TEMA 0: Introducción a los servicios de red e internet

Introducción

1. La arquitectura TCP/IP, el modelo Cliente/Servidor y los servicios en red

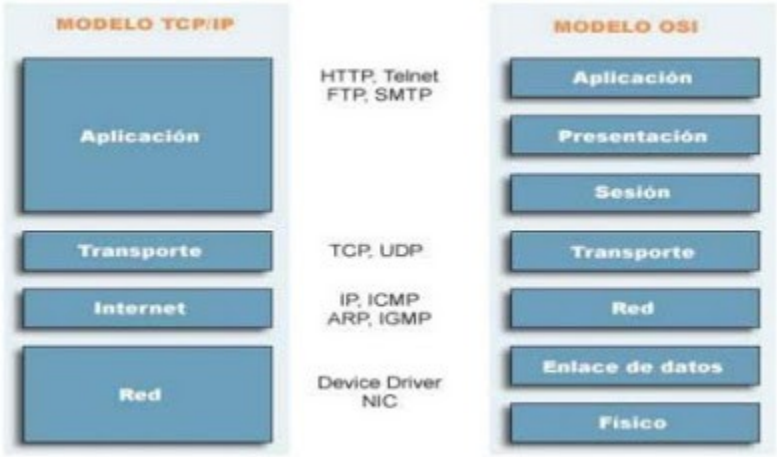
Desde un principio la arquitectura TCP/IP ha estado orientada a funcionar en un entorno cliente/servidor, lo que facilita enormemente la implantación de diversos servicios de red tanto en redes locales como en Internet.

1.1. Arquitectura TCP/IP y modelo OSI

OSI ofrecía un modelo muy bien diseñado, pero este modelo era completamente teórico, mientras que TCP/IP, que era anterior, se encontraba en pleno funcionamiento cuando OSI surgió. La arquitectura TCP/IP nos proporciona una estructura y una serie de normas de funcionamiento para poder interconectar sistemas.

En cada capa existen una serie de protocolos que ofrecen unas normas estrictas a seguir para el diálogo entre los sistemas. Cada protocolo se apoya en los protocolos de las capas inferiores para realizar su labor y, a su vez, ofrece sus servicios a las capas superiores. Es una de las características fundamentales de la arquitectura TCP/IP.

Así, por ejemplo, los protocolos FTP o SNMP de la capa de aplicación, se apoyan en los protocolos TCP o UDP de la capa de transporte y estos a su vez usan el protocolo IP de la capa de red.
La imagen muestra la correspondencia entre los niveles de OSI y los de TCP/IP.



1.2. Modelo Cliente/Servidor

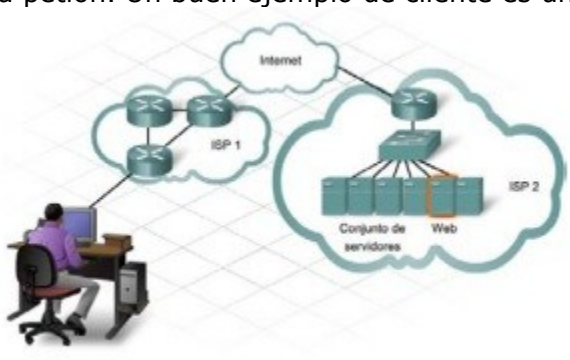
Para la comunicación de aplicaciones a través de una red se emplean fundamentalmente tres paradigmas:

- **Modelo cliente/servidor**: es el más extendido y utilizado. En él se distingue entre un proceso cliente que solicita servicios, y un proceso servidor que presta el servicio al cliente.

- **El modelo entre pares o P2P** (Point To Point) todos los nodos de la red son responsables por igual en la comunicación de las aplicaciones y no existe un elemento que centralice la comunicación.
- **El modelo híbrido**, el servidor no presta el servicio como tal, sino que generalmente pone en contacto a los clientes para que estos se comuniquen entre si.

El término **servidor** hace referencia a un host que ejecuta una aplicación de software que proporciona información o servicios a otros hosts conectados a la red. Un ejemplo conocido de dicha aplicación es un *servidor Web*. Existen millones de servidores conectados a Internet que proporcionan servicios como sitios Web, correo electrónico, transacciones financieras, descargas de música, etc. Un factor fundamental para permitir el funcionamiento de estas interacciones complejas es que todos emplean estándares o protocolos acordados.

Para solicitar y ver una página Web, el usuario utiliza un dispositivo que ejecuta software cliente de Web. **Cliente** es el nombre que se le da a una aplicación informática que se utiliza para acceder a información almacenada en un servidor, aunque también se usa el término Cliente para referirse al equipo que hace la petión. Un buen ejemplo de cliente es un explorador Web.



La característica clave de los sistemas cliente-servidor es que *el cliente envía una solicitud a un servidor, y éste responde ejecutando una función, como enviar información al cliente.* La combinación de un explorador Web y un servidor Web es quizás el ejemplo que más se utiliza en un sistema cliente-servidor.

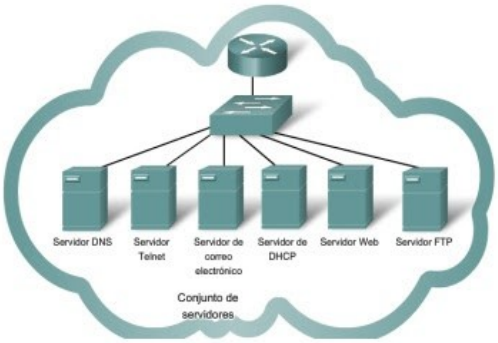
1.3. Los Servicios de Red

Un ***servicio red red*** es una función o prestación que ofrecen las **aplicaciones** y los **protocolos,** a los **usuarios** o a otras **aplicaciones**.
En este sentido, las aplicaciones son sistemas software que se comunican e intercambian información con otras aplicaciones, con ayuda de los **protocolos de la arquitectura TCP/IP**, tanto a nivel de aplicación como de niveles inferiores.

Es importante no confundir los protocolos del nivel de aplicación, con las aplicaciones que los usan:

- Las ***aplicaciones*** son los diferentes programas instalados por el usuario o que forman parte del S.O, por ejemplo, para el "servicio web", las aplicaciones en el servidor podrían ser Apache, IIS (Internet Information Server) y las aplicaciones en el cliente serían los navegadores mozilla Firefox, etc.. Las aplicaciones usan los protocolos TCP/IP para comunicarse.

- Los ***protocolos*** son normas concretas que detallan cómo se produce la comunicación entre sistemas para ofrecer los servicios de red. Por ejemplo: HTTP, HTTPS, etc. Para realizar su función, los protocolos del nivel de aplicación usan los protocolos de niveles inferiores para funcionar. P.e., el protocolo de aplicación Telnet usa el protocolo TCP de la capa de transporte, mientras que el protocolo de aplicación DHCP usa el protocolo UDP de la capa de transporte.



Ejemplos de servicios: Servidores de autenticación de usuarios, Servicio de directorio, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Correo electrónico, Servicio de impresión, Network File System (NFS).

2. Nivel de red en TCP/IP. El protocolo IP

A nivel de red se realiza el direccionamiento de los dispositivos y el encaminamiento de la información a través de la red. Todo ello se lleva a cabo con el protocolo IP, que es el principal protocolo del nivel de red de TCP/IP. El esquema de direccionamiento usado en cada nodo de la red y los procesos de encaminamiento, que se ejecutan en los dispositivos que interconectan las redes, son las funciones principales de este protocolo. La comunicación a nivel IP se hace mediante unidades de datos llamada "**datagramas**", que siguen el formato especificado en el protocolo.
Actualmente se usa mayoritariamente la versión 4 del protocolo (Ipv4), pero la vesión Ipv6 está desarrollada y empieza a implantarse.

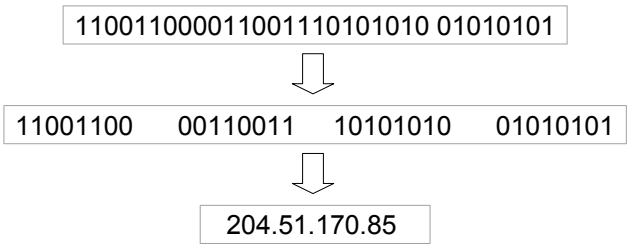
2.1 Direccionamiento IP

El protocolo IP proporciona conectividad extremo a extremo, por lo que debe ser capaz de direccionar de forma única todos los dispositivos conectados en la red y, por extensión, en toda Internet. *El direccionamiento IP no es físico, sino lógico,* lo que significa que es independiente del dispositivo físico al que se asigna y puede ser modificado por software.
Un dirección IP no identifica a un ordenador en la red, sino a una interfaz de red de un equipo de la red. Por eso un mismo equipo puede tener varias direcciones IP, una por interfaz, y eso hace posible que un mismo equipo pueda estar conectado a varias redes de forma simultánea.

2.1.1. Formato de direcciones IP

Una dirección IP es un número binario de 32 bits, lo que permite direccionar 2^{32} equipos (4.294.967.296) . Normalmente, para facilitar la legibilidad de direcciones IP se usa la notación decimal con puntos. Así, una IP se divide en 4 grupos de 8 bits, escribiendo cada uno de ellos en

decimal, y separando los cuatro números resultantes con puntos. Por tanto, una dirección IP estará formada por cuatro números entre 0 y 255 separados por puntos:



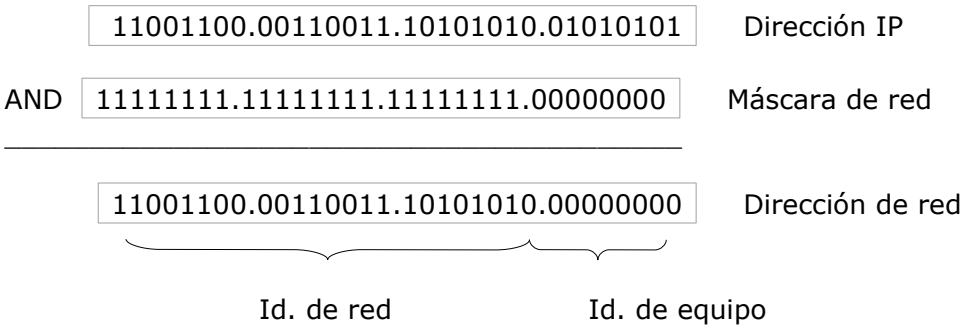
A efectos de direccionameinto y encaminamiento, cada IP consta de dos partes:

- **Identificador de la red**, que identifica la red en la que se encuentra el dispositivo
- **Identificador del host** dentro de la red

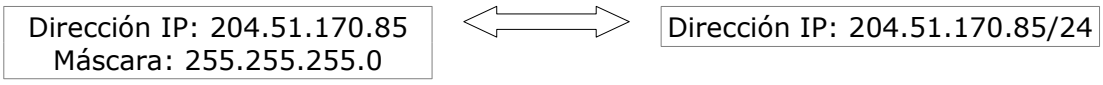
Todos los host de la misma red comparten la parte de identificador de red. Esta estructura se parece a la de un sistema de teléfono fijo con prefijo + número local.
El identificador de la red puede tener más o menos bits según el tamaño de la red: Para redes grandes, el identificador de la red tendrá pocos bits para dejar el resto de bits de la IP como identificador de host y así la red pueda contener muchos hosts. En redes pequeñas, el identificador de red puede tener más bits ya que se necesitan menos bits para identificar los equipos.

2.1.2. Máscara de red

La máscara se usa para diferenciar el prefijo de la dirección IP (identificador de red) de la parte correspondiente al identificador del host. La máscara de red es un número de 32 bits que tiene a '1' las posiciones de correspondientes al prefijo o identificador de red, y a '0' las posiciones correspondientes al identificador del host. Siempre es un número con x unos a la izquierda y el resto ceros.



La máscara también puede expresarse en notación CIDR (Classless Inter-Domain Routing) consistente en situar un sufijo a continuación de la dirección IP que indica cuántos bits d ella máscara de red están a 1:



2.1.3. Clases de direcciones IP

El identificador de red puede tener cualquier longitud. Sin embargo, para facilitar el proceso de encaminamiento se usan una serie de máscaras predeterminadas para así facilitar el proceso de encaminamiento. Así surge el conceptor de **clases de direccione**s:

- **Clase A**: Las direcciones IP usan el primer byte para el identificador de red y los tres restantes para el identificador del host. Se usa para redes grandes, con muchos hosts (2^{24}=4.294.967.296 hosts). La máscara de red equivale a 255.0.0.0 o /8
- **Clase B**: Las direcciones IP usan los dos primeros bytes para el identificador de red y los dos restantes para el identificador del host. Se usa para redes medianas, con un número medio de hosts (2^{16}=4.294.967.296 hosts). La máscara de red equivale a 255.255.0.0 o / 16.
- **Clase C**: Tres bytes para el identificador de red y uno para el identificador del host. Se usa para redes pequeñas, con pocos hosts (2^{8}=256 hosts). La máscara de red equivale a 255.255.255.0 0 /24
- **Clase D**: Se usa para multicast, es decir, envío de datagramas a un grupo de quipos de la red. No diferencian entre identificador de red y de host.
- **Clase E**: Reservadas para uso experimental en proyectos de investigación.

2.1.4. Direcciones especiales

Dentro del conjunto de direcciones IP hay algunas particularmente importantes que merecen una explicación aparte:

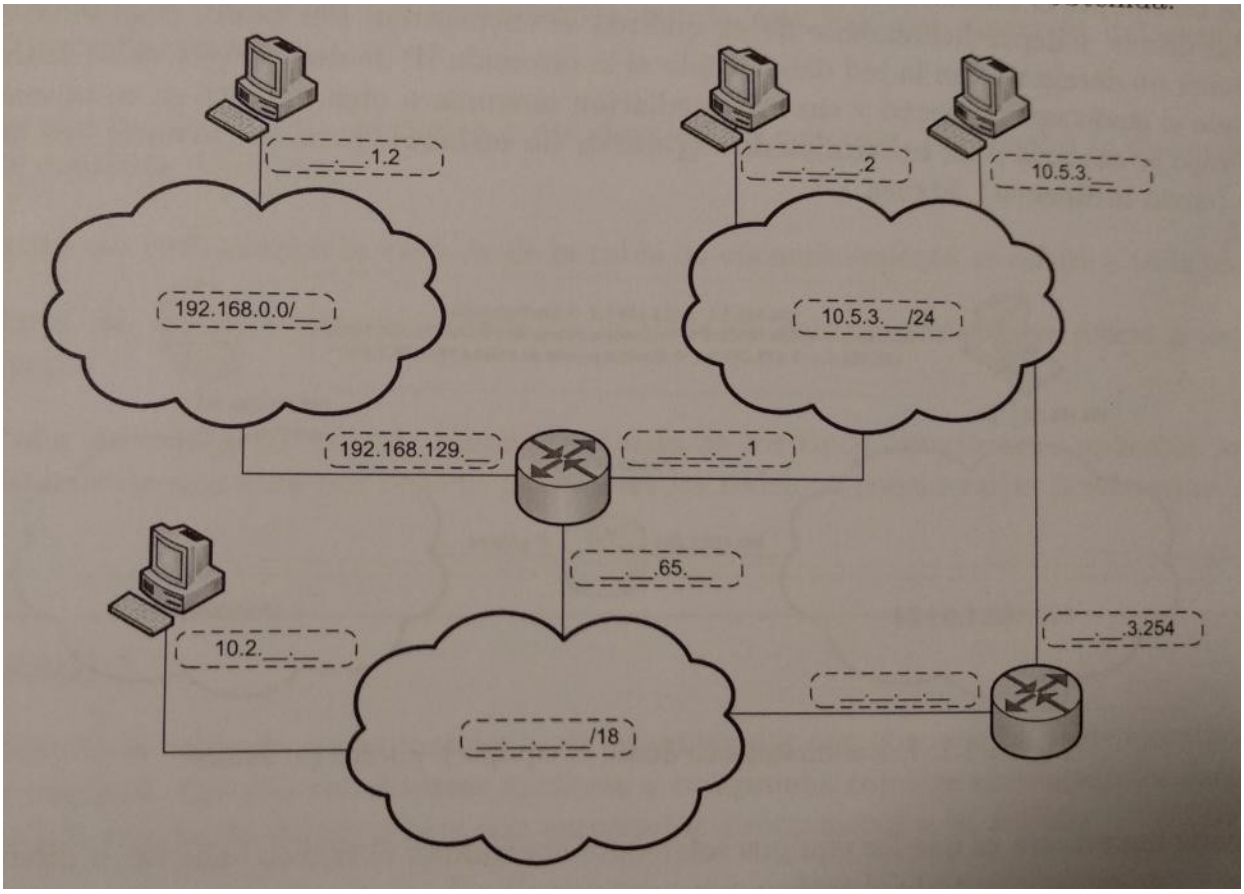
- **Dirección de red:** identifica al conjunto de la red. En ella, la parte correspondiente a la identificación del host tiene todos los bits a 0. P.e., la dirección IP de host 204.51.170.85/24 tendría la IP de red 204.51.170.0/24
- **Dirección de difusión limitada (broadcast):** Se usa para mandar un mensaje de difusión o broadcast a todos los equipos de la red. Los routers no reenvían estos paquetes. Es la misma para todas las redes (255.255.255.255)
- **Dirección de difusión dirigida**: Se usa para mandar un mensaje de difusión o broadcast al conjunto de dispositivos de la red especificada. Se usa la IP de red con los bits correspondientes al host todos a uno. Por ejemplo, la IP de broadcast de la red 204.51.170.0/24 sería 204.51.170.255.
- **Dirección de bucle local.**: Se usa para referenciar internamente a la interfaz del propio equipo. Se usa la IP 127.0.0.1

2.1.5. Direcciones públicas y privadas

Dentro del espacio de direcciones hay algunas que se han reservado para uso privado, es decir, para redes locales. Estas direcciones son accesibles desde Internet. Se distingue entre:

- **Direcciones públicas**: Identifican a un dispositivo conectado a Internet.
- **Direcciones privadas**: Se reservan para redes privadas o intranets y no pueden emplearse en Intenet. Son las pertenecientes a las siguientes redes: 10.0.0.0/8, 172.16.0.0/12 (redes entre la 172.16.0.0/16 y 172.31.0.0/16) y 192.168.0.0/16. Los routers conectados a redes públicas (Internet) descartan el tráfico dirigido a direcciones privadas como medida de seguridad.

Actividad 1: A partir del siguiente diagrama de red completa los espacios con la información adecuada relativa a direcciones de red y direcciones de los diversos dispositivos. La solución no es única.



2.2. Encaminamiento IP

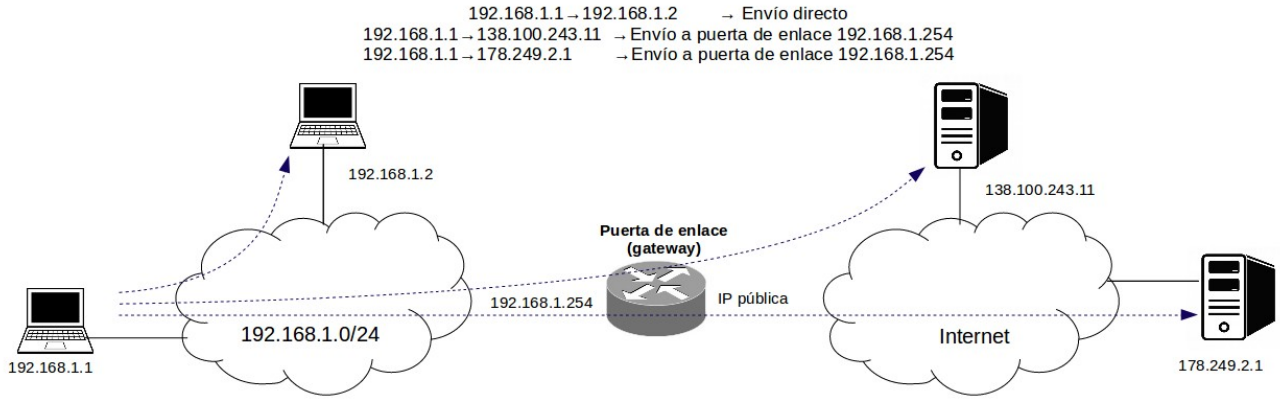
El encaminamiento IP es el proceso de llevar un datagrama desde una máquina origen a una máquina destino, independientemente de si la máquina destino está en la misma red o en otra distinta. El protocolo IP es el responsable de este encaminamiento.

2.2.1. Encaminadores o routers

Son dispositivos de nivel 3 que enlazan las direrentes redes que forman parte de una "red de redes". Un router estará conectado al menos a dos redes y **realizará el encaminamiento de todo el tráfico de datagramas que pase por él**. Para ello usará las **tablas de encaminamiento** que veremos más adelante.

Además de los routers, los propios **equipos** también van a participar en el encaminamiento. De hecho, el encaminamiento se inicia incluso antes de que un equipo coloque un datagrama en la red.

A nivel de dirección IP y desde el punto de vista de un equipo, el mundo se divide en dos: *las direcciones que están en su misma red, y las que no, independientemente de que qué otra red estén.*
Por tanto, cuando un equipo quiera poner un datagrama en la red, debe decidir si la IP de destino está un su misma red, con lo que el envío será **directo** y sin intermediación alguna, o bien no está en su misma red, en cuyo caso se enviará a un encaminador (puerta de enlace), para que lo encamine a su destino (envío **indirecto**).



* Un equipo sólo encamina tráfico saliente, mientras que un router encamina todo el tráfico que pasa por ellos. Por eso los routers son "algo más" que un equipo con dos tarjetas.

El router, cuando recibe un datagrama, debe encaminarlo. Pueden ocurrir dos cosas:

- Que el datagrama vaya dirigido a una red conectada directamente al router, en cuyo caso la entrega es directa.
- Que el datagrama vaya dirigido a una red no conectada directamente al router. En este caso el router enviará el datagrama a otro enrutador siguiendo lo especificado en su tabla de enrutamiento. Este proceso se repite hasta llegar a la red de destino o hasta agotar el TTL del datagrama.

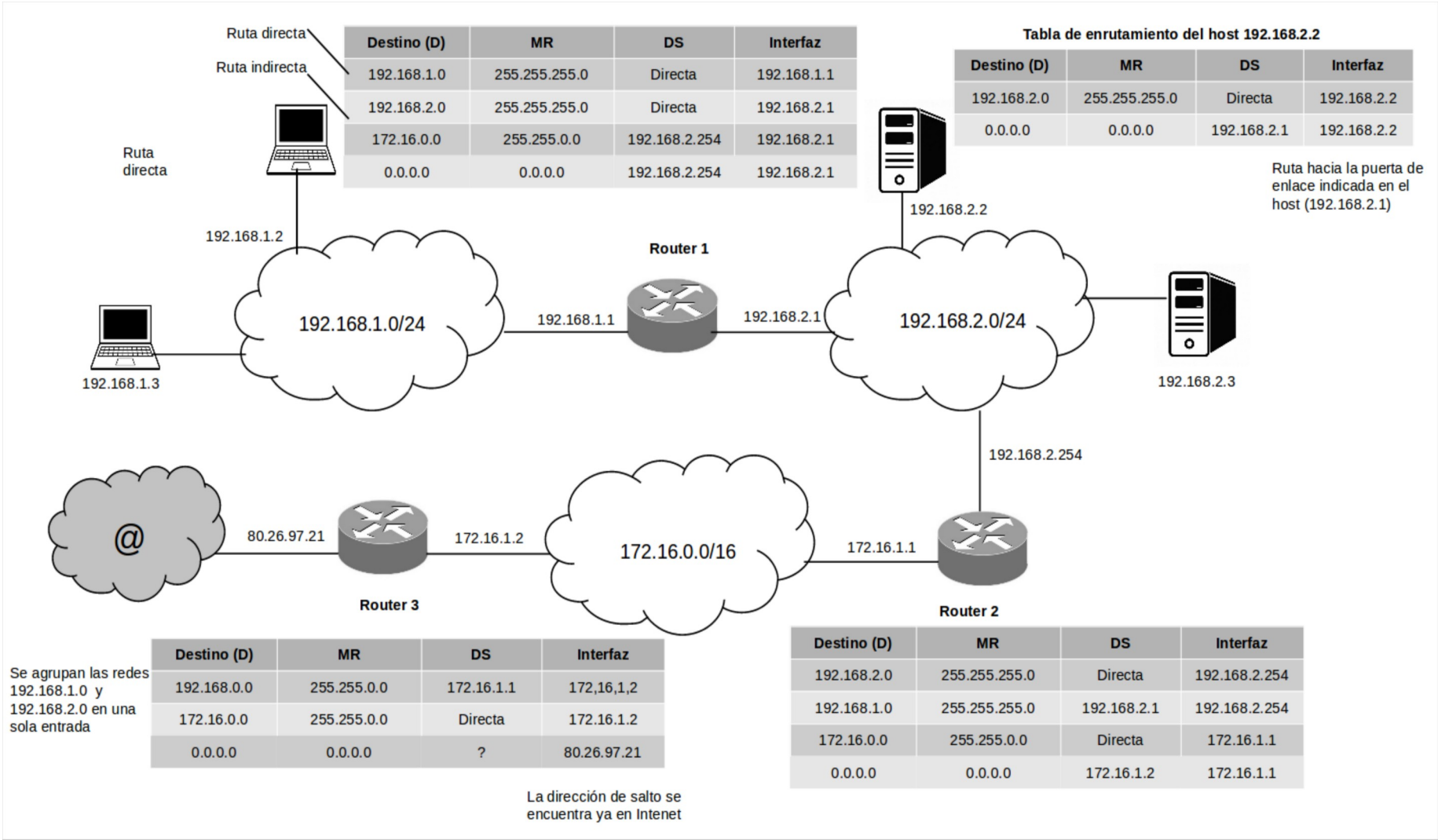
2.2.2. Tablas de encaminamiento

Las tablas de encaminamiento almacenan la información necesaria para realizar el encaminamiento de los datagramas, y están implementadas tanto en los routers como en los hosts.
La información que contienen depende de protocolo de encaminamiento usado, pero en general, los campos más importantes son:

- **Destino (D):** Dirección IP de una red o host
- **Máscara de red (MR**): asociada al destino anterior. Sirve para determinar exactamente todas las IP que incluye.
- **Dirección de salto (DS):** Dirección IP a la que se enviará el datagrama si su dirección IP de destino coincide con la especificada por *destino* y *máscara de red.*
- **Interfaz**: Dirección IP del encaminador por el que hay que enviar el datagrama a la dirección de salto.

Cada registro de la tabla encamina a un destino concreto. En general se distinguen tres tipos de destinos diferentes:

- **Ruta de red:** Cuando la entrada de la tabla de encaminamiento se refiere a toda una red
- **Ruta de host**: Cuando la entrada de la tabla de encaminamiento se refiere a un equipo o host
- **Ruta por defecto**: Cuando ninguna entrada de las anteriores es aplicable (porque el destino no coincide con ninguna entrada) se usa una ruta por defecto.



Destino (D)	MR	DS	Interfaz
192.168.1.0	255.255.255.0	Directa	192.168.1.1
192.168.2.0	255.255.255.0	Directa	192.168.2.1
172.16.0.0	255.255.0.0	192.168.2.254	192.168.2.1
0.0.0.0	0.0.0.0	192.168.2.254	192.168.2.1

Tabla de enrutamiento del host 192.168.2.2

Destino (D)	MR	DS	Interfaz
192.168.2.0	255.255.255.0	Directa	192.168.2.2
0.0.0.0	0.0.0.0	192.168.2.1	192.168.2.2

Ruta hacia la puerta de enlace indicada en el host (192.168.2.1)

Se agrupan las redes 192.168.1.0 y 192.168.2.0 en una sola entrada

Destino (D)	MR	DS	Interfaz
192.168.0.0	255.255.0.0	172.16.1.1	172,16,1,2
172.16.0.0	255.255.0.0	Directa	172.16.1.2
0.0.0.0	0.0.0.0	?	80.26.97.21

La dirección de salto se encuentra ya en Intenet

Destino (D)	MR	DS	Interfaz
192.168.2.0	255.255.255.0	Directa	192.168.2.254
192.168.1.0	255.255.255.0	192.168.2.1	192.168.2.254
172.16.0.0	255.255.0.0	Directa	172.16.1.1
0.0.0.0	0.0.0.0	172.16.1.2	172.16.1.1

2.2.3. Protocolos de encaminamiento

Al arrancar los equipos, tanto routers como hosts, las tablas de encaminamiento se inicializan con las rutas correspondientes a las redes adyacentes al mismo. A partir de ese momento se pueden seguir dos estrategias para configurar las tablas de encaminamiento:

- **Encaminamiento estático**: La configuración de las tablas de encaminamiento se hace de forma manual. Es una estrategia no adaptativa lo que significa que cualquier cambio que se produzca en la topología de red debe ser supervisado por el administrados para evitar rutas imposibles o buclas indeseados. Por eso es muy sensible a fallos y solo recomendables en redes pequeñas.
- **Encaminamiento dinámico:** El propio encaminador actualiza sus tablas gracias al uso de protocolos específicos como RIP (Routing information protocol) , OSPF (Open Shortest Path First) y BGP (Border Gateway Protocol) que permiten que los encaminadores se intercambien información de encaminamiento para mantener sus tablas lo más actualizadas posible.

3. Nivel de transporte en TCP/IP. Protocolos TCP y UDP

En los sistemas operativos multitarea y en red actuales es habitual que las comunicaciones involucren a varios procesos dentro de la misma máquina y a varias máquinas dentro de la misma red.

El protocolo IP nos permite comunicar dos máquinas remotas haciendo que los datagramas puedan ir del origen al destino, pero como a ese nivel sólo tenemos las IP's como mecanismo de diferenciación, no podríamos, por ejemplo, mantener varias comunicaciones simultáneas entre los mismos equipos, ya que a nivel IP no podríamos diferenciar los datagrams de una u otra.

El **nivel de transporte** provee de elementos para diferenciar y gestionar múltiples orígenes y destinos, y múltiples comunicaciones simultáneas en cada equipo.

3.1. Puertos de comunicaciones

Los protocolos de nivel de transporte implementan el concepto de puerto de comunicadiones, que nos permite identificar los procesos del nivel de aplicación entre los que está establecida una comunicación.

Cada proceso del nivel de aplicación tiene asociado uno o varios puertos. Cada puerto se identifica por un número binario de 16 bits, por lo que habrá 2^{16}=65535 puertos distintos.

Existen varias clases de puertos según su uso:

- **Puertos conocidos (0-1023):** Los puertos de destino que están asociados a aplicaciones y servicios de red comunes se identifican como puertos conocidos.
  La siguiente tabla muestra algunos de los puertos conocidos más comunes:

Número de puerto de destino	Abreviatura	Definición
20	Datos de FTP	Protocolo de transferencia de archivos (para transferir datos)
21	Control de FTP	Protocolo de transferencia de archivos (para establecer conexión)
23	TELNET	Red de teletipo
25	SMTP	Protocolo simple de transferencia de correo
53	DNS	Servicio de nombres de dominio
67	Cliente de DHCP v4	Protocolo de configuración dinámica de host (cliente)
68	Servidor de DHCP v4	Protocolo de configuración dinámica de host (servidor)
69	TFTP	Protocolo trivial de transferencia de archivos
80	HTTP	Protocolo de transferencia de hipertexto
110	POP3	Protocolo de oficina de correos (versión 3)

- **Puertos registrados (1024 - 49151) :** Se pueden utilizar como puertos de origen o de destino. Las organizaciones los utilizan para registrar aplicaciones específicas no estándar, como las aplicaciones IM (Internet Messages).

- **Puertos dinámicos (49152 - 65535):** A menudo se utilizan como puertos de origen (para iniciar conexiones desde el cliente). Estos puertos pueden ser utilizados por cualquier aplicación.

La correspondencia entre procesos y puertos se hace de dos formas distintas:

- **Asignación estática:** Los puertos conocidos están reservados para aplicaciones estándar y solo pueden ser usados por esos procesos.

- **Asignación dinámica**: Cuando un proceso necesita un puerto y este no se asigna estáticamente, el sistema operativo le asigna uno que está disponible (1024-65535).

En el nivel de transporte se diferencian dos protocolos independientes (TCP y UDP) y los dos manejan el concepto de puerto. Los puertos de TCP y UDP son totalmente independientes, por lo que no tiene nada que ver el puerto 53 de TCP con el mismo puerto en UDP.

3.2. Protocolo UDP

El protocolo **UDP** (User Datagram Protocol) proporciona un servicio no orientado a la conexión (al igual que IP) con todo lo que supone: sin establecimiento de conexión previo a la transmisión, sin control de flujo (se podrían entregar segmentos duplicados o desordenados),etc.

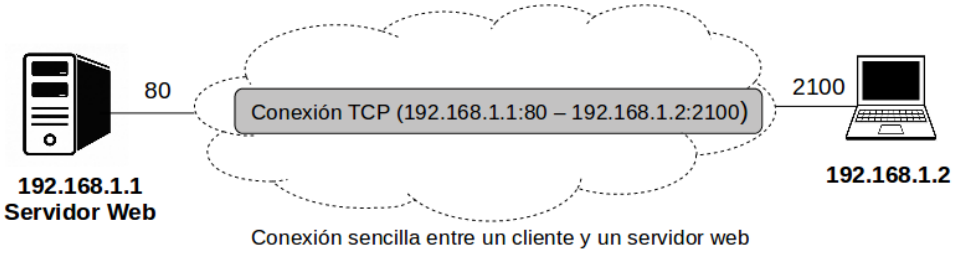
Al ser un protocolo muy básico suele usarse en casos en los que es más importante la velocidad de transmisión que la fiabilidad, o en aplicaciones con requerimientos sencillos de tipo petición-respuesta como DHCP, DNS, streaming u vozIP.

3.3. Protocolo TCP

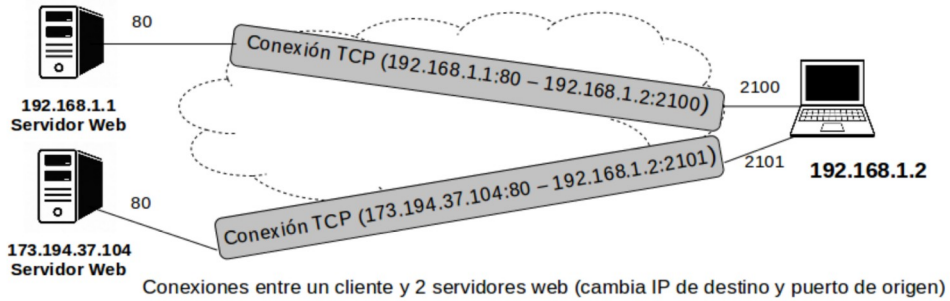
El protocolo **TCP** (Transmission Control Protocol) proporciona un servicio orientado a la conexión por lo que es muy diferente de UDP. TCP obliga al establecimiento previo de una conexión antes de empezar a transmitir y ofrece control de flujo y de errores con lo que garantiza al nivel de aplicación un servicio fiable.

3.3.1. Conexiones TCP

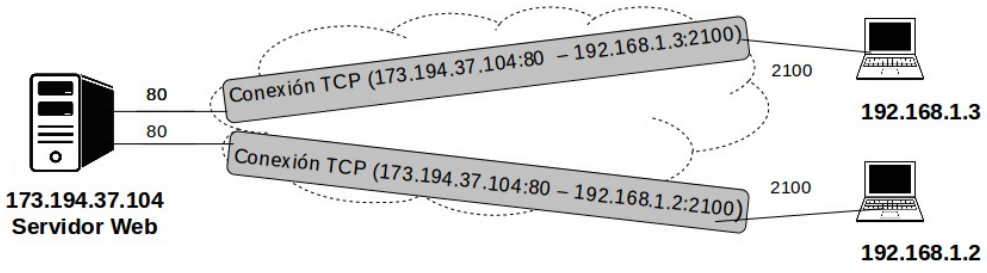
La **conexión TCP** es el paso previo imprescindible para inicar una comunicación. Una vez establecida la conexión, cualquiera de los dos extremos puede empezar a transmitir y también terminar la conexión en el momento que lo desee. La conexión TCP se define de forma única para los cuatro elementos que definen la comunicación: **(Dirección IP origen, puerto TCP origen)=> (dirección IP destino y puerto TCP destino)**. No puede haber dos conexiones TCP que tengan en común estos cuatro elementos.



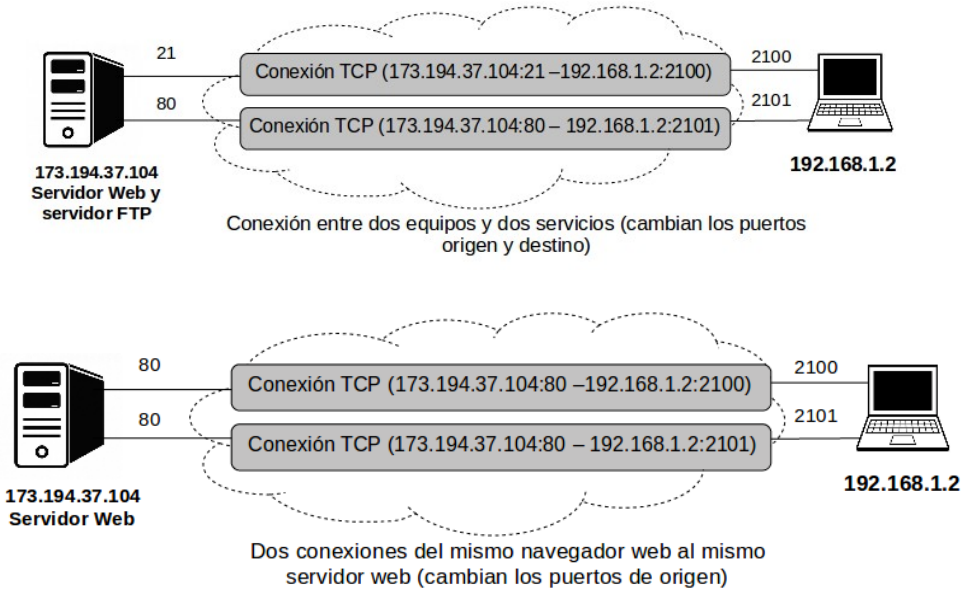
Conexión sencilla entre un cliente y un servidor web



Conexiones entre un cliente y 2 servidores web (cambia IP de destino y puerto de origen)



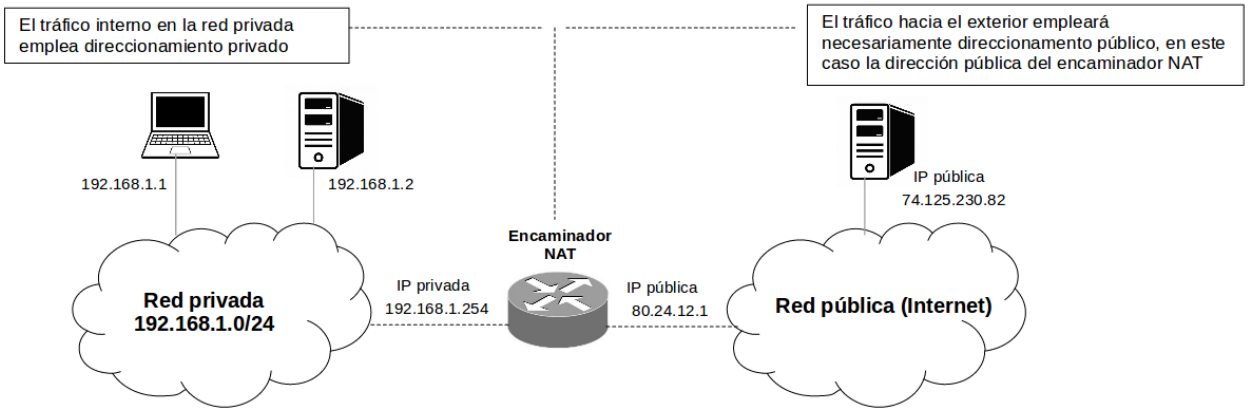
Conexiones entre 2 clientes y un servidor web (cambia IP origen)



4. Traducción de direcciones de red – NAT y PAT

El crecimiento exponencial del número de ordenadores conectados a Internet y la consiguiente demanda de direcciones IP públicas ha provocado que el espacio de direcciones IP disponibles empiece a agotarse. Para paliar en la medida de lo posible esta carencia se aplican una serie de técnicas para aprovechar al máximo el espacio de direcciones. Surgen así, entre otras, las CIDR (Classless Interdomain Routing) y Supernetting.

Además existen otro tipo de técnicas que permiten limitar el número de equipos con IP pública conectados directamente a Internet. La principal es la **traducción de direcciones de red – NAT** (*Network Address Translation),* que permite que varias direcciones IP privadas puedan acceder a Internet a través de una única IP pública (*por definición, los datagramas con dirección IP origen privada no pueden circular por Internet*). Gracias a esta técnica es posible que los equipos de una LAN con IP privada puedan, a través de un proceso de traducción, conectarse a Internet mediante una dirección IP pública común (generalmente la IP pública del router). Esta técnica proporciona además más seguridad para los equipos de la red interna, ya que permite ocultar sus direcciones originales cuando los datagramas van al exterior.



4.1. Funcionamiento

El uso más habitual de **NAT** es que una red privada pueda usar IP's privadas internamente y tener una o varias IPis públicas asignadas al router que le da salida a Internet, de forma que todos los dispositivos de la red interna salgan a Internet a través de las direcciones IP públicas.

Para que el sistema NAT funcione es necesario que el encaminador que da acceso a Internet reescriba algunos datos en los datagramas que encamina. En función de la información que se modifique tenemos varios tipos de **NAT**:

- **NAT básico**: sólo modifica la dirección IP (NAT a nivel de red)
- **NAPT** (Network Adress Port Translation) / **PAT** (Port Address Translation): Además de la dirección IP también se modifican los puertos usados en la comunicación a nivel de transporte. También se le conoce como NAT a nivel de transporte y, de hecho, ha sustituido al NAT, de forma que a partir ahora lo que llamamos NAT se refiere a NAPT.

Vamos a centrar nuestro estudio en NAPT (NAT a partir de ahora), que resulta mucho más versátil y nos permitirá cambiar los puertos usados en las máquinas de la red interna al salir fuera de nuestra red.

Por tanto, la información de los datagramas que debe ser modificada al pasar por un router NAT es la relativa a direcciones IP y puertos. Más concretamente:

- Se modifica la **IP de origen y el puerto de origen** en el tráfico saliente de la red privada.
- Se modifica la **IP de destino y el puerto de destino** en el tráfico entrante a la red privada.

El encaminador NAT dispondrá de una **tabla NAT** con los cambios que se realizan en el tráfico saliente para así poder deshacer dichos cambios cuando vuelve la respuesta en forma de tráfico entrante. Esta tabla dispondrá al menos de los siguientes campos:

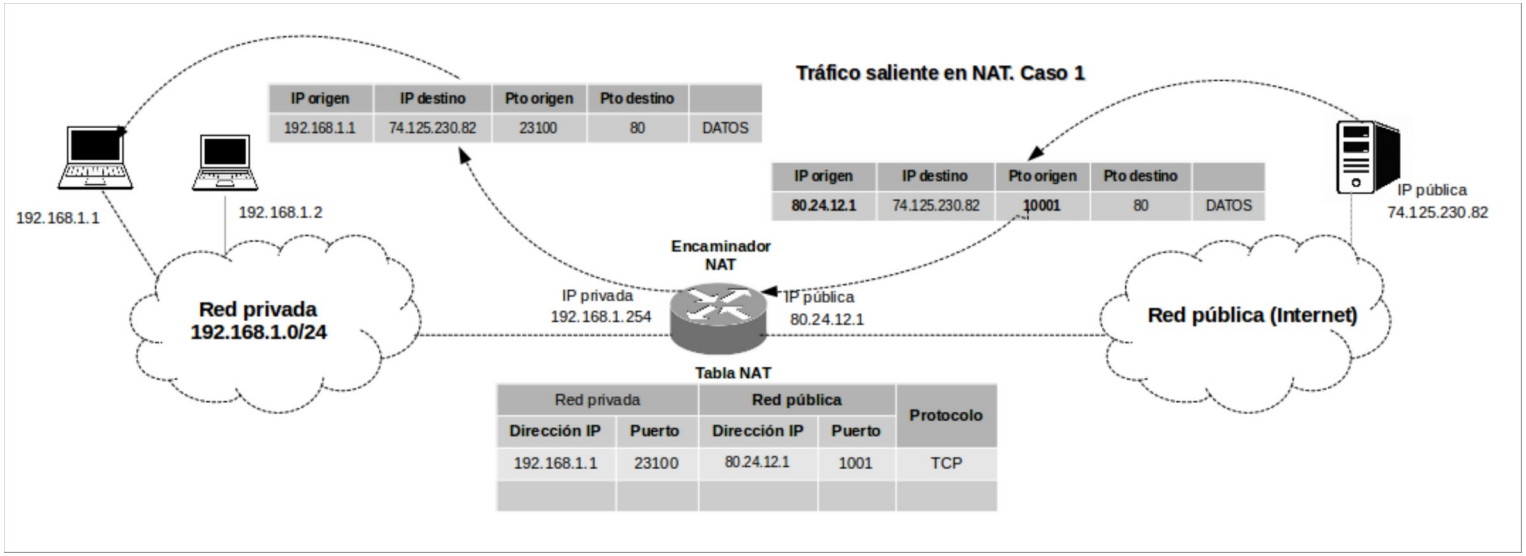
- Dirección IP interna (privada)
- Puerto interno
- Dirección IP externa (pública)

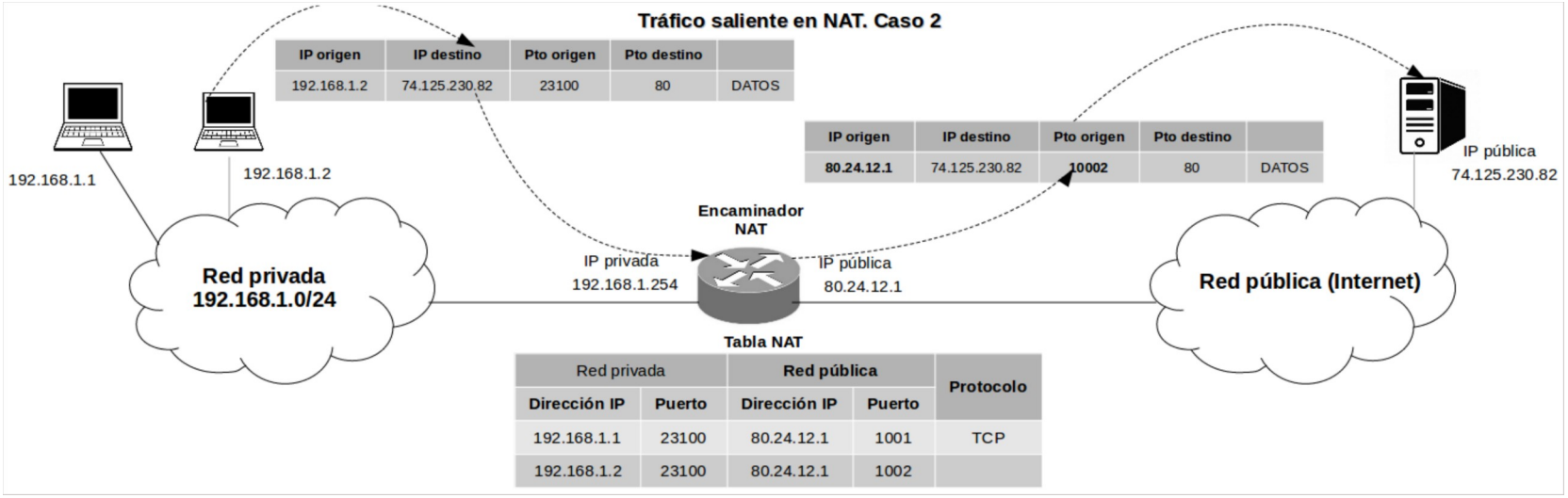
- Puerto externo
- Protocolo del nivel de transporte (TCP o UDP)

4.2. Tráfico saliente

Por tanto, la idea es que, para datagramas cuyo destino es una red distinta de la suya (p.e., Internet), el encaminador NAT o router sustituya la dirección IP de origen, privada, por su dirección pública (la del encaminador NAT o router), para que ese datagrama pueda circular sin problemas por Internet. Así, cuando el datagrama llegue a su destino parecerá que el origen del mismo es el router o encaminador NAT (al que se le puede responder puesto que tiene una IP pública). El puerto origen se traduce también por uno de entre los que tenga disponible el router NAT.

Ver gráficos página siguiente:

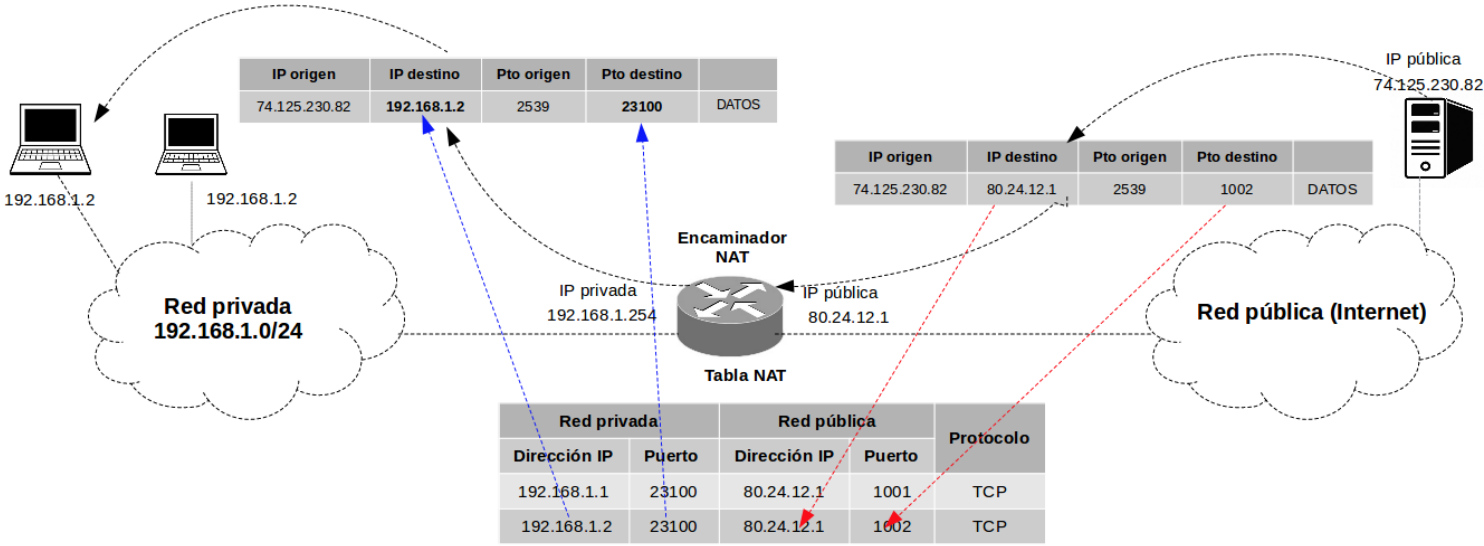

Tráfico saliente en NAT. Caso 1
IP origen | IP destino | Pto origen | Pto destino |
192.168.1.1 | 74.125.230.82 | 23100 | 80 | DATOS
IP origen | IP destino | Pto origen | Pto destino |
80.24.12.1 | 74.125.230.82 | 10001 | 80 | DATOS
192.168.1.1
192.168.1.2
IP pública
74.125.230.82
Encaminador
NAT
Red privada
192.168.1.0/24
IP privada
192.168.1.254
IP pública
80.24.12.1
Red pública (Internet)
Tabla NAT
Red privada | Red pública | Protocolo
Dirección IP | Puerto | Dirección IP | Puerto
192.168.1.1 | 23100 | 80.24.12.1 | 1001 | TCP


Tráfico saliente en NAT. Caso 2
IP origen | IP destino | Pto origen | Pto destino |
192.168.1.2 | 74.125.230.82 | 23100 | 80 | DATOS
IP origen | IP destino | Pto origen | Pto destino |
80.24.12.1 | 74.125.230.82 | 10002 | 80 | DATOS
192.168.1.1
192.168.1.2
IP pública
74.125.230.82
Encaminador
NAT
Red privada
192.168.1.0/24
IP privada
192.168.1.254
IP pública
80.24.12.1
Red pública (Internet)
Tabla NAT
Red privada | Red pública | Protocolo
Dirección IP | Puerto | Dirección IP | Puerto
192.168.1.1 | 23100 | 80.24.12.1 | 1001 | TCP
192.168.1.2 | 23100 | 80.24.12.1 | 1002

4.3. Respuesta al tráfico saliente

Cuando al encaminador NAT le llega un datagrama del exterior, comprueba si la dirección IP y el puerto de destino coincide con algún registro de su tabla NAT. Si es así, significa que el datagrama es una respuesta a un datagrama saliente anterior y, en ese caso, lo que debe hacer el encaminador es cambiar en el datagrama entrante la **IP y puerto de destino** (la IP era la del router) por la **IP y puerto internos** correspondientes a la entrada de la tabla NAT cuyos campos IP y puerto externos coinciden con la IP y puerto de destino del datagrama entrante. A continuación retransmitirá el datagrama modificado hacia la red interna, concretamente hacia la máquina que hizo la petición.

En cambio, si el datagrama que le llega al router NAT no se corresponde con ningún datagrama saliente previo, no sería respuesta a tráfico saliente, sino **tráfico entrante nuevo.** En este caso, el encaminador no sabrá a qué dirección y puerto interno debe redirigir el datagrama y, en general, **descartará** el datagrama. Existe excepciones como, por ejemplo, que el router NAT tenga un servidor escuchando en ese puerto, en cuyo caso sí se aceptará el datagrama entrante nuevo (por ejemplo, un servidor web escuchando en el puerto 80 del router NAT).



Respuesta al tráfico saliente

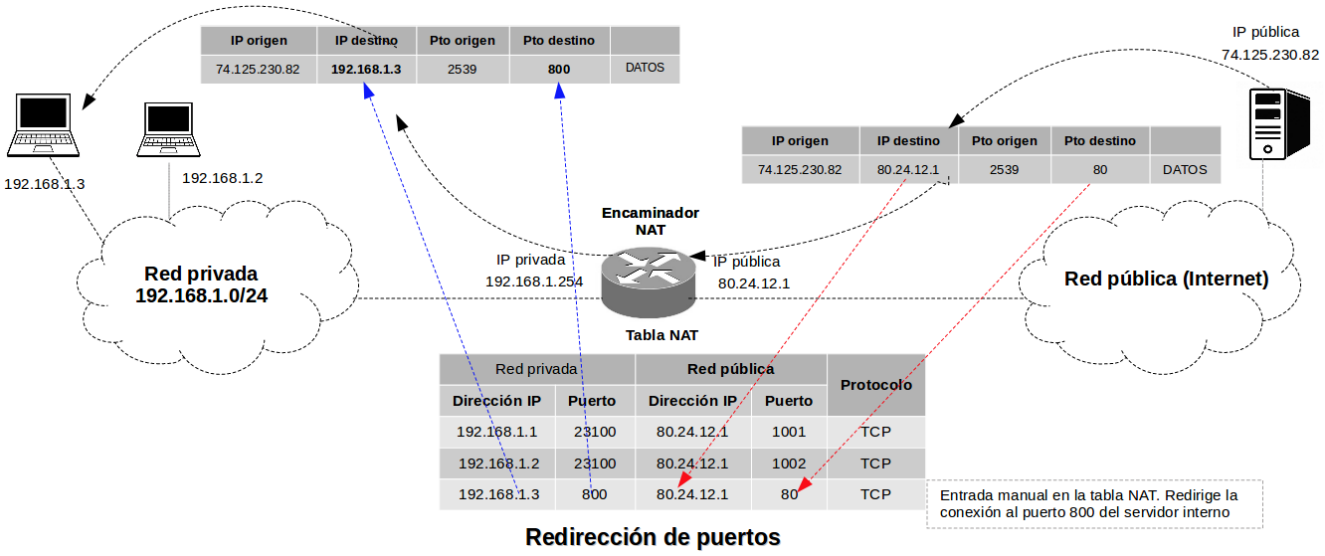
4.4. Solución al tráfico entrante nuevo. Redirección de puertos.

Sin embargo, descartar todas las conexiones entrantes a nuestra LAN puede suponer una gran limitación en nuestra red interna, ya que si en ella tenemos algún tipo de servidor que queremos qie se vea desde el exterior (correo, servidor web, etc), va a ser imposible permitir el acceso a él. Para subsanar esta carencia y a pesar del peligro que supone dejar acceder a nuestra LAN a equipos externos, es posible permitir tráfico entrante nuevo mediante la **redirección de puertos**.

La redirección de puertos (port forwarding), consiste en indicar al enrutador NAT la dirección IP del equipo de la red interna al que se va a redirigir todo del tráfico entrante nuevo dirigido a un

puerto concreto. Para ello, se deben añadir manualmente nuevas entradas a la tabla NAT que redirijan el tráfico entrante nuevo **en función del puerto al que vaya dirigido**. Así, todo el tráfico entrante dirigido, por ejemplo, al puerto 80 del router NAT será reenviado a la IP de un equipo de la LAN (y al puerto en el que escucha).

El direccionamiento de puertos nos permite disponer de varios servidores en la LAN accesibles desde la IP pública de nuestra red. Únicamente obliga a acceder a cada servicio por un puerto distinto.



4.5. Limitaciones de NAT

Algunos protocolos de aplicación incluyen la dirección IP y puerto usados en la comunicación en el campo de datos del datagrama, y no en la cabecera. Como el encaminador NAT solo puede cambiar el contenido de las cabeceras de los protocolos IP, TCP y UDP, podrían darse incongruencias en los datagramas que, por un lado indiquen una IP y un puerto en la cabecera y otros distintos en los datos. Si esto sucede y la máquina destino usa los valores de la parte de datos, no se identificará el origen del paquete.

Para evitar esto, los encaminadores NAT deben conocer el protocolo concreto de nivel de aplicación encapsulado en cada datagrama, para modificar también el campo de datos del mismo. Por suerte, las últimas implementaciones de NAT van incorporando los protocolos más comunes que encapsulan direcciones IP y puertos en el campo de datos, corrigiendo esta limitación aún a costa de un retardo en el procesamiento del datagrama.