5 Capa de red de OSI

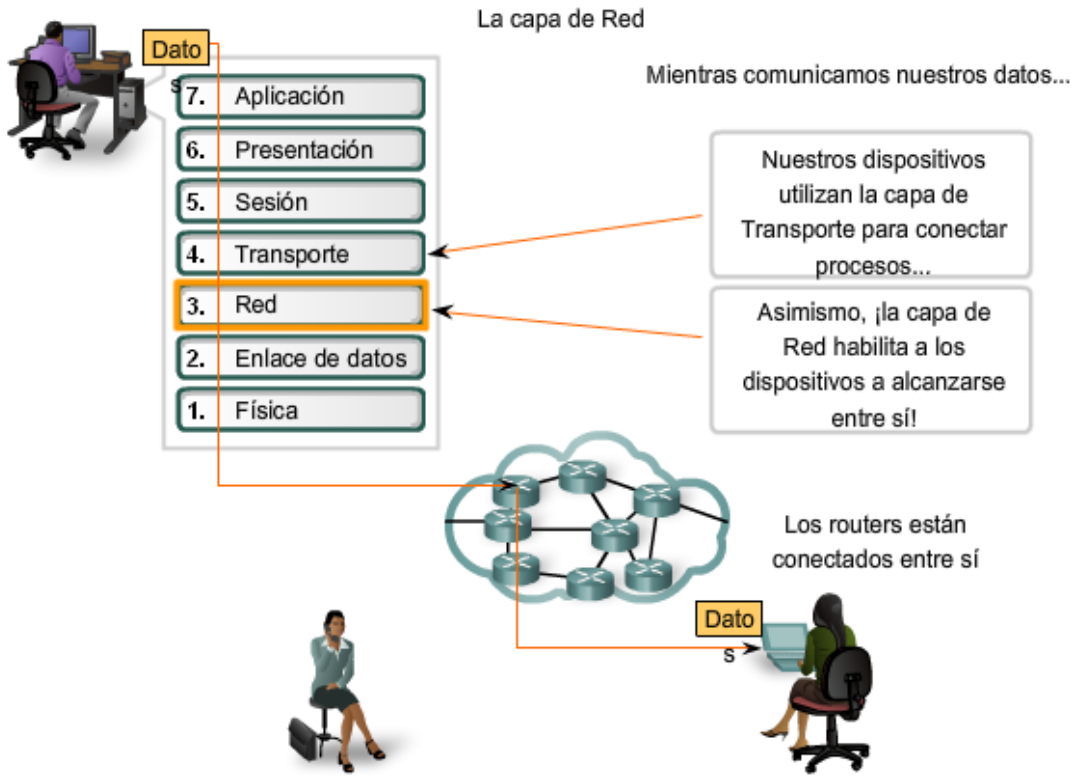
5.0 Introducción del capítulo

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.

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.

Analizaremos ahora 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.



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.

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

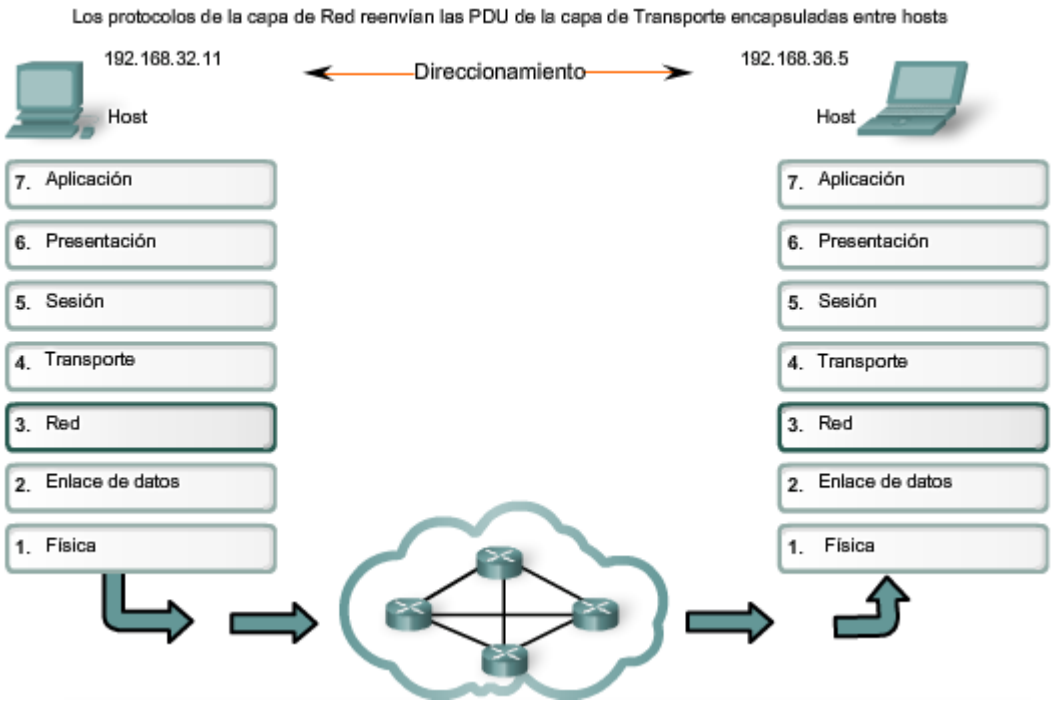
Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la 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 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.

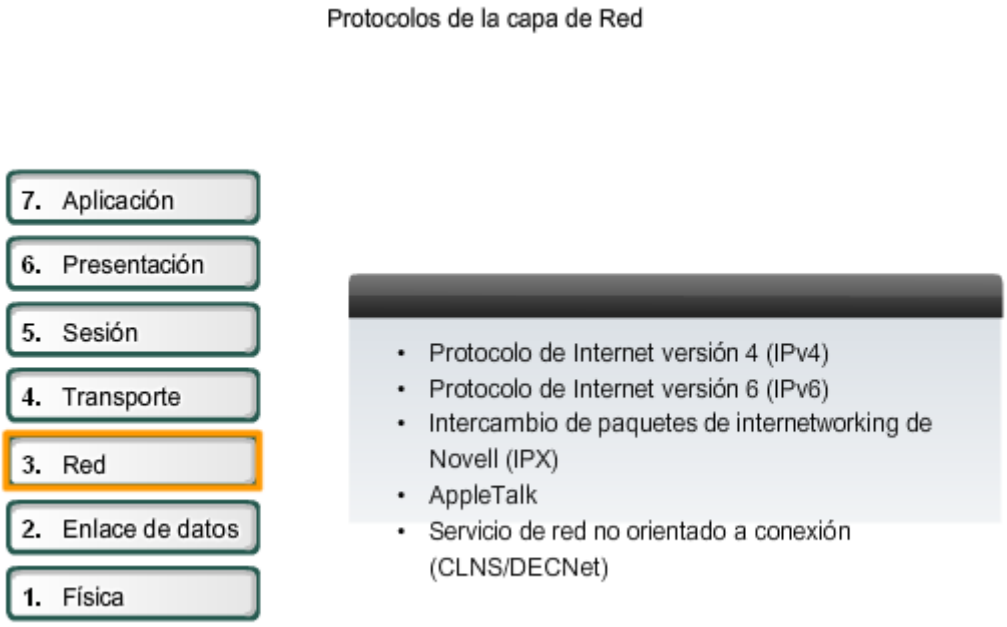


Protocolos de capa de Red

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),
- intetercambio 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 ampliamene 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. 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.

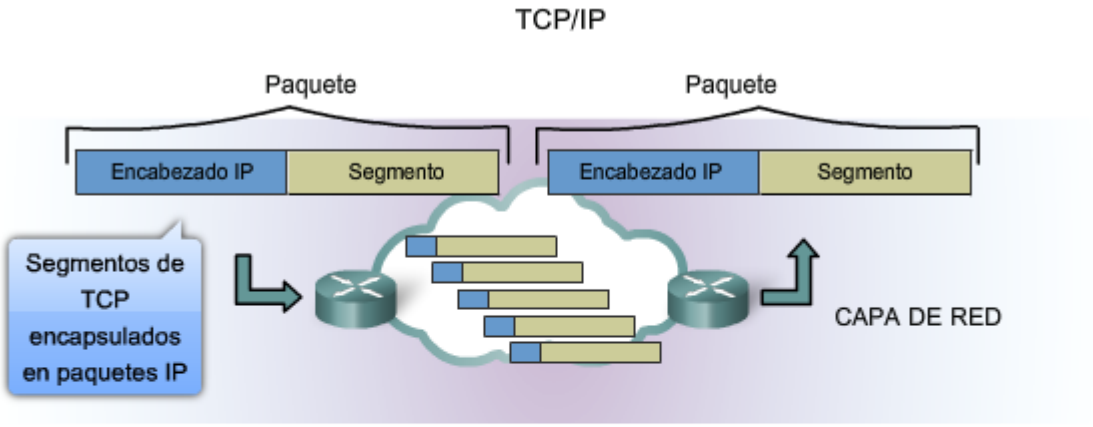
Las características de cada protocolo son diferentes. Comprender estas características le permitirá comprender la operación de los servicios descritos por este protocolo.

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.



Los paquetes IP fluyen a través de internetwork.

• 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.

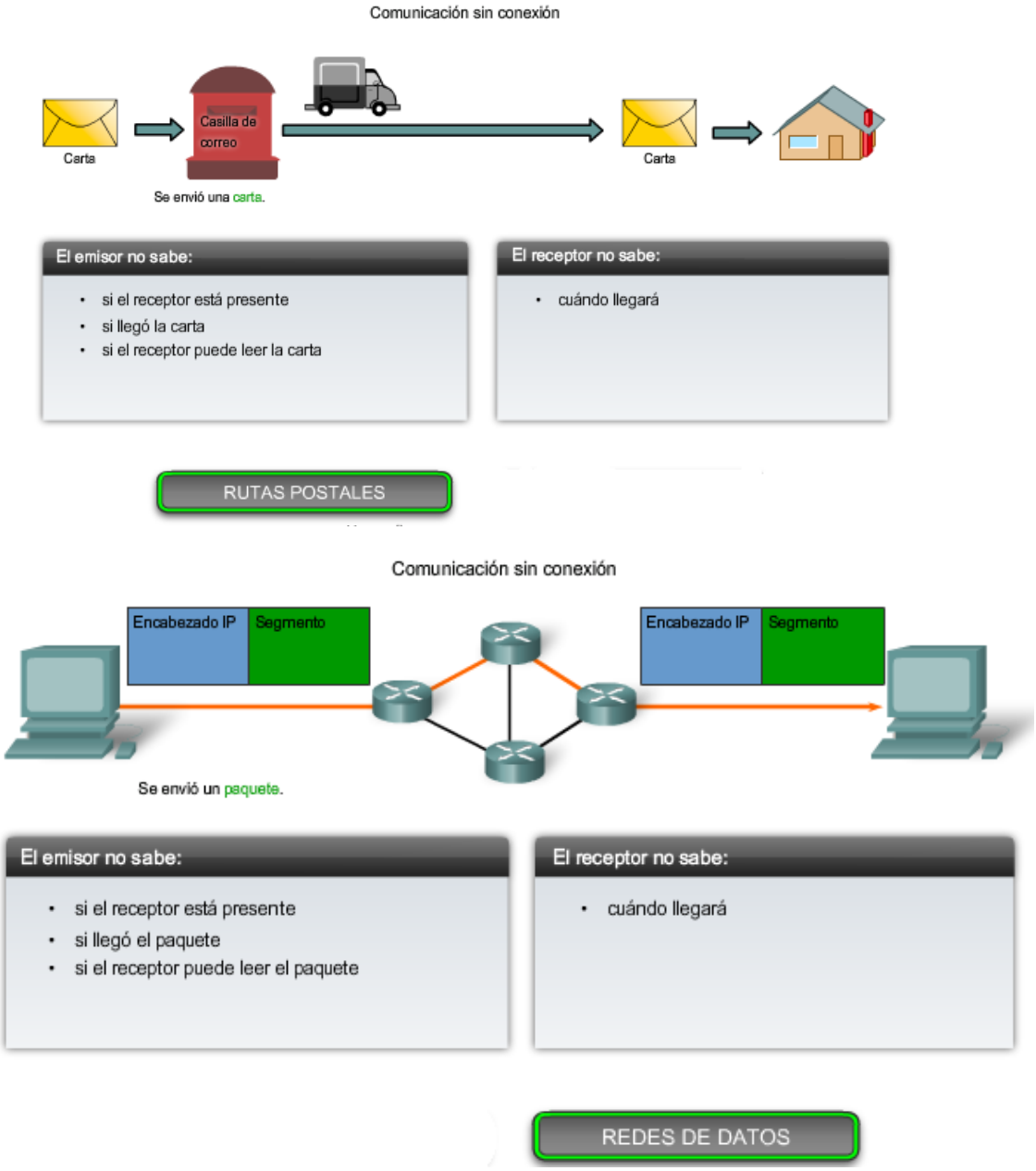
5.1.3 Protocolo IPv4: Sin conexión

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.



5.1.4 Protocolo IPv4: maximo esfuerzo

Servicio de maximo esfuerzo (no confiable)

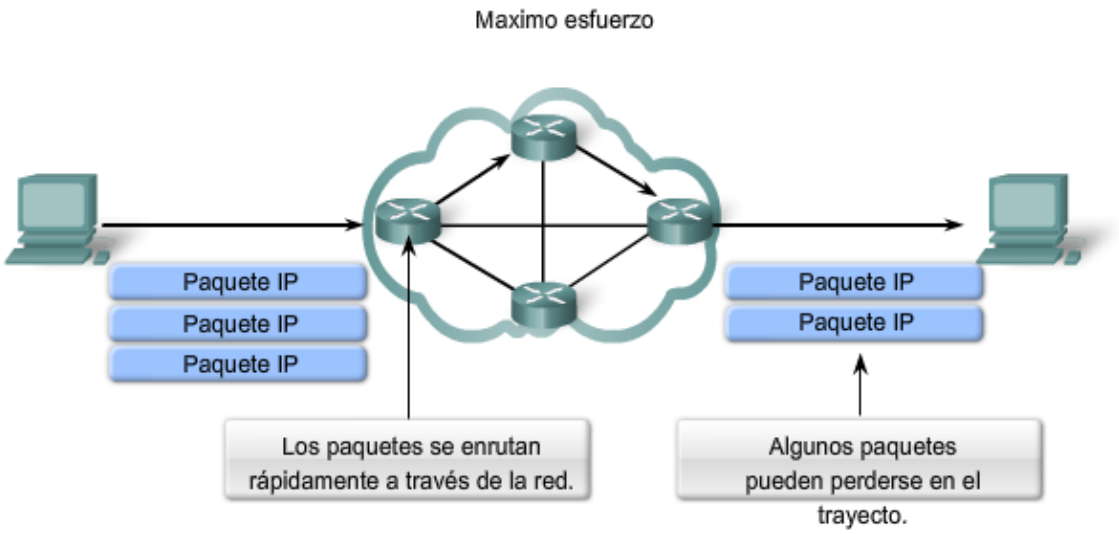
El protocolo IP no sobrecarga el servicio IP suministrando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño. Transportar estos encabezados más pequeños genera una menor sobrecarga. Menor sobrecarga significa menos demora en la entrega. Esta característica es preferible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

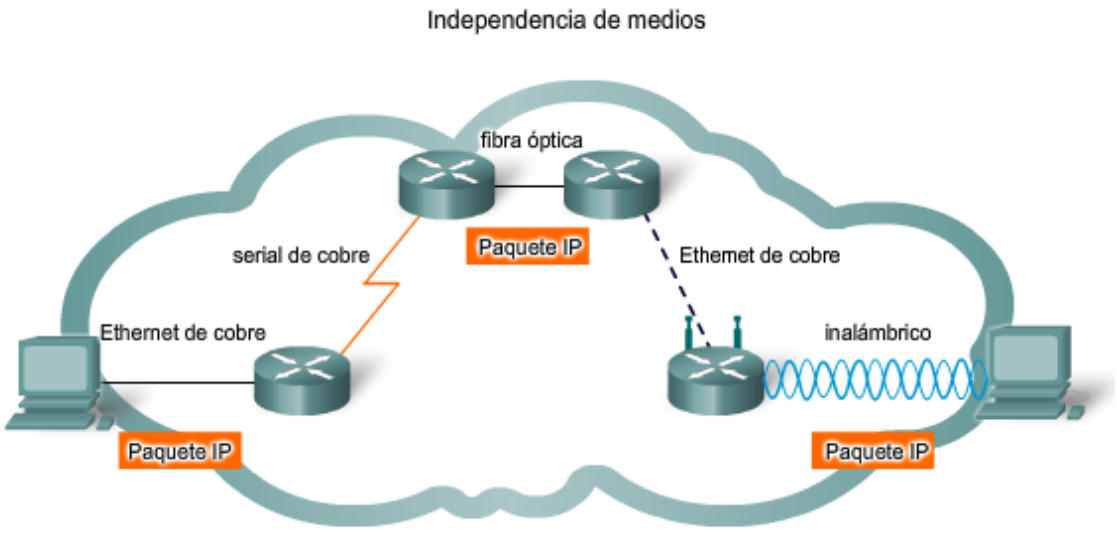
Es responsabilidad de la capa de Enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

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 intermediario, 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 paque*tes o *fragmentación*.

Enlaces

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



Los paquetes IP pueden trasladarse a través de diferentes medios.

5.1.6 Paquete IPv4: Empaquetado 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. 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.

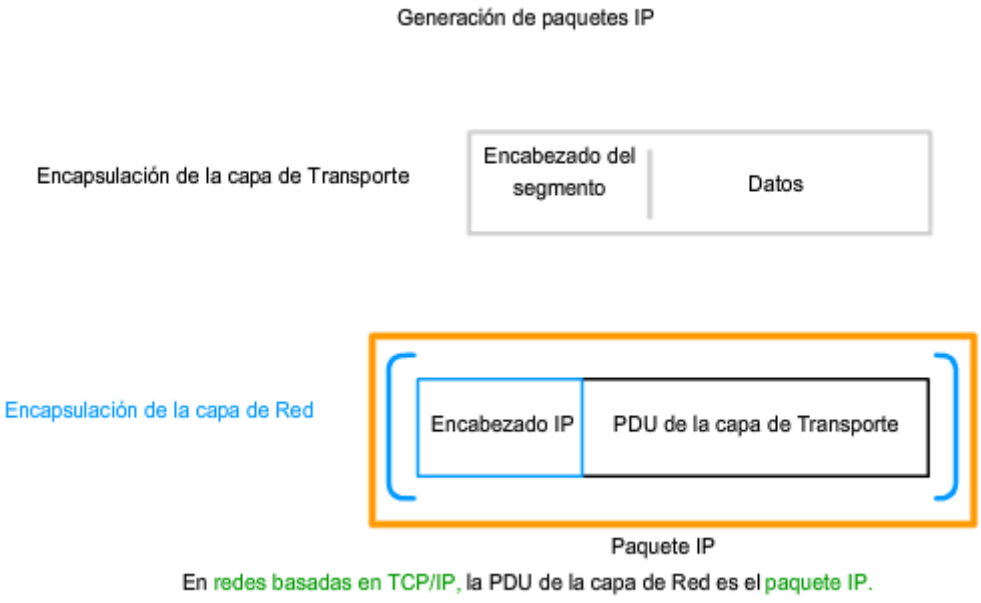
El proceso de encapsular datos por capas permite que los servicios en las diferentes capas se desarrollen y escalen sin afectar otras capas. Esto significa que los segmentos de la capa de Transporte pueden ser empaquetados fácilmente por los protocolos de la capa de Red existentes, como IPv4 e IPv6, 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 enrutamiento realizado por estos dispositivos intermediarios 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



5.1.7 Encabezado de paquete IPv4

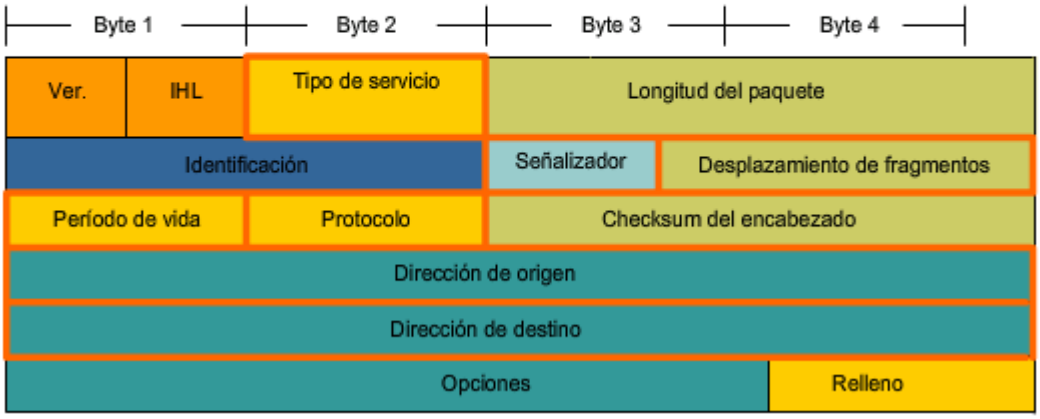
Como se muestra en la figura, un protocolo IPv4 define muchos campos diferentes en el encabezado del paquete. Estos campos contienen valores binarios que los servicios IPv4 toman como referencia a medida que envían paquetes a través de la red.

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

Campos del encabezado de paquetes IPv4



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 pero el bit DF se establece en 1, entonces el router descartará este paquete.

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

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

Otros Campos IPv4 del encabezado

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 úncamente 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.

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*4 = 20 bytes, el tamaño mínimo válido.

Longitud total = 472; tamaño del paquete (encabezado y datos) de 472 bytes.

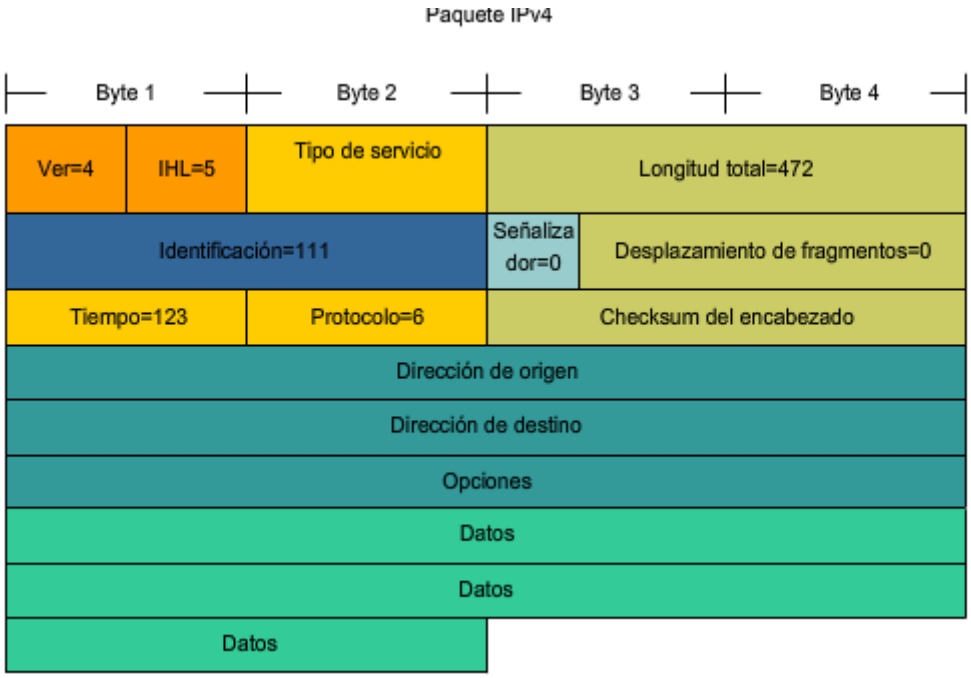
Identificación = 111; identificador original del paquete (requerido si se fragmenta posteriormente).

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: División de hosts en grupos

5.2.1 Redes: Separación de hosts 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.

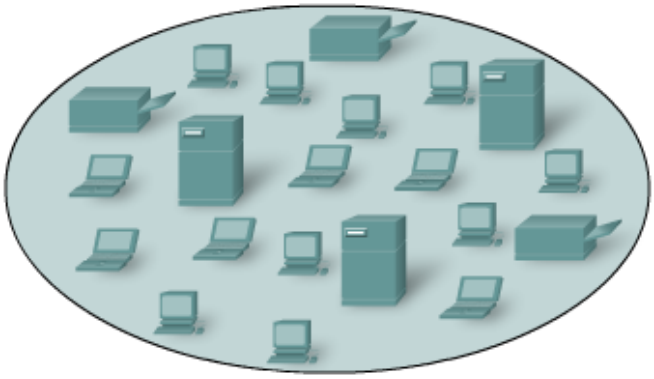
Red y subred son términos utilizados indistintamente para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP.

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.

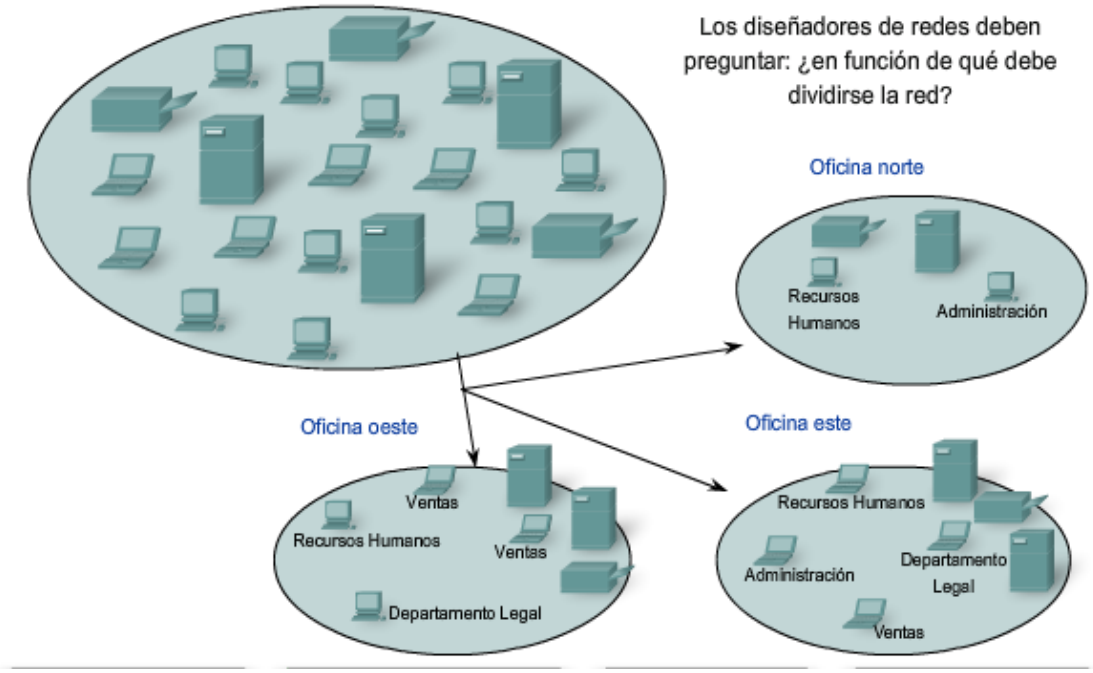
Como muestra la figura, las redes pueden agruparse basadas en factores que incluyen:

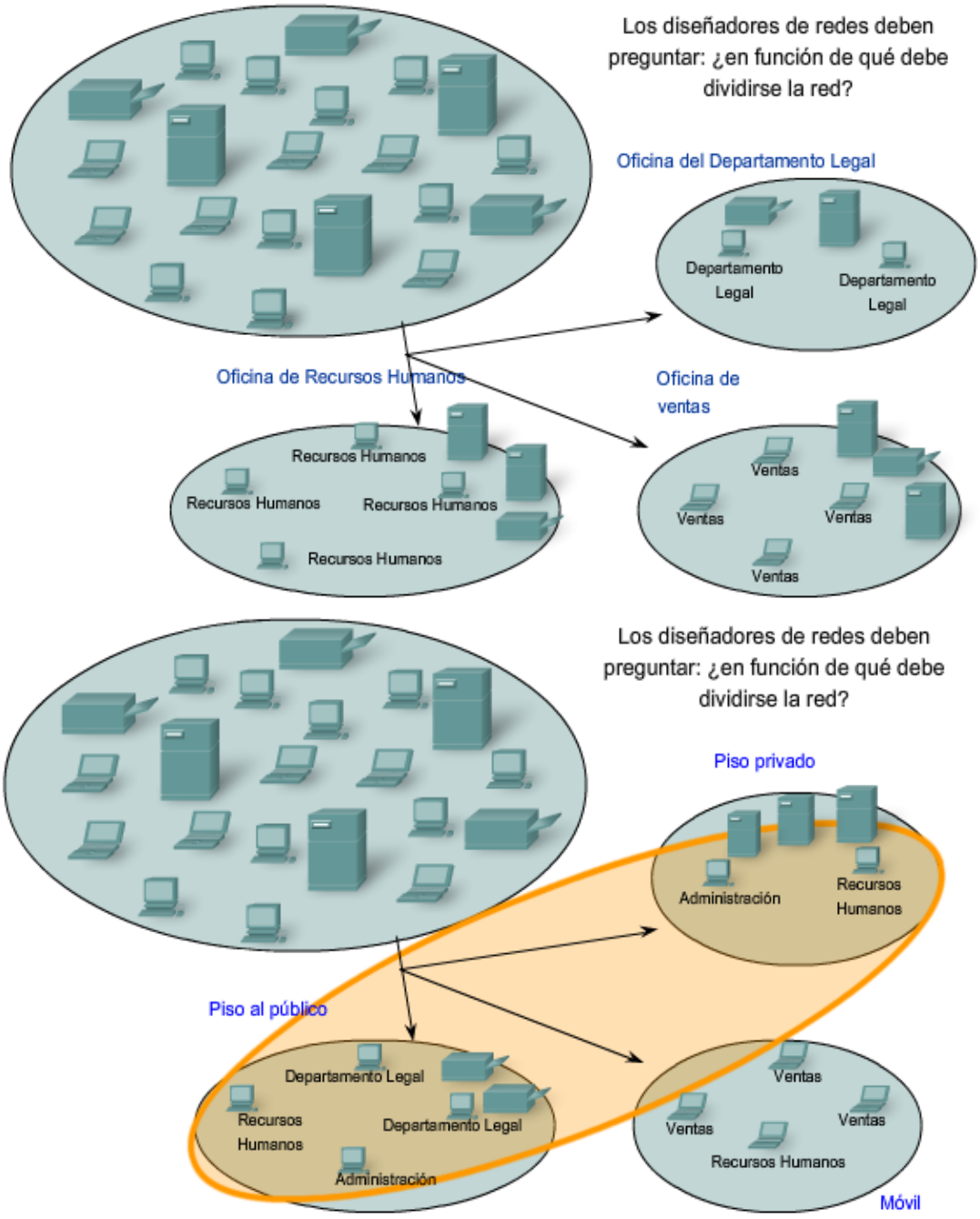
- ubicación geográfica,
- propósito, y
- propiedad.



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.





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.

Agrupación de hosts para propósitos específicos

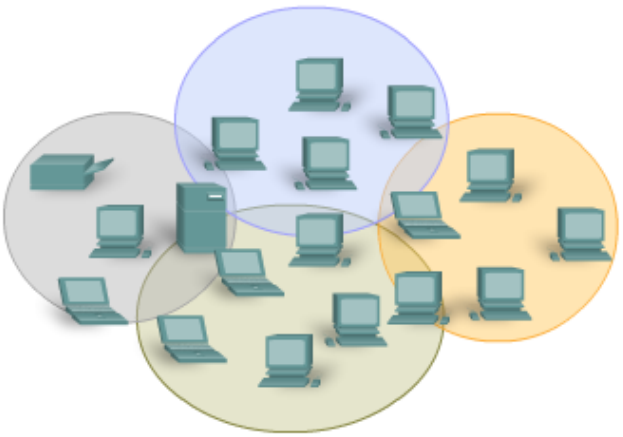
Los usuarios que tienen tareas similares usan generalmente software común, herramientas comunes y tienen patrones de tráfico común. A menudo podemos reducir

el tráfico requerido por el uso de software y herramientas específicos, ubicando estos recursos de soporte en la red con los usuarios.

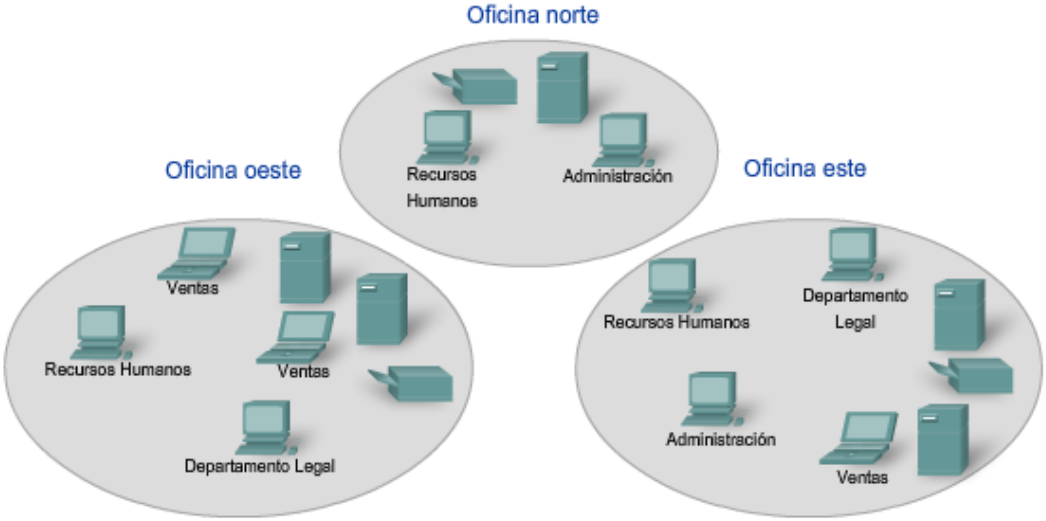
El volumen del tráfico de datos de la red generado por las diferentes aplicaciones puede variar significativamente. Dividir redes basadas en el uso facilita la ubicación efectiva de los recursos de la red así como también el acceso autorizado a esos recursos. Los profesionales en redes necesitan equilibrar 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.

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.

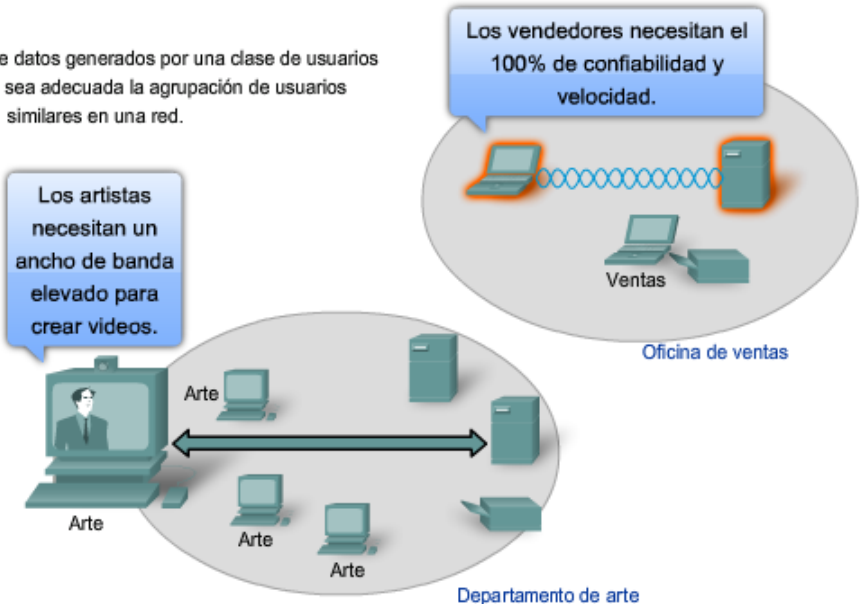


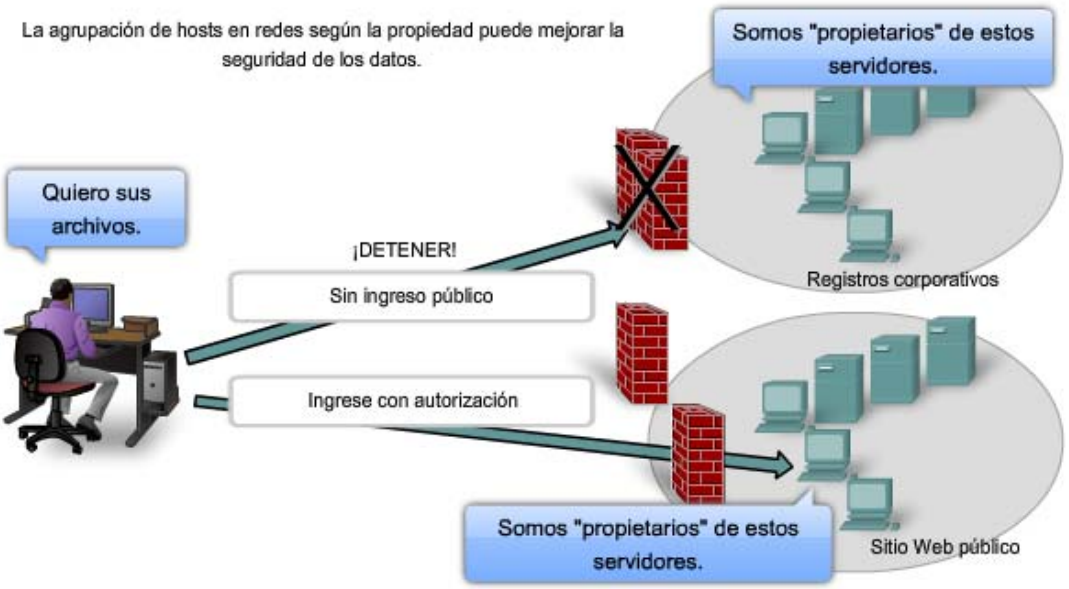
Existen muchas ventajas al dividir una red en segmentos administrables.



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.

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.





5.2.2 ¿Por qué separar hosts 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.

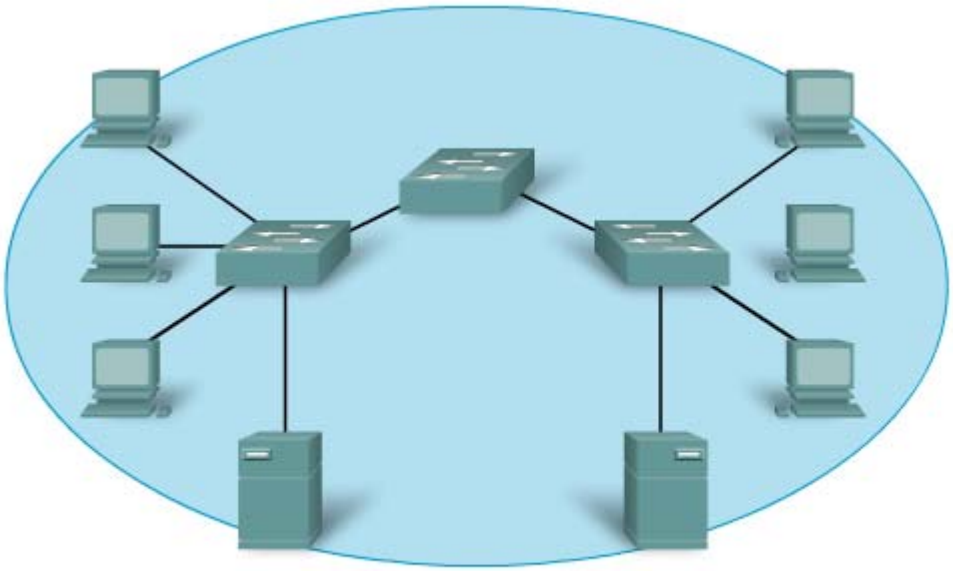
La división de grandes redes para que los host que necesitan comunicarse estén agrupados reduce el tráfico a través de los internetworks.

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.

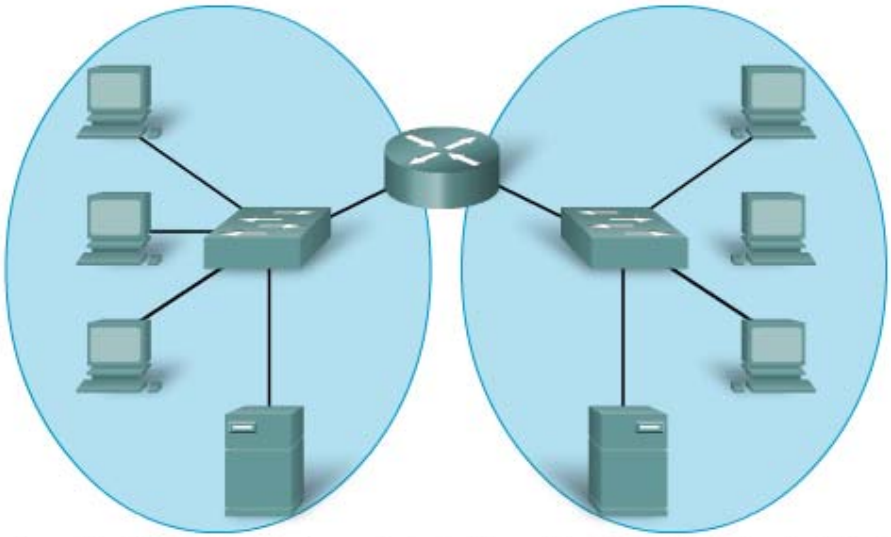
Un broadcast es un mensaje desde un host hacia **todos** los otros hosts en la red. Comúnmente, un host inicia un broadcast cuando se requiere información sobre otro host desconocido. Los broadcasts son una herramienta necesaria y útil utilizada por protocolos para permitir la comunicación de datos en 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.



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.



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.

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.

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.

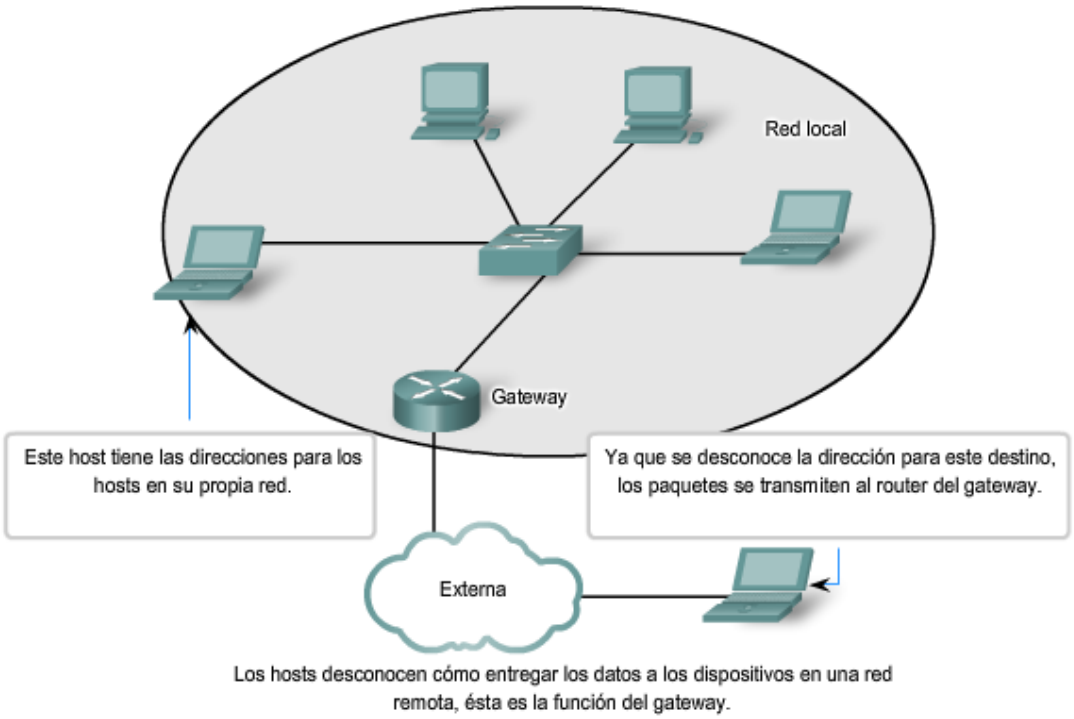
La seguridad entre redes es implementada en un dispositivo intermediario (router o firewall) en el perímetro de la red. La función del firewall realizada por este dispositivo permite que datos conocidos y confiables accedan a la red.

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 *gateway*. El gateway es un router en una red que sirve como una salida desde esa red.



5.2.5 ¿Cómo separamos los 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.

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

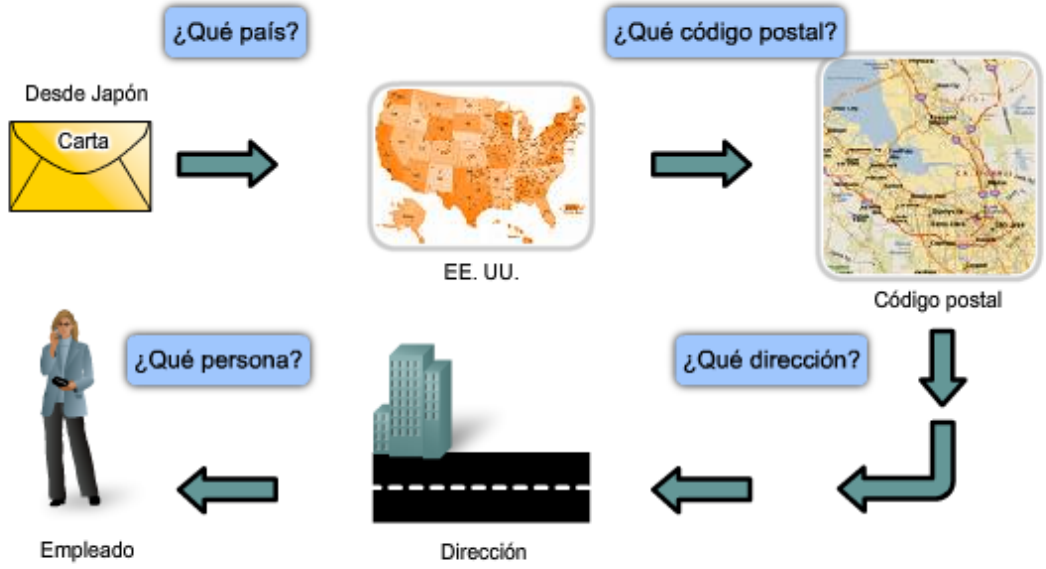
Cuando una carta se envía por correo postal en el país de origen, la autoridad postal sólo observaría el país de destino y notaría que la carta está destinada para EE. UU. En este nivel, no se necesita ningún otro detalle de dirección.

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.



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 paso se convierte a su valor decimal y la dirección completa escrita como los cuatro valores decimales separados por punto (período).

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 creado, se requiere que cada uno de los 32 bits indentifique un host individual.

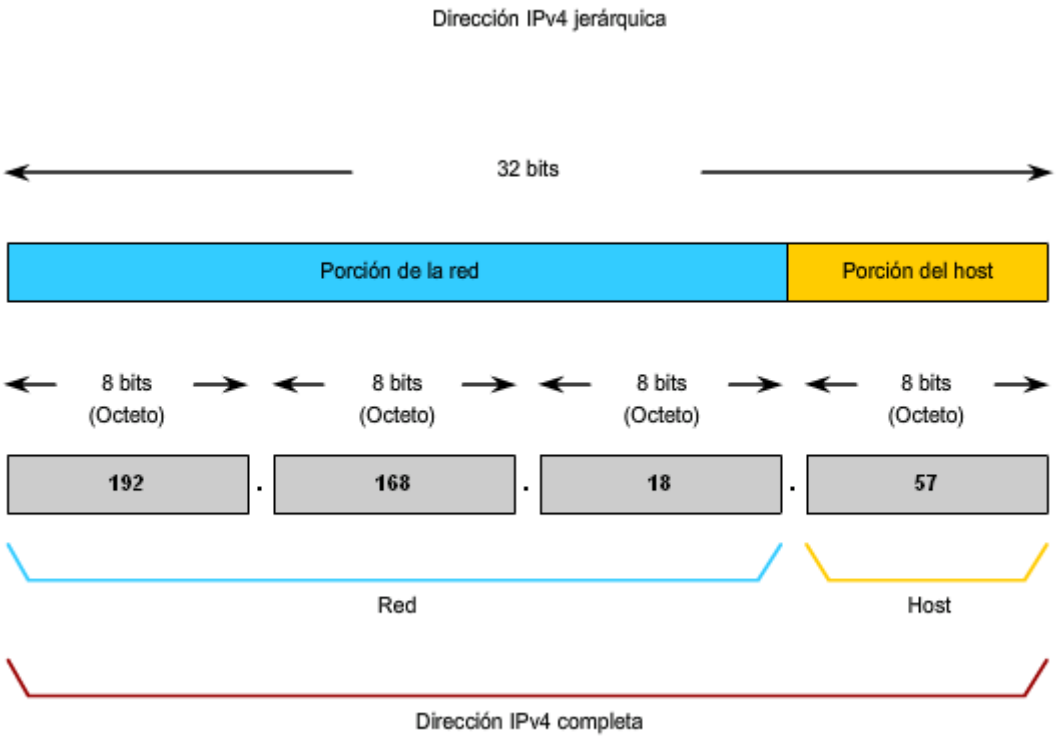
Al número de bits de una dirección utilizada como porción de red se lo denomina longitud del prefijo. Por ejemplo, si una red usa 24 bits para expresar la porción de red de una dirección, se dice que el prefijo es /24. En los dispositivos de una red IPv4, un número separado de 32 bits llamado máscara de subred indica el prefijo.

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.

Agencia de asignación de números por Internet

http://www.iana.org/



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 gateway hacia la otra red.

Como parte de su configuración, un host tiene una dirección de gateway por defecto definida. Como se muestra en la figura, esta dirección de gateway es la dirección de una interfaz de router que está conectada a la misma red que el host.

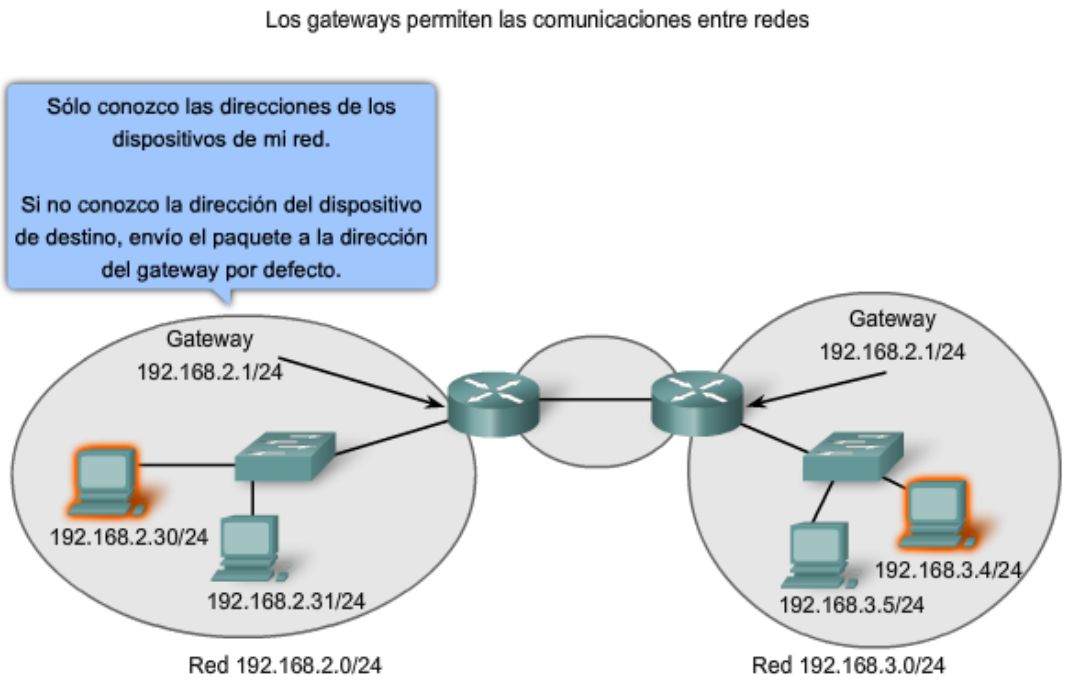
Tenga en claro que no es factible para un host particular conocer la dirección de todos los dispositivos en Internet con los cuales puede tener que comunicarse. Para comunicarse con un dispositivo en otra red, un host usa la dirección de este gateway, o gateway por defecto, para enviar un paquete fuera 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



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.

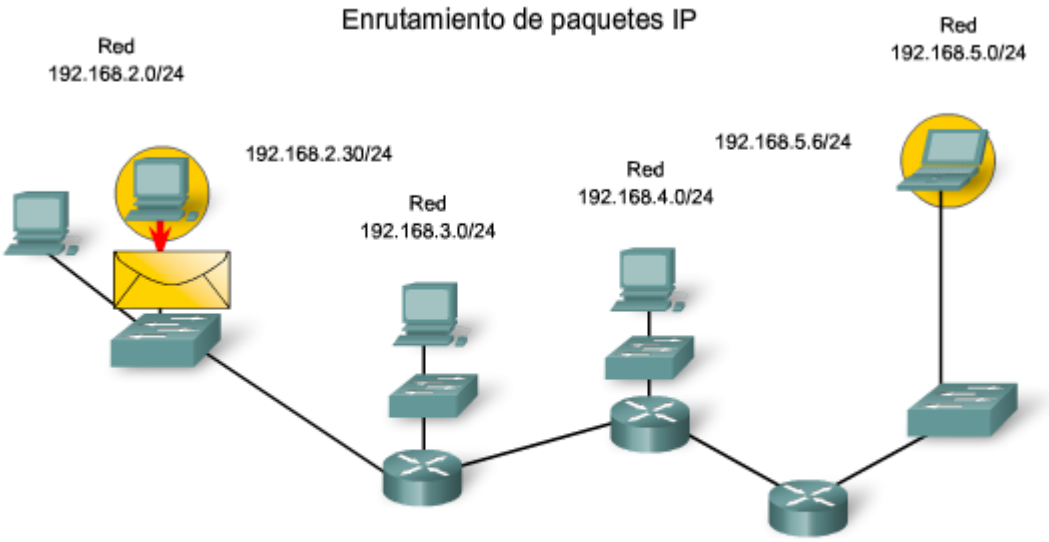
Sin embargo, si el host de destino y el host de origen no están en la misma red, el paquete puede llevar una PDU de la capa de Transporte a través de muchas redes y muchos routers. Si es así, la información que contiene no está alterada por ningún router cuando se toman las decisiones de envío.

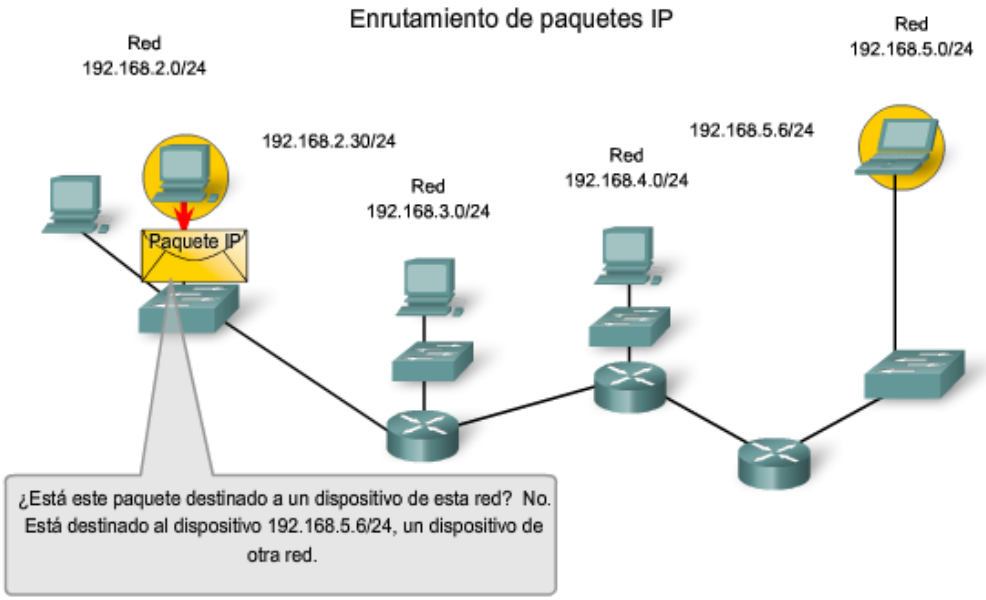
En cada salto, las decisiones de envío están basadas en la información del encabezado del paquete IP. El paquete con su encapsulación de capa de Red también se mantiene básicamente intacto a través de todo el proceso desde el host de origen hasta el host de destino.

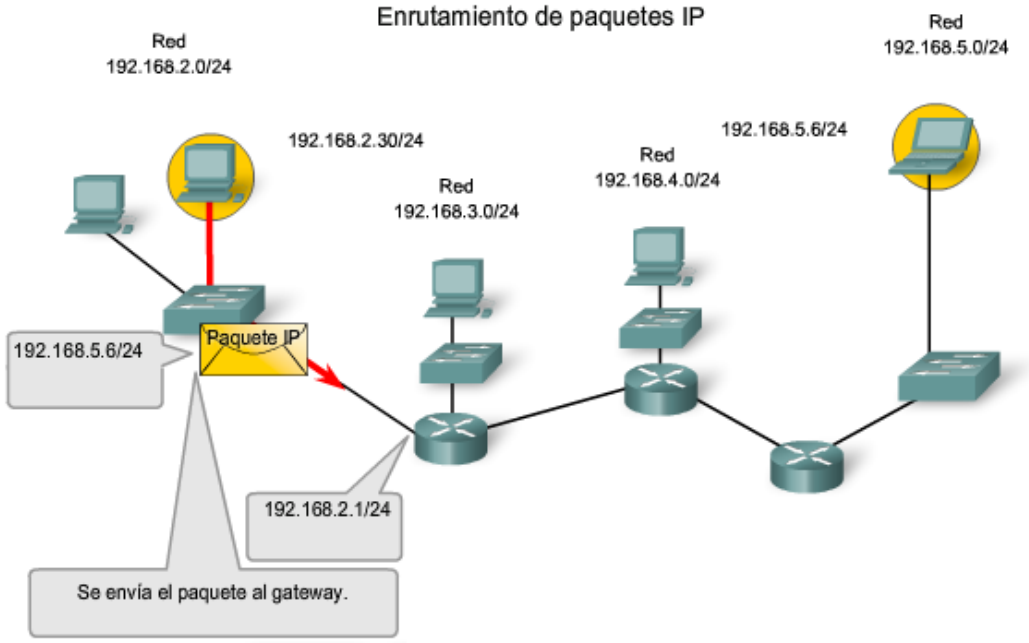
Si la comunicación se produce entre dos hosts de diferentes redes, la red local envía el paquete desde el origen hasta su router del gateway. El router examina la porción de la red de la dirección de destino del paquete y envía el paquete a la interfaz adecuada. Si la red de destino está conectado directamente a este router, el paquete es enviado

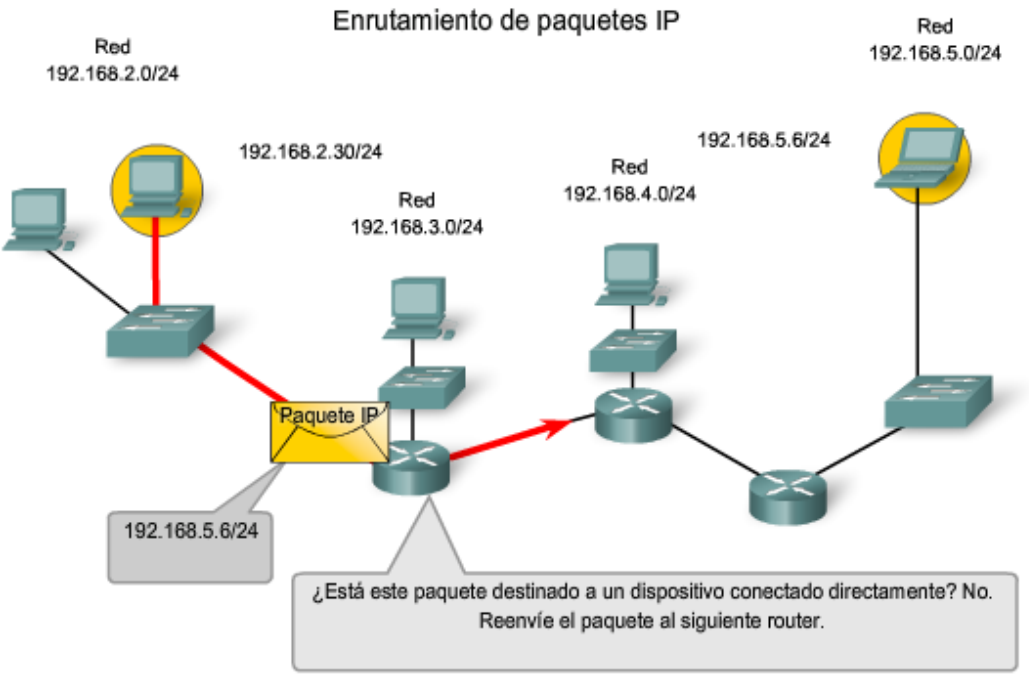
directamente a ese host. Si la red de destino no está conectada directamente, el paquete es enviado a un segundo router, que es el router del siguiente salto.

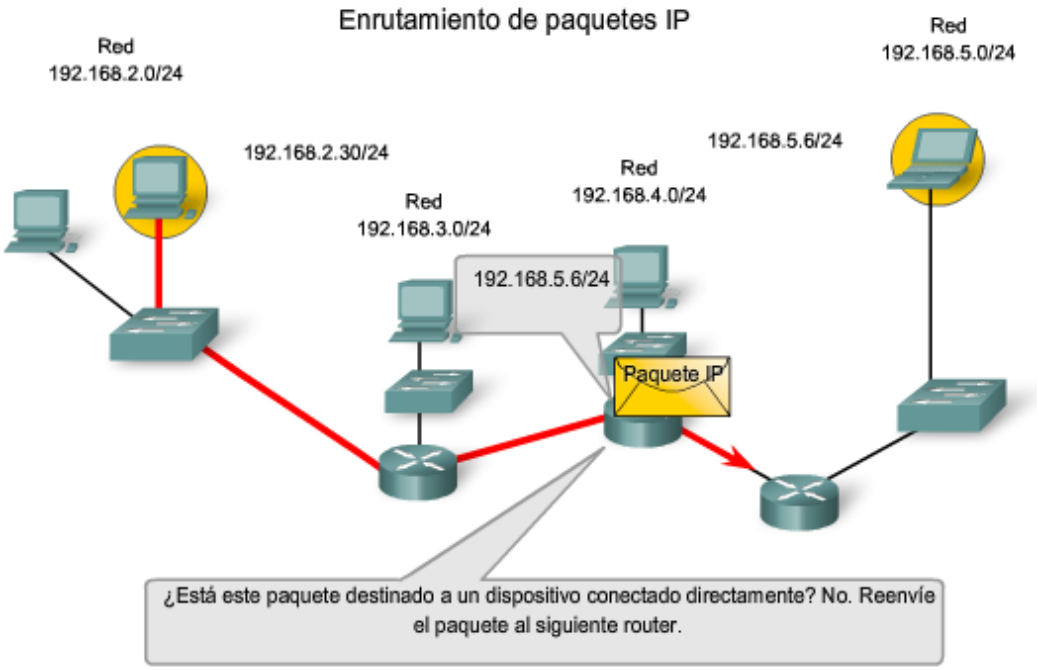
El paquete que se envía pasa a ser responsabilidad de este segundo router. Muchos routers o saltos a lo largo del camino puede procesar el paquete antes de llegar a destino.

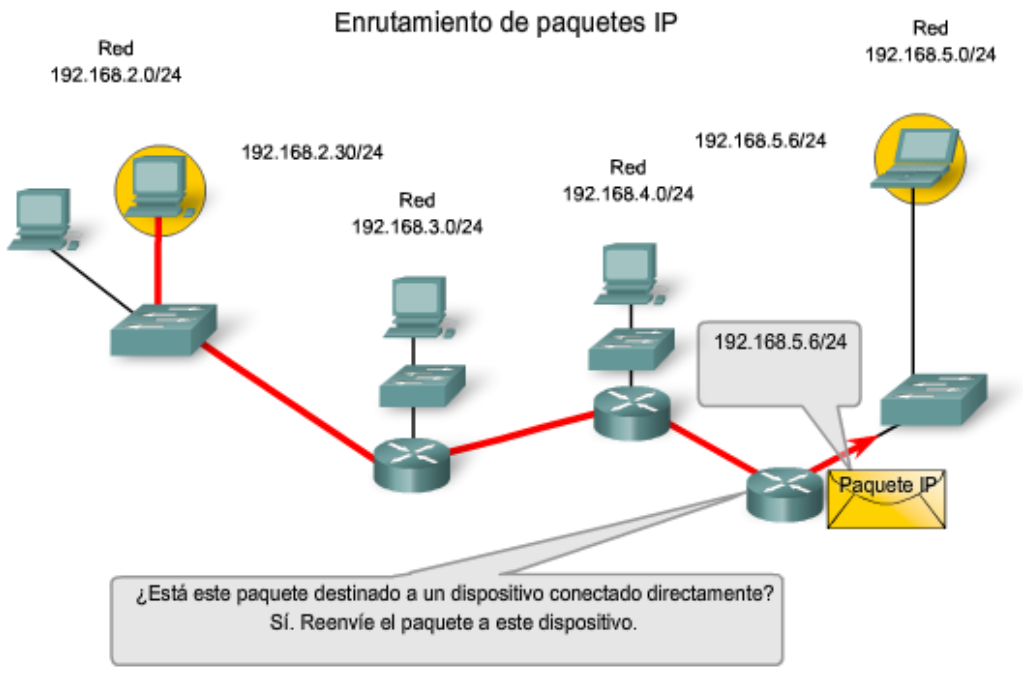


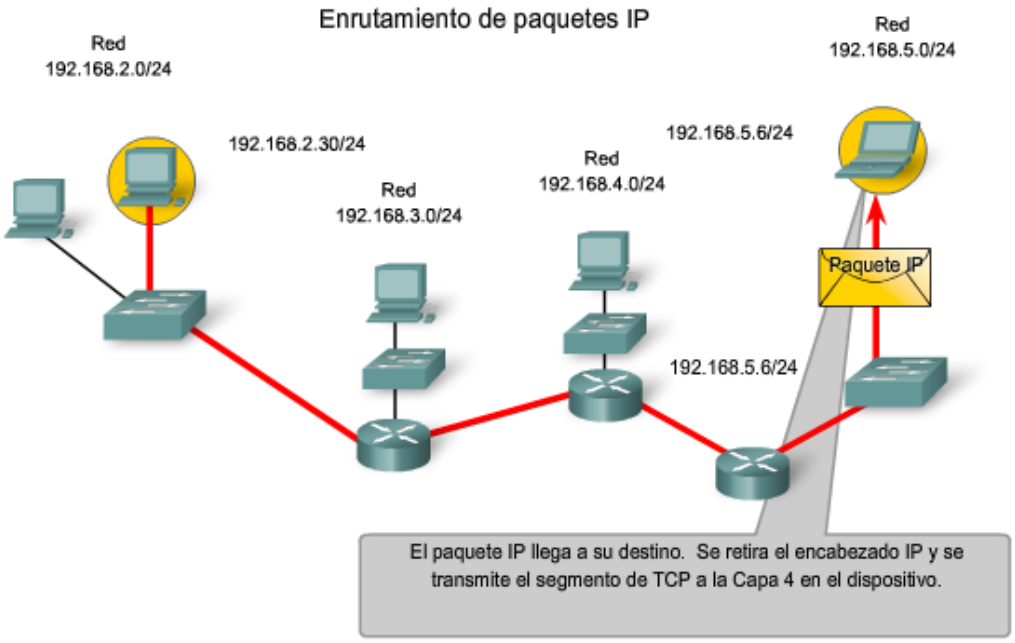



Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
192.168.5.6/24
Red
192.168.4.0/24
Red
192.168.3.0/24
Paquete IP
192.168.5.6/24
192.168.2.1/24
Se envía el paquete al gateway.


Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
192.168.5.6/24
Red
192.168.4.0/24
Red
192.168.3.0/24
Paquete IP
192.168.5.6/24
¿Está este paquete destinado a un dispositivo conectado directamente? No.
Reenvíe el paquete al siguiente router.


Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
192.168.5.6/24
Red
192.168.4.0/24
Red
192.168.3.0/24
192.168.5.6/24
Paquete IP
¿Está este paquete destinado a un dispositivo conectado directamente? No. Reenvíe el paquete al siguiente router.


Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
192.168.5.6/24
Red
192.168.4.0/24
Red
192.168.3.0/24
192.168.5.6/24
Paquete IP
¿Está este paquete destinado a un dispositivo conectado directamente?
Sí. Reenvíe el paquete a este dispositivo.



Enlaces:

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

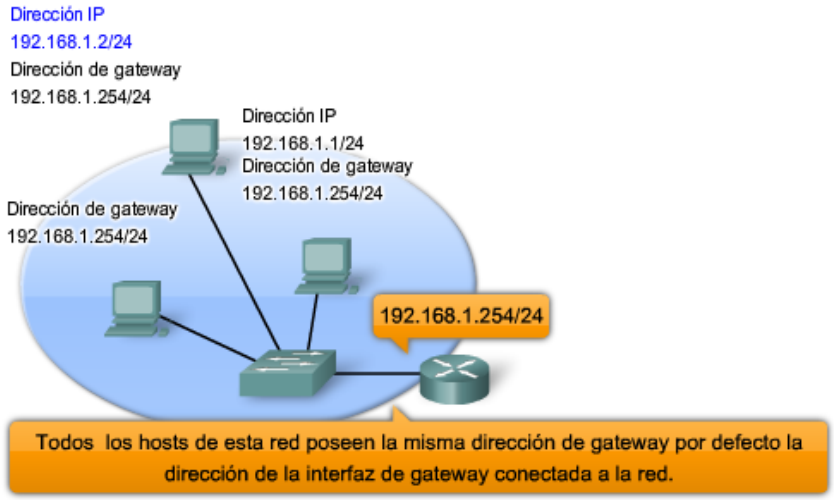
RFC 823 http://www.ietf.org/rfc/rfc0823.txt

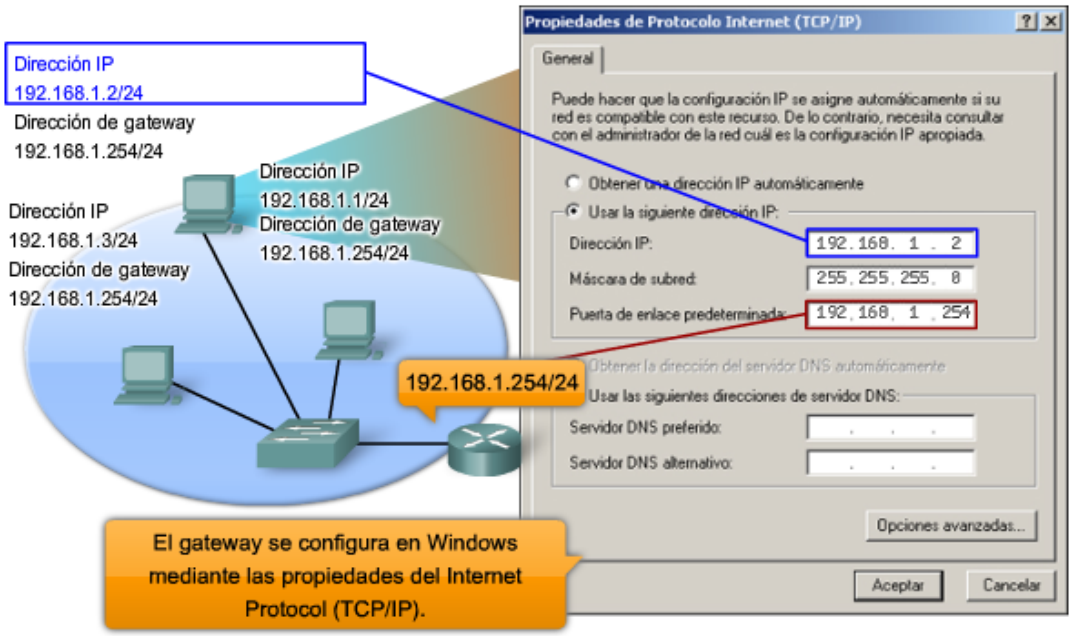
5.3.3 Gateway: La salida de nuestra red

El gateway, también conocido como gateway 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 gateway. Este gateway es una interfaz del router conectada a la red local. La interfaz del gateway 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 gateway.

Gateway por defecto

El gateway 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 gateway por defecto. Tanto la dirección IPv4 de host como la dirección de gateway deben tener la misma porción de red (y subred si se utiliza) de sus respectivas direcciones.



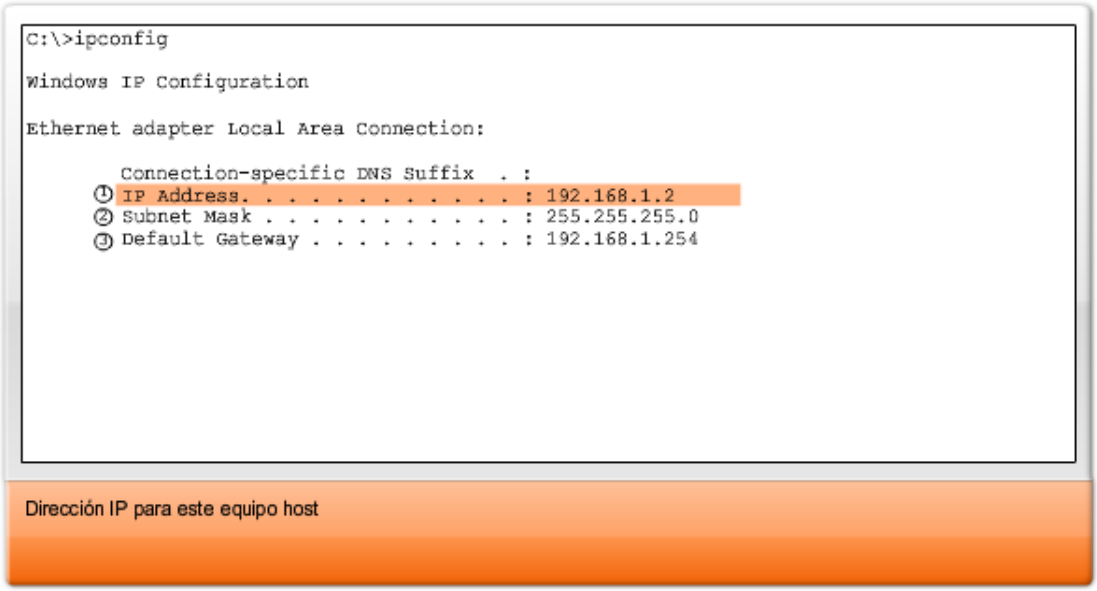


Configuración de la gateway del host
http://www.microsoft.com/technet/community/columns/cableguy/cg0903.mspx

Confirmación del gateway y la ruta

Como muestra la figura, la dirección IP desde el gateway 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.

Confirmación de la configuración del gateway



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.

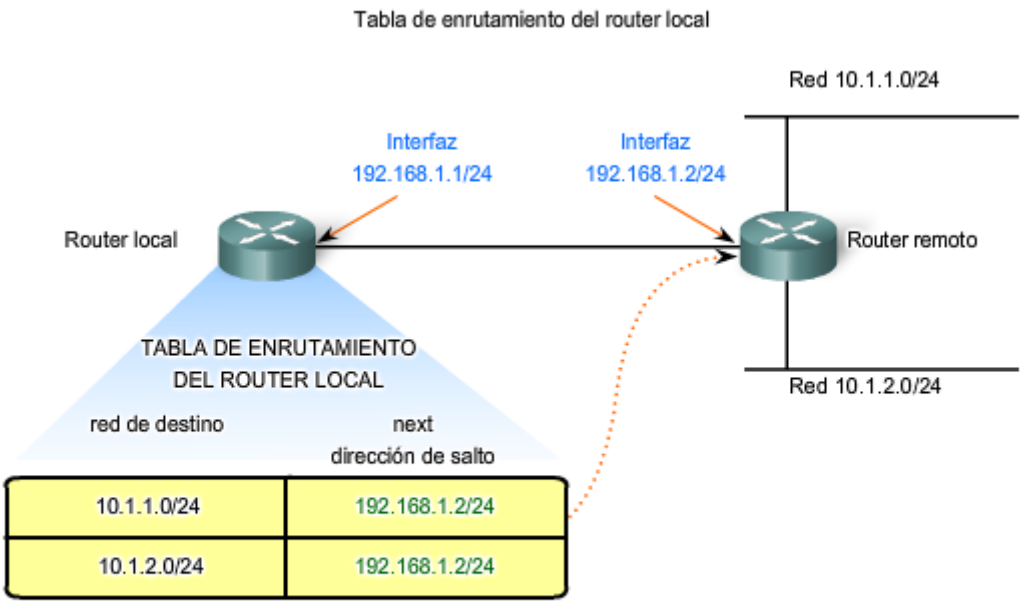
Un host debe reenviar el paquete ya sea al host en la red local o al gateway, según sea lo adecuado. Para reenviar los paquetes, el host debe tener rutas que representan estos destinos.

Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del gateway. 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 gateway. 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



El próximo salto para las redes 10.1.1.0/24 y 10.1.2.0/24 desde el router local es 192.168.1.2/24

5.3.4 Ruta: El camino hacia una red

Una ruta para paquetes para destinos remotos se agrega usando la dirección de gateway 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 está 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 adminitrador 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.

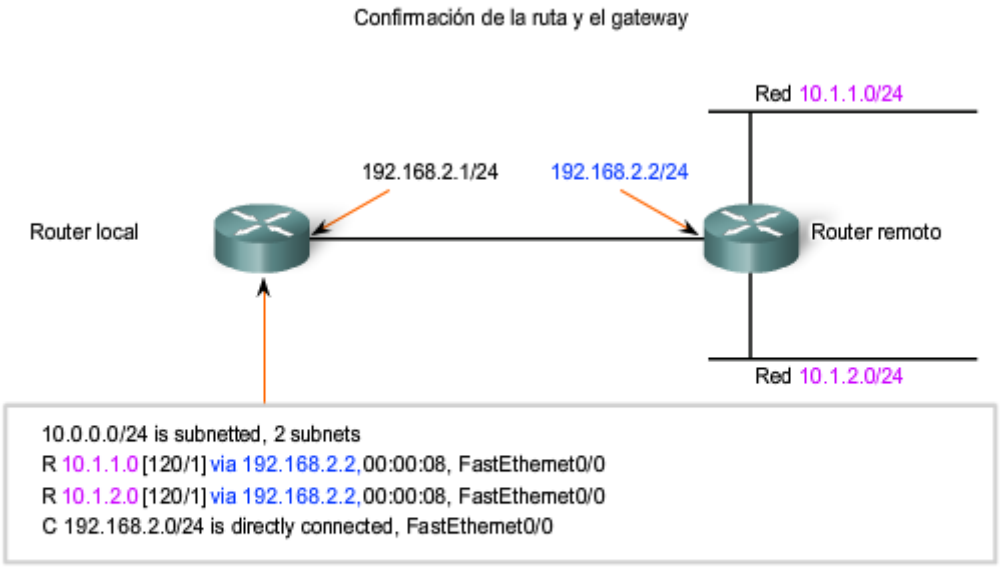
El router combina la dirección de destino en el encabezado del paquete con la red de destino de una ruta en la tabla de enrutamiento y envía el paquete al router del próximo

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.



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 gateway 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 gateway. La configuración de la dirección de gateway por defecto en el host crea la ruta default local.

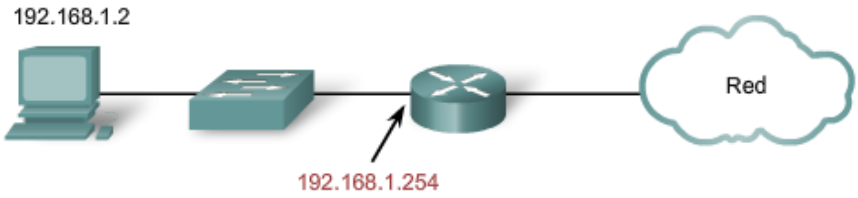
Como muestra la figura, la tabla de enrutamiento de un host de computadora puede ser analizada en la línea de comando introduciendo los comandos netstat -r, route, o route PRINT.

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




```
Interface List
0x2 ...00 0f fe 26 f7 7b ...  Gigabit Ethernet - Packet Scheduler Miniport
===========================================================================

Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.2      20
      192.168.1.0    255.255.255.0      192.168.1.2     192.168.1.2      20
Default Gateway:     192.168.1.254
// output omitted //
```

Éste es un ejemplo de la tabla de enrutamiento en un dispositivo final después de la emisión del comando netstat -r.
Observe que tiene una ruta hacia su red (192.168.1.0) y una ruta predeterminada (0.0.0.0) hacia el gateway del router para todas las demás redes.

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

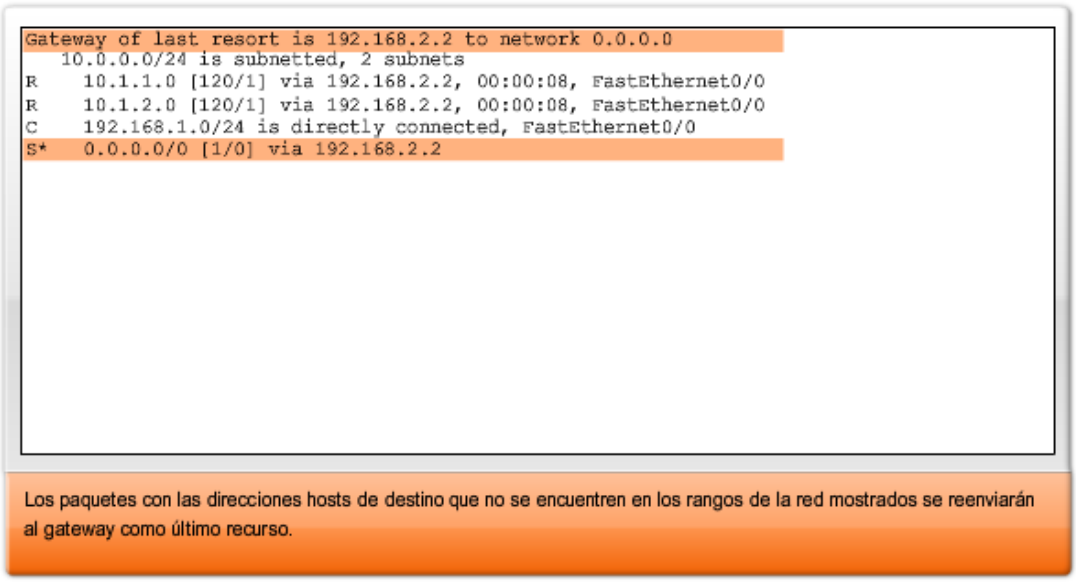
4. 0.0.0.0 (ruta default si estuviera configurada)

5. Descartada

Ruta default

Un router puede ser configurado para que tenga una ruta default. Una ruta default es una ruta que coincida 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.

La tabla de enrutamiento muestra la ruta predeterminada 0.0.0.0.



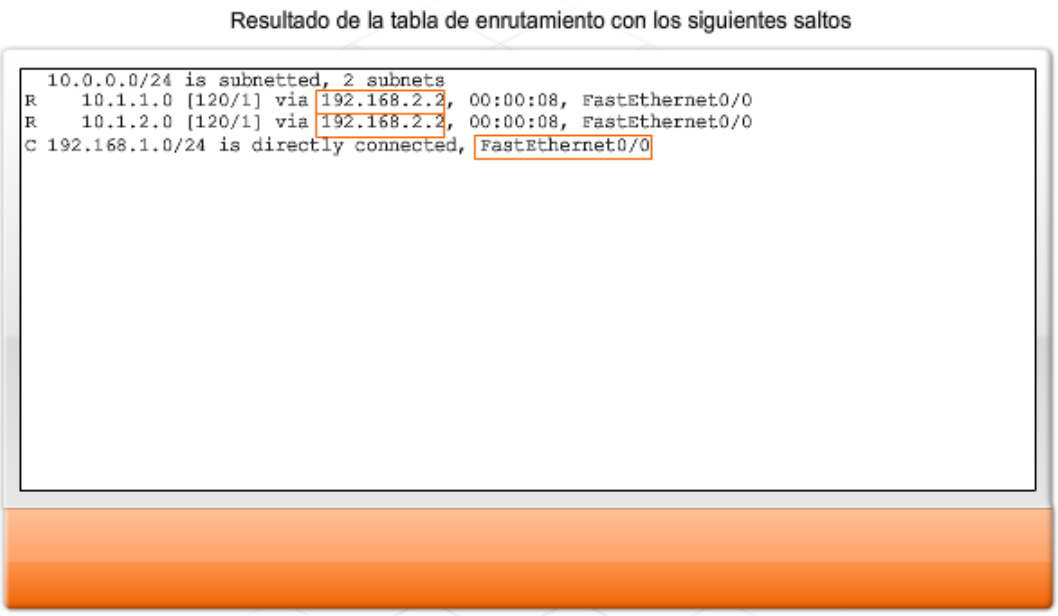
5.3.6 Siguiente salto: Dónde se envía luego el paquete

Un siguiente salto es la dirección del dispositivo que procesará luego el paquete. Para un host en una red, la dirección de gateway 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 gateway 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.



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

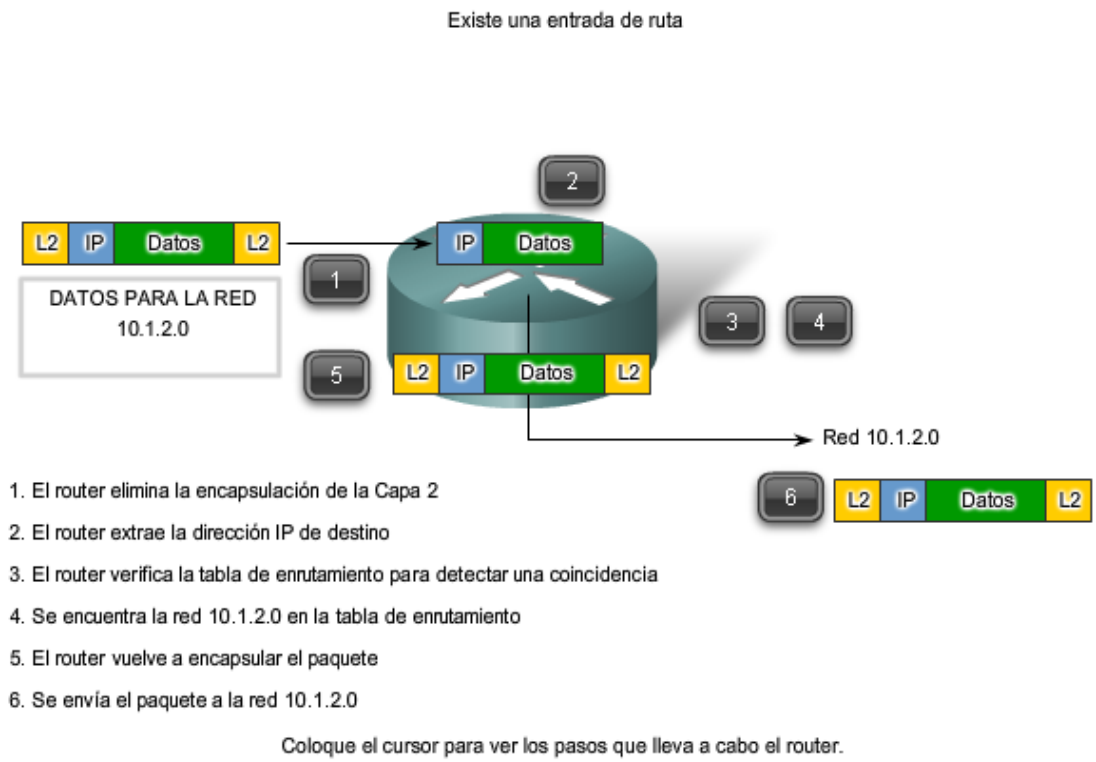
Examen del paquete

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.

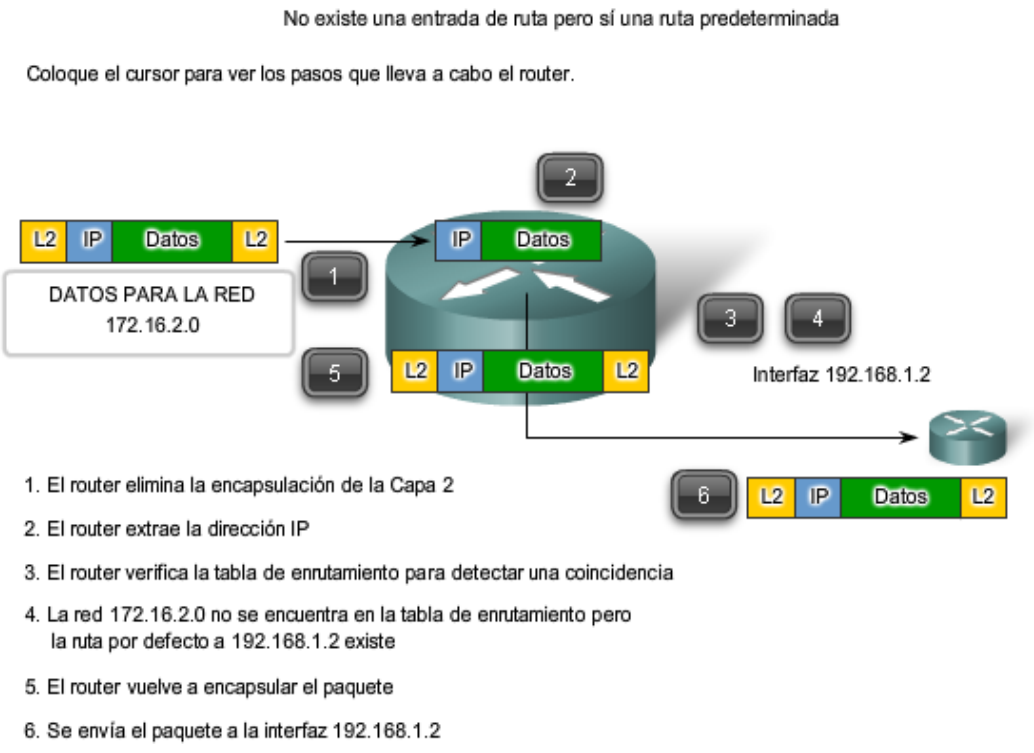


Uso de una ruta default

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*.

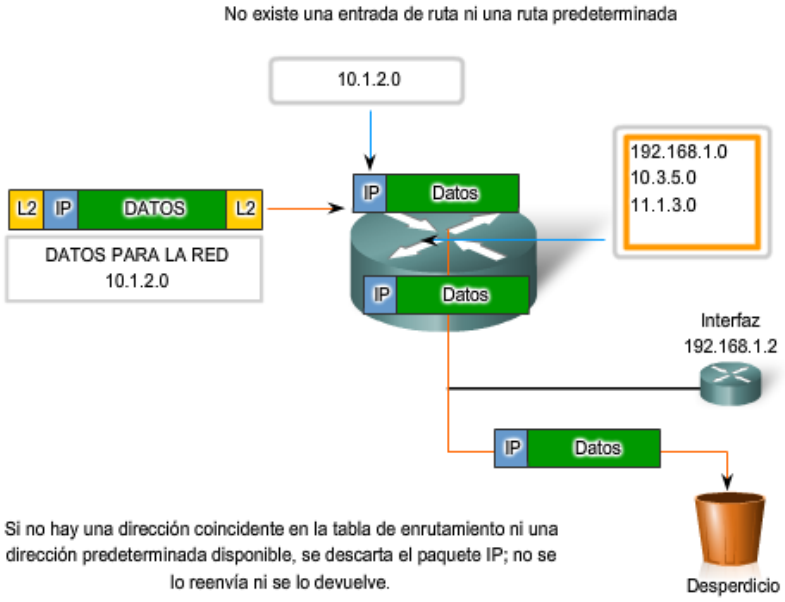
Este proceso puede producirse varias veces hasta que el paquete llega a su red de destino. El router en cada salto conoce sólo la dirección del siguiente salto; no conoce los detalles de la ruta hacia el host del destino remoto. Además, no todos los paquetes que van al mismo destino serán enviados hacia 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 gateway 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.



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.



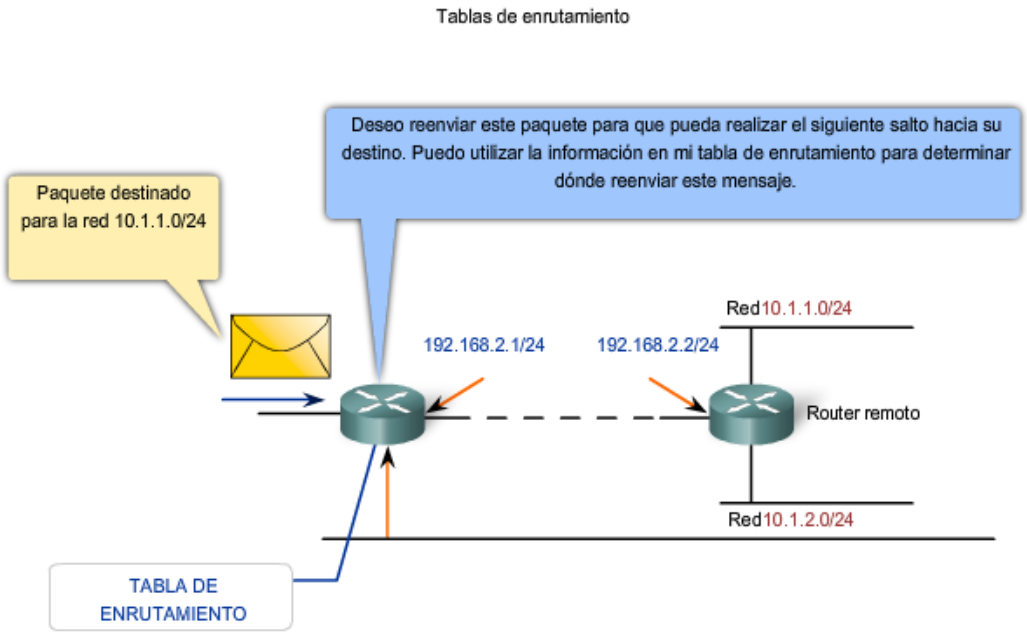
5.4 Procesos de enrutamiento: Cómo se aprenden las rutas

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.



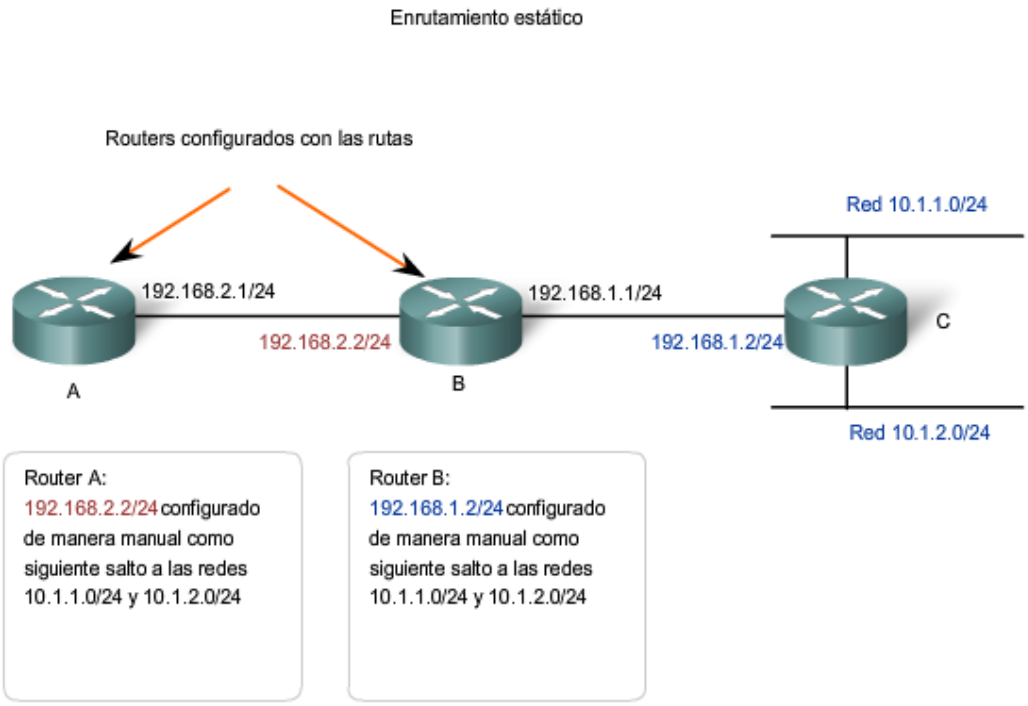
5.4.2 Enrutamiento estático

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.



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 gateway, 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 gateway 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 dinamicamente 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.