

Fundamentos de la Arquitectura TCP/IP

Ing. Gilberto Sánchez Quintanilla

Introducción

- La familia de protocolos: **Protocolo de Control de Transmisión/Protocolo de Internet** (TCP/IP - *Transmission Control Protocol/Internet Protocol*), llevan su nombre por los dos principales protocolos. **TCP** en capa de **transporte** e **IP** en capa de **red**.
- Es la base de la Internet actual, así como la base de muchas redes privadas de computadoras.

Origen e historia reciente de Internet

- Internet **comenzó a finales de los sesenta** como un experimento de la Agencia de Proyectos de Investigación Avanzada – **ARPA**.
- DARPA experimentó con la conexión de redes de computadoras, concediendo becas a múltiples universidades y compañías privadas que se involucraran en la investigación.

Origen e historia reciente de Internet

- 1969, nace una red experimental con la conexión de cuatro nodos a través de circuitos de 56 Kbps.
- La nueva tecnología resultó ser altamente exitosa y condujo a la creación de dos redes militares similares: MILNET, en los Estados Unidos, y MINET, en Europa
- Posteriormente miles de servidores y usuarios conectaron sus redes privadas (las universidades y el gobierno) a ARPANET, creando de esta forma la inicial "ARPA Internet".

Origen e historia reciente de Internet

- Hacia 1985, ARPANET era altamente utilizada y estaba cargada de atascos.
- En 1986, la NSFNET creo una arquitectura de red mas distribuida, los enlaces originales de 56 Kbps se actualizaron en 1988 a enlaces T1 mas rápidos (1.544 Mbps).
- Hacia 1991, el trafico de datos se había incrementado enormemente, lo que hizo necesario actualizar el servicio de red del *backbone* de la NSFNET a enlaces T3 (45 Mbps).

Origen e historia reciente de Internet

- A principios de los años noventa, la NSFNET todavía estaba reservada para aplicaciones de investigación y educación.
- Intereses comerciales y de propósito general clamaban por el acceso a la red, y los proveedores de servicio de Internet (ISP) emergían para dar cabida a dichos intereses.

Origen e historia reciente de Internet

- A finales de 1970 empezó a ver la luz lo que ahora conocemos como TCP/IP.
- Un conjunto de RFCs (791, 793, 768, etc.) definen el núcleo de la familia de protocolos TCP/IP.
- Quizá el mayor empujón a la adopción de TCP/IP fue la publicación en 1983 de la versión BSD 4.2 de UNIX, que incorporaba TCP/IP.

Origen e historia reciente de Internet

- Con la versión BSD 4.2 muchas universidades podían permitirse minicomputadoras adicionales y el software que ejecutaba en ellas. El resultado fue un crecimiento explosivo en el uso de ARPANET y el desarrollo de muchas herramientas y utilidades que ahora podemos conseguir gratuitamente.

Arquitectura de la familia de protocolos TCP/IP

- La pila de protocolos TCP/IP tiene una arquitectura con propiedades distintas a la del modelo OSI.
- La arquitectura es la siguiente:

Modelo OSI		Arquitectura TCP/IP
Aplicación		Aplicación
Presentación		
Sesión		
Transporte		Transporte
Red		Internet
Enlace		Interfaz de red
Física		

Arquitectura TCP/IP

- La familia de protocolos TCP/IP eligieron un modelo más simple con menos niveles para mejorar el rendimiento y facilitar la implantación.
- Este modelo conocido como DARPA, es mas simple que el modelo de ISO, constando sólo de cuatro niveles.

Arquitectura TCP/IP

■ Protocolos de la Arquitectura TCP/IP

FTP	DNS	Aplicación
Telnet	DHCP	
SMTP	SNMP	
HTTP	TFTP	
TCP	UDP	Transporte
IGMP	ICMP	
IP		Red
ARP RARP		
Interfaz de red		NIC

Arquitectura TCP/IP

■ Algunas diferencias con el modelo OSI son:

- ♦ *No hay definición en cuanto a la capa física y de enlace, pues en principio TCP/IP se diseñó para funcionar sobre las facilidades de transmisión existentes; es decir, puede funcionar sobre IEEE 802.3, 802.5, Ethernet, etc*

Aplicación	Aplicación			
Transporte	TCP		UDP	
Red	Internet Protocol			
NIC	Ethernet	Token Ring	FDDI

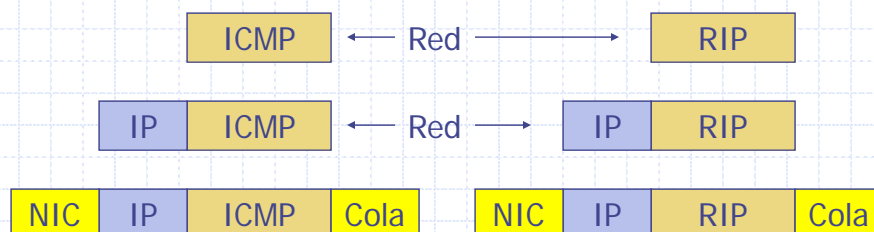
Arquitectura TCP/IP

- Una capa tiene mas de un protocolo.

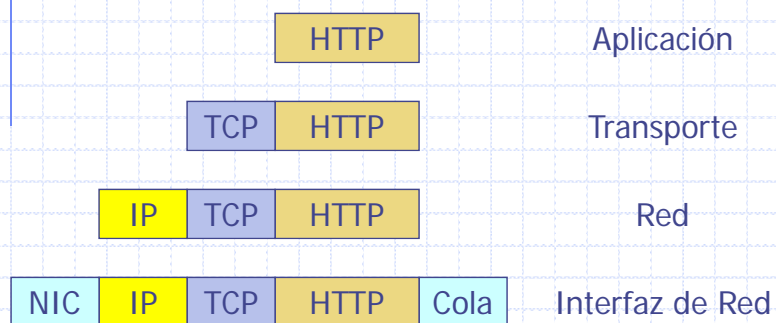
FTP	DNS	Aplicación
Telnet	DHCP	
SMTP	SNMP	
HTTP	TFTP	
TCP	UDP	Transporte
IGMP	ICMP	
IP		Red
ARP	RARP	
Interfaz de red		NIC

Arquitectura TCP/IP

- ♦ Se sigue un orden jerárquico, que permite a los protocolos utilizar los servicios de otro protocolo siempre y cuando se encuentren en la misma capa o en la capa inferior (no necesariamente la inmediata inferior).



Arquitectura TCP/IP



Arquitectura TCP/IP

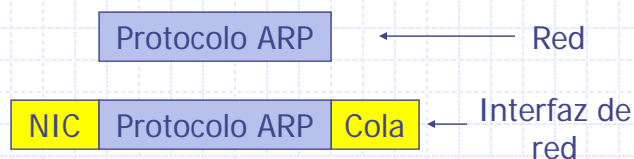
- Se basa en el protocolo IP, en un servicio no orientado a conexión (transmisión de datagramas).
- Datagrama: **La decisión de enrutamiento se realiza para cada paquete; por lo que cada paquete de una misma transmisión puede seguir trayectorias distintas. Por lo tanto puede llegar fuera de secuencia o repetidos**

Protocolo ARP

- Protocolo de Resolución de Direcciones por sus siglas en ingles ARP (*Address Resolution Protocol*) .
- ARP es el protocolo utilizado por tecnologías de red de acceso compartido basadas en difusión (broadcast), como Ethernet y Token Ring.

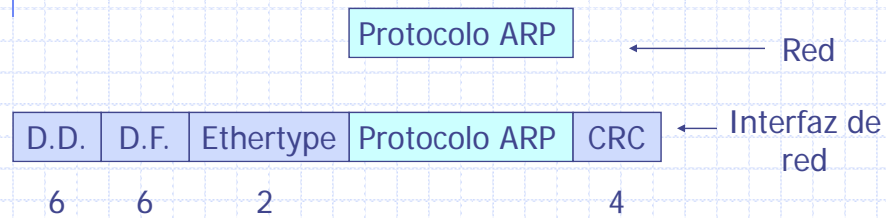
Protocolo ARP

- ARP es un protocolo de capa de red, el cual utiliza los servicios de la capa de Interfaz de red.



Protocolo ARP

- En el caso de la red Ethernet como protocolo de Interfaz de Red, identifica al protocolo ARP con el Ethertype 0x0806



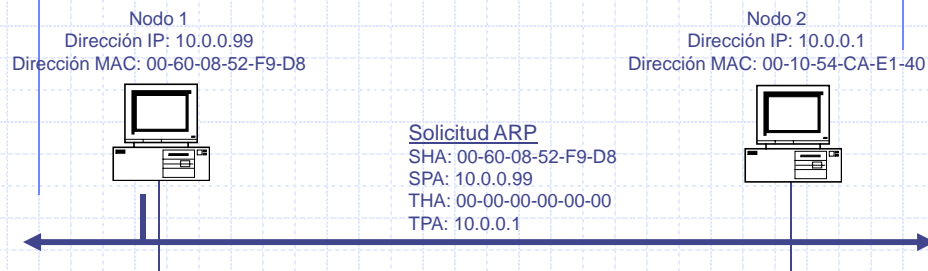
Protocolo ARP

- Este protocolo se utiliza para resolver la dirección física (dirección MAC) del siguiente nodo en base a su correspondiente dirección lógica (dirección IP).
- Esto lo realiza enviando un mensaje de broadcast (la dirección destino de la trama será FF:FF:FF:FF:FF:FF).

Protocolo ARP

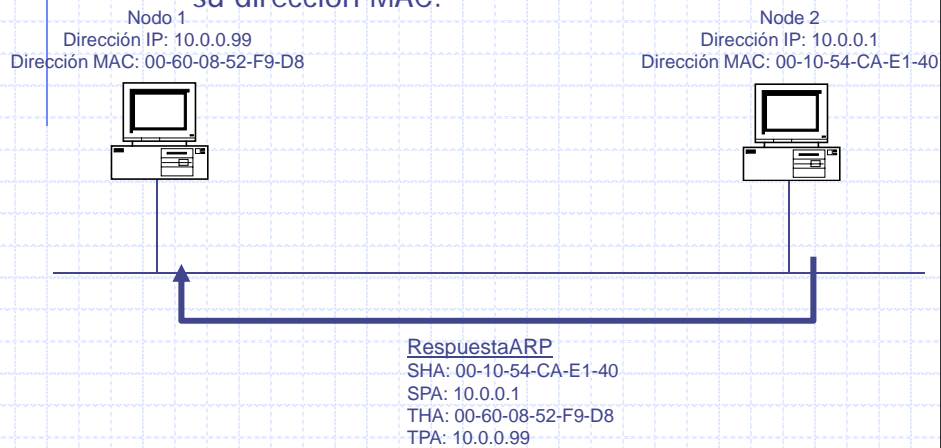
- El mensaje que envía la terminal origen se le llama: solicitud de ARP.
- Este mensaje es enviado preguntando:
 - ◆ ¿Quién tiene la dirección IP 10.0.0.1? y ¿Cuál es su dirección MAC?
- Este mensaje lo reciben todas las terminales dentro de la red de broadcast, pero solo contesta la terminal que tiene esa dirección IP.

Protocolo ARP

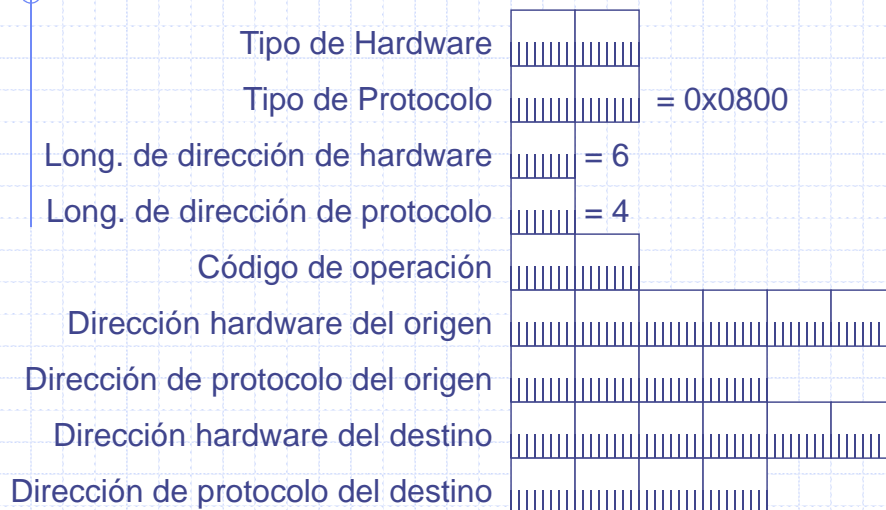


Protocolo ARP

- El mensaje que envía la terminal destino es llamado, respuesta de ARP. Y es donde envía su dirección MAC.



Mensaje de ARP



Protocolo ARP

- **Tipo de Hardware:** Campo de 2 bytes que indica el tipo de hardware que esta presente en la capa de Interfaz de red.

Valor del Tipo de hardware	Tecnología de la capa de Interfaz de red
1 (0x0001)	Ethernet (10 Mbps)
6 (0x0006)	Redes IEEE 802.3 Token Ring
15 (0x000F)	Frame Relay
16 (0x0010)	ATM

Protocolo ARP

- **Tipo de Protocolo:** Campo de 2 bytes que indica el tipo de protocolo que es utilizado para realizar el transporte de los datos.
- Es el protocolo al cual ARP le presta el servicio de resolución de direcciones.
- Para la resolución de direcciones ARP, el campo Tipo de Protocolo se configura con 0x0800.

Protocolo ARP

- **Longitud de Direcciones de Hardware:** Campo de 1 bytes que indica el tamaño de las direcciones de hardware de capa de Interfaz de red. Para Ethernet el valor es de 6 (0x06).
- **Longitud de Direcciones de protocolo:** Campo de 1 bytes que indica el tamaño de las direcciones de protocolo. Para IP (Internet Protocol) el valor es de 4 (0x04).

Protocolo ARP

- **Código de operación (opcode):** Campo de 2 bytes que indica el tipo de trama ARP. La tabla muestra los valores más utilizados de Operación ARP

Valor de Operación	Tipo de trama ARP
1 (0x0001)	Solicitud ARP
2 (0x0002)	Respuesta ARP
8 (0x0008)	Solicitud ARP inversa
9 (0x0009)	Respuesta ARP inversa

Protocolo ARP

Solicitud ARP

de la terminal 192.168.0.1 a la terminal 192.168.0.2

```
0000  ff ff ff ff ff ff 00 19  d1 ac 20 21 08 06 00 01  ..... !....
0010  08 00 06 04 00 01 00 19  d1 ac 20 21 c0 a8 00 01  ..... !....
0020  00 00 00 00 00 00 c0 a8  00 02  ..... ..
```

Respuesta ARP

de la terminal 192.168.0.2 a la terminal 192.168.0.1

```
0000  00 19 d1 ac 20 21 00 19  d1 ac 1f ca 08 06 00 01  .... !.. .....
0010  08 00 06 04 00 02 00 19  d1 ac 1f ca c0 a8 00 02  ..... .....
0020  00 19 d1 ac 20 21 c0 a8  00 01 00 00 00 00 00 00  .... !.. .....
0030  00 00 00 00 00 00 00 00  00 00 00 00  ..... ..
```

Protocolo ARP

Solicitud ARP

de la terminal a la terminal

```
0000  ff ff ff ff ff ff 08 00  46 43 44 f6 08 06 00 01  ..... FCD.....
0010  08 00 06 04 00 01 08 00  46 43 44 f6 94 cc b7 bd  ..... FCD.....
0020  00 00 00 00 00 00 94 cc  b7 fe  ..... ..
```

Respuesta ARP

de la terminal a la terminal

```
0000  08 00 46 43 44 f6 00 01  f4 43 c9 19 08 06 00 01  ..FCD... .C.....
0010  08 00 06 04 00 02 00 01  f4 43 c9 19 94 cc b7 fe  ..... .C.....
0020  08 00 46 43 44 f6 94 cc  b7 bd 00 00 00 00 00 00  ..FCD... .....
0030  00 00 00 00 00 00 00 00  00 00 00 00  ..... ..
```

Protocolo ARP

ARP gratuito y detección de IP duplicada

- ARP también se utiliza para proporcionar detección de IP duplicada mediante la transmisión de solicitudes ARP, conocida como **ARP gratuito**.
- Un ARP gratuito es una solicitud ARP para la propia dirección IP del nodo.

ARP Gratuito

- En el ARP gratuito, SPA y TPA están configurados con la misma dirección IP.
- Si un nodo envía una solicitud ARP para su propia dirección IP y no se recibe ninguna trama de respuesta ARP, el nodo determina que otros nodos no utilizan su dirección IP asignada.
- Si un nodo envía una solicitud ARP para su propia dirección IP y se recibe una trama de respuesta ARP, el nodo determina que otro nodo está utilizando su dirección IP asignada.

ARP Gratuito

Detección de conflictos de direcciones IP

- En un conflicto de direcciones IP, el nodo que se ha configurado correctamente con la dirección IP se conoce como *nodo defensor*.
- El nodo que envía el ARP gratuito (al encender) se conoce como *nodo infractor*.

ARP Gratuito

- Solicitud ARP (ARP gratuito), enviada por la terminal infractora que enciende. La dirección IP está en conflicto.

0000	ff ff ff ff ff ff 00 60	97 02 6e 8f 08 06 00 01`..n.....
0010	08 00 06 04 00 01 00 60	97 02 6e 8f a9 fe 00 01`..n.....
0020	00 00 00 00 00 00 a9 fe	00 01 01 01 01 01 01 01
0030	01 01 01 01 01 01 01 01	01 01 01 01

ARP Gratuito

- Respuesta de ARP de la terminal defensora a la terminal infractora. Cuando la terminal infractora recibe la respuesta, no toma la dirección IP.

0000	00 60 97 02 6e 8f 00 60 97 02 6d 3d 08 06 00 01	.`...n...` ..m=....
0010	08 00 06 04 00 02 00 60 97 02 6d 3d a9 fe 00 01` ..m=....
0020	00 60 97 02 6e 8f a9 fe 00 01	.`...n... ..

ARP Gratuito

- La terminal defensora envía un ARP gratuito, para informarle a todas las terminales que a ella le pertenece la IP.

0000	ff ff ff ff ff ff 00 60 97 02 6d 3d 08 06 00 01` ..m=....
0010	08 00 06 04 00 01 00 60 97 02 6d 3d a9 fe 00 01` ..m=....
0020	00 00 00 00 00 00 a9 fe 00 01 01 01 d8 00 00 00
0030	24 01 00 00 5e 01 00 00 48 00 00 00	\$...^... H...

Ruteo de Paquetes

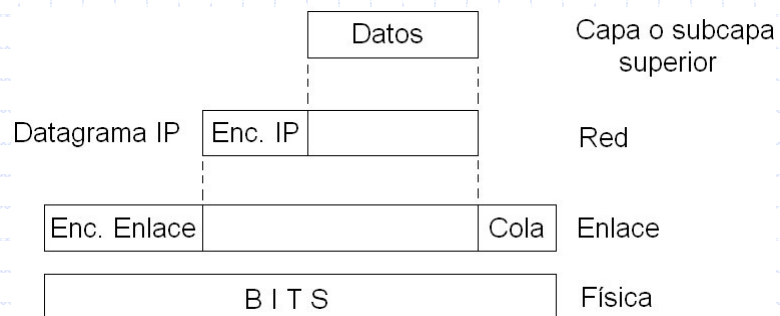
- La función mas importante de la capa de red es la de **conducir los paquetes de datos de la fuente al destino**.
- Esta función la designaremos con el nombre de **ruteo** y el dispositivo que la realiza es el **ruteador**.

Ruteo de Paquetes

- Así el **ruteo es el proceso de descubrir, seleccionar y emplear la mejor trayectoria o camino** para transmitir un paquete de datos de un nodo (ruteador) a otro nodo en una red.

Ruteo de Paquetes

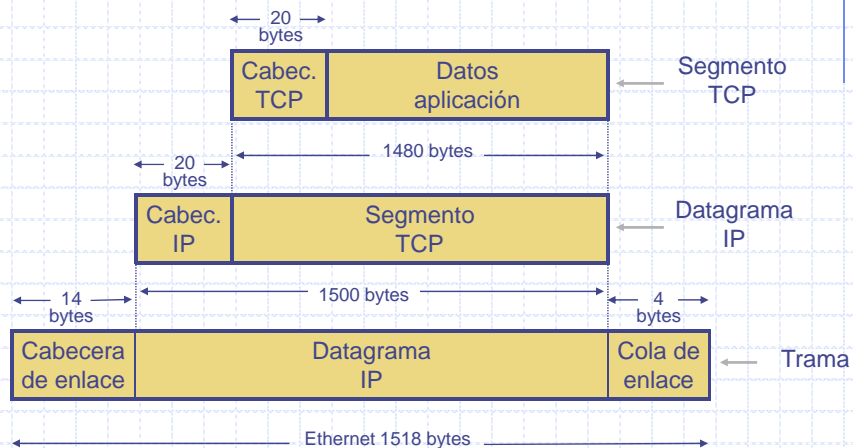
- En la red Internet un paquete es llamado datagrama IP (Internet Protocol) y tiene el siguiente formato general:



Ruteo de Paquetes

- El **encabezado IP** contiene información que controla hacia **donde y como es enviado el paquete**. El tamaño del datagrama IP es determinado por la aplicación que envía los datos y puede ser tan grande como 64 Kbytes (65,536 bytes) incluido el encabezado IP.

Ruteo de Paquetes



Ruteo de Paquetes

- Para ir de la fuente al destino, un datagrama IP sigue una trayectoria formada por una secuencia de ruteadores (hops o nodos). Hay dos métodos para llegar de la fuente al destino:
 - ♦ **Source Route**
 - ♦ **Conducción de Ruteador por Ruteador**

Ruteo de Paquetes

■ Source Route

- ♦ En este método la fuente pone en el encabezado del paquete la lista de hops (ruteadores) por los cuales pasara el mensaje.
No se utiliza actualmente.

Ruteo de Paquetes

■ Conducción de Ruteador por Ruteador

- ♦ La conducción del datagrama de la fuente al destino, se hace escogiendo en cada ruteador de la trayectoria el siguiente hop (ruteador) al cual será enviado el datagrama. En este método no es necesario que la fuente tenga toda la información acerca de cómo ir a un destino, basta con que sepa cómo ir al siguiente nodo en la ruta al destino. Este ruteador a su vez sabe a cuál ruteador remitir en seguida el paquete para hacerlo llegar a su destino.

Ruteo de Paquetes

- Con el método de conducción de ruteador por ruteador, cada uno de estos dispositivos a lo largo de la trayectoria recibe el datagrama, examinan la dirección IP destino y usan la dirección para determinar el siguiente ruteador al cual enviar el datagrama, para hacerlo llegar a su destino.
- Para realizar estas tarea los ruteadores conservan información en una tabla llamada de ruteo.

Ruteo de Paquetes

- Ejemplo: En la siguiente figura se muestran subredes (redes independientes), las cuales están conectadas con ruteadores. Cada uno de los ruteadores tiene una tabla de ruteo que incluye las direcciones de subred, para saber a que nodo (ruteador) siguiente transmitir los paquetes.

Ruteo de Paquetes

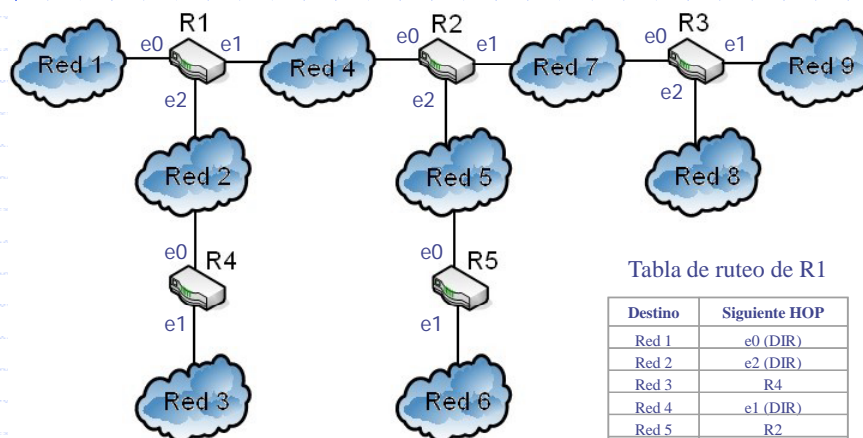


Tabla de ruteo de R1

Destino	Siguiente HOP
Red 1	e0 (DIR)
Red 2	e2 (DIR)
Red 3	R4
Red 4	e1 (DIR)
Red 5	R2
Red 6	R2
Red 7	R2
Red 8	R2
Red 9	R2

Ruteo de Paquetes

- Como observación, cabe mencionar que al inicio los ruteadores únicamente conocen las subredes (direcciones de subred) que tienen conectadas en sus interfaces; con estos datos informan a los ruteadores adyacentes lo que conocen, y ellos son informados de lo que conocen los otros ruteadores. Al conjuntar esta información recibida, los ruteadores crean sus tablas de ruteo.

Ruteo de Paquetes

- Ejercicio: Encuentre la tabla de ruteo de los ruteadores R1, R2, R3, R4 y R5.
 - ◆ Inicialice las tablas de ruteo con las direcciones de red (subred) que conoce, y posteriormente intercambie la información con los nodos adyacentes.

Direccionamiento IP

- Para administrar correctamente y solucionar problemas entre redes IP, es importante comprender todos los aspectos del direccionamiento IP.
- Uno de los aspectos más importantes de las redes TCP/IP es la asignación de direcciones IP únicas y correctas a todos los nodos de una red IP.

Direccionamiento IP

◆ Tipos de direcciones IP

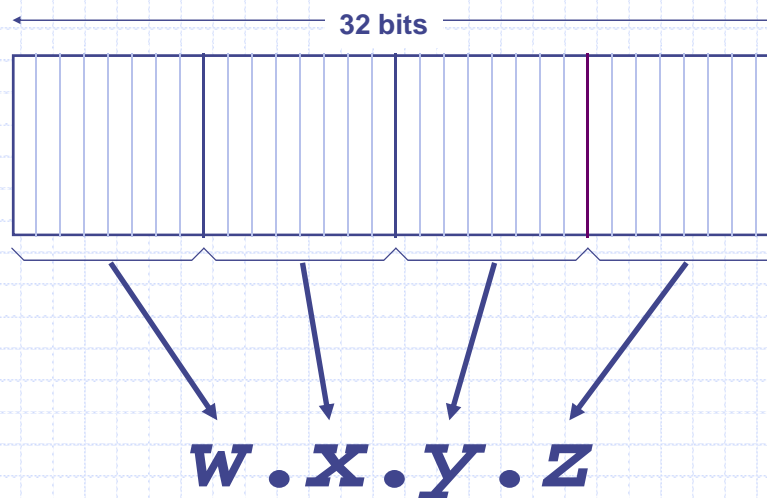
- **Unidifusión:** Se asigna a una única interfaz de red conectada a una red IP. Son utilizadas en comunicación de uno a uno.
- **Difusión:** Esta diseñada para ser procesada por todos los nodos IP del mismo segmento de red. Se utilizan en comunicaciones de uno a muchos.

Direccionamiento IP

- **Multidifusión:** Es una dirección en la que uno o varios nodos pueden escuchar en el mismo o en diferente segmento de red. Se utilizan en comunicaciones de uno a varios.

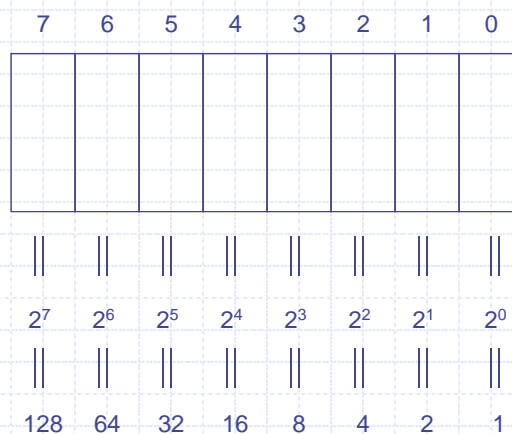
Direccionamiento IP

◆ Expresión de las direcciones IP



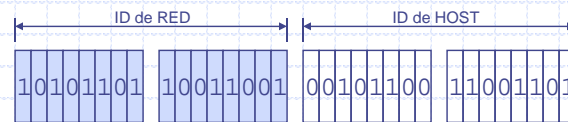
Direccionamiento IP

◆ Número de 8 bits



Direccionamiento IP

◆ Estructura de una dirección IP de unicast



Direccionamiento IP

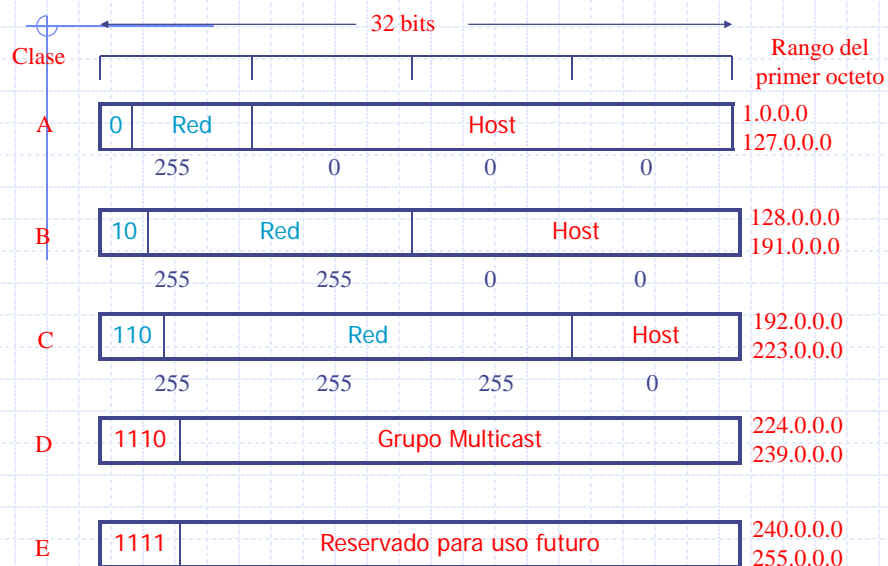
◆ Clases de direcciones IP

- Actualmente el direccionamiento de Internet no incluye clases.
- Sin embargo, las clases de direcciones de Internet son un elemento importante para comprender el direccionamiento IP.

Direccionamiento IP

- RFC 791 definió la dirección IP de unidifusión en términos de clases de direcciones para crear redes bien definidas de diversos tamaños.
- Objetivo:
 - ♦ Un pequeño número de grandes redes (redes con una gran cantidad de nodos).
 - ♦ Un número moderado de redes de tamaño mediano.
 - ♦ Un número de pequeñas redes.

Formato de direcciones IP



Direccionamiento IP

◆ Reglas de enumeración de ID de RED

- El ID de red no puede empezar con 127 en el primer octeto.
 - ◆ Las direcciones 127.x.y.z están reservadas como direcciones de bucle invertido.
- Todos los bits del ID de red no pueden ser configurados como 1.
 - ◆ Todos los ID de red definidos como 1 están reservados para direcciones de difusión.

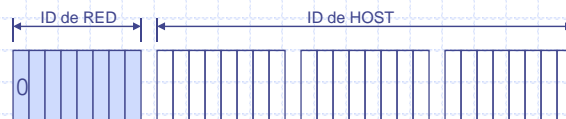
Direccionamiento IP

◆ Reglas de enumeración de ID de RED

- Todos los bits del ID de red no pueden ser configurados como 0.
 - ◆ Todos los ID de red definidos como 0 están reservados para indicar un host en la red local.
- El ID de red debe ser único en la red local.

Direccionamiento IP

◆ Direcciones de clase A

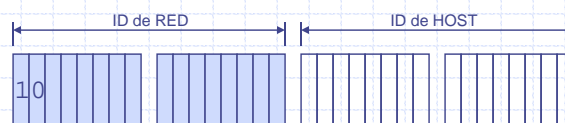


Clase de Dirección	Primer ID de RED	Ultimo ID de RED	Número de IDs de RED
Class A	1.0.0.0	126.0.0.0	126

Nota: Las direcciones 127.x.y.z están reservadas para direcciones de bucle invertido (de local host).

Direccionamiento IP

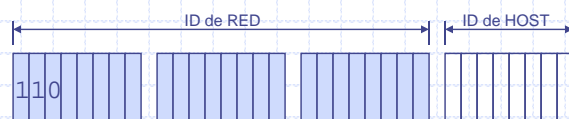
◆ Direcciones de clase B



Clase de Dirección	Primer ID de RED	Ultimo ID de RED	Número de IDs de RED
Class B	128.0.0.0	191.255.0.0	16,384

Direccionamiento IP

◆ Direcciones de clase C



Clase de Dirección	Primer ID de RED	Ultimo ID de RED	Número de IDs de RED
Class C	192.0.0.0	223.255.255.0	2,097,152

Direccionamiento IP

◆ Reglas de enumeración de ID de HOST

- Todos los bits del ID de host no se pueden configurar como 1.
 - ◆ Todos los ID de host configurados como 1 están reservados para direcciones de difusión.
- Todos los bits del ID de host no se pueden configurar como 0.
 - ◆ Todos los ID de host configurados como 0 están reservados para expresar ID de dirección IP.
- Los ID deben ser únicos en la red.

Direccionamiento IP

Intervalos de clases de direcciones de
ID de host

Clase de dirección	Primer ID de host	Ultimo ID de host	Número de host
Clase A	w.0.0.1	w.255.255.254	16,777,214
Clase B	w.x.0.1	w.x.255.254	65,534
Clase C	w.x.y.1	w.x.y.254	254

Direccionamiento IP

◆ Subredes y máscaras de subred

- En una dirección IP de red, los bits de red son fijos y los bits de host son variables.
- Originalmente, los bits de host se diseñaron para indicar ID de host en un dirección IP de red.
- Sucesivamente, los bits de host se utilizan para expresar una combinación de direcciones IP de subred e ID de host de subred, mejorando el uso de los bits de host.

Direccionamiento IP

- Las **subredes** están diseñadas para que sea más eficaz el uso de un espacio de direcciones fijo, principalmente una dirección IP de red.
 - ♦ Imagine una red de clase B con 65,534 host.
 - ♦ Es técnica posible, aunque no es práctico por su acumulación de tráfico de difusión.
- Para redes de menor tamaño y utilizar mejor los bits de host, una dirección IP de red puede ser dividida en subredes (**subconjunto de la red original basada en clases**).

Direccionamiento IP

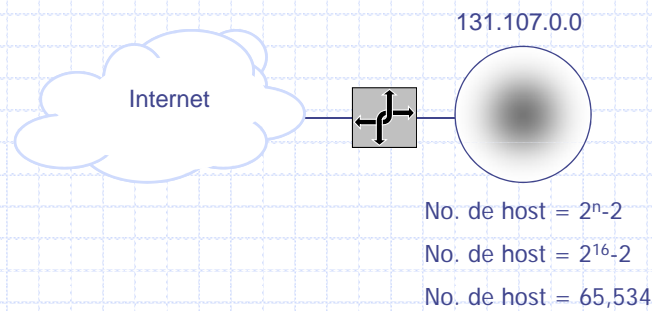
Como dividir una red en subredes

- Considere una dirección IP de clase B:
 - ♦ 131.107.0.0

$\underbrace{\hspace{1.5cm}}_{\text{RED}} \underbrace{\hspace{1.5cm}}_{\text{HOST}}$
- Los bytes 131 y 107 son fijos. Los otros dos bytes son de host (65,534 host)
- Los 16 bits de host se pueden dividir para crear subredes.

Direccionamiento IP

- ◆ Un ID de red de clase B antes de crear subredes

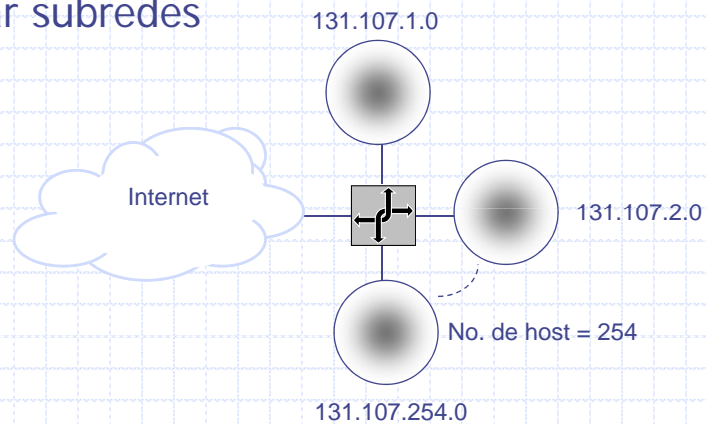


Direccionamiento IP

- Tenemos 16 bits de host, de los cuales se pueden tomar ***n bits*** para crear subredes:
 - ◆ ***No. de subredes = $2^n - 2$***
 - ◆ Donde n es el número de bits tomados de host para crear subredes.
- Suponiendo que de los 16 bits de host, se toman 8 para crear subredes y quedan 8 para host, entonces tenemos:
 - ◆ No. de subredes = $2^8 - 2 = 254$
 - ◆ No. de host = $2^8 - 2 = 254$ (en cada subred)

Direccionamiento IP

- ◆ Un ID de red de clase B después de crear subredes



Direccionamiento IP

Mascara de subred

- Para que un host o un enrutador conozca la dirección IP de red o la dirección IP de subred, requiere una configuración adicional para distinguir entre los bits de red o subred y los bits de host, de una dirección IP de host.
- Se define el uso de una máscara de bits para poder diferenciar esto.
- A esta máscara se le conoce como máscara de subred.

Máscara de subred

◆ Valor de 32-bit

- "1" indica que los bits son usados para el ID de RED
- "0" indica que los bits son usados para el ID de HOST

◆ Expresado en bits y en notación decimal

Clase de Dirección	Mascara de RED				Notación Decimal
Class A	11111111	00000000	00000000	00000000	255.0.0.0
Class B	11111111	11111111	00000000	00000000	255.255.0.0
Class C	11111111	11111111	11111111	00000000	255.255.255.0

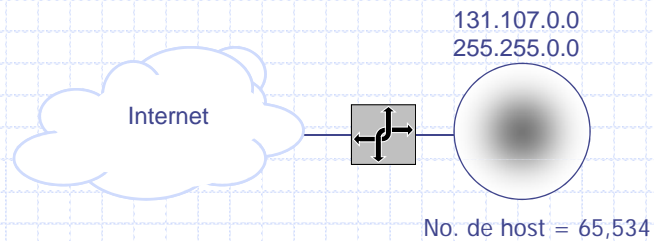
Máscara de subred

- Notación de prefijo de red para máscaras de subred predeterminadas.

Clase de dirección	Mascara de RED				Longitud del prefijo de RED
Clase A	11111111	00000000	00000000	00000000	/8
Clase B	11111111	11111111	00000000	00000000	/16
Clase C	11111111	11111111	11111111	00000000	/24

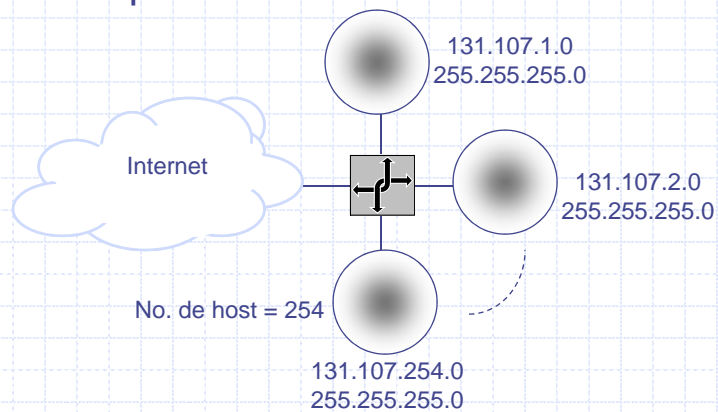
Máscara de subred

- ◆ Un ID de red de clase B y la máscara de red antes de crear subredes



Máscara de subred

- ◆ Un ID de red de clase B y la máscara de subred después de crear subredes.



Máscara de subred

- Los ID de red o subred expresados correctamente, deben ser de la siguiente forma:
 - ◆ 192.168.45.0, 255.255.255.0 o 192.168.45.0/24
 - ◆ 10.99.0.0, 255.255.0.0 o 10.99.0.0/16

Máscara de subred

- Todos los host de la misma red lógica deben utilizar los mismos bits de ID de red o subred, y la misma máscara de subred.
- Ejemplo: ¿cuáles son las direcciones IP de host de 131.107.0.0/16 y 131.107.0.0/24?

Mascara de subred

- Se le asigna la dirección de red 190.10.0.0 y su jefe le dice que cree el máximo de subredes que tengan 100 host como máximo. ¿Cuántas subredes se crean?, ¿Cuántos host por subred?, ¿Cuál es la máscara de subred?, indique el rango de subredes e indique el rango de los host en la subred 200.

Máscara de subred

- 190.10.0.0/20 MS: 255.255.11110000.00000000
 - ◆ 190.10.00010000.00000000 - 190.10.11100000.00000000
- 190.10.0.0/21 MS: 255.255.11111000.00000000
 - ◆ 190.10.00001000.00000000 - 190.10.11110000.00000000
- 190.10.0.0/22 MS: 255.255.11111100.00000000
 - ◆ 190.10.00000100.00000000 - 190.10.11111000.00000000
- 190.10.0.0/23 MS: 255.255.11111110.00000000
 - ◆ 190.10.00000010.00000000 - 190.10.11111100.00000000
- 190.10.0.0/24 MS: 255.255.11111111.00000000
 - ◆ 190.10.00000001.00000000 - 190.10.11111110.00000000

Máscara de subred

- El uso de la máscara de subred es el siguiente:
 - ♦ Determinación del ID de red o subred, utilizando la máscara de subred.
 - ♦ Se realiza una operación AND (Y) bit a bit entre la Dirección IP de host y la máscara de subred.

Bit A	Bit B	Salida
0	0	0
0	1	0
1	0	0
1	1	1

Máscara de subred

Determinación del ID de red o subred

Dirección IP	10000011	01101011	10100100	00011010
Máscara desubred	11111111	11111111	11110000	00000000

Resultado	10000011	01101011	10100000	00000000
-----------	----------	----------	----------	----------

131.107.164.26 AND 255.255.240.0 = 131.107.160.0

Máscara de subred

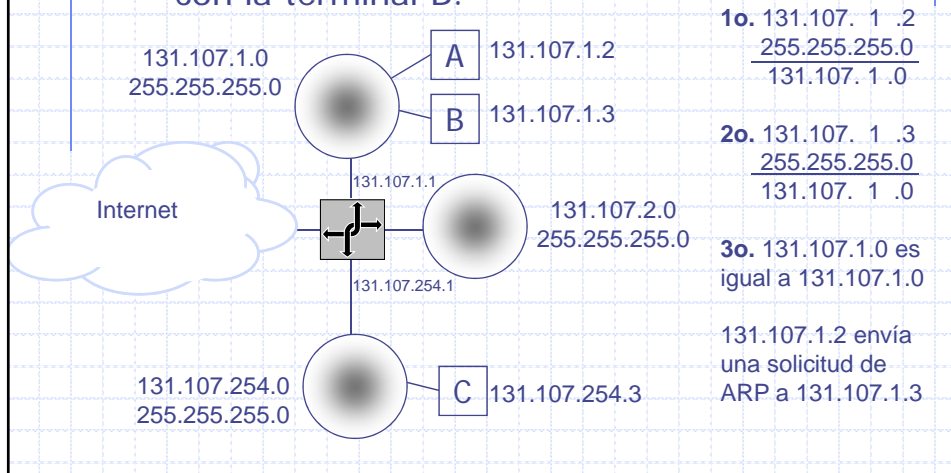
- Uso de la máscara de subred en el host:
 - ♦ El host origen utiliza su máscara de subred junto con las direcciones IP origen y destino, para determinar si el host destino esta en la misma subred o en diferente subred.
 - ♦ Primero: IP origen **AND** M. Subred = Subred A
 - ♦ Segundo: IP destino **AND** M. Subred = Subred B

Máscara de subred

- Tercero: Comparar Subred A con Subred B.
 - ♦ Si el valor de **Subred A es igual a Subred B**, el destino esta en la **misma subred**, entonces el host origen le envía una solicitud ARP al host de destino, y le envía el mensaje.
 - ♦ Si el valor de **Subred A es diferente al de la Subred B**, el destino esta en una **subred diferente**, entonces el host origen le envía una solicitud ARP a la puerta de enlace, al cual le envía el mensaje.

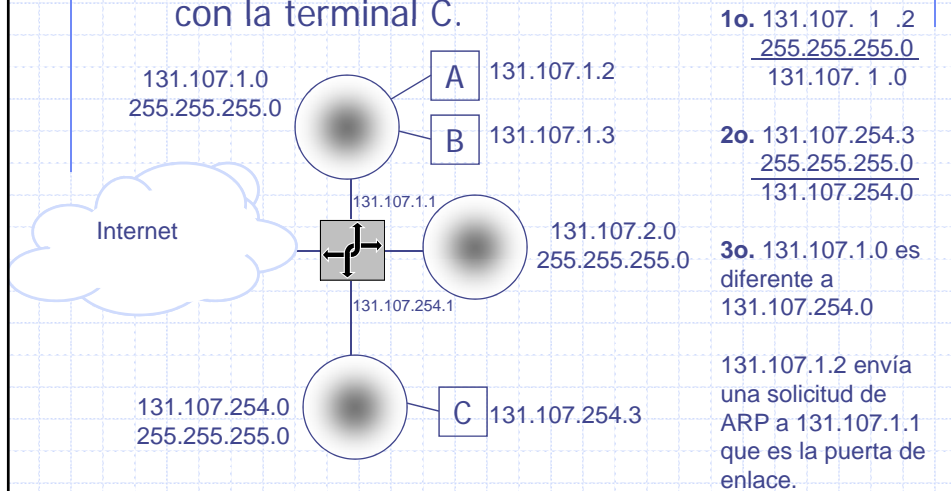
Máscara de subred

- Ejemplo: La terminal A desea comunicarse con la terminal B.



Máscara de subred

- Ejemplo: La terminal A desea comunicarse con la terminal C.



Máscara de subred

■ Ejercicio. Realice lo siguiente:

- ♦ Configure su terminal con los siguientes parametros: dirección IP (192.168.0.X), máscara de subred (255.255.255.0) y puerta de enlace (192.168.0.1).
- ♦ Ejecute el analizador de protocolos (wireshark), capturando con su interfaz de red (eth0) y filtrando con su MAC (ether host 00:20:18:66:c6:02).
- ♦ Capture y ejecute el comando `c:\>ping 192.168.0.Y`, analice las tramas ARP capturadas y concluya.
- ♦ Capture y ejecute el comando `c:\>ping 192.168.254.3`, analice las tramas ARP capturadas y concluya.

Máscara de subred

■ Uso de la máscara de subred en el ruteador.

- ♦ Como sabemos un ruteador tiene una tabla llamada de ruteo, la cual le ayuda a decidir hacia que nodo adyacente enviar el paquete.

Destino	Siguiente HOP	Mascara de ruteo	Tipo
131.107.1.0	131.107.1.254	255.255.255.0	DIR
131.107.2.0	131.107.1.1	255.255.255.0	REM
131.107.254.0	131.107.1.1	255.255.255.0	REM

Máscara de subred

- ♦ Cuando un ruteador recibe un paquete IP, este analiza la dirección IP destino y aplica una operación **AND** con la máscara de subred de la primera línea de la tabla de ruteo, obtiene una dirección de subred y la compara con el destino.
- ♦ Si no es igual se pasa a la siguiente línea hasta que la subred sea igual al destino.
- ♦ Si es igual la subred al destino, el paquete es enviado al siguiente HOP.

Máscara de subred

- ♦ Supongamos que el la IP destino es 131.107.2.3

Destino	Siguiente HOP	Mascara de ruteo	Tipo
131.107.1.0	131.107.1.254	255.255.255.0	DIR
131.107.2.0	131.107.1.1	255.255.255.0	REM
131.107.254.0	131.107.1.1	255.255.255.0	REM

$$\begin{array}{r}
 131.107.2.3 \\
 255.255.255.0 \\
 \hline
 131.107.2.0
 \end{array}$$

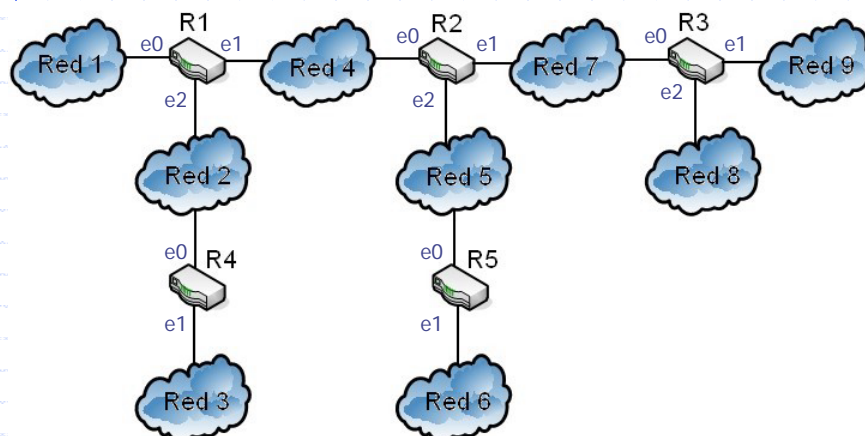
¿Es igual al destino? No
Se pasa a la siguiente línea

$$\begin{array}{r}
 131.107.2.3 \\
 255.255.255.0 \\
 \hline
 131.107.2.0
 \end{array}$$

¿Es igual al destino? Si
Entonces, envía el paquete al siguiente HOP.

Máscara de subred

- Utilice la dirección 192.1.1.0/28



Direccionamiento IP

Subredes de longitud variable

- Como se pudo observar, se puede dividir una red en subredes del mismo tamaño.
- Para maximizar el uso del espacio de direcciones fijo, las subredes que se crearon pueden ser utilizadas para crear otras subredes. Esto se conoce como subred de longitud variable.
- Se debe tener cuidado de que cada subred sea única, y con su máscara de subred, pueda distinguirse de otras subredes.

Direccionamiento IP

- Ejemplo de subred de longitud variable:
 - ♦ Se tiene 131.107.0.0/16
 - ♦ Se realiza la división en subredes de 3 bits.
 - ♦ La mitad de las direcciones están reservadas para su uso posterior.
 - ♦ Tres subredes se asignan con un máximo de 8190 direcciones IP.
 - ♦ 29 subredes se asignan con un máximo de 254 direcciones IP.
 - ♦ 62 subredes se asignan, únicamente con 2 direcciones IP.

Direccionamiento IP

Direcciones Privadas

- Cuando Internet empezó a crecer de forma exponencial, la demanda de direcciones IP publicas aumento considerablemente.
- Dado que cada nodo de la red corporativa de una organización requería una dirección IP publica, las organizaciones solicitaban suficientes direcciones IP.

Direccionamiento IP

- Las autoridades de Internet descubrieron que la mayoría de las organizaciones requerían muy pocas direcciones públicas.
- Los únicos host que requerían direcciones públicas eran los servidores WEB, FTP, e-mail, proxy y de seguridad.
- Los host de la red corporativa (interna) de la organización no requieren acceso directo a Internet, pero debían utilizar un espacio válido de direcciones IP.

Direccionamiento IP

- Direcciones de Intranet
- Los tres bloques de direcciones siguientes definen el espacio de direcciones privado:
 - ♦ 10.0.0.0/8 – La red privada de 24 bits de host, puede utilizar cualquier esquema de subredes en la organización privada.
 - ♦ 172.16.0.0/12 – Espacio de 20 bits de host. Desde la perspectiva de clases, el ID de red privada 172.16.0.0/12 es el intervalo de 14 redes de clase B de 172.17.0.0/16 a 173.30.0.0/16.

Direccionamiento IP

- 192.168.0.0/16 – Espacio de direcciones con 16 bits de host . Desde una perspectiva con clase, el ID de red privada 192.168.0.0/16 es el intervalo de 254 ID de red de clase C de 192.168.1.0/24 a 192.168.254.0/24.