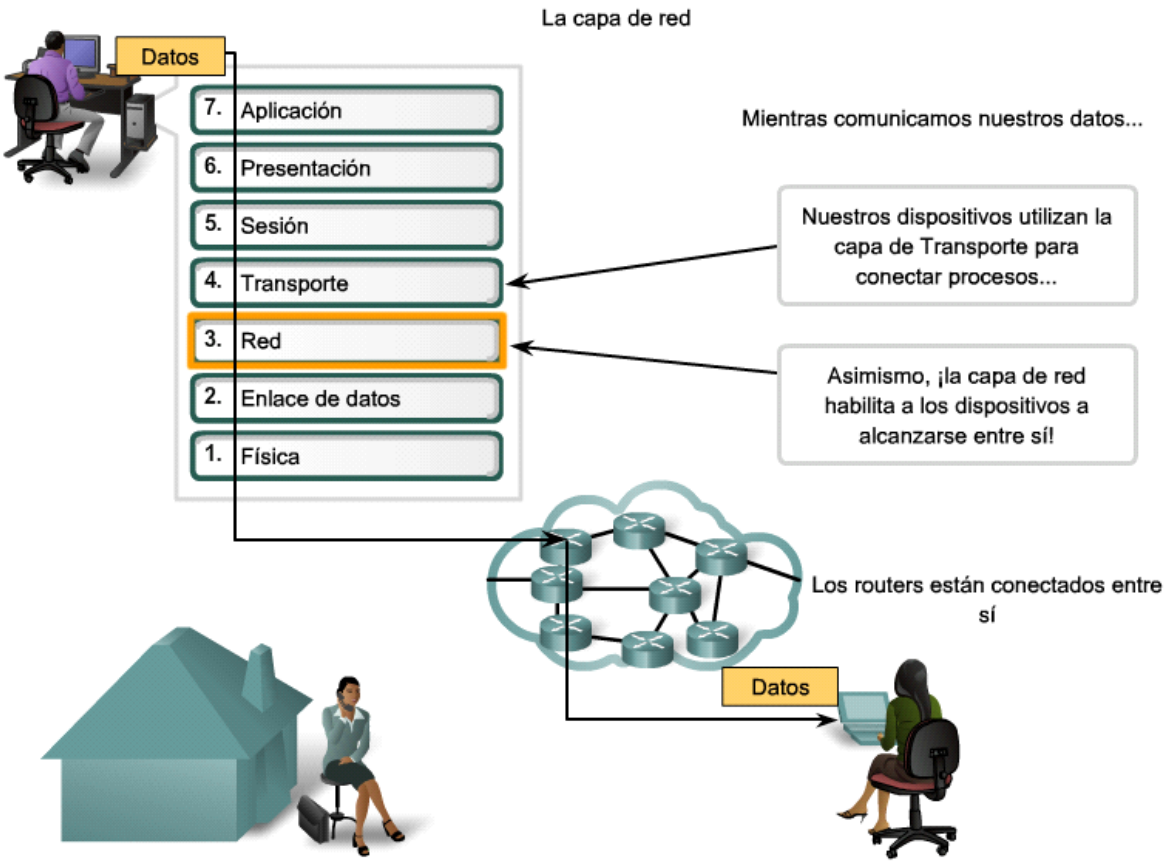
5.0.1 Introducción - La capa de Red OSI

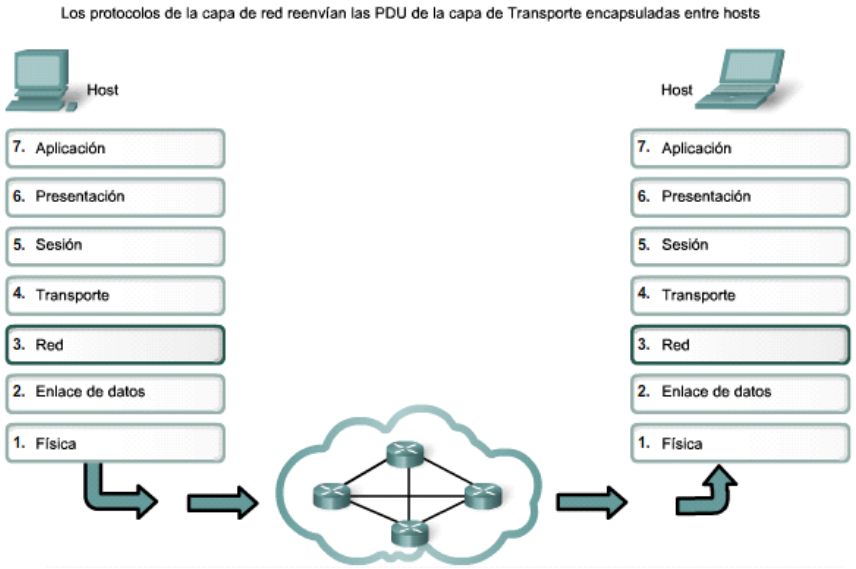
Los protocolos de la capa de red del modelo OSI especifican el direccionamiento y los procesos que permiten que los segmentos o datagramas de la capa de transporte sean empaquetados y transportados.
La encapsulación de la capa de red permite que sus contenidos pasen al destino dentro la misma red o sobre otra red con la carga mínima.
La comunicación entre redes se efectúa por medio del enrutamiento de la información.
Objetivos

- Identificación de la función de la capa de red la cual describe la transferencia de información de extremo a extremo.
- Análisis del protocolo IP, protocolo sin conexión.
- Principios de agrupamiento de dispositivos en redes.
- Direccionamiento jerárquico de dispositivos.
- Rutas, direccionamiento del siguiente salto.



5.1.1.1 La capa de red: comunicación de host a host

La capa de Red, capa tres del modelo OSI, provee los servicios para el intercambio de datos a través de la red, entre dispositivos terminales identificados.
Transporte de los datos de extremo a extremo por medio de cuatro procesos:
Direccionamiento
Agregado de una dirección única a un dispositivo que permita su identificación.
Las direcciones están clasificadas en IPv4 e IPv6. El direccionamiento es jerárquico.
Host: dispositivo terminal de datos al cual se le asigna una dirección.
Encapsulación
La capa tres o capa de red recibe el segmento o el datagrama de la capa de la capa de transporte para su encapsulado y transmisión.
La unidad de datos de protocolo PDU de la capa de red se denomina paquete.
Un paquete se encapsula con un campo correspondiente a una dirección de origen o remitente del paquete y una dirección de destino, además de otros campos.
Con posterioridad a la encapsulación, el paquete se envía a la capa de Enlace de Datos para su transmisión a través del medio de comunicación.



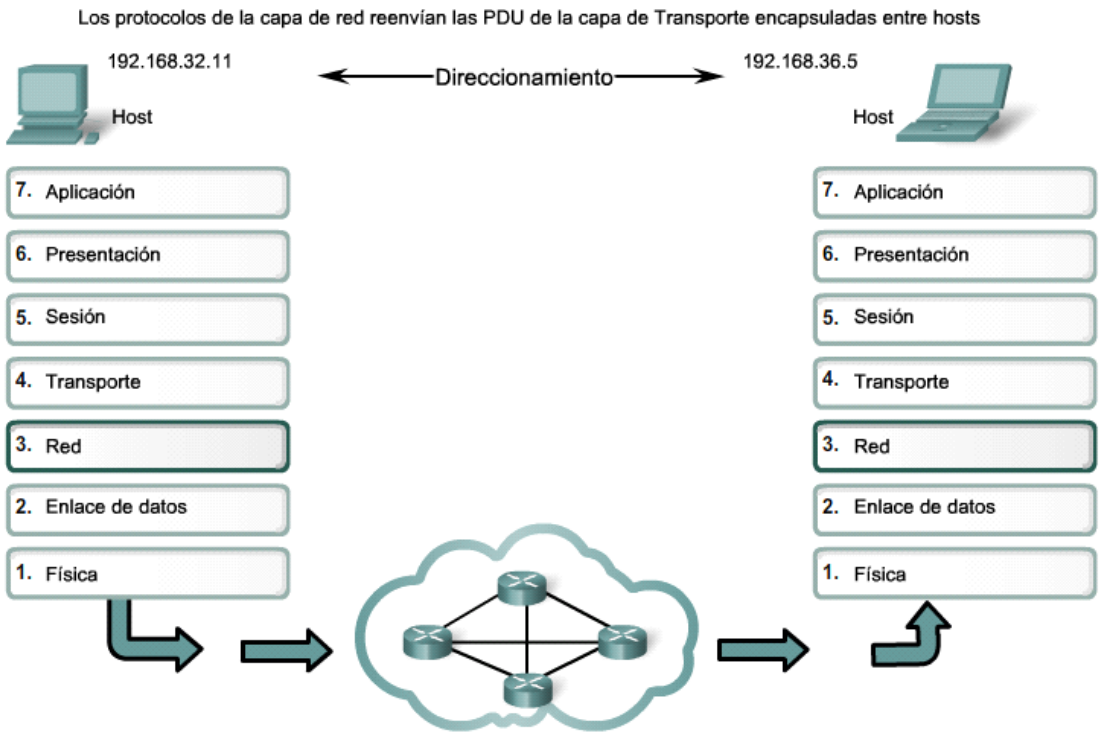
5.1.1.2 La capa de red: comunicación de host a host

Enrutamiento

La capa de red debe proporcionar los recursos para dirigir los paquetes para su entrega al host de destino.
Los host de origen y destino no siempre se encuentran en la misma red.
El paquete para llegar a mismo destino puede recorrer diferentes redes durante una comunicación.
Los enrutadores o routers son equipos que conectan las diferentes redes y permiten la estructuración de una topología.
Durante el enrutamiento, el paquete puede recorrer diferentes redes o diferentes enrutadores. Al recorrido a través de cada enrutador se le denomina salto.
A medida que se re-envía el paquete, el contenido de la PDU de la capa de transporte permanece intacto.

Des-encapsulación

El paquete que llega al receptor es procesado por la capa de red o capa tres del modelo OSI.
Cuando el paquete llega al host de destino es verificado que ha sido direccionado a dicho host.
Si la dirección es correcta, el paquete es des-encapsulado por la capa de red y la PDU de la capa de transporte es entregada al número de puerto adecuado.
La capa de red desconoce los contenidos de los datos que transporta.

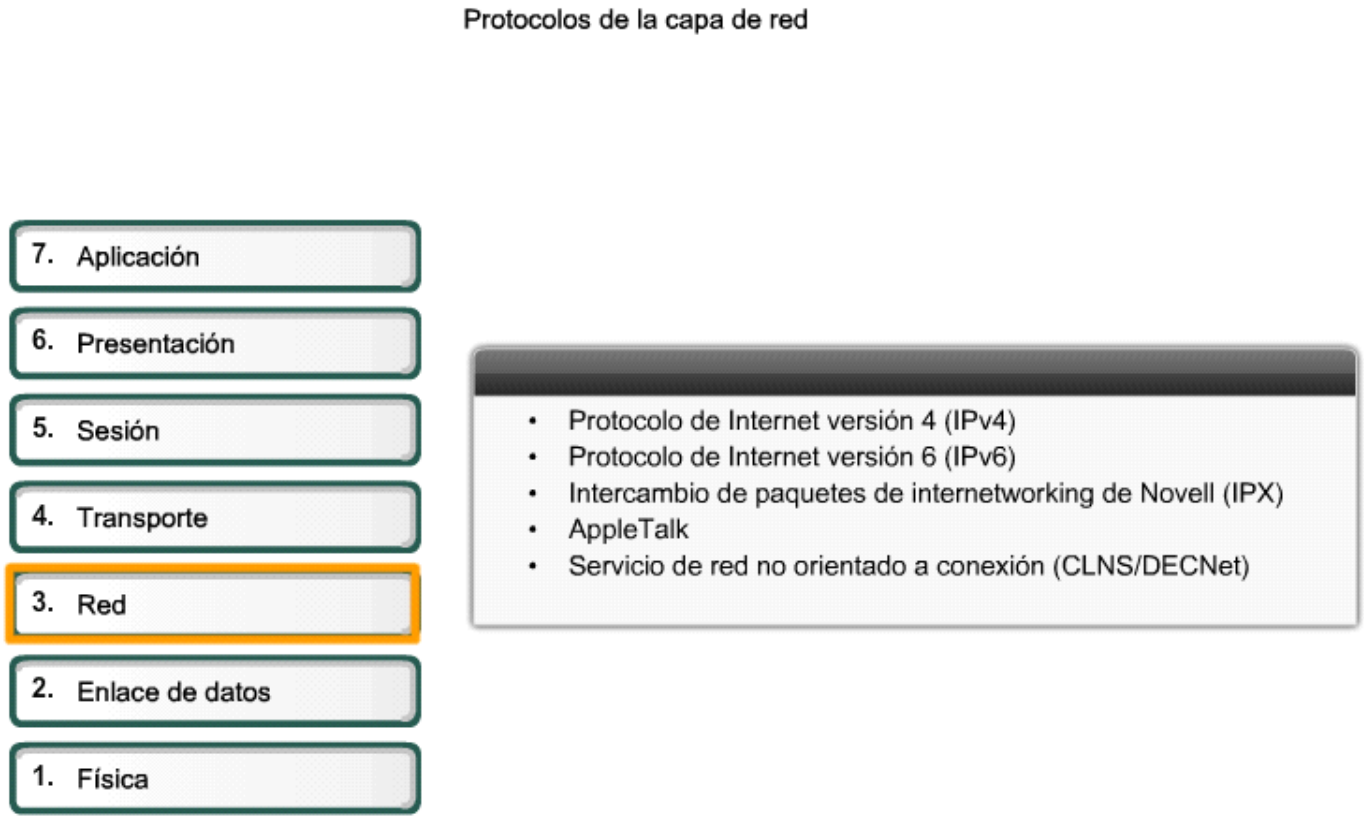


5.1.1.3 Capa de red: comunicación de host a host

Protocolos de capa de red:

- IPv4.
- IPv6.
- Paquetes de inter-red Novell.
- Apple talk.
- Servicios de red sin conexión CLNS/DECNet.

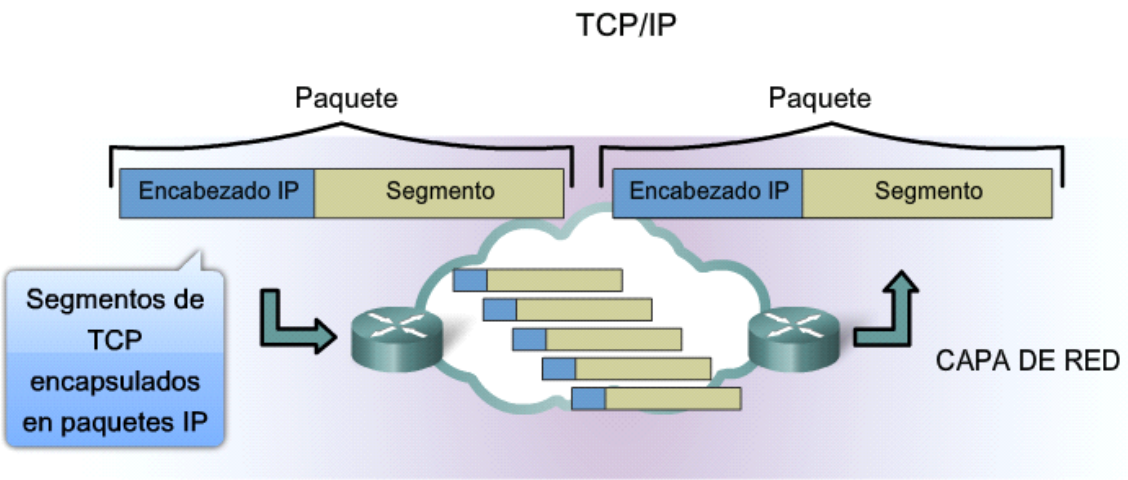
Los protocolos más utilizados son IPv4 e IPv6.



5.1.2 Protocolo de la capa de red IPv4

Rol del IPv4

Es un protocolo estandarizado para el enrutamiento de la información. Es el protocolo más utilizado en las comunicaciones a través de la red.
La siguiente versión IPv6 ha sido implementada para sustituirlo al IPv4.
Ambos protocolos IP son usados para el transporte de datagramas UDP o segmentos TCP.
El protocolo IP fue diseñado como un protocolo de bajo costo debido que solamente está limitado solamente al enrutamiento de la información de origen a destino a través de las redes.
No realiza la recuperación de los mensajes faltantes ni el control de flujo en la red.
En algunas áreas, IPv4 opera conjuntamente con IPv6.
Las características del protocolo IP son:



Los paquetes IP fluyen a través de internetwork.

- Sin conexión: no establece conexión antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): no se usan encabezados para garantizar la entrega de paquetes.
- Independiente de los medios: funciona sin importar los medios que transportan los datos.

5.1.3.1 Protocolo IPv4: sin conexión

IPv4 opera sin conexión. No establece ninguna conexión con el receptor para el envío de la información.
Los paquetes son enviados por el emisor sin notificación al receptor.
Los paquetes pueden llegar desordenados.
El protocolo TCP funciona con conexión. Establece una sesión al inicio de una comunicación.
La sobrecarga del protocolo IP es reducida debido a que el protocolo TCP implementa funciones de conexión y control de la transferencia de la información de extremo a extremo.
Ejemplo de un envío postal.

5.1.3.2 Protocolo IPv4: sin conexión

Envío de un paquete por cualquiera de las rutas.

El emisor no sabe:

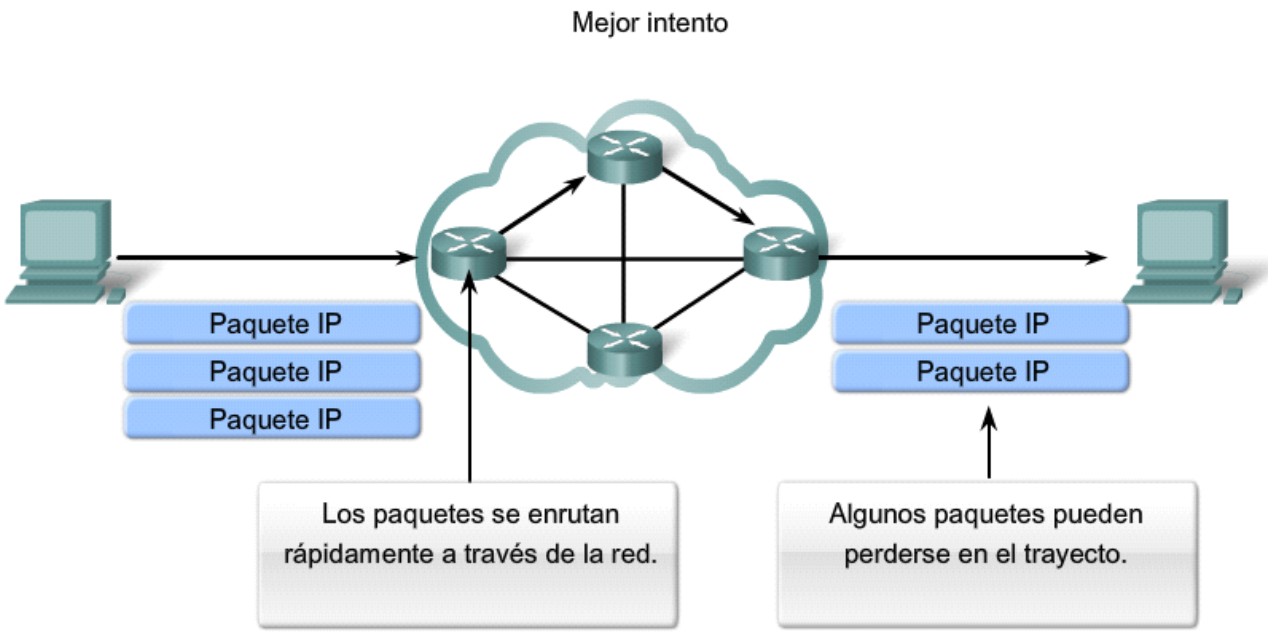
- si el receptor está presente
- si llegó el paquete
- si el receptor puede leer el paquete

El receptor no sabe:

- cuándo llegará

5.1.4 Protocolo IPv4: mejor intento, no confiable

Servicio de mejor intento (no confiable)
La cabecera del protocolo de la capa de red agrega poca sobrecarga comparado con un protocolo confiable con el TCP.
La capa de red no determina el tipo de comunicación que enruta.
La capa de transporte decide si la transferencia debe ser confiable por medio del protocolo TCP ó no confiable por medio del protocolo UDP.
Las capas superiores deben definir si algún protocolo necesita el establecimiento de los procedimientos de seguridad para la transferencia de la información de extremo a extremo.
IPv4 es considerado como un protocolo no confiable.
IPv4 no realiza rastreo de paquetes, ni acuses de recibo ni control de errores, ni retransmisión de paquetes, ni ordenamiento de paquetes recibidos. Ningún procedimiento para garantizar la entrega confiable de extremo a extremo.
Si se incluye procedimientos para que el protocolo IP sea confiable, se agregaría bastante información a la red, lo cual aumentaría el tiempo de tránsito de los paquetes a través de la red. Esto impactaría negativamente en la transferencia de los servicios de voz, video y a las aplicaciones sensibles a los retardos.



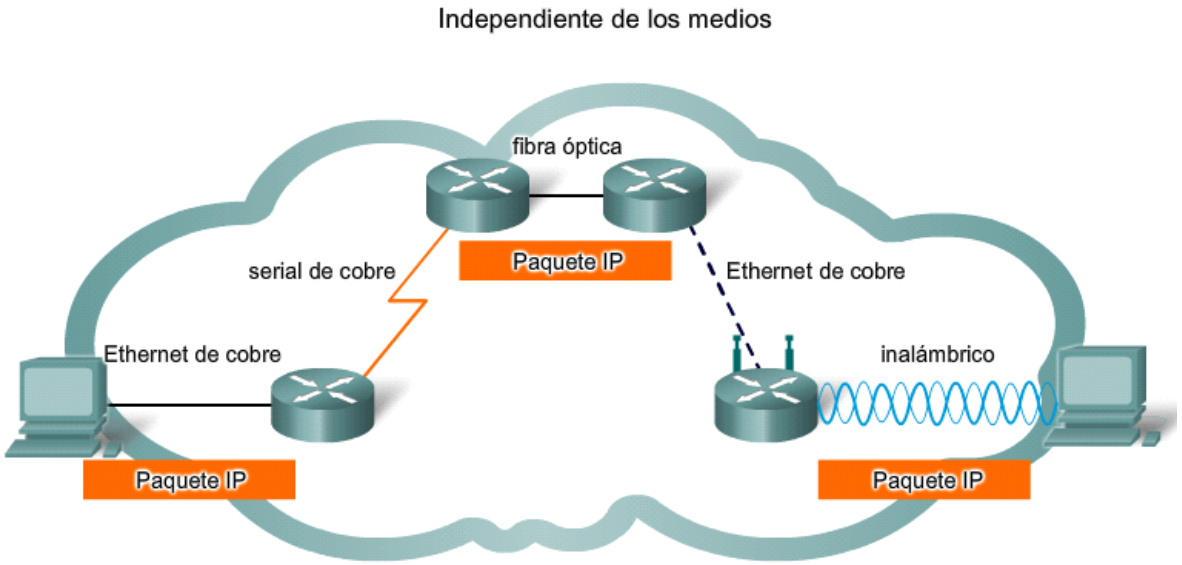
Al ser un protocolo no confiable de capa de red, IP no garantiza la recepción de todos los paquetes enviados.

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

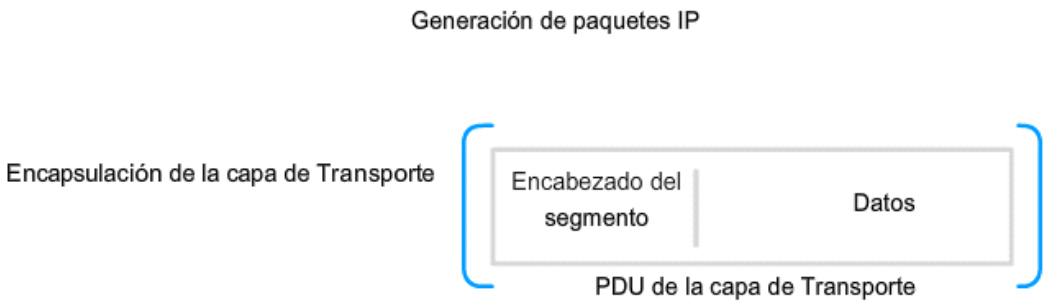
El protocolo IPv4 funciona independiente de los medios sobre el cual se envía los paquetes para el envío de la información a las capas inferiores y a la red externa.
En la gráfica se tienen señales en un medio eléctrico, señales en un medio óptico y señales en un medio inalámbrico.
La capa de enlace de datos del modelo OSI tiene como responsabilidad la recepción de los paquetes de la capa de red, para su transmisión en un medio en particular.
La capa de enlace de datos dimensiona la longitud de la trama en función del medio sobre el cual se va realizar la transmisión de la información.
La capa de red considera el tamaño máximo de la PDU que puede transportar en un determinado medio.
A esta característica se le llama MTU, unidad de transferencia de información máxima.
Una parte de la comunicación entre la capa de Enlace de Datos y la capa de red consiste en el establecimiento de la MTU.
La capa de Enlace de Datos transfiere la MTU hacia la capa de Red, para que esta última determine la longitud de la transferencia de información.
En algunos casos los enrutadores fragmentan los paquetes para el paso de la información de la red con una MTU más alta hacia otra red con una MTU más pequeña.



Los paquetes IP pueden trasladarse a través de diferentes medios.

5.1.6.1 Paquete IPv4: empaquetado de la PDU de la capa de Transporte

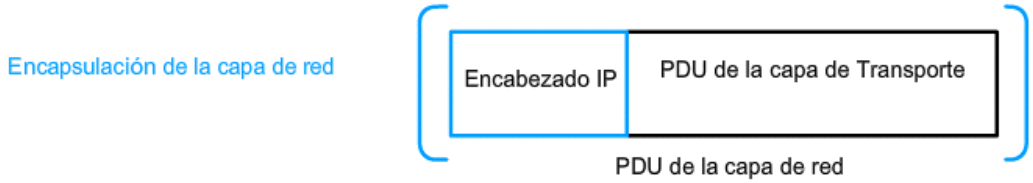
IPv4 encapsula o empaqueta datagramas UDP o segmentos TCP para su entrega al host de destino.
El datagrama o segmento permanece encapsulado desde el momento que este abandona la capa de red en el host de origen hasta que salga de la capa de red en el host de destino.
El proceso de encapsulación de los datos por capas permite que los servicios de las diferentes capas se desarrollen sin afectar a las restantes capas.
Esto permite que los datagramas UDP o segmentos TCP puedan ser empaquetados con un protocolo IPv4, IPv6 o cualquier otra clase de protocolo que se desarrolle en la capa de red.



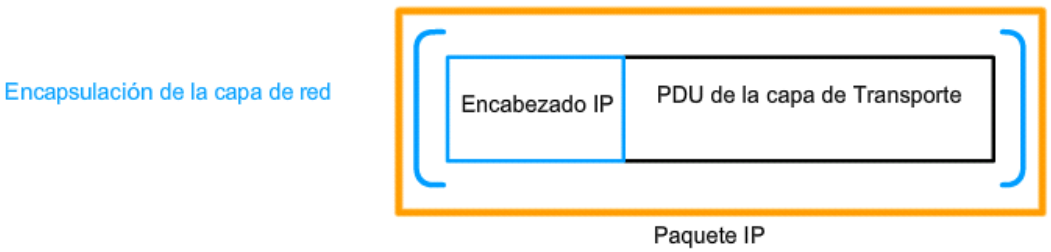
La capa de transporte agrega un encabezado para que puedan incluirse los segmentos y vuelvan a ordenarse en el destino

5.1.6.2 Paquete IPv4: empaquetado de la PDU de la capa de Transporte

Los enrutadores consideran solamente el contenido del encabezado de direccionamiento de la capa de red.
Los enrutadores podrían ser implementados con diferentes clases de protocolos de la capa de red.
La PDU de la capa de transporte se mantiene inalterable durante los procesos de la capa de red de transito de un paquete desde el nodo de origen hasta el nodo de destino.



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

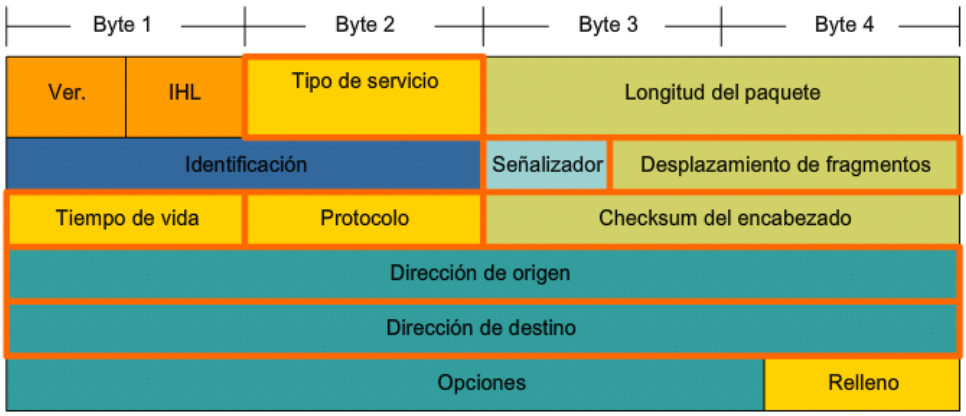


En redes basadas en TCP/IP, la PDU de la capa de red es el paquete IP.

5.1.7.1 Encabezado de paquetes IPv4

- Ver: indica la versión, consta de cuatro bits. indica si es IPv4 ó IPv6. Para IPv4 tiene el valor de 0100; para IPv6 tiene el valor de 0110.
- IHL: Internet Header Length. Consta cuatro bits. Representa el tamaño del encabezado en palabras de 32 bits u octetos. El valor mínimo de la secuencia es de cinco, el cual indica la mínima longitud de una cabecera expresado en bits $x = 5\ x\ 32 = 160\ bits$, lo cual corresponde a $x = \frac{5\ x\ 32}{8} = 20$ octetos. El valor máximo es 1111, el cual representa el valor de 15, de donde 15 x 4 = 60 octetos.

Campos del encabezado de paquetes IPv4



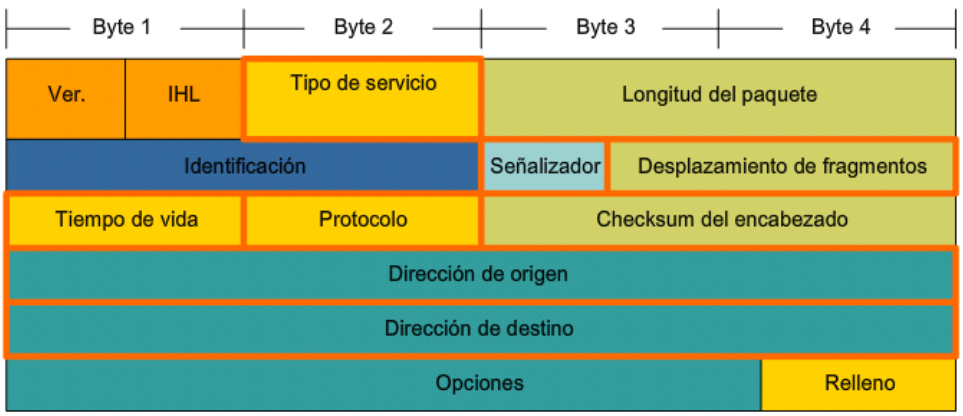
5.1.7.2 Encabezado de paquetes IPv4

- Tipo de servicio: este campo consta de ocho bits. La prioridad lo establece el dispositivo emisor del mensaje. Este campo determina la prioridad para la transferencia de la información y la ruta que deben seguir los paquetes por medio de un mecanismo de calidad de servicio QoS. Los paquetes que contienen información de voz o video deben ser procesados y transferidos prioritariamente con relación a otros paquetes.
  Los tres primeros bits de la izquierda representan la precedencia y la urgencia del envío de los mensajes, el cual se incrementa con el valor numérico de estos tres bits. El valor xxx igual a cero representa un paquete normal. El valor xxx igual a siete representa un mensaje de alta prioridad, relacionada con el control de una red.

0	1	2	3	4	5	6	7
x	x	x	D	T	R	C	0 ; sin uso

  Los otros cuatro bits están relacionados con el retardo y la confiabilidad del envío del paquete. Estos bits indican las características del servicio.
  Solamente uno de los bits D,T,R,C puede tener el valor de uno.
  0000 - Servicio normal
  1000 - El paquete solicita minimizar la demora
  0100 - El paquete solicita maximizar la tasa de transferencia
  0010 - El paquete solicita maximizar la fiabilidad
  0001 - El paquete solicita minimizar el coste

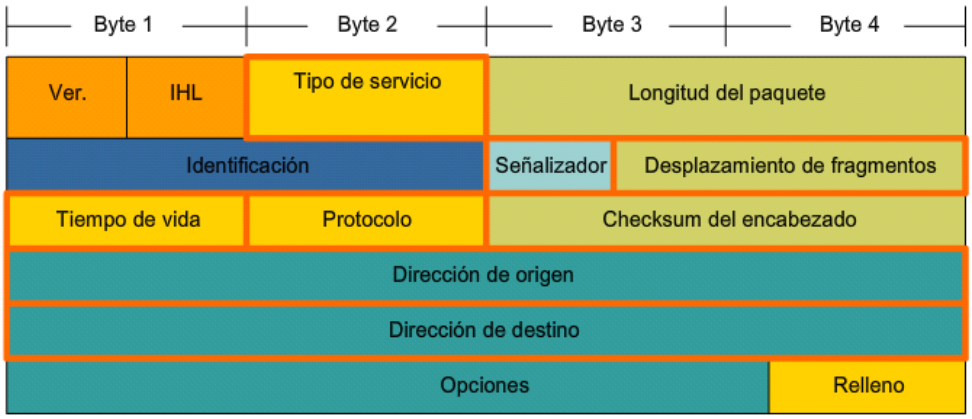
Campos del encabezado de paquetes IPv4



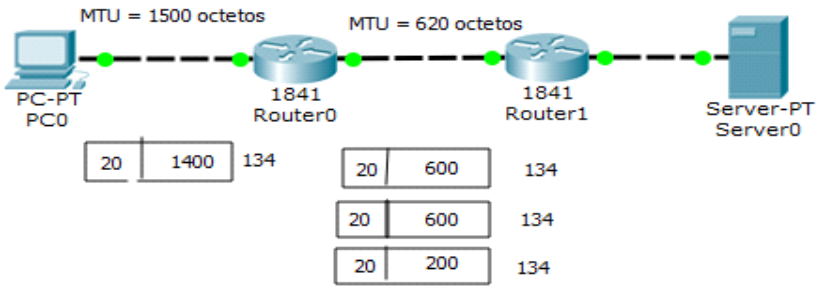
5.1.7.3 Encabezado de paquetes IPv4

- Longitud del paquete: incluye el encabezado y los datos expresado en octetos. El tamaño mínimo es de 20 octetos de encabezado y cero datos. El tamaño máximo es 65.535 octetos.
- Identificación: número de secuencia que identifica los fragmentos de un paquete original. Número generado por el emisor. Todos los paquetes fragmentados pertenecientes al mismo paquete original tienen el mismo número de identificación.

Campos del encabezado de paquetes IPv4



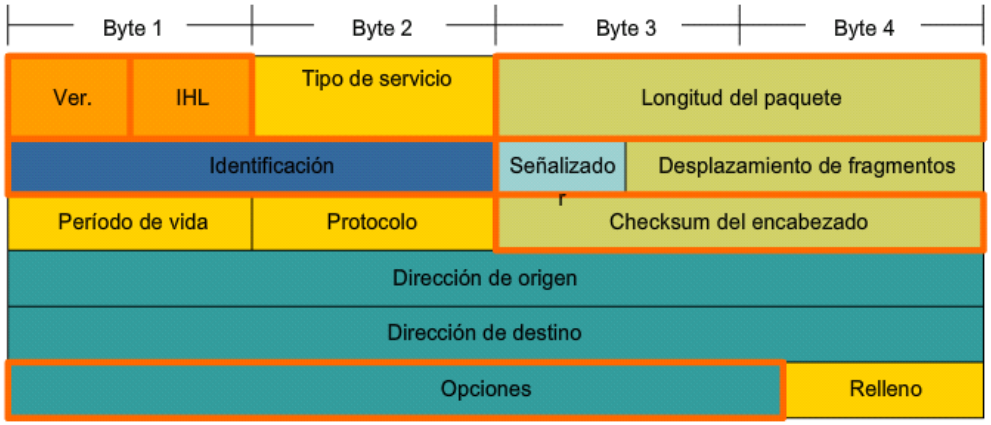
La MTU es la unidad máxima de transferencia de datos expresado en octetos en una red.
Ejemplo: PC0 emite un paquete con una MTU=1400 de octetos con el número de identificación 134.



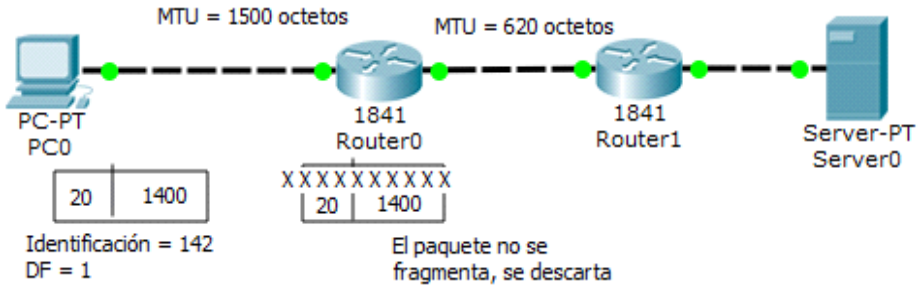
5.1.7.4 Encabezado de paquetes IPv4

- Señalizador: indicador de más fragmentos: consta de tres bits. El bit 0 es el de mayor peso.
  Bit 0: reservado con el valor fijo de cero para un paquete fragmentable o no fragmentable.
  Bit 1: DF (do not fragment), DF=0 paquete fragmentable. DF=1 paquete no fragmentable.
  Bit 2: MF (more fragments), MF=0 ultimo fragmento. MF=1 fragmento intermedio, le siguen más fragmentos.
  Si DF=1, el paquete no puede ser fragmentado. En este caso, un enrutador con una MTU mayor en la entrada comparado con la salida, no podrá fragmentar el paquete. El paquete se descarta.

Campos del encabezado de paquetes IPv4

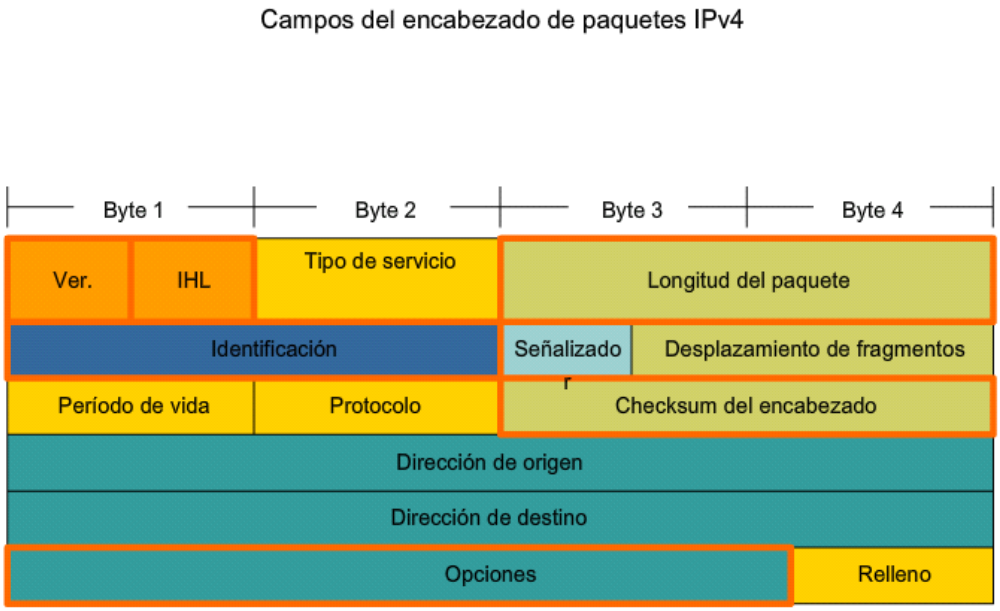


La MTU es la unidad máxima de transferencia de datos expresado en octetos en una red.
Ejemplo: PCO emite un paquete con una MTU = 1400 octetos con la identificación 142 y el bit DF = 1. El paquete no se fragmenta, se descarta.

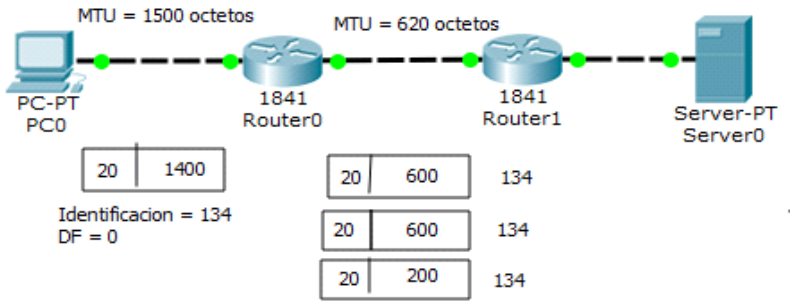


5.1.7.5 Encabezado de paquetes IPv4

Bit 1: Fragmentación de un paquete con DF=0.



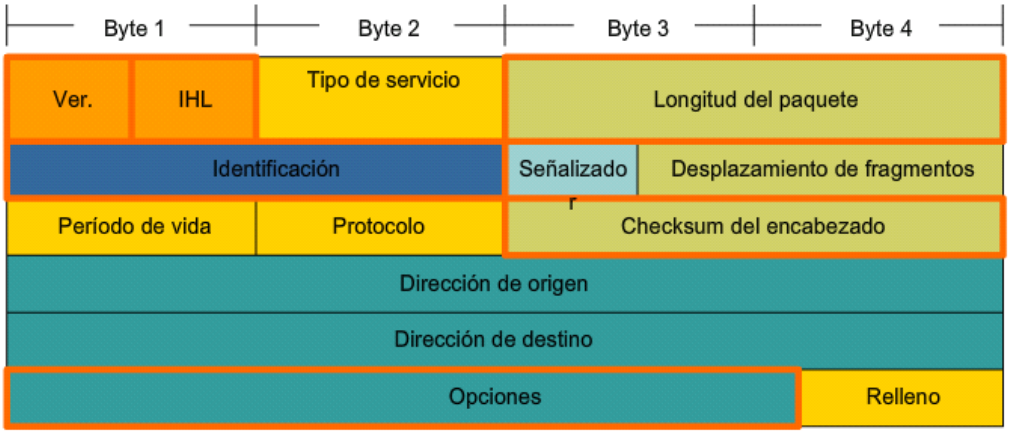
Ejemplo: PCO emite un paquete con una MTU = 1400 octetos con la identificación 134 y el bit DF=0. El paquete se fragmenta y cada fragmento tiene el mismo número de identificación igual al paquete original.



5.1.7.6 Encabezado de paquetes IPv4

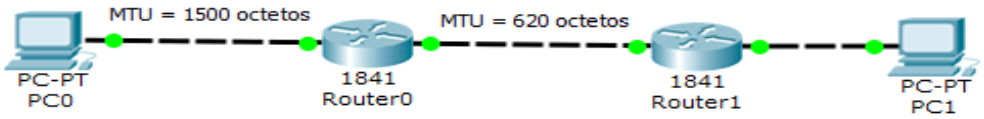
- Desplazamiento de fragmentos: consta de 13 bits. En un enrutador, cuando la MTU de la red con los datos entrantes es mayor que la MTU saliente, el paquete debe ser fragmentado. Este campo determina el lugar o la ubicación de un fragmento actual con respecto al paquete original. El valor se expresa en unidades de 64 bits u ocho octetos.
  En el campo de señalizador, compuesto por tres bits.
  El bit 0 está reservado con el valor cero.
  El bit 1 tiene el valor de DF = 0, el paquete transmitido es fragmentable.
  El bit 2 tiene puede tener los valores MF=0 lo cual indica el último fragmento y el bit MF=1 indica que es un fragmento intermedio.
  El primer fragmento ocupa siempre la posición cero en el campo del Desplazamiento de Fragmento.
  Las demás posiciones de los fragmentos se calculan en unidades de 64 bits o en octetos.

Campos del encabezado de paquetes IPv4



5.1.7.7 Encabezado de paquetes IPv4

Ejemplo: Un paquete cuya longitud es de 1420 octetos ingresa al enrutador Router0. Escriba los valores de los campos identificador, señalizador y desplazamiento de fragmento para un paquete IP que ha sido fragmentado en varias partes. El campo identificador del paquete tiene el número 301.
El bit DF=0, el paquete es fragmentable.



Paquete entrante en el enrutador R0.

Versión	Longitud de la cabecera	Tipo de servicio	Longitud total = 1420			
Identificación = 301			Bit Reservado = 0	Bit DF=0	Bit MF=0	Desplaz. Fragm. = 0

Paquete fragmentado a la salida del enrutador R0.

Versión	Longitud de la cabecera		Longitud total = 600 octetos			
Identificación = 301			Bit Reservado = 0	Bit DF=0	Bit MF=1	Desplaz. Fragm. = 0

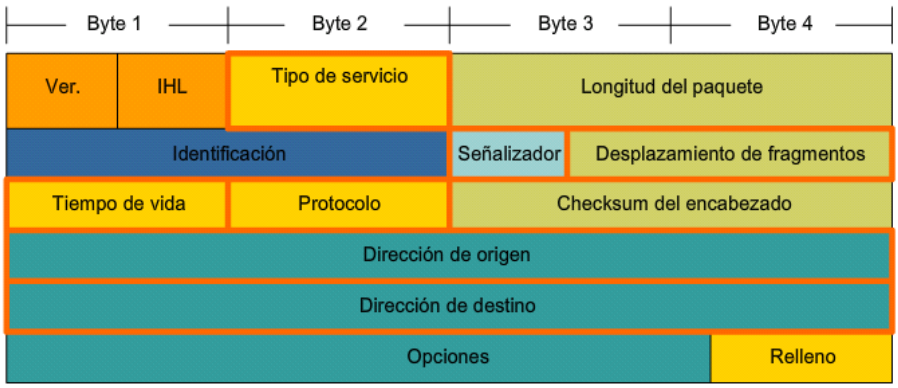
Versión	Longitud de la cabecera		Longitud total = 600 octetos			
Identificación = 301			Bit Reservado = 0	Bit DF=0	Bit MF=1	Desplaz. Fragm. = 600 octetos o 600 / 8 Desplaz. Fragm. = 75 en grupos de ocho octetos

Versión	Longitud de la cabecera		Longitud total = 200 octetos			
Identificación = 301			Bit Reservado = 0	Bit DF=0	Bit MF=0	Desplaz. Fragm. = 1200 octetos o 1200/8 Desplaz. Fragm. = 150 en grupos de ocho octetos

5.1.7.8 Encabezado de paquetes IPv4

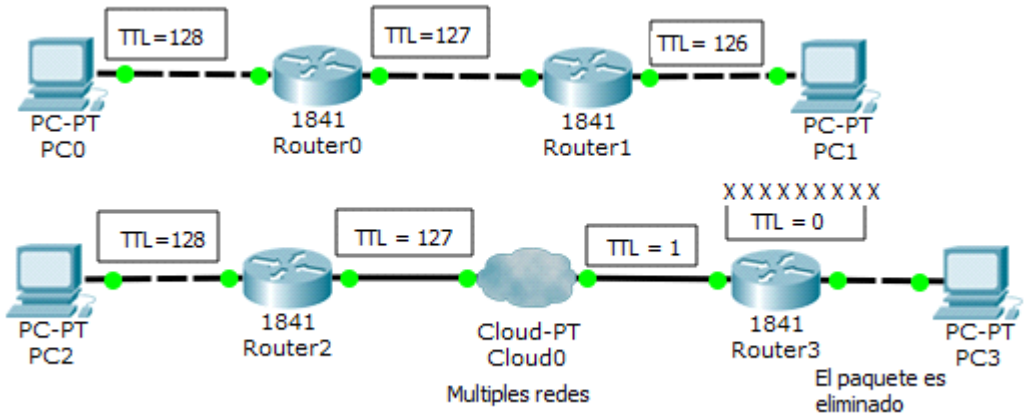
- Tiempo de vida TTL: este campo está compuesto por un valor binario de ocho bits. El valor de TTL decrece en una unidad cada vez que un paquete pasa por un enrutador. Si el paquete no llega a la red de destino, se elimina cuando TTL=0. Esto permite la eliminación de cualquier paquete que se encuentre en un recorrido cíclico indefinido en búsqueda de la red de destino.
  El valor original del campo de TTL lo establece el equipo emisor.
  Los nuevos enrutadores reenvían los paquetes hacia los enrutadores vecinos en milisegundos. También existe un descuento de una unidad por cada segundo que un paquete permanezca en un enrutador debido a la congestión.

Campos del encabezado de paquetes IPv4



5.1.7.9 Encabezado de paquetes IPv4

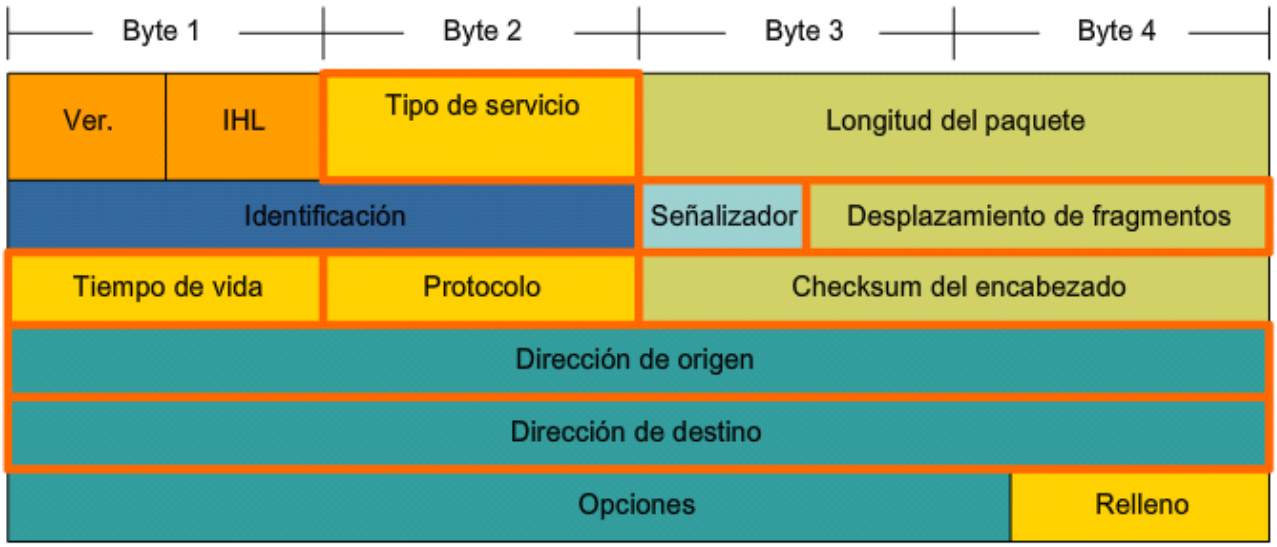
Ejemplo: Valor del campo TTL en cada una de las redes.



5.1.7.10 Encabezado de paquetes IPv4

- Protocolo: este campo consta de ocho bits. Indica el tipo de contenido que el paquete transporta. Le permite a la capa de red el paso de los datagramas o segmentos a la capa superior.
  Algunos valores para los protocolos son 01: ICMP ; 06:TCP ; 17: UDP.

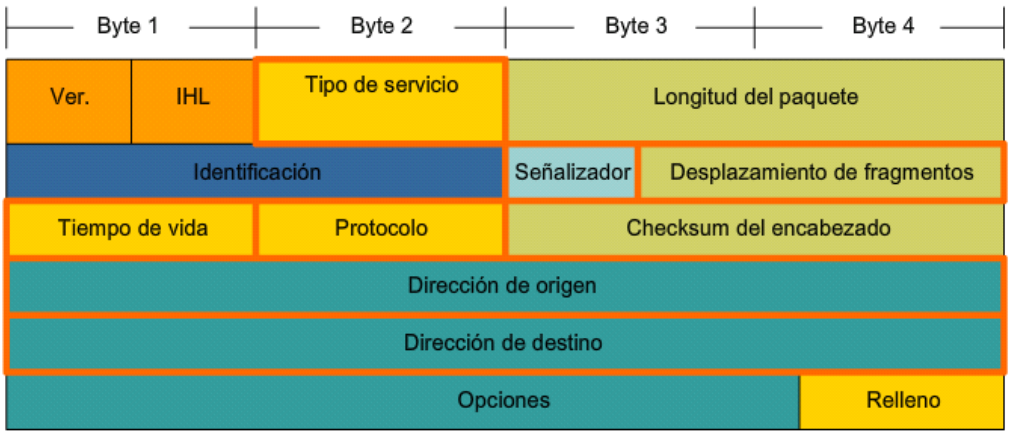
Campos del encabezado de paquetes IPv4



5.1.7.11 Encabezado de paquetes IPv4

- Checksum del encabezado: se calcula con el contenido del encabezado únicamente. El enrutador debe recalcularlo debido a los cambios de TTL y la posible fragmentación del paquete. El receptor verifica el contenido de la cabecera y del campo del checksum del encabezado. En caso de error, el paquete se descarta.

Campos del encabezado de paquetes IPv4



5.1.7.12 Calculo del Checksum con valores binarios

Ejemplo: calcule el valor de campo checksum en el transmisor. Los valores están expresados en decimal.

Octeto 1		Octeto 2	Octeto 3	Octeto 4
4	5	0	115	
0			16384	
64		17	Checksum	
192.168.0.1				
192.168.0.199				

El valor inicial del campo checksum es cero. Se suman los contenidos de los campos en grupos de 16 bits.

4 ; 5 ; 0		0100 0101	00000000
115		0000 0000	01110011
0		0000 0000	00000000
Suma		0100 0101	01110011
16384		0100 0000	00000000
Suma		1000 0101	01110011
64 ; 17		0100 0000	00010001
Suma		1100 0101	10000100
Checkum		0000 0000	00000000
192 ; 168		1100 0000	10101000
Suma	1	1000 0110	00101100
0 ; 1		0000 0000	00000001
Suma	1	1000 0110	00101101
192 ; 168		1100 0000	10101000
Suma	10	0100 0110	11010101
0 ; 199		0000 0000	11000111
Suma	10	0100 0111	10011100
Suma en C1			10
Suma cabecera		0100 0111	10011110
Checksum C1		1011 1000	01100001

El valor hexadecimal del Cheksum tomado en complemento a uno es B861.

5.1.7.13 Calculo del Checksum con valores binarios

El receptor efectúa una operación similar al transmisor, con el valor del checksum incluido, el cual fue calculado con el valor del complemento a uno de la suma. Si el resultado tiene el valor de cero, la cabecera no tiene error alguno.
Ejemplo: verifique si la siguiente cabecera recibida tiene algún error. La cabecera es la misma del ejemplo anterior, pero están expresados en hexadecimal.

Octeto 1		Octeto 2	Octeto 3	Octeto 4
4	5	00	0073	
0000			4000	
40		11	B861	
C0A8 0001				
C0A8 00C7				

La suma del encabezado tiene el valor de 0100 0111 1001 1110
El valor binario del Checksum calculado en el receptor tiene el valor 1011 1000 0110 0001
La suma de esos campos tiene el valor de 0100 0111 1001 1110
1011 1000 0110 0001
---------- ---------- ---------- ----------
FFFF FFFF FFFF FFFF
La secuencia FFFF representa el valor de cero, en el sistema de numeración de complemento a uno
Si el cálculo del checksum en el receptor es igual a cero, el paquete recibido no tiene error alguno.

5.1.7.14 Encabezado de paquetes IPv4

Ejemplo: calcule el valor de campo checksum en el transmisor. Los valores están expresados en decimal.

Octeto 1		Octeto 2	Octeto 3	Octeto 4
4	5	0	115	
0			16384	
64		17	Checksum	
192.168.0.1				
192.168.0.199				

El valor inicial del campo checksum es cero. Se realiza la suma en los grupos de 16 bits en binario o su equivalente en hexadecimal
4500 + 0073 + 0000 + 4000 + 4011 + 0000 + C0A8 + 0001 + C0A8 + 00C7 = 2479C
Se finaliza la suma de una manera similar a la suma en complemento a uno 479C + 2 = 479E
El valor del checksum se calcula con el complemento a uno del resultado 479E.
El resultado 479E expresado en binario 0100 0111 1001 1110
El complemento a uno tiene el valor de 1011 1000 0110 0001
El resultado del checksum es B861.

El receptor efectúa una operación similar al transmisor, con el valor del checksum incluido, por medio de la suma de complemento a uno. Si el resultado tiene el valor de cero, la cabecera no tiene error alguno.
Ejemplo: verifique si la siguiente cabecera recibida tiene algún error. La cabecera es la misma del ejemplo anterior, pero están expresados en hexadecimal.

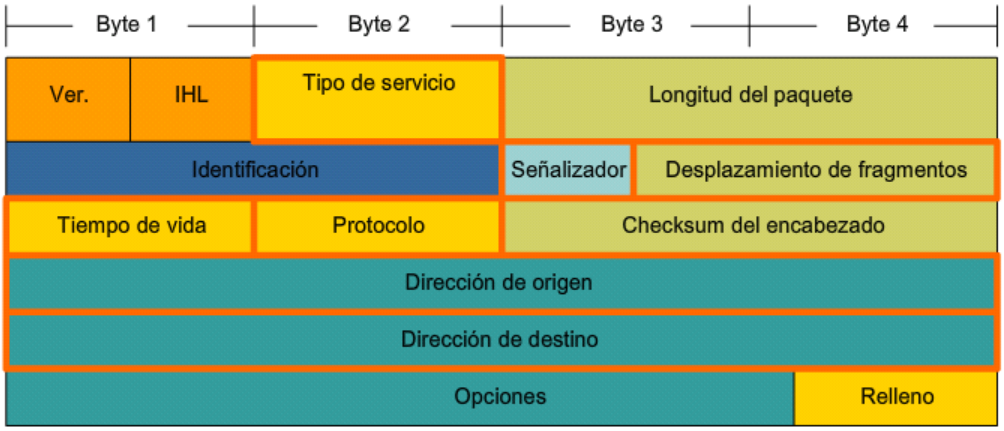
Octeto 1		Octeto 2	Octeto 3	Octeto 4
4	5	00	0073	
0000			4000	
40		11	B861	
C0A8 0001				
C0A8 00C7				

La suma calculada en complemento a uno, excepto el campo Checksum, tiene el valor de 479E.
El resultado de esta suma con el Checksum tiene el valor 479E + B861 = FFFF.
El valor de FFFF en complemento a uno es igual a cero, o efectuando el complemento a uno de esta secuencia se tiene 0000.
En consecuencia, la cabecera recibida no tiene error alguno.

5.1.7.16 Encabezado de paquetes IPv4

- Dirección IP de origen: contiene un valor binario de 32 bits que representa el host de origen del paquete. Permanece inalterable durante el recorrido del paquete. Habilita al host receptor para contestarle al host originador.
- Dirección IP de destino: contiene un valor binario de 32 bits que representa el host de destino del paquete. Permanece inalterable durante el recorrido del paquete. Los enrutadores consideran esta dirección para el enrutamiento del paquete.
- Opciones: se usa muy escasamente. Ocasiona variaciones en la longitud de la cabecera. El contenido varia de 0 a 40 octetos. Una aplicación sería el registro de los nodos por donde el paquete ha recorrido. En este caso solamente podría almacenar hasta diez direcciones.

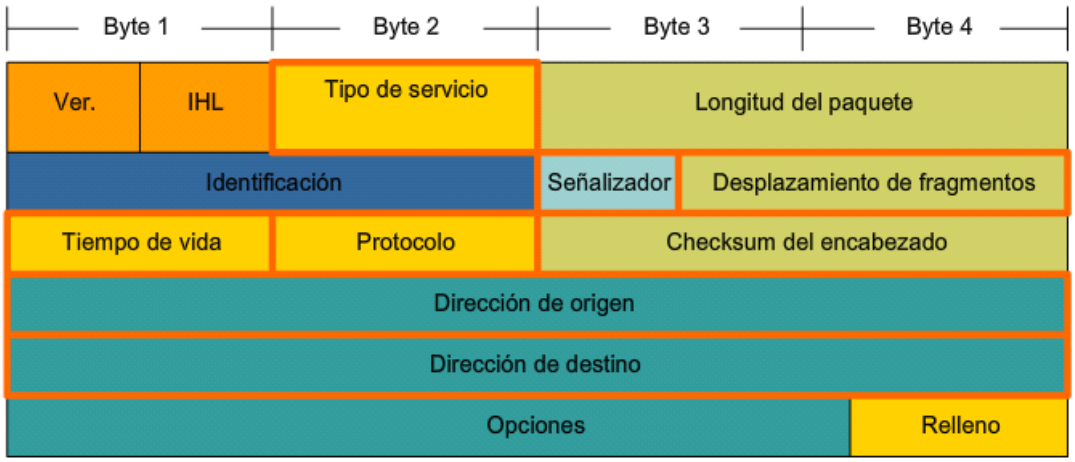
Campos del encabezado de paquetes IPv4



5.1.7.17 Encabezado de paquetes IPv4

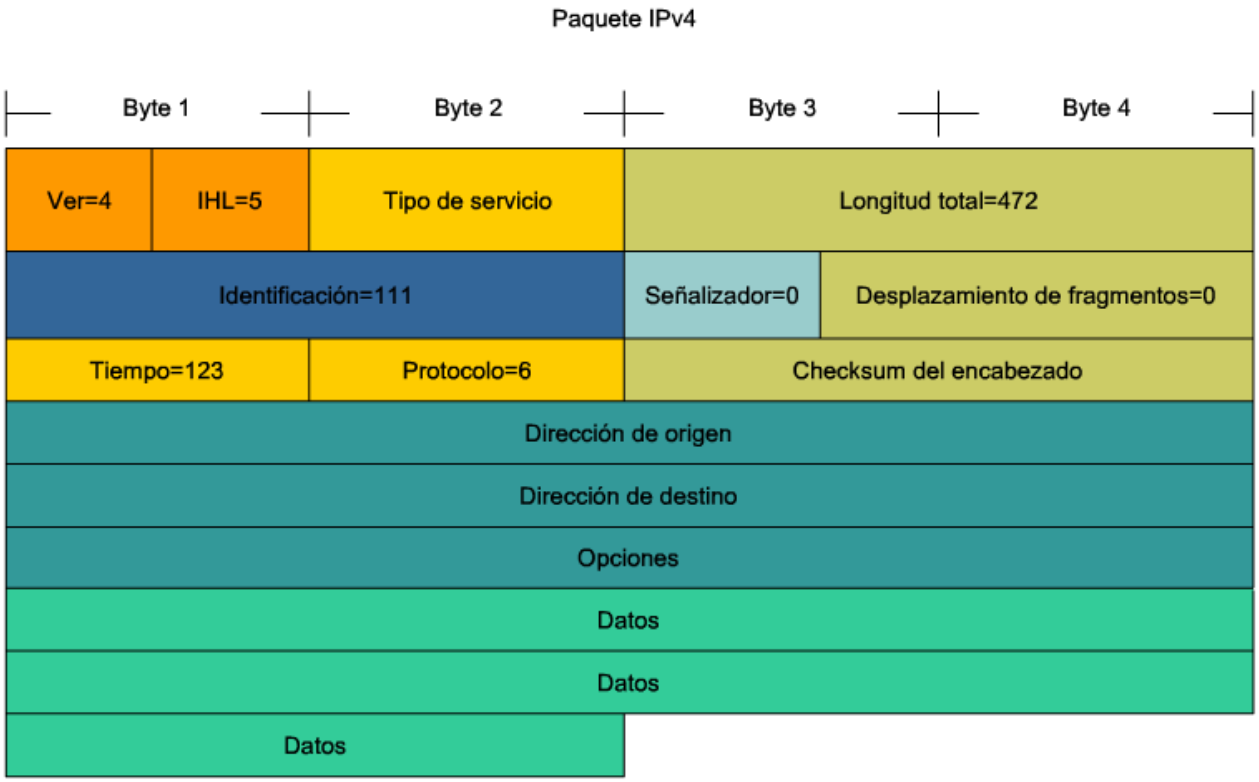
- Campo de opciones: no se requiere en todos los paquetes transmitidos. Se utiliza en las pruebas de red o en los procedimientos de depuración de los paquetes. La longitud de este campo es variable entre un octeto y 40 octetos, si se utiliza. Los contenidos del campo de opciones se presentan en octetos contiguos.
- Campo de relleno : bits con el valor cero para completar el campo de opciones con 32 bits o múltiplos de 32 bits.

Campos del encabezado de paquetes IPv4



5.1.7.18 Encabezado de paquetes IPv4

Ejemplo de un paquete IPv4.



Ver=4 ; versión IPv4.
IHL=5, tamaño en palabra de cuatro octetos. 5 x 4 = 20 octetos. Tamaño mínimo.
Longitud total = 472 octetos ; encabezado + datos = 472 octetos.
Identificador=111, valor requerido en caso que se produzca la fragmentación del paquete.
Señalizador = 0 , el paquete se puede fragmentar.
Desplazamiento de fragmento = 0, el paquete no esta fragmentado actualmente.
Tiempo de vida = 123. Disminuye cada vez que pasa por un enrutador.
Protocolo= 6, segmento TCP.

5.1.7.19 Fragmentación y MTU

El protocolo TCP/IP define una longitud máxima de un paquete IP por medio de la Unidad Máxima de Transmisión MTU.
La MTU varía en función de la configuración y las características de las interfaces. De forma predeterminada, una computadora calcula la MTU de una interfaz en función del tamaño máximo de la parte de la trama de enlace de datos donde el paquete es colocado.
El valor predeterminado de MTU en las interfaces Ethernet es 1500 octetos.
Los enrutadores no pueden reenviar paquetes por una interfaz si el paquete entrante es más largo que la MTU de la interfaz de salida..
Si la MTU de la interfaz de un enrutador es menor que el paquete que debe ser enviado, el enrutador fragmenta el paquete en paquetes más pequeños. Cada paquete fraccionado es menor o igual al valor de la MTU.
Si un paquete ha sido fragmentado por un enrutador, este no será ensamblado hasta su llegada al receptor. El ensamble se producirá en el host receptor.
Un paquete que ha sido fragmentada puede volver a ser re-fragmentado en caso que vaya a propagarse por una red con una MTU menor.

5.1.7.20 Fragmentación y MTU

Una cabecera IP consta de 20 octetos.
La longitud de los datos es dependiente del protocolo. Algunos ejemplos son:
Ethernet: la trama consta de 1518 octetos. El contenido de IP consta 1500 octetos distribuidos en 1480 octetos para los datos más 20 octetos para la cabecera.
ATM: 9180 octetos.
FDDI: 4470 octetos.
El paso de la información de una red de mayor capacidad de transporte de información a otra de menor capacidad, requiere de la fragmentación, conforme al valor de la MTU establecida para cada segmento.

5.1.7.21 Ejemplo de fragmentación y MTU

Ejemplo: Un enrutador recibe un paquete con la identificación 345, compuesto por 5140 octetos, conforme a la siguiente información el cual debe ser enrutado a una red Ethernet. Represente el paquete o los paquetes en la red Ethertnet.

<table>
<tr><td>Versión = 4</td><td>Longitud de la cabecera = 5</td><td>Tipo de servicio = 0</td><td colspan="4">Longitud total = 5140</td></tr>
<tr><td colspan="3">Identificación = 345</td><td>Bit Reservado = 0</td><td>Bit DF=0</td><td>Bit MF=0</td><td>Desplaz. Fragm. = 0</td></tr>
<tr><td colspan="2">TTL = 120</td><td>Protocolo = 01</td><td colspan="4">Checksum</td></tr>
<tr><td colspan="7">Origen 192.168.1.1</td></tr>
<tr><td colspan="7">Destino 192.168.2.2</td></tr>
<tr><td colspan="7">Datos</td></tr>
</table>

El paquete entrante debe ser fragmentado para pasar a una red Ethernet.
La trama Ethernet compuesta por la cabecera y los datos consta de 1500 octetos. La cabecera consta de 20 octetos, los datos ocupan 1500 - 20 = 1480 octetos.
El desplazamiento en fragmentos se expresa en múltiplos de ocho octetos, lo cual corresponde a un valor de 1480 / 8 = 185.
Los datos recibidos constan de 5140 - 20 = 5120 octetos, excluyendo la cabecera. En múltiplos de ocho octetos se tiene 5120 / 8 = 640.
El número de segmentos a través de la red Ethernet tiene el valor de 640 / 185 = 3,4595.
Lo cual corresponde a tres segmentos completos y el cuarto segmento con un menor número de datos.

5.1.7.22 Ejemplo de fragmentación y MTU

Cabecera 20 octetos	Datos 5120 octetos ; 5120 / 8 = 640 en múltiplos de ocho octetos

El primer fragmento consta de 185 unidades en múltiplos de ocho octetos. La posición inicial del primer fragmento es cero y ocupa hasta la posición 184.
El segundo fragmento inicia en la posición 185 y se extiende hasta la posición 369.
El tercer fragmento inicia en la posición 370 y se extiende hasta la posición 554.
El último segmento consta de menos datos, 640 - 555 = 85.
El cuarto segmento inicia desde la posición 555 hasta la posición 639.
El campo de desplazamiento de segmento consta de 13 bits y debe indicar el inicio de los datos de cada uno de los fragmentos.

0	……..	184
185	……	369
370	……	554
555	……	639

5.1.7.23 Ejemplo de fragmentación y MTU

Los datos del paquete para el primer fragmento son

Versión = 4	Longitud de la cabecera = 5	Tipo de servicio = 0	Longitud total = 1500			
Identificación = 345			Bit Reservado = 0	Bit DF=0	Bit MF=1	Desplaz. Fragm. = 0
TTL = 120		Protocolo = 01	Checksum1			
Origen 192.168.1.1						
Destino 192.168.2.2						
Datos						

Cabecera 1 ; 20	Datos : desde 1 - hasta 1480 en

5.1.7.24 Ejemplo de fragmentación y MTU

Los datos del paquete para el segundo fragmento son:

Versión = 4	Longitud de la cabecera = 5	Tipo de servicio = 0	Longitud total = 1500			
Identificación = 345			Bit Reservado = 0	Bit DF=0	Bit MF=1	Desplaz. Fragm. = 185
TTL = 120		Protocolo = 01	Checksum2			
Origen 192.168.1.1						
Destino 192.168.2.2						
Datos						

Cabecera 2 ; 20	Datos : desde 1481 - hasta 2960 en

5.1.7.25 Ejemplo de fragmentación y MTU

Los datos del paquete para el tercer fragmento son:

Versión = 4	Longitud de la cabecera = 5	Tipo de servicio = 0	Longitud total = 1500			
Identificación = 345			Bit Reservado = 0	Bit DF=0	Bit MF=1	Desplaz. Fragm. = 370
TTL = 120		Protocolo = 01	Checksum3			
Origen 192.168.1.1						
Destino 192.168.2.2						
Datos						

Cabecera 3 ; 20	Datos : desde 2961 - hasta 4440 en

5.1.7.26 Ejemplo de fragmentación y MTU

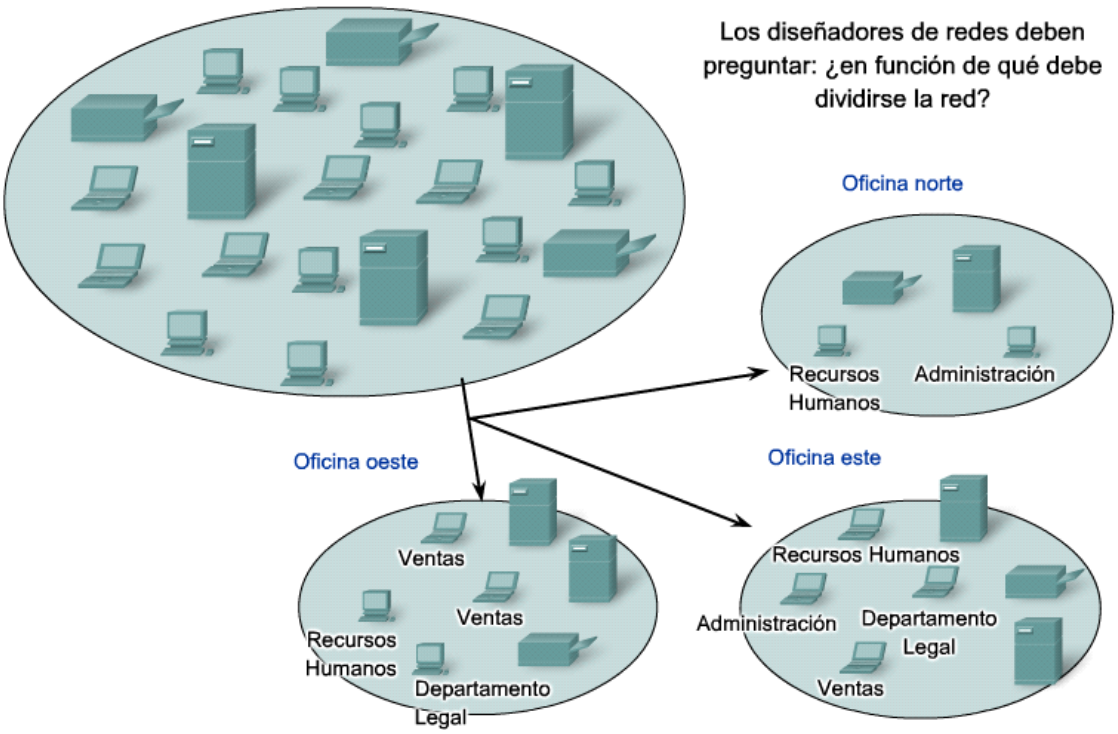
Los datos del cuarto y último paquete son

Versión = 4	Longitud de la cabecera = 5	Tipo de servicio = 0	Longitud total = 700			
Identificación = 345			Bit Reservado = 0	Bit DF=0	Bit MF=0	Desplaz. Fragm. = 555
TTL = 120		Protocolo = 01	Checksum4			
Origen 192.168.1.1						
Destino 192.168.2.2						
Datos						

Cabecera 4 ; 20	Datos : desde 4441 - hasta 5120 en

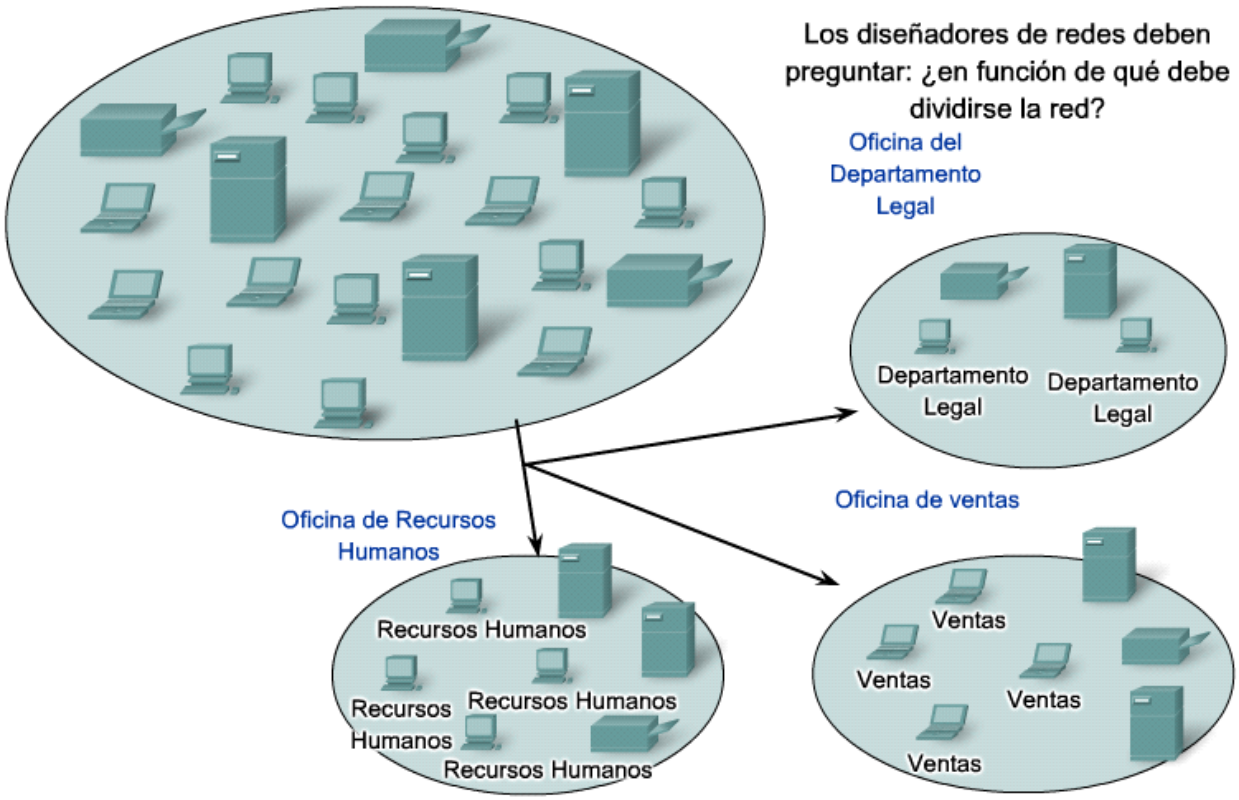
5.2.1.1 Redes: Separación de hosts en grupos comunes.

La cantidad de usuarios de las primeras redes tuvo un crecimiento inesperado.
Muchos usuarios compartían recursos comunes. Otros grupos de usuarios necesitaban operar con algunas restricciones en relación a los demás integrantes de la red.
Se facilita la administración de una red si se procede a la separación de redes en grupos conforme a algunos criterios que faciliten su control y proporcionen la seguridad funcional y limitación de acceso a determinados recursos entre otras consideraciones.
Para lograr esto, es necesario la división de una red en redes más pequeñas o subredes.
Factores que definen la separación: ubicación geográfica, propósito y propiedad.
Separación de los usuarios por su ubicación geográfica.



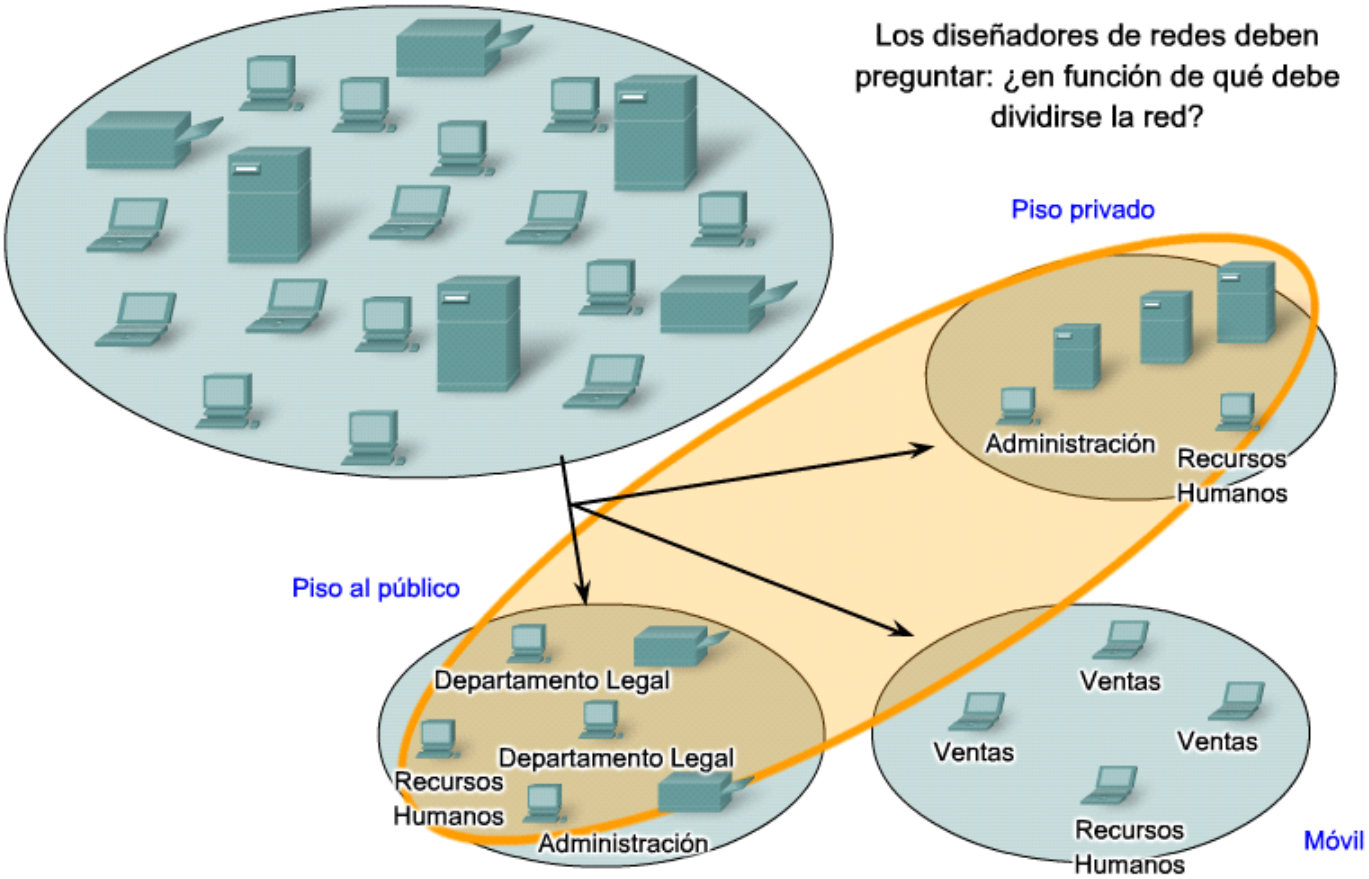
5.2.1.2 Redes: separación en grupos comunes

Separación de los hosts por el propósito: función de la dependencia o actividad que deben realizar los usuarios en cada subred.



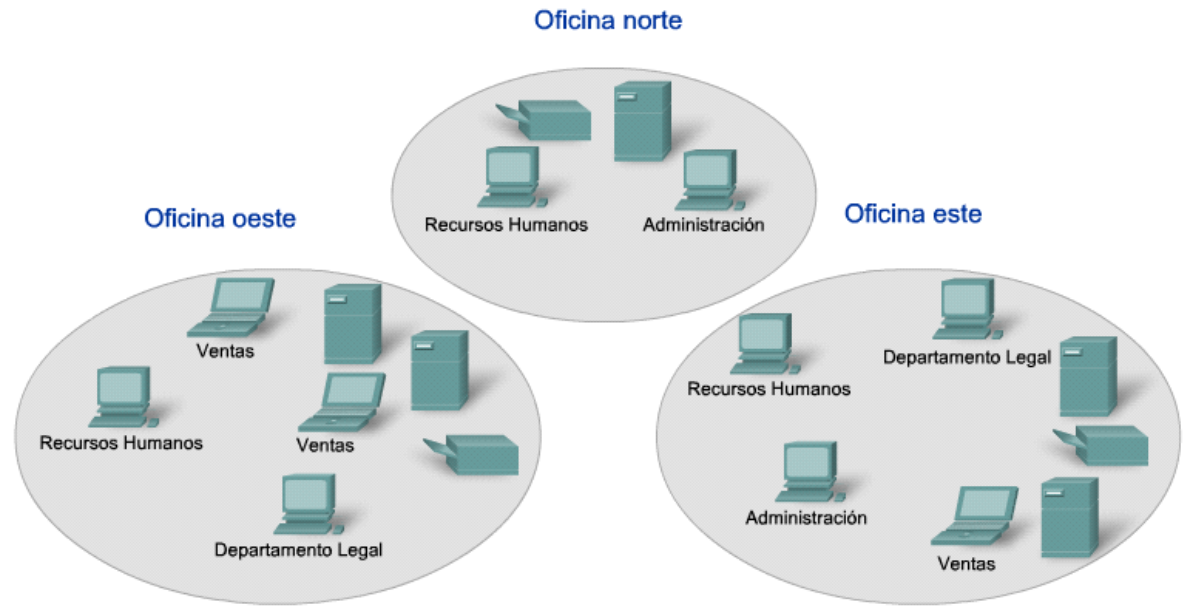
5.2.1.3 Redes: separación de host en grupos comunes

Separación de los host conforme a la propiedad o administración de las subredes.



5.2.1.4 Redes: separación de host en grupos comunes

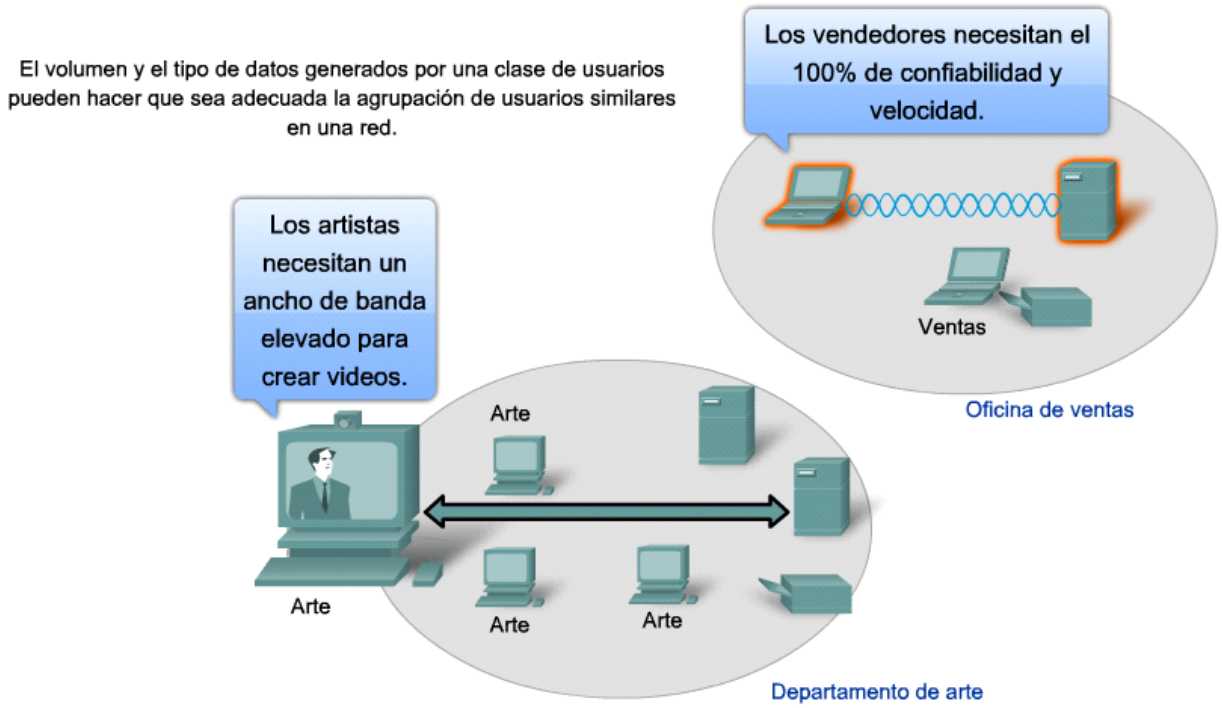
Agrupación de host de manera geográfica
Concentración de usuarios en diferentes áreas de una entidad.
Facilidad de integración a la red de los grupos dispersos por medio de enlaces de larga distancia.



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.

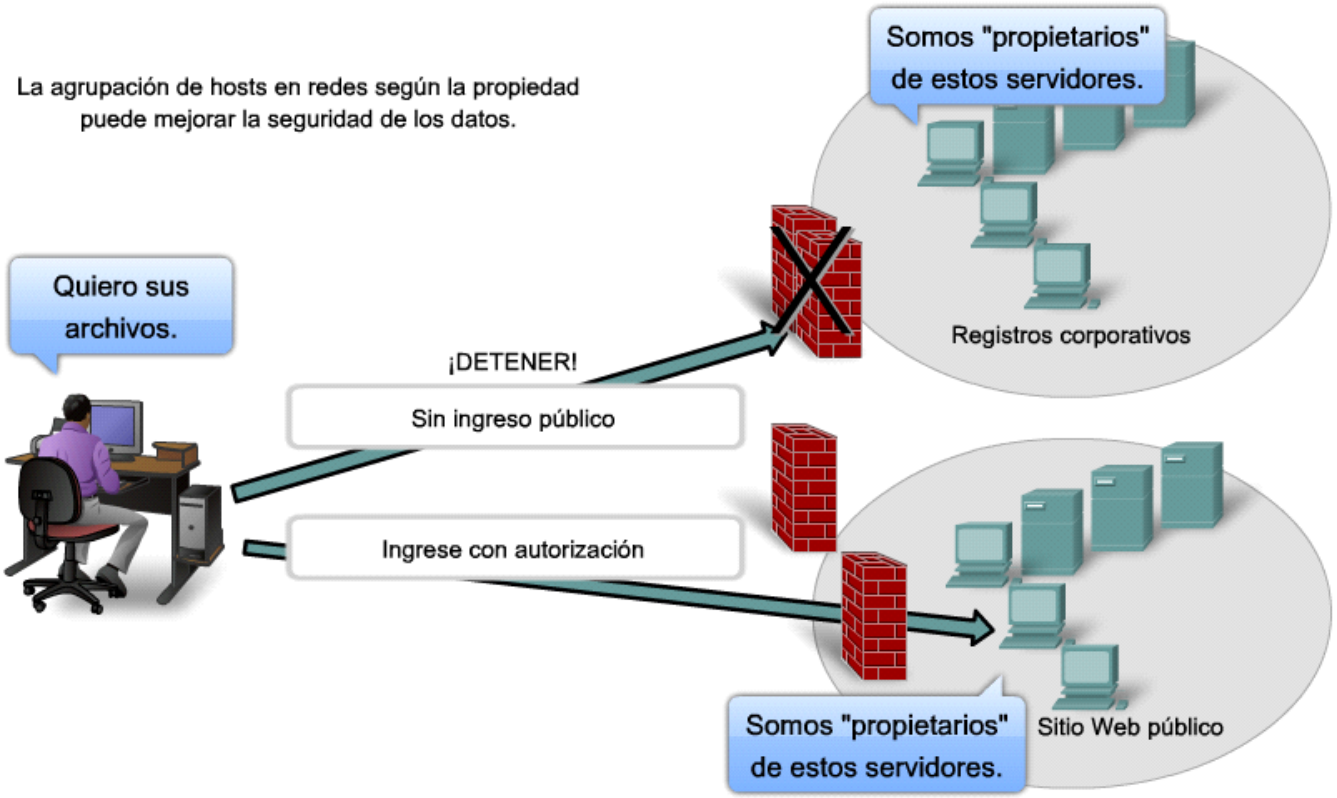
5.2.1.5 Redes: separación de hosts en grupos comunes

Agrupación de hosts conforme al propósito.
Muchos usuarios realizan tareas similares, comparten el mismo software y posiblemente tienen el mismo patrón de tráfico.
El volumen de tráfico generado por las diferentes aplicaciones puede variar significativamente.
Es necesario un equilibrio entre el número de hosts y la cantidad de tráfico que podrían generar algunos grupos de usuarios.
En una empresa los diseñadores gráficos podrían ocupar un gran ancho de banda de la red durante un horario extenso de su actividad laboral. Conforme a esto, podrían necesitar un gran ancho de banda disponible en la red.
Otros grupos de usuarios verifican el resumen de sus actividades transaccionales al final de la actividad laboral.
La asignación de algunos recursos de uso amplio en una red, puede disminuir el tráfico hacia otras redes. Por ejemplo: la incorporación de servidores con aplicaciones propias para un grupo de usuarios de alto tráfico.



5.2.1.6 Redes: separación en grupos comunes

Separación conforme a la propiedad o administración de la red.
Cada subred tiene su propio administrador. La responsabilidad del personal de red queda limitada e identificada en cada subred.

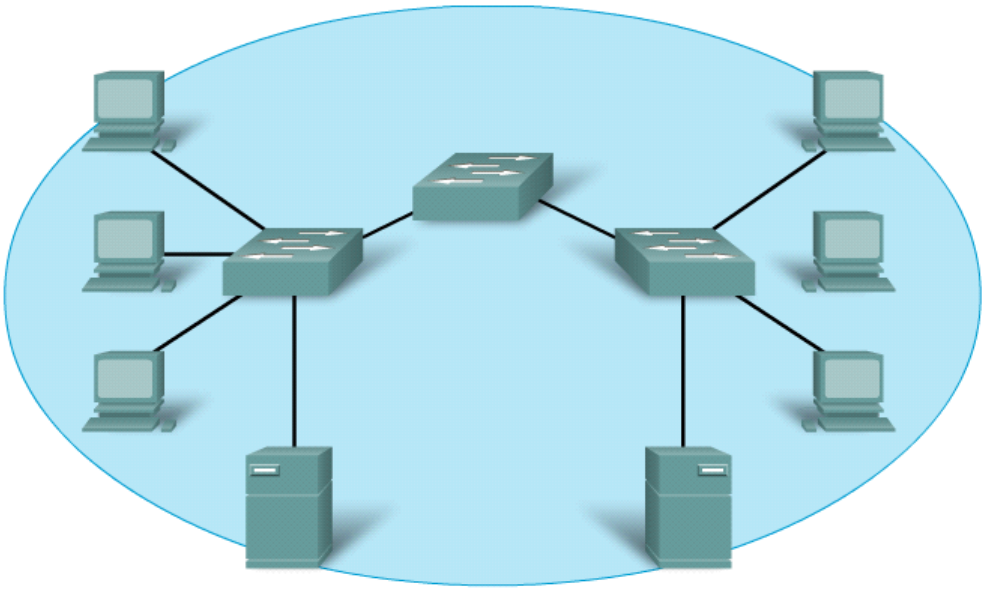


5.2.2.1 División de host en redes: rendimiento.

Los problemas mas comunes con la redes grandes son:

- Degradación del rendimiento.
- Seguridad.
- Administración de direcciones.

Además de las comunicaciones reales en una red, también se tiene la comunicación de difusión (broadcast).
La comunicación de difusión, deseable o indeseable, se propaga hacia todos los usuarios de la red.
La ocupación de la red con esta clase de trafico limita el uso de la red.
Grandes cantidades de usuarios en una red generan grandes cantidades de tráficos de difusión, con lo cual la disponibilidad de la red se reduce.
El switch no segmenta la red, no se establecen dominios de difusión (broadcast).



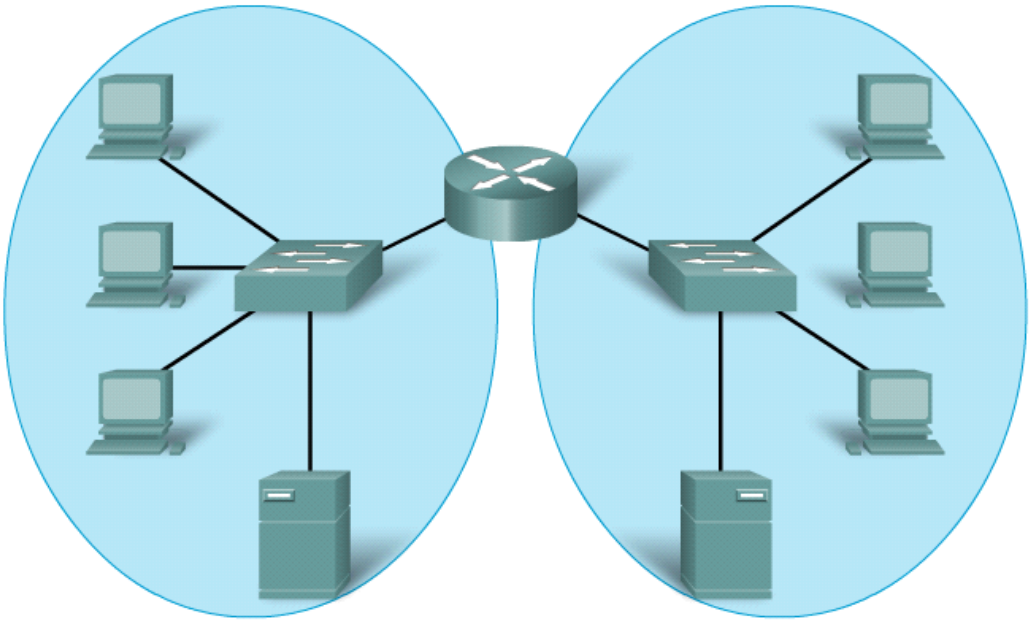
Todos los dispositivos de esta red se conectan en un dominio de broadcast cuando se establece el switch según la configuración predeterminada de fábrica. Debido a que los switches reenvían broadcasts en forma predeterminada, todos los dispositivos de esta red procesan los broadcasts.

5.2.2.2 División de host en redes: rendimiento

Mejora del rendimiento

El enrutador establece dominios de difusión (broadcast) por medio de la división de una red en subredes.

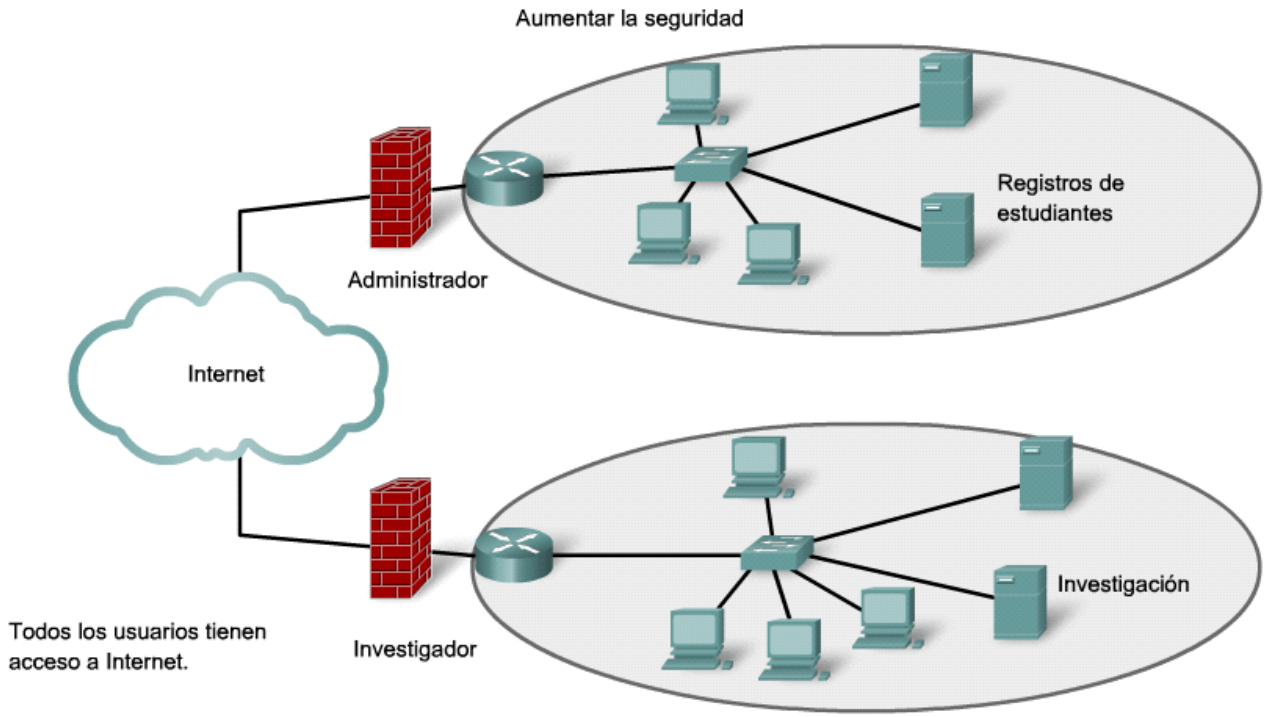
Los enrutadores no permiten el paso del tráfico de difusión (broadcast) de una red a otra red o entre subredes.



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

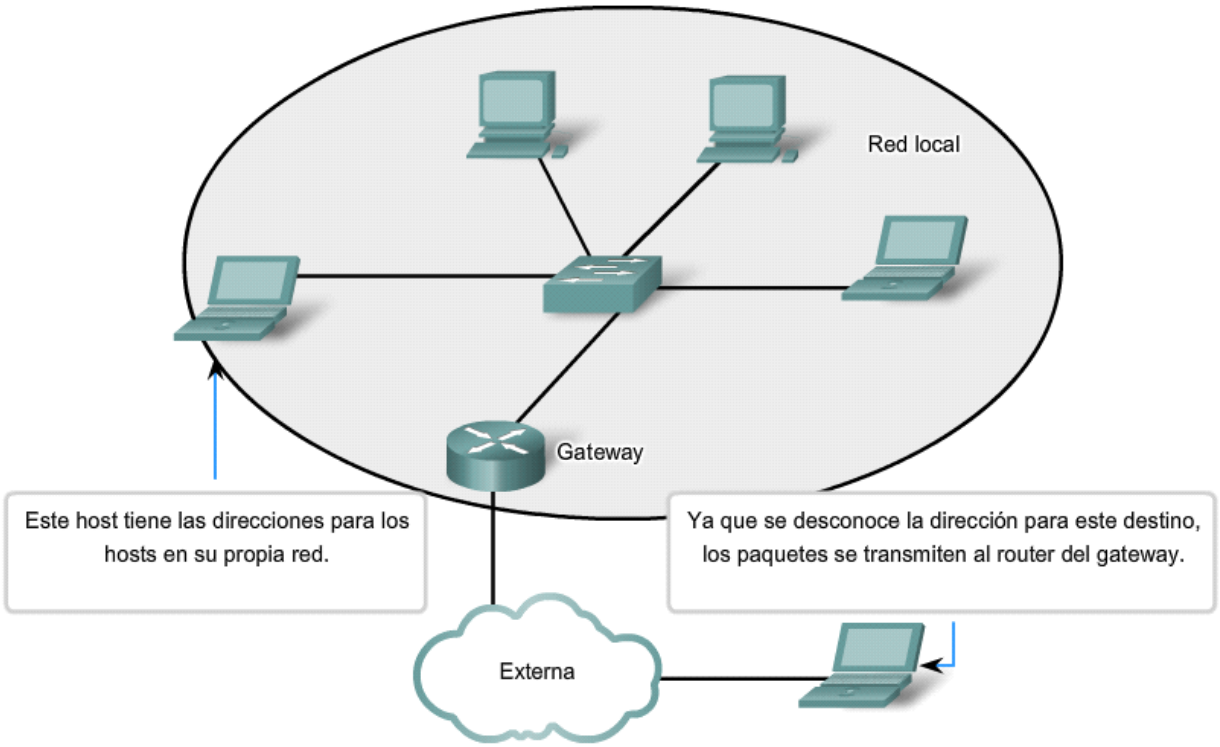
5.2.3 División de host en redes: seguridad

División de una red grande en redes más pequeñas se realiza conforme a las actividades de los usuarios o funciones que se desarrollen en algunas dependencias de una entidad.
En las redes más pequeñas es posible la implementación del control de acceso a los servidores de cada una de las redes por medio del uso de firewall en los puntos de entrada a la red.



5.2.4 División de host en redes: administración de direcciones

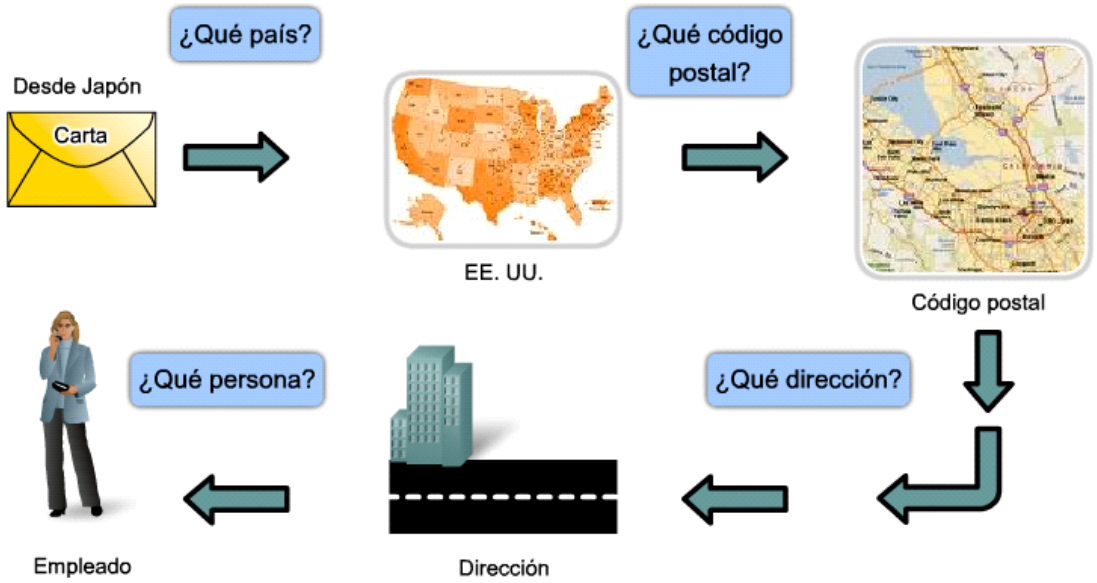
La red de Internet está compuesta por millones de hosts.
Cada host tiene una dirección única la cual no se repite en Internet.
Un host no conoce la dirección de los demás host que existen en la red global. No se le podría agregar una carga de procesamiento que degrade su comportamiento.
La división de los hosts de una red en varias redes permite la reducción de la carga en host para que pueda comunicarse con otro host.
En una red con pocos hosts, un host cualquiera puede ubicar a otro host de la misma red con poca sobrecarga de procesamiento local.
Si el destinatario se encuentra en otra red, el host entrega el tráfico a un dispositivo intermediario denominado Enrutador Gateway.
El enrutador Gateway es la puerta de salida o entrada de una red hacia otra red.



Los hosts desconocen cómo entregar los datos a los dispositivos en una red remota, ésta es la función del gateway.

5.2.5 División de host en redes: direccionamiento jerárquico

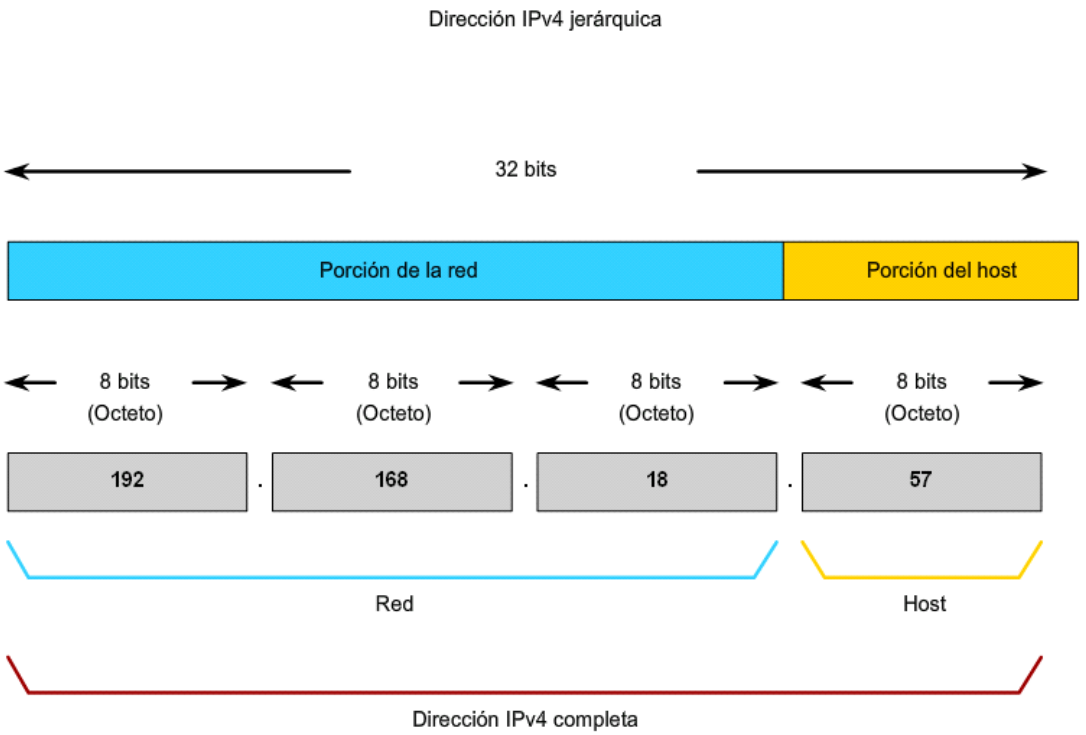
Los hosts tienen una estructura de direccionamiento jerárquico.
Las redes también tiene una estructura de direccionamiento jerárquico, lo cual permite el direccionamiento de las redes y el enrutamiento del tráfico a través de las redes.
Un ejemplo de direccionamiento jerárquico está asociado con el servicio postal. Las direcciones usadas son jerárquicas: país, estado o departamento, ciudad, calle, edificio…...nombre del destinatario.
Una dirección en Internet consta de una dirección de red y una dirección de host.
Los enrutadores intermedios solamente necesitan conocer las direcciones de red para el reenvío de un paquete hacia la red de destino.
En la red de destino se usa la dirección de host para la localización del destino de un mensaje.
Si un país tiene numerosas redes grandes, la división y agrupación de las redes en forma jerárquica permite el transporte de los paquetes hacia el destino final con poca sobrecarga en la red.



En cada paso de la entrega, la oficina de correos sólo necesita examinar el siguiente nivel jerárquico.

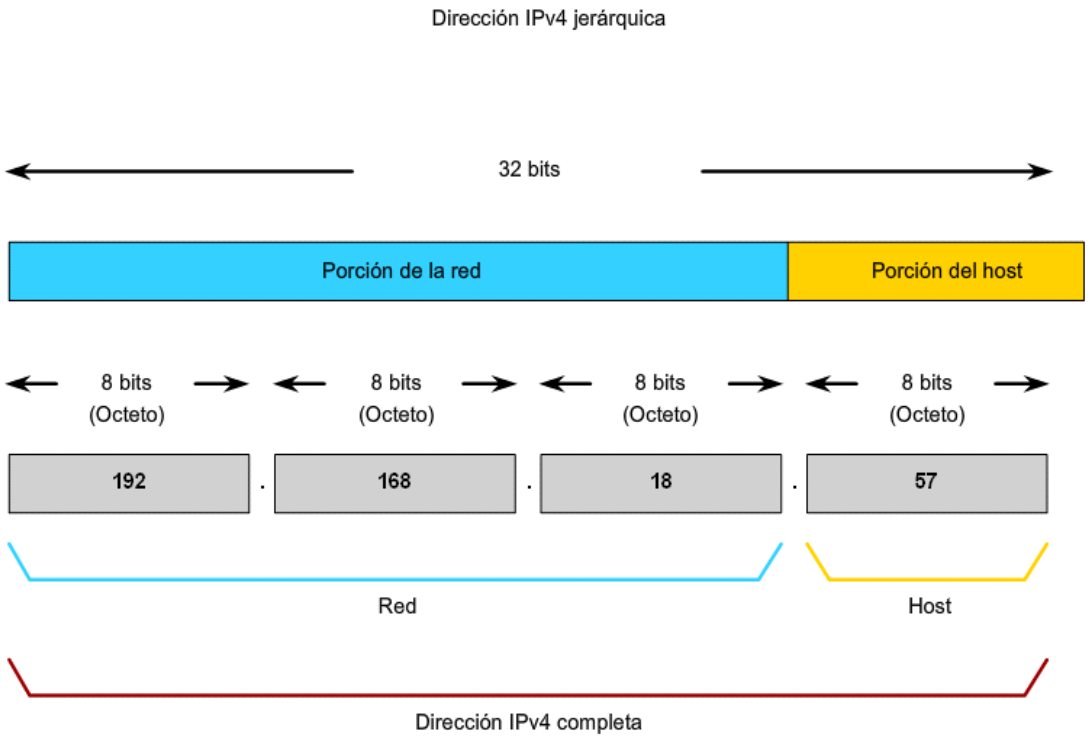
5.2.6.1 División de redes: redes a partir de redes

Si se tiene una red grande, es posible la creación de otro nivel jerárquico inferior y luego estructurar la agrupación de los hosts.
Una dirección lógica IPv4 consta de 32 bits, tiene una composición jerárquica y consta de una porción de red y una porción de host.
Las direcciones IP se dividen en cuatro grupos representados por números decimales y separados por puntos.
Por ejemplo, en la dirección 192.168.18.57, los tres primeros octetos separados por puntos 192.168.18 indican la porción de red. El último octeto 57 indica la porción de host.
El direccionamiento jerárquico permite la ubicación de cada host dentro de una determinada red.
El enrutador solamente necesita conocer las direcciones de la porción de red para enviar el paquete a su destino. No necesita conocer las direcciones de cada uno de los hosts de cada red.
Este esquema de direccionamiento jerárquico permite que todos los hosts de una red tengan la misma dirección de red. Solamente difieren en la dirección de host.



5.2.6.2 División de redes: redes a partir de redes

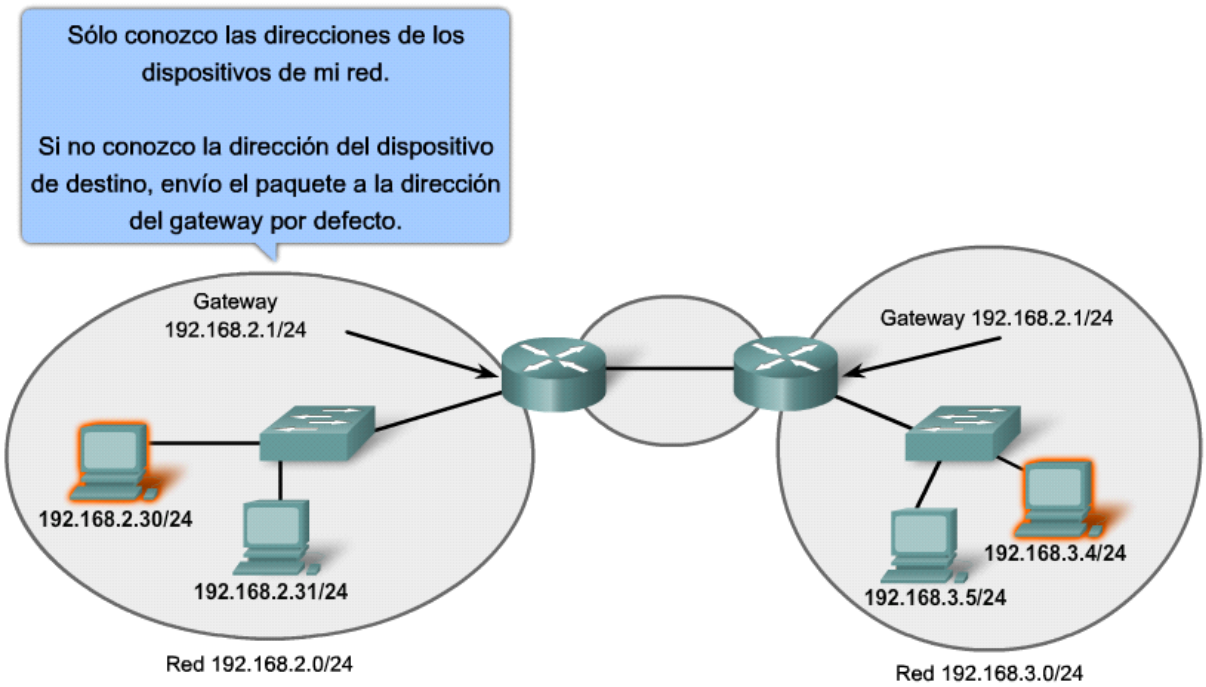
A la cantidad de bits de una dirección IP que se utiliza como porción de red, se le denomina duración o longitud de prefijo de red.
Por ejemplo, si se usan 24 bits para expresar la porción de red de una dirección IP, se dice que el prefijo es /24.
En el direccionamiento IPv4, el valor del prefijo puede ser expresado por medio de cuatro números separados por puntos, lo cual se denomina máscara de red.
El valor del prefijo de red permite el dimensionamiento de una red.
El valor del prefijo de red permite la estructuración de otro nivel jerárquico denominado subred para la agrupación de los hosts de una manera más selectiva.



5.3.1 Parámetros de dispositivos : comunicación fuera de la red

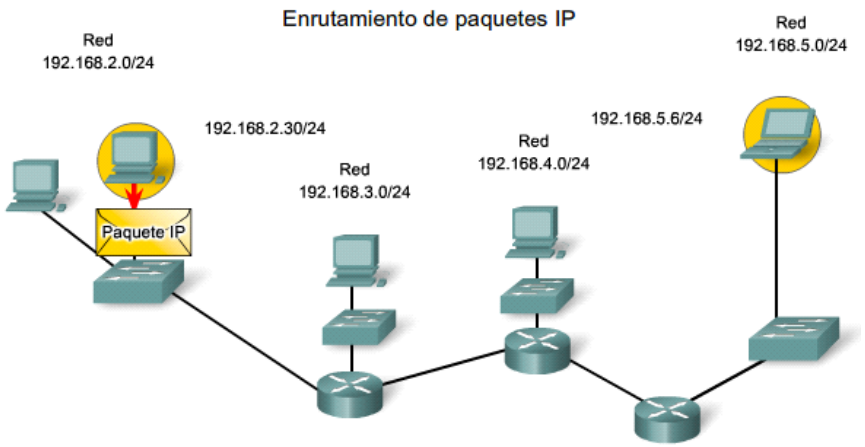
Dentro de una misma subred los hosts se comunican entre ellos sin la necesidad de un dispositivo intermediario.
Para una comunicación con un host de otra red o subred, el host originador se comunica con un enrutador gateway o gateway predeterminado, cuya interfaz de red es la misma que el originador.
Como parte de su configuración, un host tiene asignada una dirección de un enrutador gateway predeterminada. Esta se encuentra en la misma red que el host originador del tráfico.
Un host no conoce la dirección de los hosts que se encuentran fuera de su red. Para comunicarse con un host de otra red, el originador le entrega el tráfico al enrutador gateway o gateway predeterminado para que este continúe con el proceso de conexión.
El enrutador busca una ruta disponible hacia otro enrutador para el envío del tráfico hacia otras redes. Esa ruta se denomina dirección del siguiente salto.

Los gateways permiten las comunicaciones entre redes

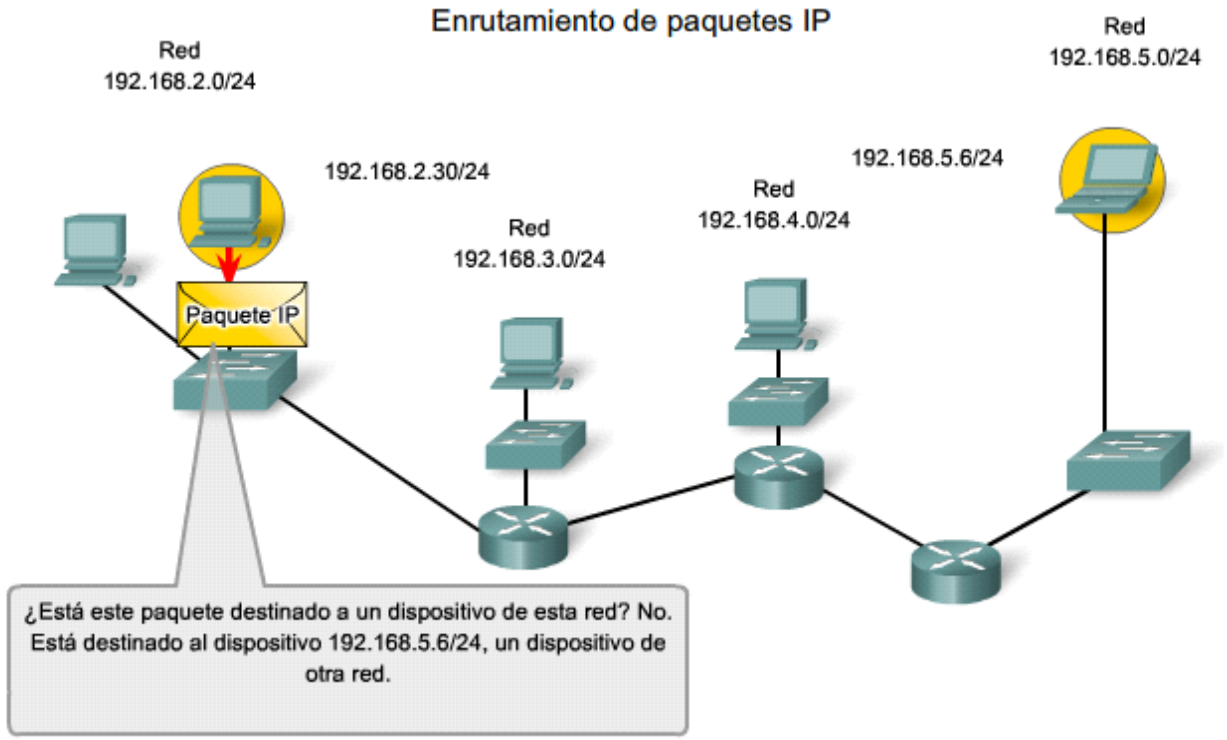


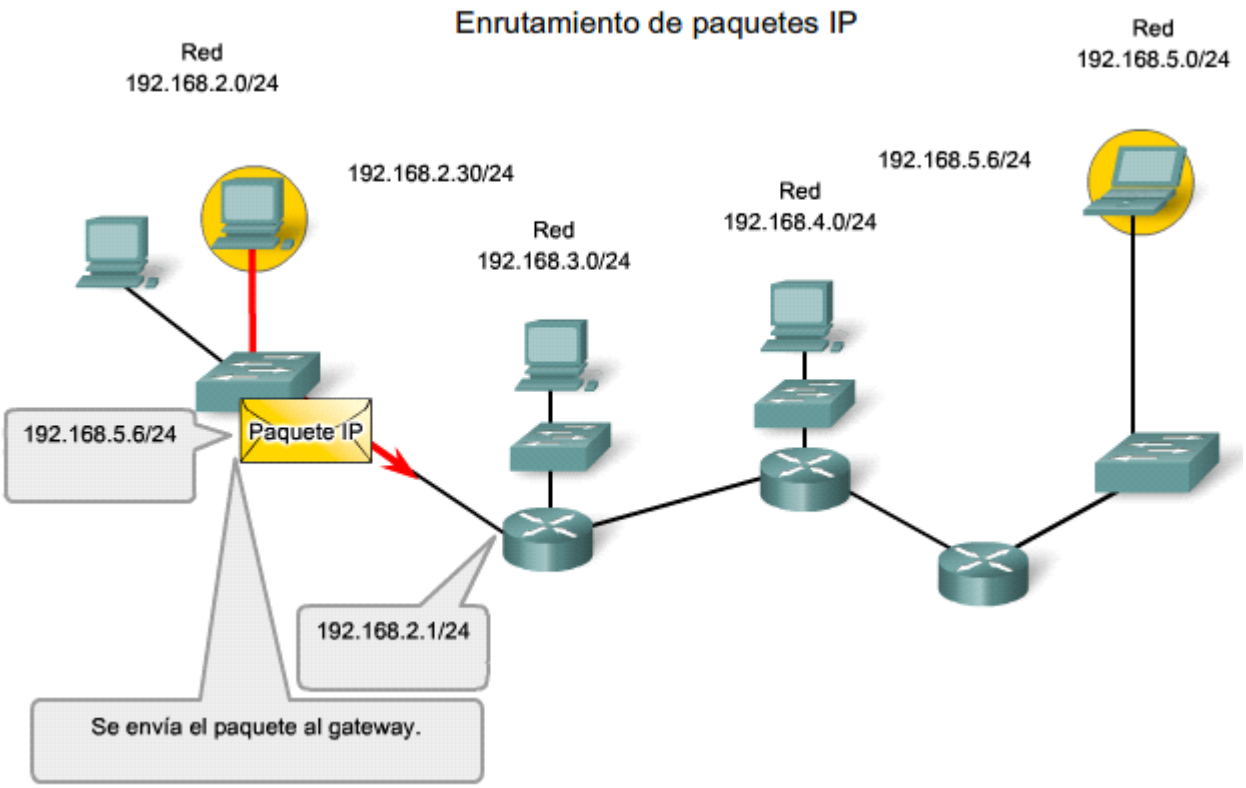
5.3.2.1 Paquetes IP: transporte de datos de extremo a extremo

El encabezado del paquete IP contiene la dirección de origen y de destino del paquete. El paquete transporta la PDU de la capa de transporte.
Si la comunicación se efectúa en la misma red, la comunicación es directa sin la intervención del enrutador gateway.
Si la comunicación es con otro host de una red diferente, la comunicación se efectúa por medio del enrutador el cual direcciona el paquete al siguiente salto.
El contenido de la PDU de la capa de transporte y las direcciones IP de origen y destino del paquete se mantienen intacto durante el proceso de re-envío de los paquetes que efectúa un enrutador.
Cuando el paquete llega a su destino se remueve la cabecera de la capa de red se entrega el contenido del segmento o del datagrama.
La dirección IP de origen y destino de los host permanecen inalterable durante todo el recorrido del paquete y durante el intercambio de las transacciones.
Para una comunicación entre dos hosts de diferentes redes, el originador envía el paquete al enrutador gateway. El enrutador examina la porción de red del paquete enviado a un host de otra red.
Si la red de destino está conectada en otra interfaz del mismo enrutador, el tráfico es direccionado directamente al host de destino.
Si la red de destino no está conectada directamente al enrutador gateway, el paquete es enviado a un segundo enrutador, denominado enrutador del siguiente salto.
A partir de ese momento, el enrutador del siguiente salto debe continuar con el proceso del envío del paquete hacia su destino.

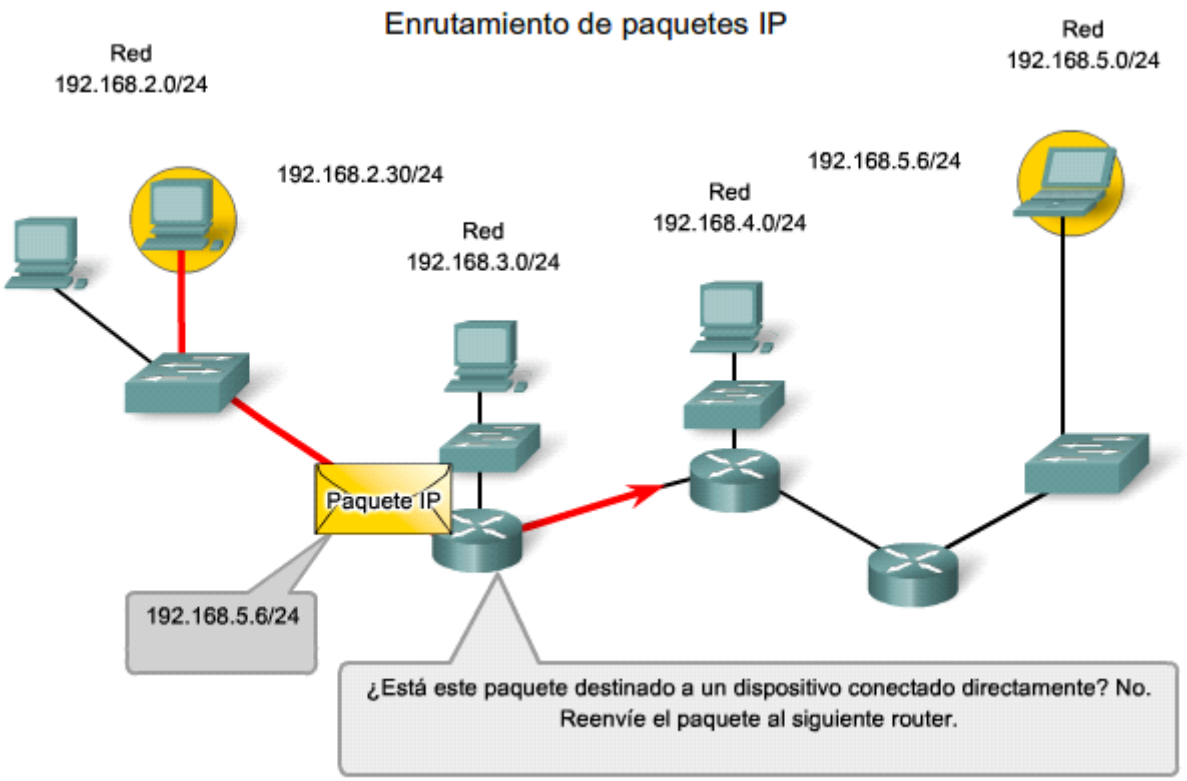


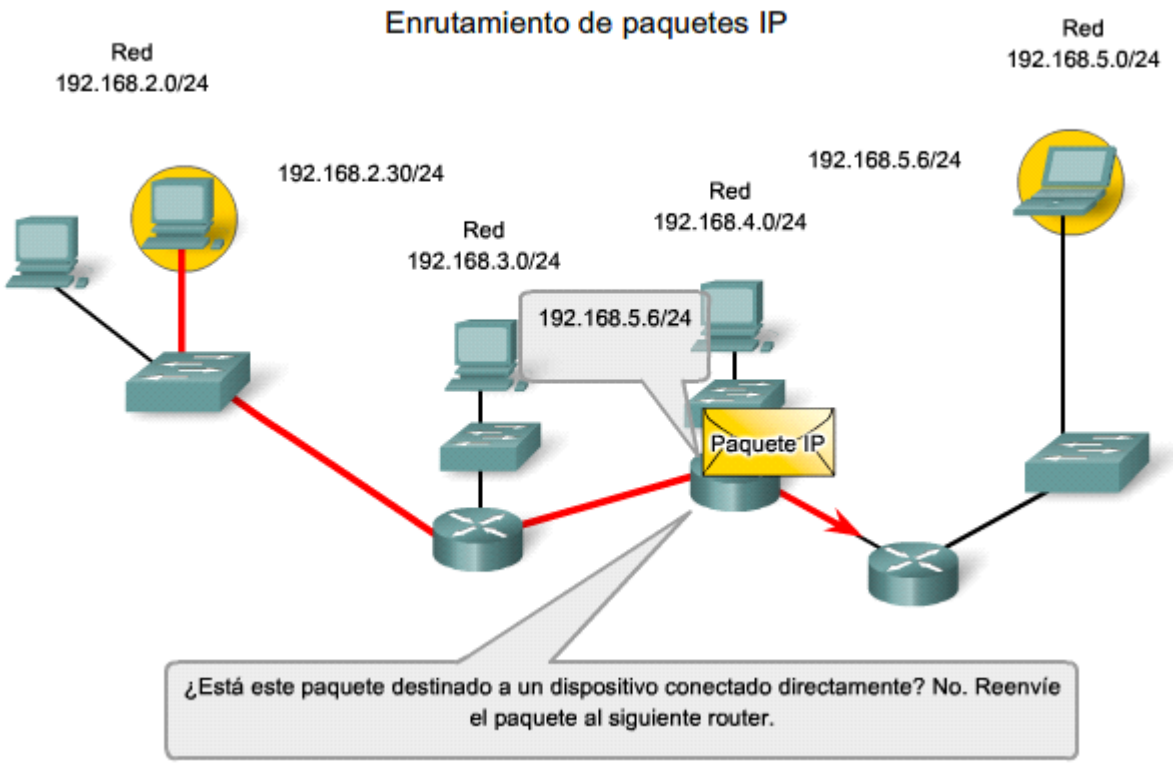
5.3.2.2 Paquetes IP: transporte de datos de extremo a extremo



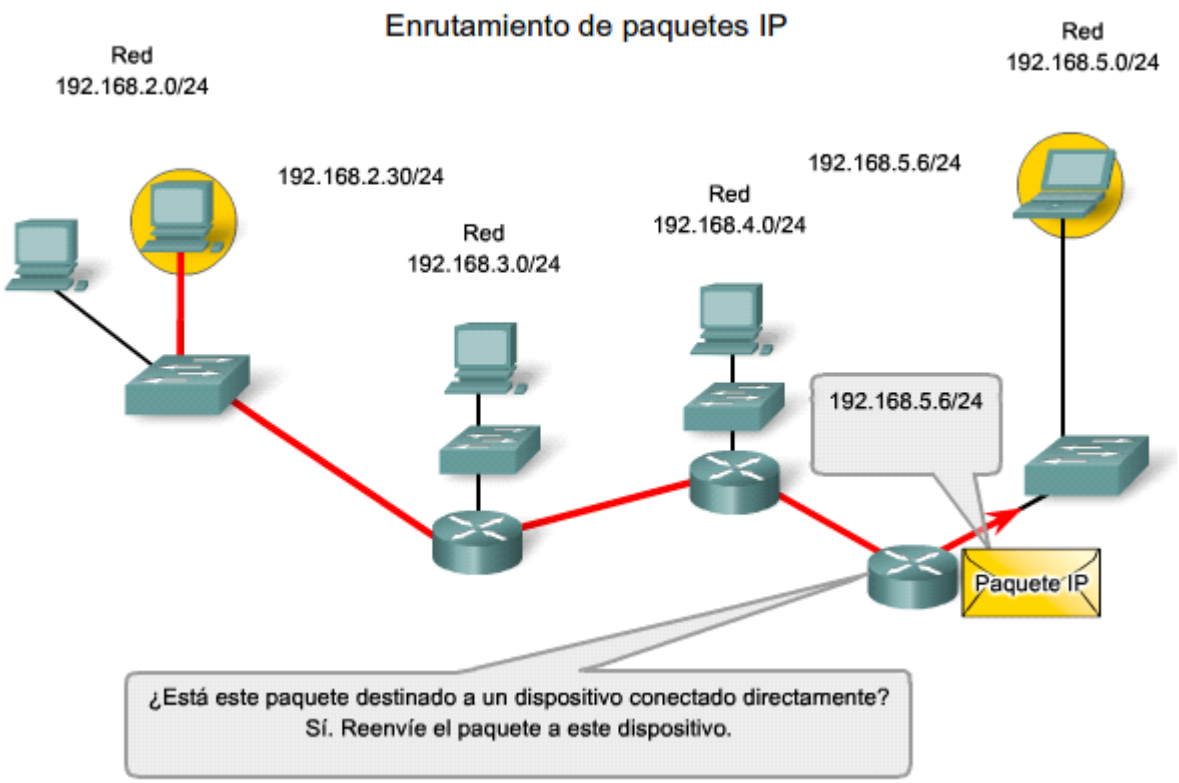


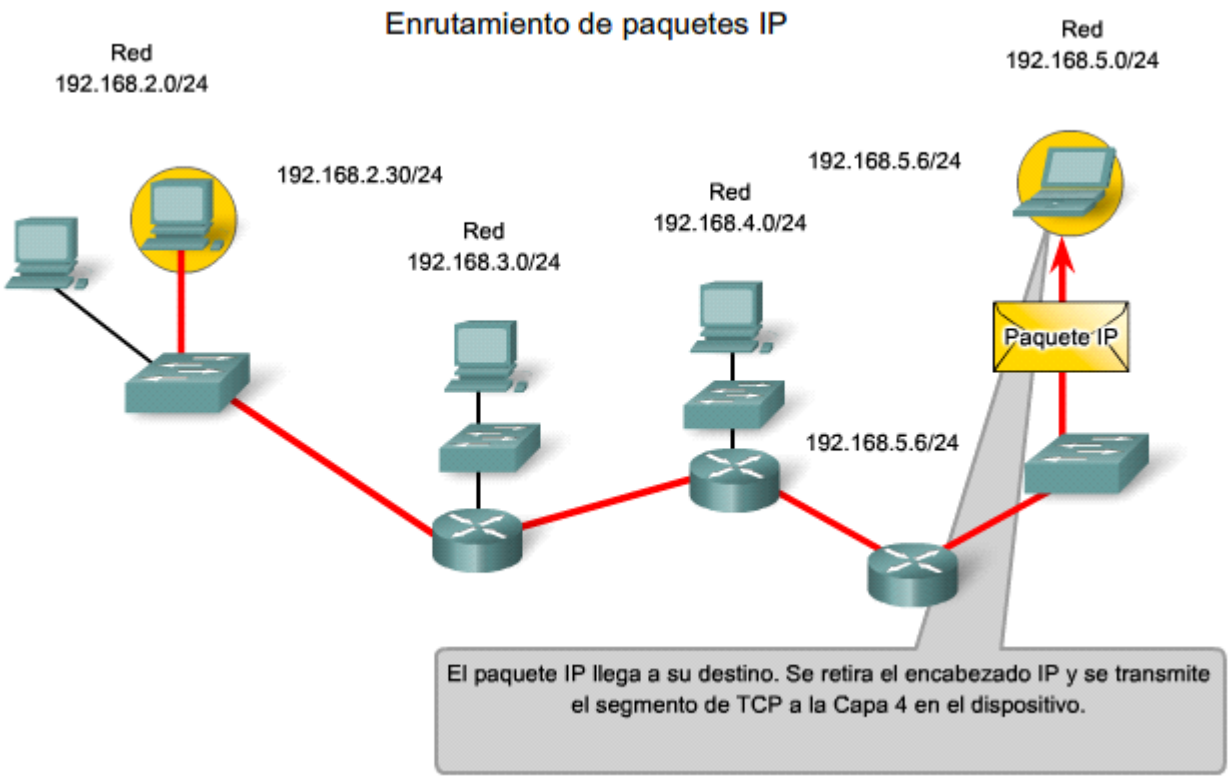
5.3.2.3 Paquetes IP: transporte de datos de extremo a extremo





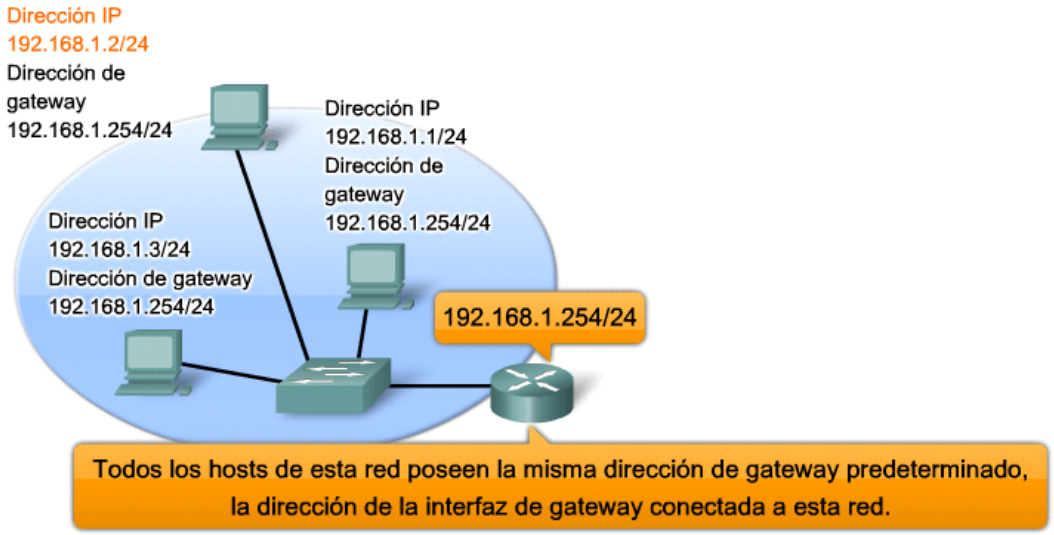
5.3.2.4 Paquetes IP: transporte de datos de extremo a extremo





5.3.3.1 Gateway: la salida de la red

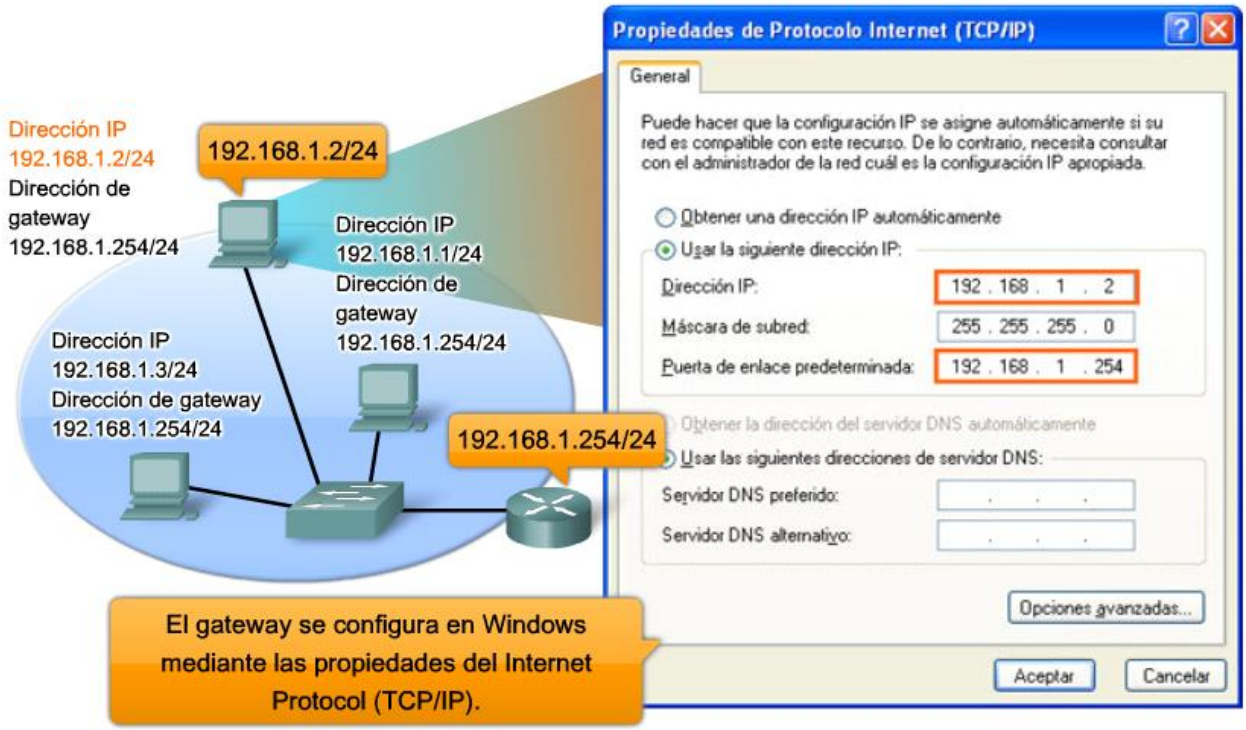
Si la porción de red de la dirección de destino del paquete es diferente a la porción de red del host de origen, el paquete debe encontrar una salida fuera de su red original.
Para esto, el paquete es enviado al enrutador gateway. El enrutador gateway tiene una interfaz conectada a la misma red local del host de origen.
La interfaz del enrutador gateway tiene una dirección cuya porción de red concuerda con la porción de red de los hosts de la misma red.



5.3.3.2 Gateway: la salida de la red

Gateway predeterminado

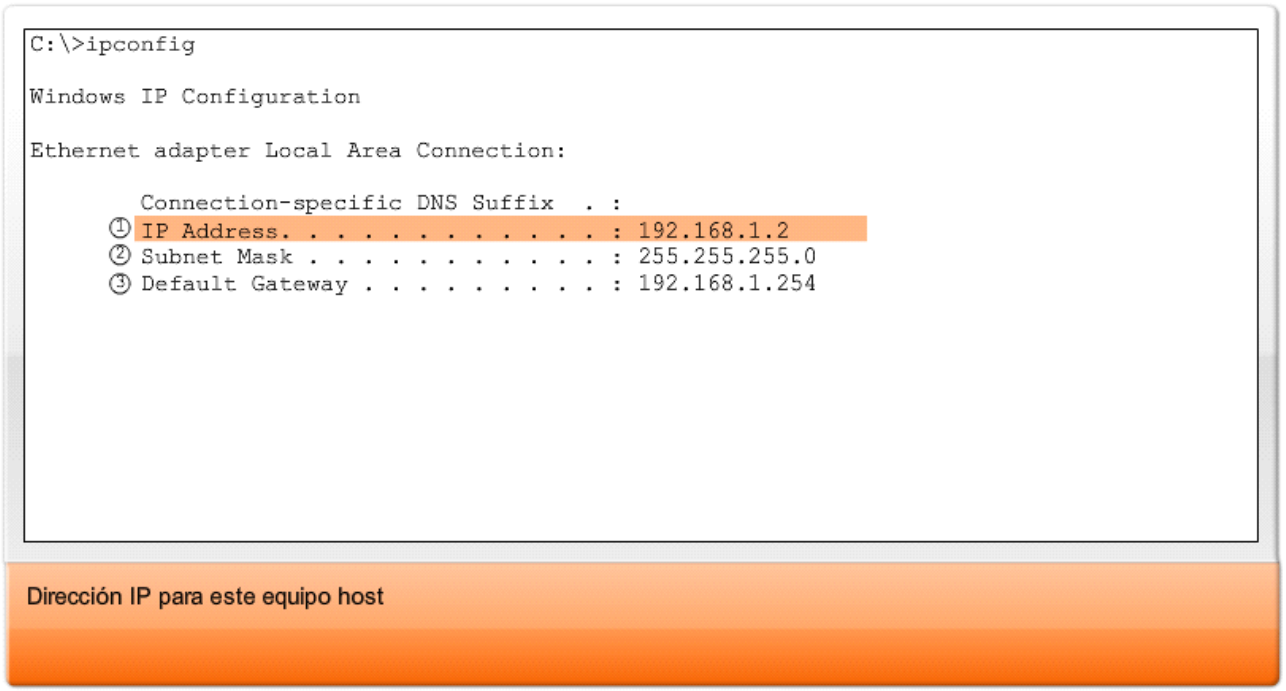
Las direcciones configurables de IPv4 correspondientes a los host de una misma red y al enrutador gateway o gateway predeterminado comparten la misma porción de red.



5.3.3.3 Gateway: la salida de la red

En la línea de comandos, el comando ipconfig permite la lectura de la dirección IP del host y la dirección IP del gateway de salida.

Confirmación de la configuración del gateway



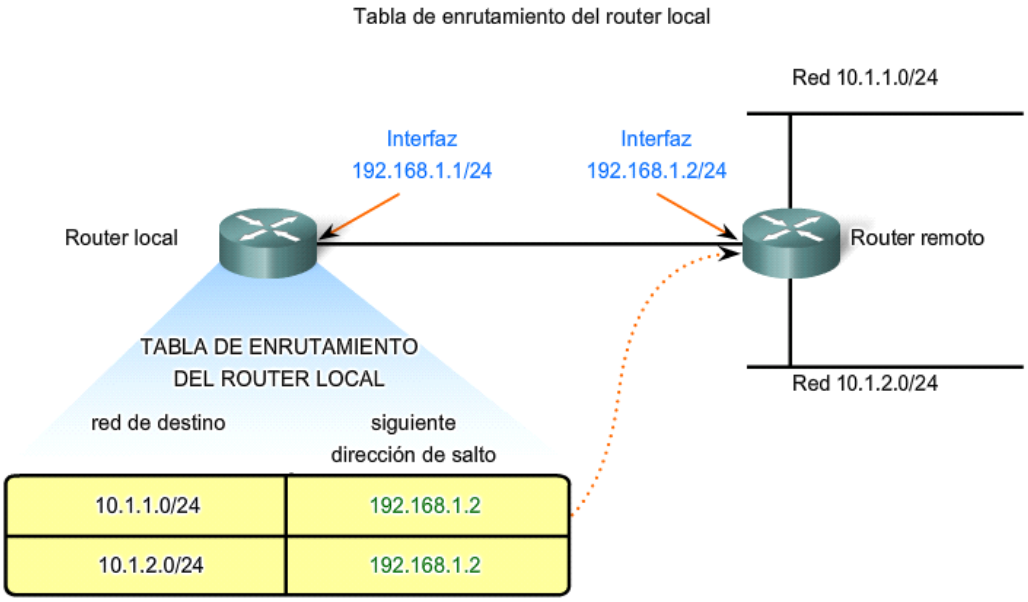
Resultado **ipconfig** de ejemplo que muestra la dirección del gateway predeterminado

5.3.3.4 Gateway: la salida de la red

Ningún paquete puede ser enviado sin una ruta. Si un paquete se origina en un host o se reenvía desde un dispositivo intermediario, debe existir una ruta para el envío del paquete hacia su destino.
Un host debe tener la capacidad de enviar un paquete a otros host de la misma red o al enrutador gateway para su posterior re-envío hacia otra red o subred.
Los paquetes destinados para otras redes son recibidos por el gateway predeterminado para su posterior entrega al destino final en el mismo enrutador o a otros enrutadores en caso que el destino final lo indique.
Un gateway predeterminado puede enviar los paquetes de una dirección o de un grupo de direcciones

- Hacia otra red en el mismo enrutador si el host de destino se encuentra conectado a otra interfaz de red del mismo enrutador.
- Hacia otro enrutador configurado como enrutador del siguiente salto.

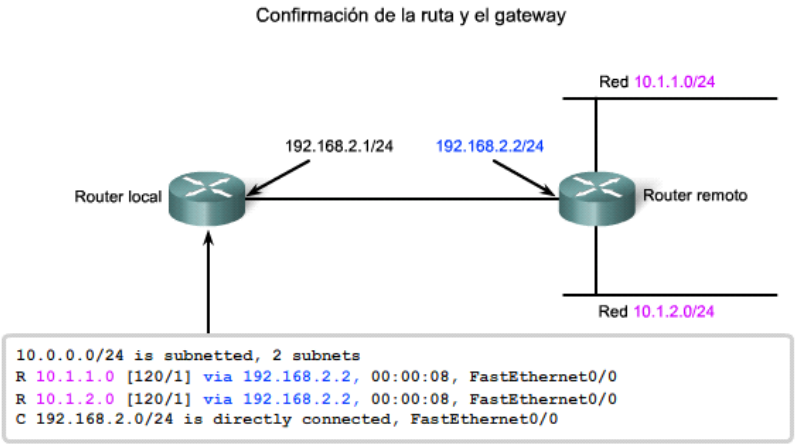
El gateway predeterminado no encamina el paquete hacia los enrutadores no contiguos ni tampoco al enrutador final donde está conectado el host de destino.



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

5.3.4.1 Ruta: el camino hacia una red

Mediante configuraciones, es posible agregar rutas a un host manualmente.
Cuando se configura una interfaz de un enrutador con una dirección IP y una máscara de red, la interfaz se vuelve parte de la red conjuntamente con los host conectados a la interfaz del enrutador. La tabla de enrutamiento incluye a esa red como una red conectada directamente al enrutador.
Todas las rutas hacia otros enrutadores deben ser configuradas manualmente o directamente por medio de los protocolos de enrutamiento.
Los enrutadores tienen tablas de enrutamiento para el re-envío de los paquetes.
Las tabla de enrutamiento almacena información acerca de las redes conectadas y las redes remotas.
Las redes conectadas están adjuntas directamente a una de las interfaces del enrutador. Estas interfaces son los gateways predeterminados para los hosts de las diferentes redes locales.
Las redes remotas no están conectadas directamente a un enrutador. En enrutamiento del paquete puede ser configurado manualmente o por medio del intercambio de información con enrutadores vecinos a través de protocolos de enrutamiento.



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

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

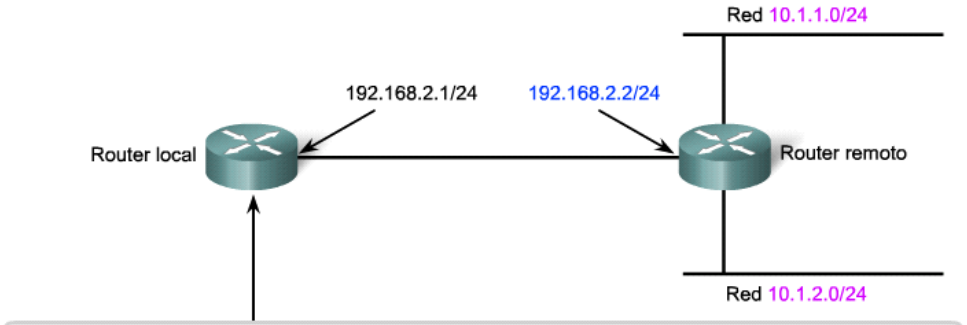
5.3.4.2 Ruta: el camino hacia una red

Los campos principales en una tabla de enrutamiento son:

- Red de destino
- Siguiente salto
- Métrica

El enrutador hace coincidir la dirección de destino del paquete con la red de destino de una ruta en la tabla de enrutamiento y re-envía el paquete al enrutador del siguiente salto que especifica esa ruta.
Si hay dos o más rutas posibles hacia el mismo destino final, se usa la métrica para decidir que ruta aparece en la tabla de enrutamiento.
Los paquetes que no tienen especificado el campo de dirección de destino son descartados.
Si una ruta de un paquete no está especificada en un enrutador, el paquete es descartado.
Los enrutadores establecen una ruta predeterminada para los paquetes cuya dirección no este especificada en una tabla de enrutamiento.

Confirmación de la ruta y el gateway




```
10.0.0.0/24 is subnetted, 2 subnets
R 10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R 10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

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

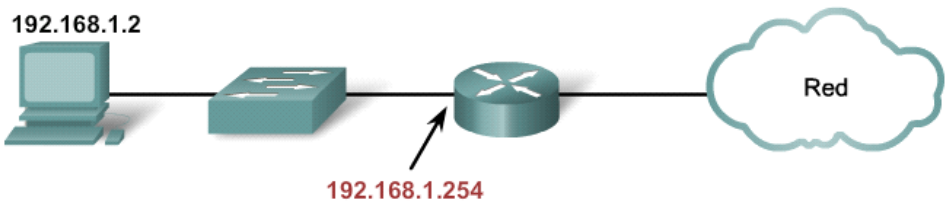
El siguiente salto para las redes 10.1.1.0/24 y 10.1.2.0/24 desde el router local es 192.168.2.2.

5.3.4.3 Ruta: el camino hacia una red

Tabla de enrutamiento del host

Un host crea las rutas para el envío de los paquetes que origina.
Estas rutas derivan de la red conectada directamente y del enrutador gateway o gateway por defecto.
Los hosts agregan todas las redes conectadas a las rutas. Estas rutas permiten a los paquetes su entrega a los hosts que están conectados a esas redes.
Los hosts también requieren una tabla de enrutamiento para asegurarse que todos los paquetes de la capa de red lleguen a la red de destino correcta.
A diferencia de los enrutadores que contiene las rutas locales y remotas, la tabla local del host contiene la dirección de la red a la cual está conectada y la ruta al gateway por defecto al cual está conectado.
La configuración de la dirección IP del gateway por defecto crea una ruta predeterminada local.
La tabla de enrutamiento de un host puede ser observada por medio de los comandos netstat -r, route o route print.
El contenido de la tabla de enrutamiento de un host puede ser editado por medio de los comandos:

- Route delete
- Route change
- Route add




```
Interface List
0x2 ...00 0f fe 26 f7 7b ...  Gigabit Ethernet - Packet Scheduler Miniport
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.2      20
      192.168.1.0    255.255.255.0      192.168.1.2     192.168.1.2      20
Default Gateway:     192.168.1.254
// se omite el resultado //
===========================================================================
```

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

5.3.5.1 Red de destino

La red de destino puede estar representada por un rango de direcciones de hosts o por una dirección de red y una dirección de host.
El enrutador selecciona la ruta más específica.
Conforme a la tabla, para llegar a las redes 10.1.1.0 y 10.1.2.0 se escoge la ruta 192.168.2.2
Si un enrutador va a enviar el tráfico hacia el host 10.1.1.55, escoge las siguientes rutas siguiendo un orden de prioridad.

- 10.1.1.0
- 10.1.0.0
- 10.0.0.0
- 0.0.0.0
- Descartado en caso que no exista una ruta hacia dicho destino.

Entradas de ruta en una tabla de enrutamiento

```
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C   192.168.2.0/24 is directly connected, FastEthernet0/0
```

La tabla de enrutamiento muestra las redes de destino.

Los paquetes con direcciones host de destino en uno de los rangos de red mostrados se harán coincidir con el próximo salto que conduce a dicha red.

5.3.5.2 Red de destino

Ruta predeterminada

Un enrutador puede ser configurado para que use una ruta predeterminada.
Una ruta predeterminada es una ruta que coincide con todas las redes de destino.
En IPv4 se usa la ruta predeterminada 0.0.0.0
La ruta predeterminada 0.0.0.0 se utiliza para el envío de todos los paquetes cuyas direcciones no están registrados en la tabla de enrutamiento del enrutador.
El enrutador envía el paquete hacia una dirección del siguiente salto especificada en el enrutador.

La tabla de enrutamiento muestra la ruta predeterminada 0.0.0.0.

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C     192.168.2.0/24 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```

Los paquetes con las direcciones hosts de destino que no se encuentren en los rangos de la red mostrados se reenviarán al gateway como último recurso.

5.3.6 Siguiente salto: envío del paquete

El siguiente salto es la red que continuara con el procesamiento del paquete en su recorrido hacia el host de destino.
Los host de una red tienen al enrutador gateway o gateway predeterminado como el siguiente salto para el enrutamiento del tráfico hacia otras redes.
En la tabla de enrutamiento de un enrutador, cada ruta enumera una dirección del siguiente salto para llegar a la dirección de destino.
A medida que cada paquete llega, la dirección de destino del paquete es comparada con la tabla de enrutamiento.
Cuando se determina una coincidencia entre la dirección de destino del paquete y el contenido de la tabla, se procede al envío del paquete hacia el siguiente salto.
El enrutador envía el paquete hacia la interfaz del siguiente enrutador contiguo con el cual está conectado.
El enrutador del siguiente salto es el gateway para los enrutadores con los cuales está conectado.
Las redes conectadas a los enrutadores no tienen dirección del siguiente salto porque no manejan direcciones IP,
El enrutador puede enviar paquetes directamente por el gateway hacia el dispositivo de destino a través de la interfaz de red con la cual tiene conexión el host de destino.
Algunas rutas pueden tener múltiples saltos para llegar a la red de destino. Algunas de esas rutas son alternativas para el envío o recepción. Esto implica que existen numerosos pasos para llegar a la misma red de destino.

Resultado de la tabla de enrutamiento con los siguientes saltos

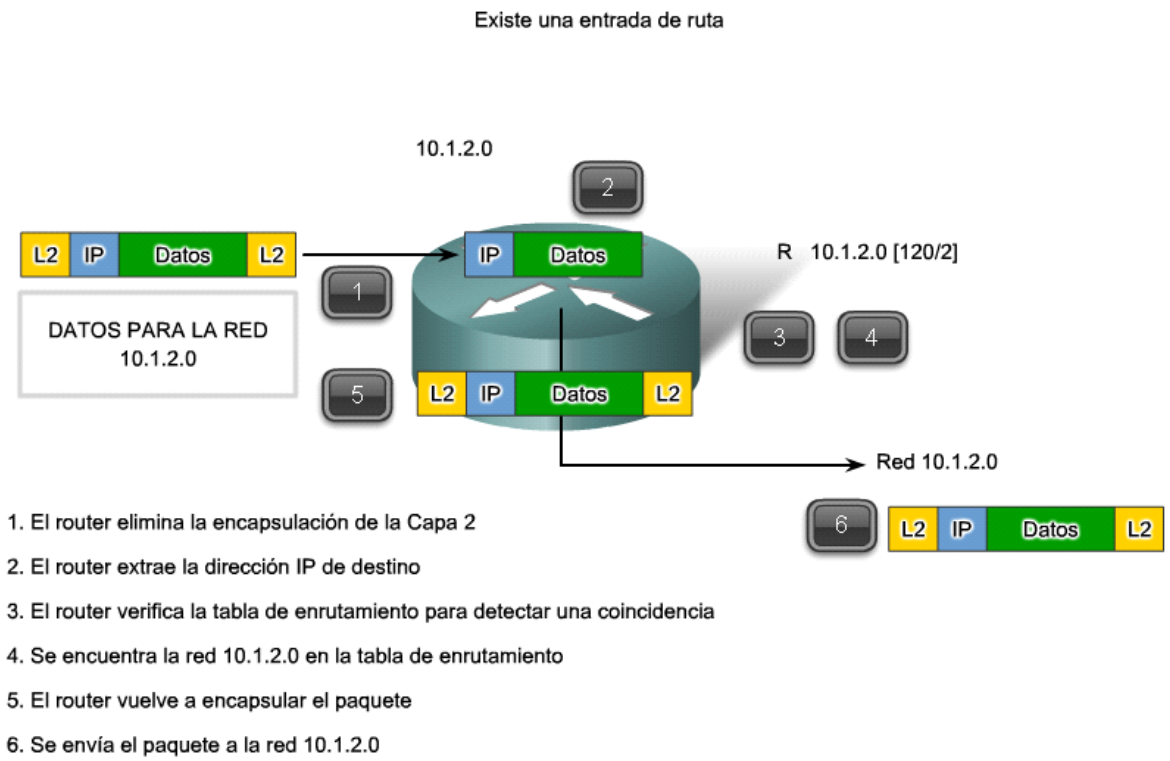
```
  10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

5.3.7.1 Envío de paquetes: traslado del paquete hacia su destino

El enrutamiento se hace salto por salto y paquete por paquete
El enrutador verifica la dirección IP de destino de cada paquete y verifica su tabla de enrutamiento antes del re-envío del paquete.
El enrutador hará una de las siguientes actividades con el paquete:

- Re-enviarlo al enrutador del siguiente salto.
- Re-enviarlo al host de destino.
- Descartarlo.

Examen del paquete
El enrutador examina los paquetes en la capa de red.
Los paquetes que llegan al enrutador están encapsulados como PDU de la capa de Enlace de Datos.
El enrutador descarta la PDU de la capa de Enlace de Datos y analiza el contenido de la capa de red.
Selección del siguiente salto
El enrutador analiza la dirección de destino del paquete entrante.
Si la dirección de destino coincide con una ruta hacia una red local conectada al mismo enrutador, el paquete es encapsulado con una cabecera de la capa de Enlace de Datos para su transmisión y es re-enviado al host de destino a través de la interfaz local del enrutador.
Si la dirección de destino coincide con una ruta hacia una red remota, el enrutador encapsula el paquete con una cabecera de la capa de Enlace de Datos para su transmisión hacia la dirección del siguiente salto.



5.3.7.2 Envío de paquetes

Uso de la ruta predeterminada

Si la tabla del enrutador no contiene una entrada para un paquete recibido, el paquete debe ser enviado por la interfaz del enrutador que especifique la ruta predeterminada y conecte con la dirección del siguiente salto.

Esta ruta predeterminada es denominado gateway de último recurso.

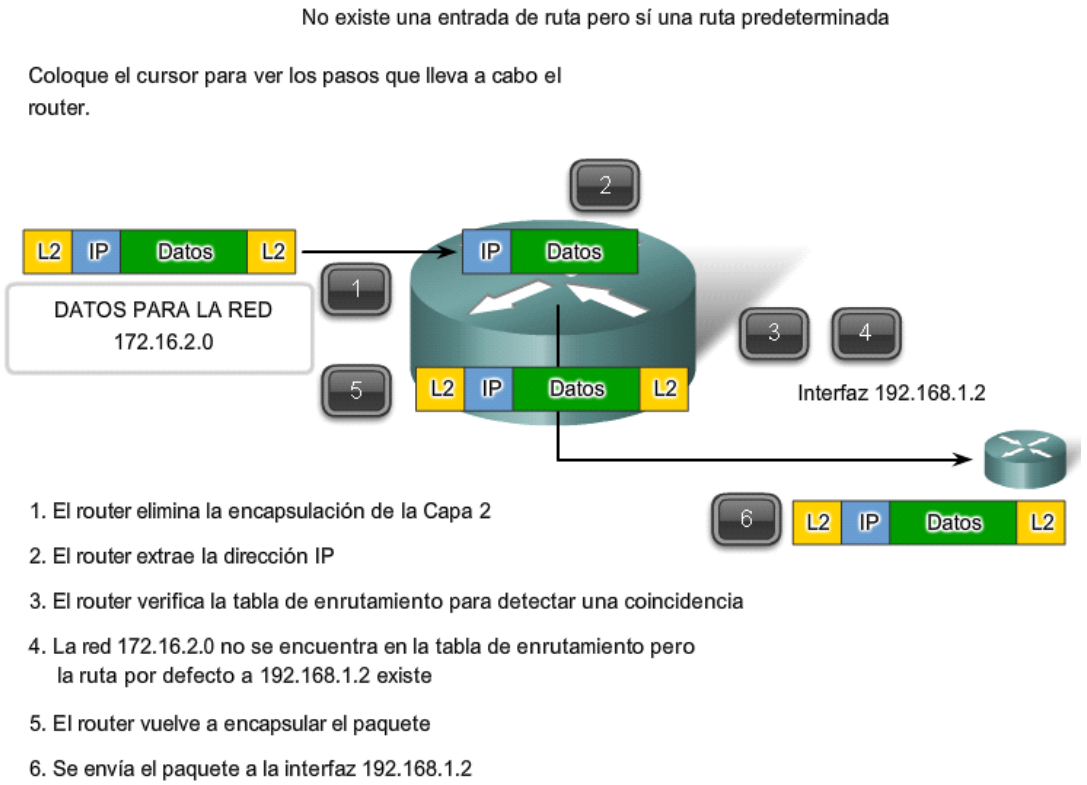
Este proceso puede repetirse varias veces, en varios enrutadores, hasta que el paquete llegue a la red de destino.

El enrutador en cada salto conoce solamente la dirección del siguiente salto. El enrutador no conoce los detalles de la ruta hacia el host de destino remoto.

No todos los paquetes que van al mismo host de destino van a seguir la misma ruta predeterminada en cada siguiente salto. Los enrutadores pueden aprender nuevas rutas mientras se lleva a cabo la comunicación y luego re-envían los paquetes hacia diferentes siguientes saltos.

Las rutas predeterminadas son importantes porque no siempre los enrutadores tienen entradas de rutas hacia cada red posible en Internet. Si el paquete es enviado hacia una ruta predeterminada, eventualmente podría llegar a un enrutador que tiene en su tabla la red de destino coincidente con la dirección IP del paquete.

En este caso en enrutador puede enviar el paquete hacia la interfaz donde está conectado el host de destino o continuar con la ruta del siguiente salto hacia una dirección más específica.

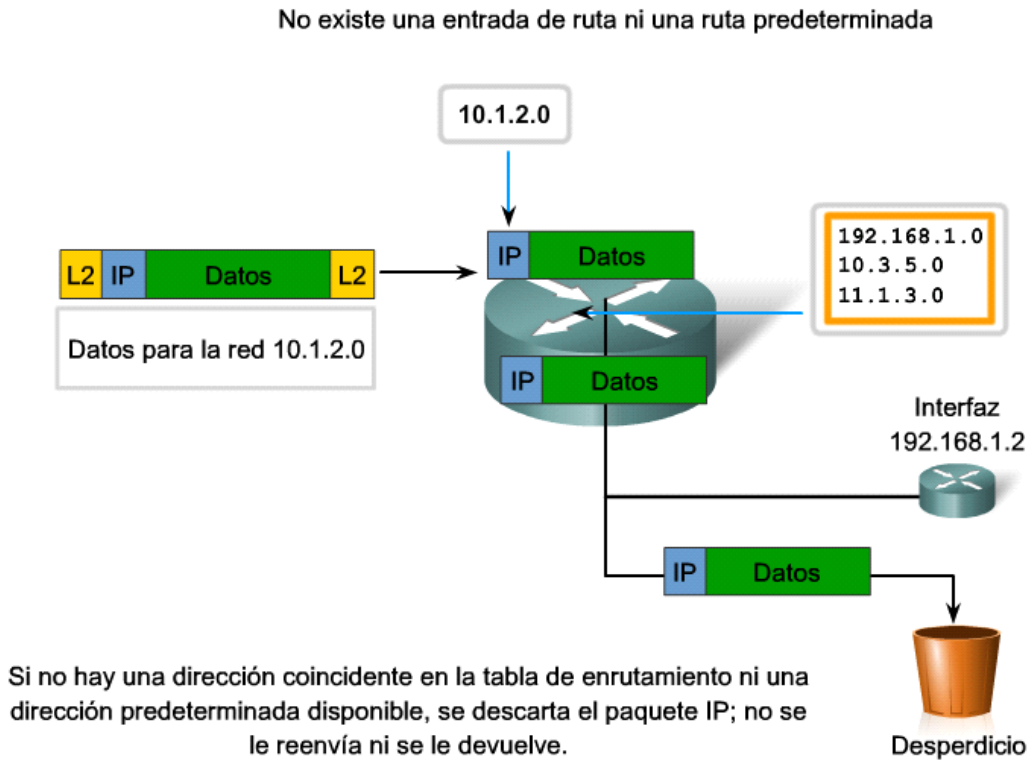


5.3.7.3 Envío de paquetes

Traslado del paquete hacia su destino

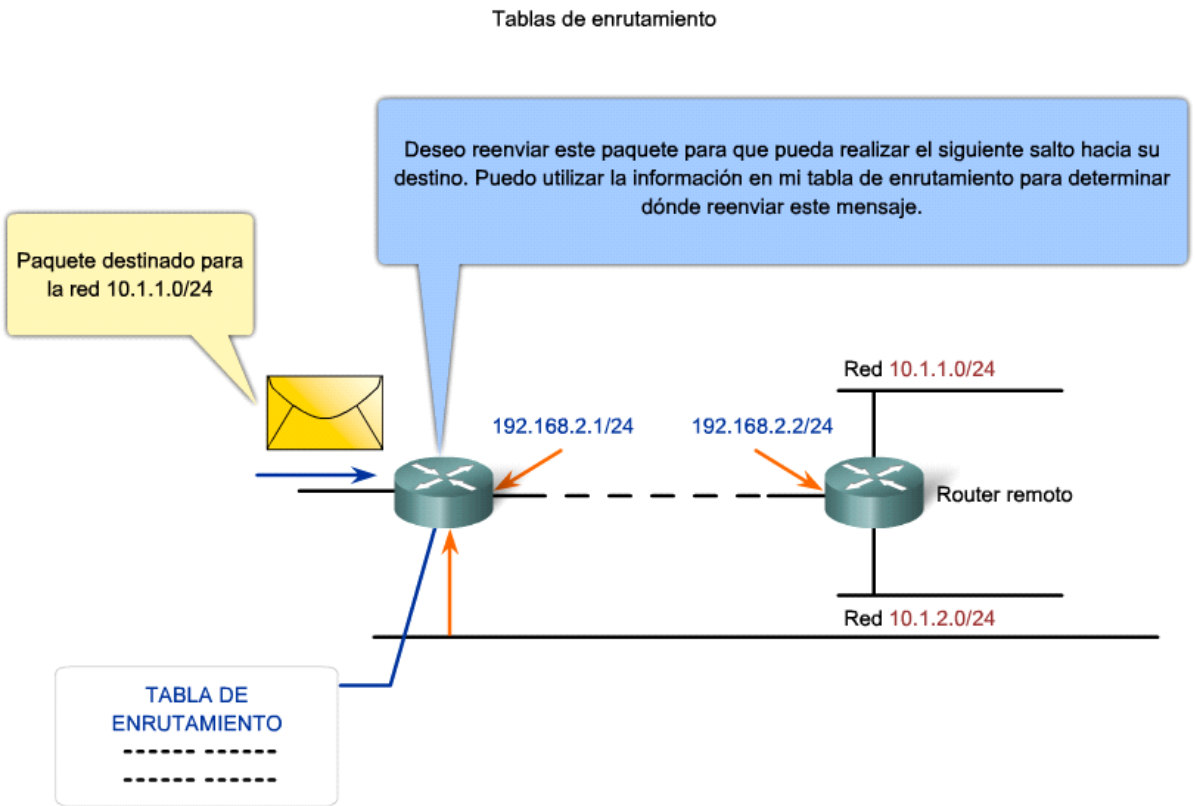
A medida que el paquete avanza por la inter-red, todos los enrutadores necesitan una tabla de enrutamiento para el re-envío del paquete. Si la tabla de algún enrutador no contiene una ruta de destino ni tampoco una ruta predeterminada, ese paquete se descarta.

Este paquete descartado no se retransmite ni se le devuelve al originador, para evitar la congestión de la red. El protocolo IP funciona sin conexión, no realiza el control de los paquetes transmitidos. Dependiendo del tipo de protocolo, las capas superiores podrían iniciar el procedimiento de recuperación de la información.



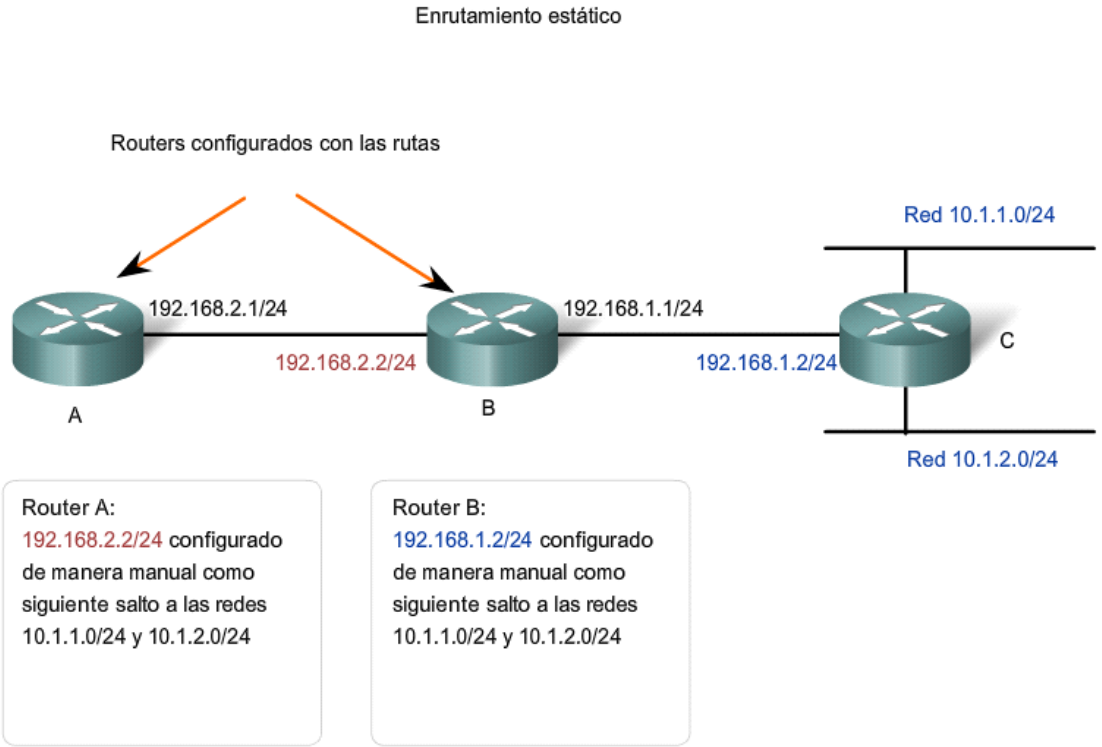
5.4.1 Protocolo de enrutamiento

El enrutamiento requiere que para cada paquete que llega a un enrutador exista una ruta específica y determinada hacia otro enrutador hasta que el paquete llegue a su destino correspondiente.
De otra manera, el paquete es descartado en ese enrutador. Se debe establecer una ruta predeterminada.
Cada enrutador necesita conocer la dirección del enrutador que contiene la dirección del siguiente salto. Un enrutador no necesita conocer las direcciones de todos los hosts ni enrutadores existentes en Internet.
La tabla de enrutamiento contiene información que el enrutador usa en sus decisiones para el re-envío de los paquetes. Para las decisiones de enrutamiento, la tabla de enrutamiento debe representar el estado más preciso de rutas de red a las que el enrutador puede acceder.
La información de enrutamiento desactualizada podría ocasionar que los paquetes sean re-enviados hacia las direcciones de siguiente salto no adecuadas, lo cual ocasionaría un retardo, extravío o descarte de un paquete.
La información de la ruta puede ser configurada manualmente o configurada dinámicamente por medio del intercambio de información de un enrutador con sus vecinos a través de los protocolos de enrutamiento.
Después que sean configurados las interfaces de un enrutador y estas sean operativas, se instala en la red asociada con cada interface en la tabla de enrutamiento como una red conectada directamente.



5.4.2 Enrutamiento estático

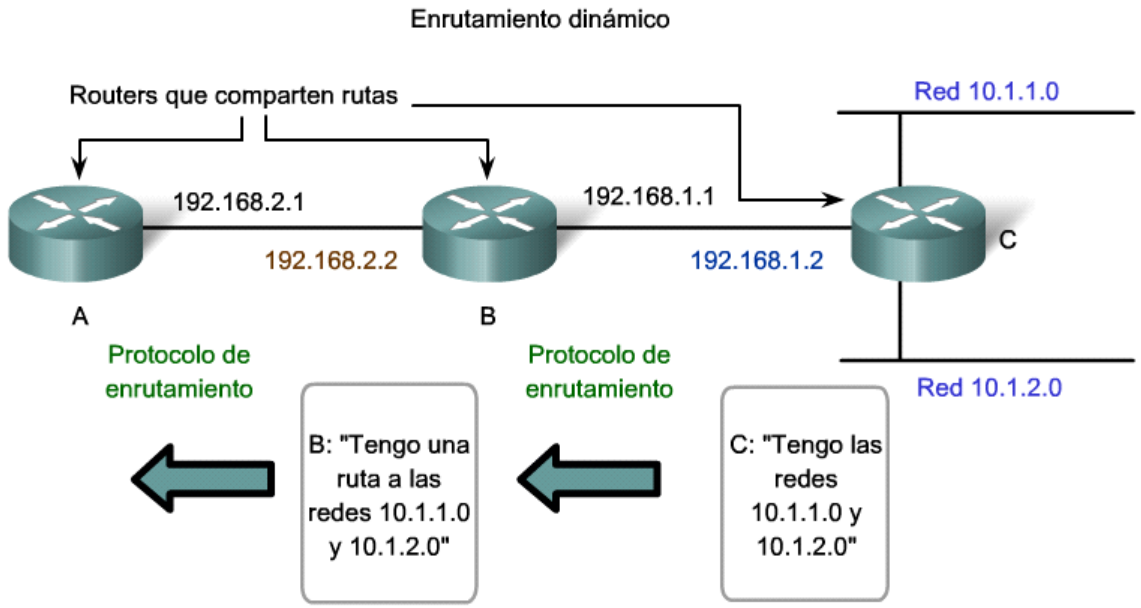
Las rutas hacia las redes remotas pueden ser configuradas manualmente. Esto se conoce como enrutamiento estático.
Una ruta predeterminada también puede ser configurada estáticamente.
Si un enrutador está conectado a otros enrutadores, se requiere el conocimiento de la estructura de inter-red. Los paquetes deben estar enrutados para utilizar las mejores direcciones de siguiente salto y deben de tener una ruta predeterminada configurada.
Cada enrutador debe estar configurado estáticamente con las direcciones de los enrutadores correspondientes a los siguientes saltos que reflejen su ubicación en la red.
Si la estructura de la inter-red cambia o si se conectan nuevas redes, estos cambios deben ser actualizados estáticamente.
Si no se realiza una actualización periódicamente y con la debida prontitud, el enrutamiento del paquete podría estar desactualizado, lo cual ocasionaría el retardo o la pérdida de los paquetes en su recorrido hacia el host de destino.



5.4.3.1 Enrutamiento dinámico

No siempre es factible el mantenimiento y la actualización permanente de las tablas de enrutamiento de los enrutadores por medio de la configuración estática manual.
Los protocolos de enrutamiento dinámico permiten que los enrutadores compartan sus tablas de enrutamiento dinámicamente.
En la configuración y funcionamiento de los enrutadores se registran los cambios que se presentan en la conexión de las interfaces con nuevas redes como también con nuevos enlaces con otros enrutadores.
Los enrutadores intercambian información de enrutamiento con otros enrutadores y actualizan sus tablas de enrutamiento inclusive para el tráfico que debe recorrer numerosas redes para llegar a su destino.
Entre los protocolos de enrutamiento se tiene

- Protocolo de información de enrutamiento RIP.
- Protocolo de enrutamiento de gateway interno mejorado EIGRP.
- Open shortest path first OSPF.



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).

5.4.3.2 Enrutamiento dinámico

El enrutamiento dinámico proporciona la actualización permanente de las tablas.
Los inconvenientes del enrutamiento dinámico son:

- Ocupación del ancho de banda de la red por el intercambio de tráfico entre los enrutadores de la red.
- Se necesita alta capacidad de procesamiento y memoria en los enrutadores para la implementación oportuna de los protocolos EIGRP y OSPF.
- La actualización permanente de las tablas de enrutamiento.

Los inconvenientes del enrutamiento estático son:

- Falta de actualización permanente de las rutas para el tráfico.
- Necesidad de realizar el trabajo manualmente.

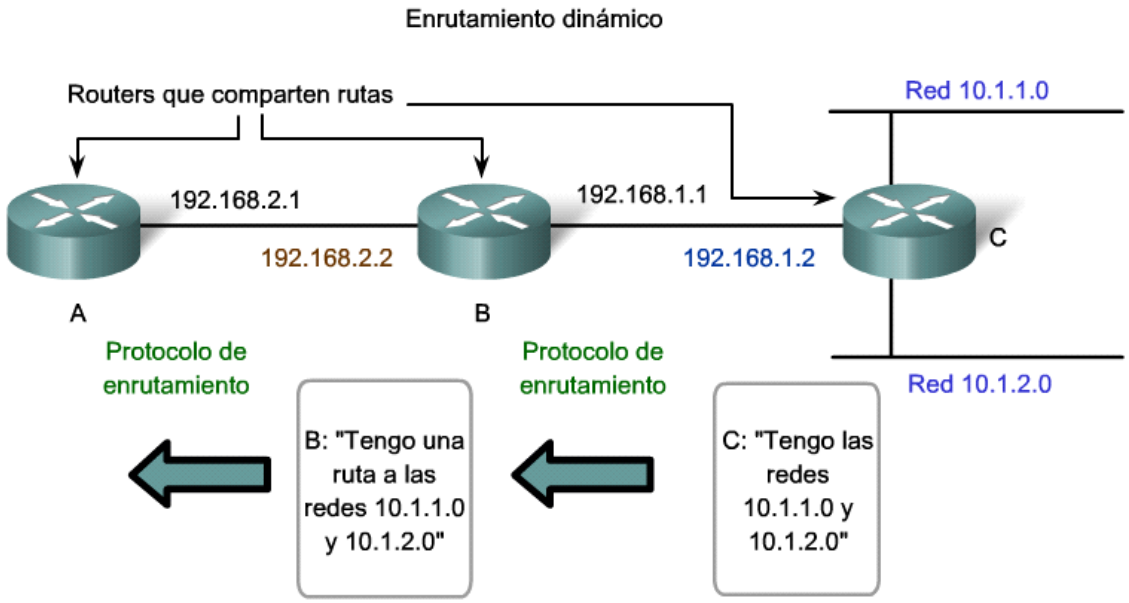
Las ventajas del enrutamiento dinámico son:

- Actualización permanente y oportuna de las tablas de enrutamiento.

Las ventajas del enrutamiento estático son:

- No presenta sobrecarga a la red.
- No se requiere alta capacidad de memoria en los enrutadores.

En muchas redes se utiliza de forma combinada el enrutamiento estático, dinámico y predeterminado.



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).