En este capítulo, aprendió a:

- Explicar la necesidad de la capa de Transporte
- Identificar la función de la capa de Transporte que ofrece la transferencia de datos de extremo a extremo entre las aplicaciones
- Describir la función de los dos protocolos de la capa de Transporte TCP/IP, TCP y UDP
- Explicar las principales funciones de la capa de Transporte que incluyen la confiabilidad, el direccionamiento de puertos y la segmentación
- Explicar la manera en que TCP y UDP manejan dichas funciones principales
- Identificar el momento apropiado para utilizar TCP o UDP y suministrar ejemplos de aplicaciones que utilizan cada protocolo

CAPITULO 5 Capa de red de OSI

5.0 Introducción del capitulo
5.0.1 Introduccion del capitulo

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

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

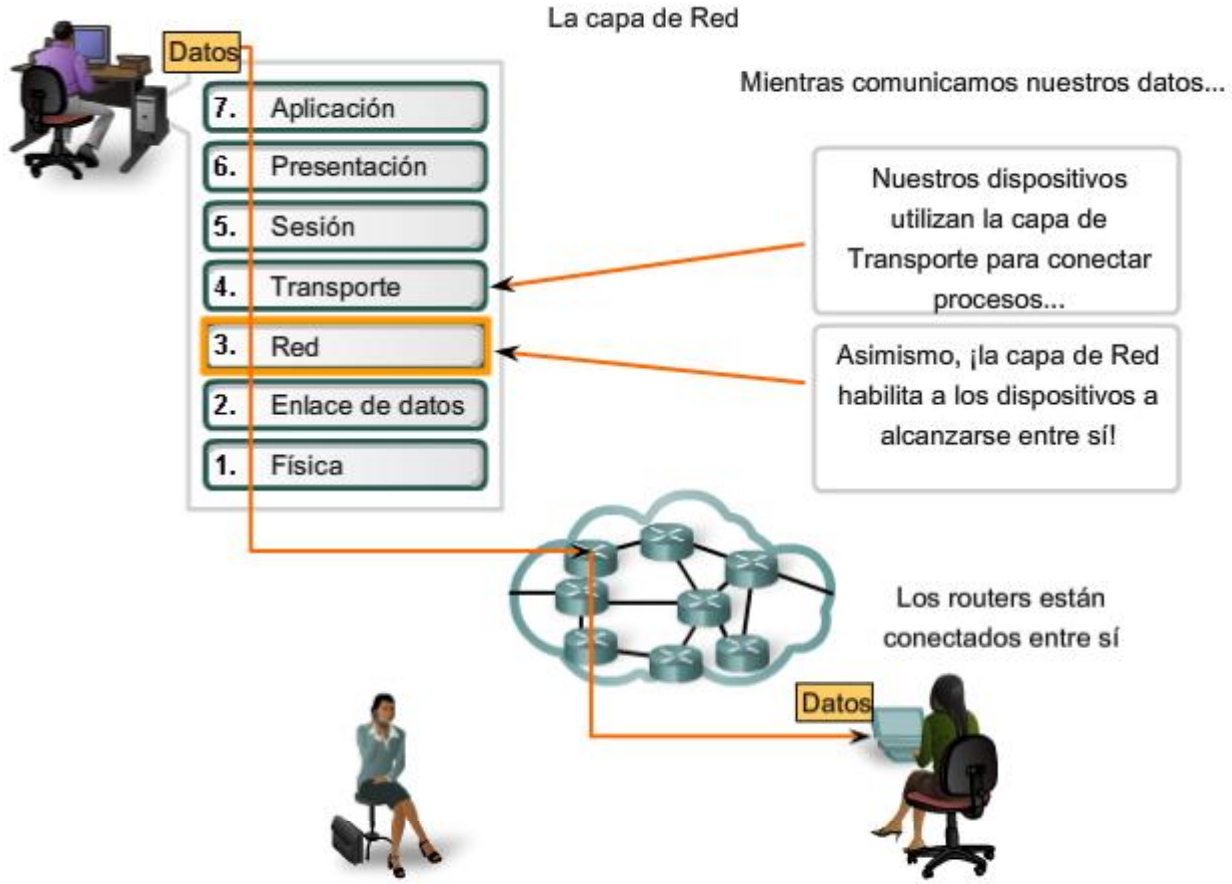
Los protocolos de la capa de Red del modelo OSI especifican el direccionamiento y los procesos que permiten que los datos de la capa de Transporte sean empaquetados y transportados. La encapsulación de la capa de Red permite que su contenido pase al destino dentro de una red o sobre otra red con una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

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

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

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



5.1 IPv4
5.1.1 Capa de Red: comunicación de host a host

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

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

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

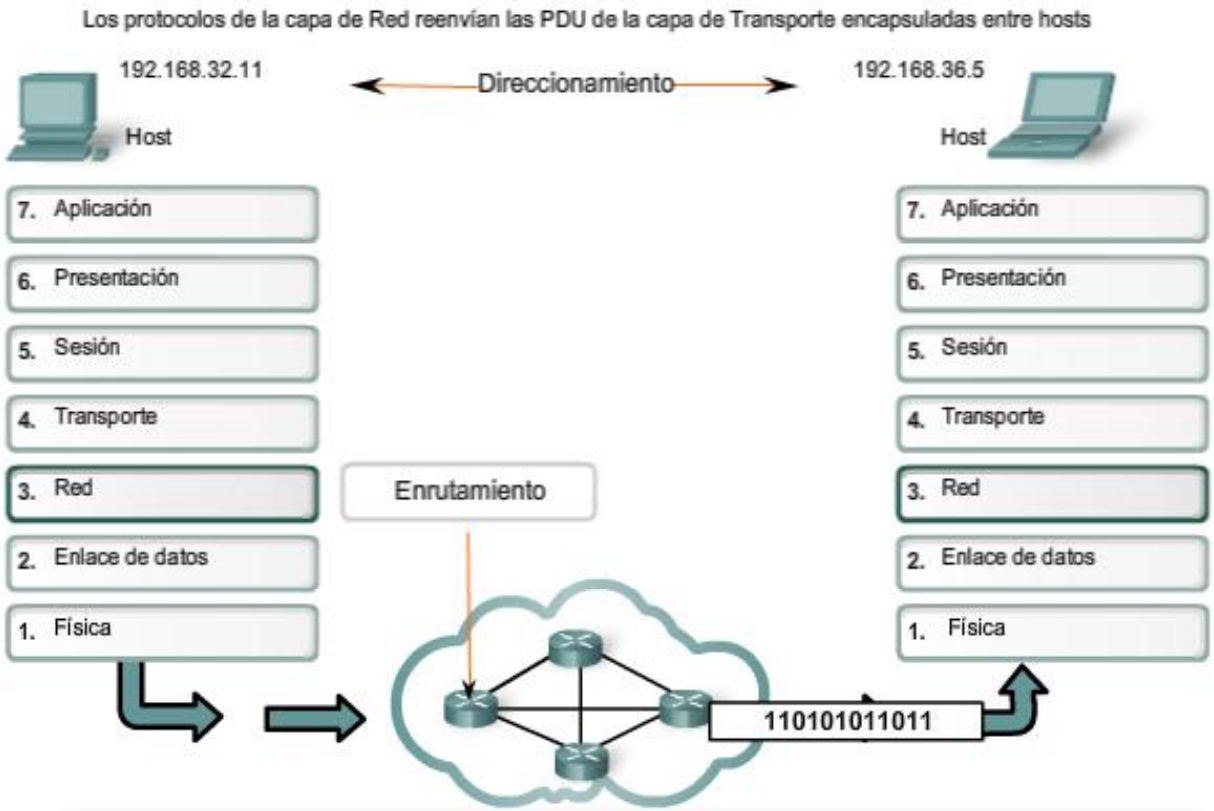
Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la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

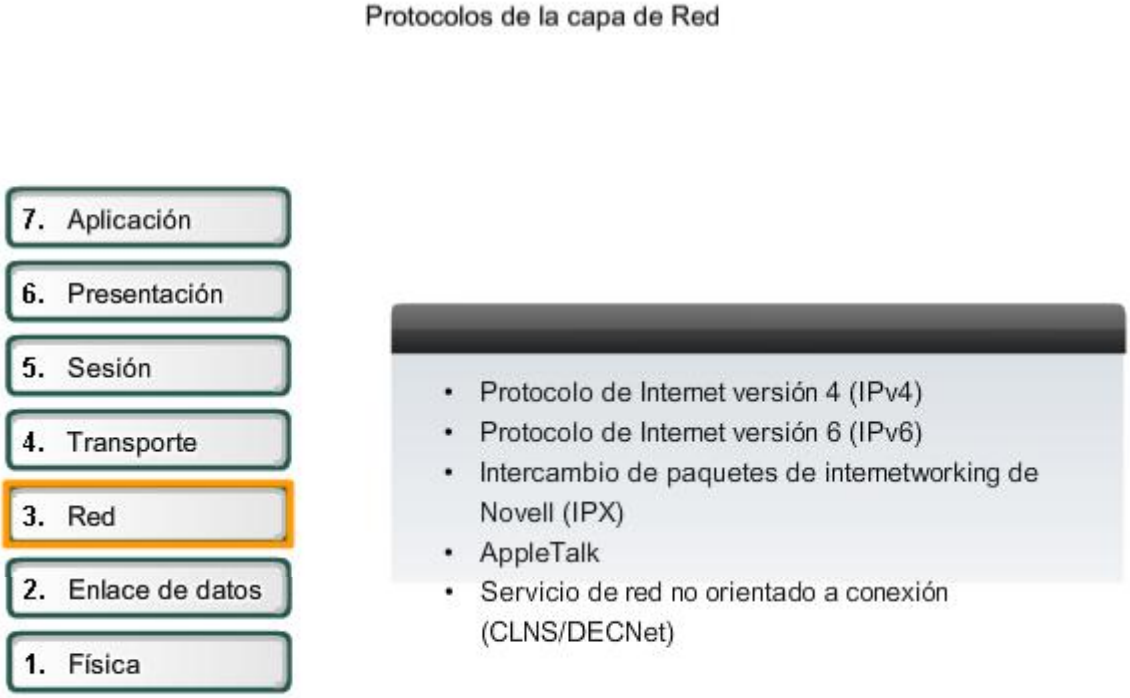


Protocolos de capa de Red

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 y es el tema de CCNA. Por lo tanto, será el ejemplo que usamos para protocolos de capa de Red en este curso.

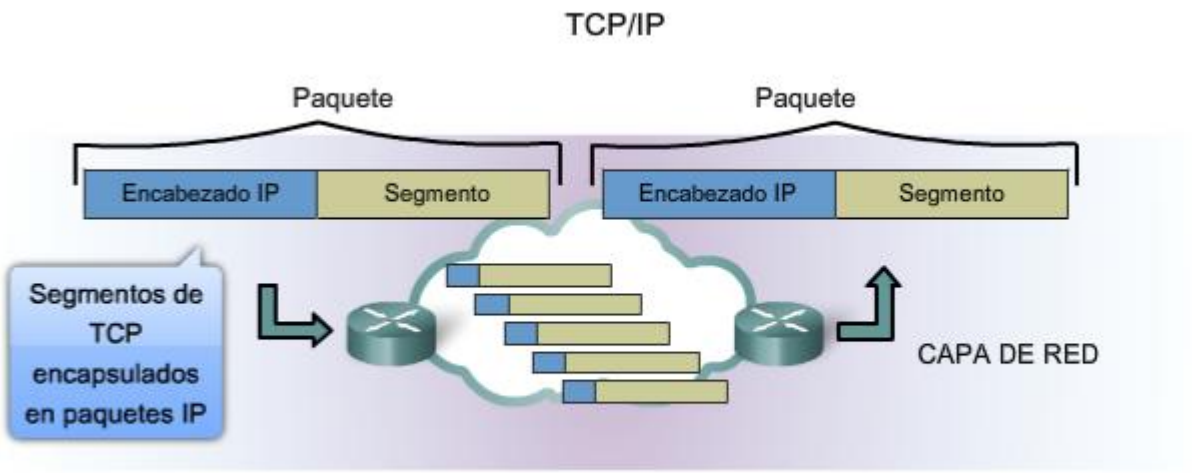
La versión 6 de IP (IPv6) está desarrollada y se implementa en algunas áreas. IPv6 operará junto con el IPv4 y puede reemplazarlo en el futuro. Los servicios provistos por IP, así como también la estructura y el contenido del encabezado de los paquetes están especificados tanto por el protocolo IPv4 como por el IPv6. Estos servicios y estructura de paquetes se usan para encapsular datagramas UDP o segmentos TCP para su recorrido a través de una internetwork.

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

El Protocolo de Internet fue diseñado como un protocolo con bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas.

Características básicas de IPv4:

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



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

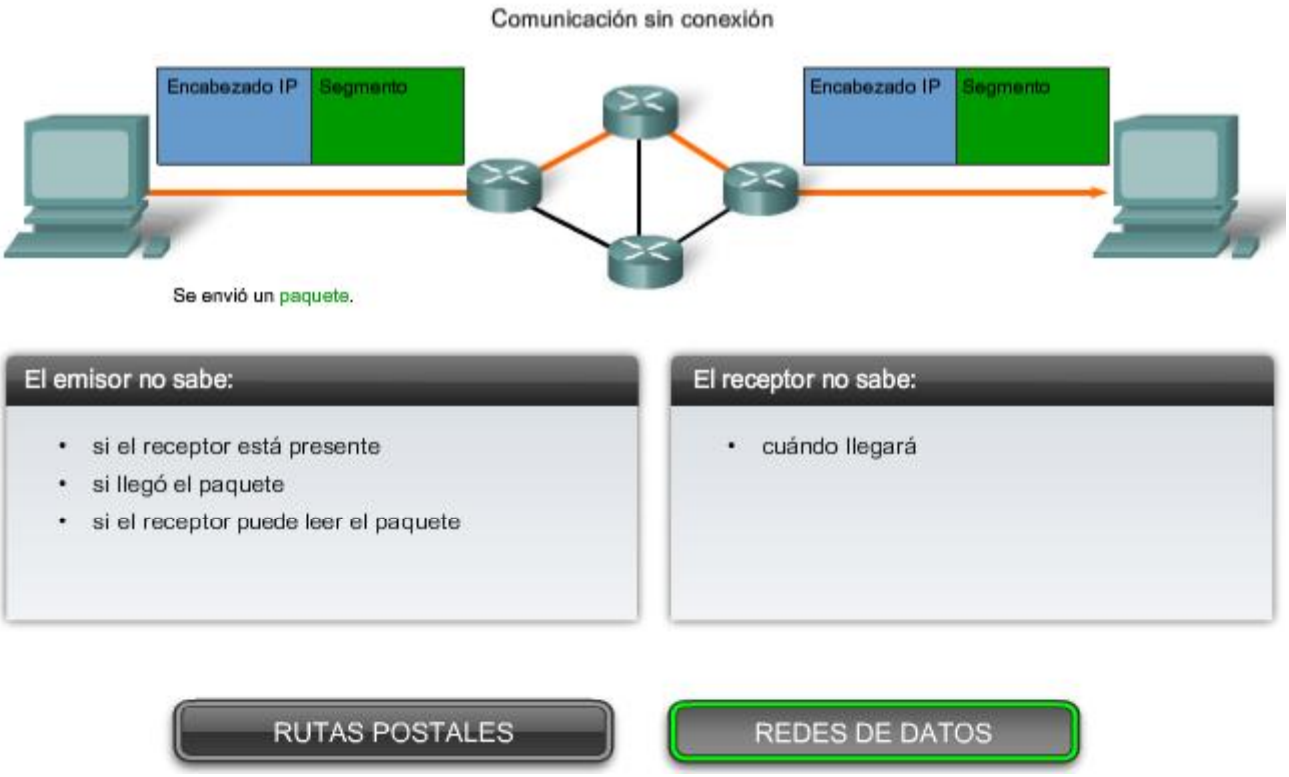
Servicio sin conexión

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: Mejor intento

Servicio de mejor intento (no confiable)

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

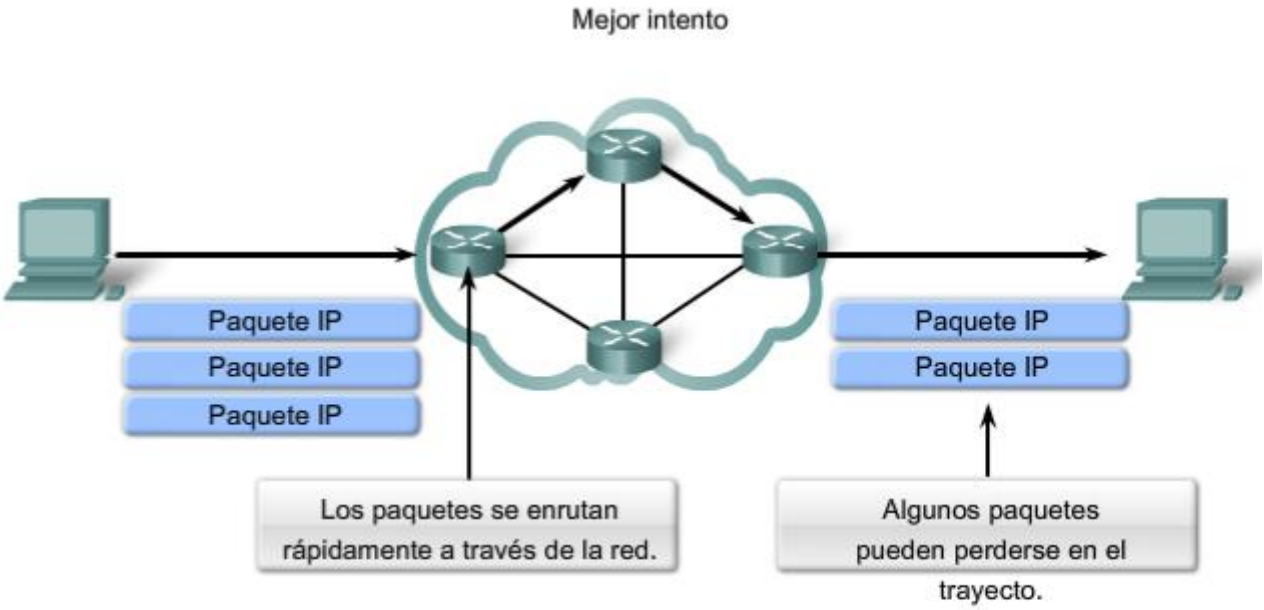
La función de la Capa 3 es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La Capa 3 no se ocupa de ni advierte el tipo de comunicación contenida dentro de un paquete. Esta responsabilidad es la función de las capas superiores a medida que se requieren.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

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.

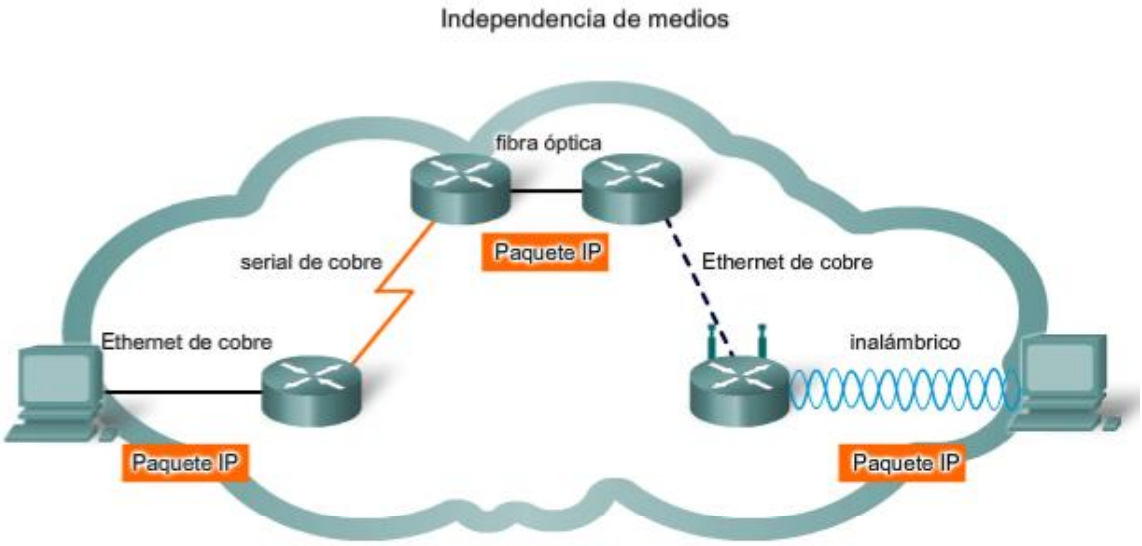
Es responsabilidad de la capa de Enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

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 paquetes 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 Protocolo 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. Haga clic en los pasos dentro de la figura para ver este proceso. La encapsulación de IPv4 permanece en su lugar desde el momento en que el paquete deja la capa de Red del host de origen hasta que llega a la capa de Red del host de destino.

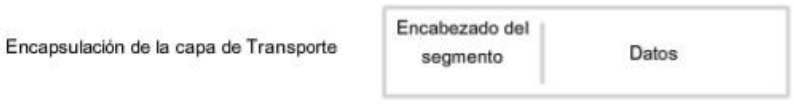
El proceso de encapsular datos por capas permite que los servicios en las diferentes capas se desarrollen y escalen sin afectar otras capas. Esto significa que los segmentos de la capa de Transporte pueden ser empaquetados fácilmente por los protocolos de la capa de Red existentes, como IPv4 e IPv6,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

Los routers pueden implementar estos protocolos de la capa de Red para operar concurrentemente en una red hacia y desde el mismo host u otro. El 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.

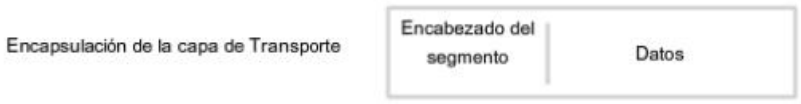
Enlaces

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

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



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



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

5.1.7 Encabezado del paquete IPv4

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

Este curso considerará estos 6 campos clave:

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

Campos IPv4 de encabezados clave

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

Dirección IP destino

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

Dirección IP origen

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

Tiempo de vida

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

Protocolo

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

Los valores de ejemplo son:
01 ICMP,
06 TCP, y
17 UDP.

Tipo de servicio

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

Desplazamiento de fragmentos

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

Señalizador de Más fragmentos

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

Señalizador de No Fragmentar

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

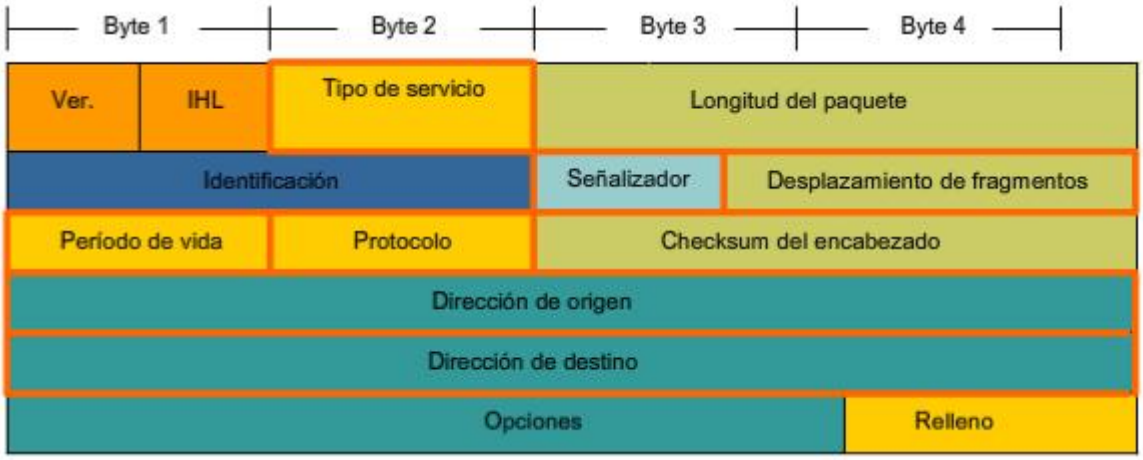
Enlaces:

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

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

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

Campos del encabezado de paquetes IPv4



Tipo de servicio

Prioridad de QoS de datos: Habilita al router para dar prioridad a la información de ruta de red y voz sobre los datos comunes.

Período de vida

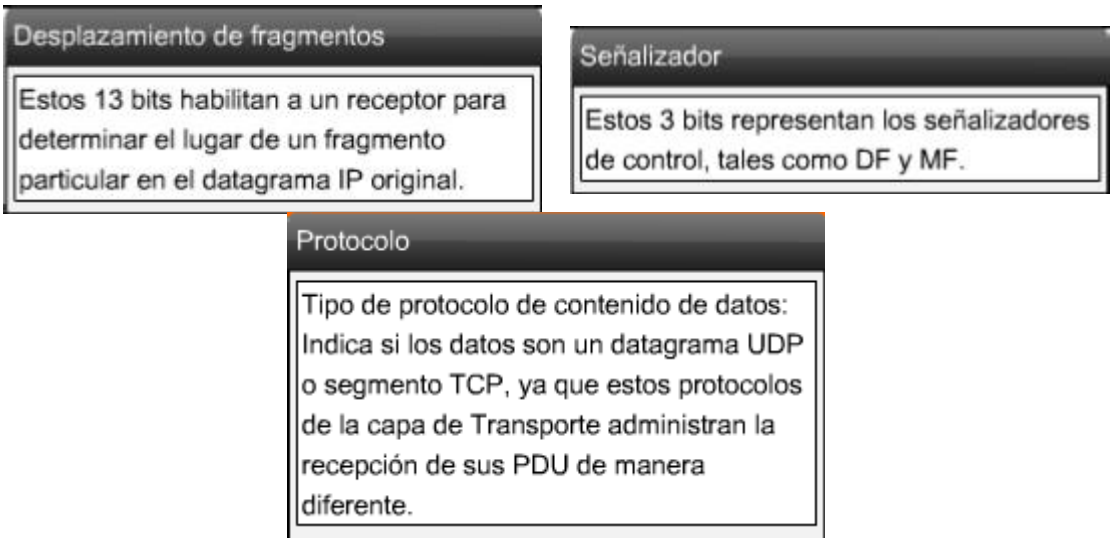
Cantidad de saltos antes de que se descarte el paquete: Este valor se reduce en cada salto para evitar que los paquetes se transmitan a través de la red en routing loops.

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 del encabezado

Versión: Contiene el número IP de la versión (4).

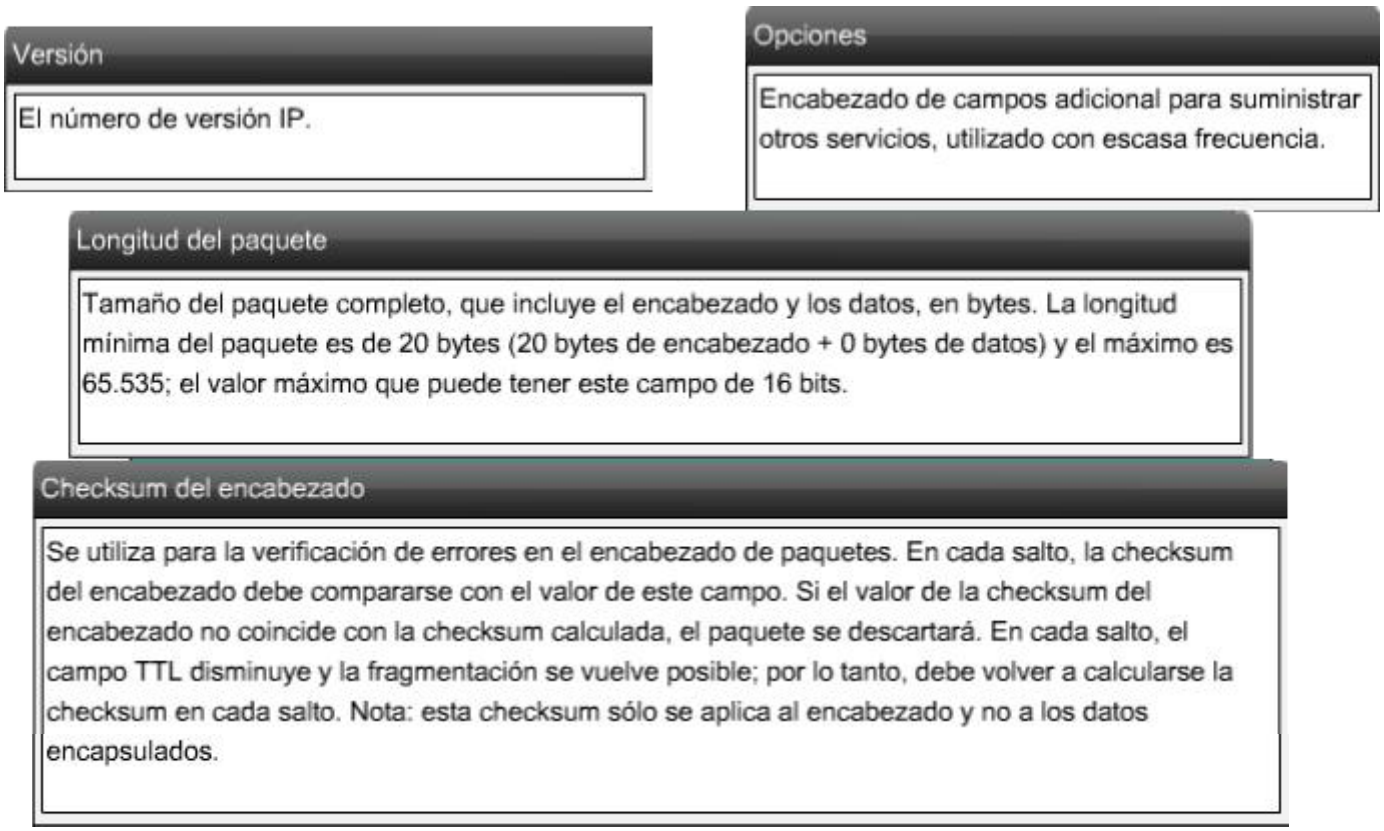
Longitud del encabezado (IHL). Especifica el tamaño del encabezado del paquete.

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.



Identificación
Identifica fragmentos de forma exclusiva en un paquete IP original.

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.

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.

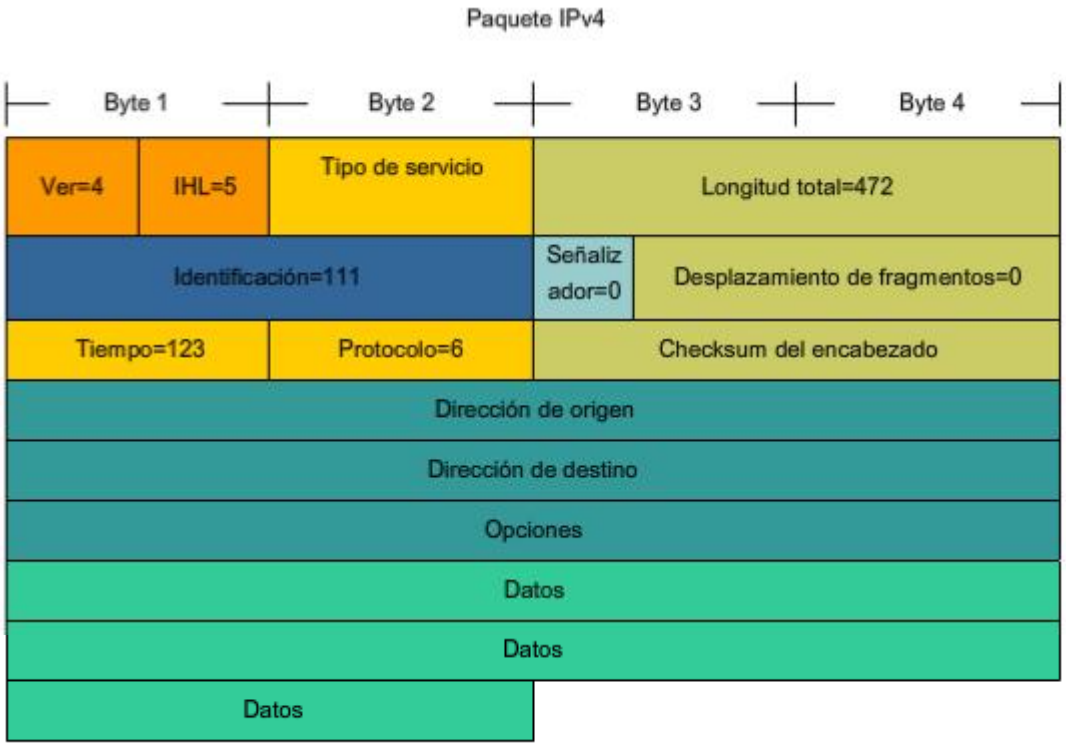
Identificación = 111; identificador original del paquete (requerido si se fragmenta posteriormente).

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 host 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.

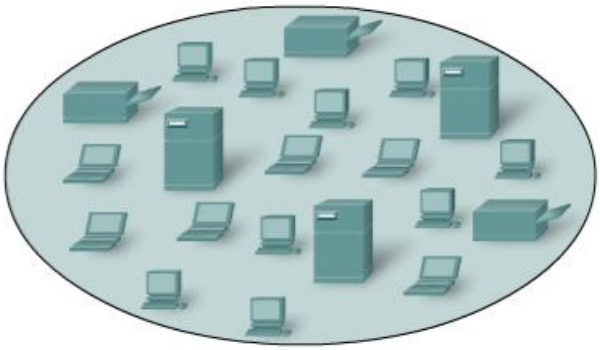
División de redes

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.

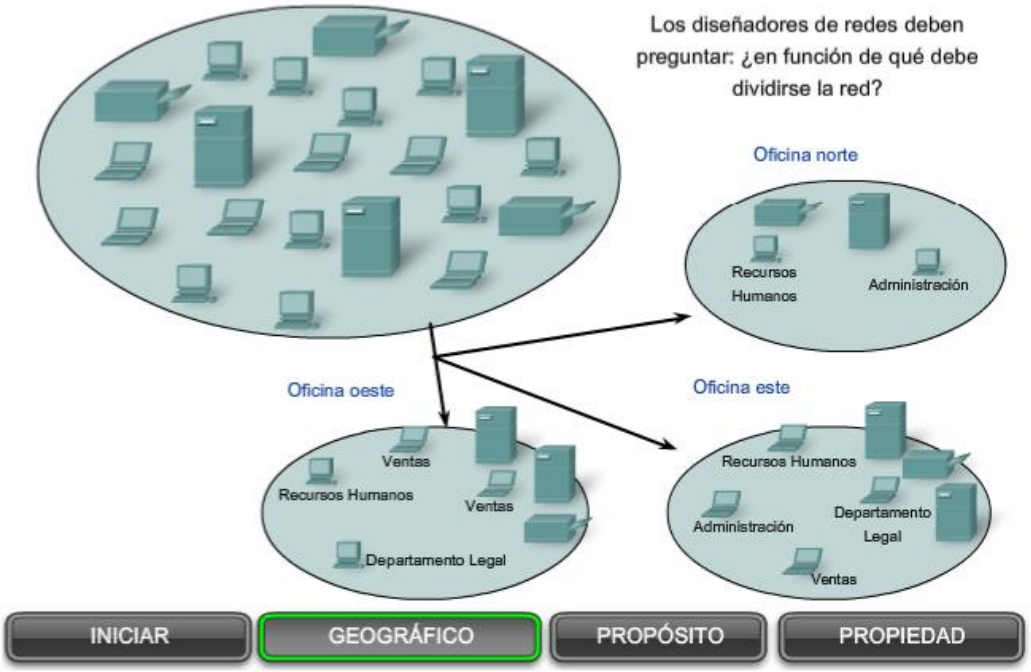
Como muestra la figura, las redes pueden agruparse basadas en factores que incluyen:
- ubicación geográfica,
- propósito, y
- propiedad.

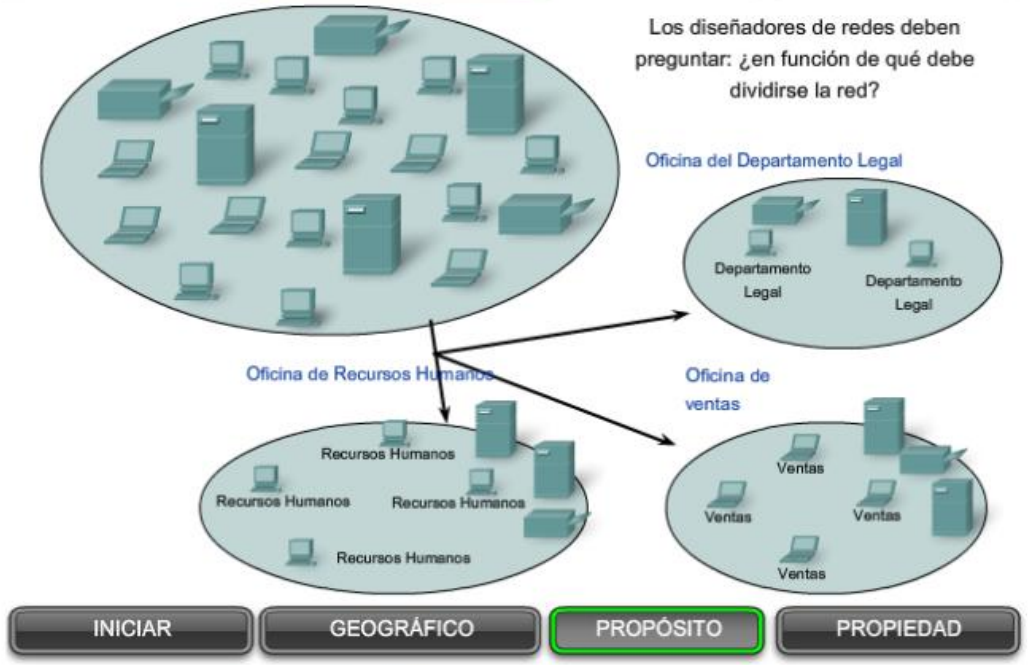


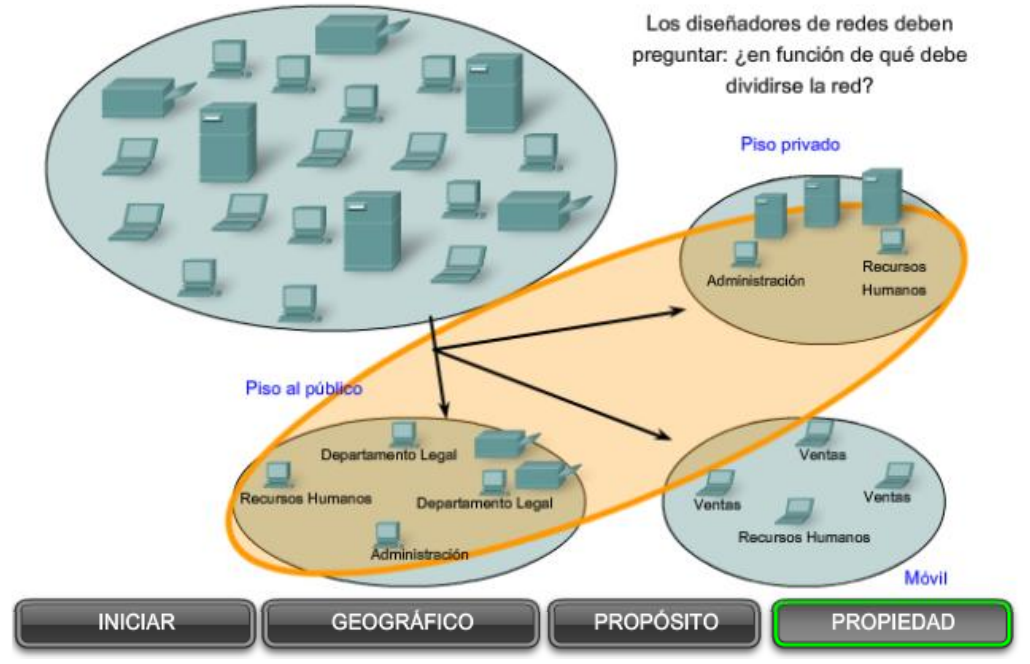
Una red amplia es demasiado compleja para que se opere y administre en forma eficiente.

Los diseñadores de redes deben preguntar: ¿en función de qué debe dividirse la red?

INICIAR | GEOGRÁFICO | PROPÓSITO | PROPIEDAD


Los diseñadores de redes deben preguntar: ¿en función de qué debe dividirse la red?
Oficina norte
Recursos Humanos
Administración
Oficina oeste
Ventas
Recursos Humanos
Ventas
Departamento Legal
Oficina este
Recursos Humanos
Administración
Departamento Legal
Ventas
INICIAR
GEOGRÁFICO
PROPÓSITO
PROPIEDAD


Los diseñadores de redes deben preguntar: ¿en función de qué debe dividirse la red?
Oficina del Departamento Legal
Departamento Legal
Departamento Legal
Oficina de Recursos Humanos
Recursos Humanos
Recursos Humanos
Recursos Humanos
Recursos Humanos
Oficina de ventas
Ventas
Ventas
Ventas
Ventas
INICIAR
GEOGRÁFICO
PROPÓSITO
PROPIEDAD


Los diseñadores de redes deben preguntar: ¿en función de qué debe dividirse la red?
Piso privado
Administración
Recursos Humanos
Piso al público
Departamento Legal
Recursos Humanos
Departamento Legal
Administración
Ventas
Ventas
Ventas
Recursos Humanos
Móvil
INICIAR
GEOGRÁFICO
PROPÓSITO
PROPIEDAD

Agrupación de hosts de manera geográfica

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

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.

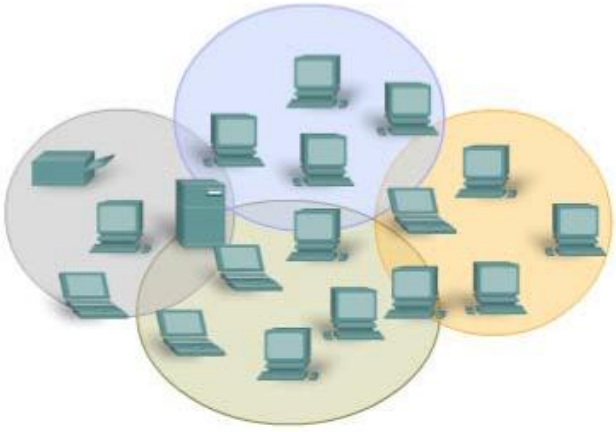
El volumen del tráfico de datos de la red generado por las diferentes aplicaciones puede variar significativamente. Dividir redes basadas en el uso facilita la ubicación efectiva de los recursos de la red así como también el acceso autorizado a esos recursos. Los profesionales en redes necesitan equilibrar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

Enlaces:

Diseño de red http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm



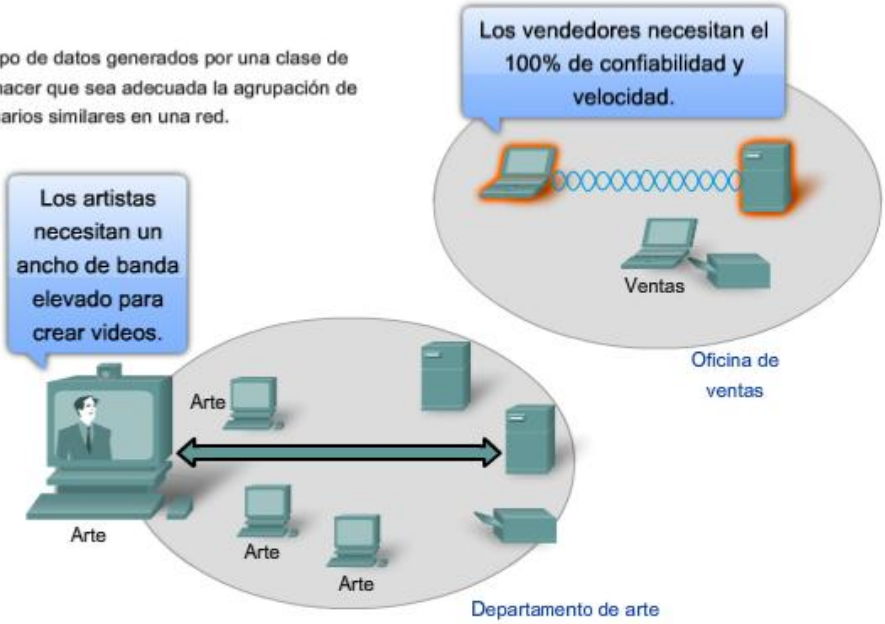
Existen muchas ventajas al dividir una red en segmentos administrables.

INICIAR GEOGRÁFICO PROPÓSITO PROPIEDAD

El simple hecho de conectar por cables la red física puede convertir la ubicación geográfica en un lugar lógico para realizar el inicio de la segmentación de una red.

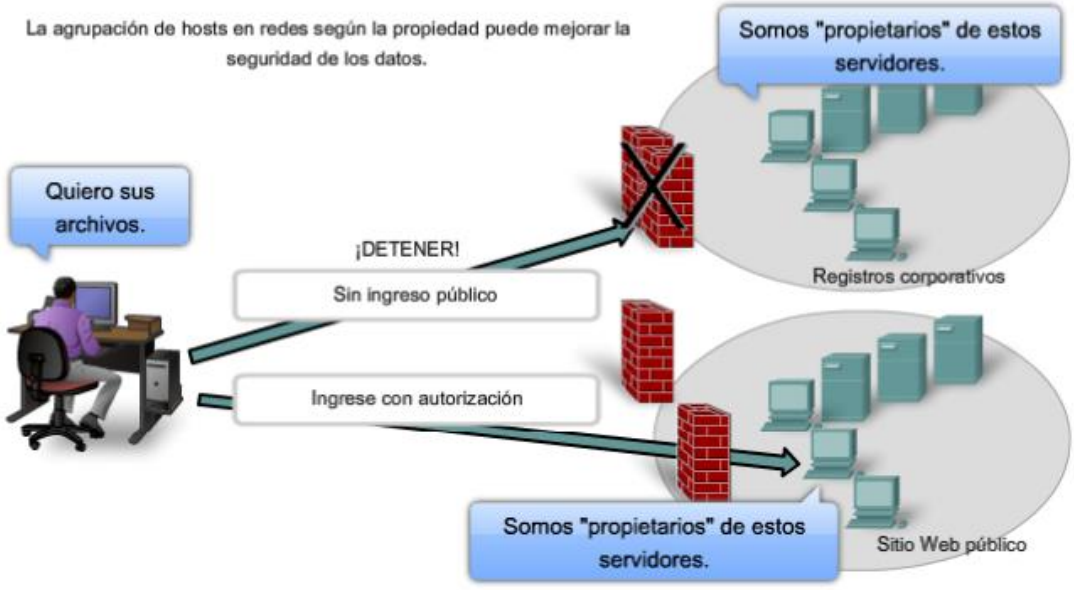
INICIAR | GEOGRÁFICO | PROPÓSITO | PROPIEDAD

El volumen y el tipo de datos generados por una clase de usuarios pueden hacer que sea adecuada la agrupación de usuarios similares en una red.



INICIAR | GEOGRÁFICO | PROPÓSITO | PROPIEDAD

La agrupación de hosts en redes según la propiedad puede mejorar la seguridad de los datos.



INICIAR | GEOGRÁFICO | PROPÓSITO | PROPIEDAD

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

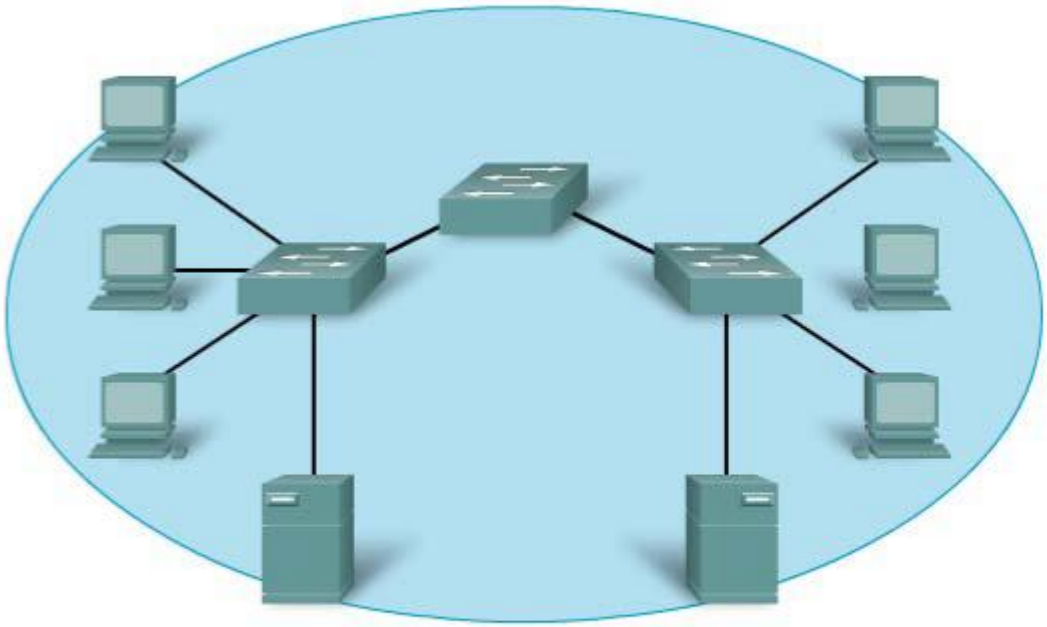
Grandes números de hosts conectados a una sola red pueden producir volúmenes de tráfico de datos que pueden extender, si no saturan, los recursos de red como la capacidad de ancho de banda y enrutamiento.

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.

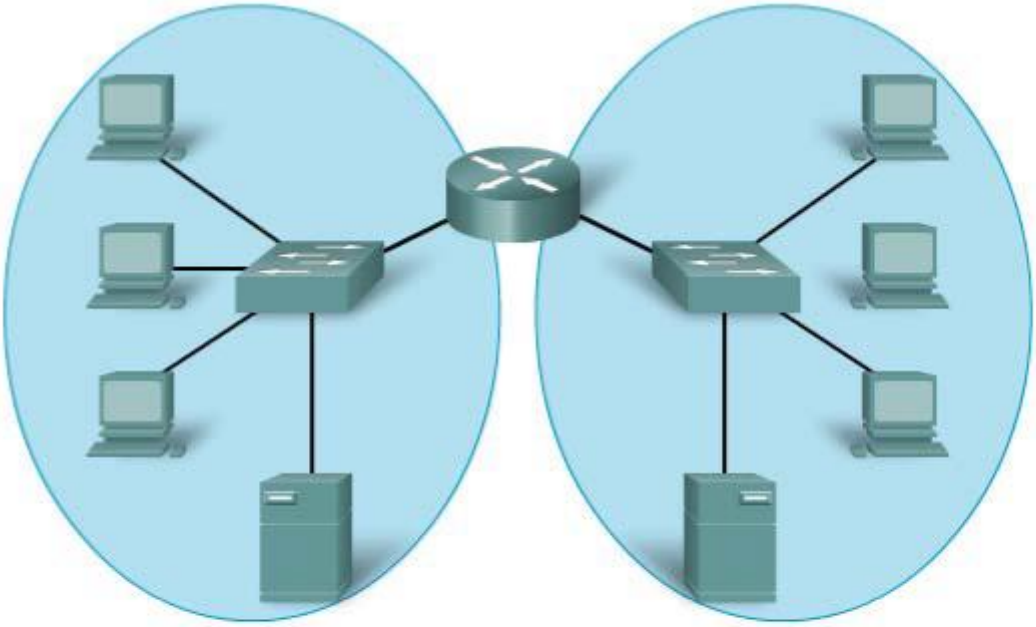
Los broadcasts están contenidos dentro de una red. En este contexto, a una red también se la conoce como un dominio de broadcast. La administración del tamaño de los dominios broadcast dividiendo una red en subredes asegura que el rendimiento de la red y de los host no se degraden hasta niveles inaceptables.



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.

Comenzar

Optimizar agrupación



El reemplazo del switch central por un router crea 2 subredes IP; por lo tanto, 2 dominios de broadcast diferentes. Todos los dispositivos están conectados pero se incluyen los broadcasts locales.

Comenzar

Optimizar agrupación

5.2.3 ¿Por qué separar hosts en redes? - Seguridad

La red basada en IP, que luego se convirtió en Internet, antiguamente tenía un pequeño número de usuarios confiables en agencias gubernamentales de EE.UU. y las organizaciones de investigación por ellas patrocinadas. En esta pequeña comunidad, la seguridad no era un problema importante.

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

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

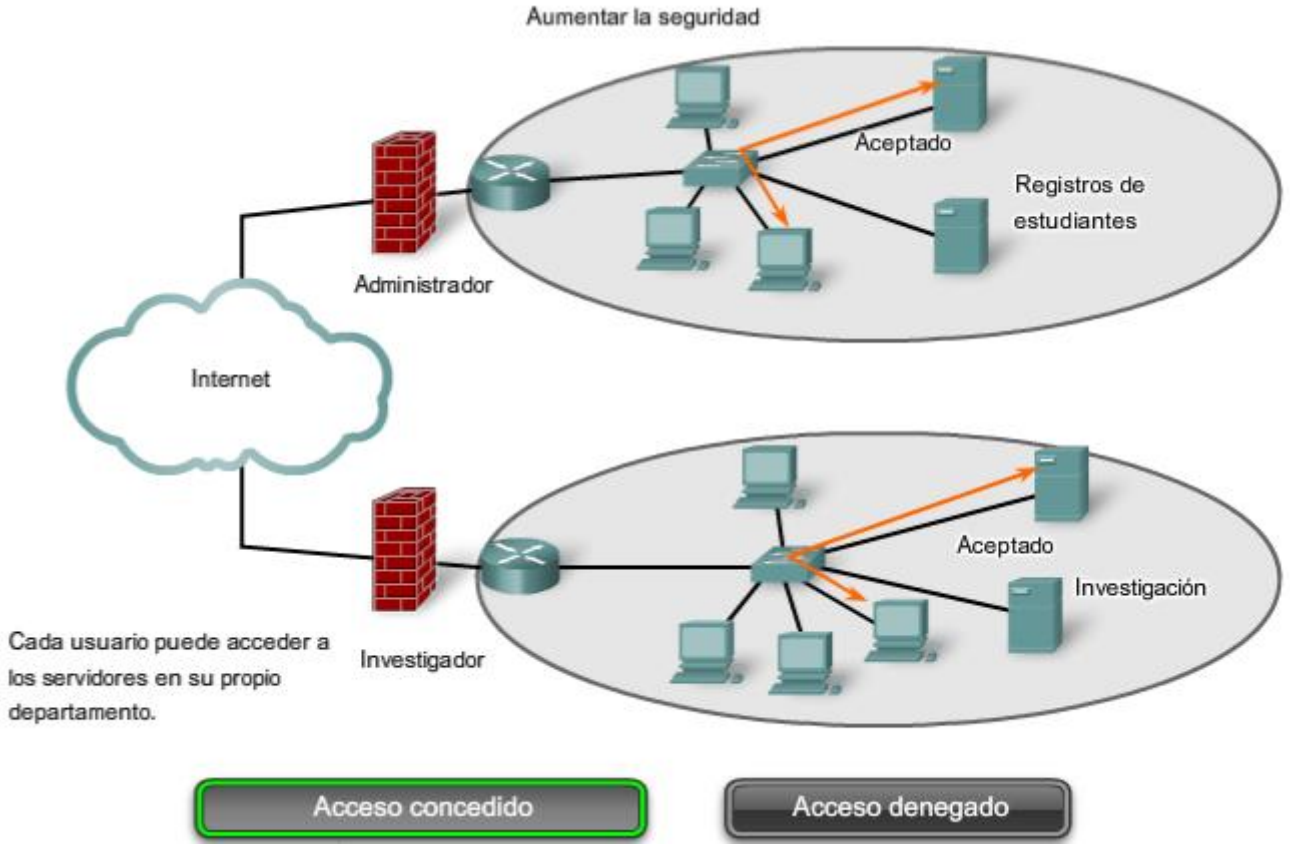
El acceso a internetwork dentro de una compañía u organización puede estar asegurado de manera similar. Por ejemplo, la red de una universidad puede dividirse en subredes para la administración, investigación y los estudiantes. Dividir una red basada en el acceso a usuarios es un medio para asegurar las comunicaciones y los datos del acceso no autorizado, ya sea por usuarios dentro de la organización o fuera de ella.

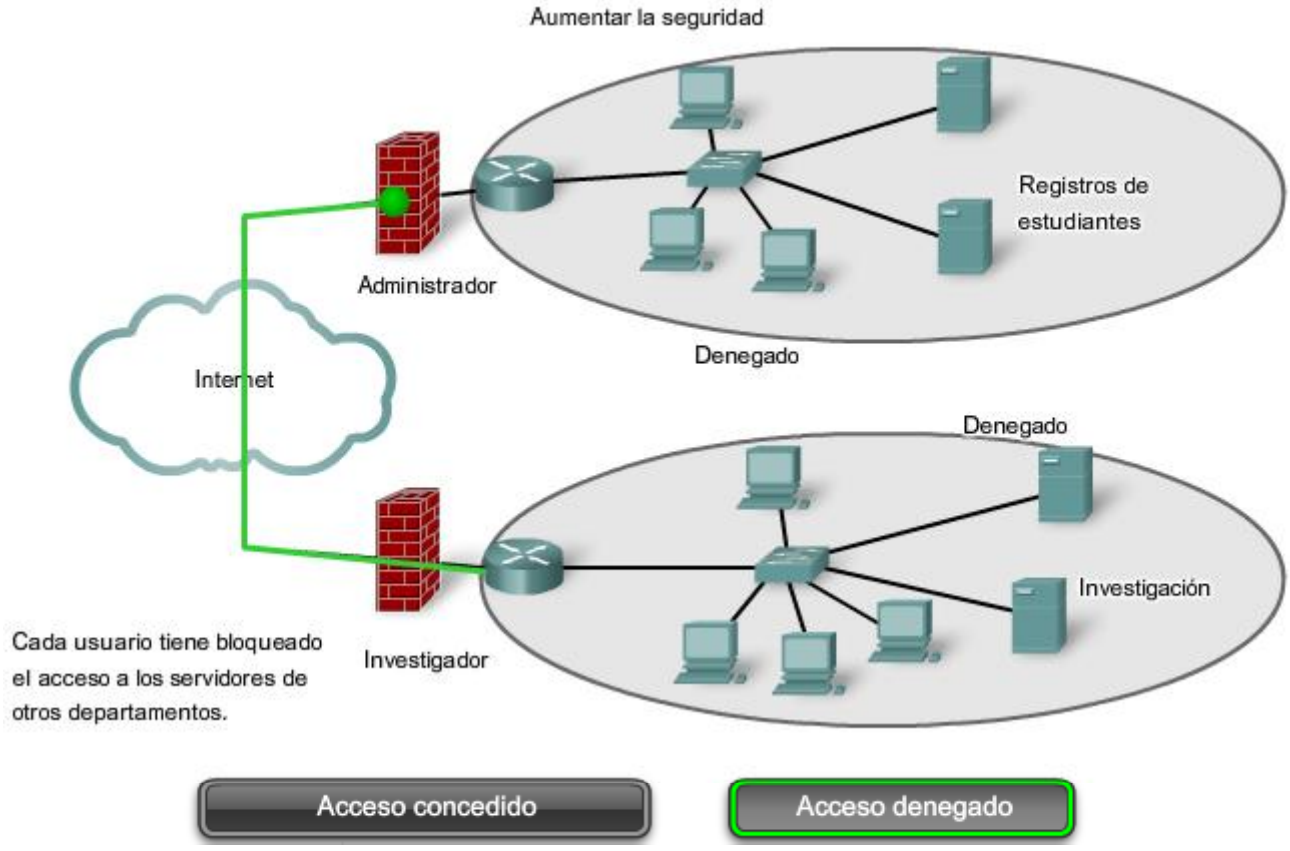
La seguridad entre redes es implementada en un dispositivo intermediario (router o firewall) en el perímetro de la red. La función del firewall realizada por este dispositivo permite que datos conocidos y confiables accedan a la red.

Enlaces:

Seguridad IP de red

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm



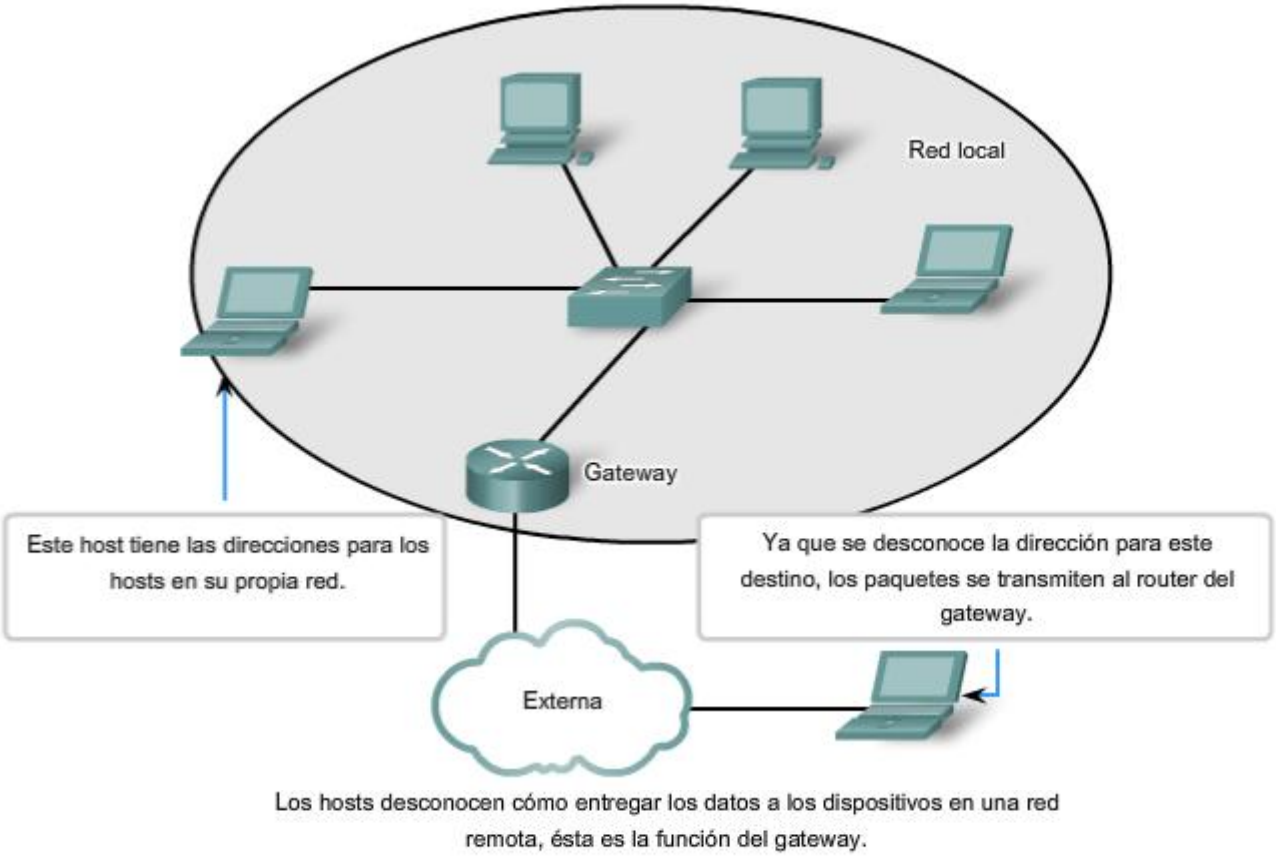


5.2.4 ¿Por qué separar hosts en redes? – Administración de direcciones

nternet 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 hots en redes? – Direccionamiento jerárquico

Para poder dividir redes, necesitamos el direccionamiento jerárquico. Una dirección jerárquica identifica cada host de manera exclusiva. También tiene niveles que ayudan a enviar paquetes a través de internetworks, lo que permite que una red sea dividida en base a esos niveles.

Para mantener las comunicaciones de datos entre redes por medio de internetworks, los esquemas de direccionamiento de capa de red son jerárquicos.

Como se ve en la figura, las direcciones postales son los principales ejemplos de direcciones jerárquicas.

Consideremos el caso de enviar una carta de Japón a un empleado que trabaja en Cisco Systems, Inc.

La carta estaría dirigida de la siguiente manera:

Nombre del empleado

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134

USA

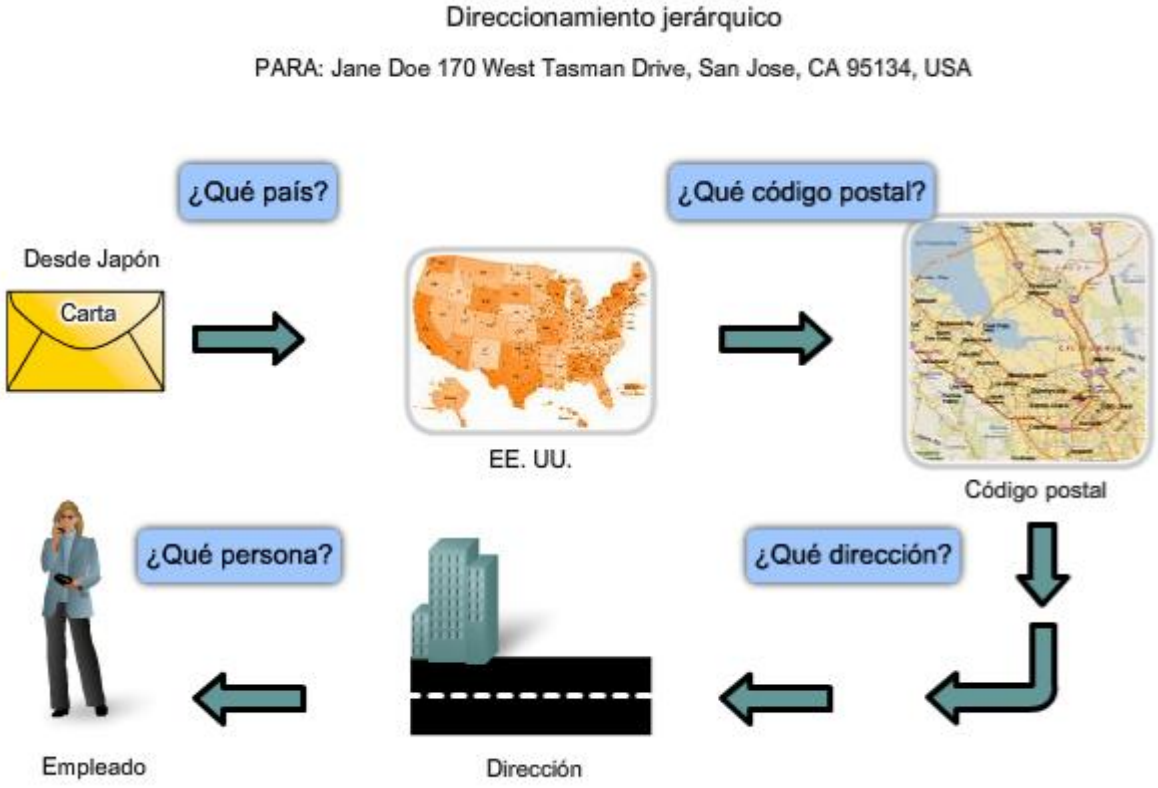
Cuando una carta se envía por correo postal en el país de origen, la autoridad postal sólo observaría el país de destino y notaría que la carta está destinada para EE. UU. En este nivel, no se necesita ningún otro detalle de dirección.

Cuando llega a EE.UU., la oficina postal primero observa el estado, California. La ciudad, calle, y nombre de la compañía no serían analizados si la carta todavía necesitara ser enviada al estado correcto. Una vez que la carta llega a California, será enviada a San Jose. Allí la portadora de correo local podría tomar la carta hacia West Tasman Drive y luego consultar la dirección y entregarla al 170. Cuando la carta esté realmente en las instalaciones de Cisco, se podría utilizar el nombre del empleado para enviarla a su último destino.

Con relación sólo al nivel de dirección relevante (país, estado, ciudad, calle, número y empleado) en cada etapa al dirigir la carta hacia el próximo salto hace que este proceso sea muy eficiente. No existe la necesidad de que cada paso en el envío conozca la ubicación exacta del destino; la carta fue dirigida a la dirección general hasta que el nombre del empleado fue finalmente utilizado en el destino.

Las direcciones jerárquicas de la red funcionan de manera muy similar. Las direcciones de la Capa 3 suministran la porción de la red de la dirección. Los routers envían paquetes entre redes refiriéndose sólo a la parte de la dirección de la capa de Red que se requiere para enviar el paquete hacia la red de destino. Para cuando llega el paquete a la red del host de destino, la dirección de destino completa del host habrá sido utilizada para entregar el paquete.

Si una red grande necesita ser dividida en redes más pequeñas, se pueden crear capas de direccionamiento adicionales. Usar el esquema de direccionamiento jerárquico significa que pueden conservarse los niveles más altos de la dirección (similar al país en una dirección postal), con el nivel medio denotando las direcciones de la red (estado o ciudad) y el nivel más bajo, los hosts individuales.



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.

Nota: El Capítulo 6 en este curso cubrirá el direccionamiento y subdireccionamiento IPv4 de red en detalle.

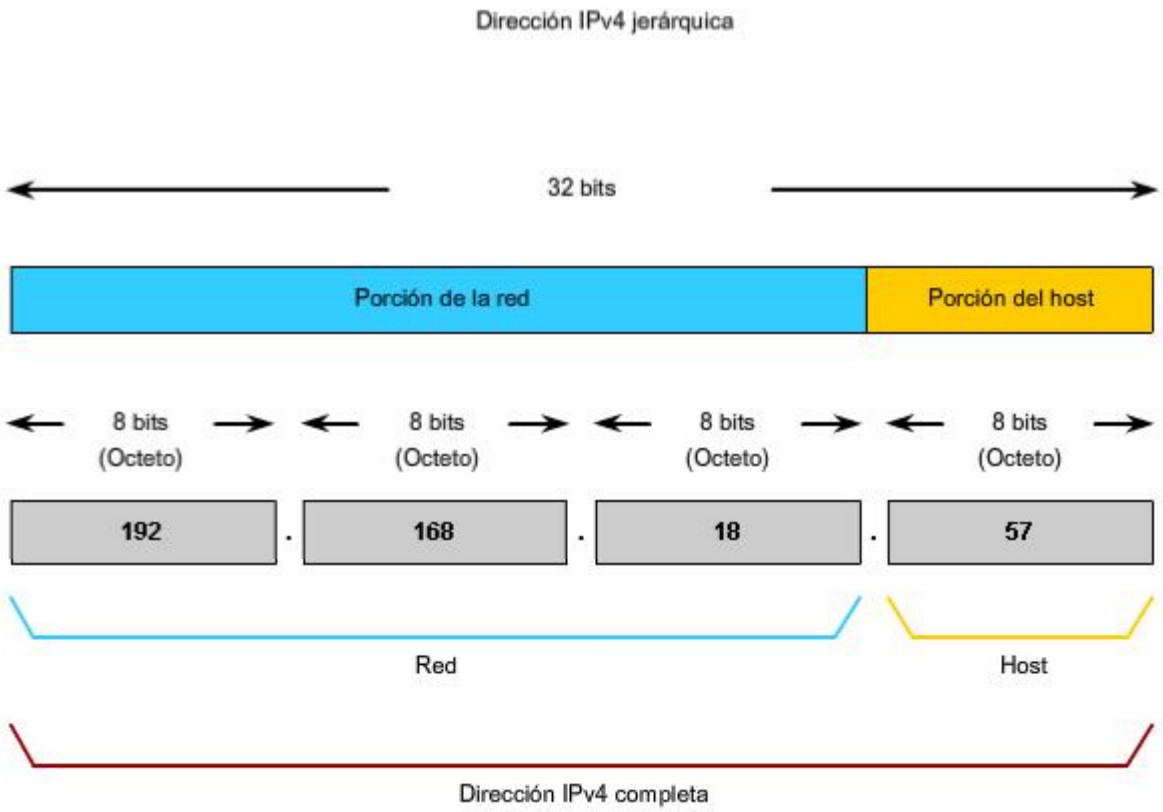
La extensión de la longitud del prefijo o máscara de subred permite la creación de estas subredes. De esta manera, los administradores de red tienen la flexibilidad de dividir redes para satisfacer las diferentes necesidades, como ubicación, administración del rendimiento de la red y seguridad, mientras asegura que cada host tenga una dirección única.

Para propósitos explicativos, en este capítulo, los primeros 24 bits de una dirección IPv4 se utilizarán como porción de red.

Enlaces:

Agencia de asignación de números por Internet

http://www.iana.org/



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.

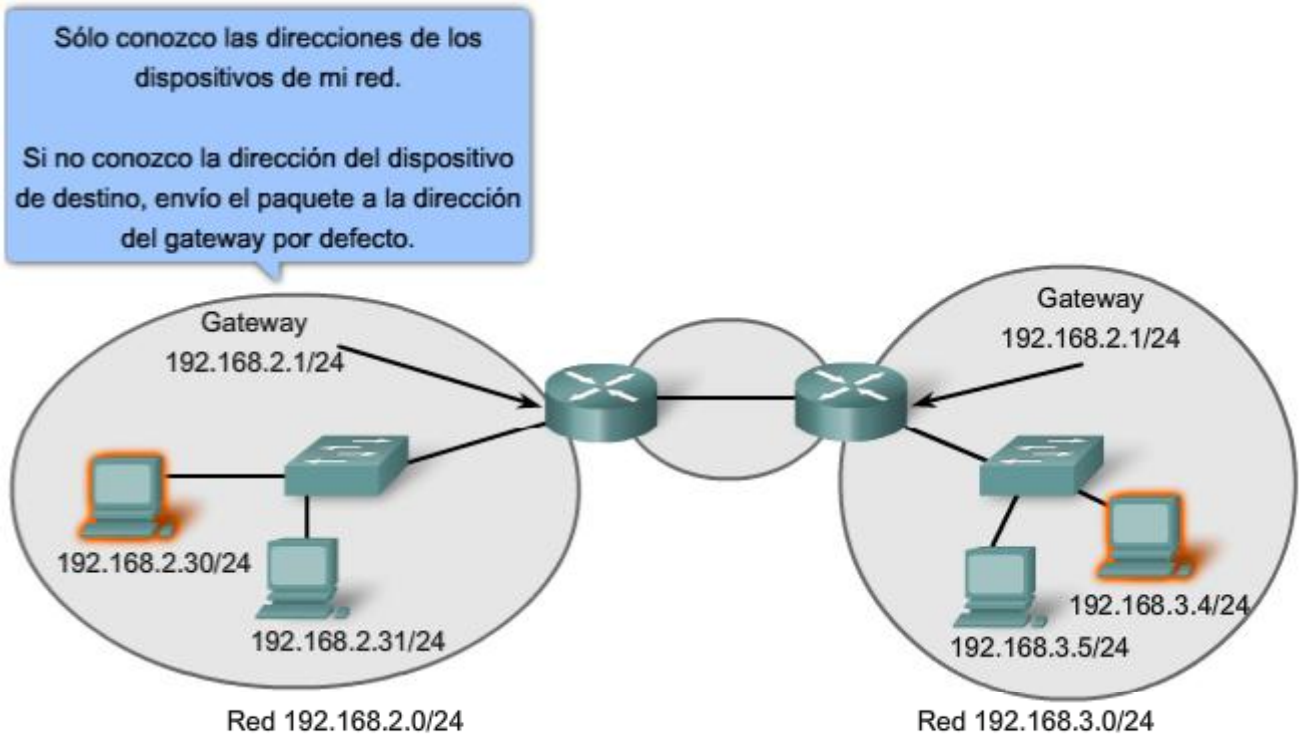
El router también necesita una ruta que defina dónde enviar luego el paquete. A esto se lo denomina dirección del siguiente salto. Si una ruta está disponible al router, el router enviará el paquete al router del próximo salto que ofrece una ruta a la red de destino.

Enlaces;

RFC 823

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

Los gateways permiten las comunicaciones entre redes



5.3.2 Paquetes IP: Cómo llevar datos de extremo a extremo

Como ya sabe, la función de la capa de Red es transferir datos desde el host que origina los datos hacia el host que los usa. Durante la encapsulación en el host origen, un paquete IP se construye en la Capa 3 para transportar el PDU de la Capa 4. Si el host de destino está en la misma red que el host de origen, el paquete se envía entre dos hosts en el medio local sin la necesidad de un router.

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

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

Si la comunicación se produce entre dos hosts de diferentes redes, la red local envía el paquete desde el origen hasta su router 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.

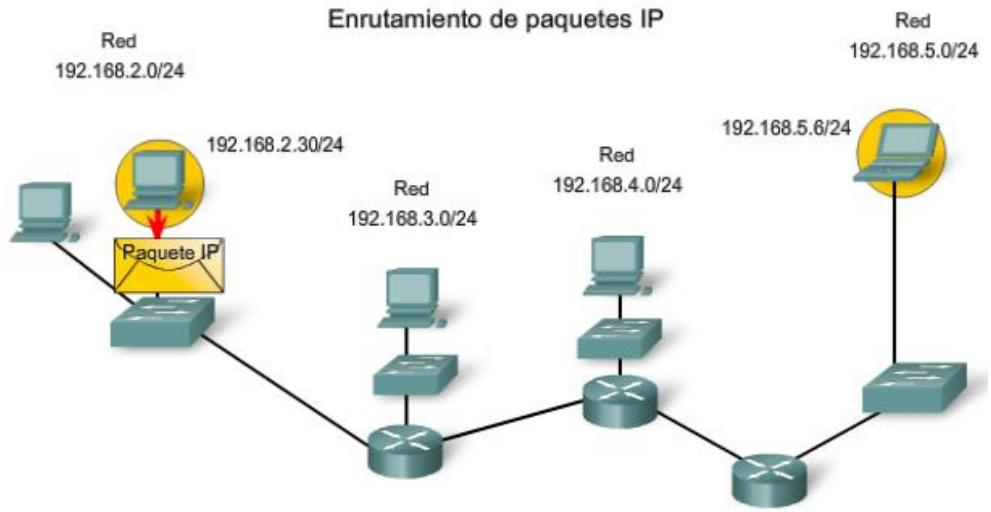
El paquete que se envía pasa a ser responsabilidad de este segundo router. Muchos routers o saltos a lo largo del camino puede procesar el paquete antes de llegar a destino.

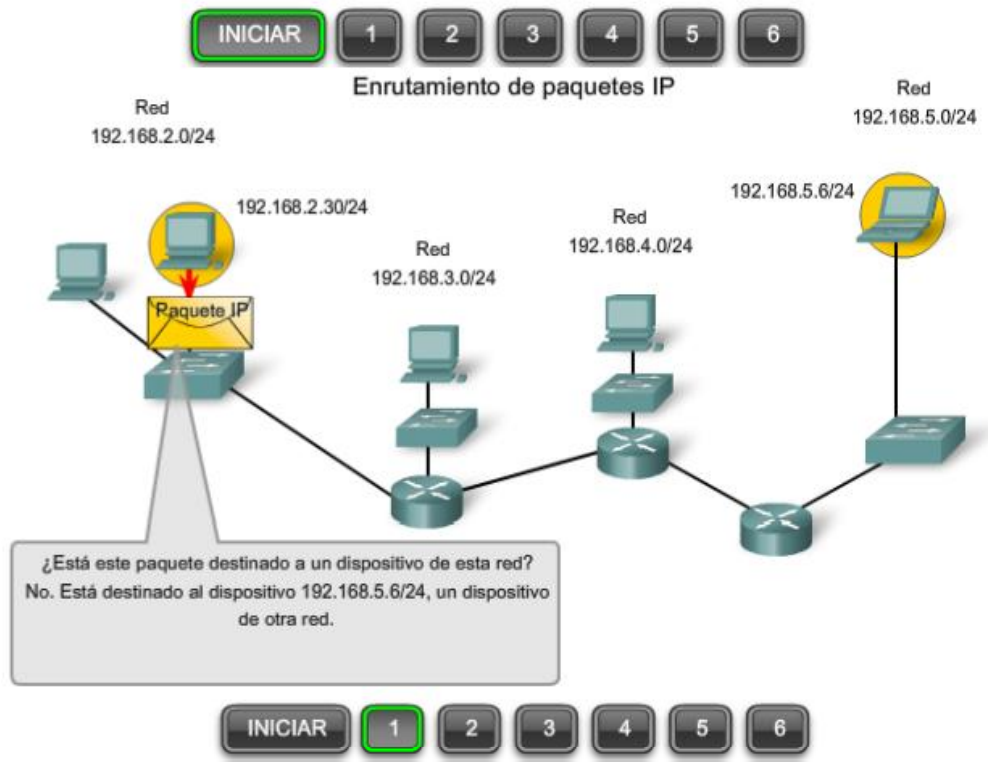
Haga clic en los pasos de la figura para seguir la ruta del paquete IP.

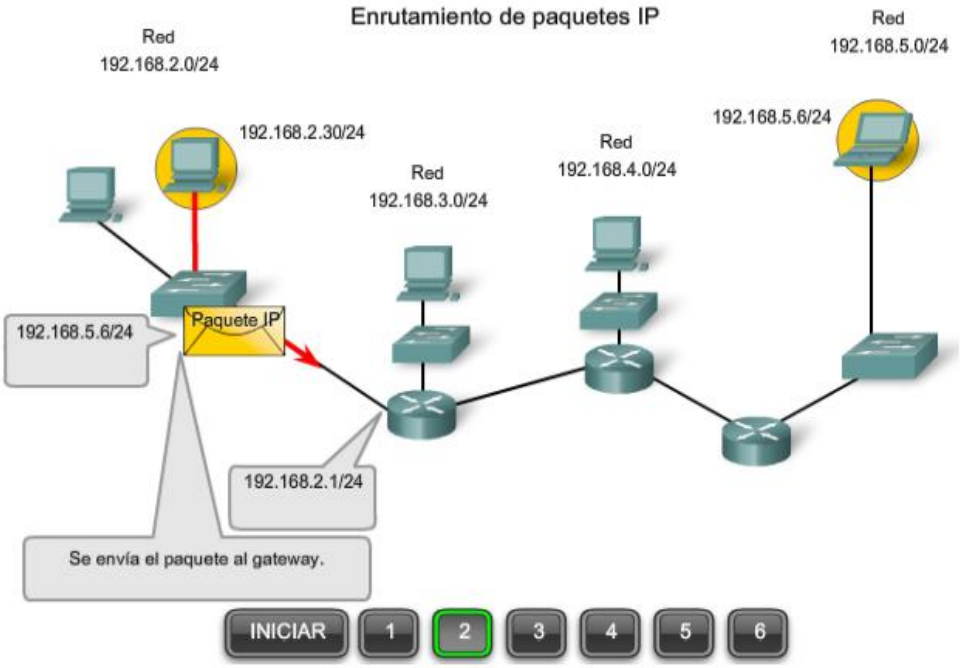
Enlaces:

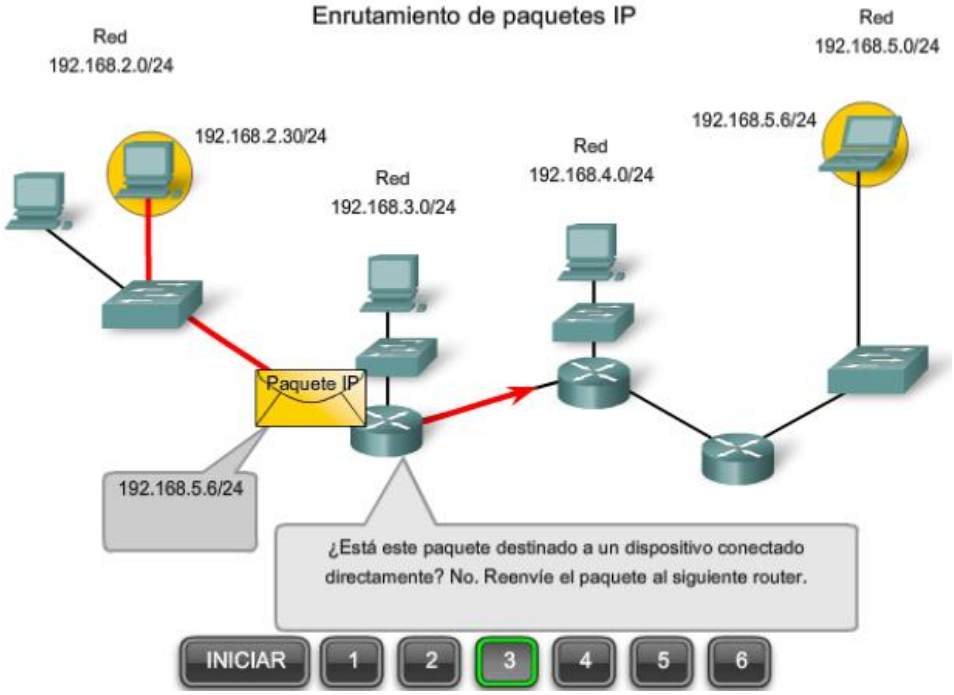
RFC 791 http://www.ietf.org/rfc/rfc0791.txt

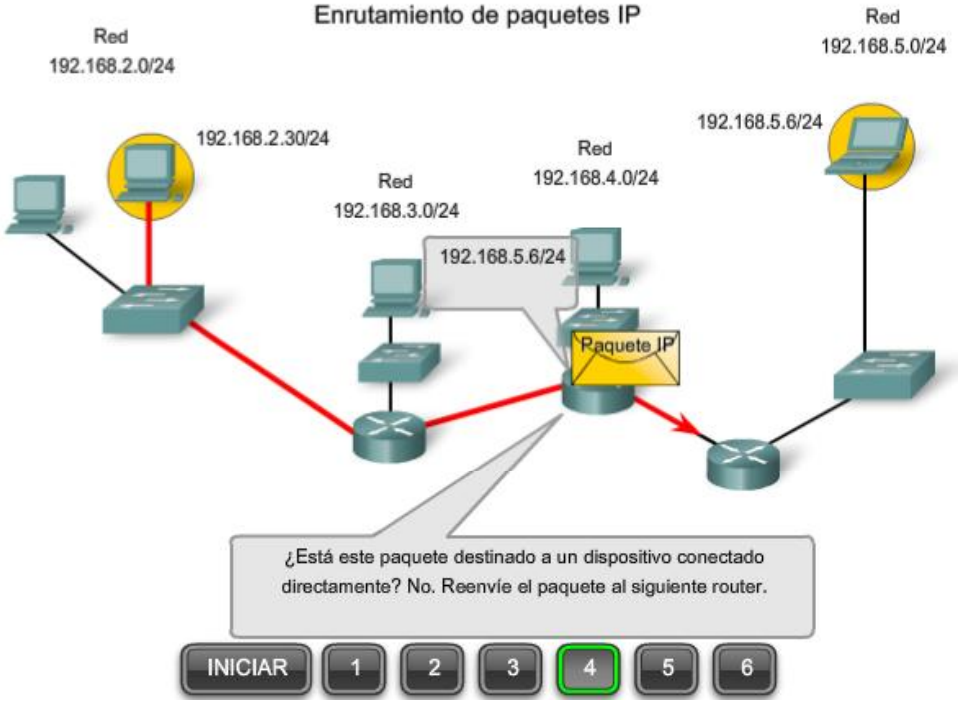
RFC 823 http://www.ietf.org/rfc/rfc0823.txt

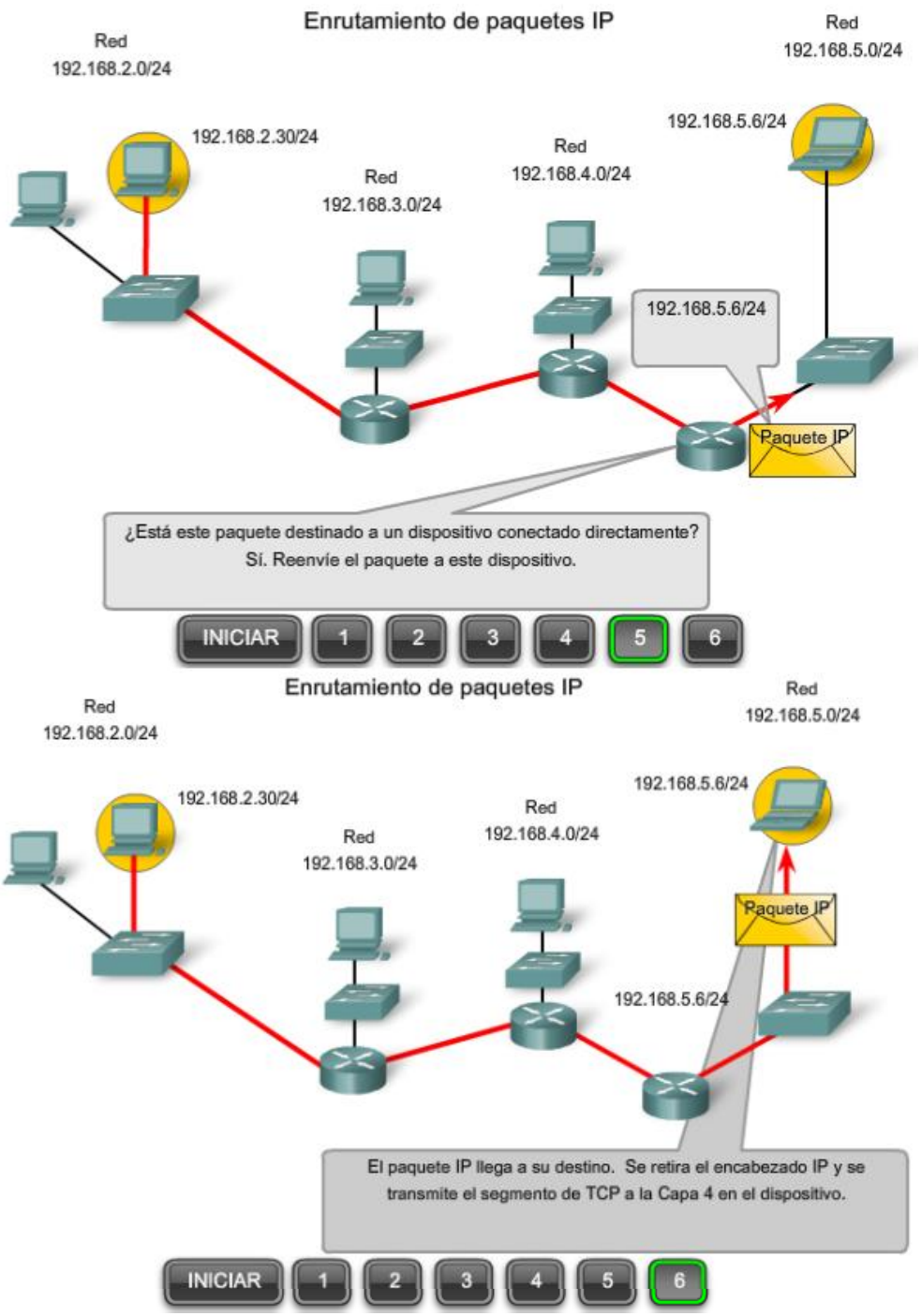





Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
Red
192.168.3.0/24
Red
192.168.4.0/24
192.168.5.6/24
Paquete IP
192.168.5.6/24
192.168.2.1/24
Se envía el paquete al gateway.
INICIAR
1
2
3
4
5
6


Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
Red
192.168.3.0/24
Red
192.168.4.0/24
192.168.5.6/24
Paquete IP
192.168.5.6/24
¿Está este paquete destinado a un dispositivo conectado directamente? No. Reenvíe el paquete al siguiente router.
INICIAR
1
2
3
4
5
6


Enrutamiento de paquetes IP
Red
192.168.2.0/24
Red
192.168.5.0/24
192.168.2.30/24
Red
192.168.3.0/24
Red
192.168.4.0/24
192.168.5.6/24
192.168.5.6/24
Paquete IP
¿Está este paquete destinado a un dispositivo conectado directamente? No. Reenvíe el paquete al siguiente router.
INICIAR
1
2
3
4
5
6



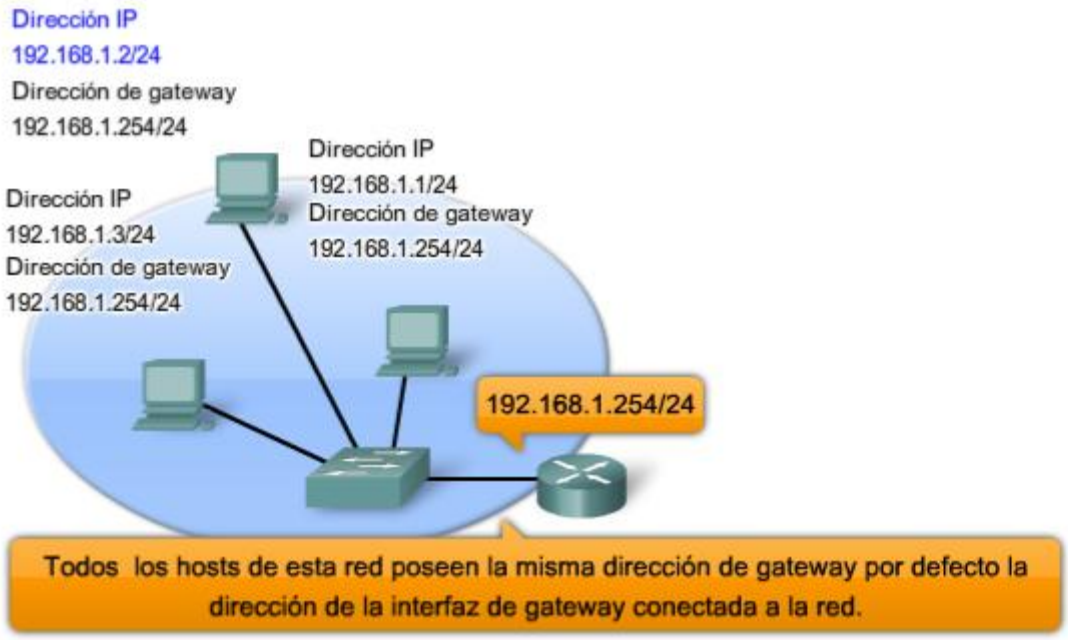
5.3.3 Gateway: La salida de nuestra red

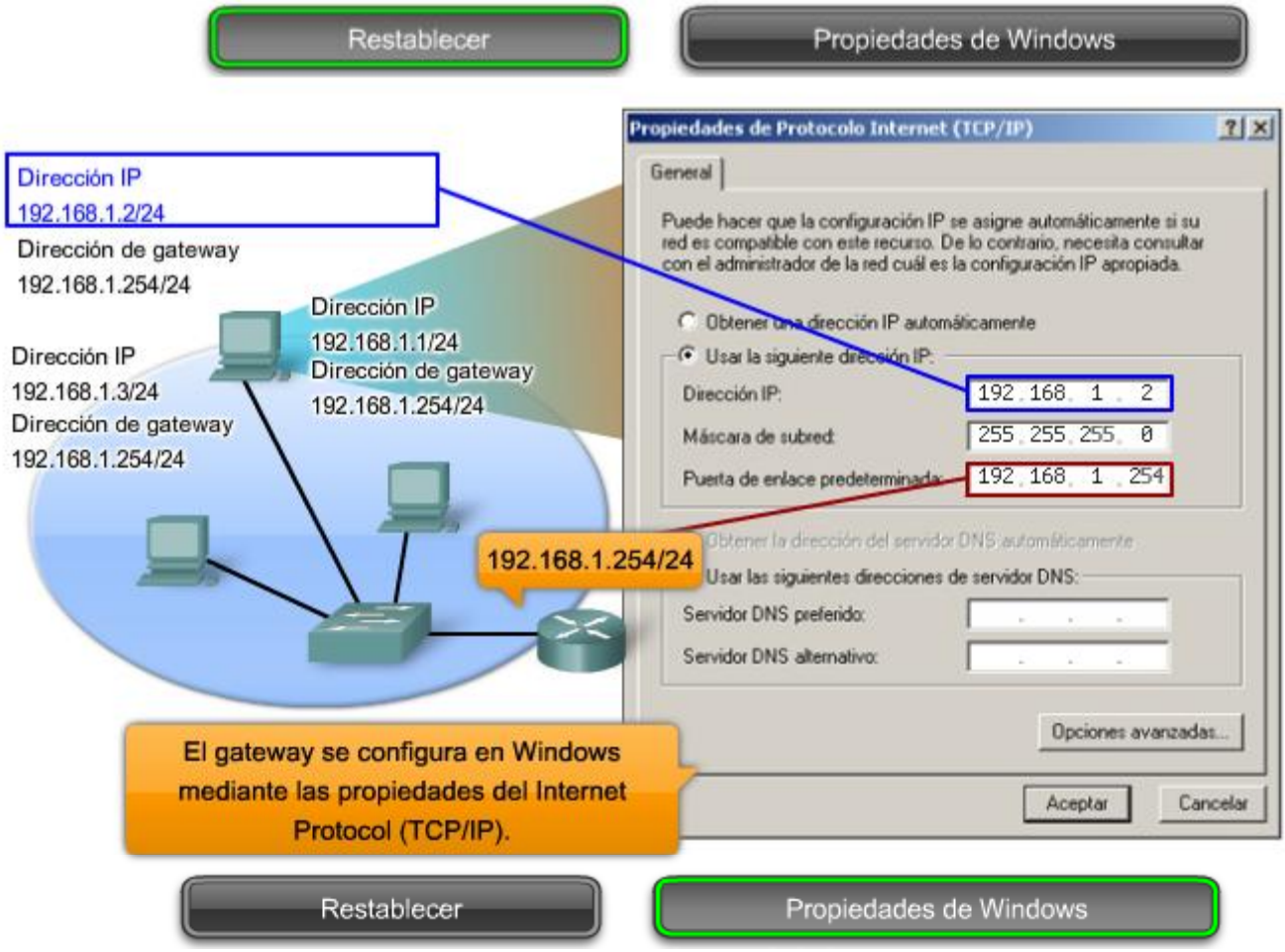
El gateway, también conocido como gateway por defecto, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host de origen, el paquete tiene que hallar la salida fuera de la red original. Para esto, el paquete 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

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
     ① IP Address. . . . . . . . . . . . : 192.168.1.2
     ② Subnet Mask . . . . . . . . . . . : 255.255.255.0
     ③ Default Gateway . . . . . . . . . : 192.168.1.254
```

Dirección IP para este equipo host

Confirmación de la configuración del gateway

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
     ① IP Address. . . . . . . . . . . . : 192.168.1.2
     ② Subnet Mask . . . . . . . . . . . : 255.255.255.0
     ③ Default Gateway . . . . . . . . . : 192.168.1.254
```

Máscara de subred de la red local

Confirmación de la configuración del gateway

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
     ① IP Address. . . . . . . . . . . . : 192.168.1.2
     ② Subnet Mask . . . . . . . . . . . : 255.255.255.0
     ③ Default Gateway . . . . . . . . . : 192.168.1.254
```

Dirección del gateway por defecto para este equipo host

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.

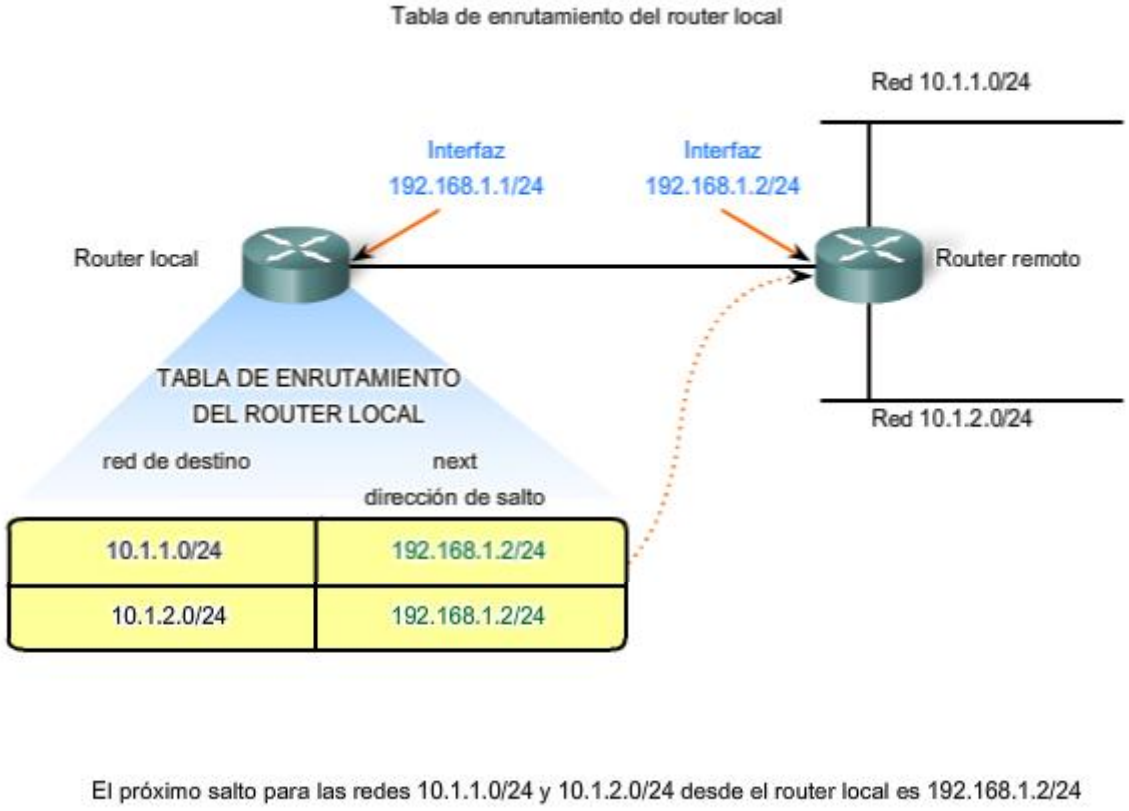
Un host debe reenviar el paquete ya sea al host en la red local o al gateway, según sea lo adecuado. Para reenviar los paquetes, el host debe tener rutas que representan estos destinos.

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:

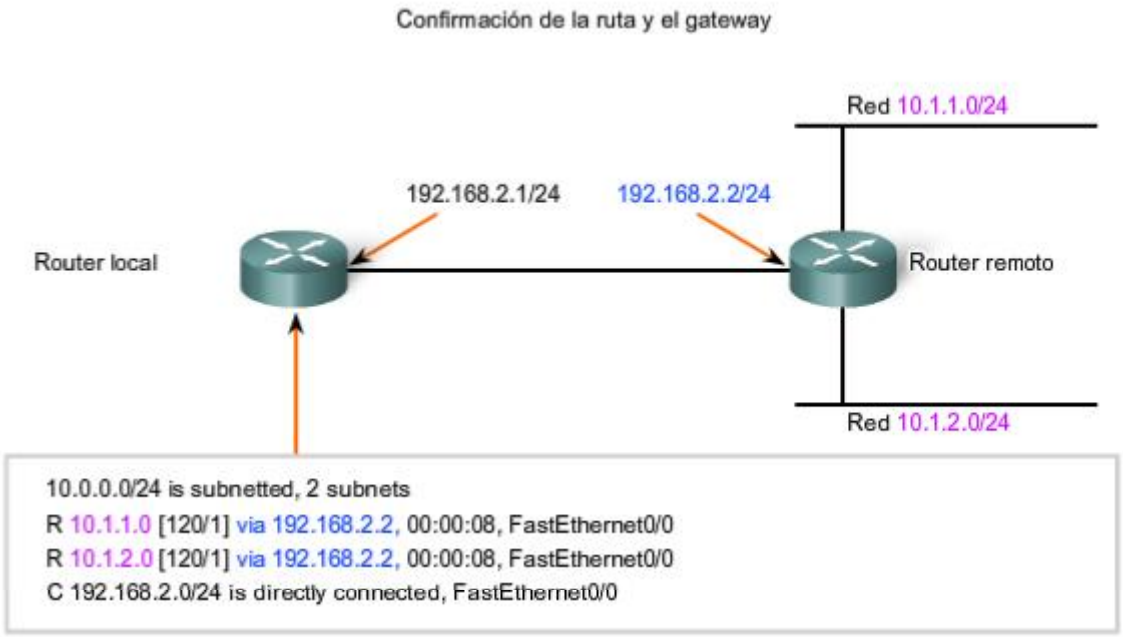
- red de destino,
- próximo salto, y
- métrica.

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.

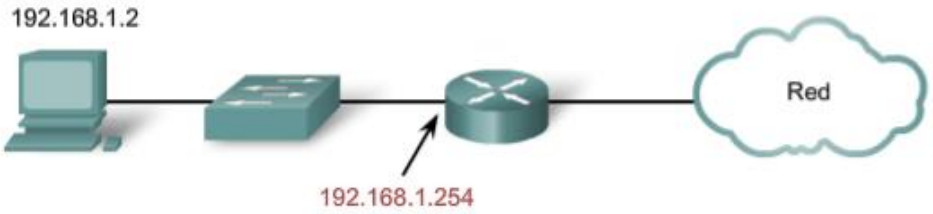
Como muestra la figura, la tabla de enrutamiento de un host de computadora puede ser analizada en la línea de comando introduciendo los comandos netstat -r, route, o route PRINT.

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

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 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.

Enlaces:

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

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.

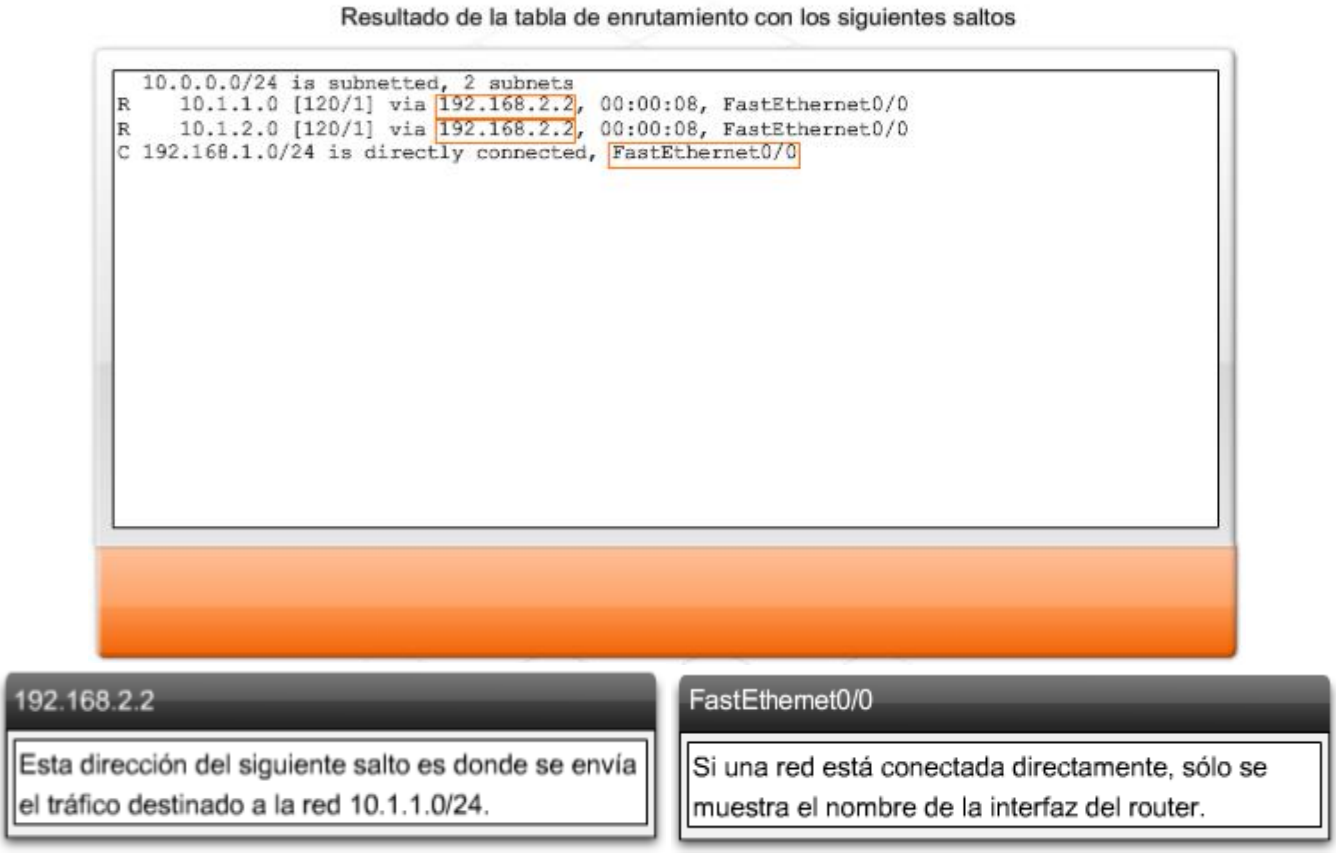
En la tabla de enrutamiento de un router, cada ruta enumera un siguiente salto para cada dirección de destino abarcada por la ruta. A medida que cada paquete llega al router, la dirección de la red de destino es analizada y comparada con las rutas en la tabla de enrutamiento. Cuando se determina una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

Enlaces:

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



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

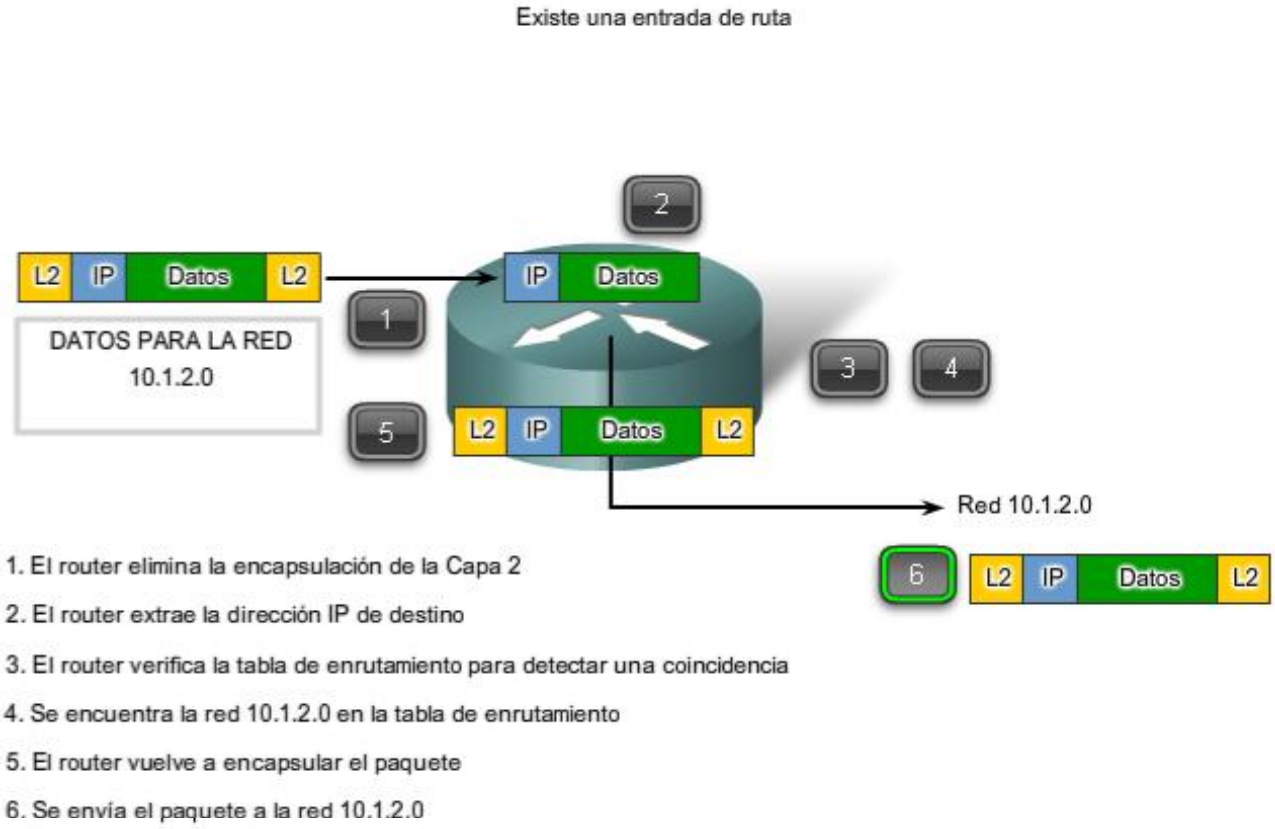
Examen del paquete

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.

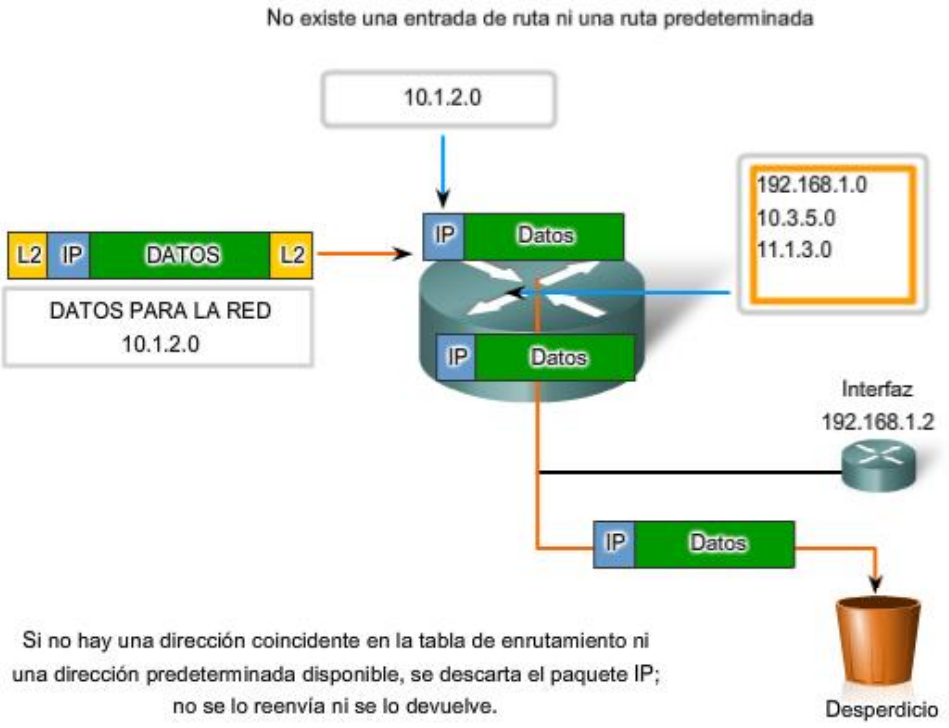
Las rutas default son importantes porque el router del gateway no siempre tiene una ruta a cada red posible en Internet. Si el paquete es reenviado usando una ruta default, eventualmente llegará a un router que tiene una ruta específica a la red de destino. Este router puede ser el router al cual esta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

Enlaces:

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



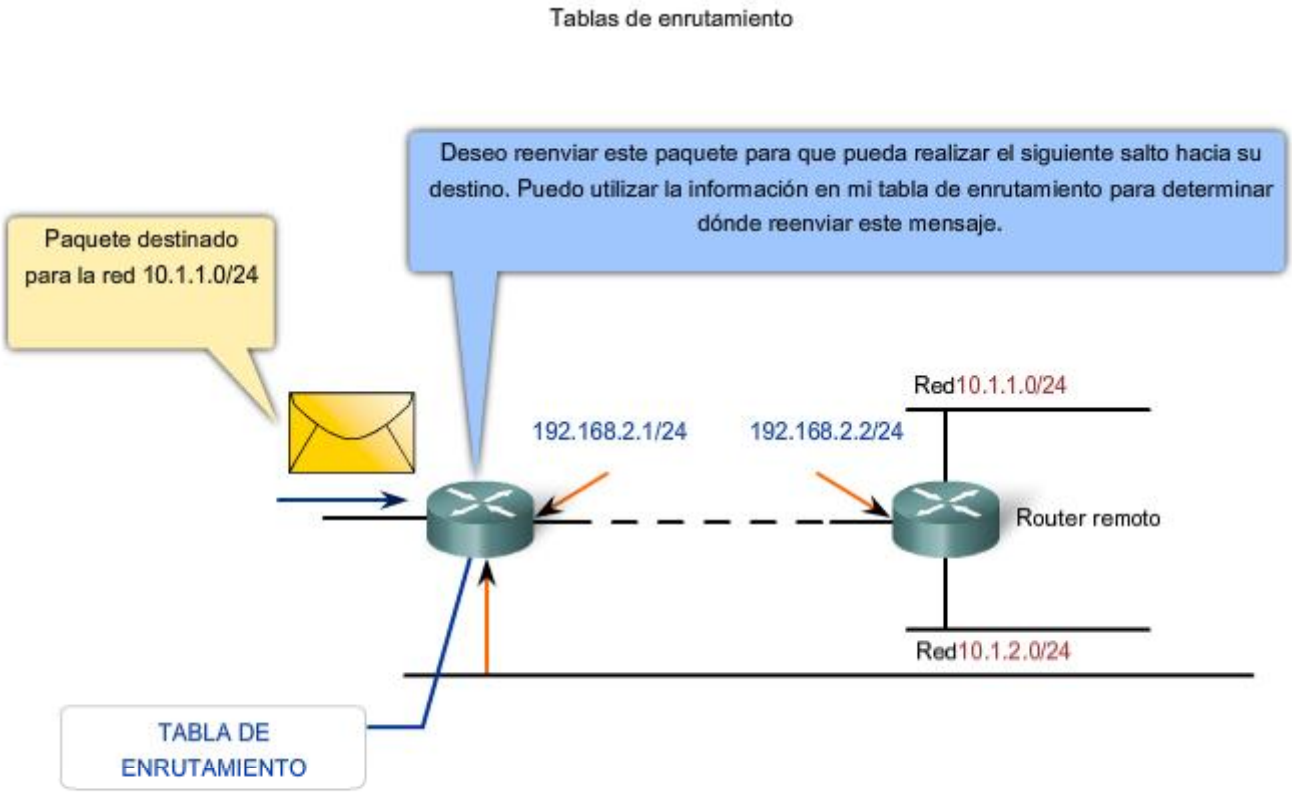
5.4 Procesos de enrutamiento: Cómo se aprenden las rutas

5.4.1 Protocolos de enrutamiento: Cómo compartir las 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.

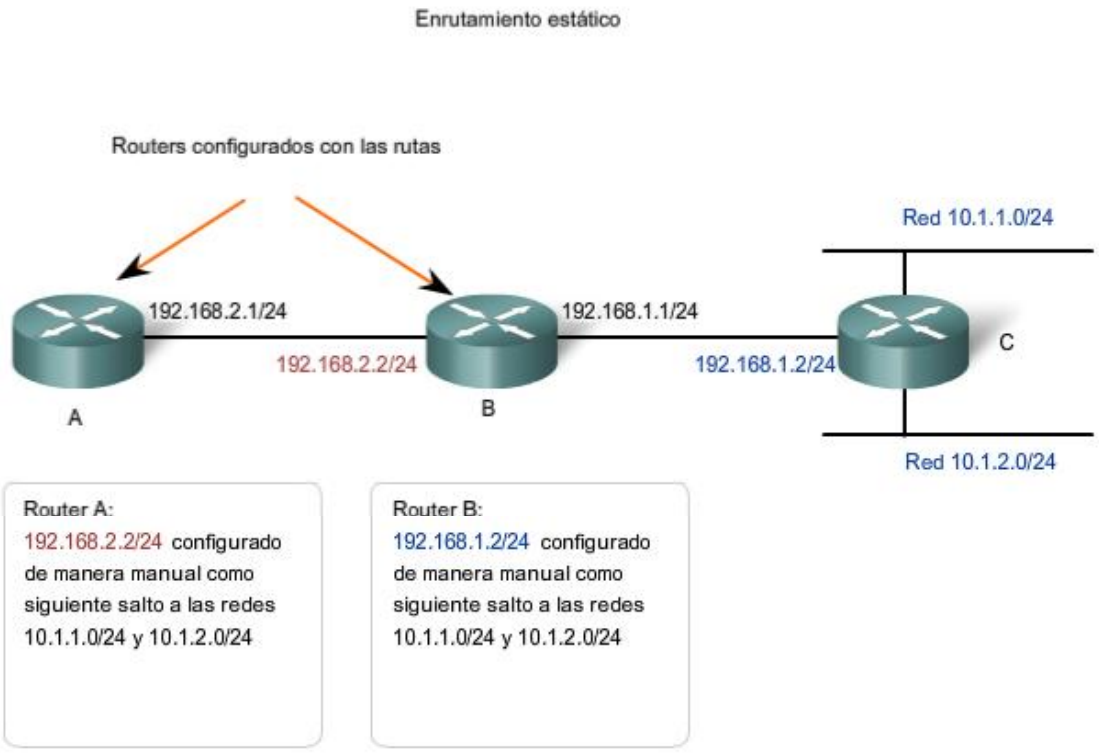


5.4.2 Enrutamiento estático

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.



5.4.2 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).

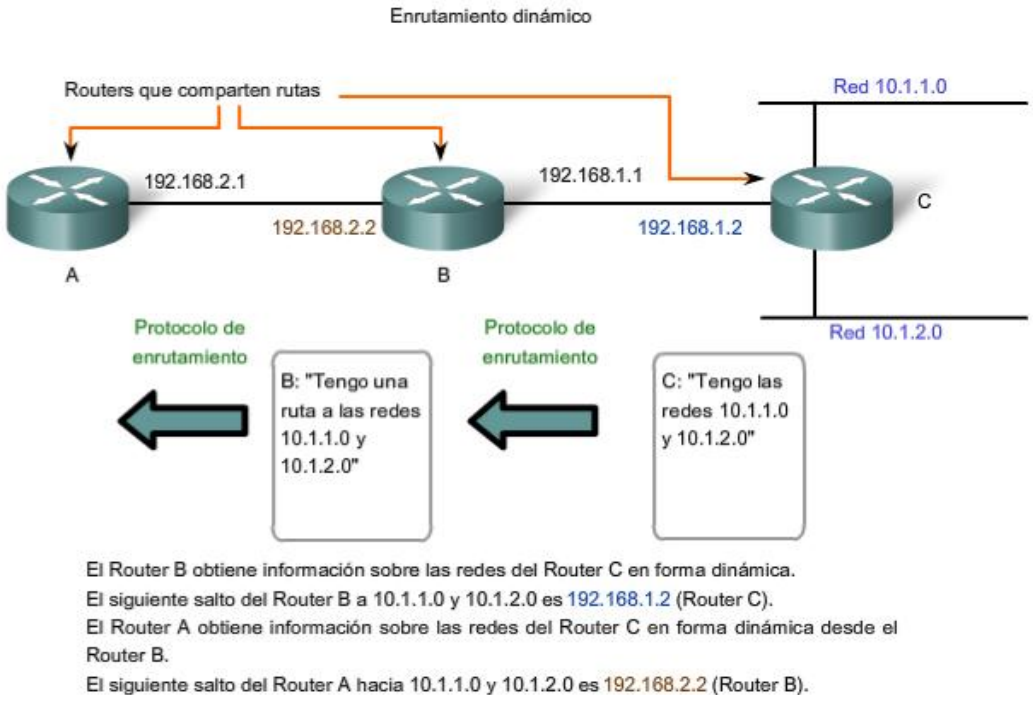
Aunque los protocolos de enrutamiento proveen routers con tablas de enrutamiento actualizadas, existen costos. Primero, el intercambio de la información de la ruta agrega una sobrecarga que consume el ancho de banda de la red. Esta sobrecarga puede ser un problema, particularmente para los enlaces del 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.

En muchas internetworks, la combinación de rutas estáticas, dinámicas y default se usa para proveer las rutas necesarias. La configuración de los protocolos de enrutamiento en routers es un componente integral del CCNA y será cubierta extensivamente en un curso posterior.

Enlaces;

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

Principios de enrutamiento http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm



El Router B obtiene información sobre las redes del Router C en forma dinámica.
El siguiente salto del Router B a 10.1.1.0 y 10.1.2.0 es 192.168.1.2 (Router C).
El Router A obtiene información sobre las redes del Router C en forma dinámica desde el Router B.
El siguiente salto del Router A hacia 10.1.1.0 y 10.1.2.0 es 192.168.2.2 (Router B).

5.6 Resumen

5.6.1 Resumen

El protocolo de capa de Red más significativo (Capa 3 de OSI) es el Protocolo de Internet (IP). La versión 4 (IPv4) de IP es el protocolo de capa de Red que se utilizará como ejemplo a lo largo de este curso.

El enrutamiento de IP de Capa 3 no garantiza una entrega confiable ni establece una conexión antes de transmitir los datos. Esta comunicación no confiable sin conexión es rápida y flexible, pero las capas superiores deben proveer mecanismos para garantizar la entrega de datos si se necesita.

La función de la capa de Red es llevar datos desde un host a otro sin tener en cuenta el tipo de datos. Los datos están encapsulados en un paquete. El encabezado del paquete tiene campos que incluyen la dirección de destino del paquete.

El direccionamiento jerárquico de la capa de Red con las porciones de red y host facilita la división de redes en subredes y permite el uso de la dirección de red para enviar paquetes hacia el destino en lugar de usar cada dirección de host individual.

Si la dirección de destino no está en la misma red como host de origen, el paquete pasa al gateway por defecto para ser enviado a la red de destino. El gateway es una interfaz de un router que analiza la dirección de destino. Si la red de destino tiene una entrada en su tabla de enrutamiento, el router envía el paquete ya sea a una red conectada o al gateway del siguiente salto. Si no hay entrada de enrutamiento, el router puede enviar el paquete a una ruta default o descartar el paquete.

Las entradas de la tabla de enrutamiento se pueden configurar manualmente en cada router para proveer enrutamiento estático, o los routers pueden comunicar la información de la ruta de manera dinámica entre ellos utilizando un protocolo de enrutamiento.

En este capítulo, aprendió a:

- Identificar la función de la capa de Red mientras describe la comunicación desde un dispositivo final hasta otro.
- Examinar el protocolo de capa de Red más común, el Internet Protocol (IP) y sus características para el suministro de un servicio sin conexión de mejor intento.
- Describir los principios utilizados para guiar la división o la agrupación de dispositivos en redes.
- Explicar la función del direccionamiento jerárquico de dispositivos y la forma en que éste permite la comunicación entre redes.
- Describir los aspectos básicos de las rutas, las direcciones de siguiente salto y el reenvío de paquetes a una red de destino.

CAPITULO 6 Direccionamiento de la red: IPv4

6.0 Introducción del capitulo
6.0.1 Introducción del capitulo

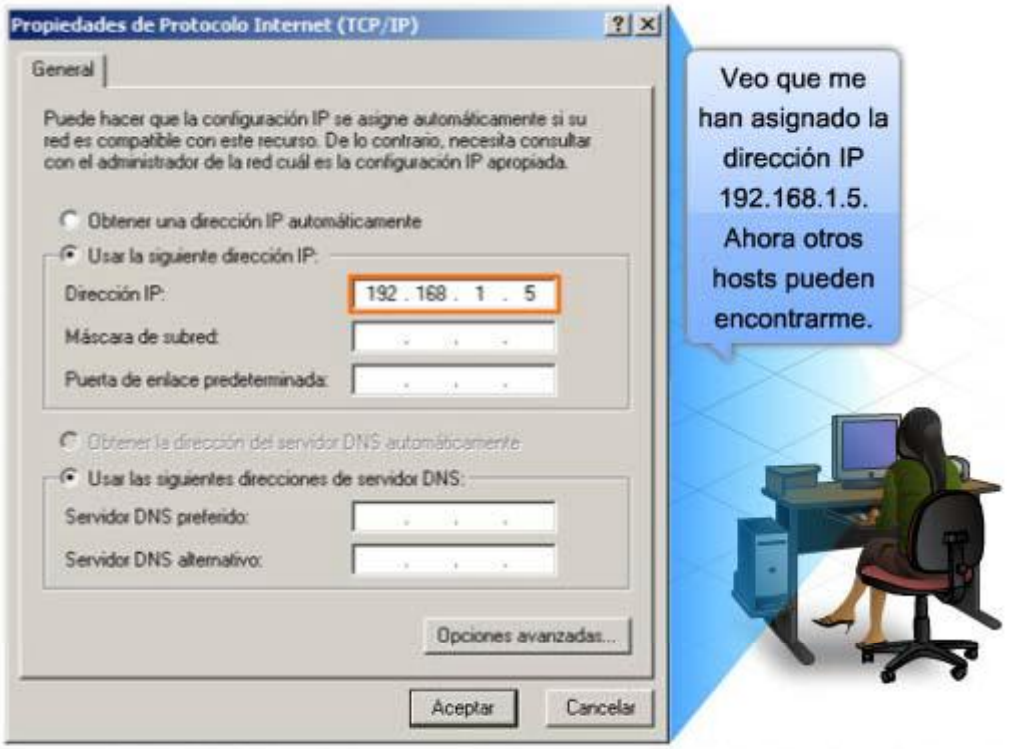
El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente.

Este capítulo examina detalladamente la estructura de las direcciones IPv4 y su aplicación en la construcción y prueba de redes y subredes IP.

En este capítulo, usted aprenderá a:

- Explicar la estructura del direccionamiento IP y a convertir entre números binarios de 8 bits y números decimales.
- Clasificar por tipo una dirección IPv4 y describir cómo se utiliza en la red.
- Explicar cómo las direcciones son asignadas a redes por los ISP y dentro de redes por los administradores.
- Determinar la porción de red de la dirección de host y explicar la función de la máscara de subred en la división de subredes.
- Calcular los componentes de direccionamiento adecuados de acuerdo con la información de la dirección IPv4 y los criterios de diseño.
- Usar las utilidades comunes de comprobación para verificar la conectividad de red y estado operativo de la stack de protocolo IP en un host.



La versión IP 4 (IPv4) es la forma actual de direccionamiento utilizada en Internet.

6.1 Direcciones IPv4
6.1.1 Estructura de una direccion IPv4

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes formamos parte de la red humana, una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteada.

Punto Decimal

Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

Por ejemplo: la dirección

10101100000100000000010000010100

es expresada en puntos decimales como

172.16.4.20

Tenga en cuenta que los dispositivos usan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

Porciones de red y de host

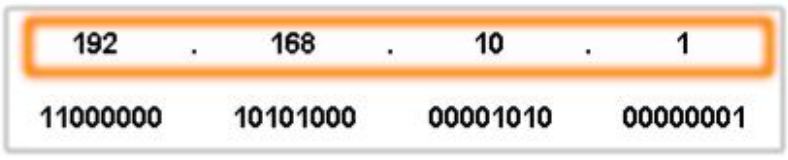
En cada dirección IPv4, alguna porción de los bits de orden superior representa la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones.

A pesar de que los 32 bits definen la dirección host IPv4, existe una cantidad variable de bits que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

Por ejemplo: si necesitamos tener al menos 200 hosts en una red determinada, necesitaríamos utilizar suficientes bits en la porción del host para poder representar al menos 200 patrones diferentes de bits.

Para asignar una dirección exclusiva a 200 hosts, se utilizará el último octeto entero. Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red.

Nota: Más adelante en este capítulo se verá cómo calcular la cantidad de hosts y cómo determinar qué porción de los 32 bits se refiere a la red.



La computadora que utiliza esta direcciP se encuentra en la red 192.168.10.0.

Direccin formato decimal punteado

Direccie 32 bits

Host

Octeto

Red

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

La computadora que utiliza esta direcciP se encuentra en la red 192.168.10.0.

Direccin formato decimal punteado

Direccie 32 bits

Host

Octeto

Red

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

La computadora que utiliza esta direcciP se encuentra en la red 192.168.10.0.

Direccin formato decimal punteado

Direccie 32 bits

Host

Octeto

Red

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

La computadora que utiliza esta direcciP se encuentra en la red 192.168.10.0.

Direccin formato decimal punteado

Direccie 32 bits

Host

Octeto

Red

192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

La computadora que utiliza esta direcciP se encuentra en la red 192.168.10.0.

Direccin formato decimal punteado

Direccie 32 bits

Host

Octeto

Red

6.1.2 Conocer los numeros: conversión de binario en decimal

Para comprender el funcionamiento de un dispositivo en una red, es necesario considerar las direcciones y otros datos de la manera en que lo hace un dispositivo: en notación binaria. Esto significa que es necesario ser hábil en la conversión de binario en decimal.

Los datos representados en el sistema binario pueden representar muchas formas diferentes de datos en la red humana. En este tema, se hace referencia al sistema binario por estar relacionado con el direccionamiento IPv4. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255.

Notación de posición

El Aprendizaje de la notación de posición para convertir binario a decimal requiere una comprensión de los fundamentos matemáticos de un sistema de numeración llamado notación de posición. Notación de posición significa que un dígito representa diferentes valores según la posición que ocupa. Más específicamente, el valor que un dígito representa es el valor multiplicado por la potencia de la base o raíz representado por la posición que el dígito ocupa. Algunos ejemplo ayudarán a aclarar cómo funciona este sistema.

Para el número decimal 245, el valor que el 2 representa es 2*10^2 (2 multiplicado por 10 elevado a la segunda potencia). El 2 se encuentra en lo que comúnmente llamamos la posición "100". Notación de posición se refiere a esta posición como posición base^2 porque la base o raíz es 10 y la potencia es 2.

Usando la notación de posición en el sistema de numeración con base 10, 245 representa:

245 = (2 * 10^2) + (4 * 10^1) + (5 * 10^0)

o

245 = (2 * 100) + (4 * 10) + (5 * 1)

Sistema de numeración binaria

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa potencias incrementadas de 2. En números binarios de 8 bits, las posiciones representan estas cantidades:

2^7 2^62^5 2^4 2^32^2 2^1 2^0

128 64 32 16 8 4 2 1

El sistema de numeración de base 2 tiene solamente dos dígitos: **0 y 1**.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esa posición representa si el dígito es 1 y no se obtiene la cantidad si el dígito es **0**, como se muestra en la figura.

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1

Un **1** en cada posición significa que el valor para esa posición se suma al total. Ésta es la suma cuando hay un 1 en cada posición de un octeto. El total es 255.

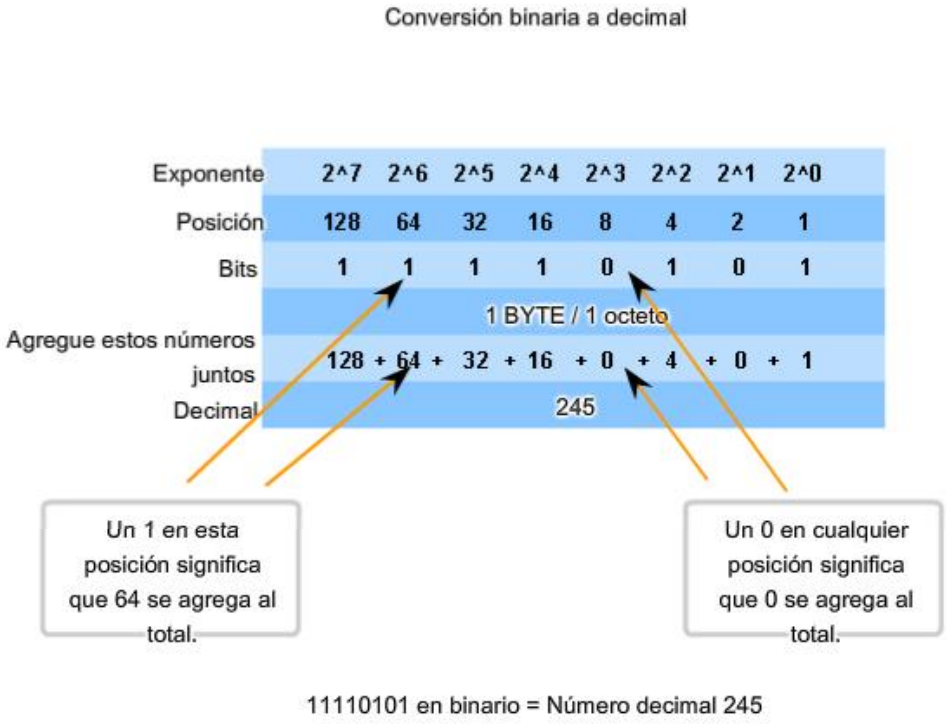
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Un **0** en cada posición indica que el valor para esa posición no se suma al total. Un **0** en cada posición produce un total de 0.

0 0 0 0 0 0 0 0

128 64 32 16 8 4 2 1
0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

Note en la figura que una combinación diferente de unos y ceros producirá un valor decimal diferente.



Observe la figura para obtener los pasos para convertir una dirección binaria en una dirección decimal.

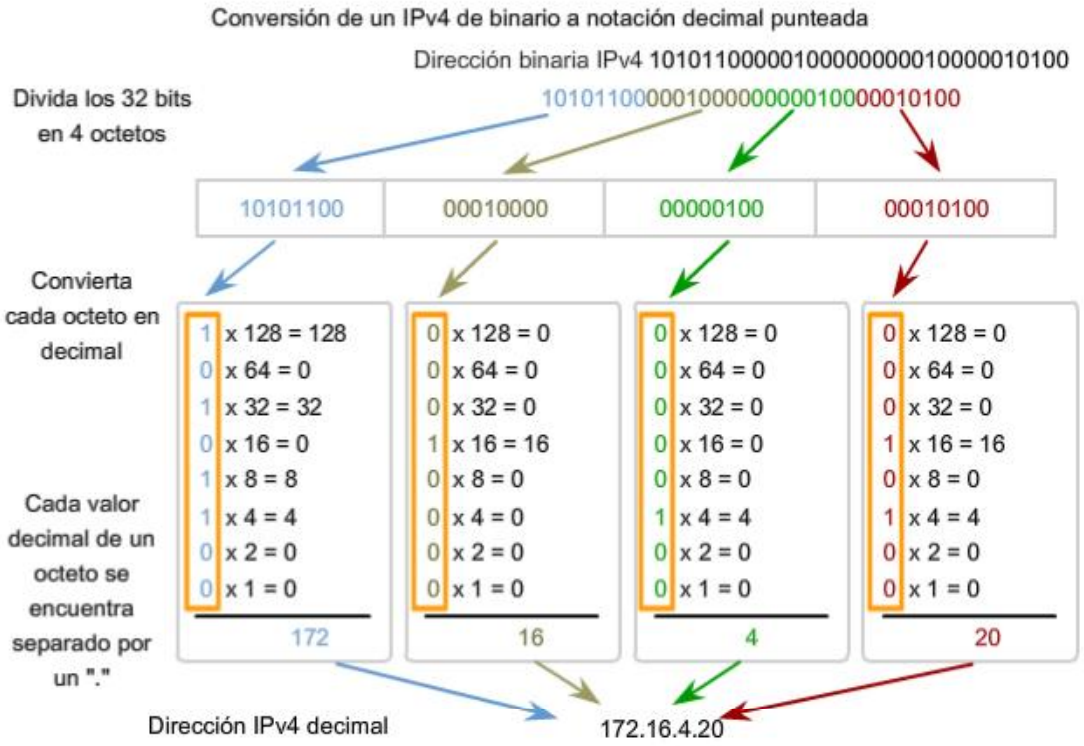
En el ejemplo, el número binario:

10101100000100000000010000010100

se convierte en:

172.16.4.20

Tenga en cuenta estos pasos:
Divida los 32 bits en 4 octetos.
Convierta cada octeto a decimal.
Agregue un "punto" entre cada decimal.



6.1.4 Conocer los numeros: conversión de decimal a binario

No sólo es necesario poder realizar una conversión de binario en decimal, sino que también es necesario poder realizar una conversión de decimal en binario. Con frecuencia es necesario examinar un octeto individual de una dirección que se proporciona en notación decimal punteada. Tal es el caso cuando los bits de red y los bits de host dividen un octeto.

Por ejemplo: si un host 172.16.4.20 utilizara 28 bits para la dirección de red, sería necesario examinar los datos binarios del último octeto para descubrir que este host está en la red 172.16.4.16. Este proceso de extraer la dirección de red de una dirección de host se explicará más adelante.

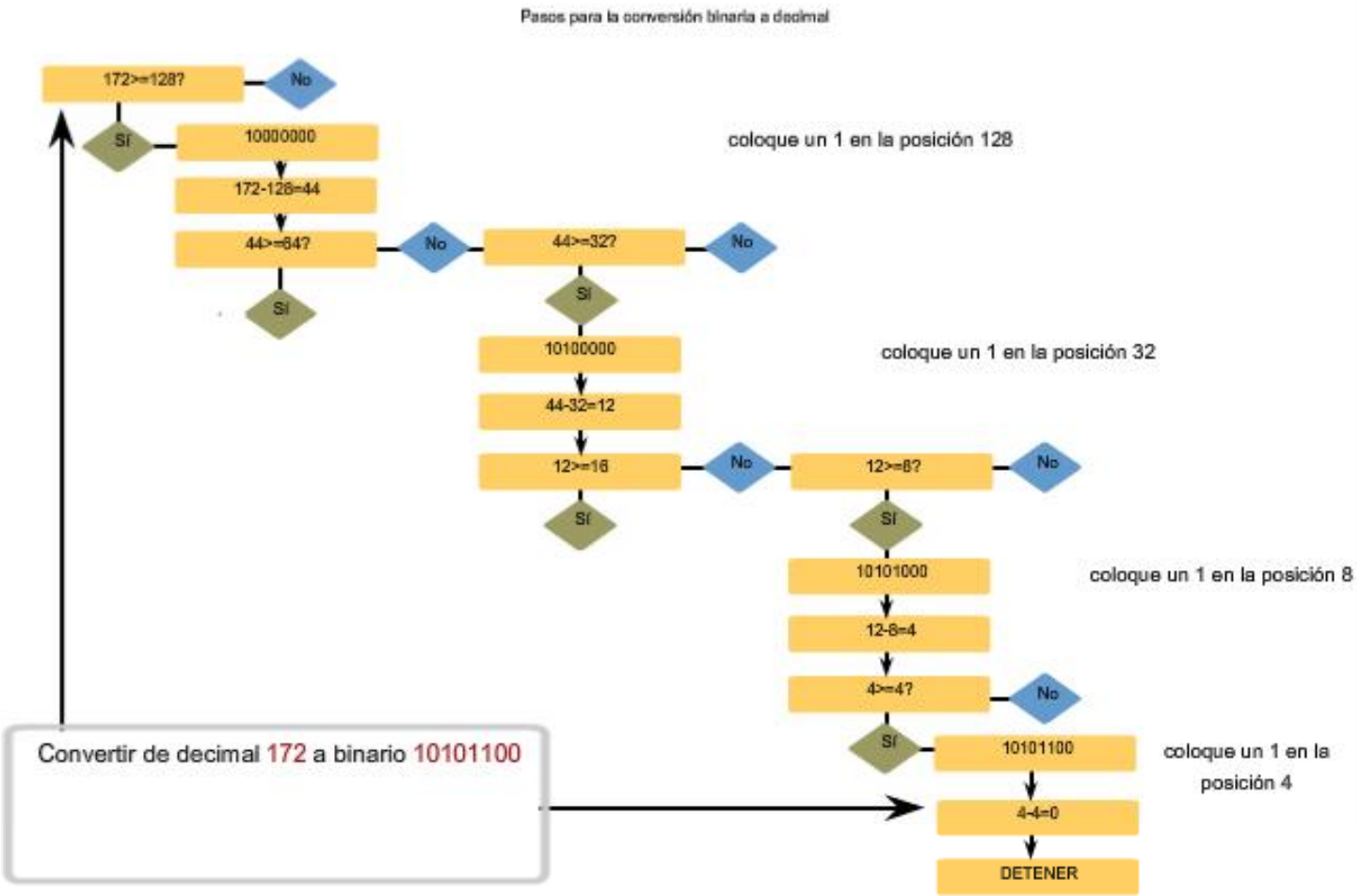
Los valores de la dirección están entre 0 y 255

Examinaremos sólo el proceso de conversión binaria de 8 bits a valores decimales de 0 a 255, porque nuestra representación de direcciones está limitada a valores decimales para un solo octeto.

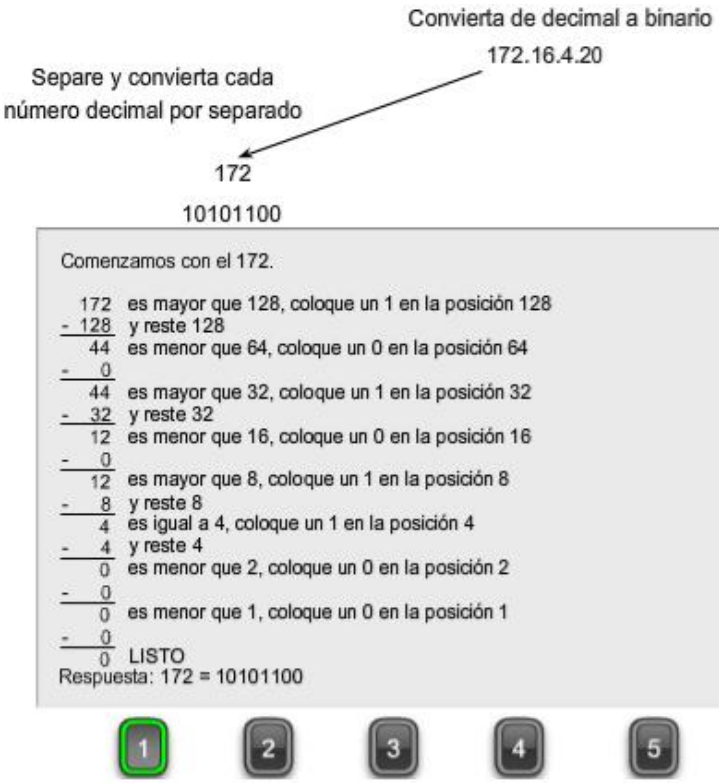
Para comenzar el proceso de conversión, empezaremos determinando si el número decimal es igual a o mayor que nuestro valor decimal más grande representado por el bit más significativo. En la posición más alta, se determina si el valor es igual o mayor que 128. Si el valor es menor que 128, se coloca un 0 en la posición de 128 bits y se mueve a la posición de 64 bits.

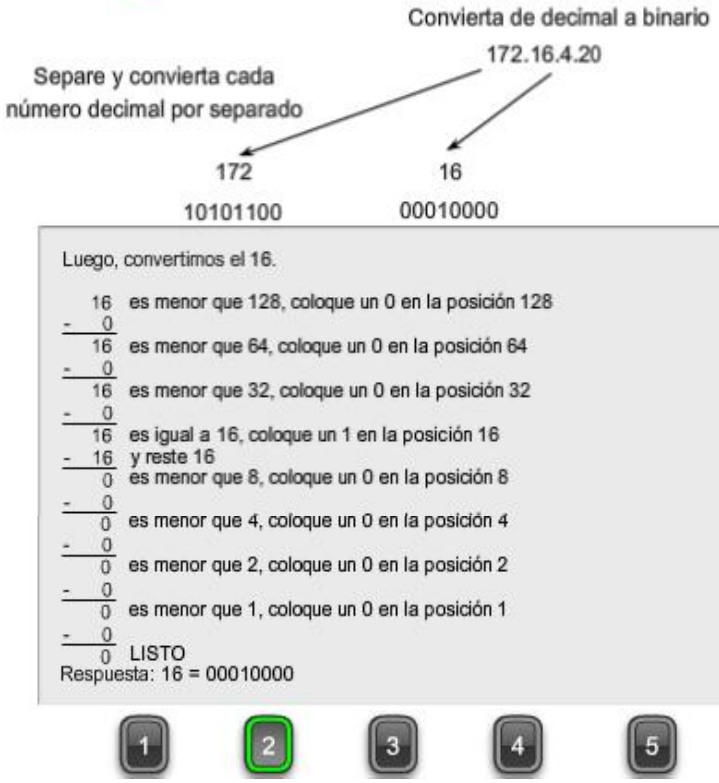
Si el valor en la posición de 128 bits es mayor o igual que 128, se coloca un 1 en la posición 128 y se resta 128 del número que se está convirtiendo. Luego se comparan los valores restantes de esta operación con el siguiente valor más pequeño, 64. Se continúa con este proceso para todas las posiciones de bits restantes.

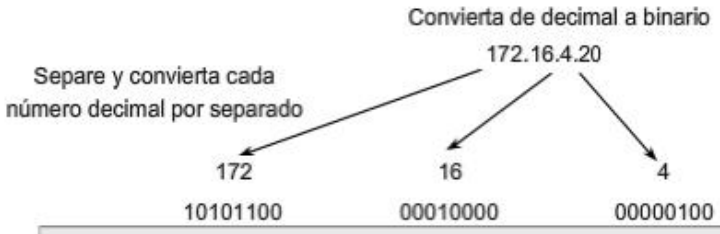
Ver la figura para obtener un ejemplo de estos pasos. Se convierte 172 en 10101100.



Siga los pasos de conversión para conocer cómo se convierte una dirección IP en binaria.





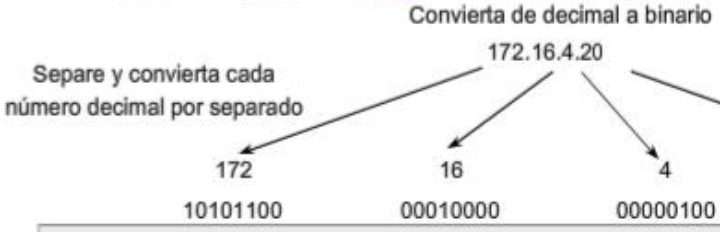


Luego, convertimos el 4.

4 es menor que 128, coloque un 0 en la posición 128
- 0
4 es menor que 64, coloque un 0 en la posición 64
- 0
4 es menor que 32, coloque un 0 en la posición 32
- 0
4 es menor que 16, coloque un 0 en la posición 16
- 0
4 es menor que 8, coloque un 0 en la posición 8
- 0
4 es igual a 4, coloque un 1 en la posición 4
- 4 y reste 4
0 es menor que 2, coloque un 0 en la posición 2
- 0
0 es menor que 1, coloque un 0 en la posición 1
- 0
0 LISTO

Respuesta: 4 = 00000100

1 2 3 4 5

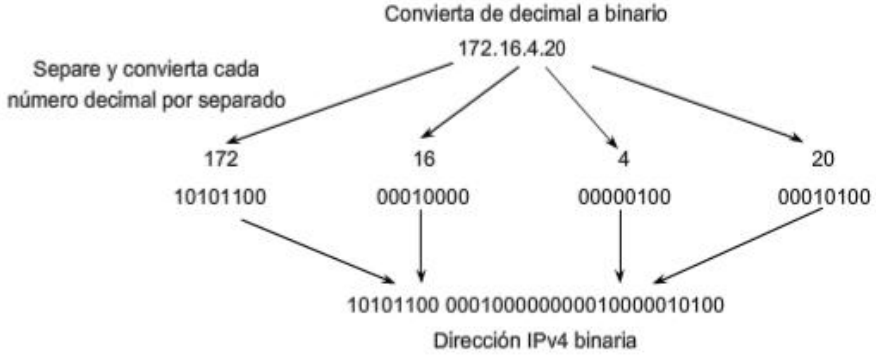


Finalmente, convertimos el 20.

20 es menor que 128, coloque un 0 en la posición 128
- 0
20 es menor que 64, coloque un 0 en la posición 64
- 0
20 es menor que 32, coloque un 0 en la posición 32
- 0
20 es mayor que 16, coloque un 1 en la posición 16
- 16 y reste 16
4 es menor que 8, coloque un 0 en la posición 8
- 0
4 es igual a 4, coloque un 1 en la posición 4
- 4 y reste 4
0 es menor que 2, coloque un 0 en la posición 2
- 0
0 es menor que 1, coloque un 0 en la posición 1
- 0
0 LISTO

Respuesta: 20 = 00010100

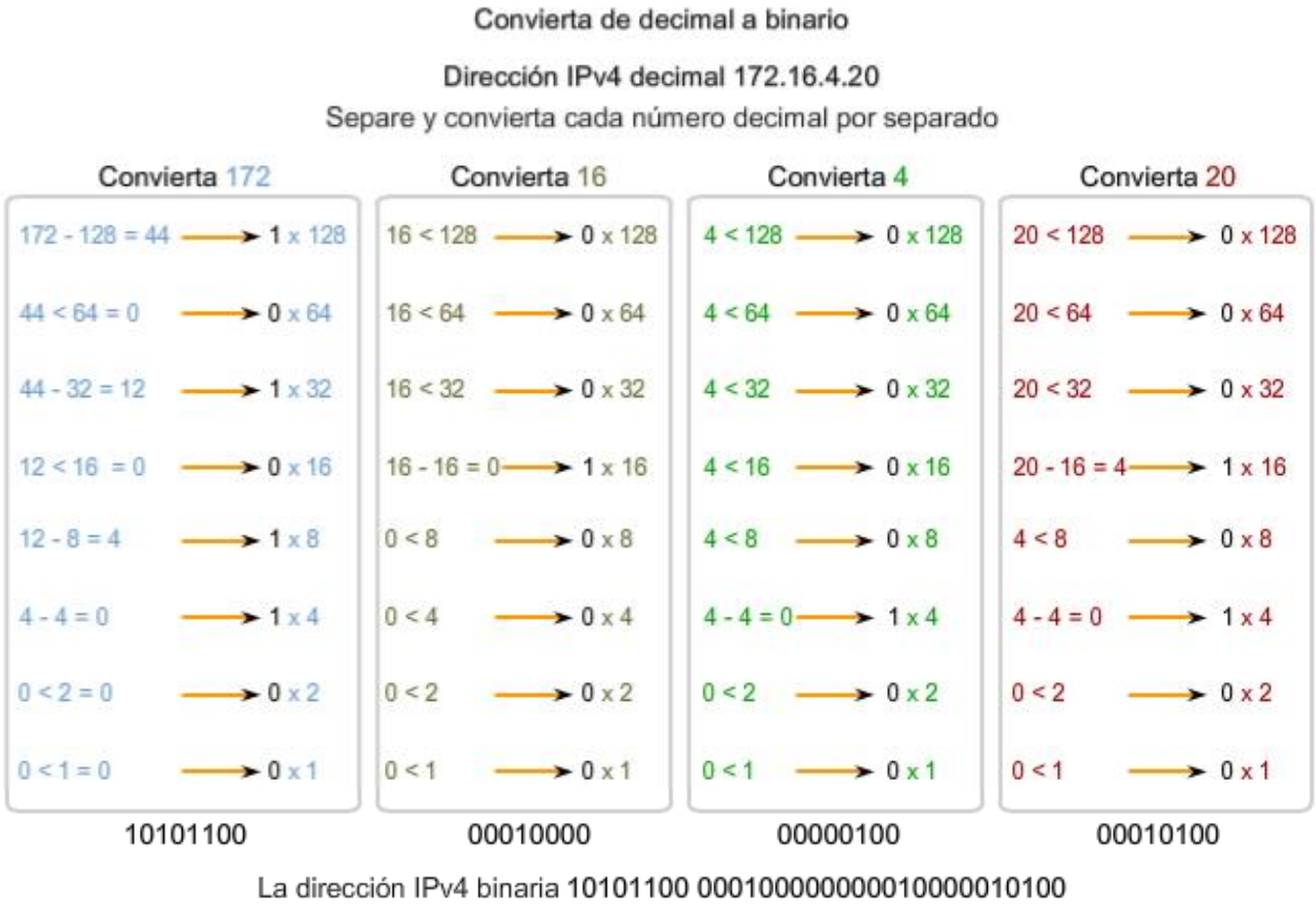
1 2 3 4 5



1 2 3 4 5

Resumen de conversión

La figura resume la conversión completa de 172.16.4.20 de notación decimal punteada a notación binaria.



6.2 Direcciones para diferentes propósitos

6.2.1 Tipos de direcciones en una red IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

Dirección de red: la dirección en la que se hace referencia a la red.

Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.

Direcciones host: las direcciones asignadas a los dispositivos finales de la red.

Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como "red 10.0.0.0". Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

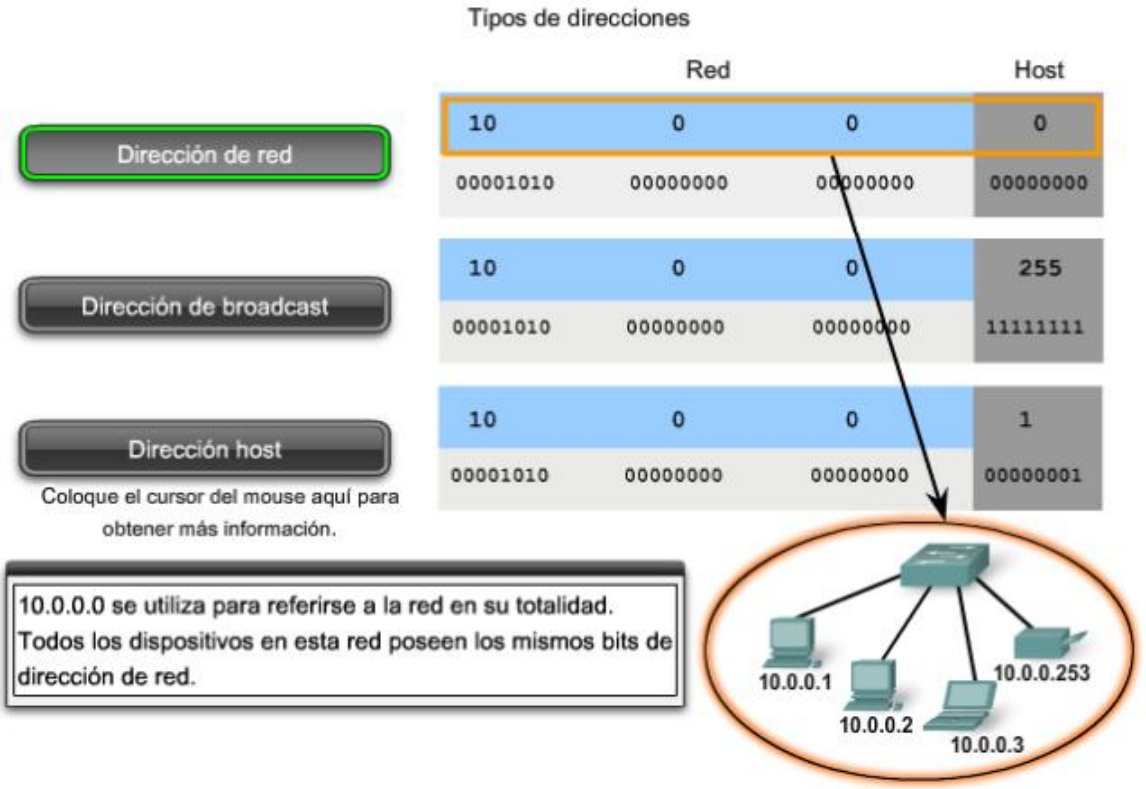
Dirección de broadcast

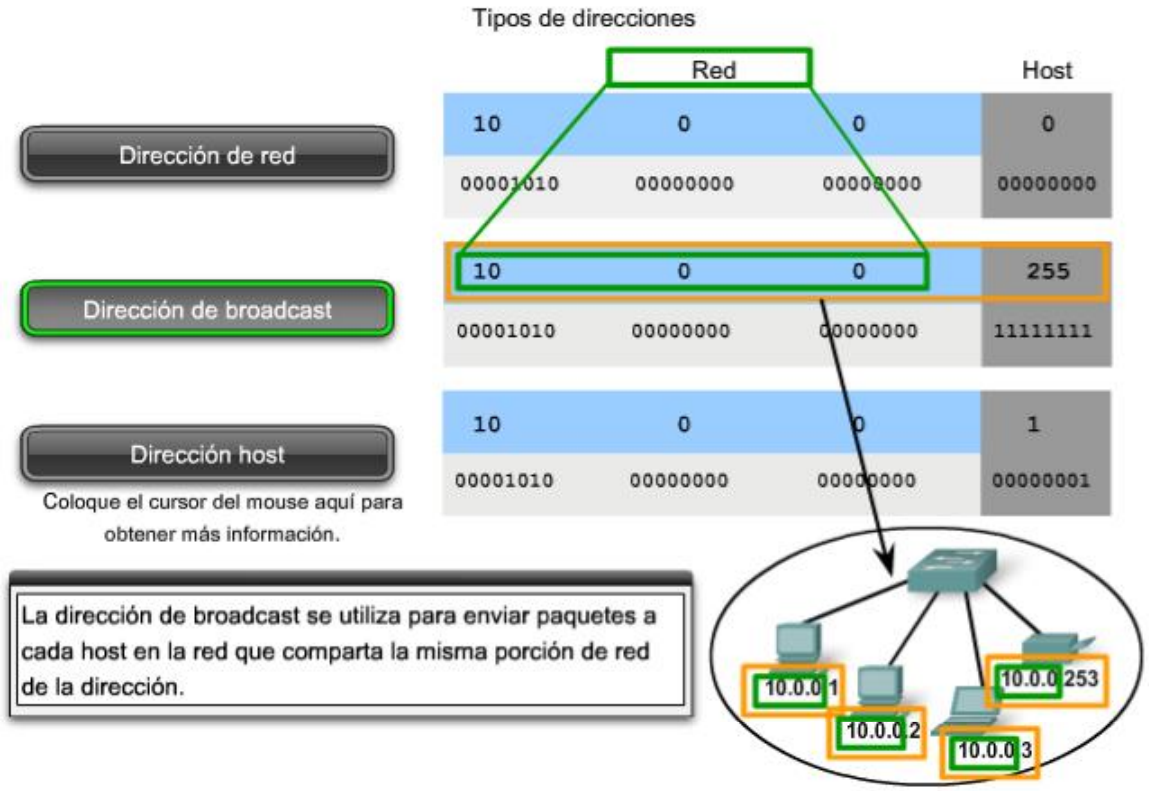
La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

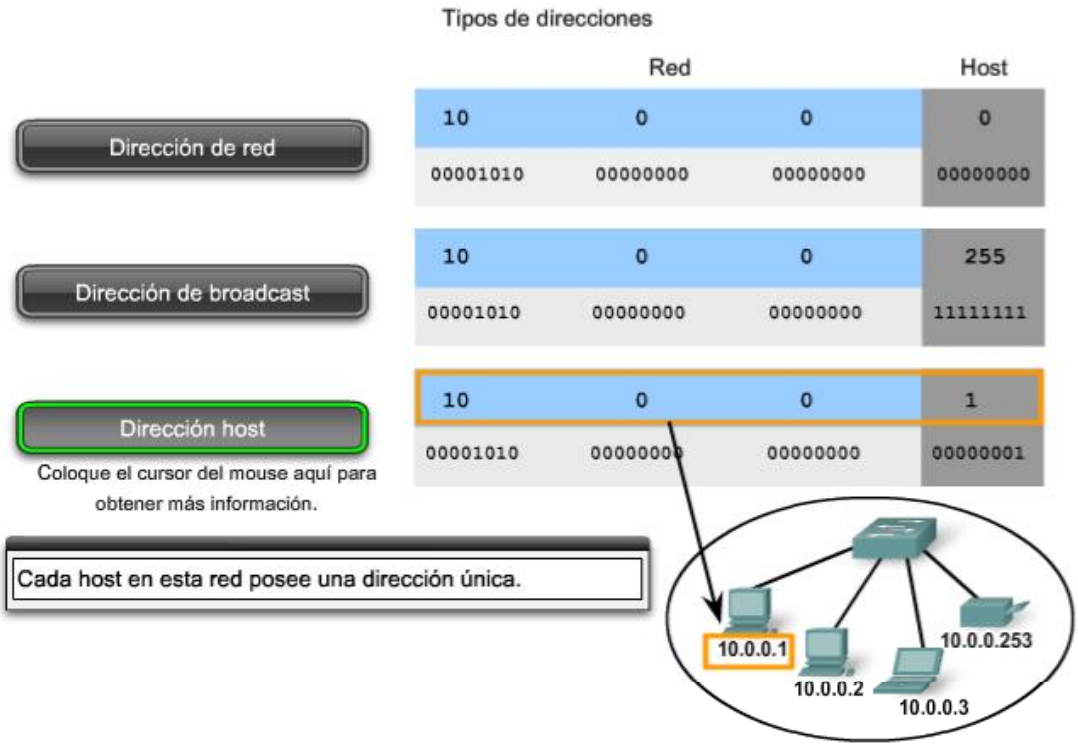
La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido.

Direcciones host

Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.







Prefijos de red

Una pregunta importante es: ¿Cómo es posible saber cuántos bits representan la porción de red y cuántos bits representan la porción de host? Al expresar una dirección de red IPv4, se agrega una longitud de prefijo a la dirección de red. La longitud de prefijo es la cantidad de bits en la dirección que conforma la porción de red. Por ejemplo: en 172.16.4.0 /24, /24 es la lobgitud de prefijo e indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host. Más adelante en este capítulo, el usuario aprenderá más acerca de otra entidad que se utiliza para especificar la porción de red de una dirección IPv4 en los dispositivos de red. Se llama máscara de subred. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza unos y ceros para indicar cuáles bits de la dirección son bits de red y cuáles bits son bits de host.

No siempre a las redes se le asigna un prefijo /24. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes longitudes de prefijos. En esta figura puede ver también que el número de hosts que puede ser direccionado a la red también cambia.

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
Representación binaria 24 bits de red	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.11111110	10101100.00010000.00000100.11111111
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

254 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
Representación binaria 25 bits de red	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.01111110	10101100.00010000.00000100.01111111
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

126 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
Representación binaria 26 bits de red	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.00111110	10101100.00010000.00000100.00111111
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

62 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31
Representación binaria 27 bits de red	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.00011110	10101100.00010000.00000100.00011111

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

30 hosts

6.2.2 Cálculo de direcciones de host, de red y de broadcast

Hasta ahora, el usuario podría preguntarse: ¿Cómo se calculan estas direcciones? Este proceso de cálculo requiere que el usuario considere estas direcciones como binarias.

En las divisiones de red de ejemplo, se debe considerar el octeto de la dirección donde el prefijo divide la porción de red de la porción de host. En todos estos ejemplos, es el último octeto. A pesar de que esto es frecuente, el prefijo también puede dividir cualquiera de los octetos.

Para comenzar a comprender este proceso para determinar asignaciones de dirección, se desglosarán algunos ejemplos en datos binarios.

Observe la figura para obtener un ejemplo de la asignación de dirección para la red 172.16.20.0 /25.

En el primer cuadro, se encuentra la representación de la dirección de red. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la dirección de red, todos estos bits de host son "0". Esto hace que el último octeto de la dirección sea 0. De esta forma, la dirección de red es 172.16.20.0 /25.

En el segundo cuadro, se observa el cálculo de la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.

El tercer cuadro muestra el cálculo de la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

El cuarto cuadro representa el cálculo de la dirección host más alta. La dirección host más alta de una red es siempre un número menor que la dirección de broadcast. Esto significa que el bit más bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

A pesar de que para este ejemplo se ampliaron todos los octetos, sólo es necesario examinar el contenido del octeto dividido.

6.2.3 Unicast, broadcast, multicast: tipos de comunicación

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

Unicast: el proceso por el cual se envía un paquete de un host a un host individual.

Broadcast: el proceso por el cual se envía un paquete de un host a todos los hosts de la red.

Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

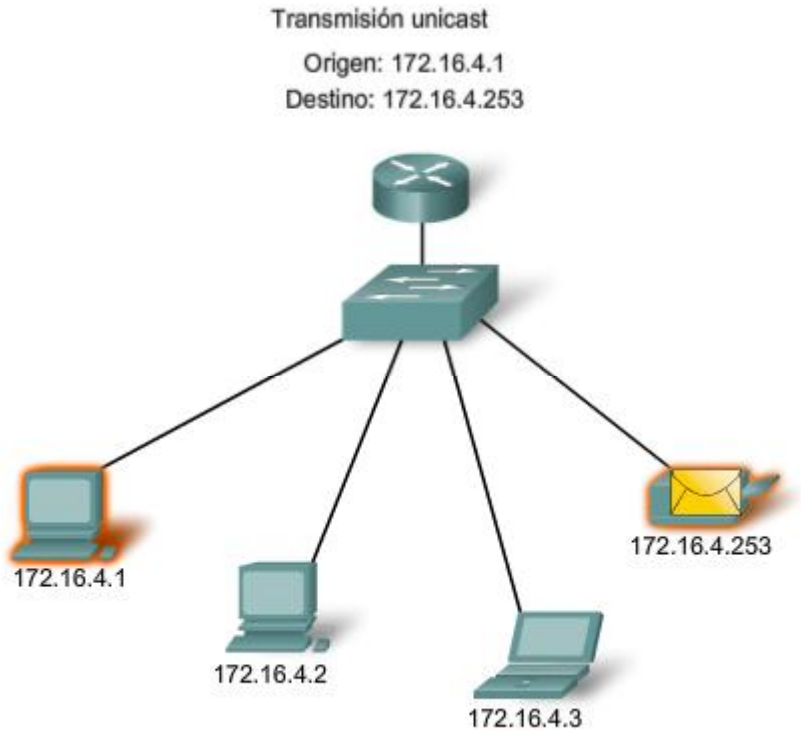
Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internetwork.

En una red IPv4, a la dirección unicast aplicada a un dispositivo final se le denomina dirección de host. En la comunicación unicast, las direcciones host asignadas a dos dispositivos finales se usan como direcciones IPv4 de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección host de origen y la dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino. Es posible enviar la comunicación utilizando un paquete unicast por medio de una internetwork con las mismas direcciones.

Nota: En este curso, todas las comunicaciones entre dispositivos son comunicaciones unicast a menos que se indique lo contrario.



Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

La transmisión de broadcast se usa para ubicar servicios/dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe brindar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior

- Solicitar una dirección
- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast.

De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente están restringidos a la red local. Esta restricción depende de la configuración del router que bordea la red y del tipo de broadcast. Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

Broadcast dirigido

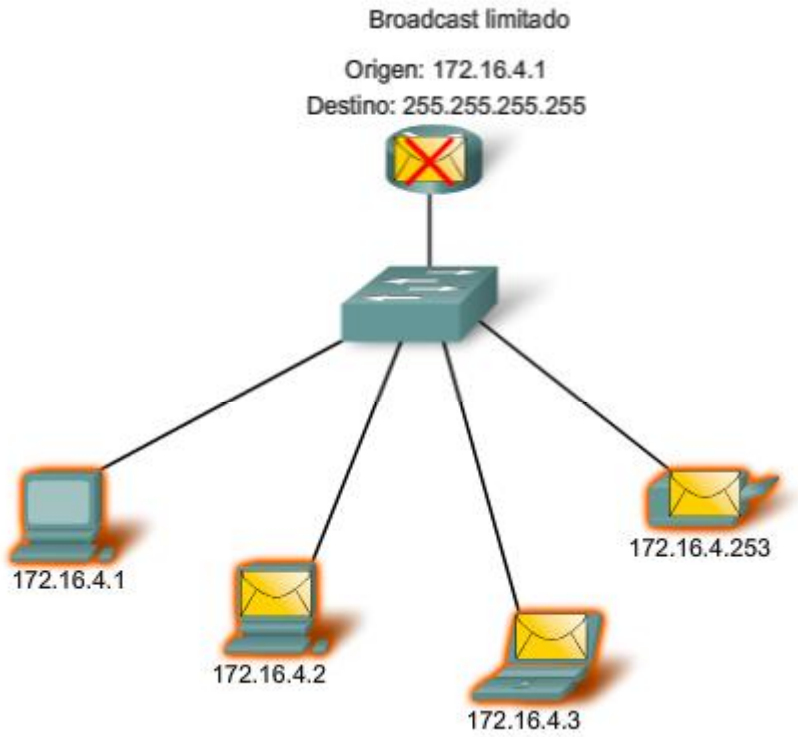
Se envía un broadcast dirigido a todos los hosts en una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local. Por ejemplo: para que un host fuera de la red se comunique con los hosts dentro de la red 172.16.4.0 /24, la dirección de destino del paquete sería 172.16.4.255. Esto se muestra en la figura. Aunque los routers no envían broadcasts dirigidos por defecto, se los puede configurar para que lo hagan.

Broadcast limitado

El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino 255.255.255.255. Los routers no envían estos broadcasts. Los paquetes dirigidos a la dirección de broadcast limitada sólo aparecerán en la red local. Por esta razón, también se hace referencia a una red IPv4 como un dominio de broadcast. Los routers son dispositivos fronterizos para un dominio de broadcast.

A modo de ejemplo, un host dentro de la red 172.16.4.0 /24 transmitiría a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

Como se mostró anteriormente, cuando se transmite un paquete, éste utiliza recursos de la red y de esta manera obliga a cada host de la red que lo recibe a procesar el paquete. Por lo tanto, el tráfico de broadcast debe limitarse para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan dominios de broadcast, subdividir las redes con tráfico de broadcast excesivo puede mejorar el rendimiento de la red.



Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino.

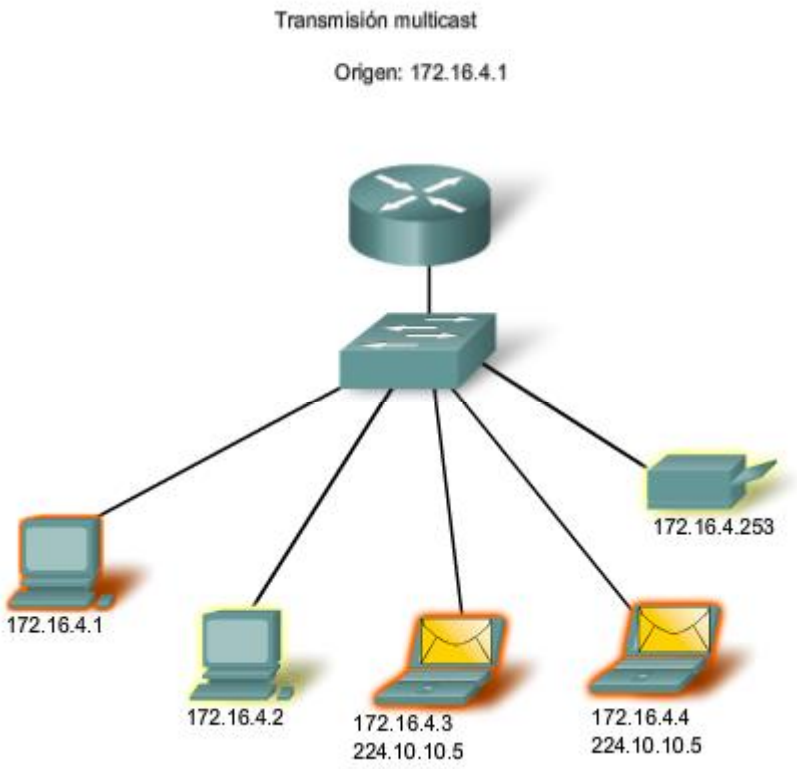
Algunos ejemplos de transmisión de multicast son:

- Distribución de audio y video
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
- Distribución de software
- Suministro de noticias

Clientes Multicast

Los hosts que desean recibir datos multicast específicos se denominan clientes multicast. Los clientes multicast usan servicios iniciados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast exclusivamente asignada. Como se puede ver, IPv4 ha apartado un bloque especial de direcciones desde 224.0.0.0 a 239.255.255.255 para direccionamiento de grupos multicast.



6.2.4 Rango de direcciones IPv4 Reservadas

Expresado en formato decimal punteado, el rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255. Como se pudo observar anteriormente, no todas estas direcciones pueden usarse como direcciones host para la comunicación unicast.

Direcciones experimentales

Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 experimentales de 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones se mencionan como reservadas para uso futuro (RFC 3330). Esto sugiere que podrían convertirse en direcciones utilizables. En la actualidad, no es posible utilizarlas en redes IPv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

Direcciones multicast

Como se mostró antes, otro bloque importante de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 multicast de 224.0.0.0 a 239.255.255.255. Además, el rango de direcciones multicast se subdivide en diferentes tipos de direcciones: direcciones de enlace locales reservadas y direcciones agrupadas globalmente. Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de alcance limitado.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones reservadas de enlace local. Estas direcciones se utilizarán con grupos multicast en una red local. Los paquetes enviados a estos destinos siempre se transmiten con un valor de período de vida (TTL) de 1. Por lo tanto, un router conectado a la red local nunca debería enviarlos. Un uso común de direcciones de enlace local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones de alcance global son de 224.0.1.0 a 238.255.255.255. Se las puede usar para transmitir datos en Internet mediante multicast. Por ejemplo: 224.0.1.1 ha sido reservada para el Protocolo de hora de red (NTP) para sincronizar los relojes con la hora del día de los dispositivos de la red.

Direcciones host

Después de explicar los rangos reservados para las direcciones experimentales y las direcciones multicast, queda el rango de direcciones de 0.0.0.0 a 223.255.255.255 que podría usarse con hosts IPv4. Sin embargo, dentro de este rango existen muchas direcciones que ya están reservadas con objetivos específicos. A pesar de que se han tratado algunas de estas direcciones anteriormente, las principales direcciones reservadas se tratan en la próxima sección.

Rangos de direcciones IPv4 reservadas

Tipo de dirección	Uso	Rango de direcciones IPv4 reservadas	RFC
Dirección host	utilizada en hosts IPv4	De 0.0.0.0 a 223.255.255.255	790
Dirección multicast	utilizada en grupos multicast en una red local	De 224.0.0.0 a 239.255.255.255	1700
Direcciones experimentales	• utilizada para investigación o experimentación • actualmente no se puede utilizar para los hosts en las redes IPv4	De 240.0.0.0 a 255.255.255.254	1700 3330

6.2.5 Direcciones públicas y privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. A estas direcciones se las denomina direcciones privadas.

Direcciones privadas

Los bloques de direcciones privadas son:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

Los bloques de direcciones de espacio privadas, como se muestra en la figura, se separa para utilizar en redes privadas. No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas. **Por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones.** Sin embargo, las redes internas aún deben diseñar esquemas de direcciones de red para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de networking.

Muchos hosts en diferentes redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública. El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a hacerse camino hacia Internet, los routers no tendrían rutas para enviarlos a la red privada correcta.

Traducción de direcciones de red (NAT)

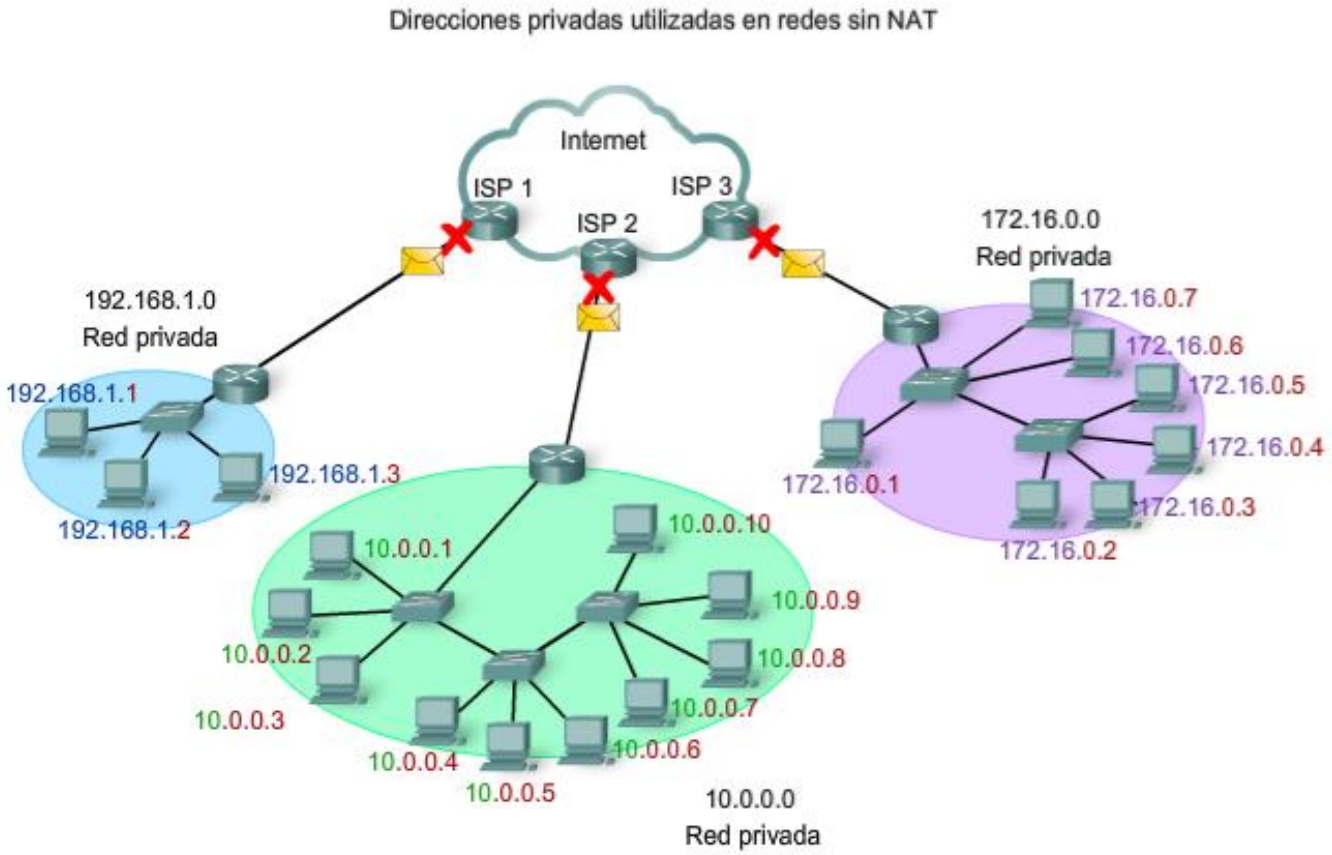
Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

NAT permite a los hosts de la red "pedir prestada" una dirección pública para comunicarse con redes externas. A pesar de que existen algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

Nota: NAT será tratado en detalle en un curso posterior.

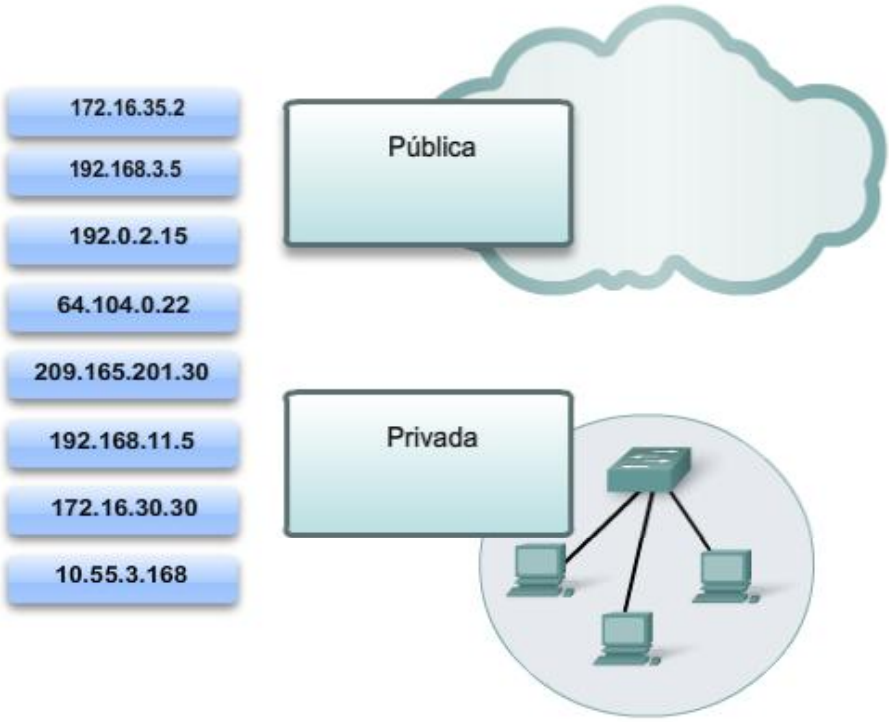
Direcciones públicas

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos.



Actividad

En esta actividad de la figura, arrastre las direcciones IP y suéltelas dentro de la categoría correcta Pública o Privada.



6.2.6 Direcciones IPv4 especiales

Hay determinadas direcciones que no pueden ser asignadas a los hosts por varios motivos. También hay direcciones especiales que pueden ser asignadas a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

Direcciones de red y de broadcast

Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son la dirección de red y la dirección de broadcast, respectivamente.

Ruta predeterminada

También anteriormente presentada, se representa la ruta predeterminada IPv4 como 0.0.0.0. La ruta predeterminada se usa como ruta "comodín" cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

Loopback

Una de estas direcciones reservadas es la dirección IPv4 de loopback 127.0.0.1. **La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos**. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back dentro del host local. Ni siquiera debe aparecer ninguna dirección en ninguna red dentro de este bloque.

Direcciones de enlace local

Las direcciones IPv4 del bloque de direcciones de 169.254.0.0 a 169.254.255.255 (169.254.0.0 /16) son designadas como direcciones de enlace local. **El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP**. Éstas pueden usarse en una pequeña red punto a

punto o con un host que no podría obtener automáticamente una dirección de un servidor de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host, DHCP).

La comunicación mediante direcciones de enlace local IPv4 sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red, como se muestra en la figura. Un host no debe enviar un paquete con una dirección de destino de enlace local IPv4 a ningún router para ser enviado, y debería establecer el TTL de IPv4 para estos paquetes en 1.

Las direcciones de enlace local no ofrecen servicios fuera de la red local. Sin embargo, muchas aplicaciones de cliente/servidor y punto a punto funcionarán correctamente con direcciones de enlace local IPv4.

Direcciones TEST-NET

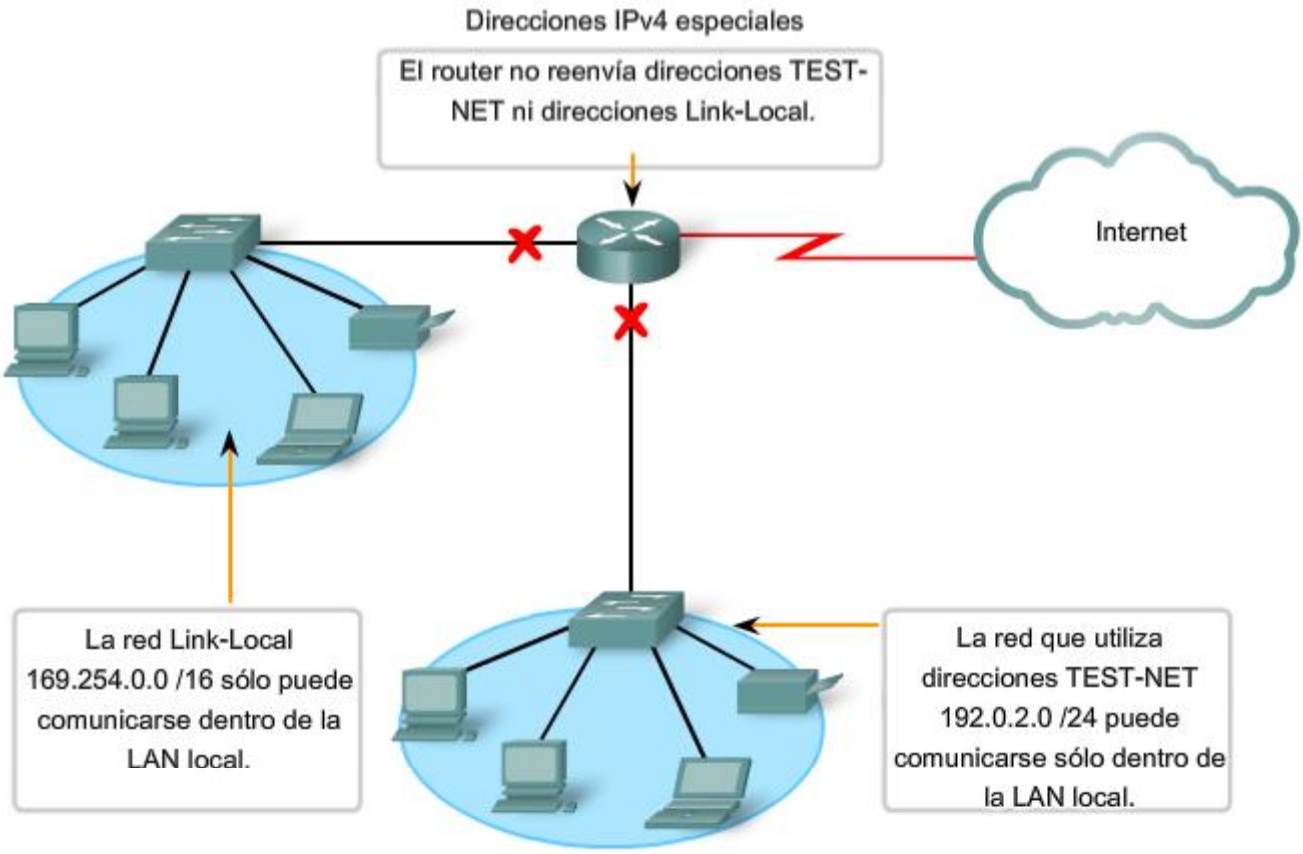
Se establece el bloque de direcciones de 192.0.2.0 a 192.0.2.255 (192.0.2.0 /24) para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. **A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración**. A menudo puede encontrar que estas direcciones se usan con los nombres de dominio example.com o example.net en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

Enlaces:

Direcciones de enlace local http://www.ietf.org/rfc/rfc3927.txt?number=3927

Direcciones IPv4 de uso especialhttp://www.ietf.org/rfc/rfc3330.txt?number=3330

Ubicación multicast: http://www.iana.org/assignments/multicast-addresses



6.2.7 Direccionamiento de IPv4 de legado

Clases de redes antiguas

Históricamente, la RFC1700 agrupaba rangos de unicast en tamaños específicos llamados direcciones de clase A, de clase B y de clase C. También definía a las direcciones de clase D (multicast) y de clase E (experimental), anteriormente tratadas.

Las direcciones unicast de clases A, B y C definían redes de tamaños específicos, así como bloques de direcciones específicos para estas redes, como se muestra en la figura. Se asignó a una compañía u organización todo un bloque de direcciones de clase A, clase B o clase C. Este uso de espacio de dirección es denominado direccionamiento con clase.

Bloques de clase A

Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo /8 fijo, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host.

Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que sólo había 128 redes de clase A posibles, de 0.0.0.0 /8 a 127.0.0.0 /8, antes de excluir los bloques de direcciones reservadas. A pesar de que las direcciones de clase A reservaban la mitad del espacio de direcciones, debido al límite de 128 redes, sólo podían ser asignadas a aproximadamente 120 compañías u organizaciones.

Bloques de clase B

El espacio de direcciones de clase B fue diseñado para satisfacer las necesidades de las redes de tamaño moderado a grande con más de 65.000 hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones host. Al igual que con la clase A, debía reservarse espacio de direcciones para las clases de direcciones restantes.

Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran **10**. De esta forma, se restringía el bloque de direcciones para la clase B a 128.0.0.0 /16 hasta 191.255.0.0 /16. La clase B tenía una asignación de direcciones un tanto más eficiente que la clase A debido a que dividía equitativamente el 25% del total del espacio de direcciones IPv4 entre aproximadamente 16.000 redes.

Bloques de clase C

El espacio de direcciones de clase C era la clase de direcciones antiguas más comúnmente disponible. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts.

Los bloques de direcciones de clase C utilizaban el prefijo /24. Esto significaba que una red de clase C usaba sólo el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red.

Los bloques de direcciones de clase C reservaban espacio de direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de **110** para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0 /16 a 223.255.255.0 /16. A pesar de que ocupaba sólo el 12.5% del total del espacio de direcciones IPv4, podía suministrar direcciones a 2 millones de redes.

Limitaciones del sistema basado en clases

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. **La asignación con clase de espacio de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4**. Por ejemplo: una compañía con una red con 260 hosts necesitaría que se le otorgue una dirección de clase B con más de 65.000 direcciones.

A pesar de que este sistema con clase no fue abandonado hasta finales de la década del 90, es posible ver restos de estas redes en la actualidad. Por ejemplo: al asignar una dirección IPv4 a una computadora, el sistema operativo examina la dirección que se está asignando para determinar si es de clase A, clase B o clase C. Luego, el sistema operativo adopta el prefijo utilizado por esa clase y realiza la asignación de la máscara de subred adecuada.

Otro ejemplo es la adopción de la máscara por parte de algunos protocolos de enrutamiento. Cuando algunos protocolos de enrutamiento reciben una ruta publicada, se puede adoptar la longitud del prefijo de acuerdo con la clase de dirección.

Direccionamiento sin clase

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema classless, se asignan los bloques de direcciones adecuados para la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase de unicast.

Clases de direcciones IP

Clase de direcciones	1er rango del octeto (decimal)	1eros bits del octeto (los bits verdes no cambian)	Partes de las direcciones de red(N) y de host(H)	Máscara de subred predeterminada (decimal y binaria)	Número de posibles redes y hosts por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16,777,214 hosts por red (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 redes (2^14) 65,534 hosts por red (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 redes (2^21) 254 hosts por red (2^8-2)
D	224-239	11000000-11011111	ND (multicast)		
E	240-255	11110000-11111111	ND (experimental)		

** Todos los ceros (0) y los unos (1) son direcciones hosts no válidas.

6.3 Asignación de direcciones

6.3.1 Planificación del direccionamiento de la red

Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red corporativa esté bien diseñada. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

- Evitar duplicación de direcciones.
- Proveer y controlar el acceso.
- Monitorear seguridad y rendimiento.

Evitar duplicación de direcciones

Como se sabe, cada host en una interwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

Brindar acceso y controlarlo

Algunos hosts ofrecen recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. El acceso a estos recursos puede ser controlado por la dirección de la Capa 3. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Por ejemplo: si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a su dirección y es posible que los clientes no puedan ubicar este recurso.

Monitorear la seguridad y el rendimiento

De igual manera, es necesario monitorear la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan

o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

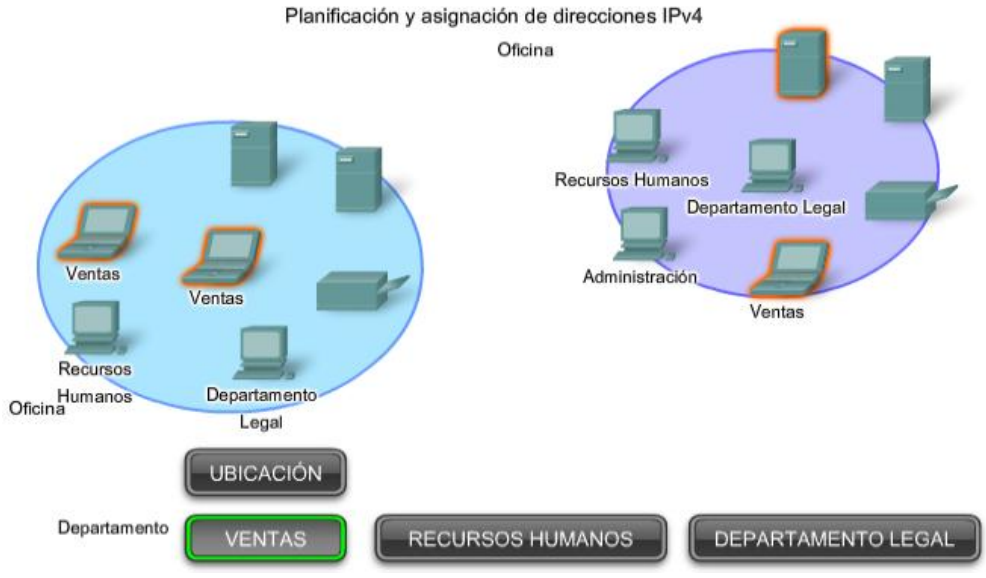
Asignación de direcciones dentro de una red

Como ya se ha explicado, los hosts se asocian con una red IPv4 por medio de una porción de red en común de la dirección. Dentro de una red, existen diferentes tipos de hosts.

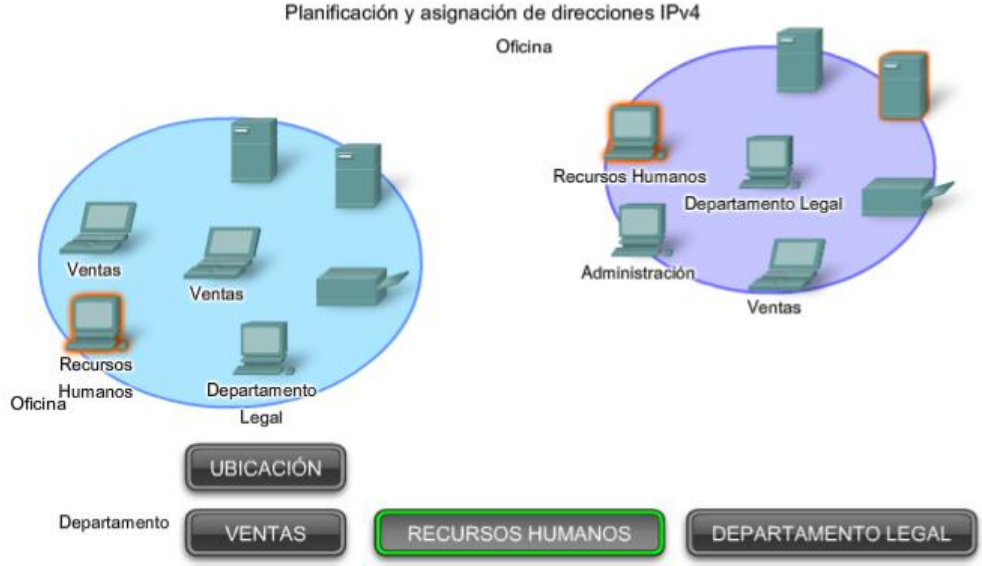
Algunos ejemplos de diferentes tipos de hosts son:

- Dispositivos finales para usuarios.
- Servidores y periféricos.
- Hosts a los que se accede desde Internet.
- Dispositivos intermediarios.

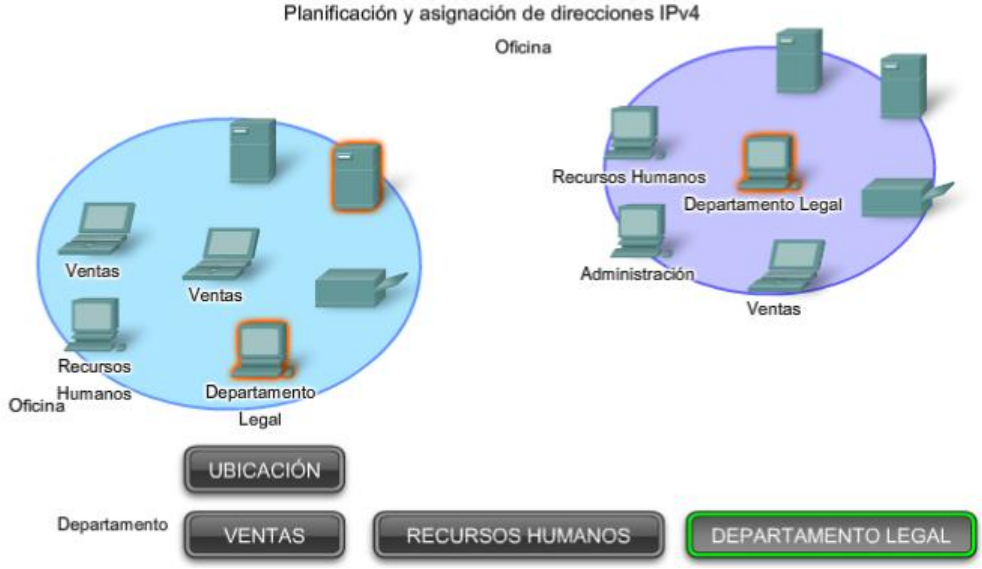
Cada uno de los diferentes tipos de dispositivos debe ser asignado en un bloque lógico de direcciones dentro del rango de direcciones de la red.



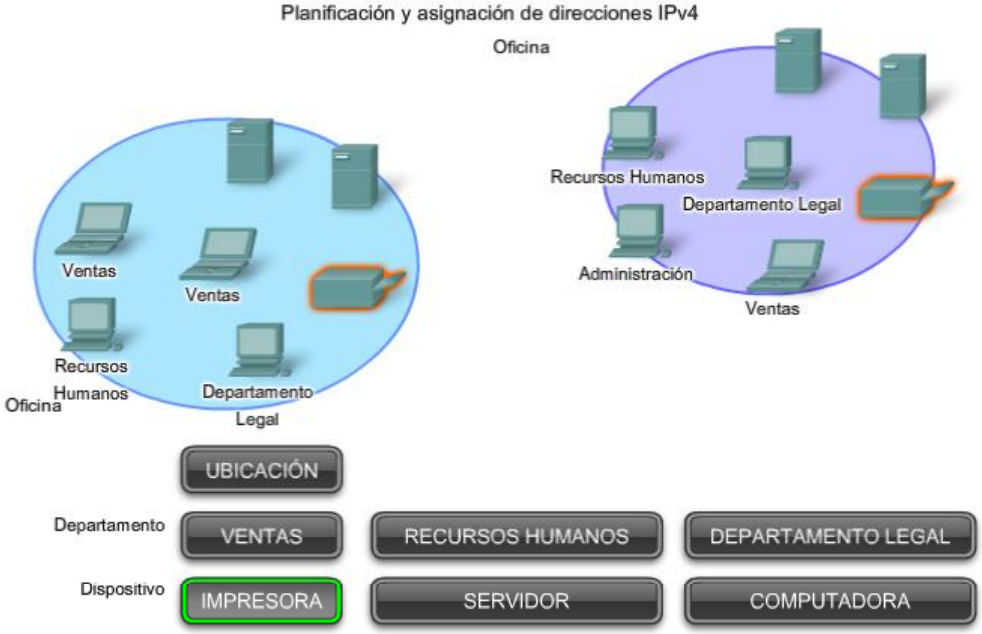
Planificación y asignación de direcciones IPv4



Planificación y asignación de direcciones IPv4



Planificación y asignación de direcciones IPv4

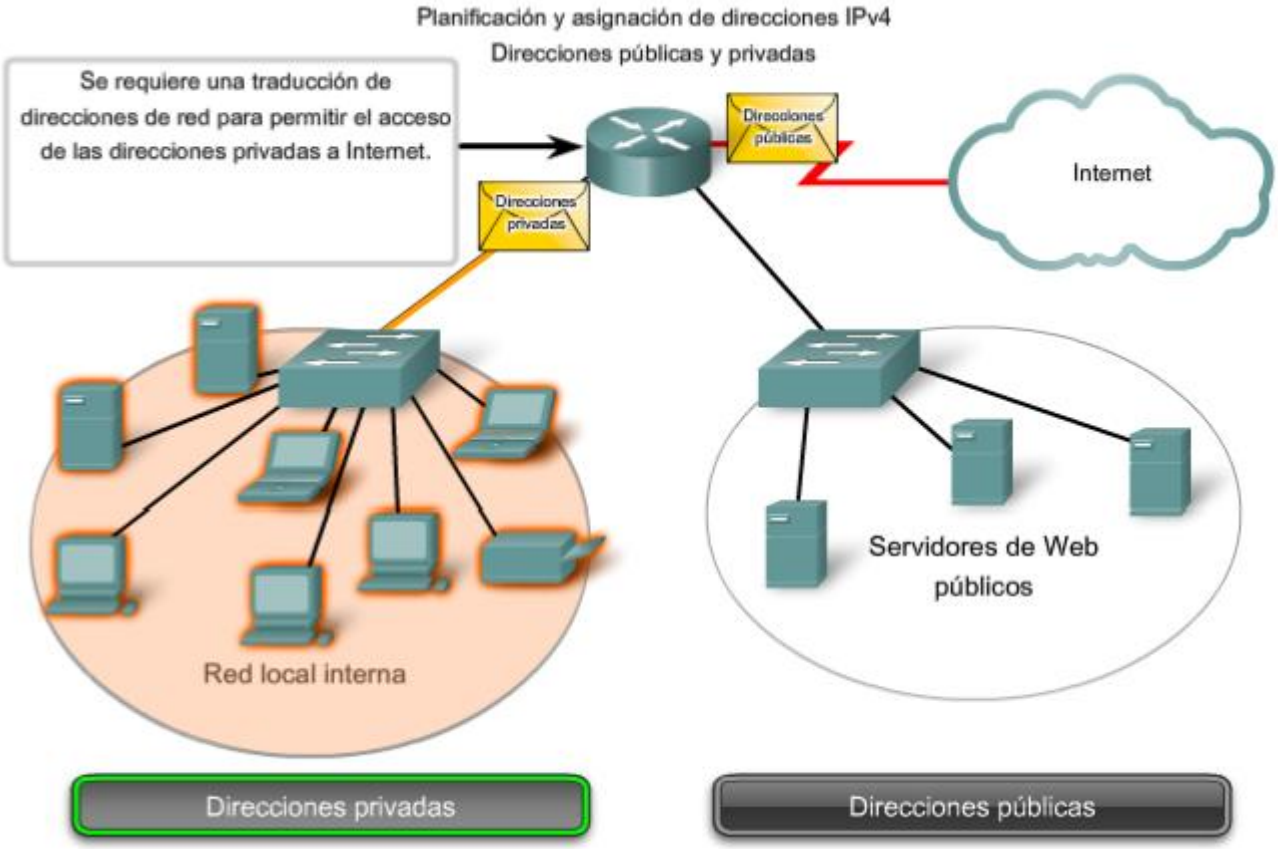


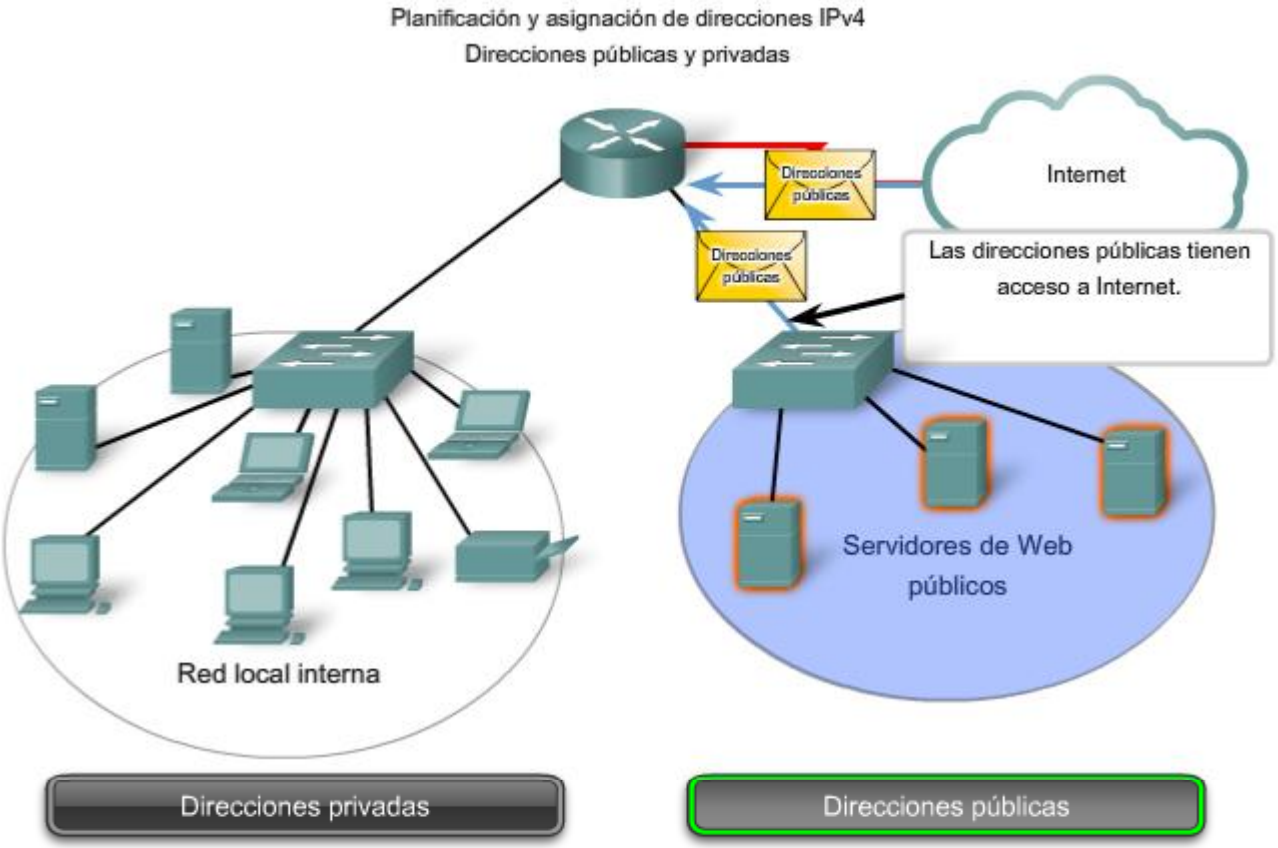
Una parte importante de la planificación de un esquema de direccionamiento IPv4 es decidir cuándo utilizar direcciones privadas y dónde se deben aplicar.

Se debe tener en cuenta lo siguiente:

- ¿Habrá más dispositivos conectados a la red que direcciones públicas asignadas por el ISP de la red?
- ¿Se necesitará acceder a los dispositivos desde fuera de la red local?
- Si los dispositivos a los que se pueden asignar direcciones privadas requieren acceso a Internet, ¿está la red capacitada para proveer el servicio de Traducción de dirección de red (NAT)?

Si hay más dispositivos que direcciones públicas disponibles, sólo esos dispositivos que accederán directamente a Internet, como los servidores Web, requieren una dirección pública. Un servicio NAT permitiría a esos dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.





6.3.2 Direccionamiento estático o dináminco para dispositivos de usuario final

Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos IP, impresoras y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

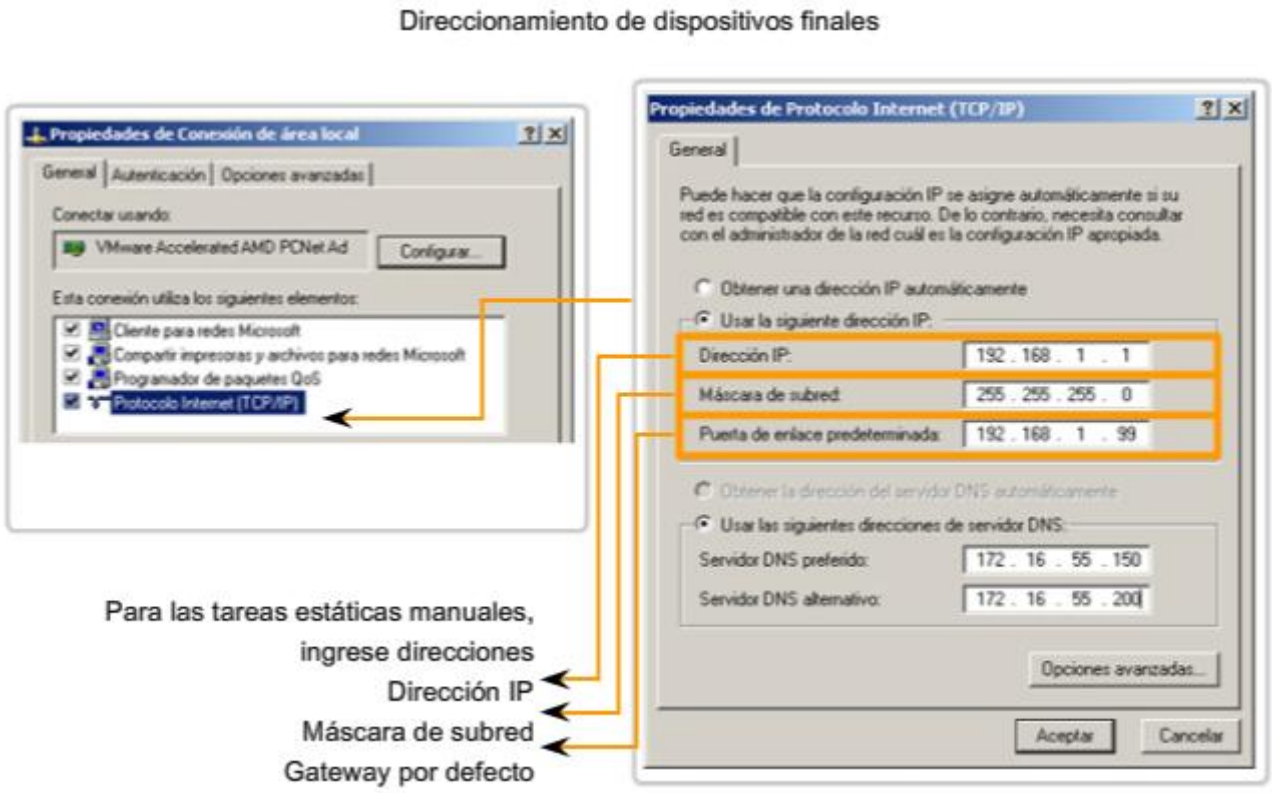
Las direcciones IP pueden asignarse de manera estática o dinámica.

Asignación estática de direcciones

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto.

Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red. Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocaría problemas si se cambiara esa dirección. Además, la asignación estática de información de direccionamiento puede proporcionar un mayor control de los recursos de red. Sin embargo, puede llevar mucho tiempo ingresar la información en cada host.

Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.



Asignación dinámica de direcciones

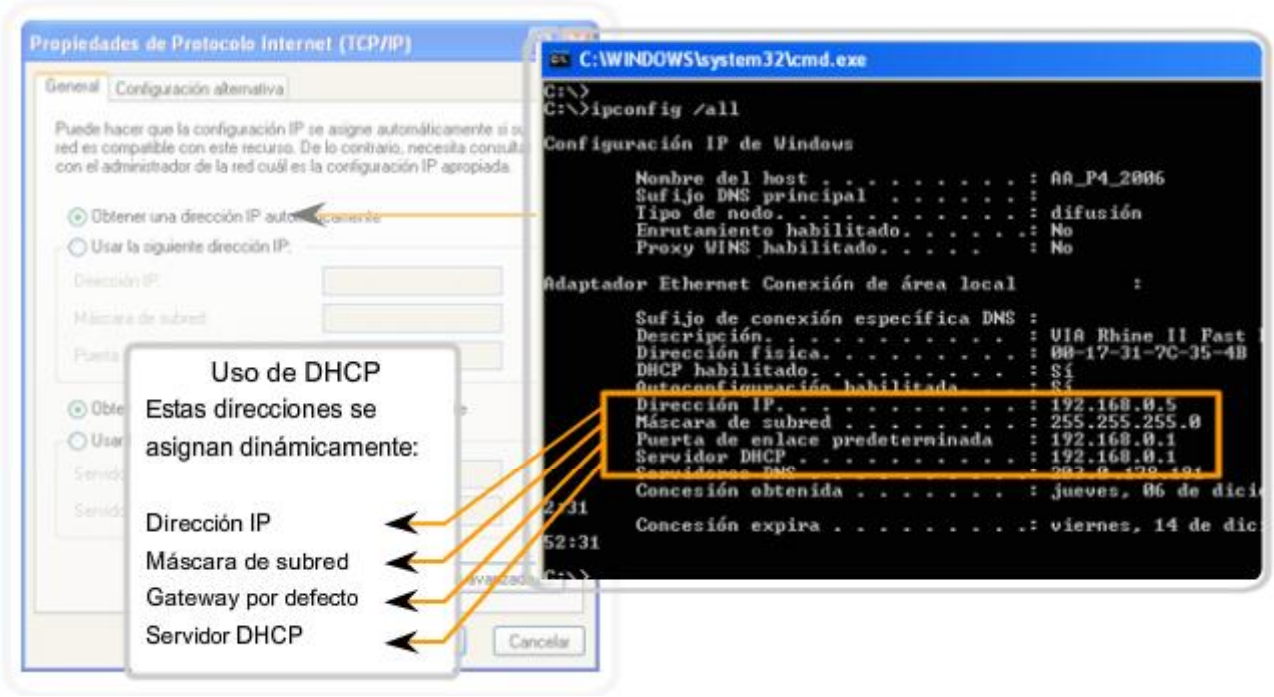
Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el Protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el gateway por defecto y otra información de configuración. La configuración del sevidor DHCP requiere que un bloque de direcciones, llamado conjunto de direcciones, sea definido para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

Asignación de direcciones dinámicas



6.3.3 Asignacion de direcciones a otros dispositivos

Direcciones para servidores y periféricos

Cualquier recurso de red como un servidor o una impresora debe tener una dirección IPv4 estática, como se muestra en la figura. Los hosts clientes acceden a estos recursos utilizando las direcciones IPv4 de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos.

Los servidores y periféricos son un punto de concentración para el tráfico de red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red debe poder identificar rápidamente estos dispositivos. Utilizar un sistema de numeración consistente para estos dispositivos facilita la identificación.

Direcciones para hosts accesibles desde Internet

En la mayoría de las internetworks, los hosts fuera de la empresa pueden acceder sólo a unos poco dispositivos. En la mayoría de los casos, estos dispositivos son normalmente algún tipo de servidor. Al igual que todos los dispositivos en una red que proporciona recursos de red, las direcciones IPv4 para estos dispositivos deben ser estáticas.

En el caso de los servidores a los que se puede acceder desde Internet, cada uno debe tener una dirección de espacio público asociada. Además, las variaciones en la dirección de uno de estos dispositivos hará que no se pueda acceder a éste desde Internet. En muchos casos, estos dispositivos se encuentran en una red numerada mediante direcciones privadas. Esto significa que el router o el firewall del perímetro de la red debe estar configurado para traducir la dirección interna del servidor en una dirección pública. Debido a esta configuración adicional del dispositivo que actúa como intermediario del perímetro, resulta aun más importante que estos dispositivos tengan una dirección predecible.

Direcciones para dispositivos intermediarios

Los dispositivos intermediarios también son un punto de concentración para el tráfico de red. **Casi todo el tráfico dentro redes o entre ellas pasa por alguna forma de dispositivo intermediario.** Por lo tanto, estos dispositivos de red ofrecen una ubicación oportuna para la administración, el monitoreo y la seguridad de red.

A la mayoría de los dispositivos intermediarios se le asigna direcciones de Capa 3. Ya sea para la administración del dispositivo o para su operación. Los dispositivos como hubs, switches y puntos de acceso inalámbricos no requieren direcciones IPv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar, monitorear o resolver problemas de funcionamiento de la red, éstos deben tener direcciones asignadas.

Debido a que es necesario saber cómo comunicarse con dispositivos intermedios, éstos deben tener direcciones predecibles. Por lo tanto, típicamente, las direcciones se asignan manualmente. Además, las direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red que las direcciones de dispositivos de usuario.

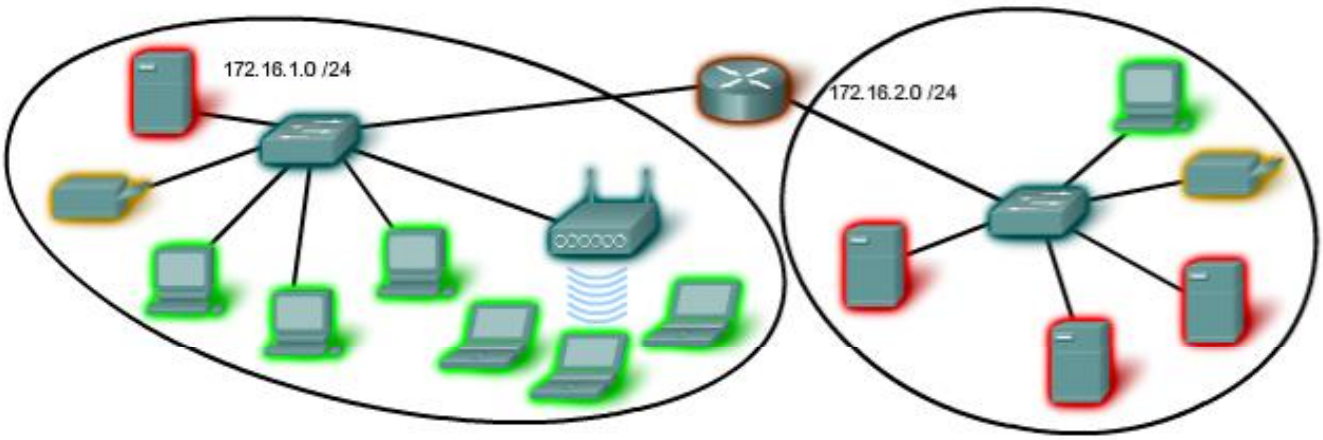
Routers y firewalls

A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall un dirección IPv4 para cada interfaz. Cada interfaz se encuentra en una red diferente y funciona como gateway para los hosts de esa red. Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red. Esta asignación debe ser uniforme en todas las redes de la empresa, de manera que el personal de red siempre conozca la gateway de la red, independientemente de cuál sea la red en la que están trabajando.

Las interfaces de router y firewall son el punto de concentración del tráfico que entra y sale de la red. Debido a que los hosts de cada red usan una interfaz de dispositivo router o firewall como gateway para salir de la red, existe un flujo abundante de paquetes en estas interfaces. Por lo tanto, estos dispositivos pueden cumplir una función importante en la seguridad de red al filtrar los paquetes según las direcciones IPv4 de origen y destino. Agrupar los diferentes tipos de dispositivos en grupos de direccionamiento lógicos hace que la asignación y el funcionamiento del filtrado de paquetes sea más eficiente.

Rangos de direcciones IP de los dispositivos

Uso	Primera dirección	Última dirección	Dirección de resumen
Dirección de red	172.16.x.0	.....	172.16.x.0 /25
Hosts de usuarios (pool de DHCP)	172.16.x.1	172.16.x.127	
Servidores	172.16.x.128	172.16.x.191	172.16.x.128 /26
Periféricos	172.16.x.192	172.16.x.223	172.16.x.192 /27
Dispositivos de red	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



6.3.4 ¿Quién asigna las diferentes direcciones?

Una compañía u organización que desea acceder a la red mediante hosts desde Internet debe tener un bloque de direcciones públicas asignado. El uso de estas direcciones públicas es regulado y la compañía u organización debe tener un bloque de direcciones asignado. Esto es lo que sucede con las direcciones IPv4, IPv6 y multicast.

Autoridad de números asignados a Internet (IANA) (http://www.iana.net) es un soporte maestro de direcciones IP. Las direcciones IP multicast y las direcciones IPv6 se obtienen directamente de la IANA. Hasta mediados de los años noventa, todo el espacio de direcciones IPv4 era directamente administrado por la IANA. En ese entonces, se asignó el resto del espacio de direcciones IPv4 a otros diversos registros para que realicen la administración de áreas regionales o con propósitos particulares. Estas compañías de registro se llaman Registros regionales de Internet (RIR), como se muestra en la figura.

Los principales registros son:

- AfriNIC (African Network Information Centre) - Región de África http://www.afrinic.net
- APNIC (Asia Pacific Network Information Centre) - Región de Asia/Pacífico http://www.apnic.net
- ARIN (American Registry for Internet Numbers) - Región de Norte América http://www.arin.net
- LACNIC (Registro de dirección IP de la Regional Latinoamericana y del Caribe) - América Latina y algunas islas del Caribe http://www.lacnic.net
- RIPE NCC (Reseaux IP Europeans) - Europa, Medio Oriente y Asia Central http://www.ripe.net

Enlaces:

asignaciones de registros de direcciones IPv4:

http://www.ietf.org/rfc/rfc1466.txt?number=1466

http://www.ietf.org/rfc/rfc2050.txt?number=2050

Asignación de direcciones IPv4: http://www.iana.org/ipaddress/ip-addresses.htm

Búsqueda de direccionamiento IP: http://www.arin.net/whois/

Entidades que supervisan la asignación de direcciones IP

Global	IANA				
Registros de Internet regionales	**AfriNIC** Región de África	**APNIC** Asia/ Región del Pacífico	**LACNIC** Región de América Latina y el Caribe	**ARIN** Región de América del Norte	**RIPE NCC** Europa, Medio Oriente, Región de Asia Central

6.3.5 Proveedores de servicios de Internet (ISP)

El papel de ISP

La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio.

En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente.

Servicios ISP

Para tener acceso a los servicios de Internet, tenemos que conectar nuestra red de datos a Internet usando un Proveedor de Servicios de Internet (ISP).

Los ISP poseen sus propios conjuntos de redes internas de datos para administrar la conectividad a Internet y ofrecer servicios relacionados. Entre los servicios que un ISP generalmente ofrece a sus clientes se encuentran los servicios

DNS, servicios de correo electrónico y un sitio Web. Dependiendo del nivel de servicio requerido y disponible, los clientes usan diferentes niveles de un ISP.

ISP Tiers

Los ISP son designados por una jerarquía basada en su nivel de conectividad a la backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior, como se muestra en la figura.

Nivel 1

En la parte superior de la jerarquía de ISP están los ISP de nivel 1. Éstos son grandes ISP a nivel nacional o internacional que se conectan directamente al backbone de Internet. Los clientes de ISP de nivel 1 son ISP de menor nivel o grandes compañías y organizaciones. Debido a que se encuentran en la cima de la conectividad a Internet, ofrecen conexiones y servicios altamente confiables. Entre las tecnologías utilizadas como apoyo de esta confiabilidad se encuentran múltiples conexiones al backbone de Internet.

Las principales ventajas para los clientes de ISP de nivel 1 son la confiabilidad y la velocidad. Debido a que estos clientes están a sólo una conexión de distancia de Internet, hay menos oportunidades de que se produzcan fallas o cuellos de botella en el tráfico. La desventaja para los clientes de ISP de nivel 1 es el costo elevado.

Nivel 2

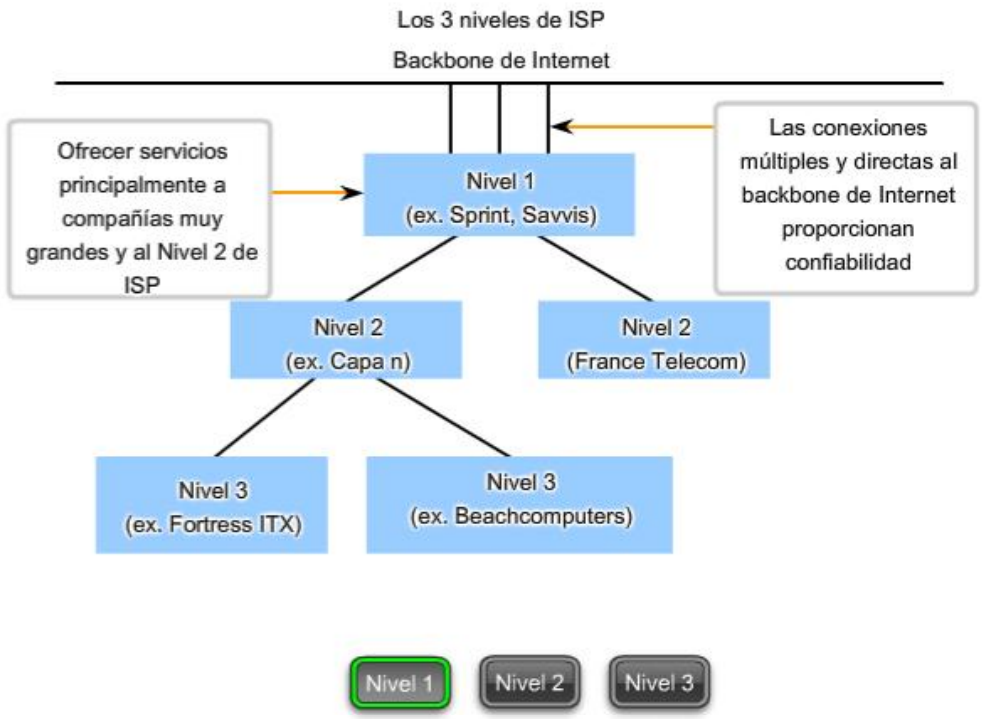
Los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1. **Los ISP de nivel 2 generalmente se centran en los clientes empresa.** Los ISP de nivel 2 normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus propios servicios como DNS, servidores de correo electrónico y servidores web. Otros servicios ofrecidos por los ISP de nivel 2 pueden incluir desarrollo y mantenimiento de sitios web, e-commerce/e-business y VoIP.

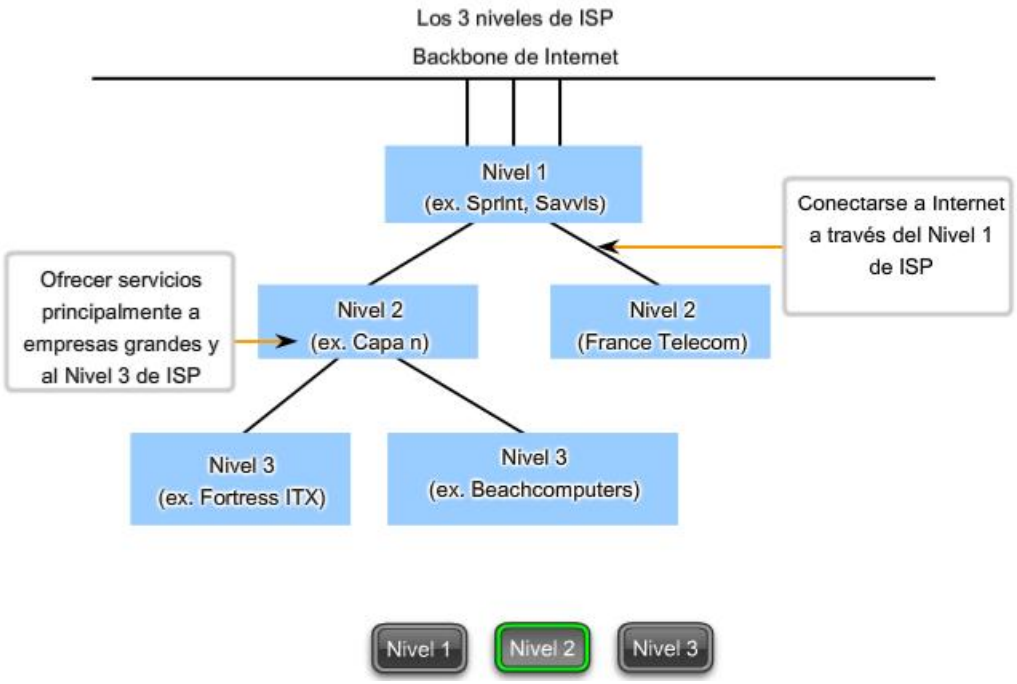
La principal desventaja de los ISP de nivel 2, comparados con los ISP de nivel 1, es el acceso más lento a Internet. Como los IPS de Nivel 2 están al menos a una conexión más lejos de la backbone de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1.

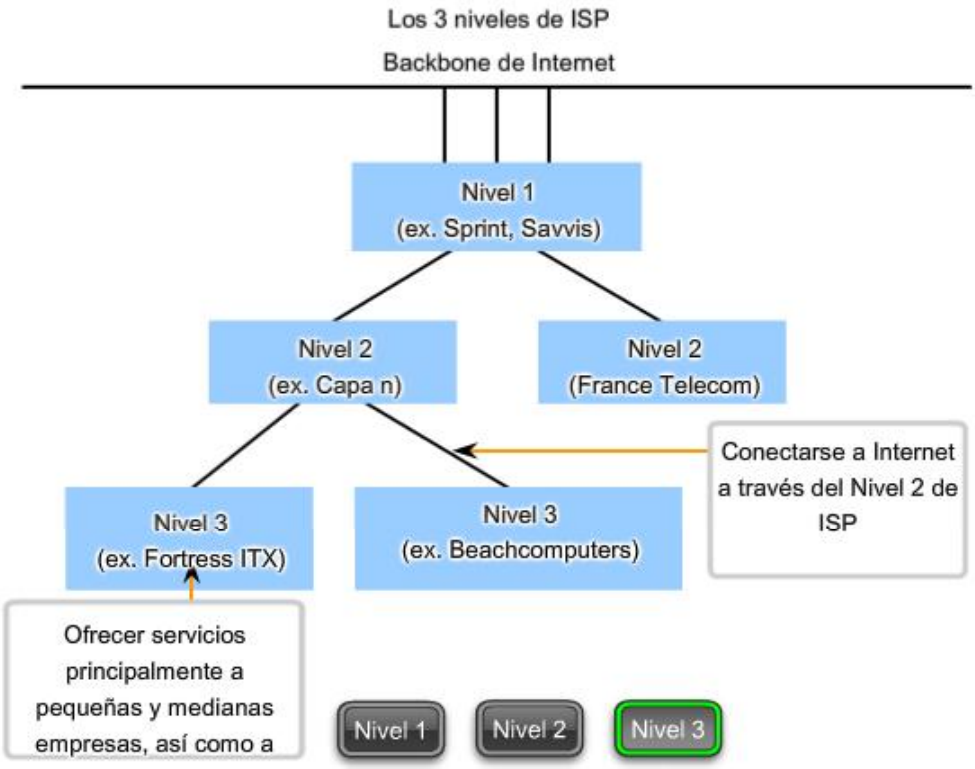
Nivel 3

Los ISP de nivel 3 compran su servicio de Internet de los ISP de nivel 2. **El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica.** Típicamente, los clientes del nivel 3 no necesitan muchos de los servicios requeridos por los clientes del nivel 2. Su necesidad principal es conectividad y soporte.

Estos clientes a menudo tienen conocimiento escaso o nulo sobre computación o redes. Los ISP de nivel 3 suelen incluir la conectividad a Internet como parte del contrato de servicios de red y computación para los clientes. A pesar de que pueden tener un menor ancho de banda y menos confiabilidad que los proveedores de nivel 1 y 2, suelen ser buenas opciones para pequeñas y medianas empresas.







6.3.6 Descripción de IPv6

A principios de los años noventa, el Grupo de trabajo de ingeniería de Internet (IETF) centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo. Esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6.

Crear mayores capacidades de direccionamiento fue la motivación inicial para el desarrollo de este nuevo protocolo. También se consideraron otros temas durante el desarrollo de IPv6, como:

- Manejo mejorado de paquetes
- Escalabilidad y longevidad mejoradas
- Mecanismos QoS (Calidad del Servicio)

Seguridad integrada

Para proveer estas características, IPv6 ofrece:

- Direccionamiento jerárquico de 128 bits: para expandir las capacidades de direccionamiento
- Simplificación del formato de encabezado: para mejorar el manejo de paquetes
- Soporte mejorado para extensiones y opciones: para escabilidad/longevidad mejoradas y manejo mejorado de paquetes
- Capacidad de rotulado de flujo: como mecanismos QoS
- Capacidades de autenticación y privacidad: para integrar la seguridad

IPv6 no es meramente un nuevo protocolo de Capa 3: es un nuevo conjunto de aplicaciones de protocolo. Se han desarrollado nuevos protocolos en varias capas del stack para admitir este nuevo protocolo. Hay un nuevo protocolo de mensajería (ICMPv6) y nuevos protocolos de enrutamiento. Debido al mayor tamaño del encabezado de IPv6, también repercute en la infraestructura de red subyacente.

Transición a IPv6

Como se puede ver en esta breve introducción, IPv6 ha sido diseñado con escalabilidad para permitir años de crecimiento de la internetwork. Sin embargo, IPv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro. Sin embargo, IPv6 podrá eventualmente reemplazar a IPv4 como protocolo de Internet dominante.

Enlaces:

IPv6: http://www.ietf.org/rfc/rfc2460.txt?number=2460

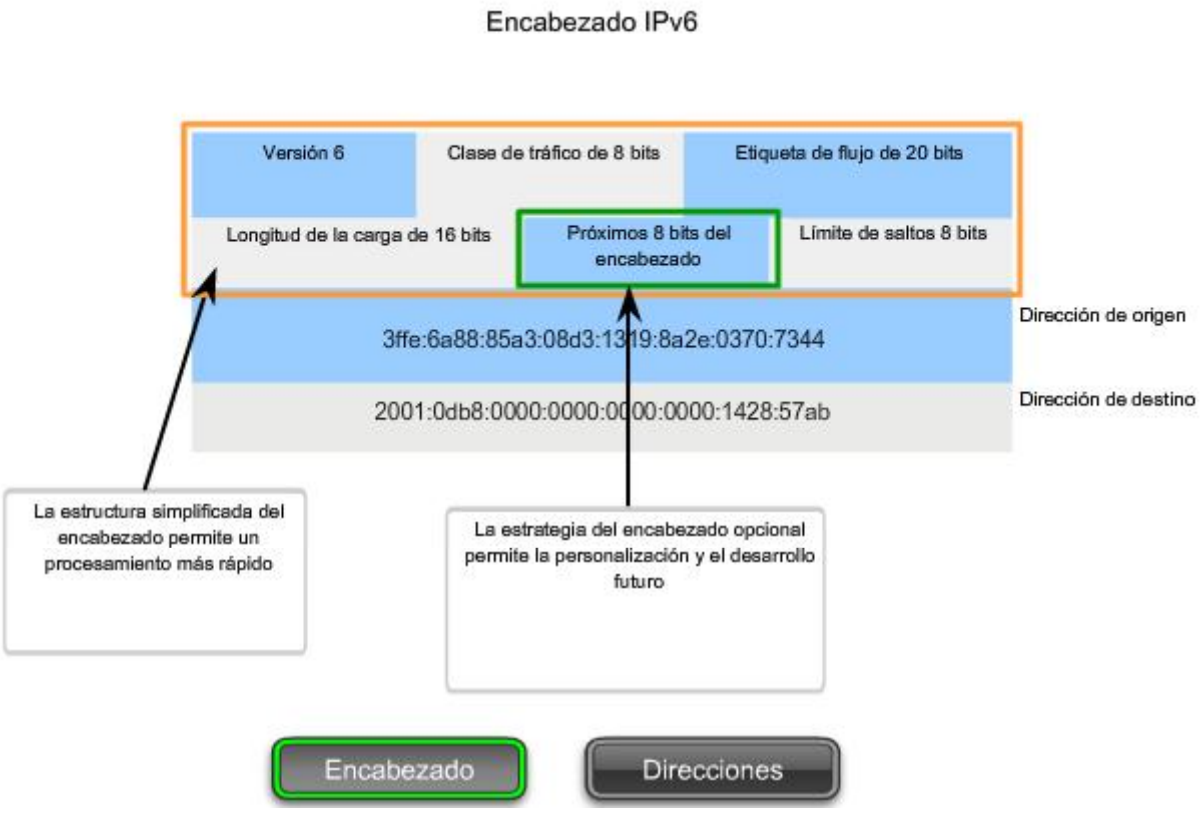
direccionamiento IPv6: http://www.ietf.org/rfc/rfc3513.txt?number=3513

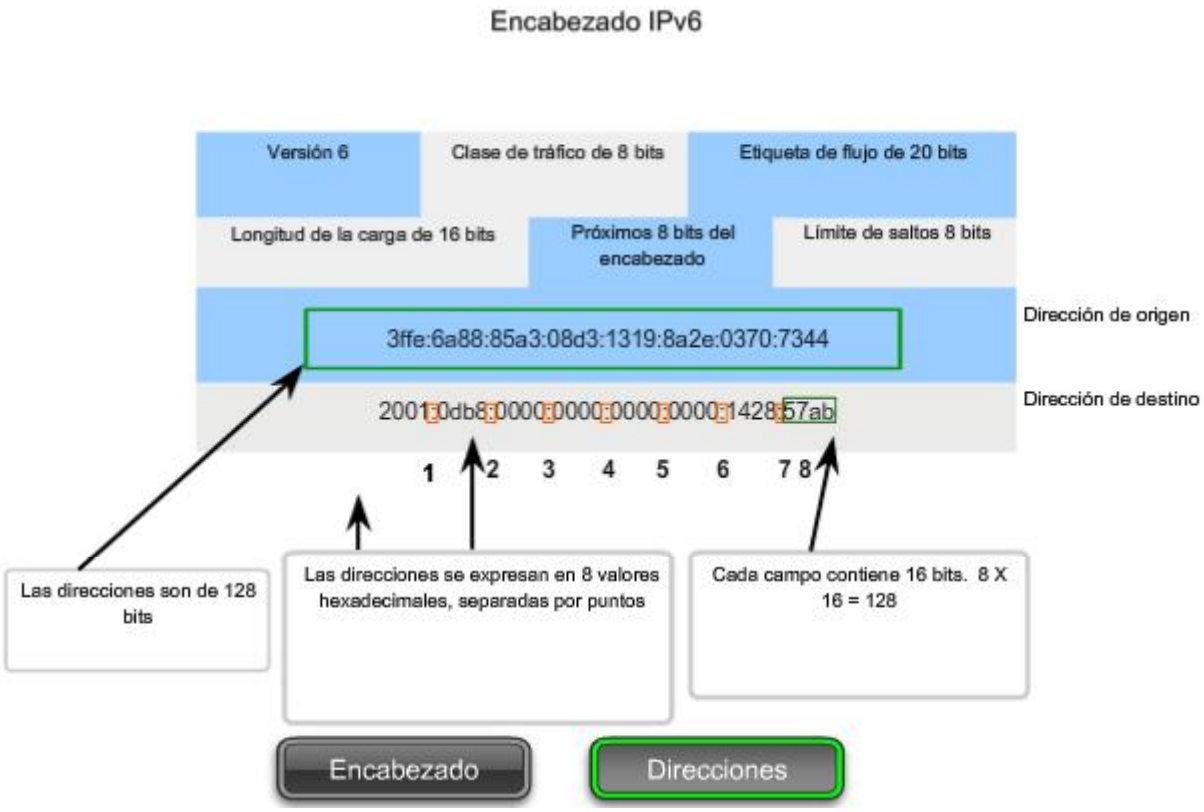
seguridad IPv6: http://www.ietf.org/rfc/rfc2401.txt?number=2401

seguridad IPv6: http://www.ietf.org/rfc/rfc3168.txt?number=3168

seguridad IPv6: http://www.ietf.org/rfc/rfc4302.txt?number=4302

ICMPv6: http://www.ietf.org/rfc/rfc4443.txt?number=4443





6.4 ¿Esta es mi red?

6.4.1 Máscara de subred: definición de las porciones de red y host

Como se enseñó anteriormente, una dirección IPv4 tiene una porción de red y una porción de host. Se hizo referencia a la duración del prefijo como la cantidad de bits en la dirección que conforma la porción de red. El prefijo es una forma de definir la porción de red para que los humanos la pueden leer. La red de datos también debe tener esta porción de red de las direcciones definidas.

Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred, como se muestra en la figura. La máscara de subred se expresa con el mismo formato decimal punteado que la dirección IPv4. La máscara de subred se crea al colocar un **1** binario en cada posición de bit que representa la porción de red y un **0** binario en cada posición de bit que representa la porción de host.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Como se muestra en la figura, un prefijo **/24** se expresa como máscara de subred de esta forma **255.255.255.0 (11111111.11111111.11111111.00000000).** Los bits restantes (orden inferior) de la máscara de subred son números cero, que indican la dirección host dentro de la red.

La máscara de subred se configura en un host junto con la dirección IPv4 para definir la porción de red de esa dirección.

Por ejemplo: veamos el host 172.16.4.35/27:

dirección

172.16.20.35

10101100.00010000.00010100.00100011
máscara de subred

255.255.255.224

11111111.11111111.11111111.11100000

dirección de red

172.16.20.32

10101100.00010000.00010100.00100000

Como los bits de orden superior de las máscaras de subred son contiguos números **1**, existe solamente un número limitado de valores de subred dentro de un octeto. Sólo es necesario ampliar un octeto si la división de red y host entra en dicho octeto. Por lo tanto, se usan patrones de 8 bits limitados en las máscaras de subred.

Estos patrones son:

00000000 = 0

10000000 = 128

11000000 = 192

11100000 = 224

11110000 = 240

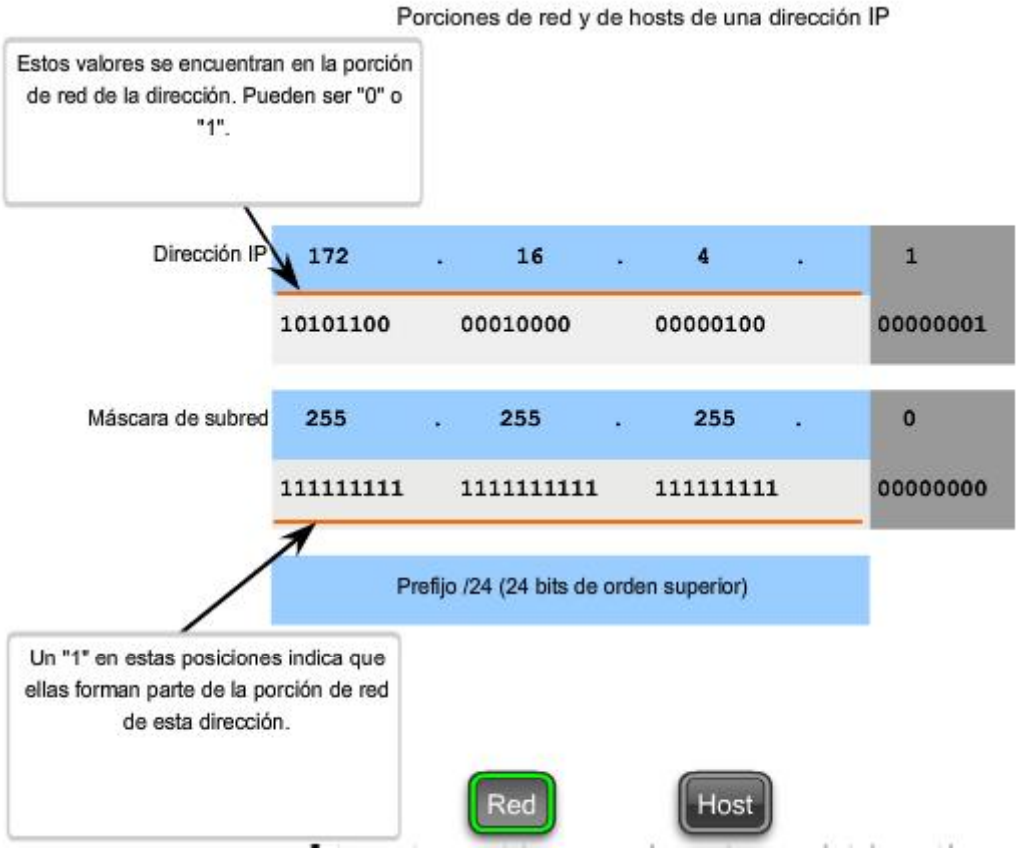
11111000 = 248

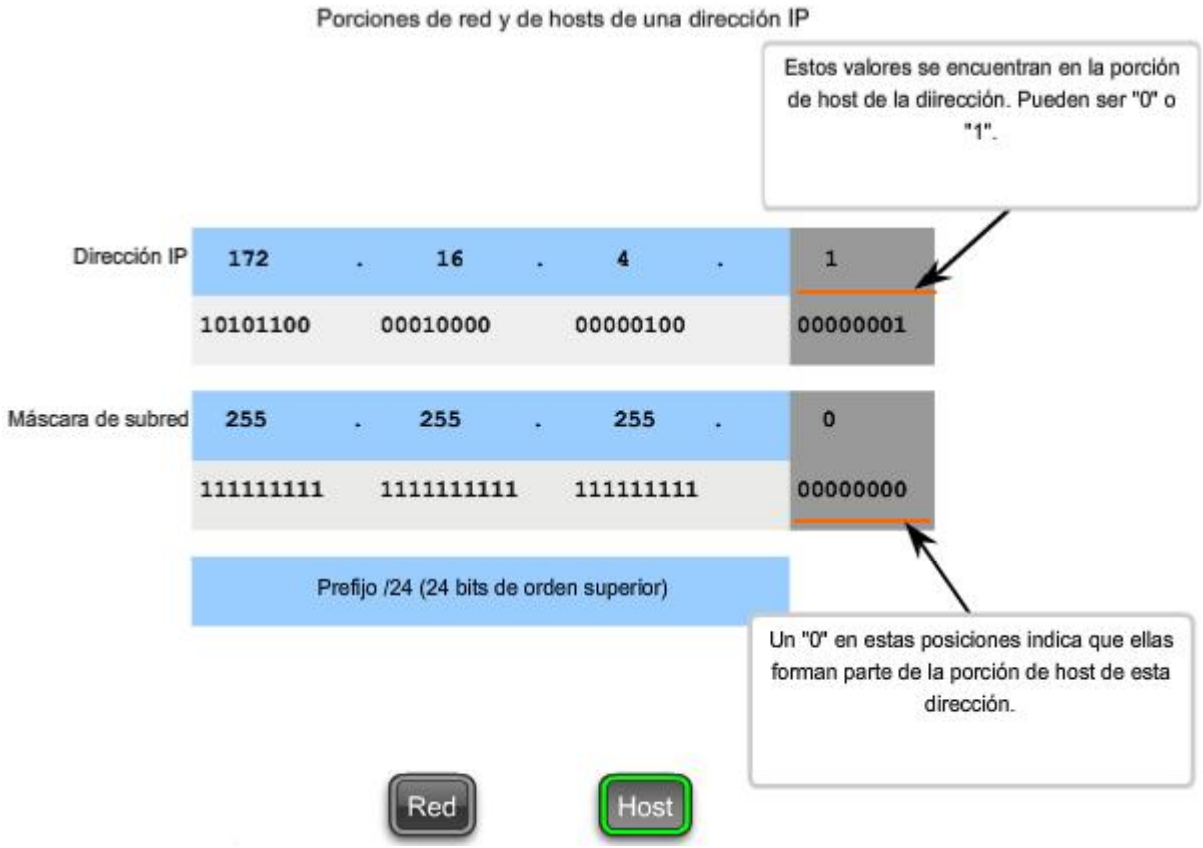
11111100 = 252

11111110 = 254

11111111 = 255

Si la máscara de subred de un octeto está representada por **255**, entonces todos los bits equivalentes de ese octeto de la dirección son bits de red. De igual manera, si la máscara de subred de un octeto está representada por **0**, entonces todos los bits equivalentes de ese octeto de la dirección son bits de host. En cada uno de estos casos, no es necesario ampliar este octeto a binario para determinar las porciones de red y host.





6.4.2 Lógica AND: ¿Qué hay en nuestra red?

Dentro de los dispositivos de redes de datos, se aplica la lógica digital para interpretar las direcciones. Cuando se crea o envía un paquete IPv4, la dirección de red de destino debe obtenerse de la dirección de destino. Esto se hace por medio de una lógica llamada AND.

Se aplica la lógica AND a la dirección host IPv4 y a su máscara de subred para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND a la dirección y a la máscara de subred, el resultado que se produce es la dirección de red.

Operación AND

AND es una de las tres operaciones binarias básicas utilizadas en la lógica digital. Las otras dos son OR y NOT. Mientras que las tres se usan en redes de datos, AND se usa para determinar la dirección de red. Por lo tanto, sólo se tratará aquí la lógica AND. La lógica AND es la comparación de dos bits que produce los siguientes resultados:

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

El resultado de la aplicación de AND con **1** en cualquier caso produce un resultado que es el bit original. Es decir, **0 AND 1** es **0** y **1 AND 1** es **1**. En consecuencia, la aplicación de AND con **0** en cualquier caso produce un **0**.Estas propiedades de la aplicación de AND se usan con la máscara de subred para "enmascarar" los bits de host de una dirección IPv4. Se aplica la lógica AND a cada bit de la dirección con el bit de máscara de subred correspondiente.

Debido a que todos los bits de la máscara de subred que representan bits de host son 0, la porción de host de la dirección de red resultante está formada por todos 0. Recuerde que una dirección IPv4 con todos 0 en la porción de host representa la dirección de red.

De igual manera, todos los bits de la máscara de subred que indican la porción de red son **1.** Cuando se aplica la lógica AND a cada uno de estos **1** con el bit correspondiente de la dirección, los bits resultantes son idénticos a los bits de dirección originales.

Motivos para utilizar AND

La aplicación de AND a la dirección host y a la máscara de subred se realiza mediante dispositivos en una red de datos por diversos motivos.

Los routers usan AND para determinar una ruta aceptable para un paquete entrante. El router verifica la dirección de destino e intenta asociarla con un salto siguiente. Cuando llega un paquete a un router, éste realiza el procedimiento de aplicación de AND en la dirección IP de destino en el paquete entrante y con la máscara de subred de las rutas posibles. De esta forma, se obtiene una dirección de red que se compara con la ruta de la tabla de enrutamiento de la cual se usó la máscara de subred.

Un host de origen debe determinar si un paquete debe ser directamente enviado a un host en la red local o si debe ser dirigido al gateway. Para tomar esta determinación, un host primero debe conocer su propia dirección de red.

Un host obtiene su dirección de red al aplicar la lógica AND a la dirección con la máscara de subred. La lógica AND también es llevada a cabo por un host de origen entre la dirección de destino del paquete y la máscara de subred de este host. Esto produce la dirección de red de destino. Si esta dirección de red coincide con la dirección de red del host local, el paquete es directamente enviado al host de destino. Si las dos direcciones de red no coinciden, el paquete es enviado al gateway.

La importancia de AND

Si los routers y dispositivos finales calculan estos procesos sin la intervención de nadie, ¿por qué debemos aprender acerca de AND? Cuanto más comprendamos y podamos predecir sobre el funcionamiento de una red, más equipados estaremos para diseñar y administrar una.

En la verificación/resolución de problemas de una red, a menudo es necesario determinar en qué red IPv4 se encuentra un host o si dos hosts se encuentran en la misma red IP. Es necesario tomar esta determinación desde el punto de vista de los dispositivos de red. Debido a una configuración incorrecta, un host puede encontrarse en una red que no era la planificada. Esto puede hacer que el funcionamiento parezca irregular, a menos que se realice el diagnóstico mediante el análisis de los procesos de aplicación de AND utilizados por el host.

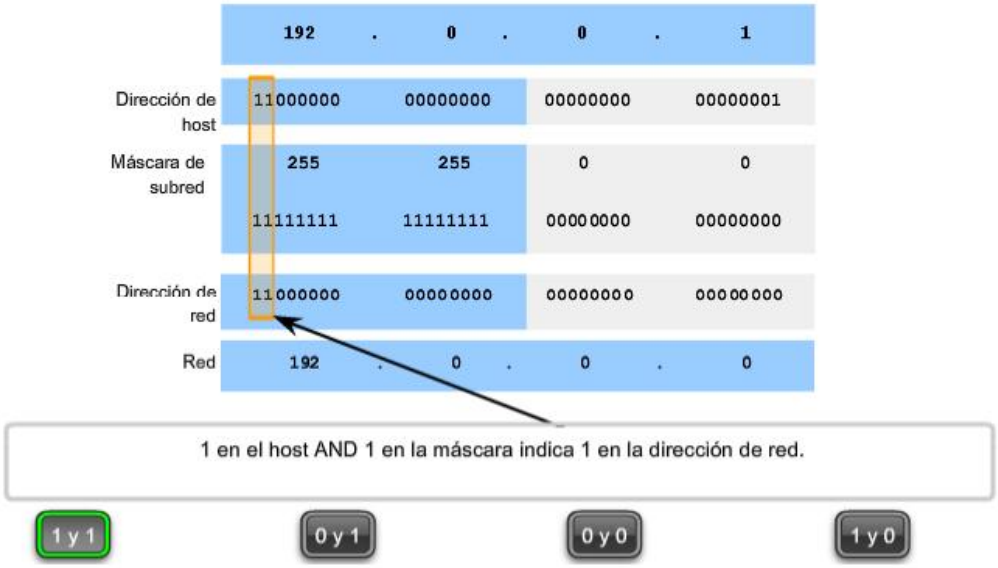
Además, un router puede tener diferentes rutas que pueden realizar el envío de un paquete a un determinado destino. La selección de la ruta utilizada para cualquier paquete es una operación compleja. Por ejemplo: el prefijo que forma estas rutas no se asocia directamente con las redes asignadas al host. Esto significa que una ruta de la tabla de enrutamiento puede representar muchas redes. Si se produjeron inconvenientes con los paquetes de enrutamiento, podrá ser necesario determinar cómo el router tomaría la decisión del enrutamiento.

A pesar de que se dispone de calculadoras de subredes, es útil para un administrador de red saber calcular subredes manualmente.

Nota: No se permite el uso de calculadoras de ningún tipo durante los exámenes de certificación.

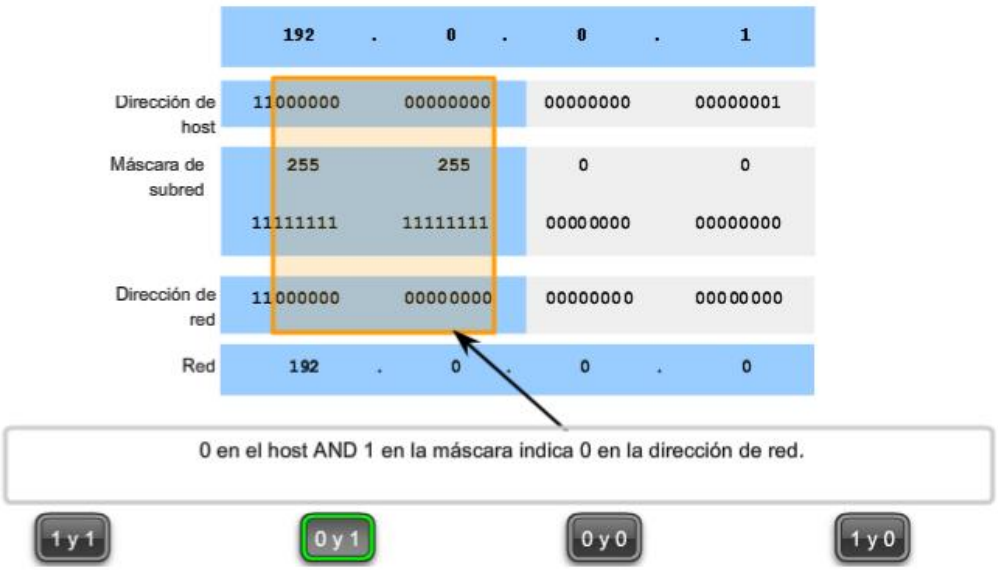
Aplicación de la máscara de subred

Un dispositivo con la dirección 192.0.0.1 pertenece a la red 192.0.0.0



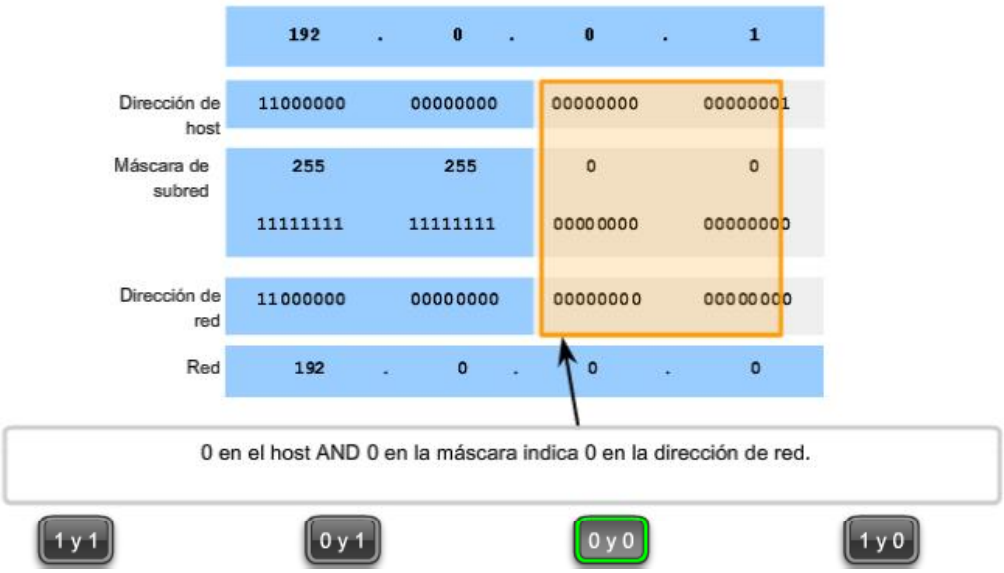
Aplicación de la máscara de subred

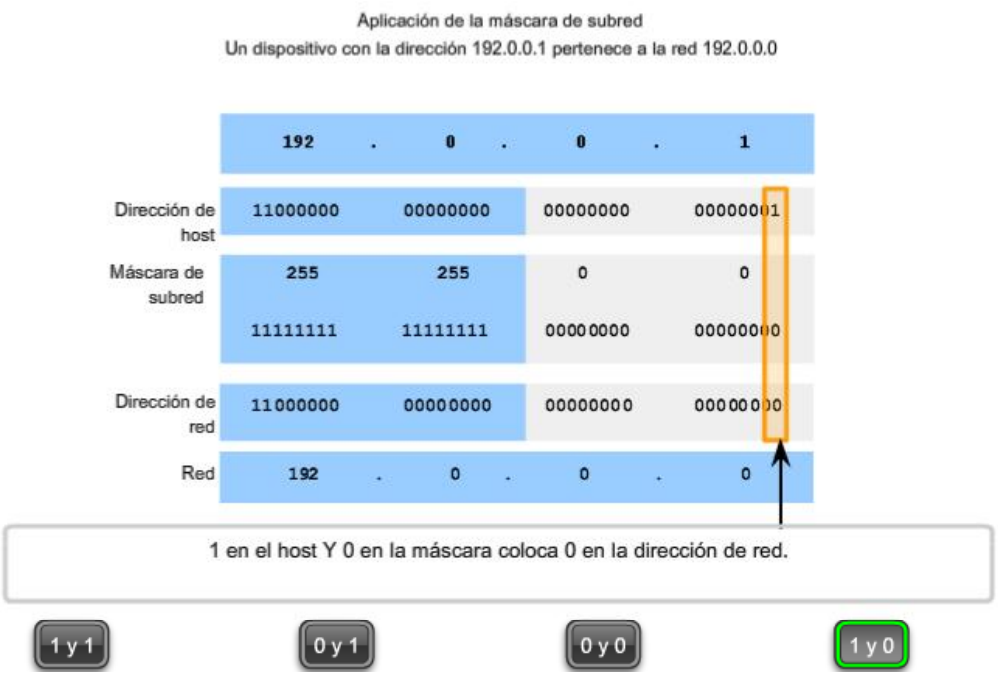
Un dispositivo con la dirección 192.0.0.1 pertenece a la red 192.0.0.0



Aplicación de la máscara de subred

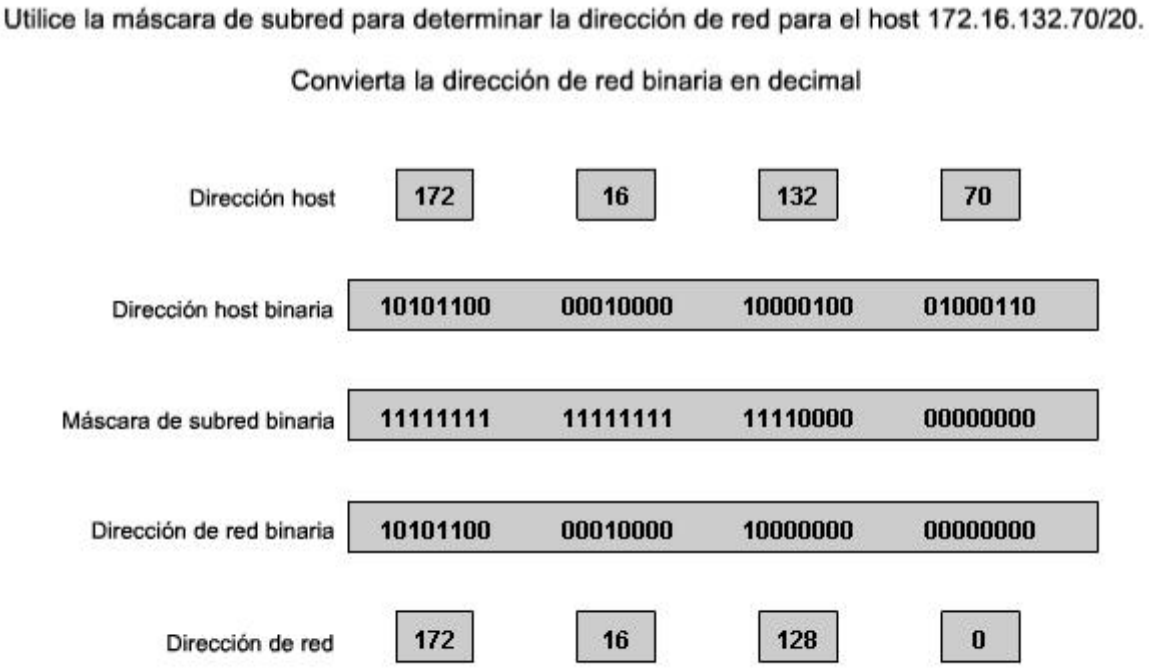
Un dispositivo con la dirección 192.0.0.1 pertenece a la red 192.0.0.0





6.4.3 El proceso de aplicación de AND

La operación AND se aplica a cada bit de la dirección binaria.



6.5 Cálculo de direcciones

6.5.1 Principios de división en subredes

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuanto más bits de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

El router A en la figura posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es "1".

Fórmula para calcular subredes

Use esta fórmula para calcular la cantidad de subredes:

2^n donde n = la cantidad de bits que se tomaron prestados

En este ejemplo, el cálculo es así:

2^1 = 2 subredes

La cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula 2^n - 2 donde n = la cantidad de bits para hosts.

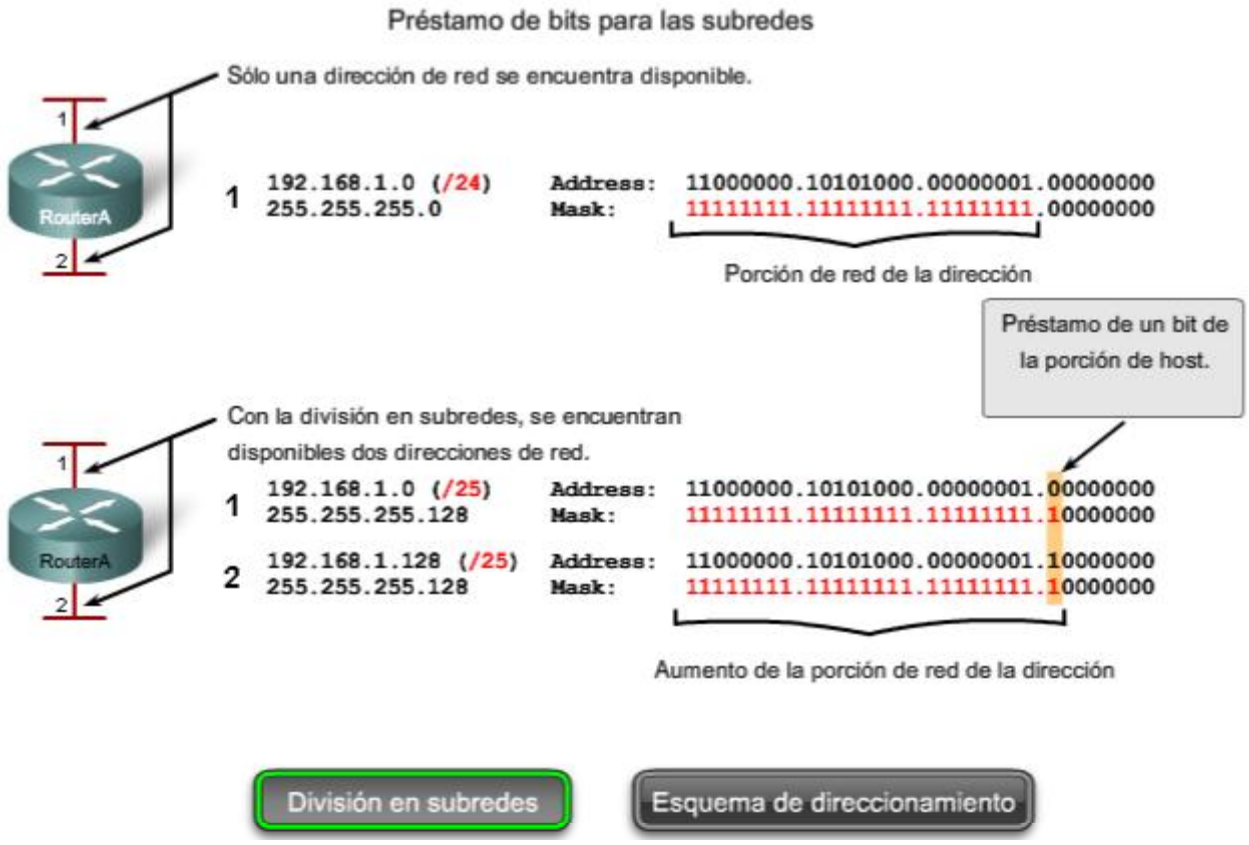
La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts.

En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: ***0***0000000 = 0

Subred 2: ***1***0000000 = 128

Vea la figura para conocer el esquema de direccionamiento para estas redes.



Ejemplo con 3 subredes

A continuación, piense en una internetwork que requiere tres subredes. Vea la figura.

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24. Tomar prestado un solo bit proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits. Esto proveerá cuatro subredes.

Calcule la subred con esta fórmula:

2^2 = 4 subredes

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

Subred 0: 0 = ***00***000000

Subred 1: 64 = ***01***000000

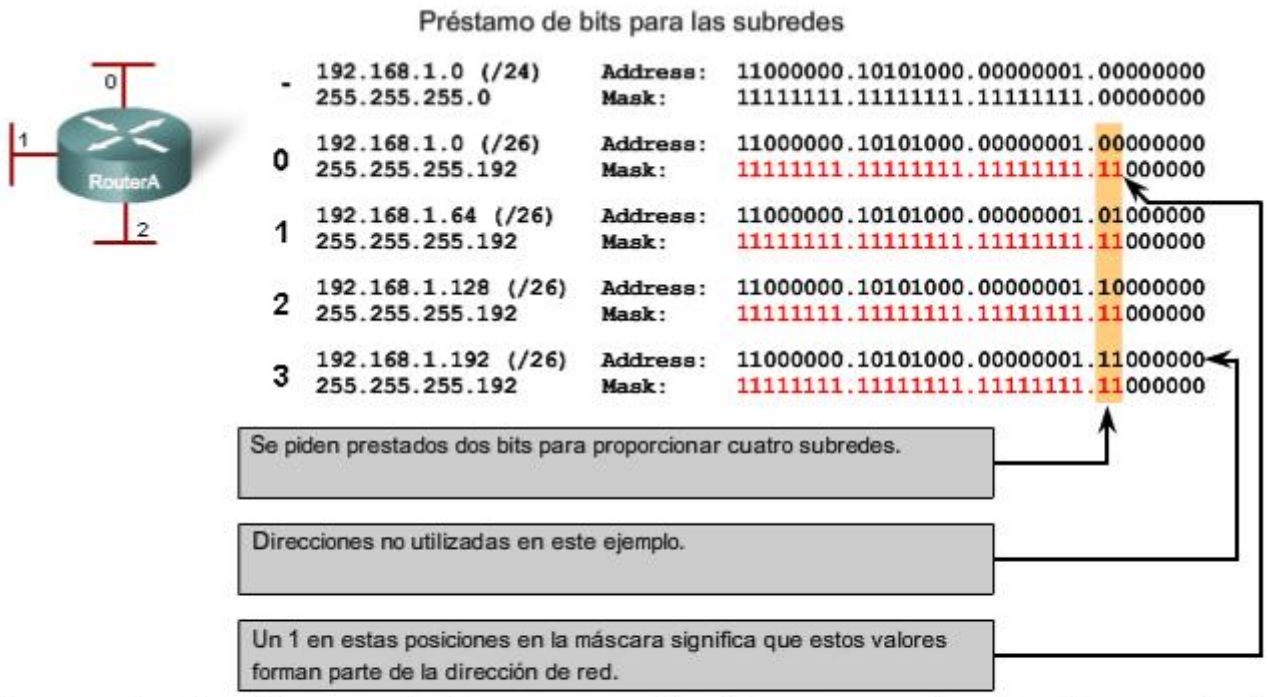
Subred 2: 128 = ***10***000000

Subred 3: 192 = ***11***000000

Aplique la fórmula de cálculo de host.

2^6 - 2 = 62 hosts por subred

Observe la figura del esquema de direccionamiento para estas redes.



Se encuentran disponibles más subredes, pero menos direcciones se encuentran disponibles por subred.

División en subredes | Esquema de direccionamiento

Préstamo de bits para las subredes

Esquema de direccionamiento: Ejemplo de 4 redes

Subred	Dirección de red	Rango de host	Dirección de broadca
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

División en subredes | Esquema de direccionamiento

Ejemplo con 6 subredes

Considere este ejemplo con cinco LAN y una WAN para un total de 6 redes. Observe la figura.

Para incluir 6 redes, coloque la subred 192.168.1.0 /24 en bloques de direcciones mediante la fórmula:

2^3 = 8

Para obtener al menos 6 subredes, pida prestados tres bits de host. Una máscara de subred 255.255.255.224 proporciona los tres bits de red adicionales.

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

0 = ***000***00000

32 = ***001***00000

64 = ***010***00000

96 = ***011***00000

128 = ***100***00000

160 = ***101***00000

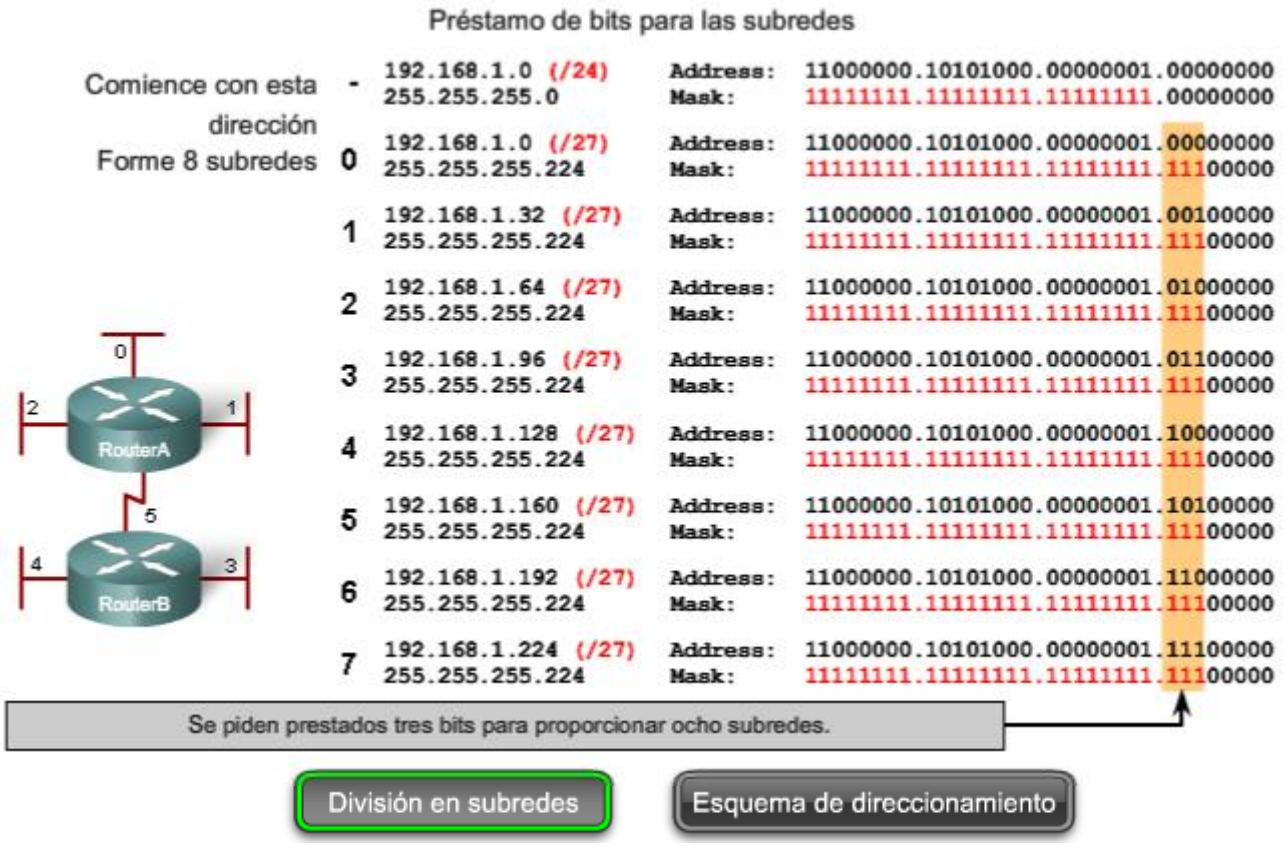
192 = ***110***00000

224 = ***11***100000

Aplique la fórmula de cálculo de host:

2^5 - 2 = 30 hosts por subred.

Observe la figura del esquema de direccionamiento para estas redes.



Préstamo de bits para las subredes

Esquema de direccionamiento: Ejemplo de 6 redes

Subred	Dirección de red	Rango de host	Dirección de broadca
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

División en subredes Esquema de direccionamiento

6.5.2 División en subredes: División en redes del tamaño adecuado

Cada red dentro de la internetwork de una empresa u organización está diseñada para incluir una cantidad limitada de hosts.

Algunas redes, como enlaces WAN punto a punto, sólo requieren un máximo de dos hosts. Otras redes, como una LAN de usuario en un edificio o departamento grande, pueden necesitar la inclusión de cientos de hosts. Es necesario que los administradores de red diseñen el esquema de direccionamiento de la internetwork para incluir la cantidad máxima de hosts para cada red. La cantidad de hosts en cada división debe permitir el crecimiento de la cantidad de hosts.

Determine la cantidad total de hosts

Vea el Paso 1 de la figura.

Primero, considere la cantidad total de hosts necesarios por toda la internetwork corporativa. Se debe usar un bloque de direcciones lo suficientemente amplio como para incluir todos los dispositivos en todas las redes corporativas. Esto incluye dispositivos de usuarios finales, servidores, dispositivos intermediarios e interfaces de routers.

Considere el ejemplo de una internetwork corporativa que necesita incluir 800 hosts en sus cuatro ubicaciones.

Determine la cantidad y el tamaño de las redes

Vea el Paso 2 de la figura.

A continuación, considere la cantidad de redes y el tamaño de cada una requeridas de acuerdo con los grupos comunes de hosts.

Se dividen las subredes de la red para superar problemas de ubicación, tamaño y control. Al diseñar el direccionamiento, se tienen en cuenta los factores para agrupar los hosts antes tratados:

- Agrupar basándonos en una ubicación geográfica común
- Agrupar hosts usados para propósitos específicos
- Agrupar basándonos en la propiedad

Cada enlace WAN es una red. Se crean subredes para la WAN que interconecta diferentes ubicaciones geográficas. Al conectar diferentes ubicaciones, se usa un router para dar cuenta de las diferencias de hardware entre las LAN y la WAN.

A pesar de que los hosts de una ubicación geográfica en común típicamente comprenden un solo bloque de direcciones, puede ser necesario realizar la división en subredes de este bloque para formar redes adicionales en cada ubicación. Es necesario crear subredes en diferentes ubicaciones que tengan hosts para las necesidades comunes de los usuarios. También puede suceder que otros grupos de usuarios requieran muchos recursos de red o que muchos usuarios requieran su propia subred. Además, es posible tener subredes para hosts especiales, como servidores. Es necesario tener en cuenta cada uno de estos factores para determinar la cantidad de redes.

También se deben tener en cuenta las necesidades de propiedad especiales de seguridad o administrativas que requieran redes adicionales.

Una herramienta útil para este proceso de planificación de direcciones es un diagrama de red. Un diagrama permite ver las redes y hacer una cuenta más precisa.

A fin de incluir 800 hosts en las cuatro ubicaciones de la compañía, se usa la aritmética binaria para asignar un bloque /22 (2^10-2=1022).

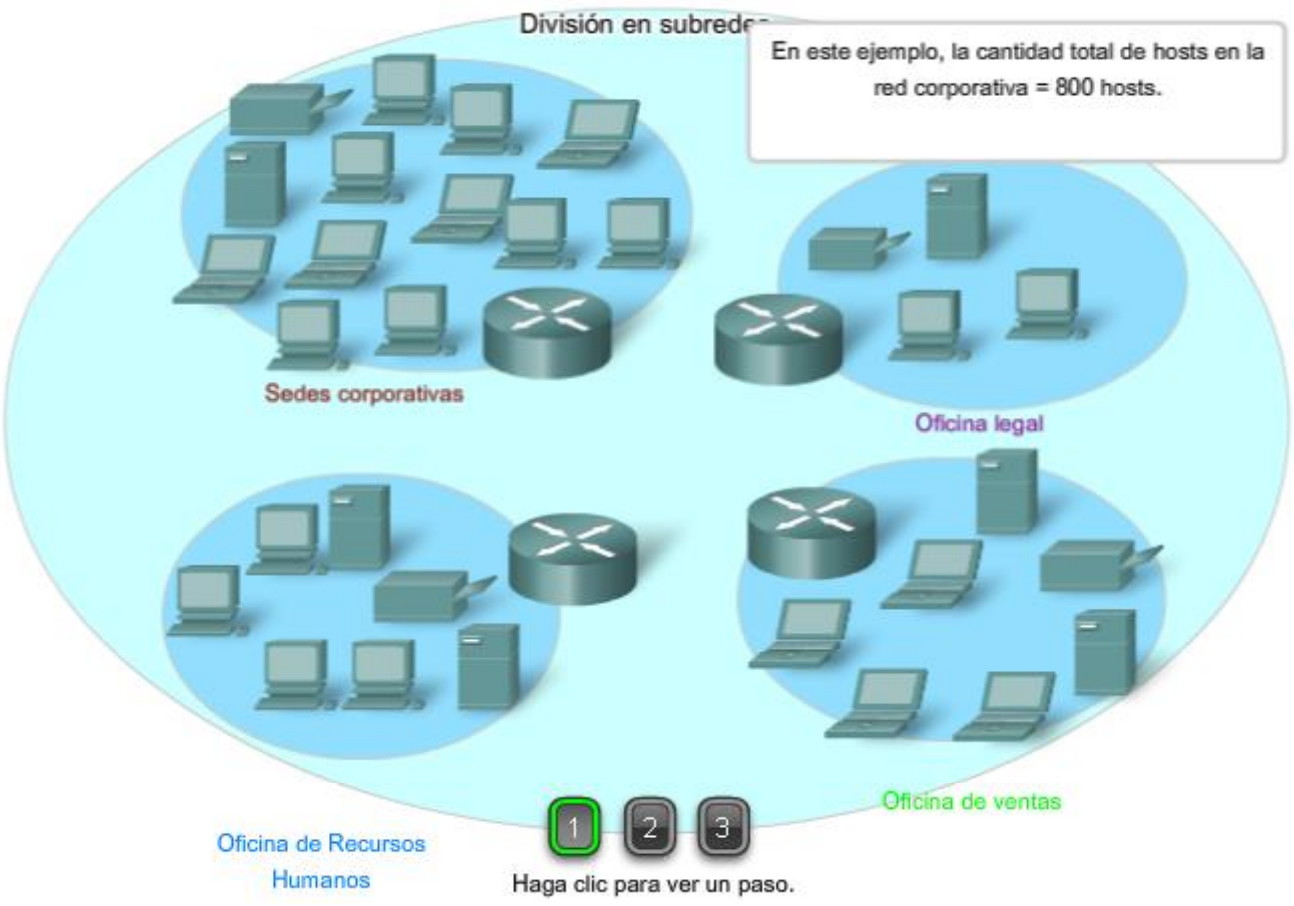
Asignación de direcciones

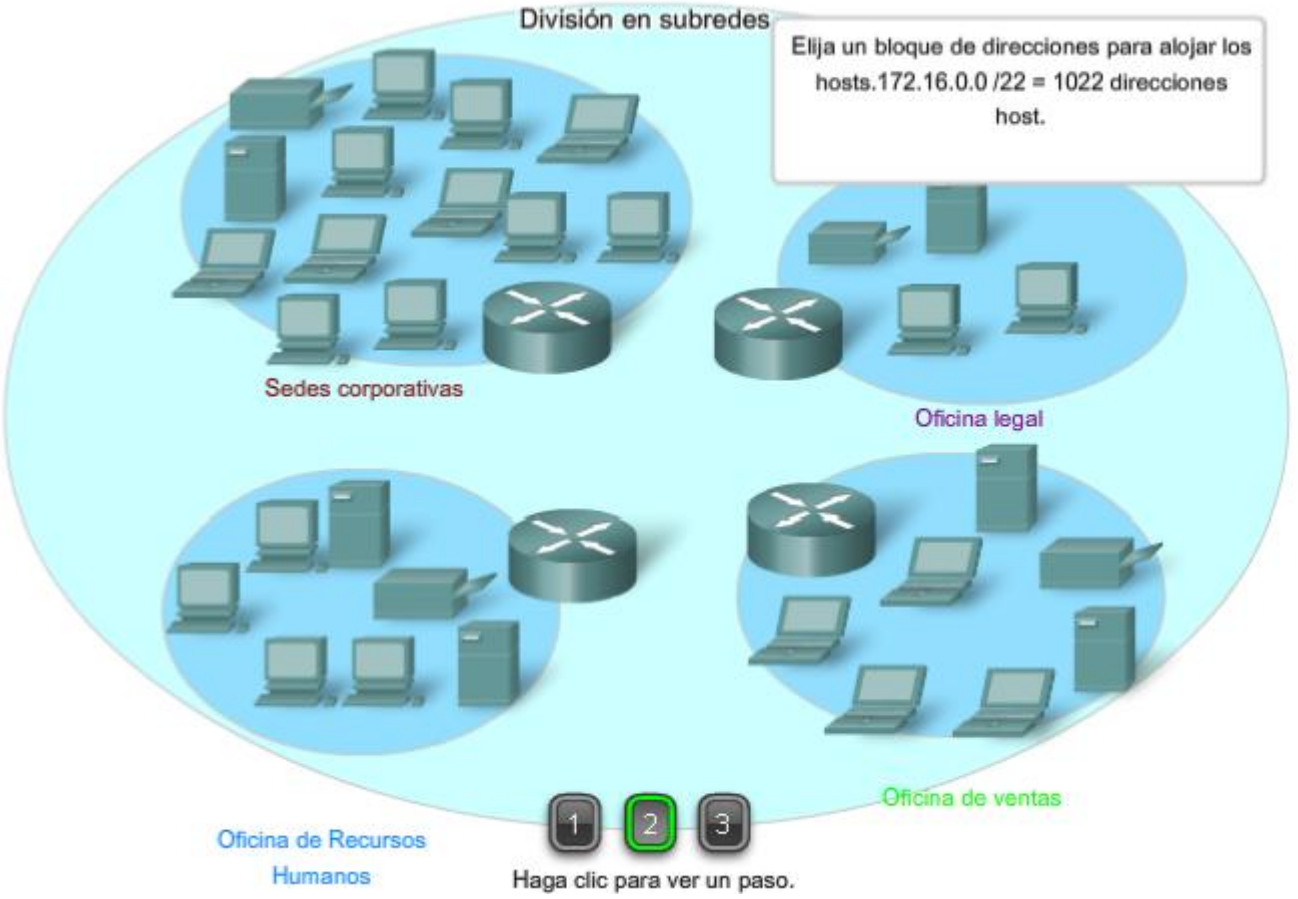
Vea el Paso 3 en la figura.

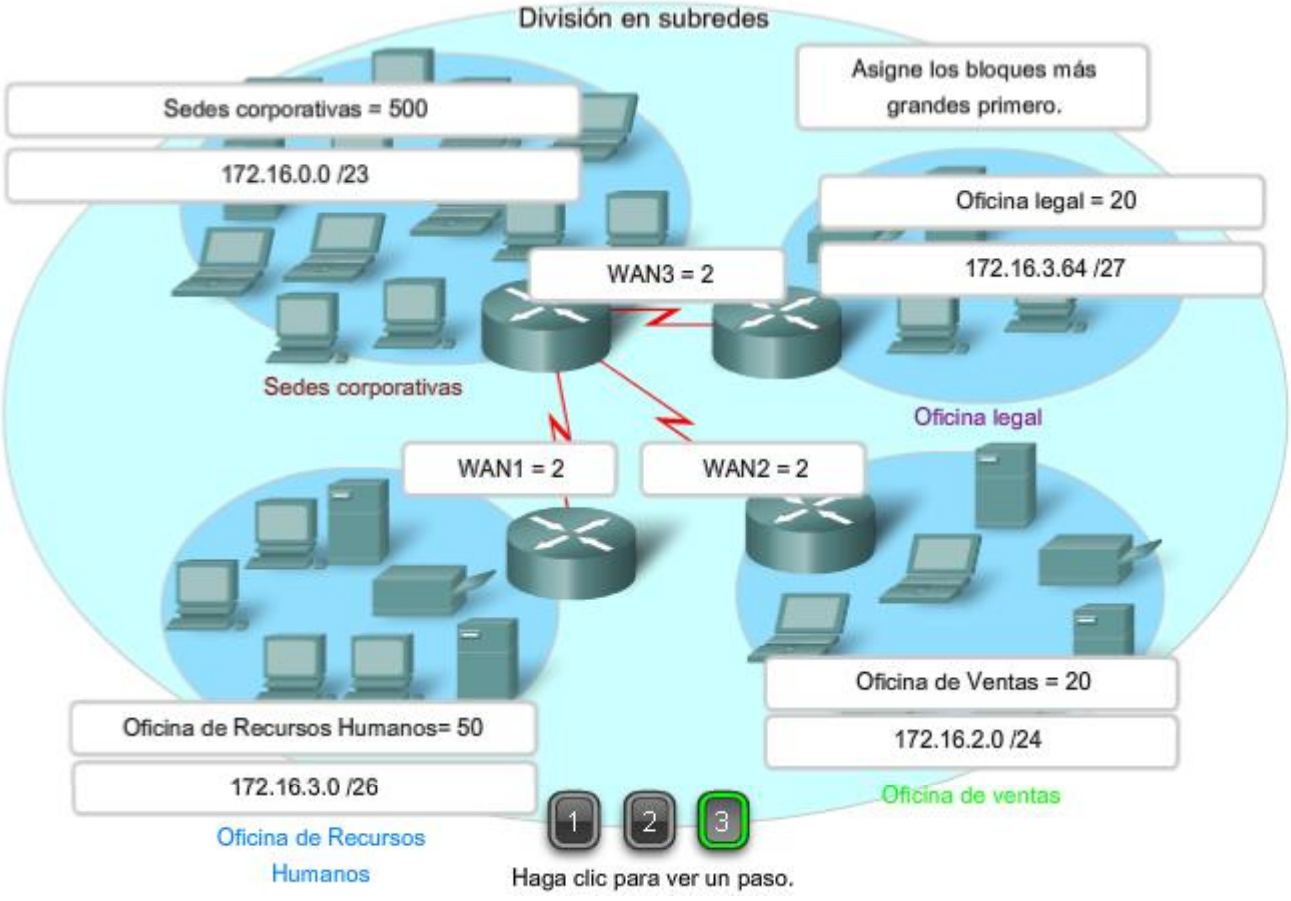
Ahora que se conoce la cantidad de redes y la cantidad de hosts para cada red, es necesario comenzar a asignar direcciones a partir del bloque general de direcciones.

Este proceso comienza al asignar direcciones de red para ubicaciones de redes especiales. Se comienza por las ubicaciones que requieren la mayoría de los hosts y se continúa hasta los enlaces punto a punto. Este proceso asegura que se disponga de bloques de direcciones lo suficientemente amplios para incluir los hosts y las redes para estas ubicaciones.

Al hacer las divisiones y asignar las subredes disponibles, es necesario asegurarse de que haya direcciones del tamaño adecuado para mayores demandas. **Además, se debe realizar una cuidadosa planificación para asegurar que los bloques de direcciones asignados a la subred no se superpongan.**







Otra herramienta útil para este proceso de planificación es una hoja de cálculo. Es posible colocar las direcciones en columnas para visualizar la asignación de direcciones.

Vea el Paso 1 de la figura.

En el ejemplo, se asignan bloques de direcciones a las cuatro ubicaciones, así como enlaces WAN.

Con los principales bloques asignados, se continúa realizando la división en subredes de cualquiera de las ubicaciones que requiera dicha división. En el ejemplo, se divide la sede corporativa en dos redes.

Vea el Paso 2 en la figura.

Esta división adicional de las direcciones a menudo se llama división en subredes. Al igual que con la división en subredes, es necesario planificar detenidamente la asignación de direcciones de manera que se disponga de bloques de direcciones.

La creación de nuevas redes más pequeñas de un bloque de direcciones determinado se hace ampliando la longitud del prefijo; es decir, agregando números 1 a la máscara de subred. De esta forma se asignan más bits a la porción de red de la dirección para brindar más patrones para la nueva subred. Para cada bit que se pide prestado, se duplica la cantidad de redes. Por ejemplo: si se usa 1 bit, existe la posibilidad de dividir ese bloque en dos redes más pequeñas. Con un solo patrón de bit podemos producir dos patrones únicos de bit, 1 y 0. Si pedimos prestados 2 bits podemos proveer 4 patrones únicos para representar redes 00, 01, 10 y 11. Los 3 bits permitirían 8 bloques y así sucesivamente.

Número total de Hosts utilizables

Recuerde de la sección anterior que al dividir el rango de dirección en subredes perdimos dos direcciones de host para cada red nueva. Éstas son la dirección de red y la dirección de broadcast.

La fórmula para calcular el número de hosts en una red es:

Hosts utilizables = 2 n- 2

Donde n es el número de bits remanentes a ser utilizados por los hosts.

Enlaces:

Calculador de subred: http://vlsm-calc.net

6.5.3 División en subredes: subdivisión de una subred

La subdivisión en subredes, o el uso de una Máscara de subred de longitud variable (VLSM), fue diseñada para maximizar la eficiencia del direccionamiento. Al identificar la cantidad total de hosts que utiliza la división tradicional en subredes, se asigna la misma cantidad de direcciones para cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían eficientes. Sin embargo, esto no es lo que suele suceder.

Por ejemplo: la topología en la Figura 1 muestra los requisitos de subred de siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres WAN. Con la dirección 192.168.20.0, es necesario pedir prestados 3 bits de los bits del host en el último octeto para satisfacer los requisitos de subred de siete subredes.

Estos bits son bits que se toman prestados al cambiar la máscara de subred correspondiente por números "1" para indicar que estos bits ahora se usan como bits de red. Entonces, el último octeto de la máscara se representa en binario con 11100000, que es 224. La nueva máscara 255.255.255.224 se representa mediante la notación /27 para representar un total de 27 bits para la máscara.

En binario, esta máscara de subred se representa como: **11111111.11111111.11111111.11100000**

Luego de tomar prestados tres de los bits de host para usar como bits de red, quedan cinco bits de host. Estos cinco bits permitirán más de 30 hosts por subred.

A pesar de que se ha cumplido la tarea de dividir la red en una cantidad adecuada de redes, esto se hizo mediante la pérdida significativa de direcciones no utilizadas. Por ejemplo: sólo se necesitan dos direcciones en cada subred para los enlaces WAN. Hay 28 direcciones no utilizadas en cada una de las tres subredes WAN que han sido bloqueadas en estos bloques de direcciones. Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de direcciones es característico del direccionamiento con clase.

Aplicar un esquema de división en subredes estándar al escenario no es muy eficiente y puede causar desperdicio. De hecho, este ejemplo es un modelo satisfactorio para mostrar cómo la división en subredes de una subred puede utilizarse para maximizar el uso de la dirección.

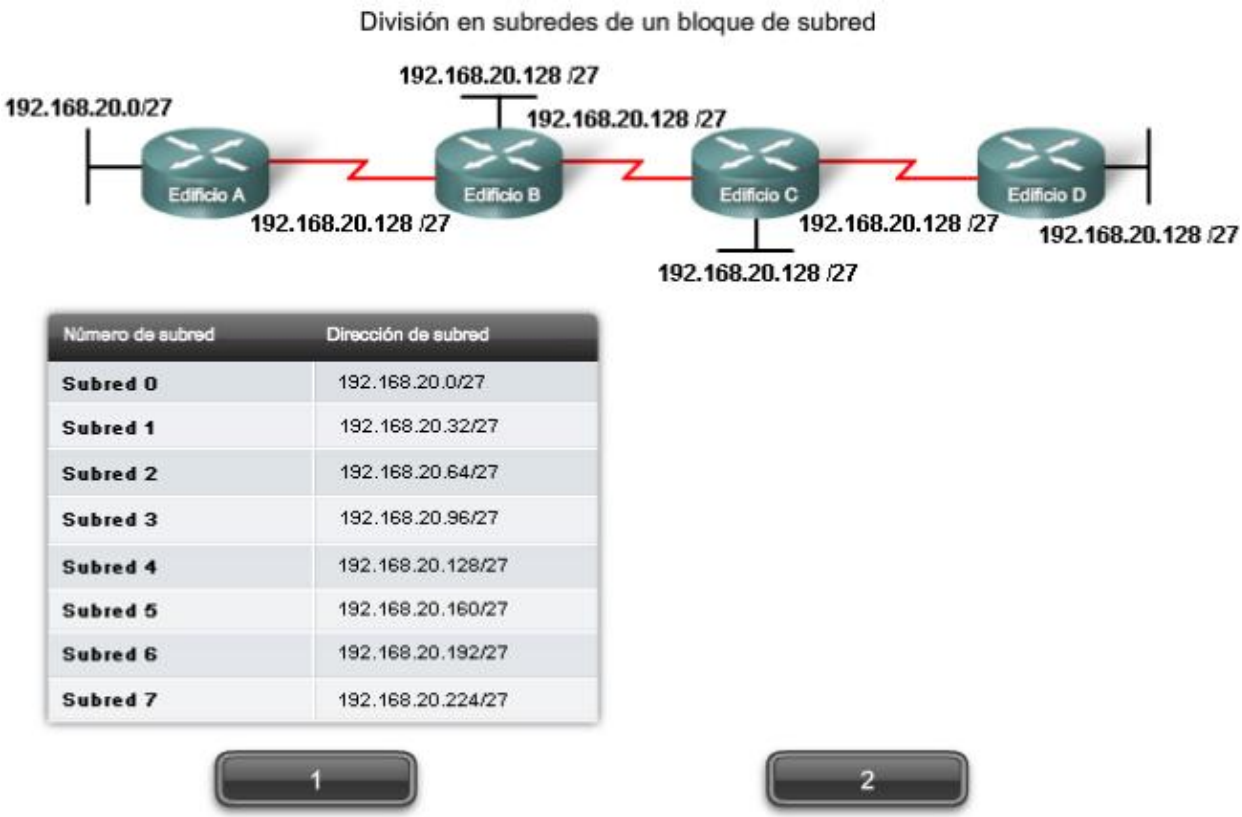
Obtención de más subredes para menos hosts

Como se mostró en ejemplos anteriores, se comenzó con las subredes originales y se obtuvieron subredes adicionales más pequeñas para usar en los enlaces WAN. Creando subredes más pequeñas, cada subred puede soportar 2 hosts, dejando libres las subredes originales para ser asignadas a otros dispositivos y evitando que muchas direcciones puedan ser desperdiciadas.

Para crear estas subredes más pequeñas para los enlaces WAN, comience con 192.168.20.192. Podemos dividir esta subred en subredes más pequeñas. Para suministrar bloques de direcciones para las WAN con dos direcciones cada una, se tomarán prestados tres bits de host adicionales para usar como bits de red.

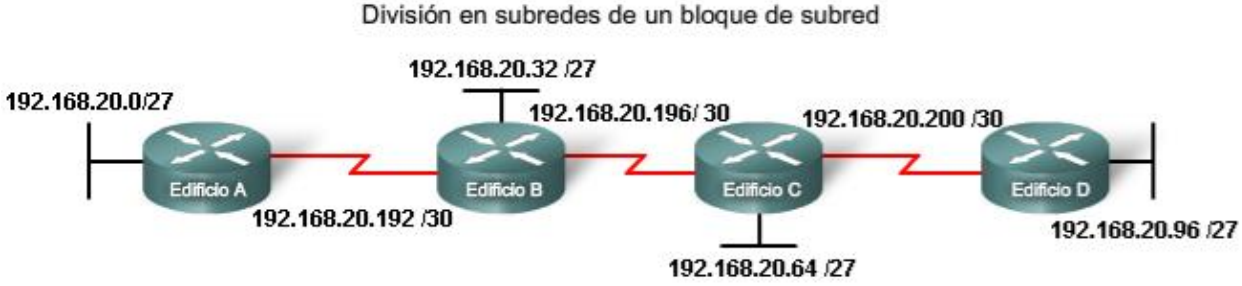
Dirección: 192.168.20.192 En binario: **11000000.10101000.00010100.11000000**
Máscara: 255.255.255.252 30 bits en binario: **11111111.11111111.11111111.11111100**

La topología en la figura 2 muestra un plan de direccionamiento que divide las subredes 192.168.20.192 /27 en subredes más pequeñas para suministrar direcciones para las WAN. De esta forma se reduce la cantidad de direcciones por subred a un tamaño apropiado para las WAN. Con este direccionamiento, se obtienen subredes 4, 5 y 7 disponibles para futuras redes, así como varias subredes disponibles para las WAN.



Número de subred	Dirección de subred
Subred 0	192.168.20.0/27
Subred 1	192.168.20.32/27
Subred 2	192.168.20.64/27
Subred 3	192.168.20.96/27
Subred 4	192.168.20.128/27
Subred 5	192.168.20.160/27
Subred 6	192.168.20.192/27
Subred 7	192.168.20.224/27

1 2



Número de subred	Dirección de subred
Subred 0	192.168.20.0/27
Subred 1	192.168.20.32/27
Subred 2	192.168.20.64/27
Subred 3	192.168.20.96/27
Subred 4	192.168.20.128/27
Subred 5	192.168.20.160/27
Subred 6	192.168.20.192/27
Subred 7	192.168.20.224/27

Número de subred	Dirección de subred
Subred 0	192.168.20.192/30
Subred 1	192.168.20.196/30
Subred 2	192.168.20.200/30
Subred 3	192.168.20.204/30
Subred 4	192.168.20.208/30
Subred 5	192.168.20.212/30
Subred 6	192.168.20.216/30
Subred 7	192.168.20.220/30

1 2

En la Figura 1, se considerará el direccionamiento desde otra perspectiva. Se tendrá en cuenta la división en subredes de acuerdo con la cantidad de hosts, incluso las interfaces de router y las conexiones WAN. Este escenario posee los siguientes requisitos:

- AtlantaHQ 58 direcciones de host
- PerthHQ 26 direcciones de host
- SydneyHQ 10 direcciones de host
- CorpusHQ 10 direccciones de host
- Enlaces WAN 2 direcciones de host (cada una)

Queda claro que, a partir de estos requerimientos, el uso de un esquema de armado estándar de subredes sería un gran desperdicio. En esta internetwork, el armado estándar de subredes bloquearía cada subred en bloques de 62 hosts, lo que llevaría a un significativo desperdicio de direcciones potenciales. Este desperdicio es especialmente evidente en la figura 2, donde se ve que la LAN PerthHQ admite 26 usuarios y que los routers de LAN SydneyHQ y CorpusHQ admiten 10 usuarios cada uno.

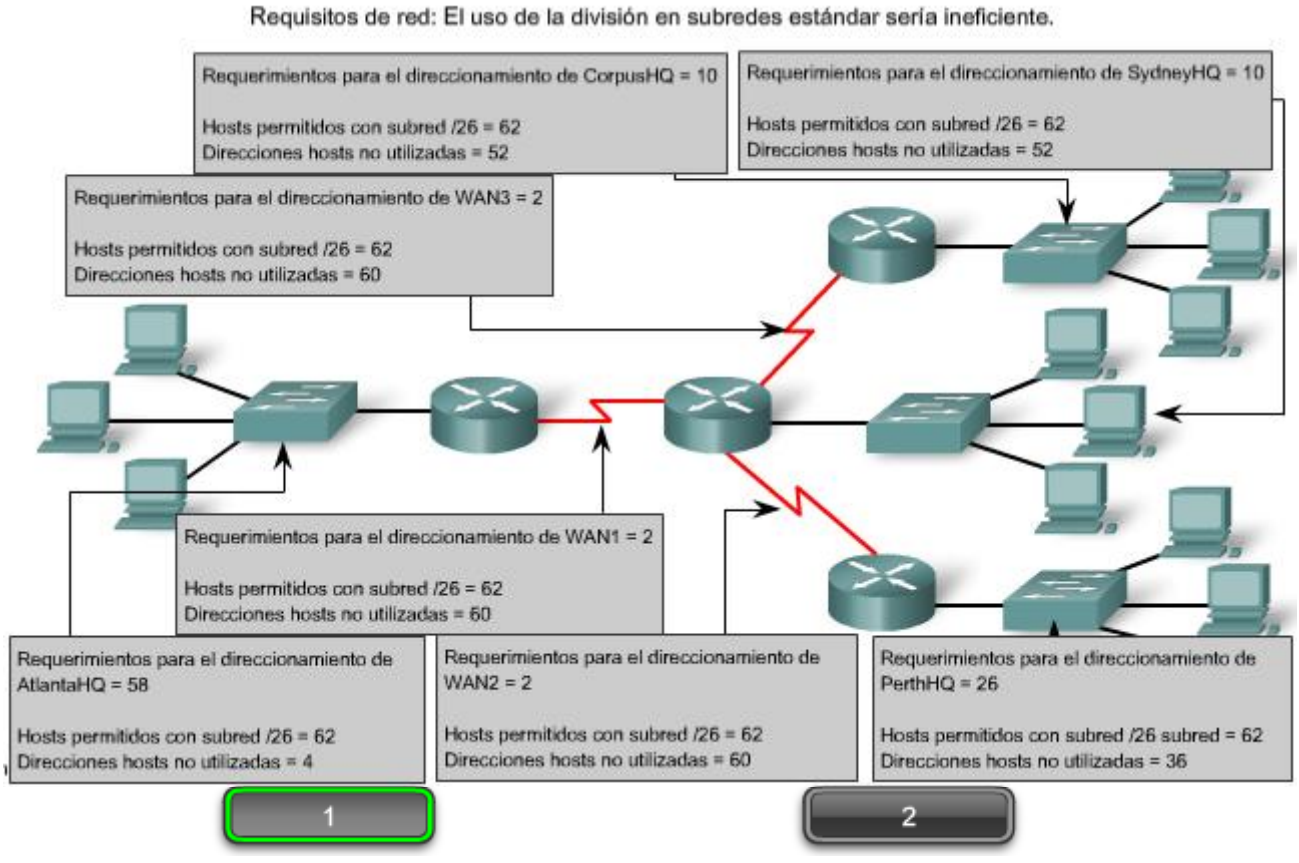
Por lo tanto, con el bloque de direcciones 192.168.15.0 /24 se comenzará a diseñar un esquema de direccionamiento que cumpla los requisitos y guarde posibles direcciones.

Obtención de más direcciones

Al crear un esquema de direccionamiento adecuado, siempre se comienza con la mayor demanda. En este caso, AtlantaHQ, con 58 usuarios, tiene la mayor demanda. A partir de 192.168.15.0, se precisarán 6 bits de host para incluir la demanda de 58 hosts; esto deja 2 bits adicionales para la porción de red. El prefijo para esta red sería /26 y la máscara de subred 255.255.255.192.

Comencemos por dividir en subredes el bloque original de direcciones 192.168.15.0 /24. Al usar la fórmula de hosts utilizables = 2^n - 2, se calcula que 6 bits de host permiten 62 hosts en la subred. Los 62 hosts satisfarían los 58 hosts requeridos del router de la compañía AtlantaHQ.
Dirección: 192.168.15.0
En binario: **11000000.10101000.00001111.00000000**
Máscara: 255.255.255.192
26 bits en binario: **11111111.11111111.11111111.11000000**

La página siguiente muestra el proceso de identificación de la próxima secuencia de pasos.



Requisitos de red: El uso de la división en subredes estándar sería ineficiente.

	Requisitos actuales	Desperdicio total de direcciones
AtlantaHQ	58 direcciones de host	4 direcciones
PerthHQ	26 direcciones de host	36 direcciones
SydneyHQ	10 direcciones de host	52 direcciones
CorpusHQ	10 direcciones de host	52 direcciones
Enlaces WAN	2 direcciones de host (cada una)	60 direcciones

Aquí se describen los pasos para implementar este esquema de armado de subredes.

Asignar la LAN de AtlantaHQ

Vea los pasos 1 y 2 en la figura.

El **primer paso** muestra un gráfico de planificación de red. El **segundo paso** en la figura muestra la entrada para AtlantaHQ. Esta entrada es el resultado del cálculo de una subred a partir del bloque original 192.168.15.0 /24 a fin de incluir la LAN más grande, la LAN AtlantaHQ con 58 hosts. Para realizar esta acción fue necesario pedir prestados 2 bits de host adicionales, para usar una máscara de bits /26.

Al compararlo, el siguiente esquema muestra cómo 192.168.15.0 se dividiría en subredes mediante el bloque de direccionamiento fijo para brindar bloques de direcciones lo suficientemente amplios:

Subred 0: 192.168.15.0 /26 rango de direcciones host de 1 a 62

Subred 1: 192.168.15.64 /26 rango de direcciones host de 65 a 126

Subred 2: 192.168.15.128 /26 rango de direcciones host de 129 a 190

Subred 3: 192.168.15.192 /26 rango de direcciones host de 193 a 254

Los bloques fijos permitirían sólo cuatro subredes y, por lo tanto, no dejarían suficientes bloques de direcciones para la mayoría de las subredes de esta internetwork. En lugar de continuar utilizando la siguiente subred disponible, es necesario asegurarse de que el tamaño de cada subred sea consecuente con los requisitos de host. Para usar un esquema de direccionamiento que se relacione directamente con los requisitos de host se debe usar un método diferente de división en subredes.

Asignación de la LAN PerthHQ

Vea al Paso 3 en la figura.

En el **tercer paso**, se observan los requisitos de la siguiente subred más grande. Ésta es la LAN PerthHQ, que requiere 28 direcciones de host, incluida la interfaz de router. Se debe comenzar con la siguiente dirección disponible 192.168.15.64 para crear un bloque de direcciones para esta subred. Al pedir prestado otro bit, se pueden satisfacer las necesidades de PerthHQ al tiempo que se limita el desperdicio de direcciones. El bit tomado deja una máscara /27 con el siguiente intervalo de direcciones:

192.168.15.64 /27 intervalo de direcciones de host 65 a 94

Este bloque de direcciones suministra 30 direcciones, lo cual satisface la necesidad de 28 hosts y deja espacio para el crecimiento de esta subred.

Asignación de las LAN SydneyHQ y CorpusHQ

Vea los Pasos 4 y 5 en la figura.

Los pasos **cuatro y cinco** proporcionan direccionamiento para las siguientes subredes más grandes: Las LAN SydneyHQ y CorpusHQ. En estos dos pasos, cada LAN tiene la misma necesidad de 10 direcciones host. Esta división en subredes requiere tomar prestado otro bit, a fin de ampliar la máscara a /28. A partir de la dirección 192.168.15.96, se obtienen los siguientes bloques de direcciones:

Subred 0: 192.168.15.96 /28 rango de direcciones host de 97 a 110

Subred 1: 192.168.15.112 /28 rango de direcciones host de 113 a 126

Estos bloques proporcionan 14 direcciones para los hosts y las interfaces del router para cada LAN.

Asignación de las WAN

Vea los Pasos 6, 7 y 8 en la figura.

Los **últimos tres pasos** muestran la división en subredes para los enlaces WAN. Con estos enlaces WAN punto a punto, sólo se necesitan dos direcciones. Con el objetivo de satisfacer los requisitos, se toman 2 bits más para usar una máscara /30. Al utilizar las próximas direcciones disponibles, se obtienen los siguientes bloques de direcciones:

Subred 0: 192.168.15.128 /30 rango de direcciones host de 129 a 130

Subred 1: 192.168.15.132 /30 rango de direcciones host de 133 a 134

Subred 2: 192.168.15.136 /30 rango de direcciones host de 137 a 138

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2	192.168.15.132	.133 - 134	.135	192.168.15.132 /30
WAN3 - 2	192.168.15.136	.137 - .138	.139	192.168.15.136 /30

Calcule la máscara de subred para cumplir con el requisito más grande - AtlantaHQ

Utilice la próxima dirección disponible .64 para calcular una máscara de subred para el próximo requisito más grande - PerthHQ.

Sydney necesita 12 direcciones. Utilice la próxima dirección disponible .96 para calcular una subred para el requisito de SydneyHQ de 10 hosts.

Utilice la próxima dirección disponible .112 para calcular una subred para CorpusHQ que también requiere 10 hosts.

Los enlaces WAN requieren 2 direcciones cada uno

El problema de red está solucionado

Los resultados muestran en nuestro esquema de direccionamiento, usando visualizaciones VLSM, una amplia gama de bloques de direcciones correctamente asignados. Como una mejor práctica, se comenzó por documentar los requisitos, de mayor a menor. Al comenzar por el requisito mayor, fue posible determinar que un esquema de bloque de direccionamiento fijo no permitiría un uso eficiente de las direcciones IPv4 y, como se muestra en este ejemplo, no suministraría suficientes direcciones.

Se tomaron prestados bits del bloque de direcciones asignado para crear los intervalos de direcciones que se ajusten a la topología. La figura 1 muestra los intervalos asignados. La figura 2 muestra la topología con la información de direccionamiento.

El uso de VLSM para asignar las direcciones permitió aplicar las guías de división en subredes para agrupar hosts según:

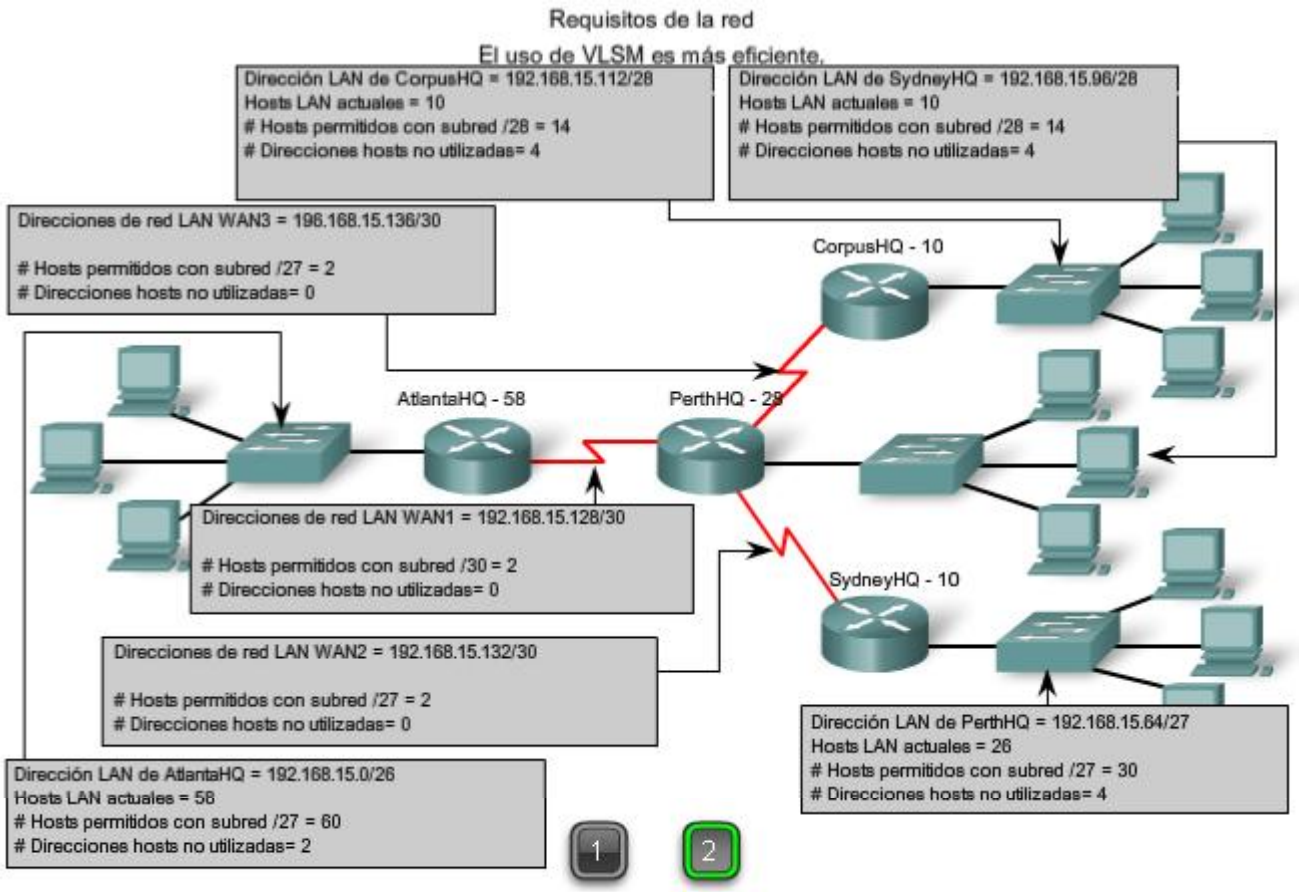
- Agrupación basada en ubicación geográfica común
- Agrupación de hosts utilizados para propósitos específicos
- Agrupación basada en propiedad

En nuestro ejemplo, basamos la agrupación en el número de hosts dentro de una ubicación geográfica común.

Requisitos de la red
El uso de VLSM es más eficiente.

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1-.62	.63	192.168.15.0/26
PerthHQ - 28	192.168.15.64	.65-.94	.95	192.168.15.64/27
SydneyHQ - 10	192.168.15.96	.97-.110	.111	192.168.15.96/28
CorpusHQ - 10	192.168.15.112	.113-.126	.127	192.168.15.112/28
WAN1 - 2	192.168.15.128	.129-.130	.131	192.168.15.128/30
WAN2 - 2	192.168.15.132	.133-.134	.135	192.168.15.132/30
WAN3 - 2	192.168.15.136	.137-.138	.139	192.168.15.136/30

1 2



Cuadro de VLSM

También se puede realizar la planificación de direcciones utilizando diversas herramientas. Un método es utilizar un cuadro de VLSM para identificar los bloques de direcciones disponibles para su uso y los que ya están asignados. Este método ayuda a evitar la asignación de direcciones que ya han sido asignadas. Con la red del ejemplo, es posible inspeccionar la planificación de direcciones usando el cuadro de VLSM para ver su uso.

El primer gráfico muestra la porción superior del cuadro. Un cuadro completo para su uso está disponible utilizando el enlace a continuación.

VLSM_Subnetting_Chart.pdf

Este cuadro se puede usar para planificar direcciones para redes con prefijos en el rango de /25 - /30. Éstos son los rangos de red de uso más frecuente para la división en subredes.

Igual que antes, se comienza con la subred que tiene la mayor cantidad de hosts. En este caso, es AtlantaHQ con 58 hosts.

Elección de un bloque de la LAN AtlantaHQ

Al observar el encabezado del cuadro de izquierda a derecha, se encuentra el encabezado que indica que el tamaño del bloque es suficiente para los 58 hosts. Ésta es la columna /26. En esta columna, se observan cuatro bloques de este tamaño:

.0 /26 rango de direcciones host de 1 a 62

.64 /26 rango de direcciones host de 65 a 126

.128 /26 rango de direcciones host de 129 a 190

.192 /26 rango de direcciones host de 193 a 254

Dado que no se han asignado direcciones, es posible elegir cualquiera de estos bloques. A pesar de que pueden existir motivos para usar un bloque diferente, comúnmente se usa el primer bloque disponible, el .0 /26. Esta asignación se muestra en la Figura 2.

Una vez que se asigna el bloque de direcciones, estas direcciones se consideran usadas. Asegúrese de marcar este bloque, al igual que cualquier otro bloque mayor que contenga estas direcciones. Al marcarlo, se pueden ver las direcciones que no pueden ser usadas y las que todavía están disponibles. Al observar la Figura 3, cuando se asigna el bloque .0 /26 a AtlantaHQ, se marcan todos los bloques que contienen estas direcciones.

Elección de un bloque para la LAN PerthHQ

A continuación, se necesita un bloque de direcciones para la LAN PerthHQ de 26 hosts. Al desplazarse por el encabezado del cuadro, se encuentra la columna con subredes de tamaño suficiente para esta LAN. Después, es necesario desplazarse hacia abajo en el cuadro hasta el primer bloque disponible. En la Figura 3, se resalta la sección del cuadro disponible para PerthHQ. El bit que se tomó prestado hace que el bloque de direcciones esté disponible para esta LAN. Aunque podríamos haber elegido cualquiera de los bloques disponibles, generalmente procedemos con el primer bloque disponible que satisface la necesidad.

El rango de dirección para este bloque es:
.64 /27 rango de dirección host 65 a 94

Elección de bloques para la LAN de SydneyHQ y la LAN de CorpusHQ

Como se muestra en la Figura 4, continuamos marcando los bloques de dirección para evitar la superposición de asignaciones de dirección. Para satisfacer las necesidades de las LAN SydneyHQ y CorpusHQ, se asignan nuevamente los próximos bloques disponibles. Esta vez se realiza un desplazamiento hasta la columna /28 y hacia abajo a los bloques .96 y .112. Note que la sección del cuadro disponible para SydneyHQ y CorpusHQ está resaltada.

Estos bloques son:

.96 /28 rango de dirección host 97 a 110

.112 /28 rango de dirección host 113 a 126

Elección de bloques para las WAN

El último requerimiento para el direccionamiento es para las conexiones WAN entre las redes. Al observar la Figura 5, se realiza un desplazamiento hacia la columna de la derecha hasta el prefijo /30. A continuación, debe desplazarse hacia abajo y resaltar tres bloques disponibles. Estos bloques suministrarán las 2 direcciones por WAN.

Estos tres bloques son:

.128 /30 rango de direcciones host de 129 a 130

.132 /30 rango de direcciones host de 133 a 134

.136 /30 rango de direcciones host de 137 a 138

Al observar la Figura 6, las direcciones asignadas a la WAN están marcadas para indicar que los bloques que las contienen ya no pueden ser asignados. Observe en la asignación de estos intervalos de WAN que se han marcado varios bloques más grandes que no pueden ser asignados. Éstos son:

.128 /25

.128 /26

.128 /27

.128 /28

.128 /29

.136 /29

Debido a que estas direcciones son parte de estos bloques más grandes, la asignación de estos bloques se superpondría con el uso de estas direcciones.

Como se ha podido observar, el uso de VLSM permite maximizar el direccionamiento y minimizar el desperdicio. El método del cuadro que se mostró es apenas otra herramienta que los administradores y técnicos de red pueden usar para crear un esquema de direccionamiento que ocasione menos desperdicio que el enfoque de bloques de tamaño fijos.

/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0				.0 (.1-.6)	.0 (.1-.2)
.4			.0 (.1-.14)		.4 (.5-.6)
.8		.0 (.1-.30)		.8 (.9 - .14)	.8 (.9 - .10)
.12					.12 (.13-.14)
.16			.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20					.20 (.21-.22)
.24				.24 (.25-.30)	.24 (.25-.26)
.28	.0 (.1-.62)				.28 (.29-.30)
.32			.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36					.36 (.37-.38)
.40		.32 (.33-.62)		.40 (.41-.46)	.40 (.41-.42)
.44					.44 (.45-.46)
.48			.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52					.52 (.53-.54)
.56				.56 (.57-.62)	.56 (.57-.58)
.60					.60 (.61-.62)
.64	.0		.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68					.68 (.69-.70)
.72		.64 (.65-.94)		.72 (.73-.78)	.72 (.73-.74)
.76					.76 (.77-.78)
.80			.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84					.84 (.85-.86)
.88				.88 (.89-.94)	.88 (.89-.90)
.92					.92 (.93-.94)
.96	.64 (.65-.126)		.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100					.100 (.101-.102)
.104		.96 (.97-.126)		.104 (.105-.110)	.104 (.105-.106)
.108					.108 (.109-.110)
.112			.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116					.116 (.117-.118)
.120				.120 (.121-.126)	.120 (.121-.122)
.124					.124 (.125-.126)

1 2 3 4 5 6

/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0	Bloquear AtlantaHQ			.0 (.1-.6)	.0 (.1-.2)
.4			.0 (.1-.14)		.4 (.5-.6)
.8		.0 (.1-.30)		.8 (.9 - .14)	.8 (.9 - .10)
.12					.12 (.13-.14)
.16			.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20					.20 (.21-.22)
.24				.24 (.25-.30)	.24 (.25-.26)
.28	.0 (.1-.62)				.28 (.29-.30)
.32			.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36					.36 (.37-.38)
.40		.32 (.33-.62)		.40 (.41-.46)	.40 (.41-.42)
.44					.44 (.45-.46)
.48			.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52					.52 (.53-.54)
.56				.56 (.57-.62)	.56 (.57-.58)
.60					.60 (.61-.62)
.64	.0		.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68					.68 (.69-.70)
.72		.64 (.65-.94)		.72 (.73-.78)	.72 (.73-.74)
.76					.76 (.77-.78)
.80			.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84					.84 (.85-.86)
.88				.88 (.89-.94)	.88 (.89-.90)
.92					.92 (.93-.94)
.96	.64 (.65-.126)		.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100					.100 (.101-.102)
.104		.96 (.97-.126)		.104 (.105-.110)	.104 (.105-.106)
.108					.108 (.109-.110)
.112			.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116					.116 (.117-.118)
.120				.120 (.121-.126)	.120 (.121-.122)
.124					.124 (.125-.126)

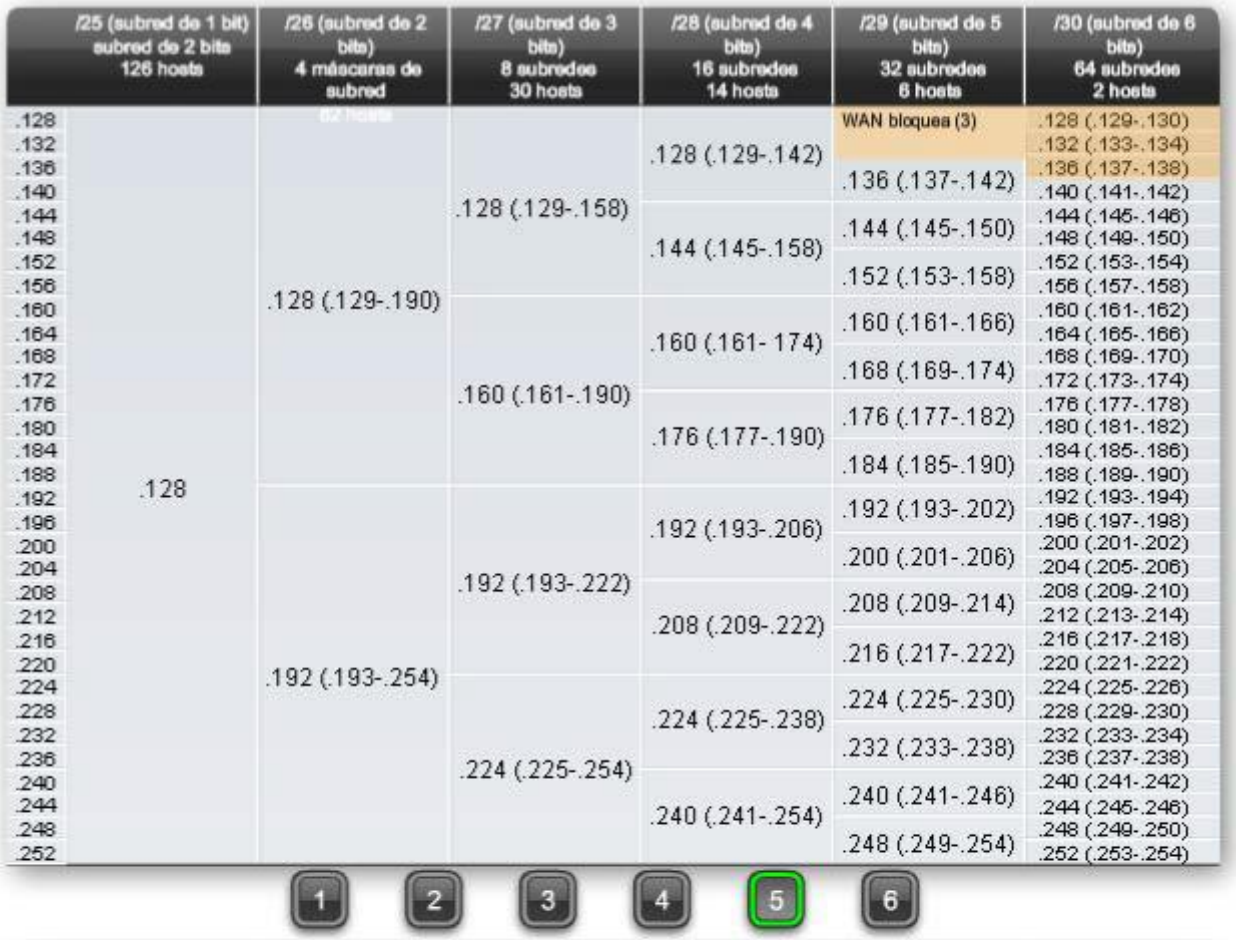
1 2 3 4 5 6

	/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0	Dirección asignada	.0 (.1-.62)	.0 (.1-.30)	.0 (.1-.14)	.0 (.1-.6)	.0 (.1-.2)
.4						.4 (.5-.6)
.8					.8 (.9 - .14)	.8 (.9 - .10)
.12						.12 (.13-.14)
.16				.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20						.20 (.21-.22)
.24					.24 (.25-.30)	.24 (.25-.26)
.28						.28 (.29-.30)
.32			.32 (.33-.62)	.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36						.36 (.37-.38)
.40					.40 (.41-.46)	.40 (.41-.42)
.44						.44 (.45-.46)
.48				.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52						.52 (.53-.54)
.56					.56 (.57-.62)	.56 (.57-.58)
.60						.60 (.61-.62)
.64	.0	.64 (.65-.126)	Bloquear PerthHQ .64 (.65-.94)	.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68						.68 (.69-.70)
.72					.72 (.73-.78)	.72 (.73-.74)
.76						.76 (.77-.78)
.80				.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84						.84 (.85-.86)
.88					.88 (.89-.94)	.88 (.89-.90)
.92						.92 (.93-.94)
.96			.96 (.97-.126)	.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100						.100 (.101-.102)
.104					.104 (.105-.110)	.104 (.105-.106)
.108						.108 (.109-.110)
.112				.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116						.116 (.117-.118)
.120					.120 (.121-.126)	.120 (.121-.122)
.124						.124 (.125-.126)

1 2 3 4 5 6

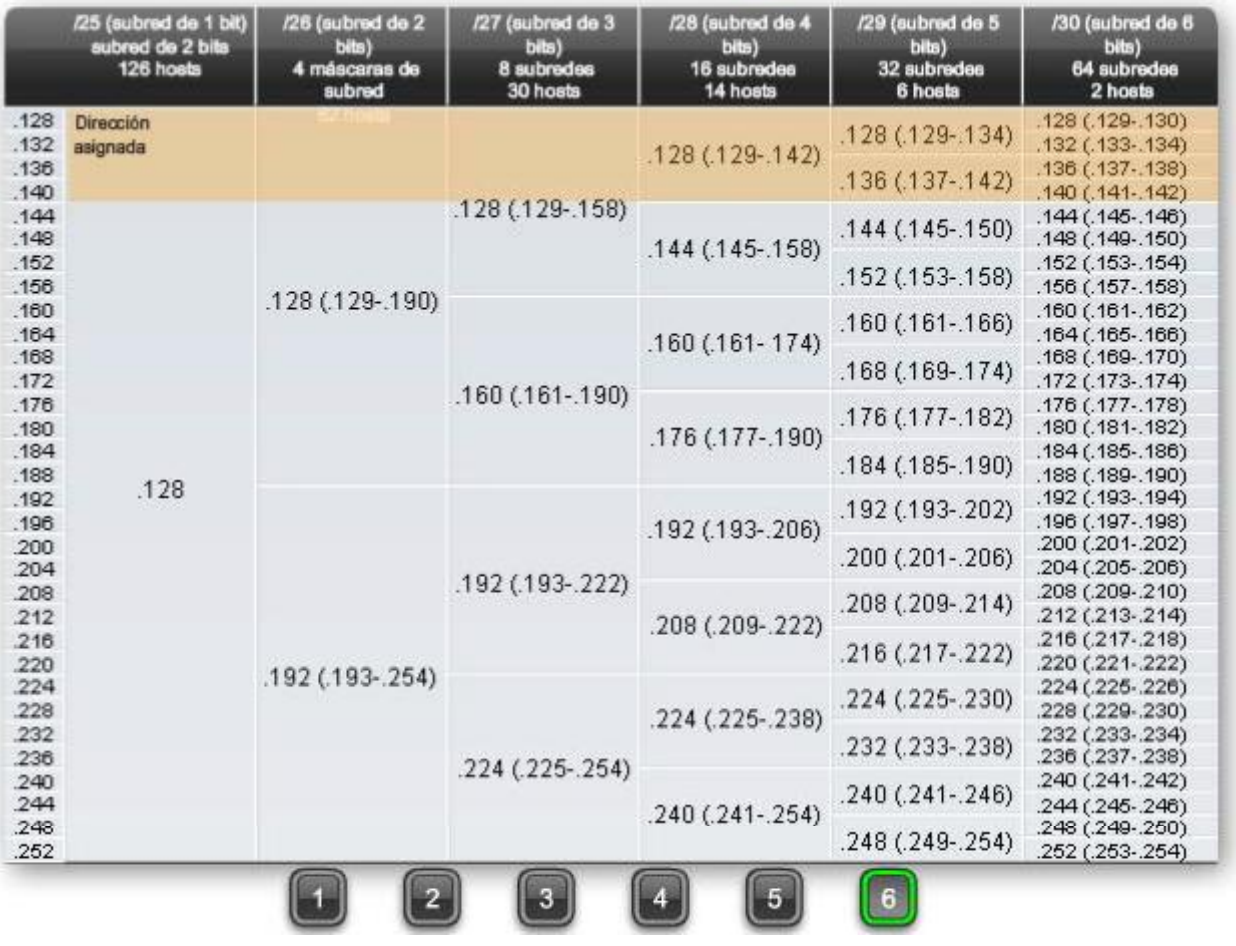
	/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0	Dirección asignada	.0 (.1-.62)	.0 (.1-.30)	.0 (.1-.14)	.0 (.1-.6)	.0 (.1-.2)
.4						.4 (.5-.6)
.8					.8 (.9 - .14)	.8 (.9 - .10)
.12						.12 (.13-.14)
.16				.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20						.20 (.21-.22)
.24					.24 (.25-.30)	.24 (.25-.26)
.28						.28 (.29-.30)
.32			.32 (.33-.62)	.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36						.36 (.37-.38)
.40					.40 (.41-.46)	.40 (.41-.42)
.44						.44 (.45-.46)
.48				.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52						.52 (.53-.54)
.56					.56 (.57-.62)	.56 (.57-.58)
.60						.60 (.61-.62)
.64	.0	.64 (.65-.126)	.64 (.65-.94)	.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68						.68 (.69-.70)
.72					.72 (.73-.78)	.72 (.73-.74)
.76						.76 (.77-.78)
.80				.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84						.84 (.85-.86)
.88					.88 (.89-.94)	.88 (.89-.90)
.92						.92 (.93-.94)
.96			Bloquear SydneyHQ .96 (.97-.126) Bloquear CorpusHQ	.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100						.100 (.101-.102)
.104					.104 (.105-.110)	.104 (.105-.106)
.108						.108 (.109-.110)
.112				.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116						.116 (.117-.118)
.120					.120 (.121-.126)	.120 (.121-.122)
.124						.124 (.125-.126)

1 2 3 4 5 6



	/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.128	.128	.128 (.129-.190)	.128 (.129-.158)	.128 (.129-.142)	WAN bloquea (3)	.128 (.129-.130)
.132						.132 (.133-.134)
.136					.136 (.137-.142)	.136 (.137-.138)
.140						.140 (.141-.142)
.144				.144 (.145-.158)	.144 (.145-.150)	.144 (.145-.146)
.148						.148 (.149-.150)
.152					.152 (.153-.158)	.152 (.153-.154)
.156						.156 (.157-.158)
.160			.160 (.161-.190)	.160 (.161- 174)	.160 (.161-.166)	.160 (.161-.162)
.164						.164 (.165-.166)
.168					.168 (.169-.174)	.168 (.169-.170)
.172						.172 (.173-.174)
.176				.176 (.177-.190)	.176 (.177-.182)	.176 (.177-.178)
.180						.180 (.181-.182)
.184					.184 (.185-.190)	.184 (.185-.186)
.188						.188 (.189-.190)
.192		.192 (.193-.254)	.192 (.193-.222)	.192 (.193-.206)	.192 (.193-.202)	.192 (.193-.194)
.196						.196 (.197-.198)
.200					.200 (.201-.206)	.200 (.201-.202)
.204						.204 (.205-.206)
.208				.208 (.209-.222)	.208 (.209-.214)	.208 (.209-.210)
.212						.212 (.213-.214)
.216					.216 (.217-.222)	.216 (.217-.218)
.220						.220 (.221-.222)
.224			.224 (.225-.254)	.224 (.225-.238)	.224 (.225-.230)	.224 (.225-.226)
.228						.228 (.229-.230)
.232					.232 (.233-.238)	.232 (.233-.234)
.236						.236 (.237-.238)
.240				.240 (.241-.254)	.240 (.241-.246)	.240 (.241-.242)
.244						.244 (.245-.246)
.248					.248 (.249-.254)	.248 (.249-.250)
.252						.252 (.253-.254)

1 2 3 4 5 6



	/25 (subred de 1 bit) subred de 2 bits 126 hosts	/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.128	Dirección asignada			.128 (.129-.142)	.128 (.129-.134)	.128 (.129-.130)
.132						.132 (.133-.134)
.136					.136 (.137-.142)	.136 (.137-.138)
.140						.140 (.141-.142)
.144	.128	.128 (.129-.190)	.128 (.129-.158)	.144 (.145-.158)	.144 (.145-.150)	.144 (.145-.146)
.148						.148 (.149-.150)
.152					.152 (.153-.158)	.152 (.153-.154)
.156						.156 (.157-.158)
.160			.160 (.161-.190)	.160 (.161- 174)	.160 (.161-.166)	.160 (.161-.162)
.164						.164 (.165-.166)
.168					.168 (.169-.174)	.168 (.169-.170)
.172						.172 (.173-.174)
.176				.176 (.177-.190)	.176 (.177-.182)	.176 (.177-.178)
.180						.180 (.181-.182)
.184					.184 (.185-.190)	.184 (.185-.186)
.188						.188 (.189-.190)
.192		.192 (.193-.254)	.192 (.193-.222)	.192 (.193-.206)	.192 (.193-.202)	.192 (.193-.194)
.196						.196 (.197-.198)
.200					.200 (.201-.206)	.200 (.201-.202)
.204						.204 (.205-.206)
.208				.208 (.209-.222)	.208 (.209-.214)	.208 (.209-.210)
.212						.212 (.213-.214)
.216					.216 (.217-.222)	.216 (.217-.218)
.220						.220 (.221-.222)
.224			.224 (.225-.254)	.224 (.225-.238)	.224 (.225-.230)	.224 (.225-.226)
.228						.228 (.229-.230)
.232					.232 (.233-.238)	.232 (.233-.234)
.236						.236 (.237-.238)
.240				.240 (.241-.254)	.240 (.241-.246)	.240 (.241-.242)
.244						.244 (.245-.246)
.248					.248 (.249-.254)	.248 (.249-.250)
.252						.252 (.253-.254)

1 2 3 4 5 6

6.5.4 Determinación de la dirección de red

La actividad en la figura ofrece práctica para la determinación de direcciones de red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host, deberá ingresar la dirección de red correcta. Luego, se mostrará si la respuesta es correcta.

Actividad

De acuerdo con la dirección IP host y la máscara de subred, ingrese la dirección de red en binario y en decimal.

Dirección host	10	32	72	32
Máscara de subred	255	255	252	0
Dirección host en binario	00001010	00100000	01001000	00100000
Máscara de subred en binario	11111111	11111111	11111100	00000000
Dirección de red en binario				
Dirección de red en decimal				

6.5.5 Cálculo de la cantidad de host

La actividad en la figura ofrece práctica para determinar la cantidad máxima de hosts para una red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host, deberá ingresar la cantidad máxima de hosts para la red descrita. Luego, se mostrará si la respuesta es correcta.

Actividad

Según la dirección de red y la máscara de subred, ingrese la cantidad de hosts posibles. Luego, haga clic en cantidad de hosts para ingresar su respuesta.

Dirección de red	10	0	0	0
Máscara de subred	255	255	252	0
Dirección de red en binario	00001010	00000000	00000000	00000000
Máscara de subred en binario	11111111	11111111	11111100	00000000
Cantidad de hosts				

6.5.6 Determinación de direcciones válidas para hosts

La actividad en la figura ofrece práctica para determinar direcciones hosts, de red y de broadcast para una red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host, deberá ingresar direcciones hosts, de red y de broadcast. Luego, se mostrará si la respuesta es correcta.

Actividad

Dadas la dirección de red y la máscara de subred, defina el rango de hosts, la dirección de broadcast y la siguiente dirección de red. Haga clic en el octeto de la tabla para ingresar la información.

Dirección de red en formato decimal	10	104	47	0
Máscara de subred en formato decimal	255	255	255	0
Dirección de red en formato binario	00001010	01101000	00101111	00000000
Máscara de subred en formato binario	11111111	11111111	11111111	00000000
Primer dirección IP de host utilizable en formato decimal	1er octeto	Segundo	3er octeto	4to octeto
Última dirección IP de host utilizable en formato decimal	1er octeto	Segundo	3er octeto	4to octeto
Dirección de broadcast en formato decimal	1er octeto	Segundo	3er octeto	4to octeto
Siguiente dirección de red en formato decimal	1er octeto	Segundo	3er octeto	4to octeto

6.6 Prueba de la capa de Red

6.6.1 Ping 127.0.0.1 – Prueba del stack local

Ping es una utilidad para probar la conectividad IP entre hosts. Ping envía solicitudes de respuestas desde una dirección host específica. Ping usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control Message Protocol (Protocolo de mensajes de control de Internet, ICMP). Ping usa un datagrama de solicitud de eco ICMP.

Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

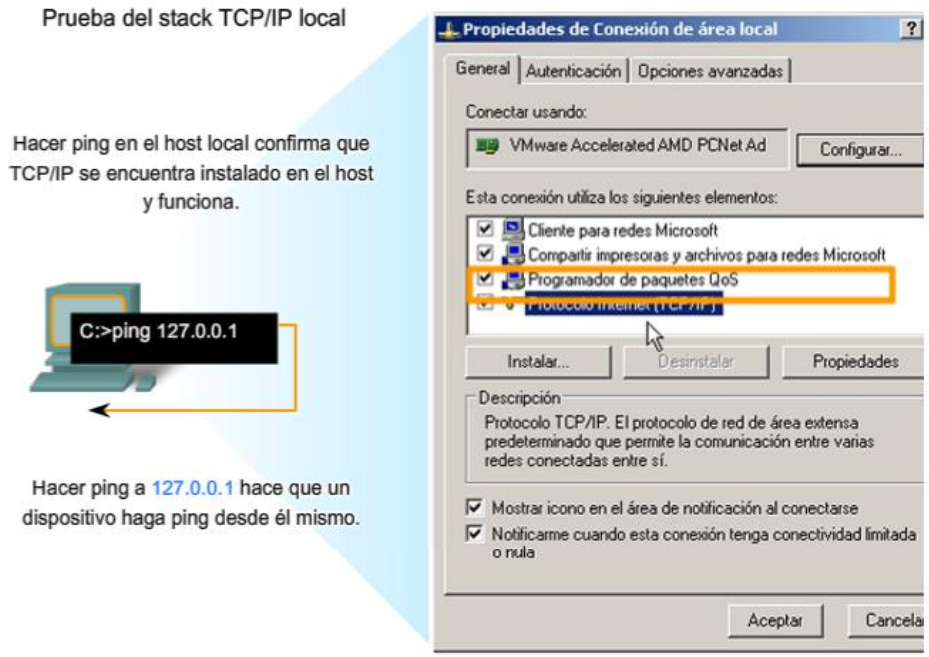
A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. Ping posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

Ping del loopback local

Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna del IP en el host local. Para hacer esta prueba, se realiza el ping de la dirección reservada especial del loopback local (127.0.0.1), como se muestra en la figura.

Una respuesta de 127.0.0.1 indica que el IP está correctamente instalado en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior del stack de red. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el TCP/IP no funciona en el host.



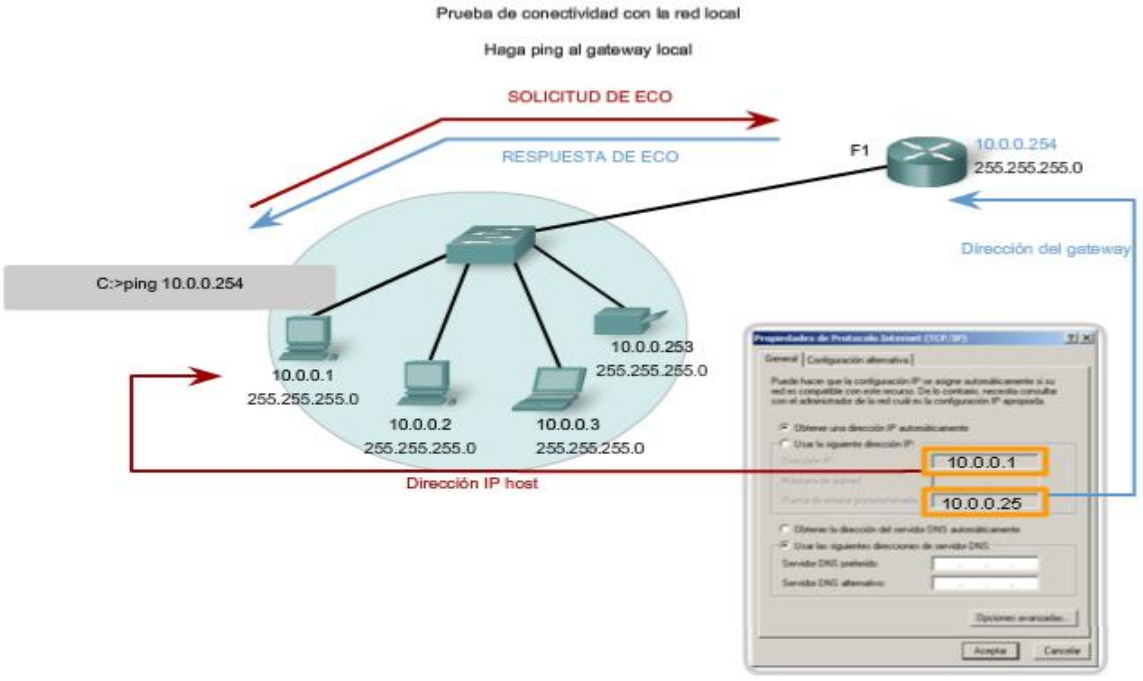
6.6.2 Ping de gateway – Prueba de la conectividad de la LAN local

También es posible utilizar el ping para probar la capacidad de comunicación del host en la red local. Generalmente, esto se hace haciendo ping a la dirección IP del gateway del host, como se muestra en la figura. Un ping en el gateway indica que la interfaz del host y del router que funcionan como gateway funcionan en la red local.

Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de gateway no responde, se puede intentar con la dirección IP de otro host que sepa que funciona en la red local.

Si el gateway u otro host responden, entonces los hosts locales pueden comunicarse con éxito en la red local. Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway.

Una posibilidad es que se tiene la dirección equivocada para el gateway. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping. También puede suceder que otros hosts tengan la misma restricción de seguridad aplicada.



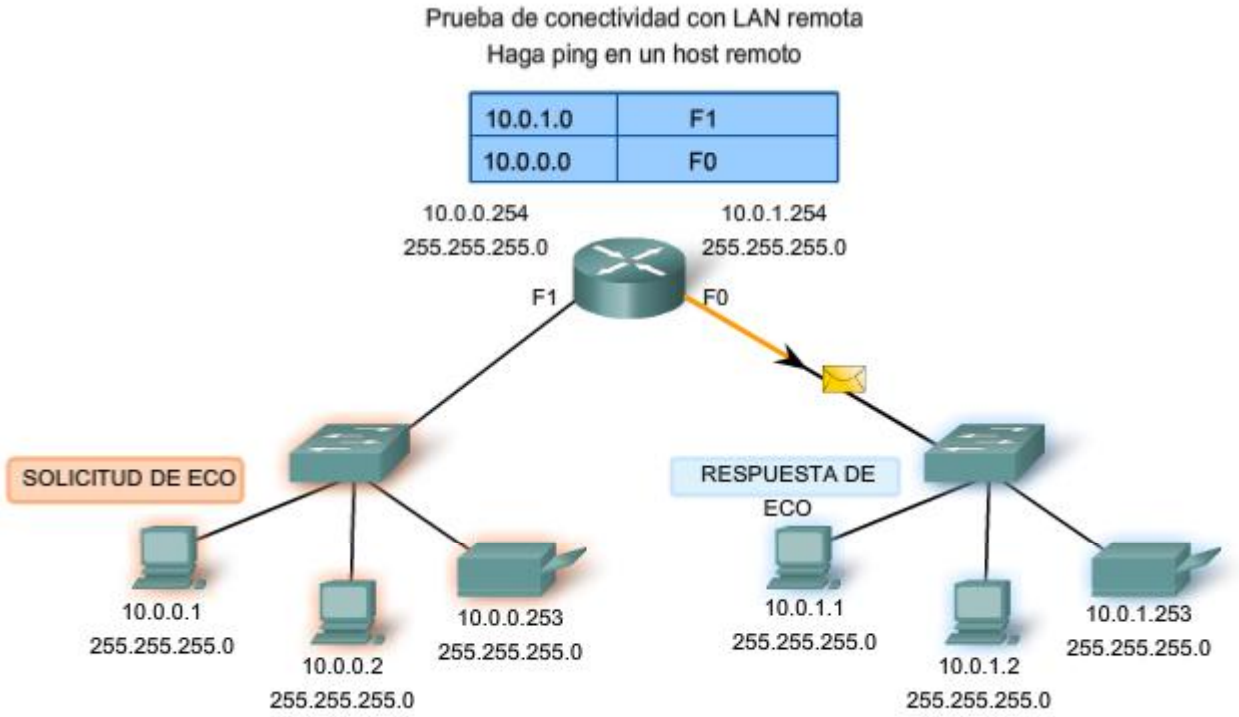
6.6.3 Ping de host remoto – Prueba de conectividad con una LAN remota

También se puede utilizar el ping para probar la capacidad de comunicación del host IP local en una internetwork. El host local puede hacer ping a un host que funciona en una red remota, como se muestra en la figura.

Si el ping se realiza con éxito, se habrá verificado la operación de una porción amplia de la internetwork. Esto significa que se ha verificado la comunicación del host en la red local, el funcionamiento del router que se usa como gateway y los demás routers que puedan encontrarse en la ruta entre la red y la red del host remoto.

Además, se ha verificado el mismo funcionamiento en el host remoto. Si, por algún motivo, el host remoto no pudo usar su red local para comunicarse fuera de la red, entonces no se habría producido una respuesta.

Recuerde: muchos administradores de red limitan o prohíben la entrada de datagramas ICMP en la red corporativa. Por lo tanto, la ausencia de una respuesta de ping podría deberse a restricciones de seguridad y no a elementos que no funcionan en las redes.



6.6.4 Traceroute (tracert) – Prueba de la ruta

El ping se usa para indicar la conectividad entre dos hosts. Traceroute (tracert) es una utilidad que permite observar la ruta entre estos hosts. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallas. Si los datos llegan a destino, entonces el rastreador menciona la interfaz en cada router que aparece en el camino.

Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo. Esto indica el lugar donde se encuentra el problema o las restricciones de seguridad.

Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona el tiempo de ida y vuelta (RTT) para cada salto a lo largo del camino e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Se usa un asterisco (*) para indicar la pérdida de un paquete.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si tenemos altos tiempos de respuesta o pérdidas de datos de un salto particular, ésta es una indicación de que los recursos del router o sus conexiones pueden estar estresados.

Tiempo de vida (TTL)

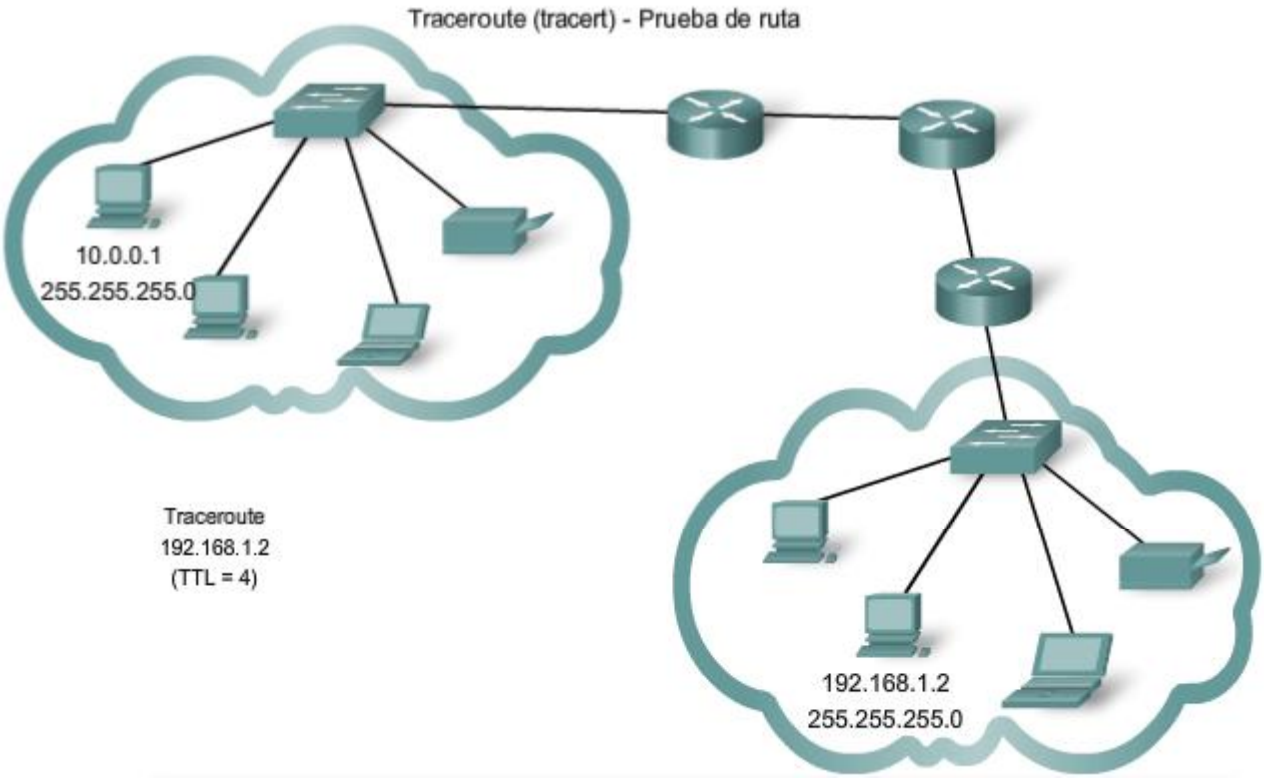
Traceroute hace uso de una función del campo Tiempo de vida (TTL) en el encabezado de Capa 3 y Mensaje excedido en tiempo ICMP. El campo TTL se usa para limitar la cantidad de saltos que un paquete puede cruzar. Cuando un paquete ingresa a un router, el campo TTL disminuye en 1. Cuando el TTL llega a cero, el router no envía el paquete y éste es descartado.

Además de descartar el paquete, el router normalmente envía un mensaje de tiempo superado de ICMP dirigido al host de origen. Este mensaje de ICMP estará conformado por la dirección IP del router que respondió.

La primera secuencia de mensajes enviados desde traceroute tendrá un campo de TTL de uno. Esto hace que el TTL expire el límite de tiempo del paquete en el primer router. Este router luego responde con un mensaje de ICMP. Traceroute ahora posee la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes expiran el límite de tiempo a lo largo del camino. El campo TTL continúa aumentando hasta que se llega a destino o hasta un máximo predefinido.

Una vez que se llega al destino final, el host responde con un mensaje de puerto inalcanzable de ICMP o un mensaje de respuesta de eco de ICMP, en lugar del mensaje de tiempo superado de ICMP.



6.6.5 ICMPv4. Protocolo que admite pruebas y mensajeria

A pesar de que IPv4 no es un protocolo confiable, ofrece el envío de mensajes en caso de determinados errores. Estos mensajes se envían mediante servicios del Control Messaging Protocol (Protocolo de mensajes de control de Internet, ICMPv4). El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP bajo determinadas condiciones, no es hacer que el IP sea confiable. Los mensajes de ICMP no son obligatorios y a menudo no se permiten por razones de seguridad.

ICMP es el protocolo de mensajería para el conjunto de aplicaciones TCP/IP. ICMP proporciona mensajes de control y error y se usa mediante las utilidades ping y traceroute. A pesar de que ICMP usa el soporte básico de IP como si fuera un protocolo ICMP de mayor nivel, en realidad es una capa 3 separada del conjunto de aplicaciones TCP/IP.

Los tipos de mensajes ICMP, y los motivos por los que se envían, son vastos. Se tratarán algunos de los mensajes más comunes.

Los mensajes ICMP que se pueden enviar incluyen:

- Confirmación de host
- Destino o servicio inalcanzable
- Tiempo excedido
- Redirección de ruta
- Disminución de velocidad en origen

Confirmación de host

Se puede utilizar un Mensaje de eco del ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. El host que recibe el mensaje de eco responde mediante la respuesta de eco de ICMP, como se muestra en la figura. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

Destino o servicio inalcanzable

Se puede usar el destino inalcanzable de ICMP para notificar a un host que el destino o servicio es inalcanzable. Cuando un host o gateway recibe un paquete que no puede enviar, puede enviar un paquete de destino inalcanzable de ICMP al host que origina el paquete. El paquete de destino inalcanzable tendrá códigos que indican el motivo por el cual el paquete no pudo ser enviado.

Entre los códigos de destino inalcanzable se encuentran:

0 = red inalcanzable

1 = host inalcanzable

2 = protocolo inalcanzable

3 = puerto inalcanzable

Los códigos para las respuestas red inalcanzable y host inalcanzable son respuestas de un router que no puede enviar un paquete. Si un router recibe un paquete para el cual no posee una ruta, puede responder con un código de destino inalcanzable de ICMP = 0, que indica que la red es inalcanzable. Si un router recibe un paquete para el cual posee una ruta conectada pero no puede enviar el paquete al host en la red conectada, el router puede responder con un código de destino inalcanzable de ICMP = 1, que indica que se conoce la red pero que el host es inalcanzable.

Los códigos 2 y 3 (protocolo inalcanzable y puerto inalcanzable) son utilizados por un host final para indicar que el segmento TCP o el datagrama UDP en un paquete no pudo ser enviado al servicio de capa superior.

Cuando el host final recibe un paquete con una PDU de capa 4 que se enviará a un servicio no disponible, el host puede responder al host de origen con un código de destino inalcanzable de ICMP = 2 o con un código = 3, que indica que el servicio no está disponible. Es posible que el servicio no esté disponible debido a que no hay un daemon en funcionamiento que proporcione el servicio o porque la seguridad del host no permite el acceso al servicio.

Tiempo superado

Un router utiliza un mensaje de tiempo superado de ICMP para indicar que no se puede enviar un paquete debido a que el campo TTL del paquete ha expirado. Sin un router recibe un paquete y dismimuye el campo TTL del paquete a cero, éste descarta el paquete. El router también puede enviar un mensaje de tiempo superado de ICMP al host de origen para informar al host el motivo por el que se descartó el paquete.

Redireccionamiento de ruta

Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways. SI un router recibe un paquete para el cual tiene una ruta y para el próximo salto se conecta con la misma interfaz del paquete recibido, el router puede enviar un mensaje de redireccionamiento de ICMP al host de origen. Este mensaje informará al host de origen acerca del próximo salto en una ruta de la tabla de enrutamiento.

Disminución de velocidad en origen

El mensaje de disminución de velocidad en origen de ICMP puede usarse para informar al origen que deje de enviar paquetes por un tiempo. Si un router no posee suficiente espacio en búfer para recibir paquetes entrantes, un router descartará los paquetes. SI debe hacerlo, también puede enviar un mensaje de disminución de velocidad en origen de ICMP a los hosts de origen por cada mensaje que descarta.

Un host de destino también puede enviar un mensaje de disminución de velocidad en origen si los datagramas llegan demasiado rápido para ser procesados.

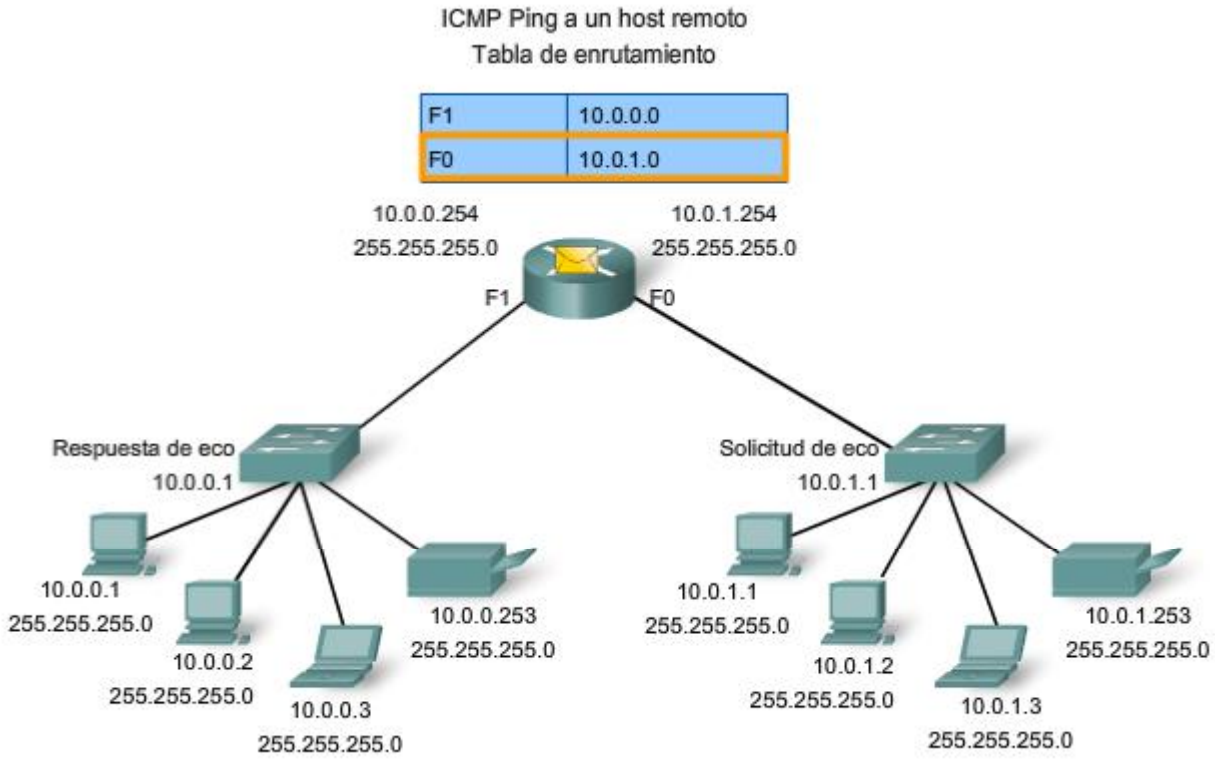
Cuando un host recibe un mensaje de disminución de velocidad en origen de ICMP, lo informa a la capa de transporte. El host de origen puede utilizar el mecanismo de control de flujo de TCP para adaptar la transmisión.

Enlaces:

RFC 792 http://www.ietf.org/rfc/rfc0792.txt?number=792

RFC 1122 http://www.ietf.org/rfc/rfc1122.txt?number=1122

RFC 2003 http://www.ietf.org/rfc/rfc2003.txt?number=2003



6.8 Resúmenes del capitulo

6.8.1 Resumen y revisión

Las direcciones IPv4 son jerárquicas y tienen porciones de red, subred y host. Una dirección IPv4 puede representar una red completa, un host específico o la dirección de broadcast de la red.

Se usan diferentes direcciones para comunicaciones de datos unicast, multicast y broadcast.

Las autoridades de direccionamiento y los ISP asignan intervalos de direcciones a los usuarios, que a su vez pueden asignar estas direcciones a sus dispositivos de red de manera estática o dinámica. El intervalo de direcciones asignado puede dividirse en subredes calculando y aplicando máscaras de subred.

Se requiere una planificación de direccionamiento cuidadosa para hacer buen uso del espacio de red disponible. Los requisitos de tamaño, ubicación, uso y acceso son consideraciones a tener en cuenta en el proceso de planificación de direcciones.

Una vez implementada, una red IP debe ser probada para verificar su conectividad y rendimiento operativo.

En este capítulo, aprendió a:

- Explicar la estructura del direccionamiento IP y demostrar la capacidad para convertir números decimales y binarios de 8 bits.
- Dada una dirección IPv4, clasificarla por tipo y describir cómo se utiliza en la red.
- Explicar cómo se asignan las direcciones a redes mediante ISP y dentro de redes a través de administradores.
- Determinar la porción de la red de la dirección host y explicar el rol de la máscara de subred en la división de redes.
- Según un IPv4, direccionar información y diseñar criterios, calcular los componentes de direccionamiento adecuados.
- Utilizar utilidades de prueba comunes para verificar y probar la conectividad de la red y el estado operativo del stack del protocolo IP en un host.