4 - Ingresar al modo Configuración de línea de terminal virtual (Telnet).

interface Interface_name - Ingresar al modo Configuración de interfaz.

Modo configuración de línea

login - Habilitar la comprobación de contraseñas en el inicio de sesión.

password password - Establecer la contraseña de línea.

Modo configuración de interfaz

ip address ip_address netmask - Establecer la dirección IP de la interfaz y máscara de subred.

description description - Establecer la descripción de la interfaz.

clock rate value - Establecer la frecuencia de reloj para el dispositivo DCE.

no shutdown - Establecer la activación de la interfaz.

shutdown - Administrativamente, establecer la desactivación de la interfaz.

En este capítulo, aprendió a:

- Definir el rol del Sistema Operativo Internetwork (IOS).
- Definir el propósito de un archivo de configuración.
- Identificar diferentes clases de dispositivos que tienen el IOS incorporado.
- Identificar los factores que contribuyen al conjunto de comandos IOS disponibles para un dispositivo.
- Identificar los modos de operación IOS.
- Identificar los comandos básicos IOS.
- Indicar las similitudes y diferencias de los comandos show básicos.