CAPA DE RED TCP/IP

IPv4

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
- Encapsulación
- Enrutamiento
- Desencapsulación

Direccionamiento: Primero, la capa de red debe proporcionar 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.

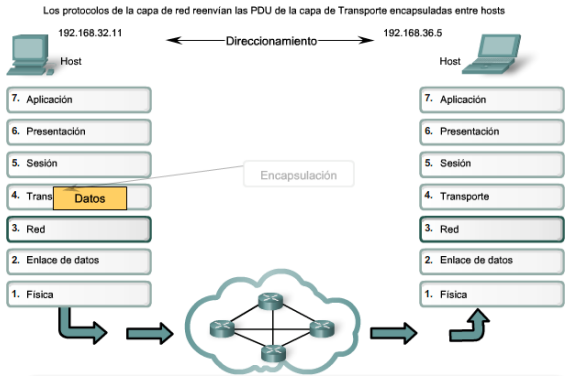
Encapsulación: Segundo, la capa de red debe proporcionar encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de 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 denomina dirección de origen. Después de que la capa de red completa el proceso de encapsulación, el paquete se envía a la capa de enlace de datos a fin de prepararse para el transporte a través de los medios.

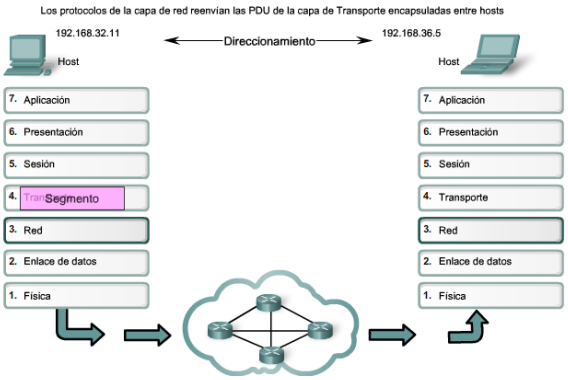
Enrutamiento: Luego, la capa de red debe proporcionar los servicios para dirigir estos paquetes a su host de destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser 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. Este proceso se conoce como enrutamiento.

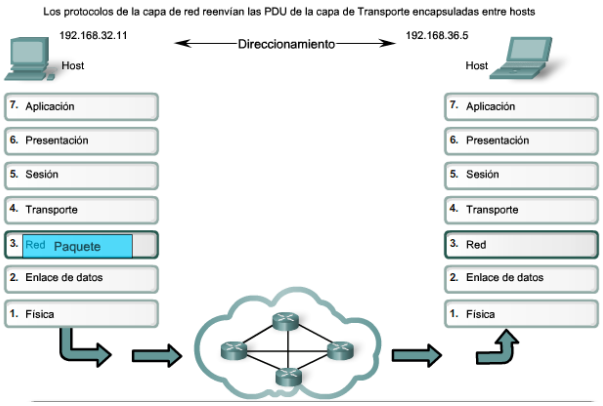
Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que se reenvía el paquete, su contenido (la unidad de datos del protocolo [PDU] de la capa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

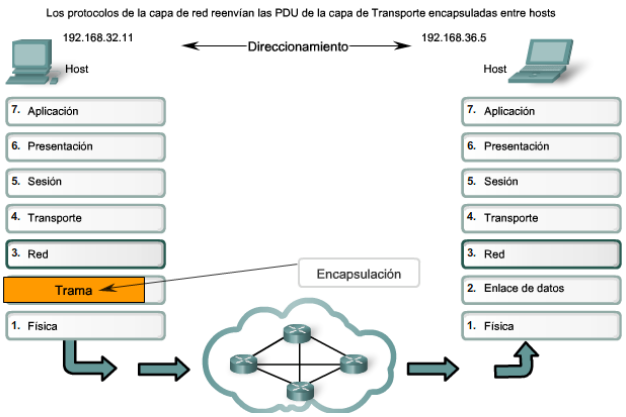
Desencapsulación: Finalmente, el paquete llega al host de destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a este dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

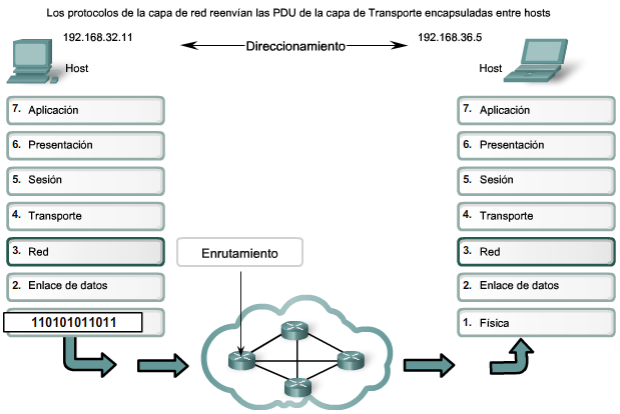
A diferencia de la capa de transporte (Capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host final, los protocolos de la capa de transporte especifican la estructura y el procesamiento del paquete utilizados para llevar los datos desde un host hasta otro host. Operar ignorando los datos de aplicación que se llevan en cada paquete permite a la capa de red llevar paquetes para múltiples tipos de comunicaciones entre diversos hosts.

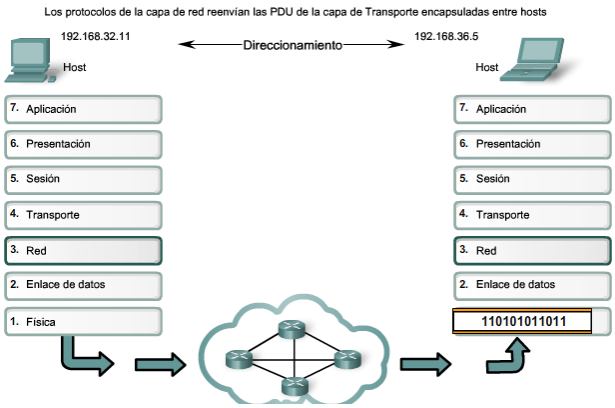


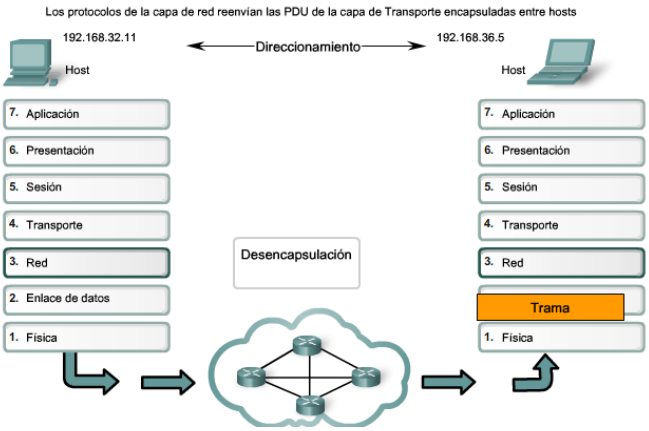


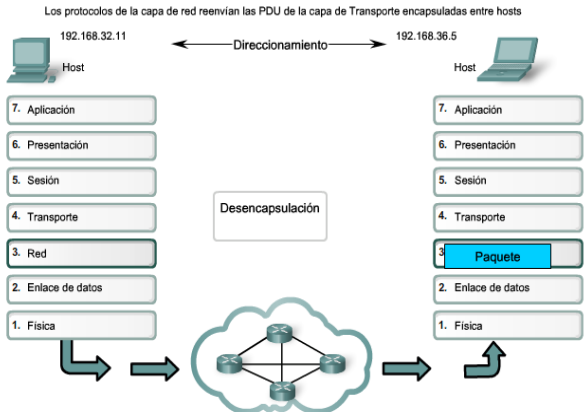


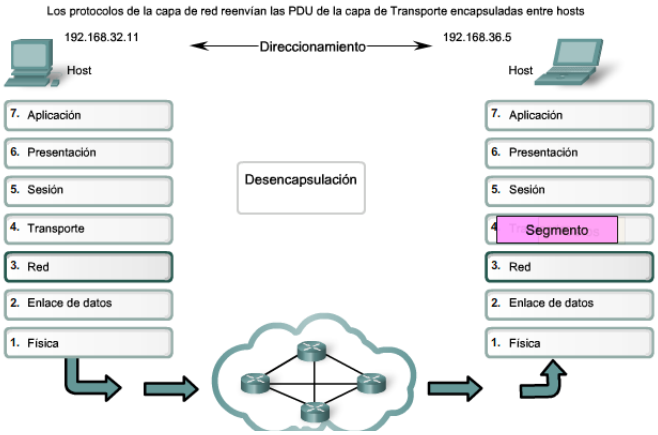


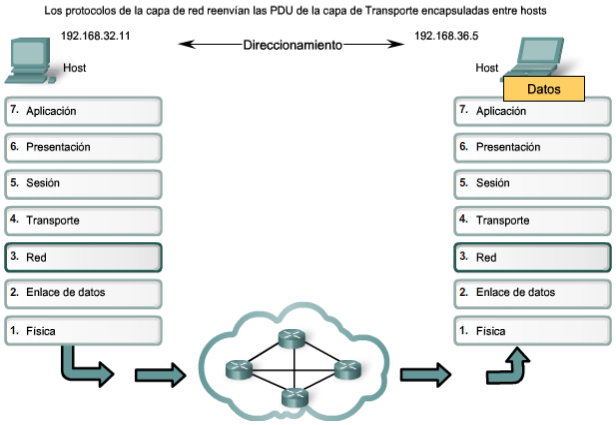










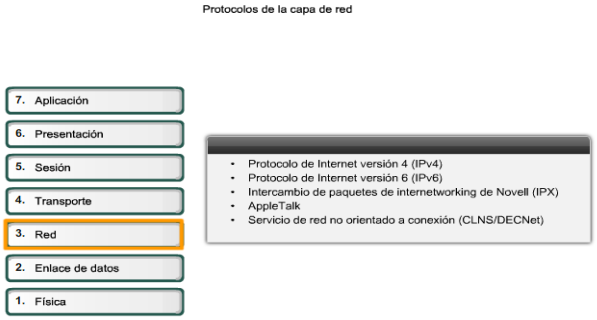


Protocolos de la capa de red:

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

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)
- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

El Protocolo de Internet (IPv4 e IPv6) es el protocolo de transporte de datos de la Capa 3 más ampliamente utilizado. Los demás protocolos no se analizarán en profundidad.



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 la suite 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.

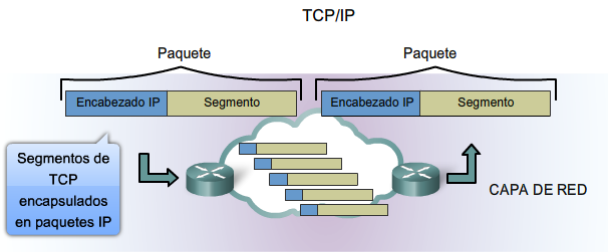
La versión 6 de IP (IPv6) está desarrollada y se implementa en algunas áreas. IPv6 operará junto con el IPv4 y puede reemplazarlo en el futuro. Los servicios provistos por IP, así como también la estructura y el contenido del encabezado de los paquetes están especificados tanto por el protocolo IPv4 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 de 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.
- Independiente de los medios: funciona sin importar los medios que transportan los datos.



Los paquetes IP fluyen a través de internetwork.

- 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.
- Independiente de los medios: funciona sin importar los medios que transportan los datos.

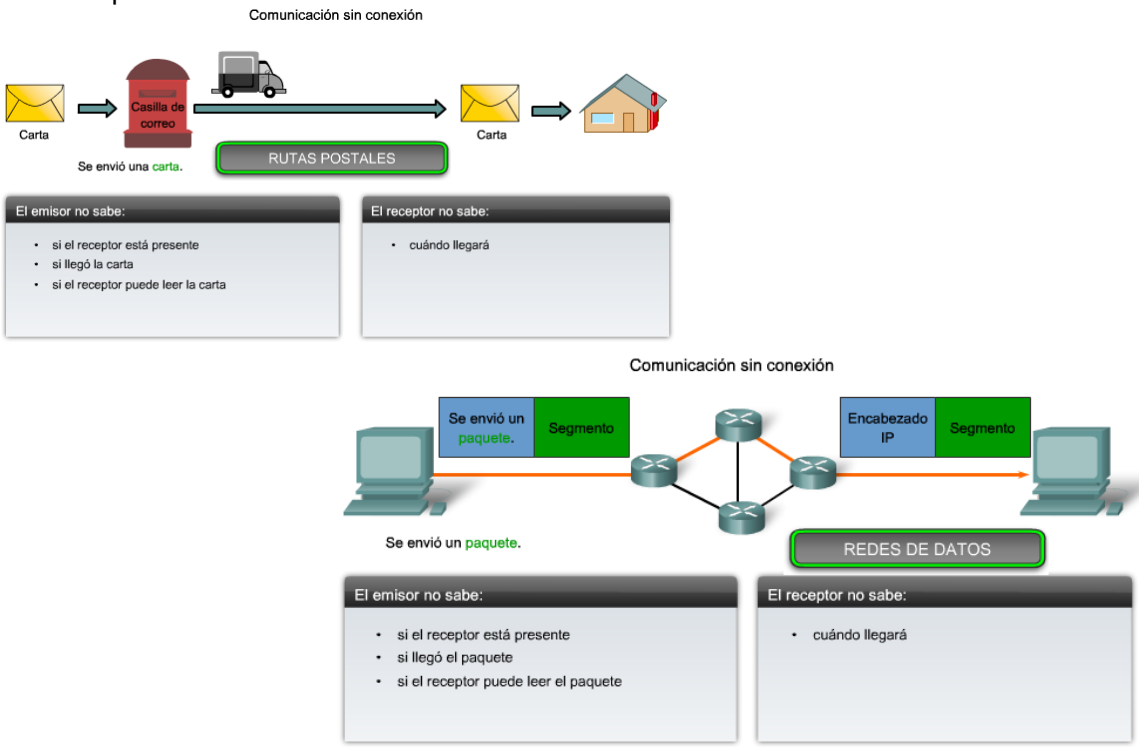
PROTOCOLO IPv4

Servicio sin conexión

Un ejemplo de comunicación sin conexión es enviar una carta a alguien sin notificar al destinatario 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 de datos de control 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 al 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.



PROTOCOLO IPv4

Servicio de mejor intento (no confiable)

El protocolo IP no sobrecarga el servicio IP proporcionando 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 se prefiere para un protocolo de Capa 3.

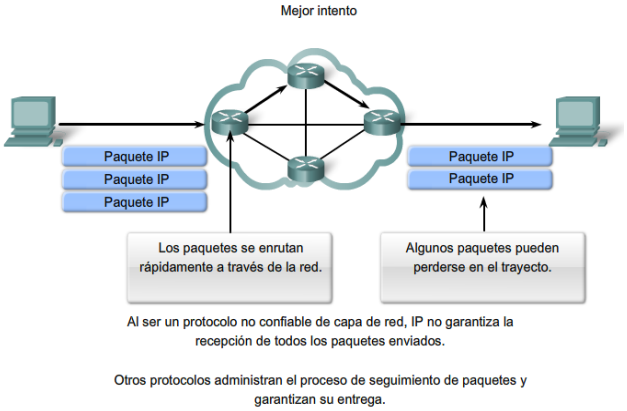
La función de la Capa 3 es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La Capa 3 no se ocupa de ni advierte el tipo de comunicación contenida dentro de un paquete. Esta responsabilidad es la función de las capas superiores a medida que se requieren.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

Se suele considerar que el IP es 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.



PROTOCOLO IPv4

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 señales de radio.

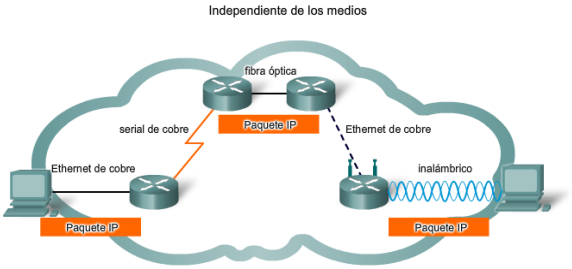
Es responsabilidad de la capa de enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

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 reenvía 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



Los paquetes IP pueden trasladarse a través de diferentes medios.

PAQUETE IPv4

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 IPv4 permanece en su lugar desde el momento en que el paquete abandona la capa de red del host de origen hasta que llega a la capa de red del host de destino.

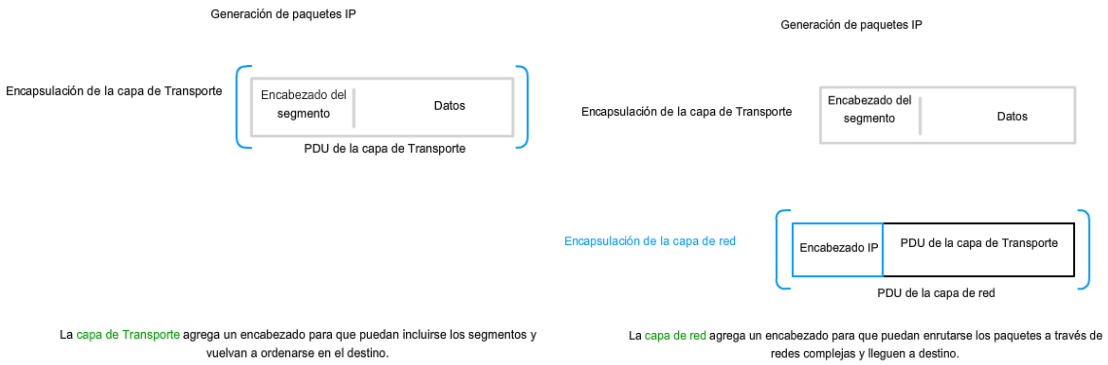
El proceso de encapsulación de datos por capas permite que los servicios en las diferentes capas se desarrollen y escalen sin afectar otras capas. Esto significa que los segmentos de la capa de transporte pueden ser empaquetados fácilmente por los protocolos de la capa de red existentes, como IPv4 e IPv6, o por cualquier protocolo nuevo que pueda desarrollarse en el futuro.

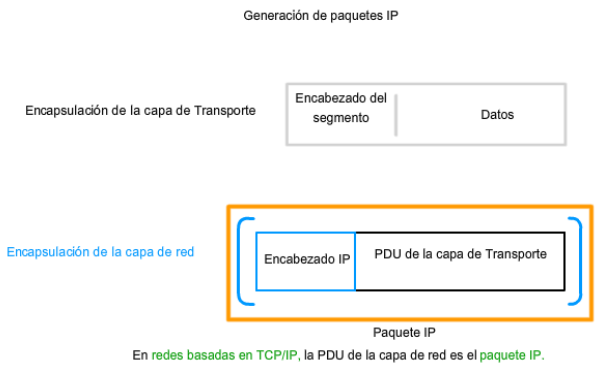
Los routers pueden implementar estos diferentes protocolos de la capa de red para operar concurrentemente en una red hacia y desde el mismo host u otro. El enrutamiento realizado por estos dispositivos intermediarios sólo considera el contenido del encabezado del paquete que encapsula el segmento.

En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada, se mantiene inalterable durante los procesos de la capa de red.

Enlaces

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





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 reenvían paquetes a través de la red.

Considere estos 6 campos clave:

- Dirección IP de origen
- Dirección IP de destino
- Tiempo de vida (TTL)
- Tipo de servicio (ToS)
- Protocolo
- Desplazamiento de fragmentos

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

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

Tiempo de vida: El campo Tiempo de vida (TTL) es un valor binario de 8 bits que indica el resto 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 reenviados indefinidamente entre los routers en un routing loop. Si se permitiera que los routing loops de enrutamiento continúen, la red se congestionaría con paquetes de datos que nunca llegarían a destino. La disminución del valor TTL en cada salto garantiza que éste finalmente llegue a cero y que el paquete con el campo TTL vencido se descartará.

Protocolo: Este valor binario de 8 bits indica el tipo de contenido que el paquete traslada. El campo 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
- 17 UDP

Tipo de servicio: El campo 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 aquéllos 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 tiene que fragmentar un paquete cuando lo reenvía 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 desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

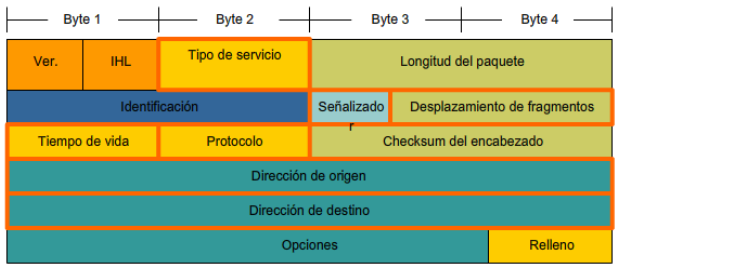
Señalizador de Más fragmentos: El señalizador de Más fragmentos (MF) es un único bit en el campo Señalizador usado con el desplazamiento de fragmentos para la fragmentación y reconstrucción de paquetes. Cuando está configurado el señalizador Más fragmentos, significa que no es el último fragmento de 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 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 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 Número de protocolo IP
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.

Tiempo 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

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 de origen

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.

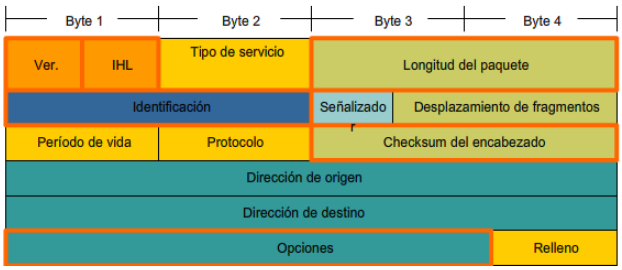
Dirección de destino

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 de encabezados

- **Versión**: contiene el número de la versión IP (4).
- **Longitud del encabezado (IHL):** especifica el tamaño del encabezado del paquete.
- **Longitud del paquete**: este campo muestra en bytes el tamaño completo del paquete, incluidos el encabezado y los datos.
- **Identificación**: este campo se utiliza principalmente para identificar únicamente los fragmentos de un paquete IP original.
- **Checksum del encabezado**: el campo Checksum se utiliza para controlar errores del encabezado del paquete.
- **Opciones**: existen medidas para campos adicionales en el encabezado IPv4 para proporcionar otros servicios pero éstos son rara vez utilizados.

Campos del encabezado de paquetes IPv4



IHL (Longitud del encabezado)

El tamaño del encabezado del paquete. Es necesario ya que el campo Opciones indica que el tamaño del encabezado puede variar y el protocolo necesita conocer el lugar donde finaliza el encabezado y donde comienzan los datos durante el procesamiento del paquete.

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

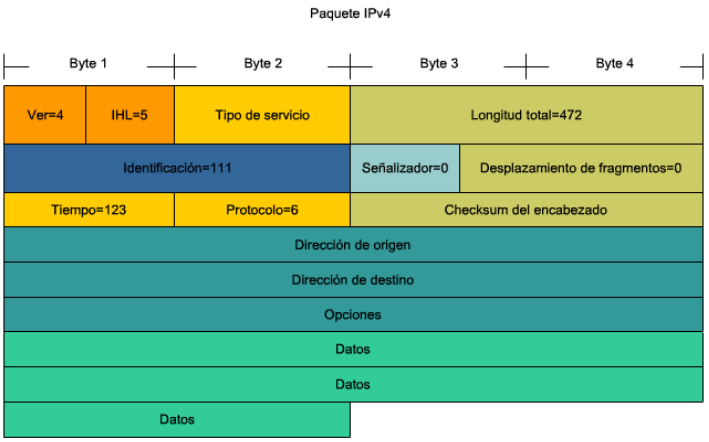
Se utiliza para la verificación de errores en el encabezado de paquetes. En cada salto, la checksum del encabezado debe compararse con el valor de este campo. Si el valor de la checksum del encabezado no coincide con la checksum calculada, el paquete se descartará. En cada salto, el campo TTL disminuye 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

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).
Tiempo 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 que lleva este paquete son un segmento TCP.



REDES: DIVISIÓN DE HOST EN GRUPOS

SEPARACIÓN DE HOSTS EN GRUPOS

Una de las principales funciones de la capa de red es proporcionar un mecanismo para direccionar hosts. A medida que crece la cantidad de hosts de la red, se requiere más planificación para administrar y direccionar la red.

División de redes

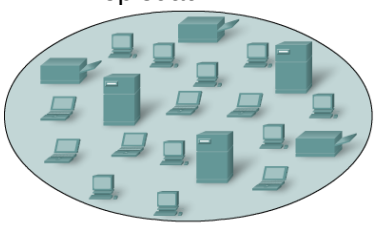
En lugar de tener todos los hosts conectados en cualquier parte a una vasta red global, es más práctico y manejable agrupar los hosts en redes específicas. Históricamente, las redes basadas en IP tienen su raíz como una red grande. Como esta red creció, también lo hicieron los temas relacionados con 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.

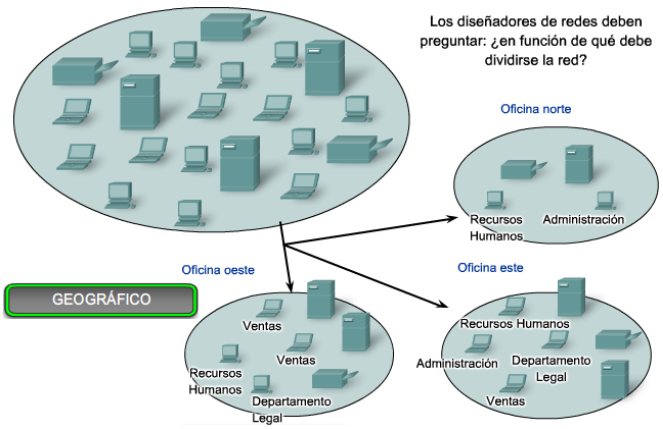
Red y subred son términos utilizados indistintamente para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP.

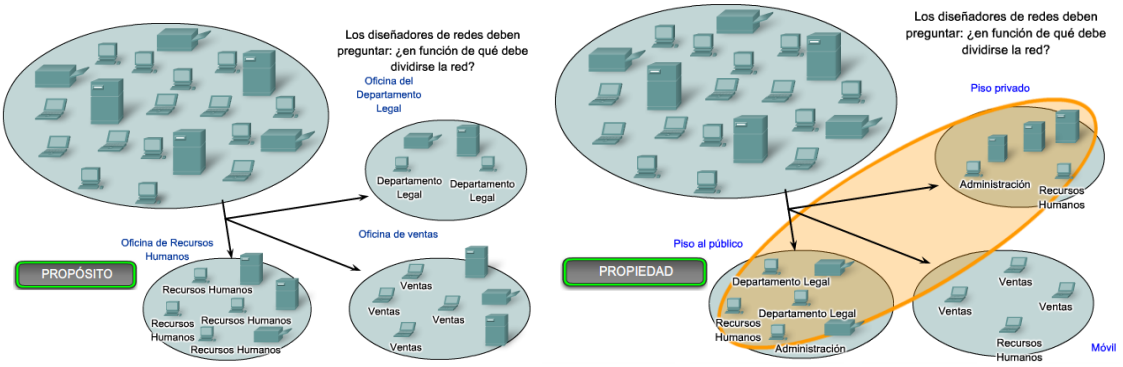
De manera similar, a medida que nuestras redes crecen, pueden volverse demasiado grandes para manejarlas como una única red. En ese punto, necesitamos dividir nuestra red. Cuando planeamos la división de la red, necesitamos agrupar aquellos hosts con factores comunes en la misma red.

Las redes pueden agruparse según factores que incluyen:

- Ubicación geográfica
- Propósito
- Propiedad





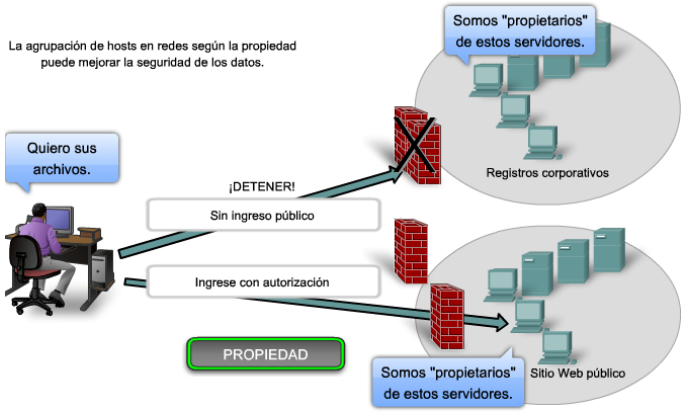


Agrupación de manera geográfica: Podemos agrupar hosts de redes geográficamente. El agrupamiento de hosts en la misma ubicación, como cada construcción en un campo o cada piso de un edificio de niveles múltiples, en redes separadas puede mejorar la administración y operación de la red.

Agrupación 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 esta situación, 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.



RENDIMIENTO: Como se mencionó anteriormente, a medida que las redes crecen, presentan problemas que pueden reducirse al menos parcialmente dividiendo la red en redes más pequeñas interconectadas.

Los problemas comunes con las redes grandes son:

- Degradación del rendimiento
- Problemas de seguridad
- Administración de direcciones

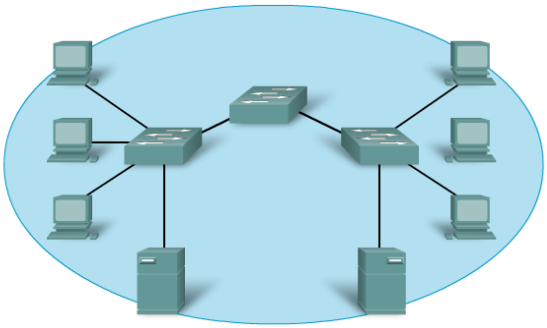
Mejora del rendimiento: Grandes cantidades de hosts conectados a una sola red pueden producir volúmenes de tráfico de datos que pueden extender, sin saturar, los recursos de red como la capacidad de ancho de banda y enrutamiento.

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

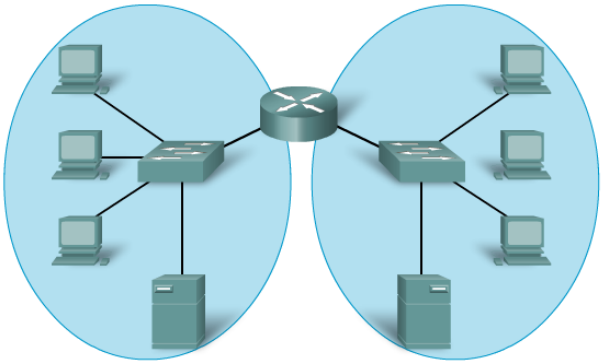
Además de las comunicaciones de datos reales entre los hosts, la administración de la red y el tráfico de control (sobrecarga) también aumentan con la cantidad de hosts. Los factores que contribuyen de manera significativa con esta sobrecarga pueden ser los broadcasts de red.

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 también se interrumpen o degradan.

Los broadcasts se contienen 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 de broadcast al dividir una red en subredes asegura que el rendimiento de la red y de los host no se degrade 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.

SEGURIDAD: La red basada en IP, que luego se convirtió en Internet, antiguamente tenía una pequeña cantidad 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.

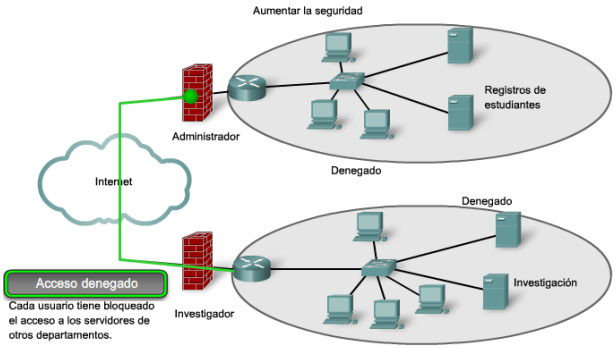
La situación ha cambiado porque las personas, las empresas y las organizaciones han desarrollado sus propias redes IP que se conectan a Internet. Los dispositivos, servicios, comunicaciones y datos son propiedad de esos dueños de redes. Los dispositivos de red de otras compañías y organizaciones no necesitan conectarse a su red.

La división de redes basada en la propiedad significa que el acceso a los recursos externos de cada red y desde estos pueden estar prohibidos, permitidos o monitoreados.

El acceso a internetwork dentro de una compañía u organización puede asegurarse 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.

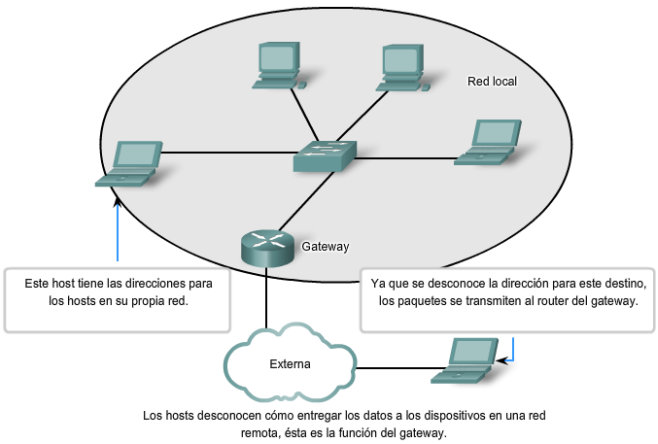
La seguridad entre redes se implementa en un dispositivo intermediario (router o firewall) en el perímetro de la red. La función del firewall que realiza este dispositivo permite que sólo datos conocidos y confiables accedan a la red.



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.



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 reenviar paquetes a través de internetworks, lo que permite que una red se divida según 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 jerárquicas de la capa de 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, se habrá utilizado la dirección de destino completa del host para entregar el paquete.

Si una red grande necesita dividirse 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.

DIVISIÓN 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 IPv4 lógica de 32 bits tiene una composición jerárquica y consta de 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 octeto se convierte a su valor decimal y la dirección completa se escribe como los cuatro valores decimales separados por punto (período).

Por ejemplo: 192.168.18.57

En este ejemplo, como se muestra en 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 se denomina direccionamiento jerárquico, debido a que la porción de red indica la red en la que cada dirección host única está ubicada. Los routers sólo necesitan conocer cómo llegar a cada red en lugar de conocer la ubicación de cada host individual.

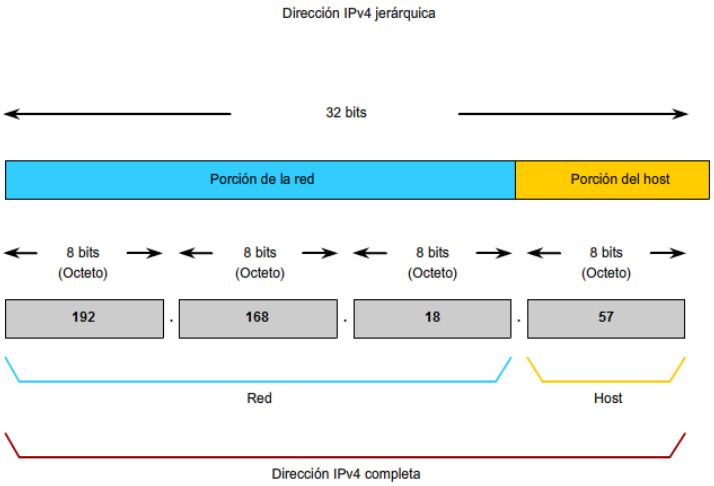
Con el direccionamiento jerárquico de IPv4, la porción de la red de la dirección para todos los hosts en una red es la misma. Para dividir una red, la porción de la red de la dirección es extendida para usar bits desde la porción del host de la dirección. Estos bits de host pedidos prestados luego se 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. Independientemente de la cantidad de subredes creada, se requiere que cada uno de los 32 bits identifique un host individual.

A la cantidad de bits de una dirección que se utiliza como porción de red se la denomina duración de 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 duración de 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.

Autoridad de números asignada por Internet
http://www.iana.org/

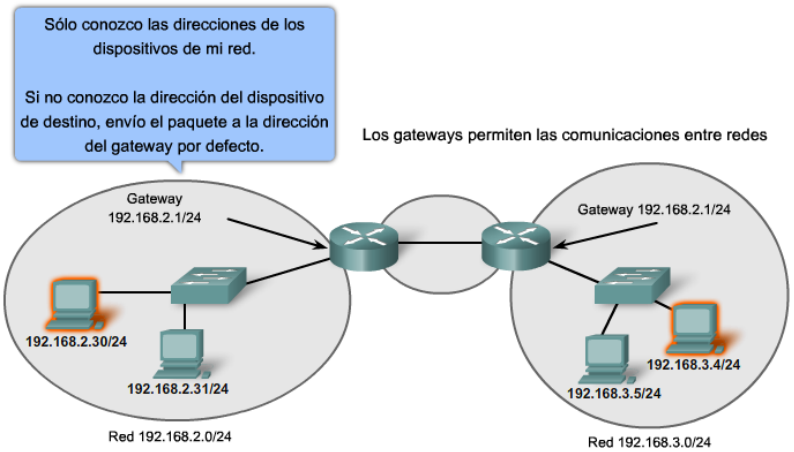


ENRUTAMIENTO

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 predeterminado 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 predeterminado, para reenviar un paquete fuera de la red local.

El router también necesita una ruta que defina dónde reenviar luego el paquete. A esto se lo denomina dirección del siguiente salto. Si el router cuenta con una ruta disponible, el router reenviará el paquete al router del siguiente salto que ofrezca una ruta hacia la red de destino.

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

PAQUETES IP:
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.

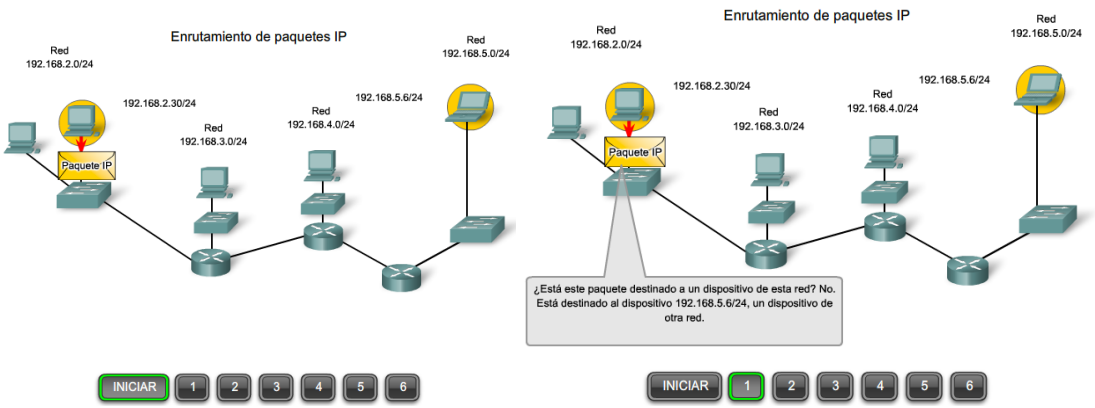
Sin embargo, si el host de destino y el host de origen no están en la misma red, el paquete puede llevar una PDU de la capa de transporte a través de muchas redes y muchos routers. Si es así, la información que contiene no está alterada por ningún router cuando se toman las decisiones de envío.

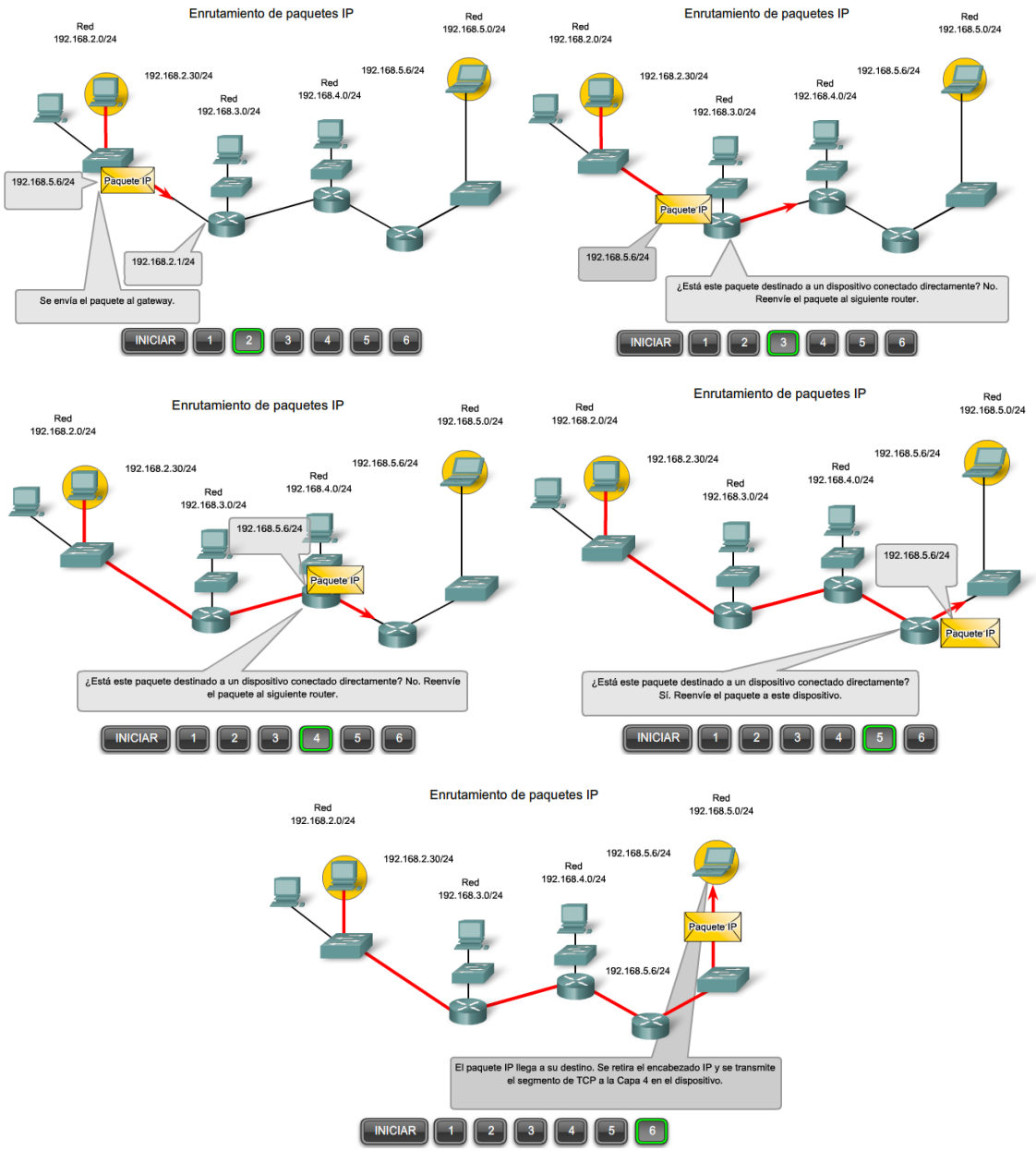
En cada salto, las decisiones de envío están basadas en la información del encabezado del paquete IP. El paquete con su encapsulación de capa de red también se mantiene básicamente intacto a través de todo el proceso desde el host de origen hasta el host de destino.

Si la comunicación se produce entre dos hosts de diferentes redes, la red local envía el paquete desde el origen hacia su router de 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 conectada directamente a este router, el paquete se reenvía 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 reenvía pasa a ser responsabilidad de este segundo router. Muchos routers o saltos a lo largo del camino pueden procesar el paquete antes de llegar al destino.

Enlaces:
RFC 791 http://www.ietf.org/rfc/rfc0791.txt
RFC 823 http://www.ietf.org/rfc/rfc0823.txt

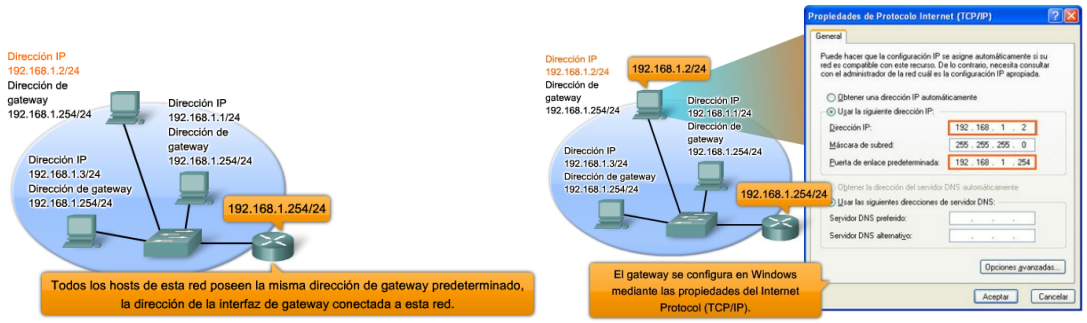




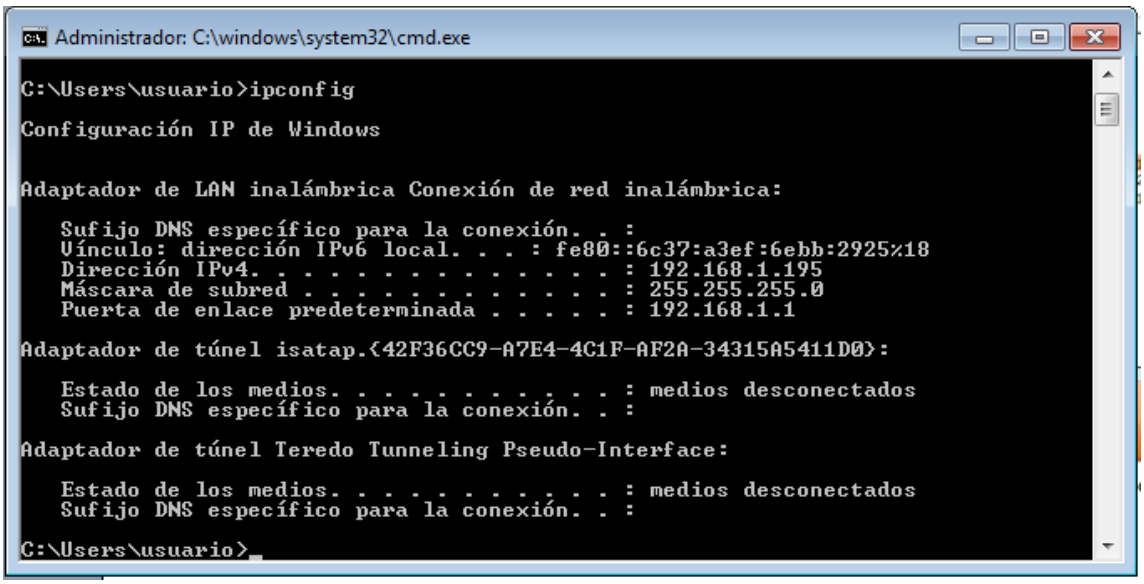
GATEWAY: El gateway, que también se conoce como gateway predeterminado, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host de origen, el paquete tiene que hallar la salida fuera de la red original. Para 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 la dirección como gateway.

Gateway predeterminado: El gateway predeterminado se configura en un 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 del gateway del host
http://www.microsoft.com/technet/community/columns/cableguy/cg0903.mspx



Confirmación del gateway y la ruta
Como se muestra en la figura, la dirección IP desde el gateway predeterminado de un host se puede ver introduciendo los comandos ipconfig o route print en la línea de comandos de un computadora con Windows. El comando route también se usa en un host Linux o UNIX.



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.

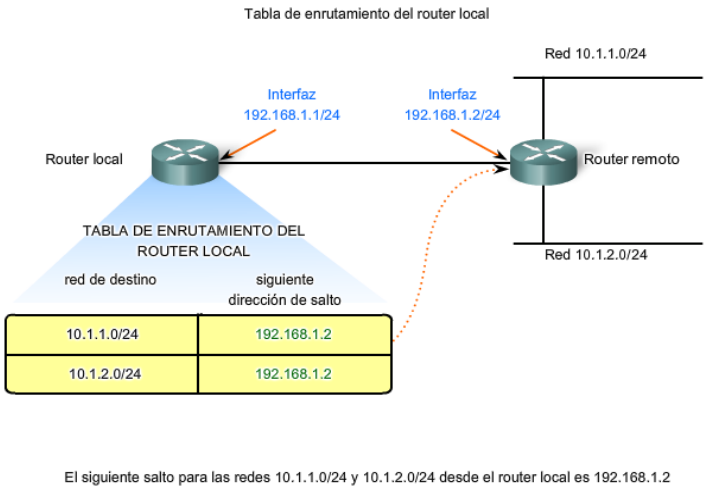
Un host debe reenviar el paquete ya sea al host en la red local o al gateway, según sea lo adecuado. Para reenviar los paquetes, el host debe tener rutas que representan estos destinos.

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 no existe una ruta a una red de destino, el paquete no puede reenviarse.

La red de destino puede ser una cantidad 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 siguiente salto y luego reenvía el paquete hacia esta dirección del siguiente salto.

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



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

RUTA: Una ruta para paquetes para destinos remotos se agrega usando la dirección de gateway predeterminado como el siguiente salto. Aunque usualmente no se hace, mediante las configuraciones se pueden agregar rutas manualmente a un host.

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 información sobre 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. El administrador de red puede configurar manualmente las rutas a estas redes en el router o bien pueden obtenerse automáticamente a través de protocolos de enrutamiento.

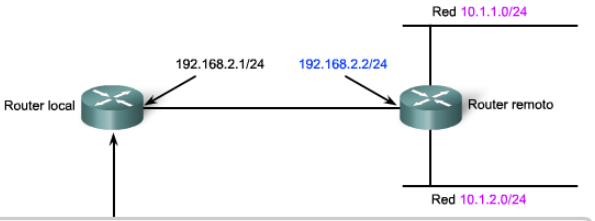
Los routers en una tabla de enrutamiento tienen tres características principales:

- Red de destino
- Siguiente salto
- Métrica

El router hace coincidir la dirección de destino del encabezado del paquete con la red de destino de una ruta en la tabla de enrutamiento y reenvía el paquete al router del siguiente salto que especifica dicha 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 puede ser analizada con el comando show ip route.

Confirmación de la ruta y el gateway




```
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 192.168.2.0/24 is directly connected, FastEthernet0/0
```

Éste es el resultado de la tabla de enrutamiento del router local cuando se emite "show ip route".

El siguiente salto para las redes 10.1.1.0/24 y 10.1.2.0/24 desde el router local es 192.168.2.2.

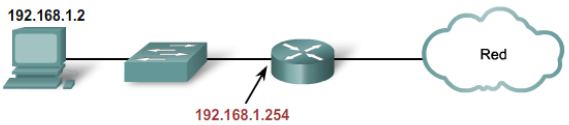
Como sabemos, el router no puede reenviar los paquetes sin una ruta. Si una ruta que representa la red de destino no está en la tabla de enrutamiento, el paquete será descartado (es decir, no se reenviará). La ruta encontrada puede ser una ruta conectada o una ruta hacia una red remota. El router también puede usar una ruta predeterminada para reenviar el paquete. La ruta predeterminada se usa cuando la ruta de destino no está representada por ninguna otra ruta en la tabla de enrutamiento.

Tabla de enrutamiento del host: Un host crea las rutas que se utilizan 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 predeterminado en el host crea la ruta predeterminada local.

Como se muestra en 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.




```
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
// se omite el resultado //
===========================================================================
```

Éste es un ejemplo de una 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.

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

RED DE DESTINO
Entradas de 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 host y, algunas veces, un rango de direcciones de red y 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.

Un paquete destinado a la subred de una red más grande se enrutaría usando la ruta a la subred. No obstante, un paquete direccionado a una subred diferente dentro de la misma red más grande se enrutaría 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:

- 10.1.1.0
- 10.1.0.0
- 10.0.0.0
- (ruta predeterminada si estuviera configurada)
- Descartada

Entradas de ruta en una tabla de enrutamiento

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 predeterminada: Un router puede configurarse para que tenga una ruta predeterminada. Una ruta predeterminada 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 predeterminada 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 se reenvían al router del siguiente salto asociado con la ruta predeterminada.

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

La tabla de enrutamiento muestra la ruta predeterminada 0.0.0.0.

SIGUIENTE SALTO: Un siguiente salto es la dirección del dispositivo que procesará luego el paquete. Para un host en una red, la dirección de gateway predeterminado (interfaz del router) es el siguiente salto para todos los paquetes destinados a otra red.

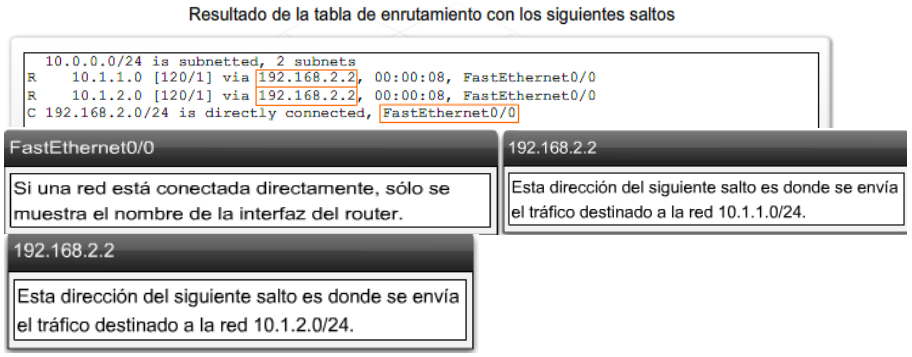
En la tabla de enrutamiento de un router, cada ruta enumera un siguiente salto para cada dirección de destino que abarca la ruta. A medida que cada paquete llega al router, la dirección de la red de destino es analizada y comparada con las rutas en la tabla de enrutamiento. Cuando se determina una ruta 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.

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

Resultado de la tabla de enrutamiento con los siguientes saltos



ENVIO DE PAQUETE: 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 examina la dirección IP de destino para cada paquete y luego verifica la tabla de enrutamiento para reenviar la información.

El router hará una de tres cosas con el paquete:

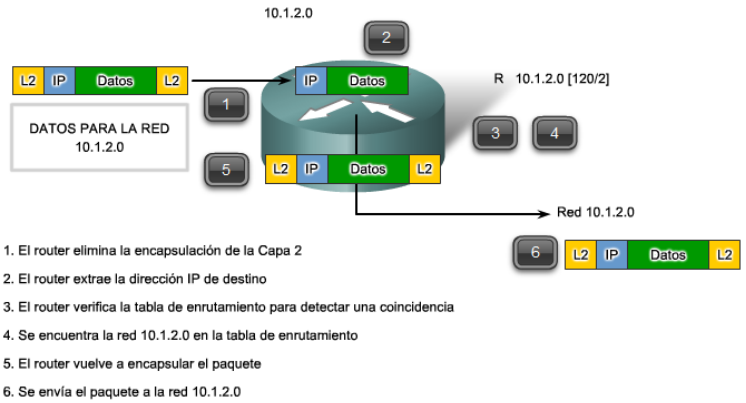
- Reenviarlo al router del siguiente salto

- Reenviarlo al host de destino
- Descartarlo

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 se muestra en 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 reenviarse hacia la interfaz.

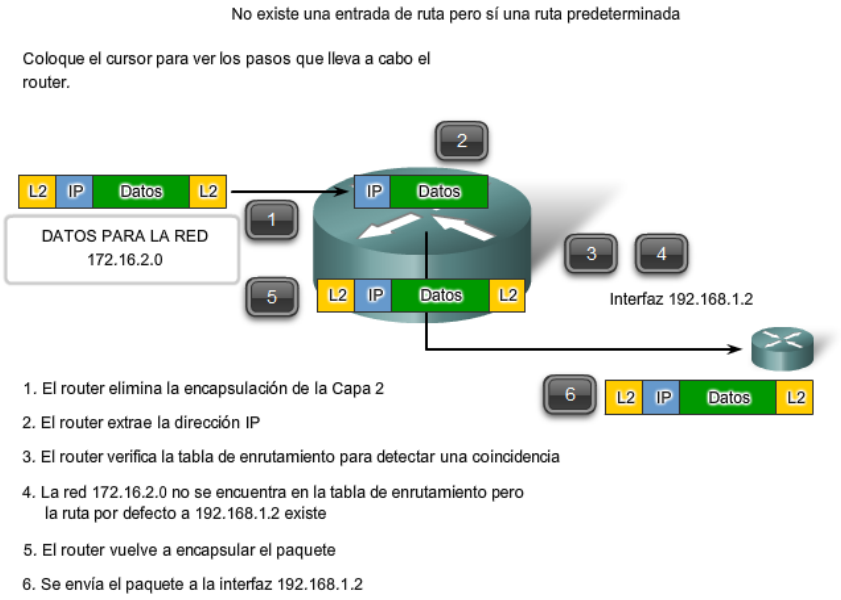
Si la ruta que coincide con la red de destino del paquete es una red remota, el paquete es reenviado a la interfaz indicada, encapsulado por el protocolo de la Capa 2 y enviado a la dirección del siguiente salto.



Uso de la ruta predeterminada: Como se muestra en 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 que indica la ruta predeterminada, 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 predeterminada se conoce también 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.

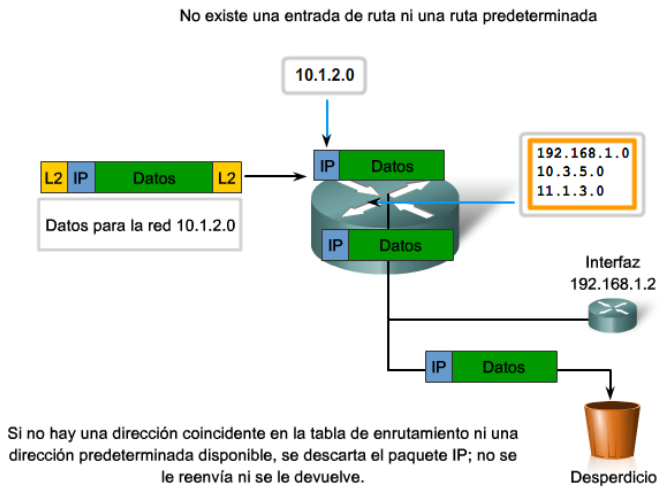
Las rutas predeterminadas son importantes porque el router del gateway no siempre tiene una ruta a cada red posible en Internet. Si el paquete es reenviado usando una ruta predeterminada, eventualmente llegará a un router que tiene una ruta específica a la red de destino. Este router puede ser el router 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 predeterminada, 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



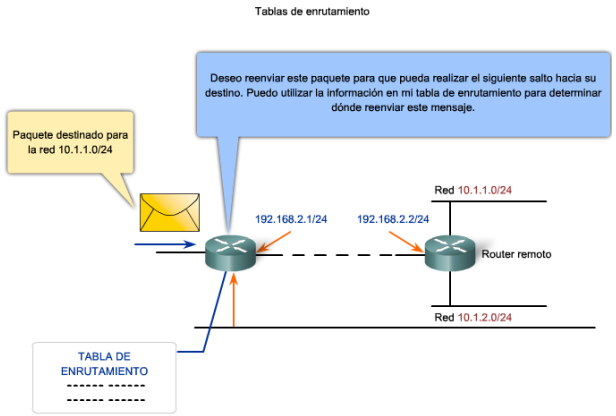
PROCESOS DE ENRUTAMIENTO

PROTOCOLOS DE ENRUTAMIENTO

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, lo que causa 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.

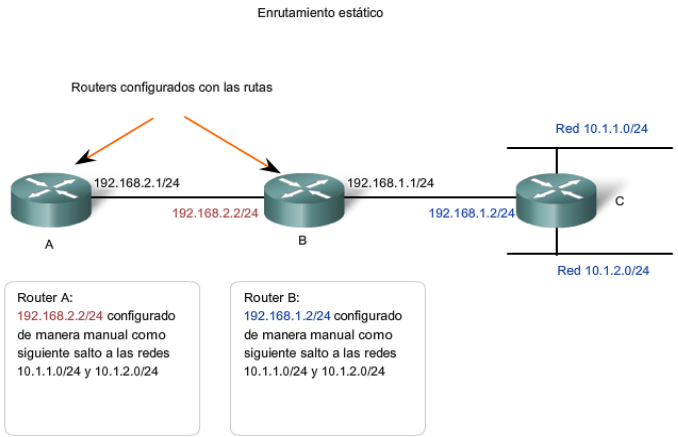


ENRUTAMIENTO ESTÁTICO

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 predeterminada también puede configurarse estáticamente.

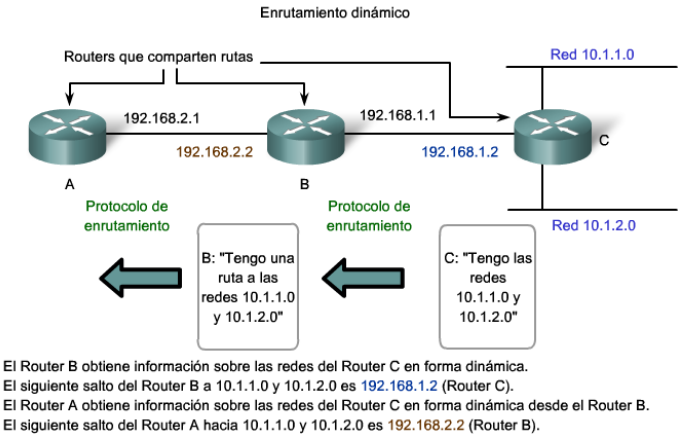
Si el router está conectado a otros routers, se requiere conocimiento de la estructura de internetworking. Para asegurarse de que los paquetes están enrutados para utilizar los mejores posibles siguientes saltos, cada red de destino necesita tener una ruta o una ruta predeterminada configurada. Debido a que los paquetes se reenvían 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, lo que causa demoras y posibles pérdidas de paquetes.



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 interno mejorado (EIGRP)
- Open Shortest Path First (OSPF)

Aunque los protocolos de enrutamiento proporcionan 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 en la red ni ubica entradas directamente 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 predeterminadas se usa para proporcionar las rutas necesarias.

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

Bibliografía:

- Apuntes teóricos de la Cátedra en distintos formatos.
- Cisco Systems: Academia de Networking de Cisco Systems: Guía del primer año. — 2ª ed. – Madrid: Pearson Educación, 2002. ISBN 8420532967
- Curso Cisco Systems: Academia de Networking de Cisco Systems – Verción 4.0
- Curso visual y práctico: Administrador de Redes Instalación y configuración de hardware y software. – USERS-CISCO.
- Stallings, William: Comunicación y Redes de Computadores / W. Stallings. – 7ª. – Madrid: Pearson Educación, 2004. ISBN 9788420541105

Preguntas de Reflexión

¿Qué realiza la capa de red en la pdu de la capa de transporte para que está pueda permitir la comunicación entre host? ¿Mencione la función del campo tiempo de vida en el encabezado del paquete ipv4 y señalizadores? ¿Enumere y explique las característica, funcionalidad de IP? ¿Explique como esta formada un dirección lógica? ¿Describa la funcionalidad de la tabla de enrutamiento y como está constituida? ¿Menciones que acciones, decisiones puede tomar un router con un paquete?