



# **MODULO I:**

## **Protocolos de**

### **Capa Internet: IPv4**

# Objetivos



- Repaso de Protocolo IPv4
- Protocolo DHCP
- Network Address Translation (NAT)
- Protocolo ICMP
- Multidifusión ("Multicasting")

# Internet Protocol (IP): RFC 791



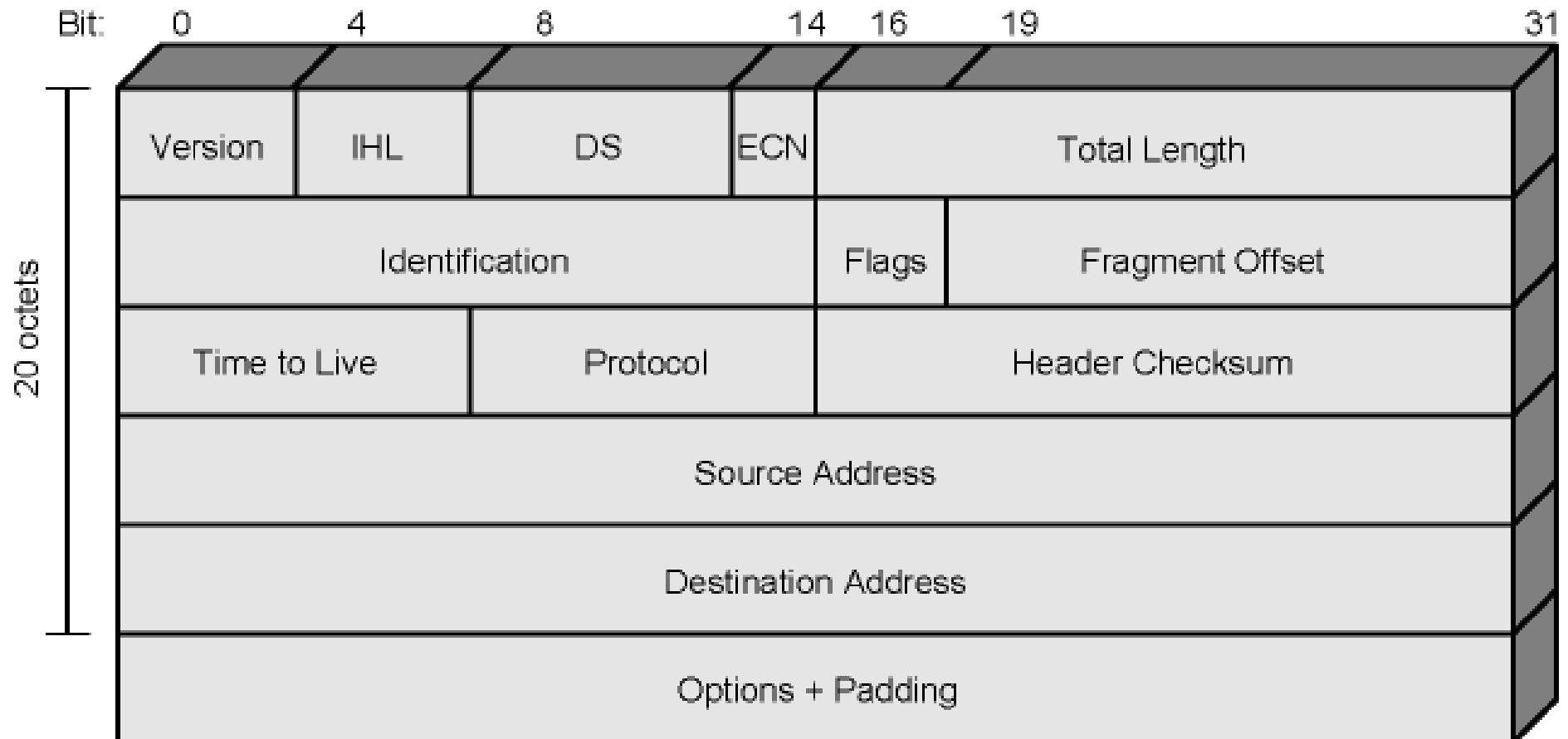
- Función principal de IP:
  - Direcccionar y rutear paquetes
- Protocolo no orientado a conexión ("Connectionless")
  - No se establece una conexión entre el nodo origen y destino antes de enviar un paquete de datos
  - Uso de datagramas independientes
- Protocolo No-Confiable ("Unreliable")
  - No detecta datagramas dañados y/o perdidos
  - No detecta datagramas fuera de secuencia
  - No se utiliza ningún tipo de ACK
- La Confiabilidad es Responsabilidad de Protocolos y Aplicaciones de niveles superiores.
- IP Fragmenta y Reensambla Paquetes

# Principios de Diseño



- Ruteo
- Tiempo de Vida del Datagrama
- Fragmentación y reensamblaje
- Control de Error
- Control de Flujo
- Direcccionamiento

# Encabezado del Datagrama IPv4



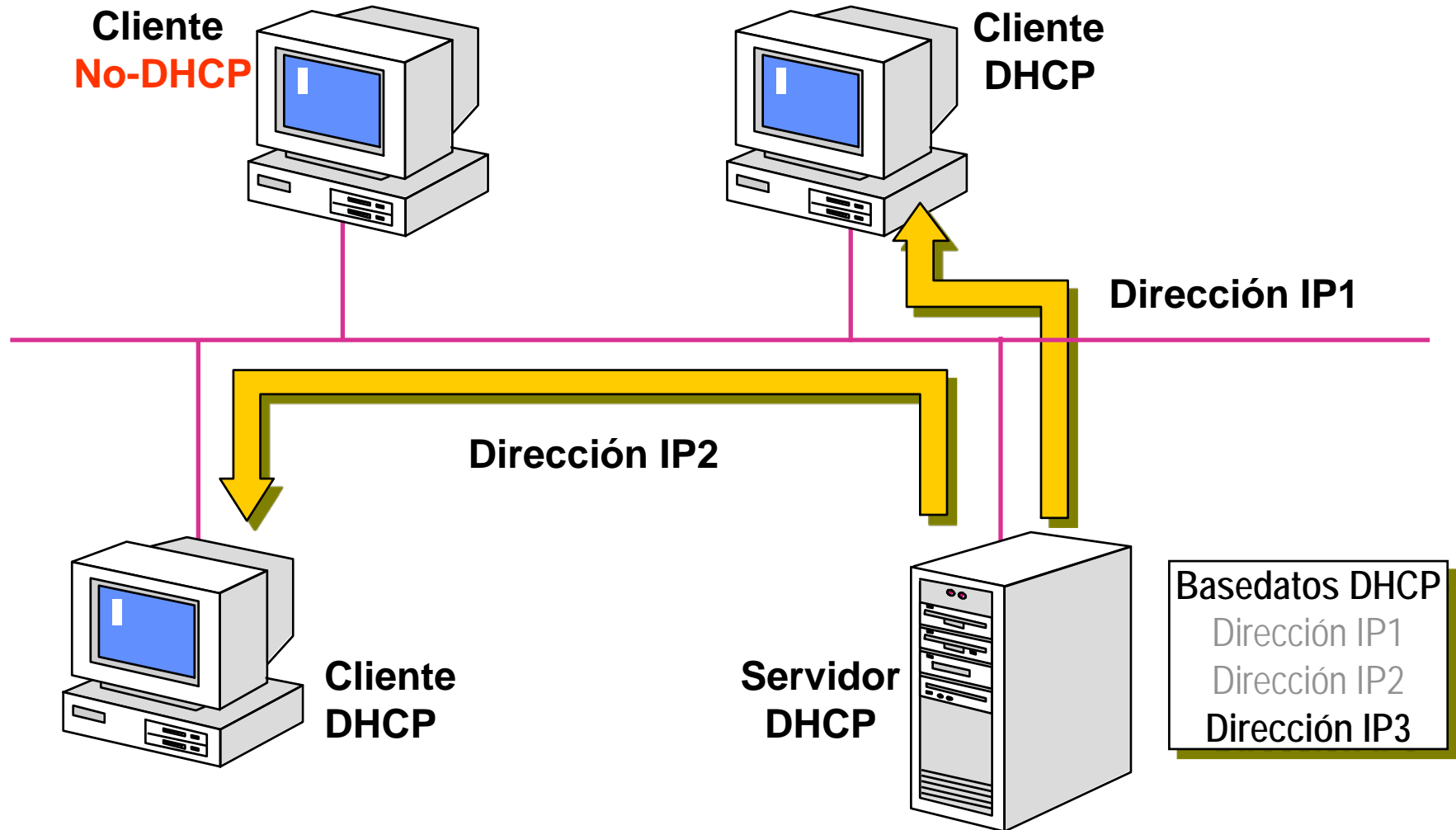
# Configuración de IP Manual vs. Automatica

- Configuración de TCP/IP Manual. Inconvenientes:
  - En caso de errores, dificulta la detección del origen del problema.
  - Pueden aparecer problemas de comunicación como consecuencia de información incorrecta.
    - No solo por dirección IP errónea, sino también **por mal configuración de máscara de subred o default gateway**
  - Sobrecarga Administrativa de Red
    - Especialmente cuando existen movimientos de hosts entre distintas redes (o subredes)
- Configuración de TCP/IP Automática. Ventajas:
  - La información de direcciones IP es provista automáticamente.
    - Ni los usuarios ni los administradores deben configurar las direcciones IP de hosts
  - Se eliminan muchos problemas de configuración
    - Se provee además de la dirección IP, máscara de subred y default gateway otro tipo de información en forma automática.

# DHCP ("Dynamic Host Configuration Protocol")

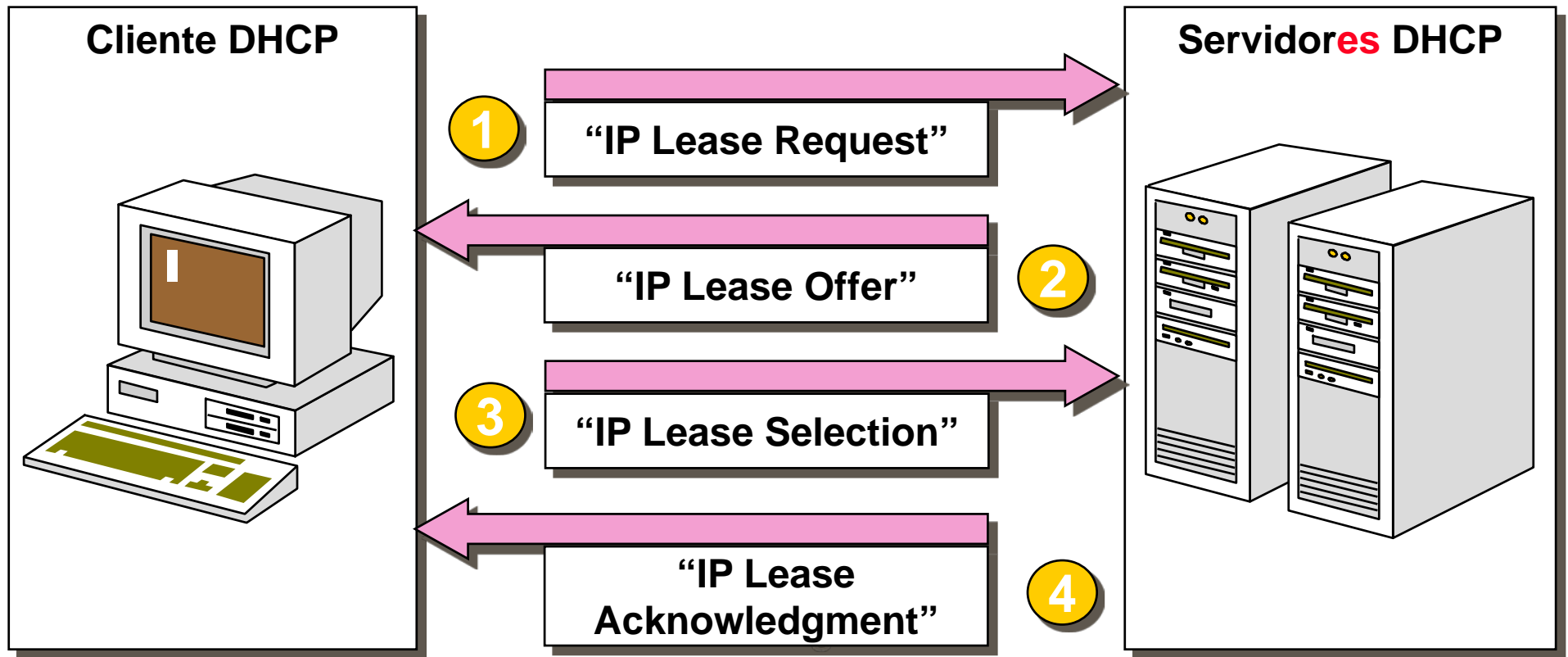
- DHCP centraliza y administra la asignación de configuración de IP, asignando en forma automática:
  - Dirección IP
  - Máscara de Subred
  - Valores opcionales ("default gateway", Servidores DNS, etc)
- DHCP (RFC 1541 – 2131) es una extensión al protocolo BOOTP (RFC 951/1542)
- DHCP trabaja en la capa de **aplicación**.
- Utiliza UDP como protocolo de Transporte
  - En el Cliente: Puerto 68 (BOOTPC)
  - En el Servidor: Puerto 67 (BOOTPS)
- Para su funcionamiento, utiliza un esquema cliente/servidor:
  - Servidor DHCP ofrece configuración IP a los clientes de un "pool" de ofertas
  - Si el cliente acepta la oferta, se alquila la configuración por un cierto **tiempo**
  - Si el cliente **no** puede alquilar la configuración (por cualquier motivo), el cliente **no** puede inicializar TCP/IP ya que no posee dirección IP.

# DHCP ("Dynamic Host Configuration Protocol")





# Operación de DHCP



# Operación básica de DHCP: Fase 1

- Solicitud de Alquiler ("IP Lease Request")
  - Cliente inicializa versión "limitada" de TCP/IP
  - Realiza un "broadcast" solicitando ubicación de server DHCP y alquiler de configuración IP (Paquete **DHCPDISCOVER**)
    - IP Source Add: **0.0.0.0** ("Este" host)
    - IP Dest. Add: **255.255.255.255** (Local broadcast)
    - Source **MAC** Add (para saber host que envió el broadcast)
  - Este proceso se realiza en las siguientes situaciones:
    - TCP/IP se inicializa por primera vez como un cliente DHCP
    - Cliente solicita una dirección IP específica y ha sido negada
    - Cliente cambia su NIC
    - Cliente liberó el alquiler y solicita uno nuevo.

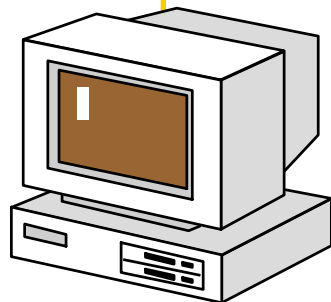
# Operación básica de DHCP: Fase 2

- Oferta de alquiler ("IP Lease Offer")
  - **Todos** los servidores DHCP que pueden ofrecer una configuración de IP válida, envían una oferta al cliente (paquete **DHCPOFFER**).
  - El servidor envía un "broadcast" porque no sabe todavía la dirección IP del cliente.
    - El estándar dice que también puede enviar un paquete unicast a la MAC del cliente (es decir direccionamiento a nivel Hw).
    - Depende de la implementación del Servidor el mecanismo utilizar
  - Si no existen servidores DHCP on-line, el cliente retransmite el broadcast varias veces.
  - Ver próxima transparencia por campos que contiene.

# Solicitud del Alquiler y Oferta

## DHCPDISCOVER

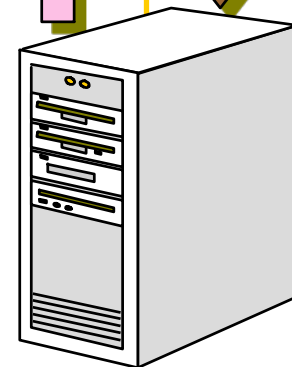
Source IP Address = 0.0.0.0  
Dest. IP Address = 255.255.255.255  
Hardware Address = 08004....  
**ID = X**



**Cliente DHCP**

## DHCPOFFER

Source IP Address = 131.107.3.24  
Dest. IP Address = 255.255.255.255  
Offered IP Address = **131.107.3.13**  
Client Hardware Address = 08004...  
Subnet Mask = **255.255.255.0**  
Length of Lease = **72 hours**  
Server Identifier = 131.107.3.24  
**ID= X**



**Servidor DHCP**

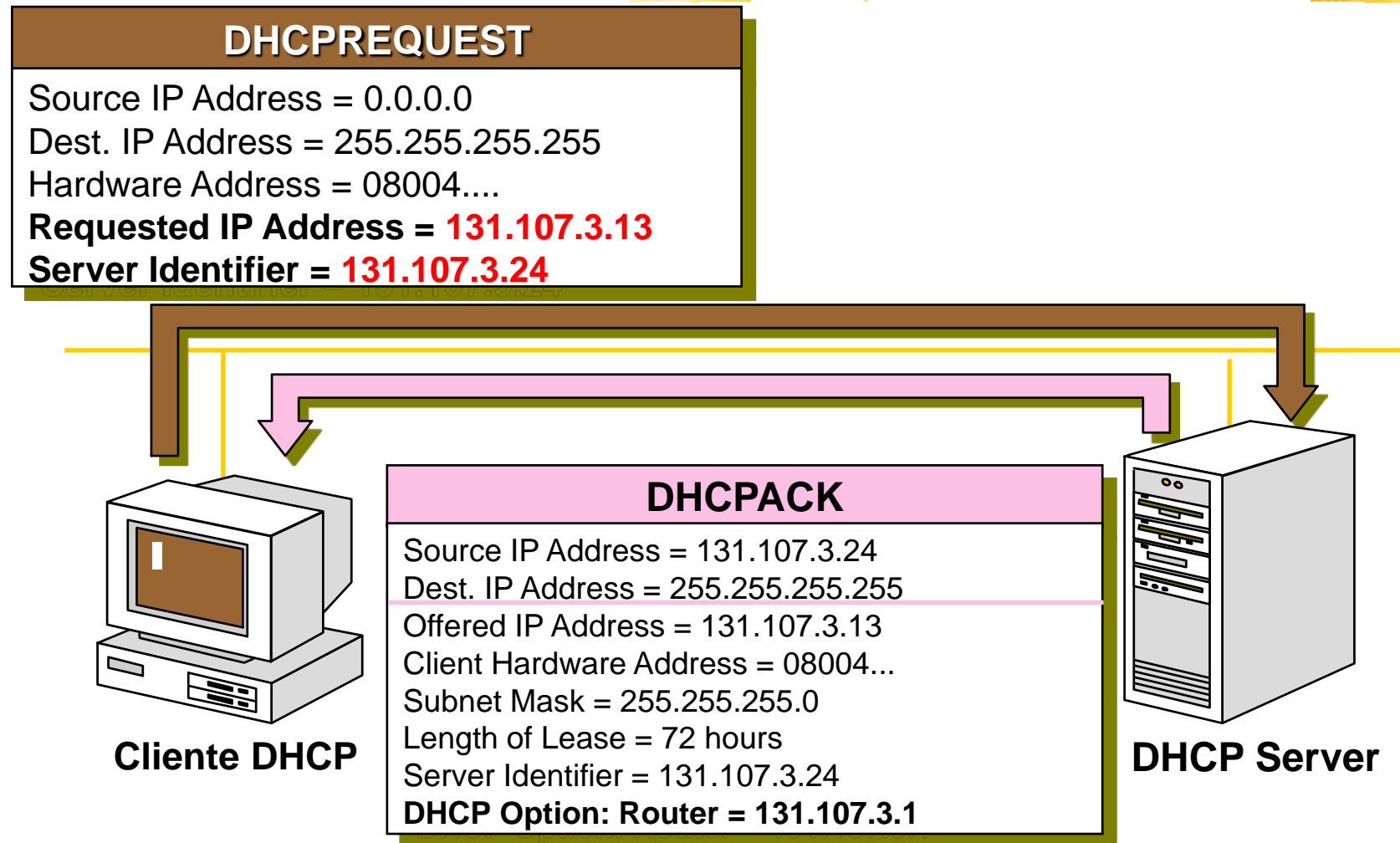
# Operación básica de DHCP: Fase 3

- Selección de oferta de IP ("IP Lease Selection")
  - Cliente selecciona configuración IP de las ofertas que recibe y hace un "broadcast" aceptando el alquiler (Paquete **DHCPREQUEST**).
    - El "**broadcast**" lo realiza para que los servidores DHCP sepan del alquiler
    - Se incluye la identificación del servidor al que se le alquiló la dirección IP (server ID), para que la reserve y envíe en su fase 4 un ACK.
    - Además los otros servidores saben con este mensaje que sus ofertas no fueron seleccionadas.
  - Para el proceso de **renovación** de alquiler se comienza por esta fase.

# Operación básica de DHCP: Fase 4

- Confirmación de alquiler ("IP Lease ACK")
  - Exitoso
    - El servidor DHCP que hizo la oferta responde al mensaje enviando un mensaje de confirmación (paquete **DHCPACK**)
    - Todos los otros servidores DHCP **descartan** su oferta (vuelven la oferta al pool de direcciones para alquilar)
    - El cliente termina la inicialización de IP
  - No Exitoso (Fallo en la fase de renovación)
    - Se emite un paquete **DHCPNAK** cuando:
      - El cliente trata de alquilar su dirección IP previa y esta dirección no está disponible (**renovación** de una IP).
    - Si se recibe un DHCPNAK se vuelve a la fase 1 (envío de DHCPDISCOVER)

# Selección del Alquiler y ACK

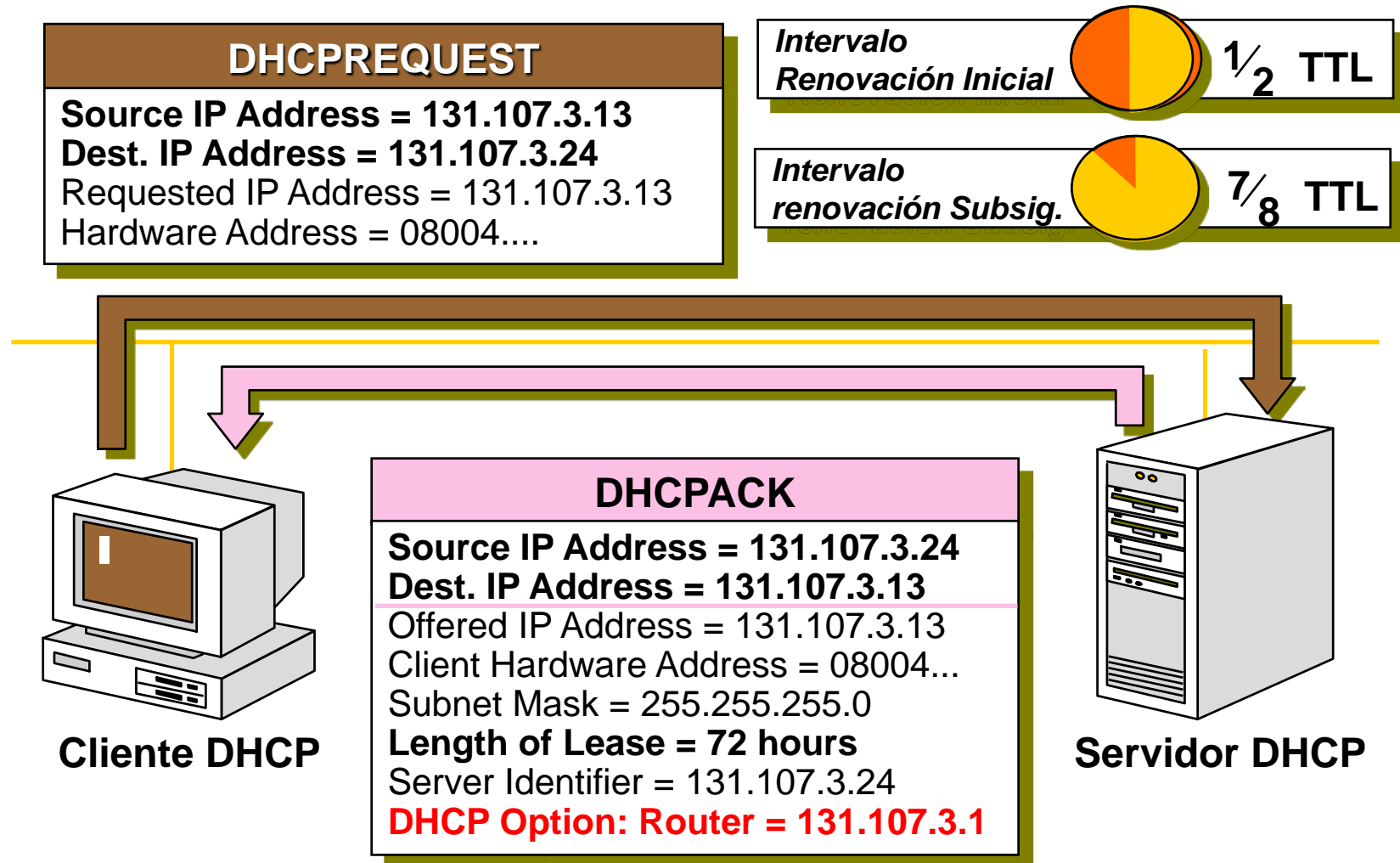


# Renovación de Alquiler

- Todos los clientes intentan renovar alquiler cuando el 50% del tiempo de alquiler ha expirado. (50% sugerido por RFC 2131)
- Envía un paquete DHCPREQUEST **directamente** al servidor DHCP del cual obtuvo el alquiler (unicast)
- Si el servidor está activo, envía DHCPACK y renueva alquiler por un nuevo TTL
- Si el servidor no está activo, no se renueva el alquiler, y cliente sigue usando la dirección que tenía.
- Si no puede renovar con el servidor DHCP original, el cliente luego de varios reintentos, intenta alquilar una IP con **cualquier** servidor DHCP cuando transcurrió el 87,5% del TTL. Envía un DHCPREQUEST con dirección destino: 255.255.255.255
- Cualquier servidor puede contestar con un DHCPACK (renueva el alquiler) o DHCPNACK (fuerza a pasar a la fase 1)
- Si no puede renovar o alquilar, se aborta la comunicación IP



# Renovación del Alquiler



# Configuración de Ámbito en DHCP (Ejemplo: Microsoft)

The screenshot shows the 'DHCP Manager - (Local)' application window. On the left, the 'DHCP Servers' pane shows a tree view with '\*Local Machine\*' selected. The main area is titled 'Option Configuration' and contains a 'Create Scope - (Local)' dialog box. This dialog box is used to define a new IP address pool. It includes fields for 'Start Address', 'End Address', and 'Subnet Mask'. There is also an 'Exclusion Range' section with 'Start Address' and 'End Address' fields, and buttons for 'Add ->' and '<- Remove'. A large 'Excluded Addresses' list box is on the right. The 'Lease Duration' section has radio buttons for 'Unlimited' and 'Limited To', with the latter set to 3 days, 00 hours, and 00 minutes. At the bottom, there are fields for 'Name' and 'Comment', and 'OK', 'Cancel', and 'Help' buttons.

**DHCP Manager - (Local)**

Server Scope DHCP Options View Help

**DHCP Servers**

- \*Local Machine\*

Ready

**Option Configuration**

**Create Scope - (Local)**

IP Address Pool

Start Address: . . .

End Address: . . .

Subnet Mask: . . .

Exclusion Range:

Start Address: . . . Add ->

End Address: . . . <- Remove

Excluded Addresses:

Lease Duration

☐ Unlimited

☒ Limited To: 3 Day(s) 00 Hour(s) 00 Minutes

Name:

Comment:

OK Cancel Help

# Consideraciones de Implementación



- ¿Serán todas las Computadoras Clientes DHCP?
  - Clientes no-DHCP tienen direcciones estáticas
  - Deben ser excluidas tales direcciones del servidor
- ¿Es posible reservar a un host una dirección IP específica?
  - Direcciones Fijas o Estáticas
  - Reserva de Dirección
  - Se debe proveer la Dirección de Hardware del Cliente.
  - Útil para impresoras, "print servers", etc.

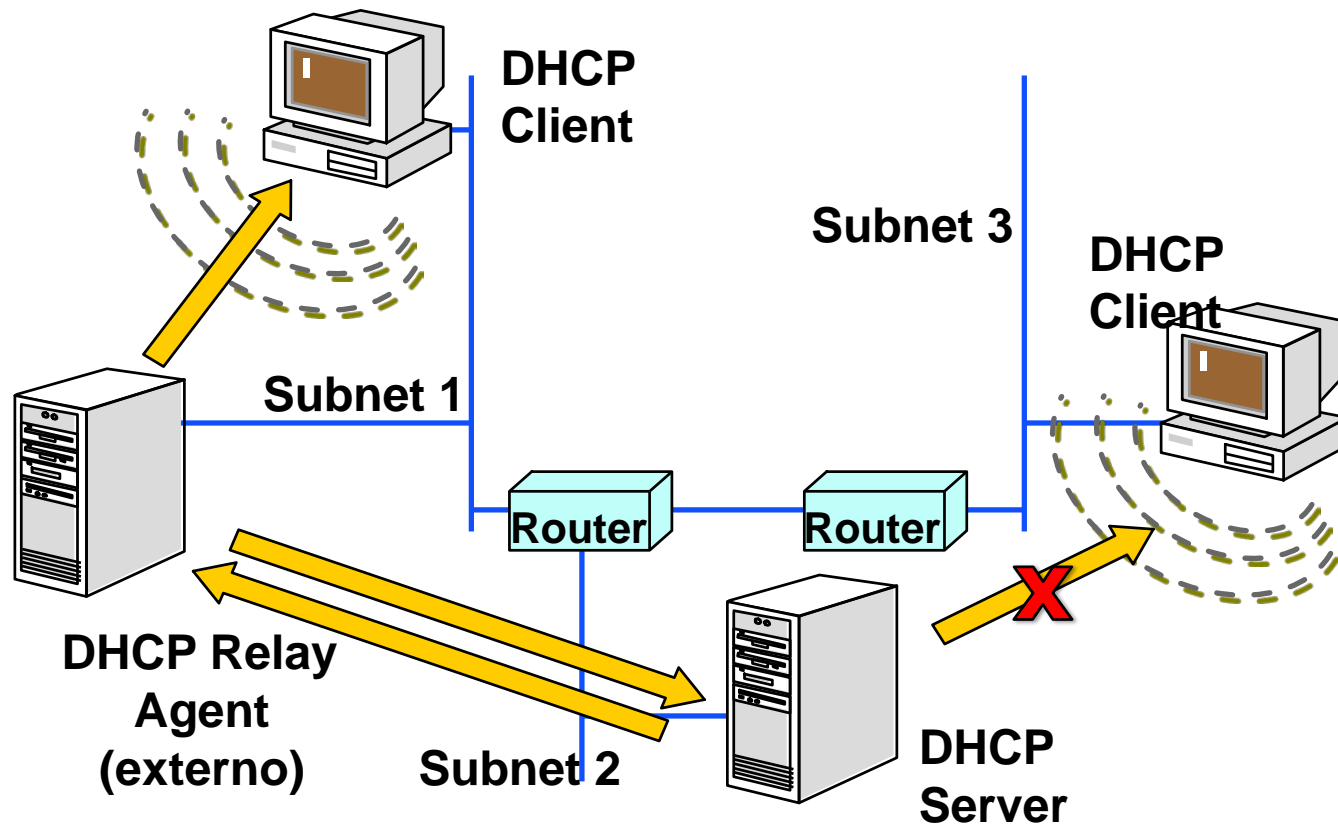
# Consideraciones de Implementación



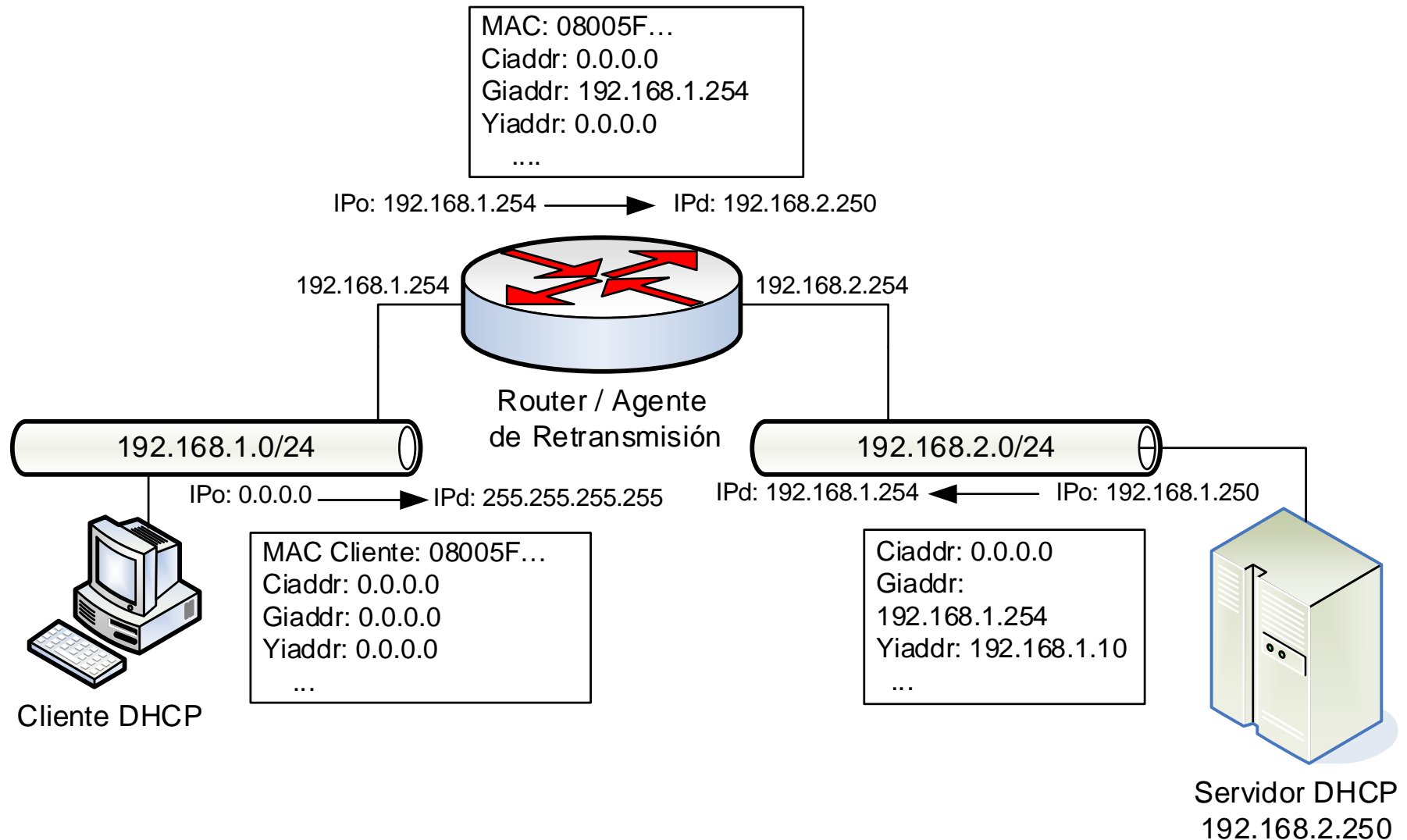
- ¿Qué “Opciones” pueden obtener los Clientes DHCP del Servidor?
  - DNS Server, WINS Server, Default Gateway y otras.
  - Pueden ser especificadas para todos los clientes, para clientes en una subred o para clientes individuales.
- ¿Proveerá un Servidor DHCP Direcciones IP a Subredes Múltiples?
  - Dos soluciones:
    - Los “routers” deben soportar RFC 1542
    - Un agente externo, debe actuar como **BOOTP/DHCP Relay Agent**.
  - Caso contrario, cada subred, debe poseer un servidor DHCP.

# DHCP Relay Agent (externo)

- Convierten los paquetes de broadcast, en paquetes dirigidos a servidores DHCP específicos



# Ejemplo DHCP Relay (en router)



# Consideraciones de Implementación

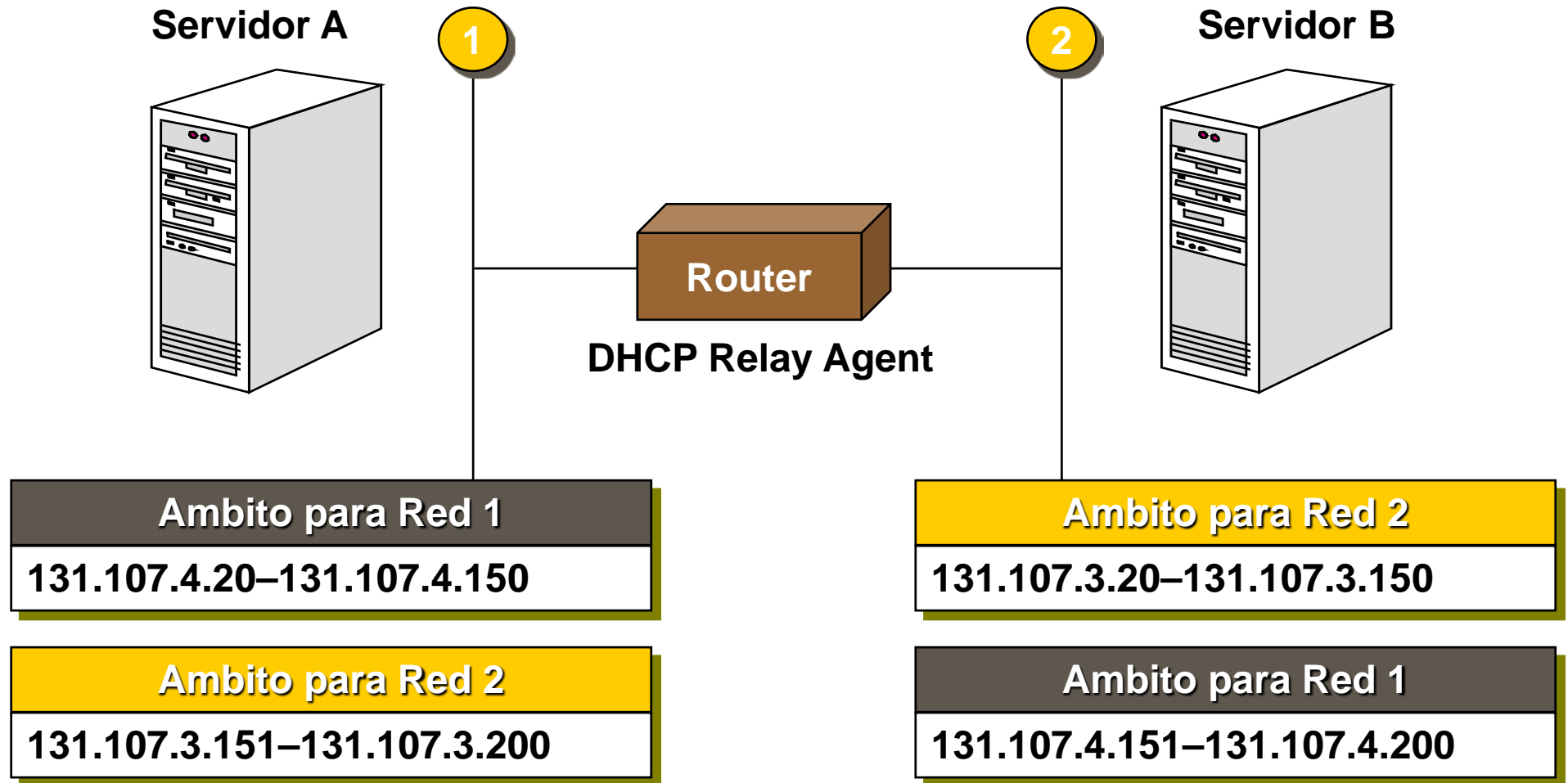
- ¿Cómo se elige la duración máxima del Alquiler?
  - Depende de la relación que existe entre número de hosts y número de direcciones IP disponible.
  - Si  $N^{\circ} \text{ Hosts} < N^{\circ} \text{ Direcciones IP}$ 
    - Elegir un TTL alto (varios días o incluso meses)
  - Si  $N^{\circ} \text{ Hosts} > N^{\circ} \text{ Direcciones IP}$ 
    - Elegir un TTL bajo (horas o minutos)
  - Ejemplo:
    - Los ISP's normalmente eligen TTL bajos ya que normalmente tienen mayor número de clientes potenciales que direcciones IP para entregar a estos clientes.
    - En empresas privadas, es conveniente elegir TTL amplios para disminuir los peligros de renovaciones fallidas de direcciones IP.

# Tiempo de Alquiler (Ventajas/Desventajas)


Tiempo de alquiler bajo		Tiempo de alquiler alto	
Ventajas	Desventajas	Ventajas	Desventajas
Propagación rápida de cambios de configuración a los clientes.	La dirección IP de los clientes puede llegar a cambiar con cierta frecuencia, terminando conexiones TCP	Asignación de direcciones estable.	Pueden quedar exhaustos los rangos de direcciones a alquilar en los servidores.
Baja probabilidad de agotamiento de direcciones IP de los ámbitos.	Mayor sobrecarga en los servidores DHCP y en la red.	Bajo tráfico de mensajes DHCP (broadcast).	No se propagan cambios de opciones rápidamente.
Ante un cambio en el esquema de direcciones, rápida obtención de nuevas direcciones por los clientes.	Los servidores DHCP de alta disponibilidad, puesto que una caída puede dejar fuera de servicio a muchos clientes.	Bajo impacto por la interrupción de servidor DHCP.	Difícil implementación de cambios de direccionamiento IP global.



# Implementación de Múltiples Servidores DHCP



# Requerimientos para Implementación de DHCP



## ➤ Servidor DHCP

- MS Windows 2000/3 (Servidores), Unix (y variantes)
- Routers, Access Points, etc.
- Dirección IP **Estática**, Máscara Subred y default gateway
- Servicio de DHCP Server Instalado y Activo
- Ambito ("Scope") de Direcciones configurado y activo
- Otras configuraciones

## ➤ Cliente DHCP

- MS Windows 2000, Windows XP, MS Windows Vista, Windows 7/8
- Unix (Linux) en sus diferentes distribuciones
- MacOS
- Switches, Access Points, etc.
- Habilitado para DHCP (cliente)

# Renovación y Liberación Manual



- El proceso de renovación de IP es automático y transparente para el cliente.
  - El método depende del Sistema Operativo (diferente para MS que para Linux).
- Si se necesita liberar la dirección IP manualmente existen comandos de DHCP que generan paquetes DHCPRELEASE (por ejemplo en movimientos de hosts de una subred a otra).
- Para eso los sistemas operativos ofrecen comandos.
  - Ejemplo: En MS Windows
    - IPCONFIG /RELEASE – Libera un alquiler >(**DHCPRELEASE**)
    - IPCONFIG /RENEW – Renueva alquiler (**DHCPFORCERENEW**)

# Seguridad en DHCP




- DHCP no es un protocolo seguro
  - Es posible instalar servidores DHCP no autorizados en una red y entregar direcciones IP con fines maléficos.
  - Pueden existir clientes de DHCP no autorizados
- Se puede implementar seguridad a otro nivel, como IPSEC (nivel capa internet)
- Se puede utilizar Autenticación de DHCP
  - RFC 3118
  - Poco utilizado en implementaciones actuales.

# Problemas de Direcciones IPv4



- Problemas con esquema de direcciones de IPv4:
  - Ineficiencia en el esquema de direccionado:
    - Direcciones clase A, B y C, cuando asignadas, desperdician direcciones.
    - Por ejemplo, en una clase C, si se usan 100 direcciones, se desperdician 154 direcciones
  - Tablas de ruteo de routers en Internet saturadas
    - En 1994 estaban llegando al punto de saturación, deteniéndose el crecimiento de Internet.
  - Gran cantidad de hosts en Internet
    - Más de 1.000 millones
    - Direcciones IP (públicas) imposibles de asignar.
- Solución (a largo plazo): IPv6
- Solución intermedia:
  - Direcciones "Classless"
  - NAT ("Network Address Translation")

# NAT (RFC 1631 - 1994) – “Informational”



- Con NAT se traducen direcciones IP privadas a direcciones IP Públicas.
- El principio de funcionamiento de NAT tiene las siguientes motivaciones:
  - La mayoría de los hosts son clientes. Estos hosts **privados** acceden a servidores **públicos** que se encuentran en la Internet.
  - La comunicación se inicia del cliente al servidor (no del servidor al cliente).
  - Un pequeño porcentaje de hosts en una red privada se comunican a Internet en un dado momento.
  - Comunicación a Internet sale a través de un router (actúa como un punto central de comunicación)

# NAT: Ventajas y Desventajas

## ➤ Ventajas:

- Compartimiento de (algunas) direcciones públicas.
- Simple expansión de la red privada
- Mejora la Seguridad de la Comunicación
- Facilita la Administración de la Red (privada)
- Flexibilidad en el servicio de ISP (se puede cambiar el ISP sin cambios en la red privada).

## ➤ Desventajas:

- Complejidad
- Algunas aplicaciones pueden no funcionar bien (Ftp por ejemplo pasa puertos y direcciones IP en sus PDU).
- Problemas con Protocolos de Seguridad (IPSec por ejemplo detecta cambios en el header IP)
- **Reducción de Performance**
- Problemas con algunas aplicaciones como voz sobre IP, peer to peer....

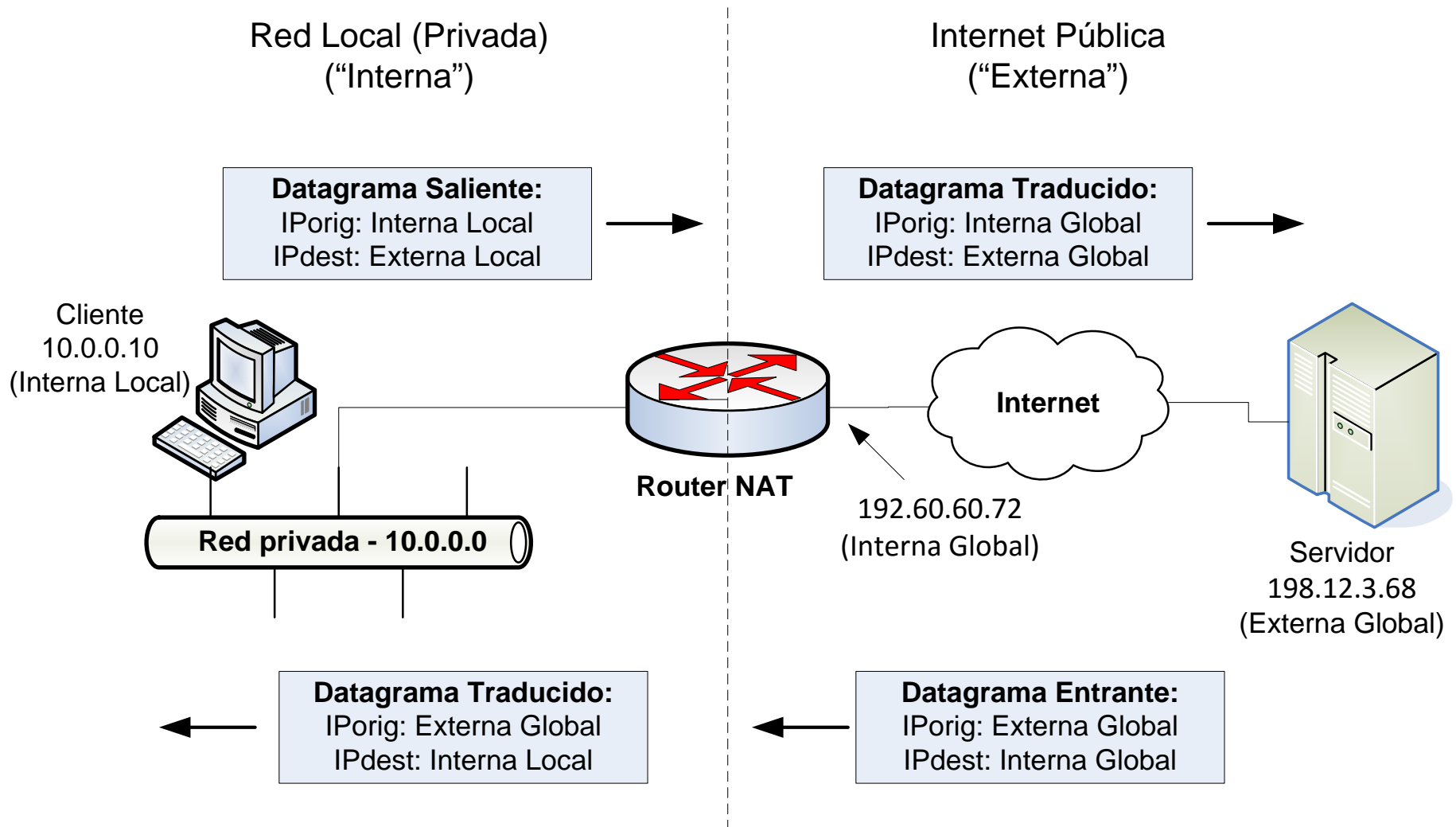
# NAT: Ejemplo de Funcionamiento



- Se podría hacer una analogía entre NAT y una central telefónica privada de una empresa:
  - Manejo de NAT – Recepcionista en una empresa.
  - Juan deja instrucciones a recepcionista que no le transfiera llamadas telefónicas, a menos que él se lo pida.
  - Luego Juan llama a Carlos y deja un mensaje para que le devuelva el llamado.
  - Juan notifica a Recepcionista que está esperando llamado de **Carlos**.
  - Cliente llama al **número principal** de la empresa, le dice a la recepcionista que es **Carlos**.
  - Recepcionista busca si alguien en la empresa estaba esperando una llamada de **Carlos**.
  - Encuentra que Juan estaba esperando y le transfiere la llamada a él.



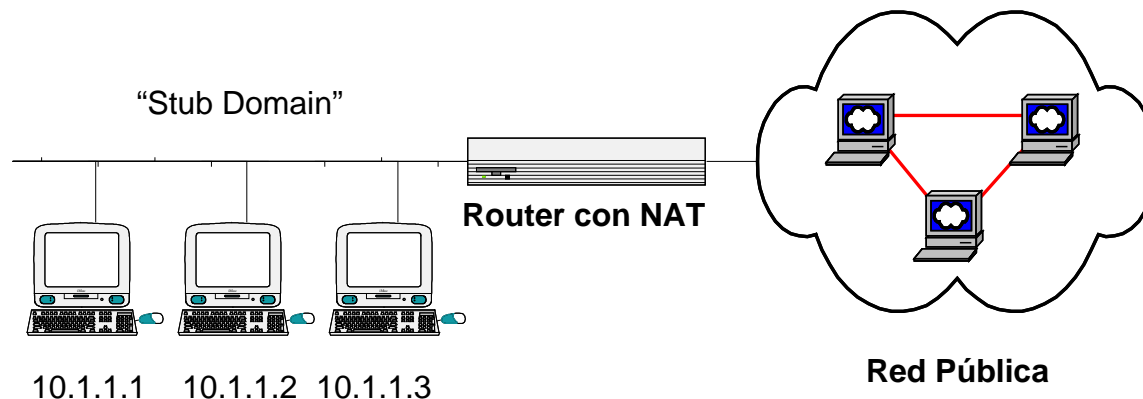
# NAT: Terminología



# Tipos de NAT

## ➤ NAT estático

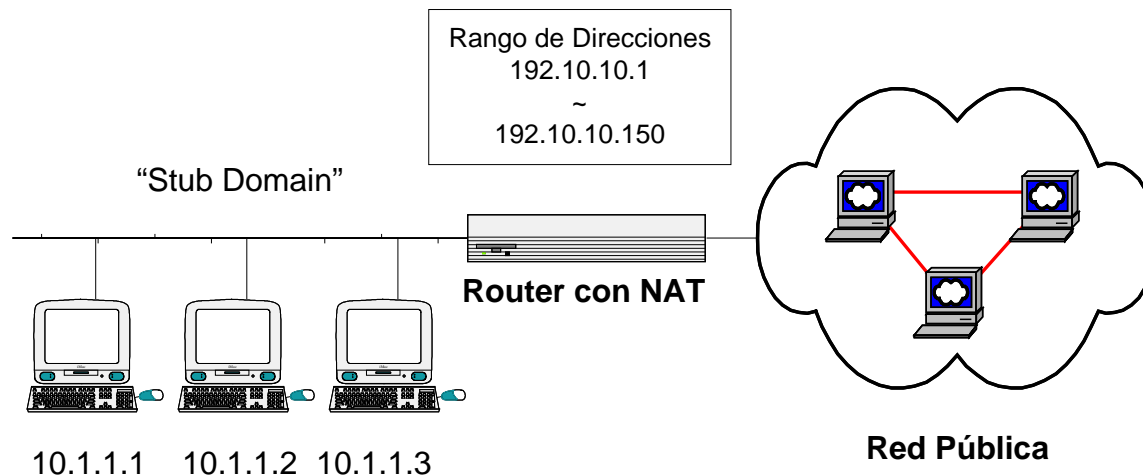
- Mapea en forma **fija** y **permanente** una dirección interna local a una interna global.
- En el escenario de abajo:
  - 10.1.1.1 Direcc. Interna Local (Privada)  
-> Dirección Interna Global 192.10.10.1 (Pública)
  - 10.1.1.2 (Privada) -> 192.10.10.2 (Pública)
  - 10.1.1.3 (Privada) -> 192.10.10.3 (Pública)



# Tipos de NAT

## ➤ NAT Dinámico

- Mapea una dirección Interna Local (Privada) a una Interna Global (IP pública) obtenida de un grupo de direcciones públicas disponibles.
- También el mapeo es uno a uno, pero puede variar en el tiempo.
- En el escenario de abajo, 10.1.1.1 se traducirá a la primera dirección disponible del rango 192.10.10.1 ~ 192.10.10.150



# Tipos de NAT



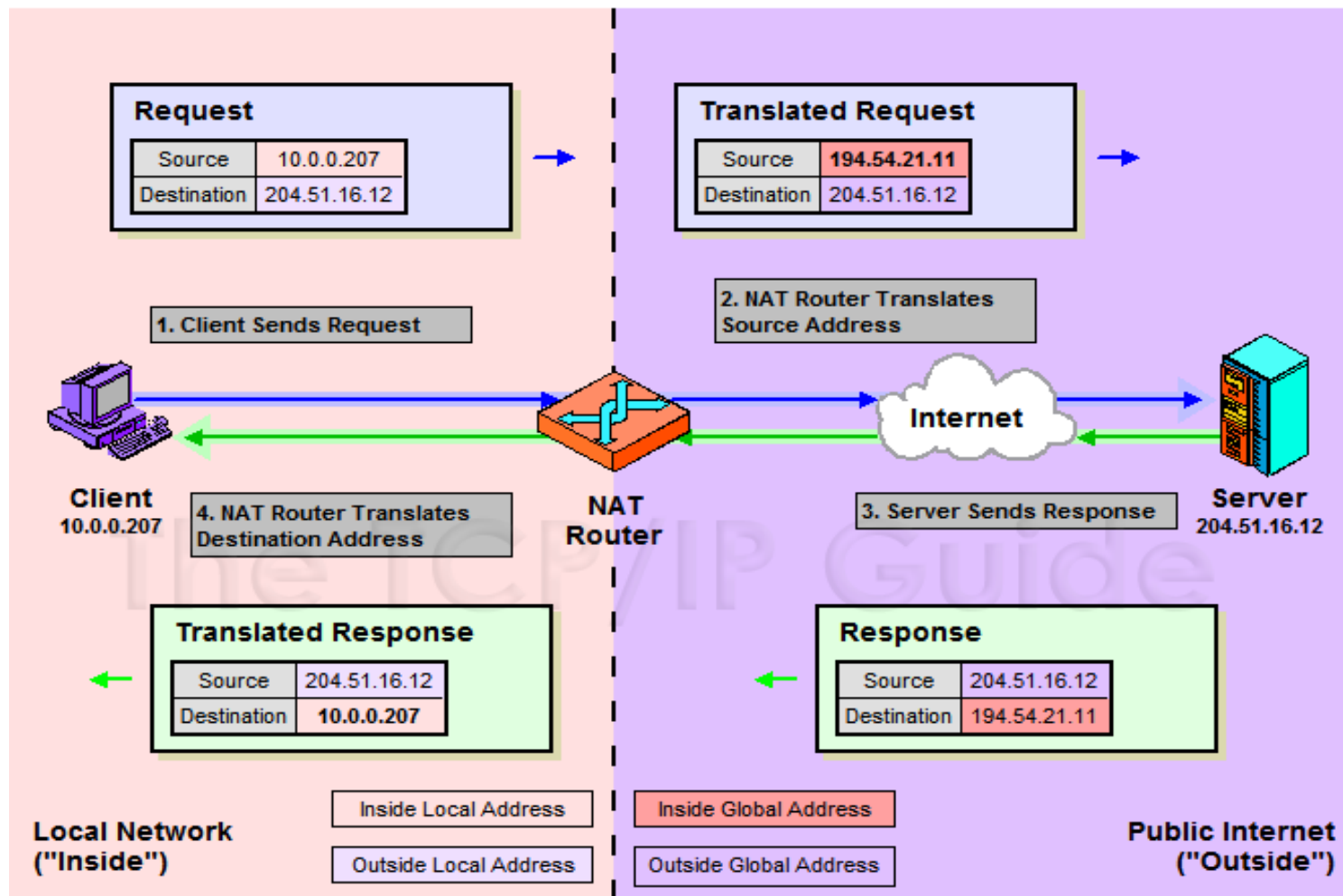
## ➤ NAT Estático

- Ideal para dispositivos que necesitan siempre ser representados con la misma dirección pública a la red externa.
- Requiere intervención (manual) del operador
- No permite compartimiento de IP

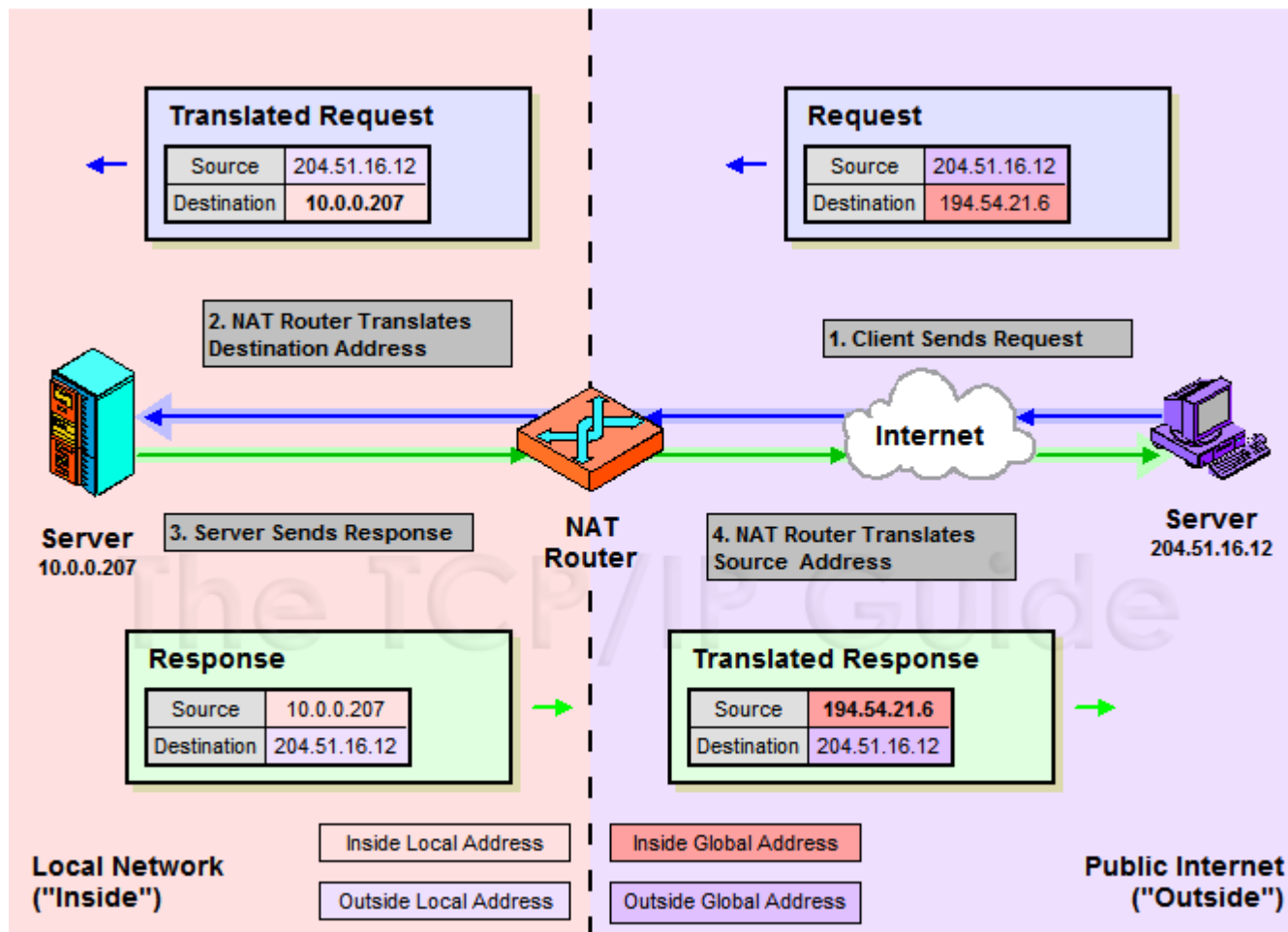
## ➤ NAT Dinámico

- Permite compartimiento de direcciones IP (objetivo de NAT)
  - Mayor complejidad de instalación pero una vez configurado, el otorgamiento de direcciones IP es automático.
- Es posible combinar NAT Estático y Dinámico.
- Se debe tener precaución en no sobrelapar direcciones IP

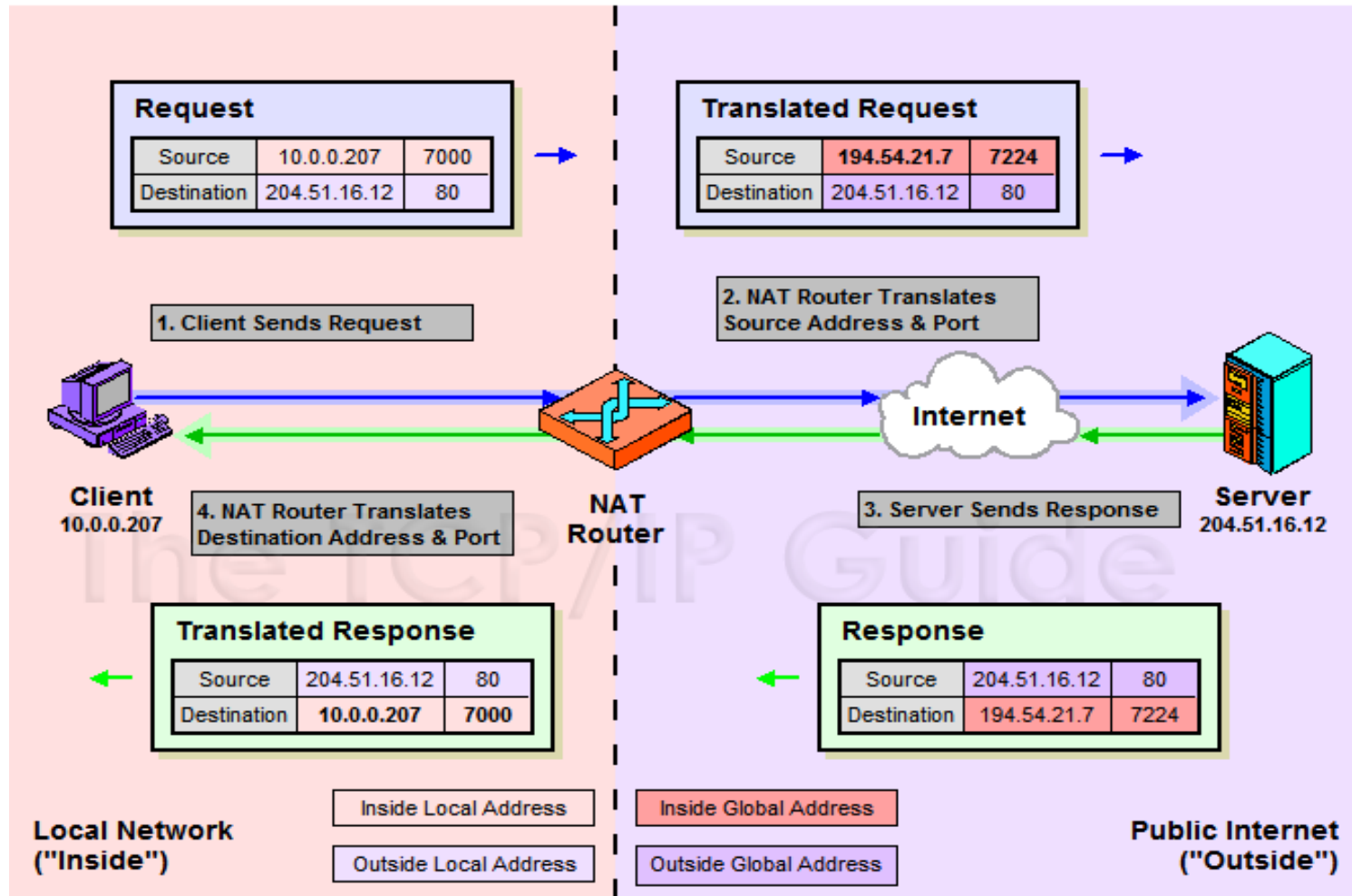
# NAT: Modo Básico de Operación (unidireccional)



# NAT Bidireccional (RFC 2694)



# Port Address Translation (PAT): Ejemplo de operación



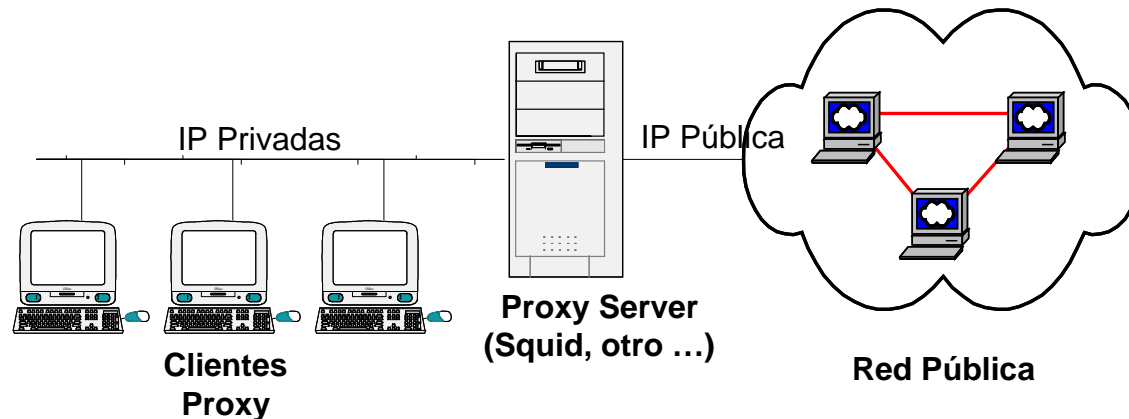
# NAT: Sobrelapamiento de Direcciones Privadas y Públicas

- Situaciones de solapamiento entre direcciones públicas y privadas
  - Conexiones de redes privadas entre si
    - Las direcciones IP Privadas son (RFC 1918):
      - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
      - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
      - 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)
    - Las direcciones automáticas IP Privadas (APIPA) son:
      - 169.254.0.0 - 169.254.255.255 (169.254.0.0/16) (RFC 3927)
  - Asignación de Espacio Público a Redes Privadas
    - Ejemplo: Se configura una red privada con dirección 18.0.0.0 que es publica (MIT)
  - Problema de unión de dos empresas con el mismo rango de direcciones privadas.
- Problema que aparece:
  - Cuando un datagrama se envía de la red privada, el router NAT no puede saber si la red destino es la privada o la pública.
- Solución: "Twice NAT" (no se cubre en el curso)



# NAT vs Web Proxy

- “Web Proxy”
  - Actúa como un medio “Web Server”
    - Los clientes de red, realizan solicitudes al Proxy, el cual a su vez, traslada las mismas al servidor Web (público) en nombre del cliente.
  - Puede almacenar páginas temporalmente (“local caching”)
  - Tecnología Proxy es una alternativa a NAT (acceso compartido a una única conexión de Internet).
- Diferencia Fundamental entre NAT y Web Proxy:
  - NAT es transparente al host origen y destino. Web Proxy en general no lo es.
  - Con Web Proxy, el host origen debe ser configurado.



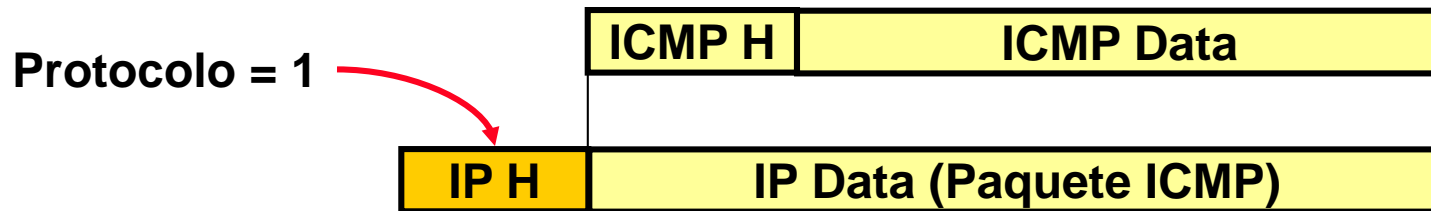
# NAT: Consideraciones



- NAT no es totalmente transparente
  - Algunas aplicaciones utilizan direcciones IP y puertos que pueden ser traducidos por NAT.
    - Los routers deben soportar estas aplicaciones (FTP es un ejemplo)
  - Recálculo de Checksums de TCP y UDP
    - Como el "checksum" del header TCP y UDP se computa sobre un pseudo header IP que contiene la dirección IP, se debe recalcular, debido al cambio de direcciones IP producidos por NAT
  - ICMP
    - Debe rehacer ciertos mensajes ICMP que incluyen Header de IP (Ejemplo: Destination Unreachable)
  - NAT incluso puede tener que modificar números de secuencia en TCP (ejemplo: Ip privada: 10.0.0.207 - 10 ASCII en FTP, IP traducida: 193.54.21.11: 12 ASCII. Al hacer la substitución, cambia el tamaño del payload, se deben acomodar los numeros de secuencia de TCP)

# Internet Control Message Protocol (ICMP)

- ICMP: RFC 792 (Año 1981)
- Permite a “**hosts**” y “routers” enviar mensajes de error y control a nivel IP.
- ICMP “reporta” errores. No los “corrige”
  - Los reporta al host origen
- Los mensajes ICMP son encapsulados en datagramas IP
  - El protocolo ICMP interpreta el dato encapsulado.
  - Se identifica el PDU ICMP a través del campo **protocolo** del header IP (Protocolo = 1 -> ICMP)



# Mensajes ICMP



- Los mensajes ICMP se dividen en dos grandes clases:
  - Mensajes **Informativos** (o de consulta)
  - Mensajes de **Error**.
- En general, no se puede generar un paquete ICMP de **error** en respuesta a:
  - Un mensaje de **error** ICMP
  - Un mensaje de broadcast o multicast
  - Un fragmento de datagrama excepto el primero
  - Un datagrama con una dirección origen no-unicast

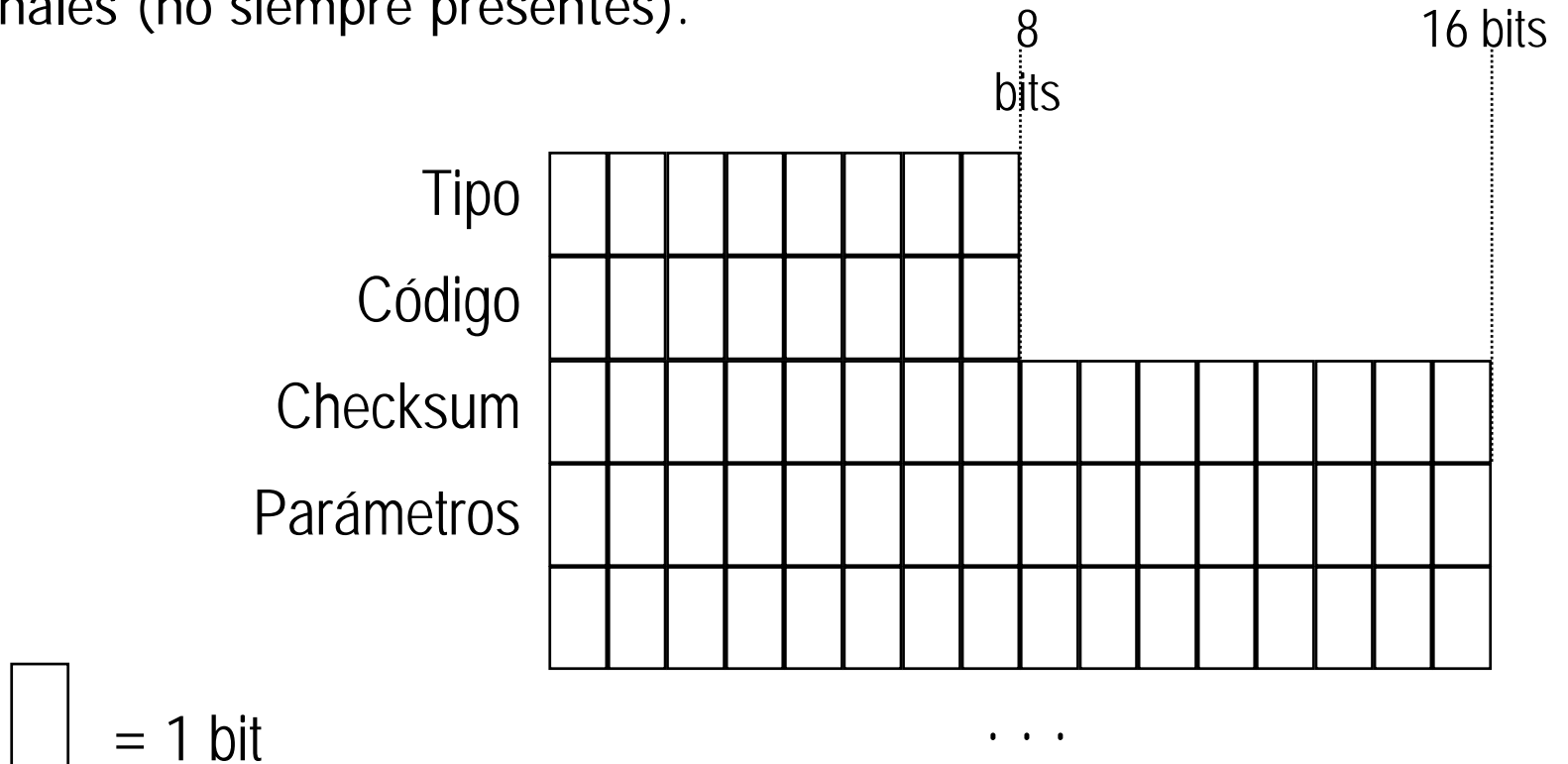
# ICMP



- Algunas de las funcionalidades que implementa ICMP son:
  - Retardar la velocidad de transmisión ("source quench") (Msg **Error**)
  - Echo request y echo reply (utilizado por utilitario **ping**) (Msg **Informativo**)
  - Detección de rutas circulares o muy largas (Msg **Error**)
  - Cambio de tablas de ruteo en hosts (Msg **Error**)
  - Detección de pérdidas de Fragmentos IP (Msg **Error**)
  - Retardo de tiempos en la Internet (Msg **Informativo**)
  - Otros

# ICMP: Formato del Encabezamiento

- El **encabezamiento** del datagrama ICMP tienen una **porción fija de 64 bits**, donde los primeros 32 bits son ocupados por los campos de Tipo, Código y Checksum y los últimos 32 bits por parámetros adicionales (no siempre presentes).



# ICMP: Formato del Encabezamiento

## ➤ Campo Tipo (8 bits)

➤ Especifica el significado del mensaje ICMP

Tipo	Mensaje ICMP
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
<b>9</b>	<b>Router Advertisement</b>
<b>10</b>	<b>Router Solicitation</b>
11	Time Exceeded for a Datagram

# ICMP: Formato del Encabezamiento

## ➤ Campo tipo ...

Tipo	Mensaje ICMP
12	Parameter Problem in a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Replay (obsolete)
<b>17</b>	<b>Address Mask Request</b>
<b>18</b>	<b>Address Mask Reply</b>



# ICMP: Formato del Encabezamiento

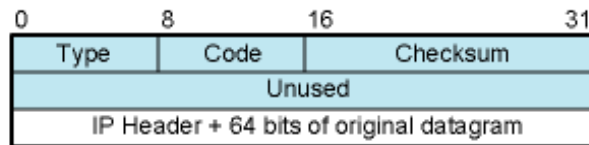
- Campo Código (8 bits)
  - Información adicional del campo **Tipo**
  - Ejemplo:
    - Tipo = 3 (destino no-alcanzable)
    - Código = 0 (Red no-alcanzable)
    - Código = 1 (Host no-alcanzable)
    - Código = 2 (Protocolo no-alcanzable)
    - Código = 3 (Puerto no-alcanzable)
    - Código = 4 (Fragmentación necesaria y DF en 1)
    - Código = 5 (Ruta origen fallida)
  - Otro Ejemplo:
    - Tipo = 11
    - Código = 0 (TTL = 0)
    - Código = 1 (Tiempo de reensamblaje de fragmento excedido)

# ICMP: Formato del Encabezamiento

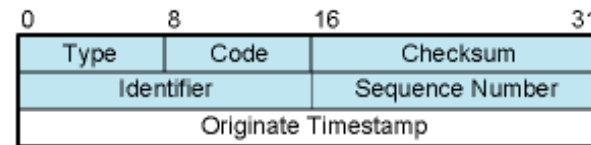
- Campo Checksum
  - Código para detección de errores en el mensaje ICMP ("header" y **datos**)
- Parámetros
  - Dependiendo del campo Tipo el mensaje ICMP agrega datos a continuación del header
  - En los casos que ICMP de error, se incluye el **Header IP + 64 bits del campo de datos original**
    - Esto permite al host origen contrastar el mensaje ICMP con el datagrama IP y analizar el header (o parte) del protocolo encapsulado en el datagrama.
  - Ejemplo: Tipo = 8 (Echo Req) – 0 (Echo Reply)

Parámetros {	Tipo	Código	Checksum
	Identificador		Número Secuencia
	Datos Adicionales		

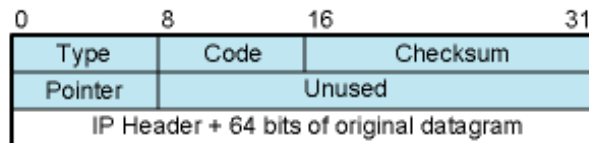
# ICMP: Formatos de Mensajes



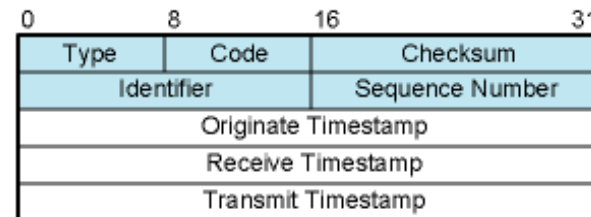
(a) Destination Unreachable; Time Exceeded; Source Quench



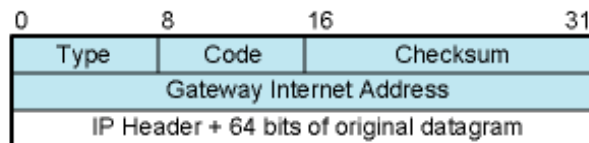
(e) Timestamp



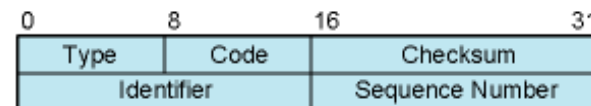
(b) Parameter Problem



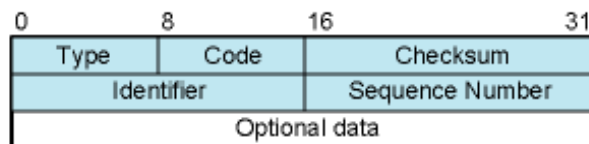
(f) Timestamp Reply



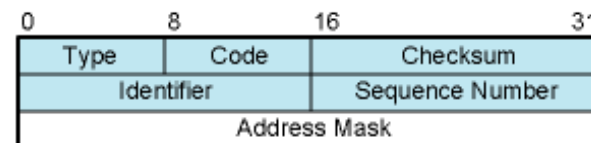
(c) Redirect



(g) Address Mask Request

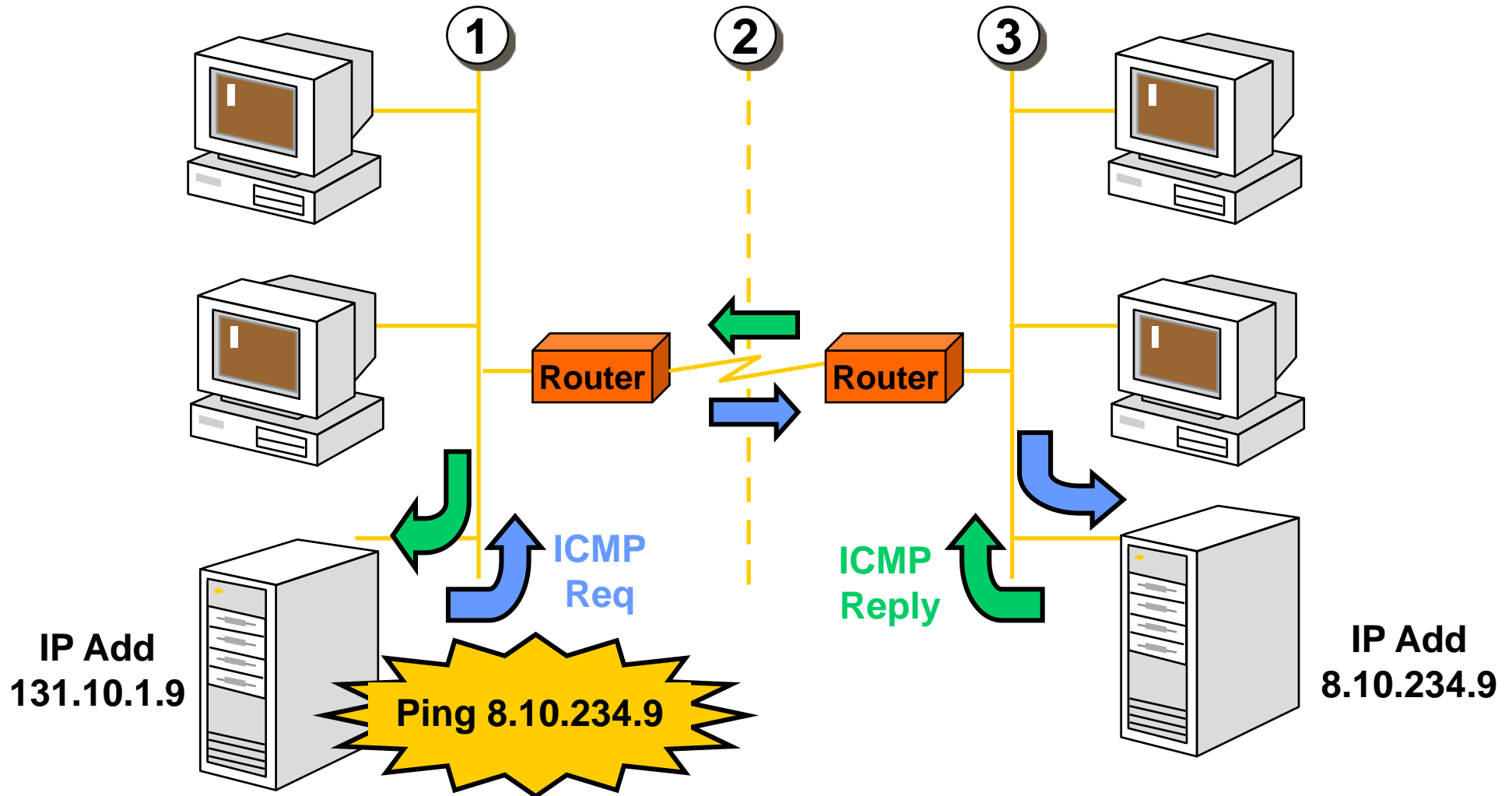


(d) Echo, Echo Reply



(h) Address Mask Reply

# Ping: Echo Request y Echo Reply



# Ping: Uso



- El comando ping se utiliza para testear si un host (o router) es alcanzable.
- Ping permite testear:
  - Software IP máquina origen
  - Routers intermedios en el camino de ida
  - Software IP máquina destino
  - Routers intermedios en el camino de vuelta
  - Direccionamiento IP en todo el trayecto ida/vuelta
  - Retardo "round-trip"

# Multicasting (Multidifusión)

- Los datagramas IP pueden ir dirigidos a:
  - Un Host en particular ("Unicast")
  - Todos los Hosts de una subred ("Broadcast")
  - Un grupo de Hosts ("**Multicast**")
- Multidifusión
  - Propiedad de IP de enviar un datagrama desde una fuente a los miembros de un grupo de hosts IP (denominado "multicast group")
  - Implementación Opcional en IPv4 (no en IPv6)
- Usos
  - Multimedia (audio, video)
  - Teleconferencia
  - Bases de Datos
  - Computación distribuida
  - Grupos de Trabajo de Tiempo real
  - Protocolos de Comunicación
  - Distribución de Software

# Direcciones Multicast

- IPv4 soporta Multicast
  - Direcciones IP **Clase D**
    - Comienzan con 1110
    - 28 bits restantes sin estructura indican el Identificador de Grupo.
    - Rango: 224.0.0.0 ~ 239.255.255.255
- IPv6 soporta Multicast en forma obligatoria (no opcional como IPv4).
- “Host group”
  - Conjunto de hosts que poseen la misma dirección de IP Multicast.
  - Un “host group” se puede distribuir en múltiples subredes
  - Un host puede pertenecer a varios grupos simultáneamente.
- Algunas direcciones de grupos multicast no pueden ser utilizadas (reservadas):
  - 224.0.0.0 Reservada (no puede ser asignada a ningún grupo)
  - 224.0.0.1: “All systems group” – Todos los hosts en una subred.
  - 224.0.0.2: “All routers group”. – Todos los routers en una subnet.
  - En general: 224.0.0.1 a 224.0.0.255 reservadas para protocolos de ruteo y mantenimiento de grupos multicast.
- También hay direcciones reservadas por aplicaciones (224.0.1.1 NTP, 224.0.1.118 por IBM Tivoli)

# Direcciones Multicast

- IP trata en forma diferente a las direcciones IP Multicast que Unicast
  - No puede ser usada como **dirección origen**
  - No se pueden generar mensajes ICMP (**error**) relacionados a paquetes multicast
- Multicasting no está previsto para todos los protocolos de acceso al medio.
- Ethernet (y otras tecnologías LAN) provee traducción de direcciones IP multicast a direcciones de Hardware.
  - La MAC Address (6 Bytes) tiene un bit denominado G/I (Group/Individual bit).
  - Si G/I se encuentra en 1, la dirección MAC es multicast:
  - MAC ADD: 01.00.00.00.00.00 – Multicast (G/I: **LSB** Primer Octeto).
  - MAC ADD reservadas por IANA para Multicast: 01:00:5E:00:00:00 a 01:00:5E:7F:FF:FF (23 bits disponibles)
- El mapeo de una IP Multicast a una MAC Multicast se hace tomando los 23 bits menos significativos de la IP e insertándolos en la MAC ADD (LSB)
  - Posibles conflictos de mapeos a resolver por el host (para saber si corresponde o no al grupo multicast).



# Multicast: Generalidades



## ➤ Implementación en LAN:

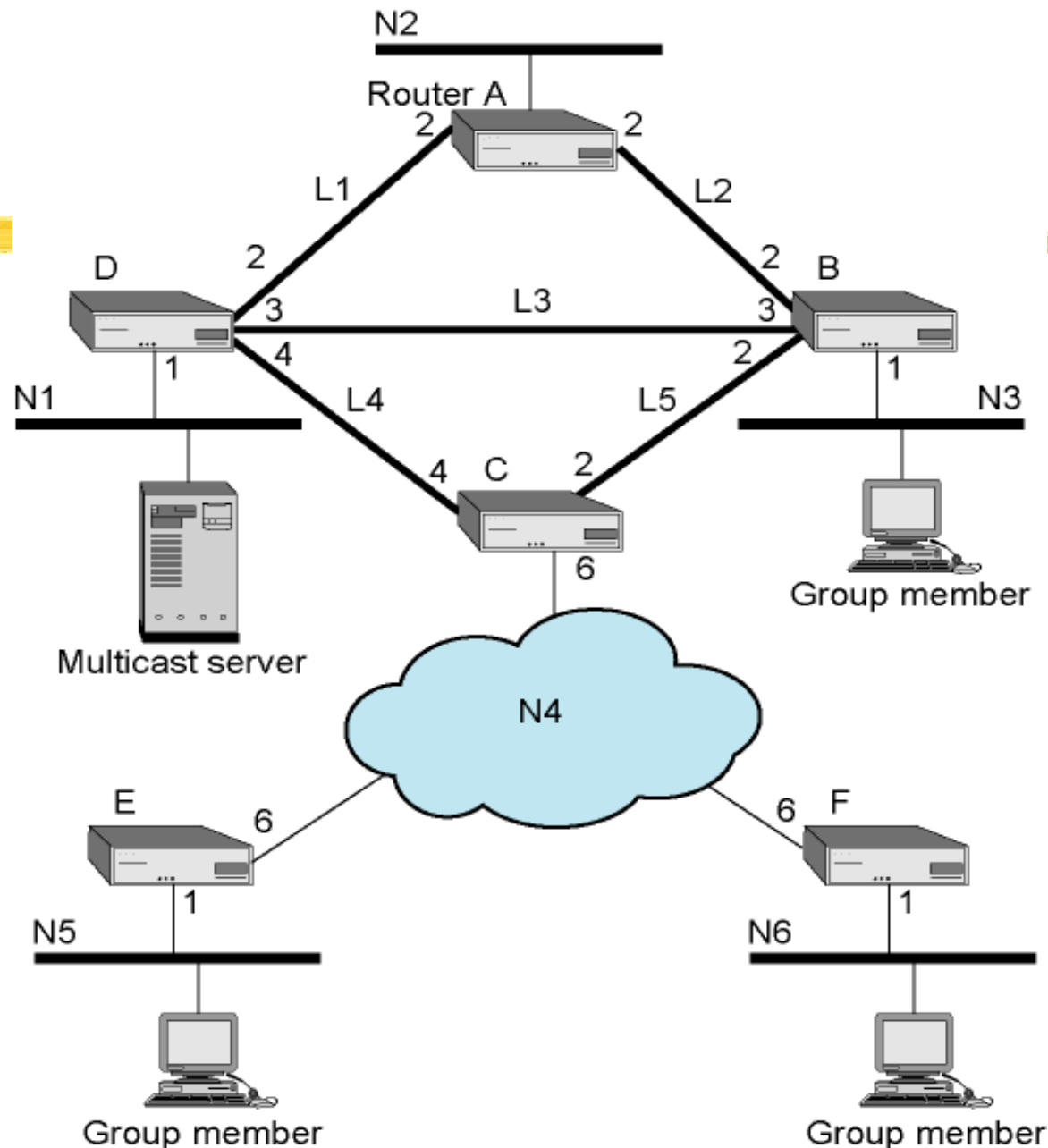
- Simple por la naturaleza de difusión de datos inherente a una LAN.
- Direcciones multicast a nivel MAC
- Los miembros del grupo multicast, aceptan los paquetes dirigidos a ellos.

## ➤ Implementación en WAN:

- El grupo de hosts se distribuye por toda la internet.
- Los routers deben utilizar mecanismos especiales para enviar paquetes multicast a los miembros

# Configuración de Ejemplo

- Un servidor “multicast” y un grupo de tres miembros que residen en redes remotas.
- El servidor no sabe la ubicación de los miembros del grupo.
- El router de cada red, es responsable por la traducción de la dirección multicast IP a una dirección multicast de Hardware.
- El número asociado a cada link, es el costo del mismo.



# Broadcast y Unicast Múltiple

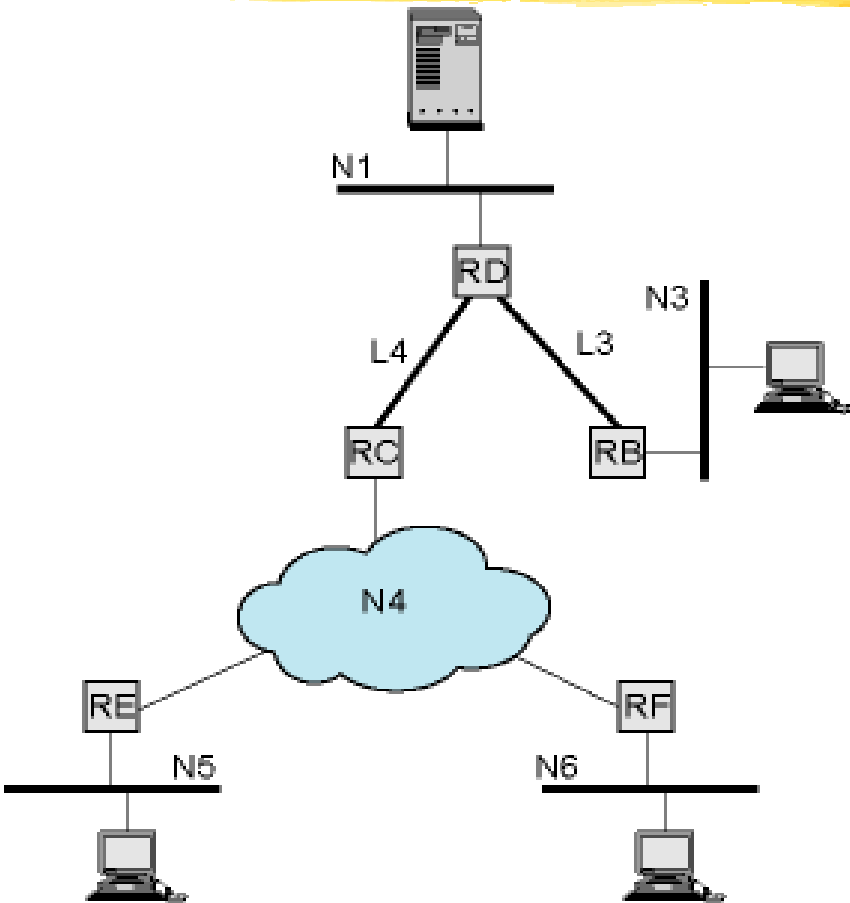


- Transmisión tipo “Broadcast”
  - Servidor envía una copia de cada paquete a cada red por el camino de menor costo.
  - Requiere 13 copias del datagrama.
- Transmisión tipo “Unicast” múltiple:
  - Servidor envía paquetes solamente a redes que tienen hosts en grupos.
  - El servidor en este caso debe conocer la ubicación de cada miembro del grupo.
  - Requiere 11 copias del datagrama.
- Ambos métodos son ineficientes porque generan copias innecesarias del datagrama origen.

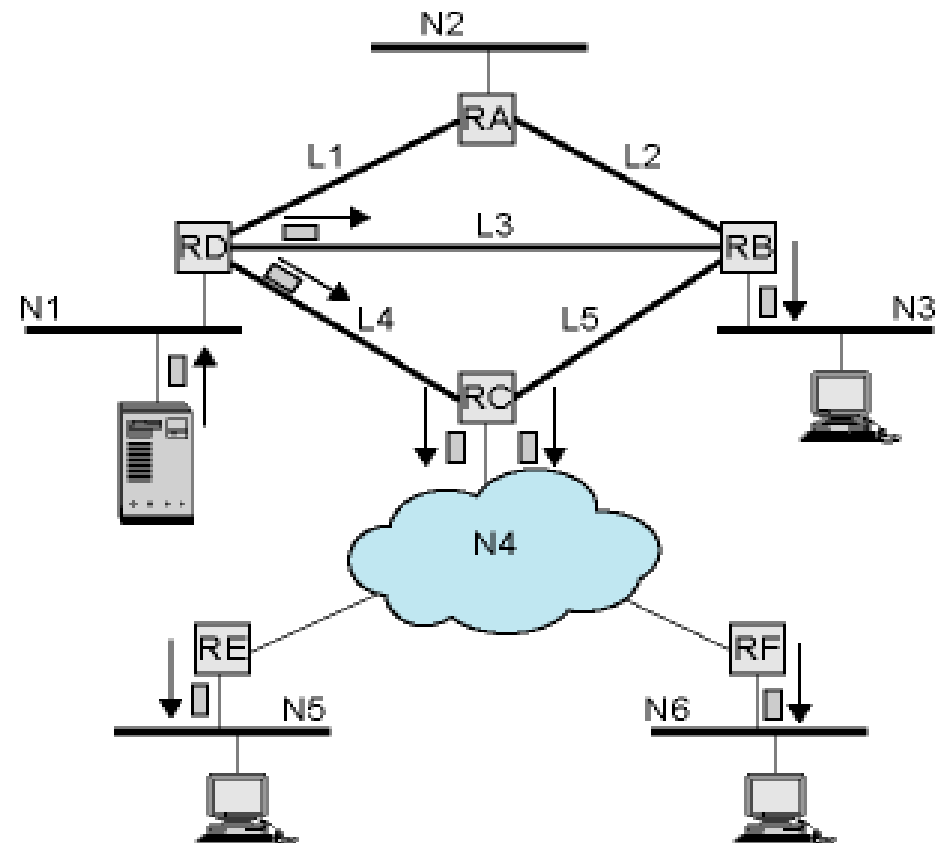
# Multicast real

- El método que se utiliza en un sistema de multidifusión real, es más complejo, disminuyéndose el número de datagramas generados.
- El método es:
  - Determinar el camino de menor costo desde el host **origen** ("multicast server") a cada red que posee un host del grupo.
    - Se obtiene un "spanning tree" de la configuración
    - Este "spanning tree" no es un "full spanning tree", sino que contiene solo las redes que poseen **miembros del grupo** multicast.
  - Transmitir un único paquete a través del spanning tree.
  - En los routers que conectan a redes WAN **replicar** paquetes en las **bifurcaciones** del "spanning tree"
- Con este esquema se requieren solo 8 datagramas

# Ejemplo de Transmisión Multicast



(a) Spanning tree from source to multicast group



(b) Packets generated for multicast transmission

# Requisitos para Multicasting

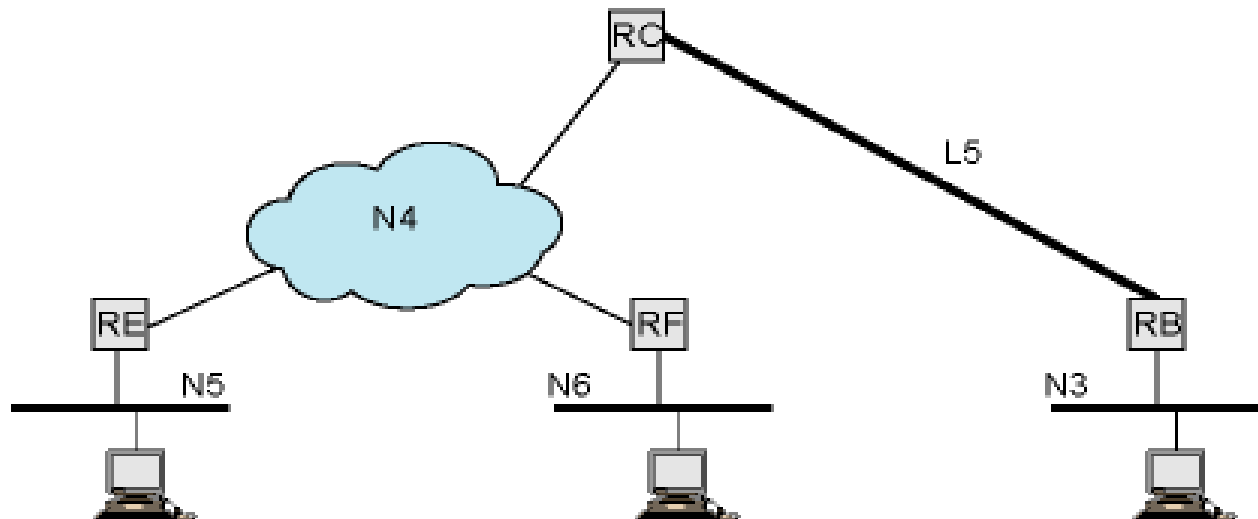
- Routers tienen que poder reenviar más de una copia del paquete (en ejemplo, routers D y C).
- Se necesita una convención para identificar las direcciones multicast
  - IPv4 - Clase D
  - IPv6 – Prefijo de 8 bit (todos 1's), campo de "flags" de 4 bits, campo de "scope" de 4 bits, identificador de grupo de 112
- Cada nodo (router o nodo origen) debe traducir entre direcciones IP multicast y una lista de redes que contengan miembros del grupo.
  - Esto permite al nodo construir el "spanning tree".
- Router debe traducir entre direcciones **IP** multicast y direcciones multicast de **hardware** (MAC Multicast Address).
  - En IEEE 802, la MAC Address Multicast tiene el G/L en 1.

# Requisitos para Multicasting

- Generalmente las direcciones “multicast” son **dinámicas**, con hosts uniéndose o abandonando grupos multicast.
  - Se requiere mecanismo para que los hosts **anuncien** a los routers cuando se unen o abandonan a grupos de multicast. (Protocolo IGMP)
- Routers deben intercambiar dos tipos de información:
  1. Que redes incluyen miembros de un grupo dado.
  2. Información para resolver el camino más corto a cada red.
  - Esto implica la necesidad de un protocolo de ruteo **especial** para “multicasting”
- Cada router debe rutear en base a la dirección origen (unicast) y destino **multicast**.
  - Si no se cumple esta condición, es posible que lleguen paquetes duplicados a un mismo nodo.
  - Ver transparencia siguiente por el “Spanning Tree” formado desde C.

# Spanning Tree desde C al grupo de Multicast

- Cuando router C construye el "spanning tree", resulta la topología mostrada abajo, pudiendo el miembro de N3, recibir dos paquetes (el original, mas el generado por C).
- Para solucionar esto, C debe construir el árbol con N1 (lugar donde se encuentra el host origen del multicast) como **root**, y rutear en base a ese árbol (es decir debe tener en cuenta IP origen y destino).

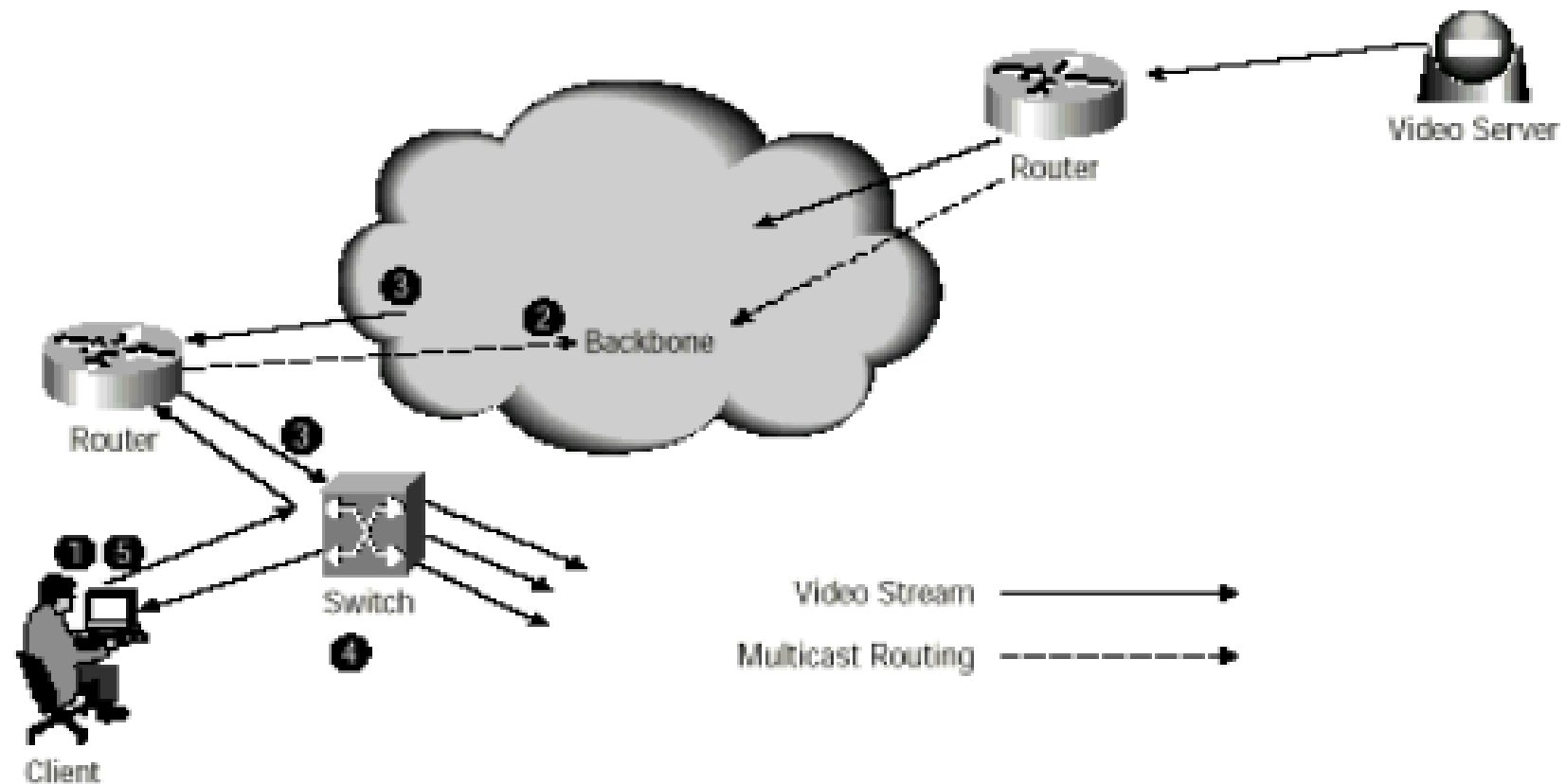




# Protocolos relacionados con Multicast

- IGMP - Internet Group Management Protocol (RFC 3376)
  - Version actual: IGMP v3, año 2002
  - Apto para IPv4
  - Para IPv6 se incluye IGMP dentro de ICMPv6
  - Protocolo que permite a los hosts unirse y abandonar grupos de multicast sobre una LAN.
- Protocolos de ruteo de Multicasting
  - DVMRP (Distance Vector Multicast Routing Protocol)
    - Primer Protocolo de ruteo multicast diseñado.
    - Distance Vector (como RIP)
    - Apropiado para LAN
  - MOSPF (Multicast Open Shortest Path First)
    - Extensión de OSPF
    - Incluye información de multicasting en los mensajes OSPF
  - PIM (Protocol Independent Multicast)
    - Se divide en PIM-DM (Dense Mode) y PIM-SM (Sparse Mode)
    - PIM-DM apropiado para LAN's y PIM-SM para WAN's
  - Otros protocolos:
    - CBT (Core Based Trees)
    - Simple Multicast
    - EXPRESS

# Ejemplo: Recepción de datos de un Servidor de Video Con Multicasting



# Ejemplo.



1. Cliente envía un mensaje IGMP de “join” al router designado.
2. Router guarda el mensaje de “join” y usa protocolo de ruteo multicast (PIM u otro) para adicionar el segmento al árbol de distribución.
3. Tráfico multicast IP que se trasmite del server es distribuido a la subred del cliente. Se utiliza la dirección MAC “multicasting”.
4. El switch recibe el paquete multicast y examina la tabla de direcciones (“forwarding table”):
  - Realiza “flooding” (no hay entrada MAC en tabla)
  - Direccionamiento directo (a todos los puertos designados en la tabla)
5. Cliente detiene su participación en el grupo de multicast enviando un mensaje IGMP (Versión 2 o 3).

# Implementación de Multicast

## ➤ Requerimientos:

- Protocolos TCP/IP con soporte de IP multicasting en Server y Estaciones.
- Aplicaciones de Clientes y Servidores deben soportar IP multicast.
- (Deseable) LAN con Switches que permitan IGMP “snooping”.
  - Permite que el switch escuche mensajes IGMP entre hosts y routers.
  - Cuando Switch recibe un mensaje “IGMP Join” de un host, adiciona el puerto del host a la Dirección Destino del Grupo.
  - Cuando Switch recibe un mensaje “IGMP Leave”, quita el puerto de la tabla de direcciones.
- WAN: Routers deben implementar ruteo de IP multicast.
  - Al menos los routers de ingreso/egreso a la intranet.
  - Routers internos o Switches Capa 3 pueden usar tunneling de IP (encapsulación de Multicast en paquetes Unicast).