REDES DE COMPUTADORES

Grado en Ingeniería en Informática
Doble Grado en Ingeniería en Informática y ADE

Curso académico 2023/2024

Práctica 4. Encaminamiento IP avanzado

CONTENIDOS

1. OBJETIVOS
2. DIRECCIONAMIENTO IP PRIVADO. MECANISMOS NAT/PAT
3. DIRECCIONAMIENTO DE REDES IP Y TABLAS DE ENCAMINAMIENTO
4. PROTOCOLO DHCP
5. CUESTIONES A REALIZAR
6. DOCUMENTACIÓN COMPLEMENTARIA

1. Objetivos

- Analizar el mecanismo **NAT** (Traducción de Direcciones de Red) para proporcionar conectividad entre una red IP privada (LAN con direccionamiento IP privado) y una red IP pública (Internet).
- Conocer los mecanismos de direccionamiento IP y definición de tablas de encaminamiento en routers.
- Conocer el funcionamiento del protocolo DHCP.

2. Direccionamiento IP privado. Mecanismos NAT/PAT

El mecanismo NAT (Traducción de Direcciones de Red) tiene como objetivo conseguir que las estaciones de una red con direccionamiento IP privado puedan tener conectividad con Internet. Este mecanismo se describe en el documento RFC 1631 y se basa en un escenario como el que se presenta en la siguiente figura.

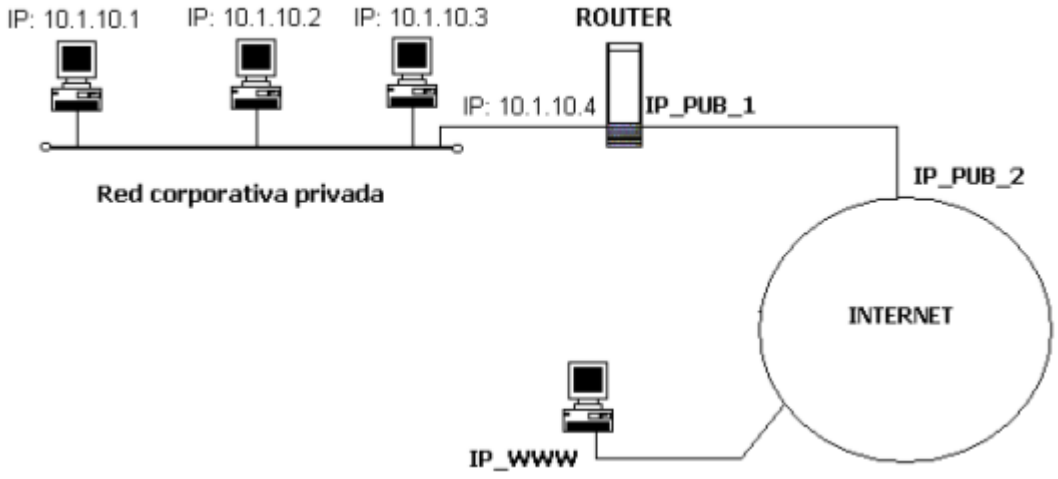


Figura 1. Escenario de funcionamiento para NAT

El **direccionamiento IP privado** son un conjunto de redes IP que no están asignadas a ningún equipo de Internet. En concreto, las redes IP privadas existentes son:

a) 10.0.0.0/8

b) 172.16.0.0/16 - 172.31.0.0/16

c) 192.168.0.0/24 - 192.168.255.0/24

El resto de direcciones IP disponibles se denominan direcciones **IP públicas** y se caracterizan porque los routers de Internet son capaces de encaminar paquetes a esos destinos (además de que son direcciones únicas en Internet).

Un paquete IP con destino una dirección IP privada es rechazado por los routers del *backbone* (troncal) de Internet. El empleo del direccionamiento IP privado permite poder asignar direcciones IP dentro de una red privada sin restricciones ni costes, ya que disponer de una dirección IP pública (o legal) tiene un coste económico asociado.

El problema surge cuando se necesita conectar estas redes privadas con Internet. La conexión se realiza empleando un router que dispone de una o varias direcciones IP públicas asociadas. El router debe transformar los paquetes procedentes de la red privada modificando la dirección IP origen por las direcciones IP públicas que tiene asociadas.

Este mecanismo, Traducción de Direcciones de Red (NAT – *Network Address Translator*), precisa de una determinada nomenclatura.

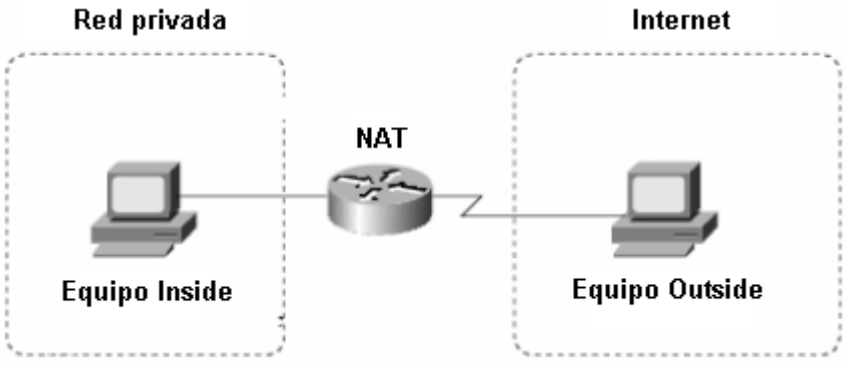


Figura 2. Nomenclatura en el mecanismo de NAT

El router que implementa el mecanismo de NAT separa dos redes: **la red *inside*** y **la red *outside***. La red *inside* se corresponde con la red privada que tiene direccionamiento privado. La red *outside* es la red con direccionamiento público (Internet).

Además, se introducen los términos ***local*** y ***global***. El término *local* hace referencia a la red interna y el término *global* hace referencia a Internet. Así, pueden definirse los siguientes tipos de direcciones IP:

INSIDE LOCAL: Direcciones IP de las máquinas de la red privada en la red privada.
INSIDE GLOBAL: Direcciones IP de las máquinas de la red privada en Internet.
OUTSIDE LOCAL: Direcciones IP de las máquinas de Internet en la red privada.
OUTSIDE GLOBAL: Direcciones IP de las máquinas de Internet en Internet.

Con esta nomenclatura, el router que realiza NAT tiene que transformar las cabeceras IP's de los paquetes de la siguiente forma:

IP origen	IP destino	
INSIDE LOCAL	OUTSIDE LOCAL	DATOS
OUTSIDE LOCAL	INSIDE LOCAL	DATOS

IP origen	IP destino	
INSIDE GLOBAL	OUTSIDE GLOBAL	DATOS
OUTSIDE GLOBAL	INSIDE GLOBAL	DATOS

Para entender mejor el funcionamiento de esta traducción, considérese el siguiente escenario de funcionamiento.

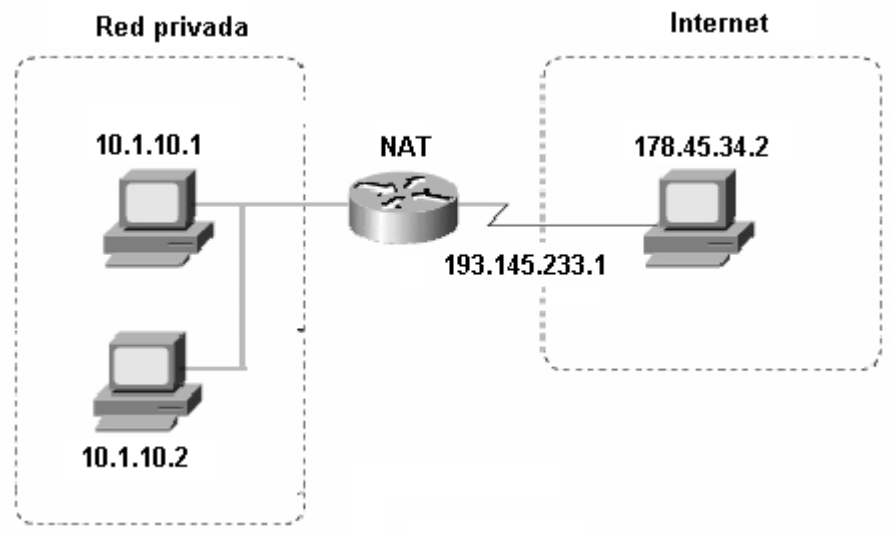


Figura 3. Ejemplo de funcionamiento de NAT

En el escenario de funcionamiento de la figura 3 las direcciones IP de la traducción de NAT serán:

INSIDE LOCAL: 10.1.10.1, 10.1.10.2
INSIDE GLOBAL: 193.145.233.1
OUTSIDE LOCAL: 178.45.34.2 (las direcciones IP de las máquinas de Internet son las mismas en la red privada que en Internet).
OUTSIDE GLOBAL: 178.45.34.2

Así, la traducción a realizar será:

IP origen	IP destino	
10.1.10.1	178.45.34.2	DATOS
178.45.34.2	10.1.10.1	DATOS

IP origen	IP destino	
193.145.233.1	178.45.34.2	DATOS
178.45.34.2	193.145.233.1	DATOS

Hay que notar que los paquetes son traducidos en los dos sentidos de la comunicación.

Sin embargo el mecanismo de traducción indicando anteriormente tiene un grave problema, y es que será válido **sólo si hay UNA máquina de la red privada intercambiando datos con un determinado destino de Internet**. Si las estaciones 10.1.10.1 y 10.1.10.2 intercambian información con el mismo destino 178.45.34.2, las traducciones son incapaces de realizarse en el sentido Internet - red privada.

IP origen	IP destino	
10.1.10.1	178.45.34.2	DATOS
10.1.10.2	178.45.34.2	DATOS

IP origen	IP destino	
193.145.233.1	178.45.34.2	DATOS
193.145.233.1	178.45.34.2	DATOS

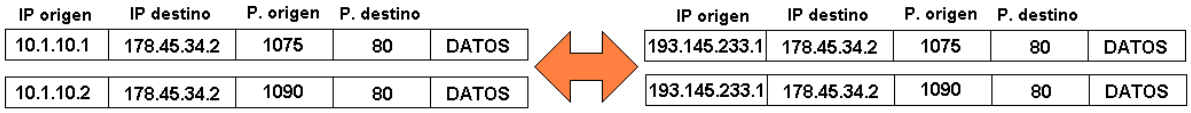
El router es incapaz de conocer a qué máquina de la red interna tiene que entregar el paquete procedente del equipo de Internet.

Para solucionar este problema sería necesario tener una dirección IP pública para cada máquina de la red interna, por lo que no sería operativo. Sin embargo, ya que la mayor parte de las comunicaciones se fundamentan en la capa de transporte, pueden emplearse los números de puerto de las conexiones de transporte para identificar máquinas de la red interna empleando una única dirección IP pública en el router.

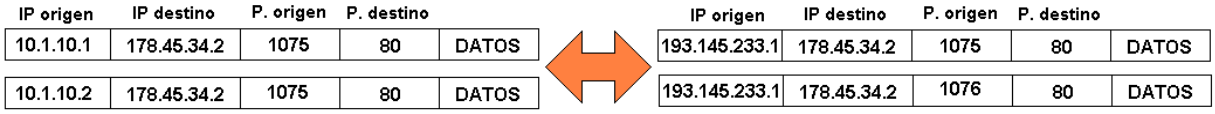
PAT (*Port Address Translator*) permite complementar a NAT para conseguir que una sola dirección ***inside global*** pueda ser compartida por varias estaciones de la red privada.

Al emplear PAT, se mantienen los mismos números de puerto de origen en la traducción de NAT, y será posible identificar máquinas distintas.

Supóngase que en el escenario de la figura 3, la estación 178.45.34.2 es un servidor web, y las dos estaciones de la red privada intentan acceder a él. La traducción quedaría en la forma:



De esta forma puede emplearse el número de puerto de origen para identificar a qué máquina de la red interna está asociado el paquete. Existe un caso particular y es cuando el puerto origen empleado en los dos equipos de la red interna son los mismos (esto ocurre frecuentemente, ya que los números de puerto origen se generan secuencialmente por parte del sistema operativo de los equipos). En este caso, el router modifica el número de puerto origen en el paquete traducido, empleando uno que no esté siendo usado por otra traducción.



La información acerca de las traducciones que realiza el router se almacena en su memoria, empleando una tabla denominada **tabla de traducciones**. Esta tabla tiene el siguiente formato:

Inside global	***Inside local***	***Outside local***	***Outside global***
193.145.233.1:1075	10.1.10.1:1075	178.45.34.2:80	178.45.34.2:80
193.145.233.1:1076	10.1.10.2:1075	178.45.34.2:80	178.45.34.2:80

Esta tabla puede consultarse en un router Cisco con el comando IOS **"sh ip nat translations"**.

El mecanismo NAT/PAT sólo es válido para el tráfico TCP y UDP. Sin embargo, el sistema operativo IOS de Cisco está desarrollado para permitir traducir tráfico que no emplee la capa de transporte (GRE, ICMP, etc.). El mecanismo de traducción en estos casos no está normalizado y es cada fabricante de hardware el que determina qué protocolos soporta en la traducción y cómo la realiza.

3. Direccionamiento de redes IP y tablas de encaminamiento

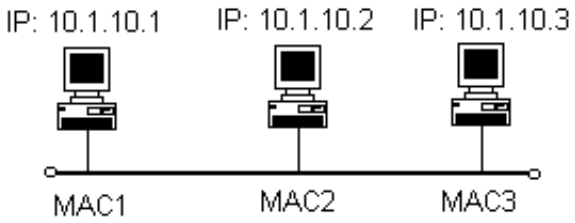
3.1 Direccionamiento IP

En Internet, para que un dispositivo tenga conectividad en la red es necesario configurar los parámetros que lo permiten: dirección IP, máscara de red y puerta de enlace por defecto.

En la actualidad, existen dos tipos de tecnologías a la hora de construir redes de computadores, que son las redes de difusión y redes punto a punto.

Redes de difusión

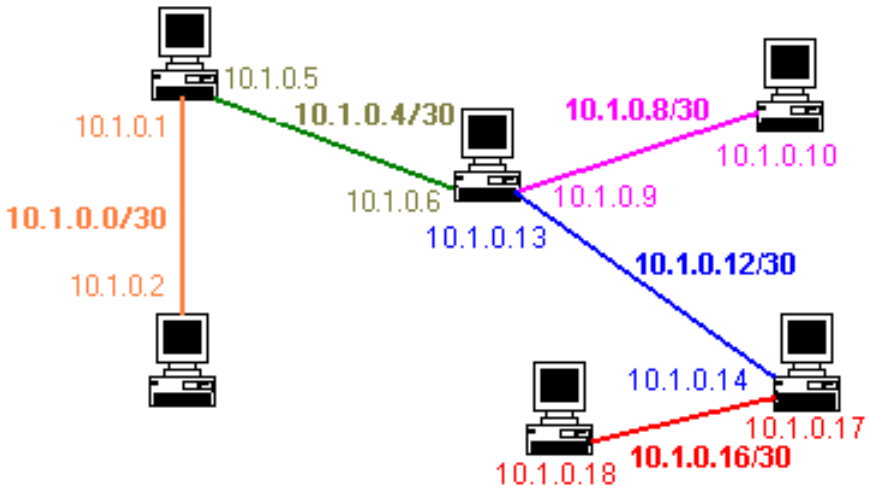
En una red de difusión todos los equipos comparten un mismo medio físico y sus direcciones IP deben estar asignadas en una misma red IP. El valor de la máscara de red asignada determina el número de direcciones IP disponibles, siendo la máscara de 24 bits (/24) el valor más frecuentemente usado (hasta 254 equipos). Estas redes IP pueden ser de clase C (máscara de 24 bits) o es posible crear subredes con una máscara de 24 bits en redes IP de clase A o C.



Subred IP 10.1.10.0/24

Redes punto a punto

Las redes punto a punto consisten en un medio físico con dos equipos únicamente, dispuestos en los extremos del medio de comunicación. En estos casos, la red IP precisa de dos direcciones IP para los extremos de la comunicación, más la dirección de red y de difusión. Así, estas redes tendrán asignada una máscara de 30 bits, por lo que serán subredes de otras redes IP de clase A, B o C.



Redes punto a punto con máscaras de 30 bits

3.2 Tablas de encaminamiento

La tabla de encaminamiento de un dispositivo conectado a Internet especifica la manera en que los paquetes IP son transmitidos en el medio y se consigue conectividad con cualquier dirección IP.

Todos los dispositivos conectados a Internet precisan de tabla de encaminamiento, aunque su complejidad dependerá del tipo de dispositivo.

Los equipos finales de los usuarios de Internet (PCs, Smartphones, tablets, decodificadores de vídeo, etc.) disponen de una tabla de encaminamiento muy sencilla: se especifica la red IP a la que está conectado y la puerta de enlace por defecto para la conectividad a Internet.

Sin embargo, los routers disponen de tablas de encaminamiento más complejas, pues conocen la estructura de la red y tienen conectividad a varias redes IP.

Estructura de una tabla de encaminamiento

Una tabla de encaminamiento consta de filas que se denominan **entradas**. Para cada entrada se especifican un conjunto de valores dispuestos en columnas y que precisan al menos de 3 valores: red IP de destino, máscara de red y puerta de enlace. Así, cada entrada en la tabla de encaminamiento especifica una red IP a la que el dispositivo puede encaminar paquetes.

Además, es posible distinguir entre 3 diferentes tipos de entradas:

1. **Redes directas**: Entradas asociadas a redes IP a las que el dispositivo está conectado directamente. En estas entradas, la dirección IP de la puerta de enlace es la dirección IP del dispositivo en esa red.
2. **Redes alcanzables**: Entradas asociadas a redes IP a las que el dispositivo puede encaminar un paquete empleado un router. La puerta de enlace es la dirección IP del router.
3. **Puerta de enlace por defecto**: Entrada asociada a cualquier dirección IP que no esté definida en ninguna entrada de la tabla de encaminamiento. En esta entrada se especifica la dirección IP de la puerta de enlace por defecto del dispositivo (será la última entrada en la tabla de encaminamiento).

Dirección IP destino	Máscara	Puerta de enlace
10.1.1.0	255.255.255.0	10.1.1.20
10.3.0.0	255.255.0.0	10.1.1.4
0.0.0.0	0.0.0.0	10.1.1.1

Tabla de encaminamiento con entradas de diferente tipo

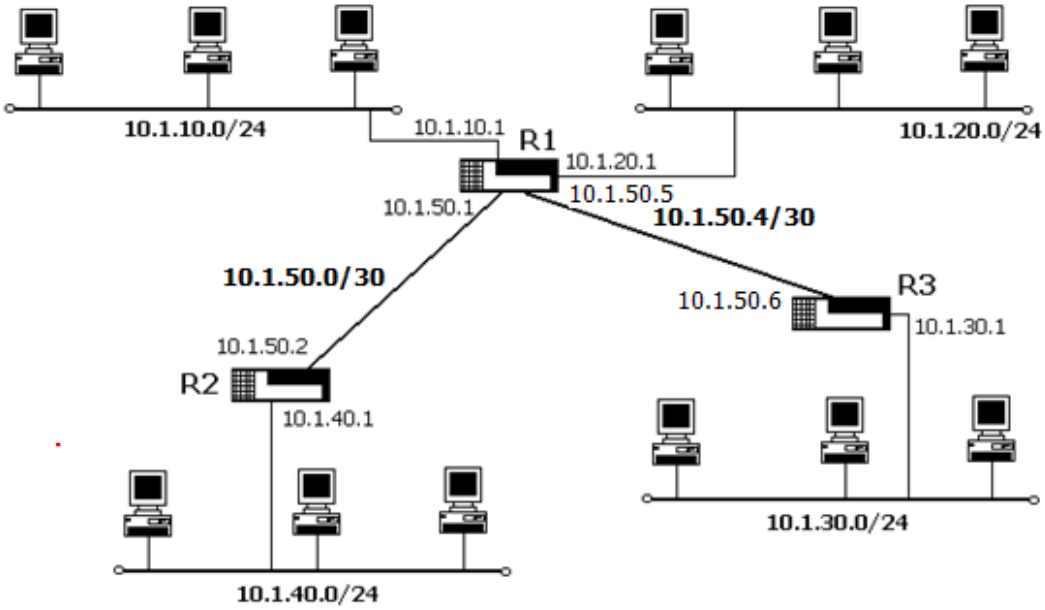
Cuando un dispositivo tiene que transmitir un paquete IP, recorre todas las entradas de la tabla de encaminamiento (desde la primera a la última) buscando en qué entrada está identificada la dirección IP de destino del paquete. Una vez identificada la entrada en la tabla, el paquete IP se transmite dependiendo del valor de la puerta de enlace:

Si es una red conectada directamente, se determinará la dirección MAC de la dirección IP de destino y se transmitirá el paquete.

Si es una red alcanzable o la puerta de enlace por defecto, se determinará la dirección MAC de la puerta de enlace y se transmitirá el paquete.

Configuración de tablas de encaminamiento

Dado el siguiente esquema de red con redes de difusión y redes punto a punto, es posible determinar las entradas de las tablas de encaminamiento de los routers existentes.



Router R1

Destino	Máscara	Puerta de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.1.20.0	255.255.255.0	10.1.20.1
10.1.50.0	255.255.255.252	10.1.50.1
10.1.50.4	255.255.255.252	10.1.50.5
10.1.40.0	255.255.255.0	10.1.50.2
10.1.30.0	255.255.255.0	10.1.50.6

Router R2

Destino	Máscara	Puerta de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.252	10.1.50.2
10.1.10.0	255.255.255.0	10.1.50.1
10.1.20.0	255.255.255.0	10.1.50.1
10.1.30.0	255.255.255.0	10.1.50.1

Router R3

Destino	Máscara	Puerta de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.4	255.255.255.252	10.1.50.6
10.1.10.0	255.255.255.0	10.1.50.5
10.1.20.0	255.255.255.0	10.1.50.5
10.1.40.0	255.255.255.0	10.1.50.5

Cuando en una tabla de encaminamiento varias entradas emplean la misma puerta de enlace, a veces es posible agruparlas en una sola entrada. Una opción es emplear una dirección IP de red que englobe a todas las direcciones IP especificadas en las entradas que tienen la misma puerta de enlace. Otra opción es emplear la entrada de puerta de enlace por defecto.

De esta forma, las tablas de encaminamiento del router R2 y R3 podrían simplificarse como:

Router R2

Destino	Máscara	Puerta de enlace
10.1.40.0	255.255.255.0	10.1.40.1
10.1.50.0	255.255.255.252	10.1.50.2
0.0.0.0	0.0.0.0	10.1.50.1

Router R3

Destino	Máscara	Puerta de enlace
10.1.30.0	255.255.255.0	10.1.30.1
10.1.50.4	255.255.255.252	10.1.50.6
0.0.0.0	0.0.0.0	10.1.50.5

4. Protocolo DHCP

El protocolo DHCP (*Dynamic Host Configuration Protocol)*, definido en la norma RFC 2131, permite la configuración automática de los parámetros del protocolo IP que una máquina necesita para tener conectividad a Internet. Estos parámetros básicos son:

- Dirección IP.
- Máscara de red.
- Dirección de la puerta de enlace por defecto.
- Direcciones IP de los servidores DNS (para realizar la traducción de nombres de dominio, por ejemplo www.ua.es, a direcciones IP).

El funcionamiento del servicio DHCP se fundamenta en un servidor (*DHCP Server*) que proporciona la información de configuración IP a aquellas máquinas que lo solicitan *(DHCP Clients*).

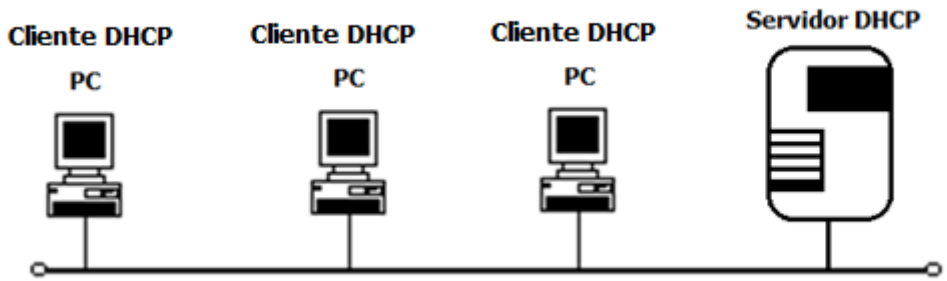


Figura 4. Arquitectura del servicio DHCP.

El protocolo DHCP define un conjunto de mensajes que se intercambian entre el servidor DHCP y los clientes DHCP, conteniendo información de los parámetros IP a configurar. Los mensajes DHCP se intercambian entre los clientes y los servidores empleando el protocolo UDP. Los mensajes DHCP enviados desde los servidores a los clientes emplean como puerto origen el 67 y como puerto destino el 68. Los mensajes DHCP enviados desde los clientes a los servidores emplean como puerto origen el 68 y como puerto destino el 67.

El diálogo básico entre un cliente DHCP y los servidores DHCP que existen en una red se indica en la figura 5. Los mensajes DHCP necesarios para obtener una dirección IP para una máquina, y liberarla posteriormente para que esté disponible a otros equipos son:

DHCP DISCOVER: Mensaje DHCP que envía el cliente a la dirección MAC de difusión y que informa a los servidores DHCP existentes de que una máquina necesita una configuración IP.

DHCP OFFER: Mensaje DHCP que envía un servidor DHCP al cliente (o a todos los clientes existentes) informando de una configuración IP disponible.

DHCP REQUEST: Mensaje DHCP que envía el cliente a la dirección MAC de difusión informando a los servidores DHCP existentes de la configuración IP que solicita (en base a los mensajes DHCP OFFER recibidos).

DHCP ACK: Mensaje DHCP que envía el servidor DHCP al cliente informando de que la configuración IP solicitada se asigna y se reserva por un tiempo (lease time) al cliente.

Cuando expira el tiempo de reserva (lease time) el cliente tiene que renovarlo con un paquete DHCP REQUEST y recibir un paquete DHCP ACK.

DHCP RELEASE: Mensaje DHCP que envía un cliente al servidor DHCP informando de que ya no precisa la configuración IP, por lo que estará disponible en el servidor DHCP para otra máquina.

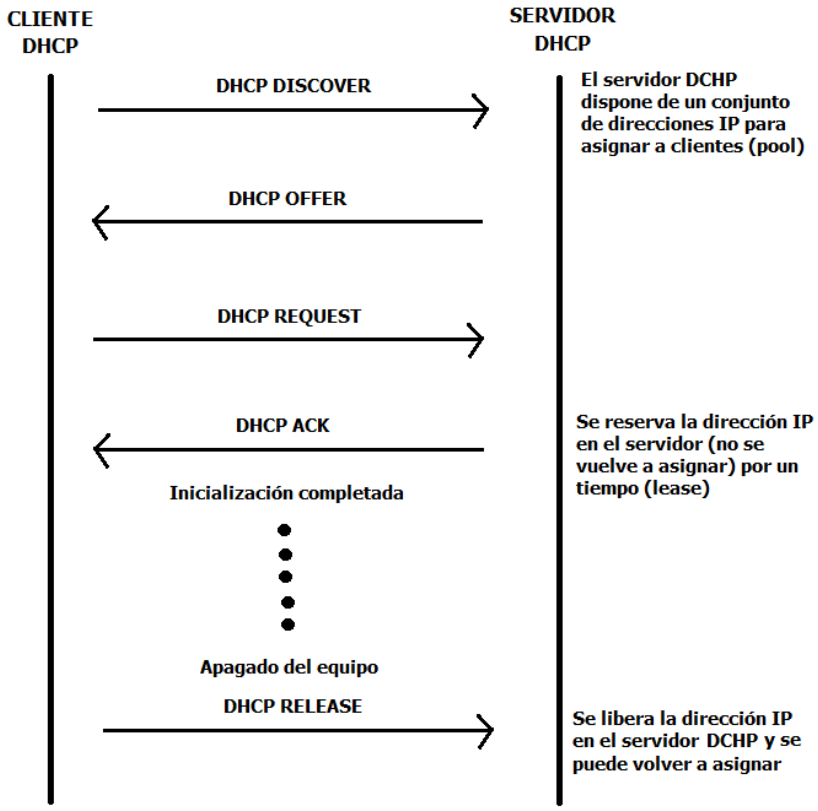


Figura 5. Diálogo entre un cliente DHCP y un servidor DHCP.

En ocasiones, no es posible tener un servidor DHCP en cada segmento de red de una corporación grande (por ejemplo, la Universidad de Alicante). Para ello, se dispone de varios servidores DHCP en una red y los mensajes DHCP se envían entre los servidor DHCP y un dispositivo que existe en cada segmento de red. Este dispositivo, denominado Agente de Reenvío (*BOOTP Relay Agent*) se encarga del traspaso de los mensajes DHCP desde los servidores DHCP a los clientes y viceversa.

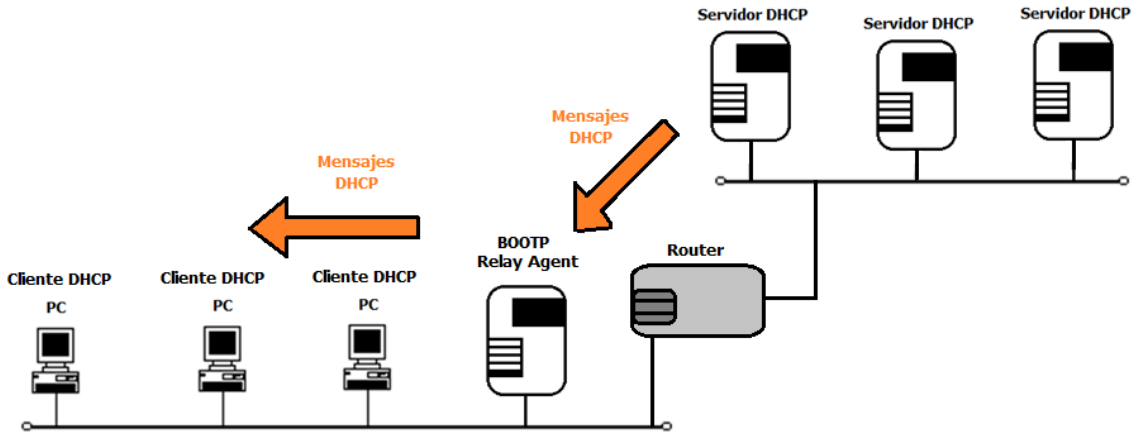


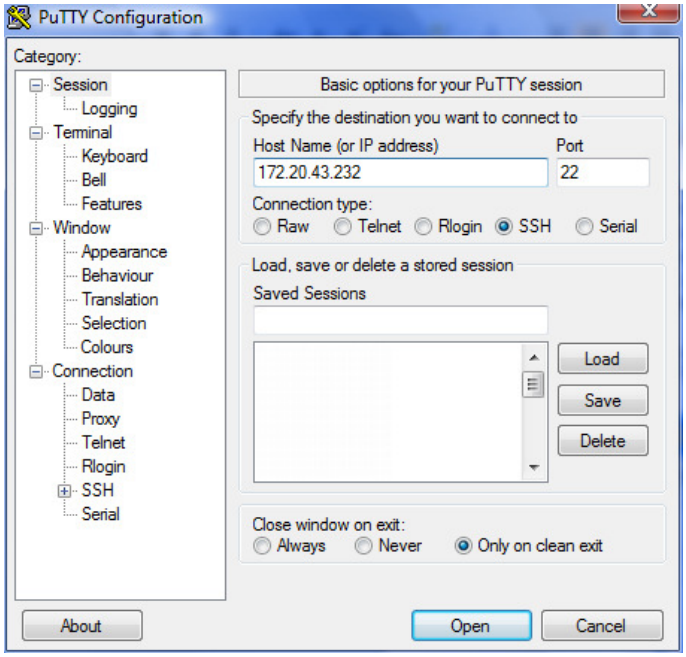
Figura 6. Intercambio de mensajes DHCP con un Agente de reenvío (Relay Agent).

5. Cuestiones a realizar

Acceso a un sistema linux

Para la realización de la práctica 4 se ha habilitado el acceso al equipo Linux2 del laboratorio (que actúa también como router). Desde cada PC se accederá al equipo Linux2 empleando una conexión **telnet segura**. 'Telnet' es un protocolo de acceso remoto a un equipo, accediendo a la consola del sistema en modo texto. La condición de segura se consigue cifrando los paquetes de información entre el cliente y el servidor con el estándar **TLS** (sustituto del no recomendado SSL). Para ello se emplea el servicio **SSH** (*Secure Shell*), que permite el cifrado de una conexión remota telnet.

Para el empleo del servicio SSH se empleará una aplicación ampliamente extendida que se denomina PUTTY.EXE. Esta aplicación está disponible en los PC's del laboratorio L24.



Para realizar la conexión SSH al equipo Linux2 hay que especificar en el campo 'Host Name' la dirección IP 172.20.43.232 y en el campo 'Port' el valor 22, el puerto asociado al servicio SSH. Para establecer la conexión sólo hay que pulsar en el botón '**Open**'.

En el nombre de usuario y contraseña se empleará como **nombre de usuario 'pcxx', donde xx es el número del PC, y la contraseña será la misma que el nombre de usuario**.

5.1 NAT

En el esquema de red del laboratorio, el router R1 emplea la funcionalidad de NAT para permitir la conectividad con Internet.

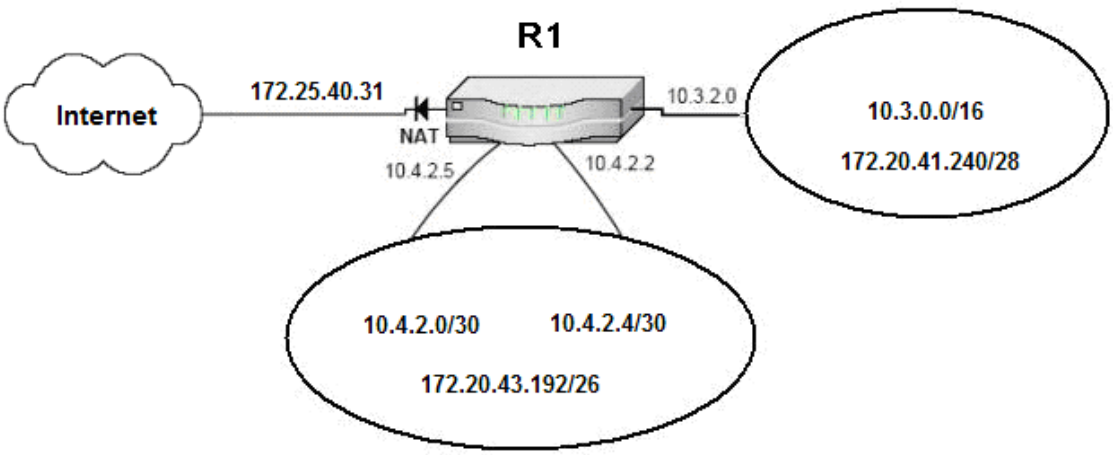


Figura 7. Funcionamiento de NAT en el laboratorio de prácticas

El router R1 está configurado para que todo el tráfico de las redes IP del laboratorio que tenga como destino una dirección IP de Internet (IP pública) sea traducido empleando la dirección IP 172.25.40.31 (**Inside global**).

Para poder comprobar que se realizan las traducciones es necesario visualizar la tabla de traducciones del router R1.

NOTA: El router R1 del laboratorio, cuando realiza traducciones NAT, cambia SIEMPRE el valor del puerto origen (TCP/UDP) por el primer valor de puerto NO empleado en ninguna traducción a partir del valor 4096.

1. Visualización de traducción de paquetes

Desde el PC del alumno, con la aplicación Netcat (**nc.exe**) (**disponible en la carpeta C:\sw\Netcat\ de los PCs del aula L24**) se enviarán paquetes TCP SYN a un servidor web de Internet y se visualizará la traducción de los paquetes SYN (el servidor web al que se accederá no existe y por tanto no se establecerá una conexión).

Cada alumno empleará una dirección IP de Internet distinta, en concreto **150.150.150.64+x**, donde **x** es el número de PC del alumno (es decir, 1, 2, 3, 4, etc.).

Para visualizar la tabla de traducciones NAT del router R1 está disponible en el servidor Linux2 (172.20.43.232) el script '**NAT-R1**' que obtiene el contenido de la tabla de traducciones NAT del router R1 y la visualiza en pantalla. Para ello deberá realizarse una conexión SSH a Linux2 con Putty.

Inicia el monitor de red en el PC del alumno para capturar el tráfico sin traducir generado por el alumno. Emplea un filtrado por la dirección IP 150.150.150.64+x.

Una vez iniciada la captura del tráfico se enviarán paquetes SYN al servicio web del destino 150.150.150.64+x con la aplicación **nc.exe**.

C:\sw\Netcat\nc –nvw 1 150.150.150.64+x 80

Espera la finalización de la aplicación nc que envía paquetes TCP SYN.

En la conexión SSH al servidor Linux2, ejecuta el comando **'NAT-R1**'.

a) Determina cómo se realiza la traducción del paquete SYN en el router R1.

Ten en cuenta que las traducciones están activas durante un cierto tiempo en el router. Si no se reciben paquetes asociados a una traducción, ésta se elimina de la tabla para dejarla libre a otras.

Empleando netcat, envía paquetes SYN con diferentes valores de puerto origen al mismo servidor. Para ello emplea la opción **-p puerto** de netcat. Nótese que el número de puerto origen será distinto para cada alumno.

C:\sw\Netcat\nc -p 2064+x -nv 150.150.150.64+x 80
C:\sw\Netcat\nc -p 3064+x -nv 150.150.150.64+x 80
C:\sw\Netcat\nc -p 4064+x -nv 150.150.150.64+x 80

Recuerda que **x** es el número de PC del aula en el que trabaja el alumno.

b) ¿ Cómo se emplea el puerto origen a la hora de realizar la traducción ?

2. Empleo de la misma dirección Outside Global por varios usuarios.

Trabaja en colaboración con un compañero para determinar cómo funciona NAT cuando varios PCs distintos envían paquetes a la misma dirección IP de Internet.

Para ello debéis emplear el mismo número de puerto origen a un mismo destino. Un alumno ejecuta el comando:

C:\sw\Netcat\nc -p 2064+x –nv 150.150.150.64+x 80

Y el otro ejecuta:

C:\sw\Netcat\nc -p 2064+x -nv 150.150.150.64+x 80

Donde **x** es el mismo valor para ambos alumnos.

Por ejemplo, los alumnos que trabajan en los PC's **PC01** y **PC02** ejecutarán los comandos:

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.65 80

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.65 80

a) Determina qué puertos origen emplea el router R1 en la traducción visualizando la información de la tabla de traducciones.

b) ¿ Qué ocurre si el acceso se produce a números de puerto destino diferentes y la misma dirección IP de Internet ? ¿ Cómo se realiza la traducción ?

Continuando con el ejemplo de los alumnos en los PC's **PC01** y **PC02** se ejecutaría:

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.65 80

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.65 81

c) ¿ Y si el acceso se produce a números de puerto destino diferentes y diferentes direcciones IP de Internet ? ¿ Cómo se realiza la traducción ?

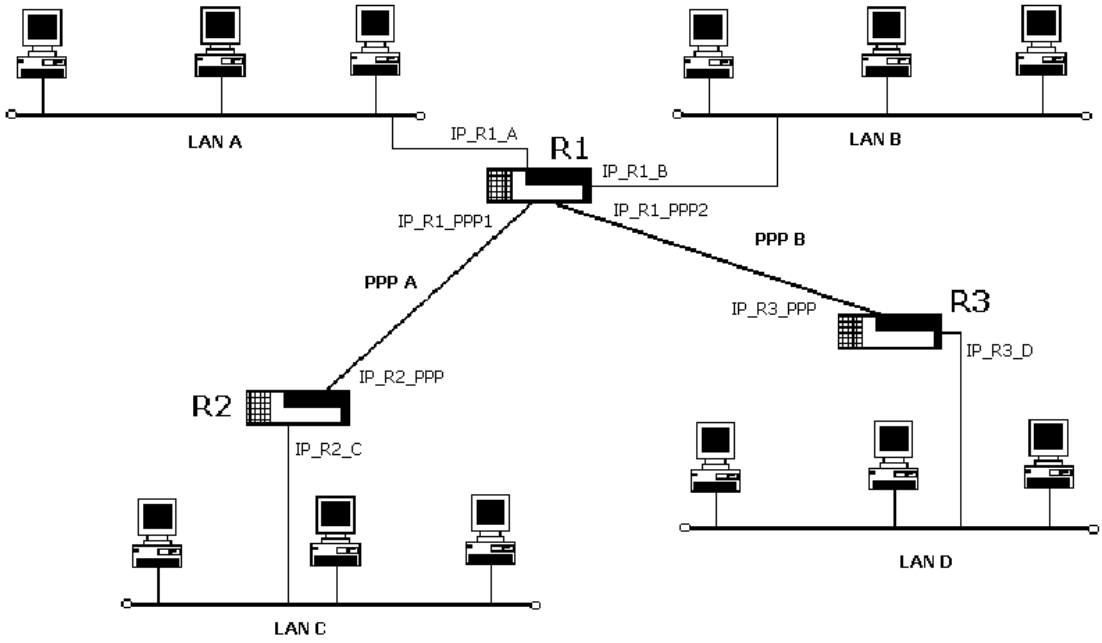
Continuando con el ejemplo de los alumnos en los PC's **PC01** y **PC02** se ejecutaría:

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.65 80

C:\sw\Netcat\nc -p 2065 -nv 150.150.150.66 81

5.2. Construcción de tablas de encaminamiento

Dado el siguiente esquema de red, considera que todo el conjunto es la red **10.1.0.0/16**. Establece las subredes necesarias de manera que las redes de difusión (LAN A, B, C y D) tengan una máscara de 24 bits y en las redes punto a punto se emplee la máscara adecuada. Indica así mismo la tabla de encaminamiento de los routers R1, R2 y R3 para que exista conectividad entre todas las redes de difusión y además, que los routers R2 y R3 sólo tengan **4 entradas** en sus tablas de encaminamiento. **No puede emplearse en la tabla de encaminamiento la entrada de puerta de enlace por defecto (0.0.0.0/0).**



Para ello completa las siguientes tablas:

DIRECCIONAMIENTO IP

Red	Dirección/Máscara		Red	Dirección/Máscara
LAN A			**LAN D**	
LAN B			**PPP A**	
LAN C			**PPP B**	
Dirección IP	**Valor**		**Dirección IP**	**Valor**
IP_R1_A			**IP_R2_C**	
IP_R1_B			**IP_R2_PPP**	
IP_R1_PPP1			**IP_R3_D**	
IP_R1_PPP2			**IP_R3_PPP**	

TABLA DE ENCAMINAMIENTO DEL ROUTER R1

Destino/Máscara	Puerta de enlace

TABLA DE ENCAMINAMIENTO DEL ROUTER R2

Destino/Máscara	Puerta de enlace

TABLA DE ENCAMINAMIENTO DEL ROUTER R3

Destino/Máscara	Puerta de enlace

5.3 Protocolo DHCP

Estudia el intercambio de mensajes DHCP en el laboratorio de prácticas cuando se asignan y liberan direcciones IP en los PCs del aula.

Inicia el monitor de red Wireshark y ejecuta, en una ventana de línea de comandos **con permisos de administrador**, los siguientes comandos:

C:\ipconfig /release (liberación de la dirección IP asignada al equipo).

C:\ipconfig /renew (solicitud de asignación de dirección IP al equipo).

El comando 'ipconfig /renew' finalizará en un tiempo de hasta varios minutos.

Detener la captura del monitor de red y analiza los paquetes del protocolo DHCP capturados.

1. Liberación de dirección IP

Identifica el paquete DHCP Release que ha transmitido tu PC y analiza el contenido del mensaje con el monitor de red.

a) ¿ Cuál es la dirección IP del Servidor DHCP indicado en el contenido del mensaje DHCP (*DHCP Server Identifier*) ?
b) ¿ Coincide la dirección IP del servidor DHCP con la dirección IP a la que se envía el paquete ?

2. Asignación de dirección IP

Identifica el paquete DHCP Discover que ha transmitido tu PC y analiza el contenido del mensaje con el monitor de red.

a) ¿ Se indica a qué servidor DHCP se envía el mensaje ?
b) ¿ A qué dirección IP y MAC va dirigido el paquete con el mensaje DHCP Discover ?
c) ¿ Se solicita en el mensaje DHCP una dirección IP en concreto para el cliente (*Requested IP Address*)?

Identifica los paquetes DHCP Offer capturados y analiza el contenido de los mensajes con el monitor de red.

a) ¿ Cuántos mensajes DCHP Offer se capturan ? ¿ Proceden todos de la misma dirección IP ?
b) ¿ En qué se diferencia el contenido de los mensajes DHCP Offer capturados ?
c) ¿ Crees que existe un Relay Agent en la red del laboratorio ? ¿ Cuál es su dirección IP ?

Identifica los paquetes DHCP Request y DHCP ACK en la captura y analiza el contenido de los mensajes con el monitor de red.

a) ¿ A qué servidor DHCP envía la petición de configuración (DHCP Request) tu PC ?

Selecciona el paquete DHCP ACK procedente del servidor DHCP indicado en el mensaje DHCP Request. Emplea para ello el dato de la opción *DHCP Server Identifier* en el mensaje DHCP Request.

b) ¿ Qué dirección IP y máscara de red se asignará a tu PC ?
c) Indica la dirección IP de la puerta de enlace por defecto que se asignará.
d) ¿ Por cuánto tiempo será válida la asignación de la dirección IP a tu PC (*Lease time*) ?

6. Documentación complementaria

- Documentación **man** de Linux Red Hat.
- **RFC 2663** IP Network Address Translator (NAT). IETF.
- **RFC 2131** Dynamic Host Configuration Protocol. IETF.