UT1.2 Repaso Direccionamiento IP. Tablas de enrutamiento,

(Curso 2015 - 2016)

Asignación de direcciones IP v4

- La función principal de IP consiste en agregar información de direcciones a los paquetes de datos y enrutarlos a través de la red. Para entender cómo IP lleva esto a cabo, es necesario familiarizarse con los conceptos que determinan las direcciones de destino intermedias y finales de los paquetes de datos. Comprender el modo en que IP utiliza la información de dirección permitirá garantizar que IP enrute los datos al destino correcto.

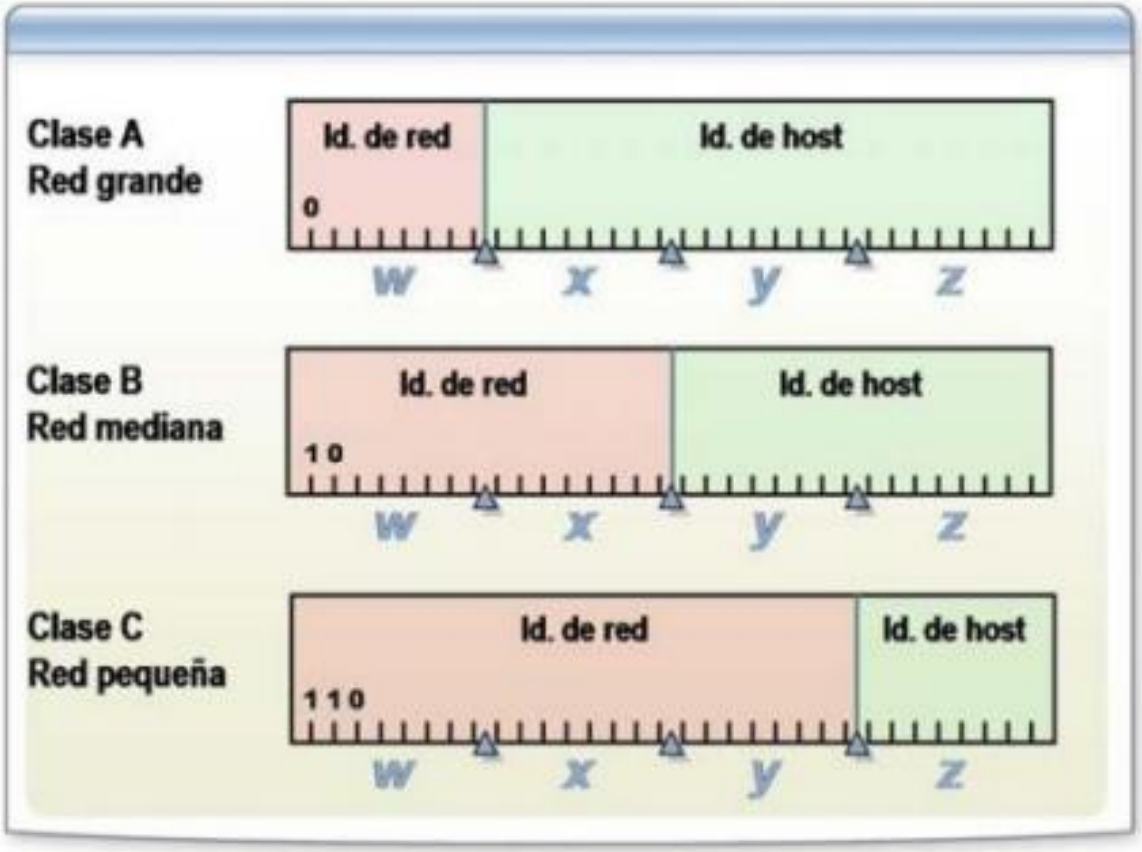
Asignación de direcciones IP v4

- Para conectarse a Internet para navegar y otros usos se necesitará también una puerta de enlace y unos servidores de DNS. Ejemplos avanzados de configuraciones IP también incluyen segmentación de redes, uso de NAT (network address translation) y CIDR (classless interdomain routing).

Clases de redes

- Se pueden obtener direcciones registradas a través de un ISP (Internet Service Provider, Proveedor de servicios de Internet) o la IANA (Internet Assigned Numbers Authority, autoridad de números asignados de Internet). El tamaño y el tipo de red determinan la clase de dirección.

Clases de redes



Máscara de subred predeterminadas

Clase	Primeros bits del primer octeto	Rango de direcciones en decimal	N° máximo de redes	N° máximo de host por red	Máscara predeterminada
A	**0**	0.0.0.0 - 127.255.255.255	2^7	2^{24}-2	255.0.0.0
B	**10**	128.0.0.0 - 191.255.255.255	2^{14}	2^{16}-2	255.255.0.0
C	**110**	192.0.0.0 - 223.255.255.255	2^{21}	2^8-2	255.255.255.0

Cálculo del número máximo de redes Ejemplo para Clase A

- Tal y como hemos visto antes las direcciones de la clase A siempre empiezan por 0. Su identificativo de red (tal y como indica la máscara predeterminada) está compuesto por 8 bits por lo que sólo nos quedan 7 bits (el primer bit "0" es fijo) para obtener todas las combinaciones posibles. El número máximo de redes será por lo tanto 2 elevado a 7.
- Para calcular el número máximo de hosts por subred realizamos la operación 2 elevado al número de bits del identificativo de host (en este caso 24) y le restamos la dirección IP de red (combinación de todo ceros) y la de broadcast (combinación de todo unos).

Notación CIDR

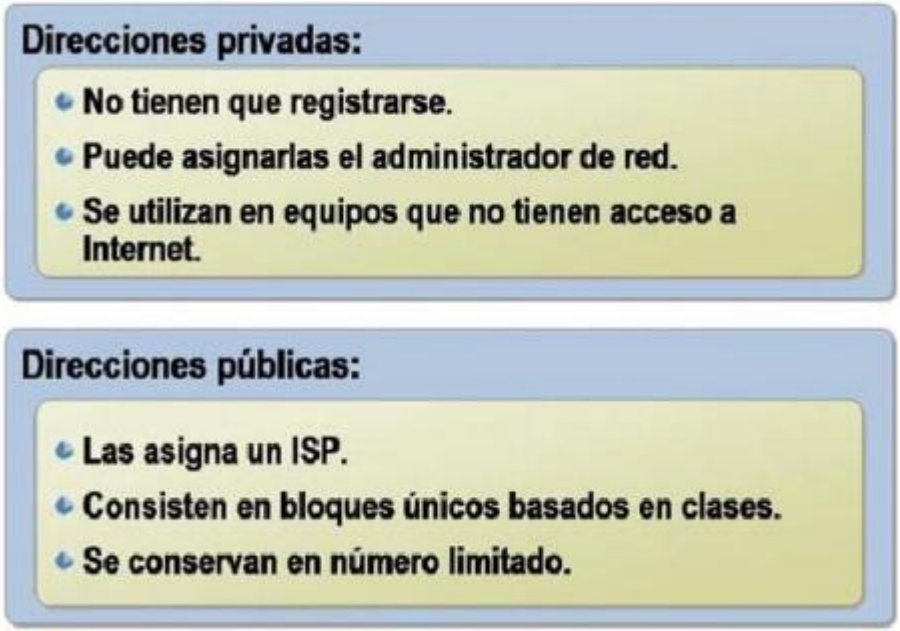
- Tal y como se ha mencionado antes la dirección de red viene definida por la dirección IP y por la máscara de red. Existe otra notación para identificar estos datos. Se denomina notación CIDR y consiste en añadir a la dirección IP una "/" y a continuación especificar el número de bits a uno que tiene la máscara. De esta forma las máscaras predeterminadas de las clases A, B y C serían las siguientes:
  - Clase A: "/8"
  - Clase B: "/16"
  - Clase C: "/24"

Direcciones IP especiales

- Existen algunas direcciones IP que no se deben asignar a ningún host:
- La dirección 0.0.0.0 es reservada por la IANA para utilizar por un interfaz de red cuando su IP no está definida.
- La dirección que tiene todos los bits del identificativo de host a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene todos los bits del identificativo de host a uno sirve para enviar mensajes por multidifusión. Se denomina dirección de broadcast.
- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina dirección de bucle local o loopback.

IP Públicas privadas

- Direcciones públicas: identifican a un dispositivo conectado a Internet.
- Direcciones privadas: son rangos de direcciones reservados para redes privadas o intranets y no pueden emplearse en Internet.



IP Públicas

- Una dirección IP privada nunca se asigna como dirección pública y nunca duplica direcciones públicas.
- Las siguientes direcciones IP están reservadas para redes privadas:
  - Clase A: 10.0.0.0 a 10.255.255.255
  - Clase B: 172.16.0.0 a 172.31.255.255
  - Clase C: 192.168.0.0 a 192.168.255.255

Envía de peticiones de un host con dirección IP privada a Internet

- Un host con una dirección privada debe enviar sus peticiones de tráfico de Internet a una puerta de enlace de capa de aplicación (como un servidor proxy) que tenga una dirección pública válida. O bien, el host debe tener un conversor de direcciones de red (NAT) que convierta la dirección privada en una dirección pública y envíe sus peticiones por Internet.

Actividad 1

A partir del siguiente diagrama de red, Figura1.6, completa los espacios con la información adecuada relativa a las direcciones de red y las direcciones de los diversos dispositivos. La solución no es única. Comenta posteriormente la idoneidad de la solución obtenida.

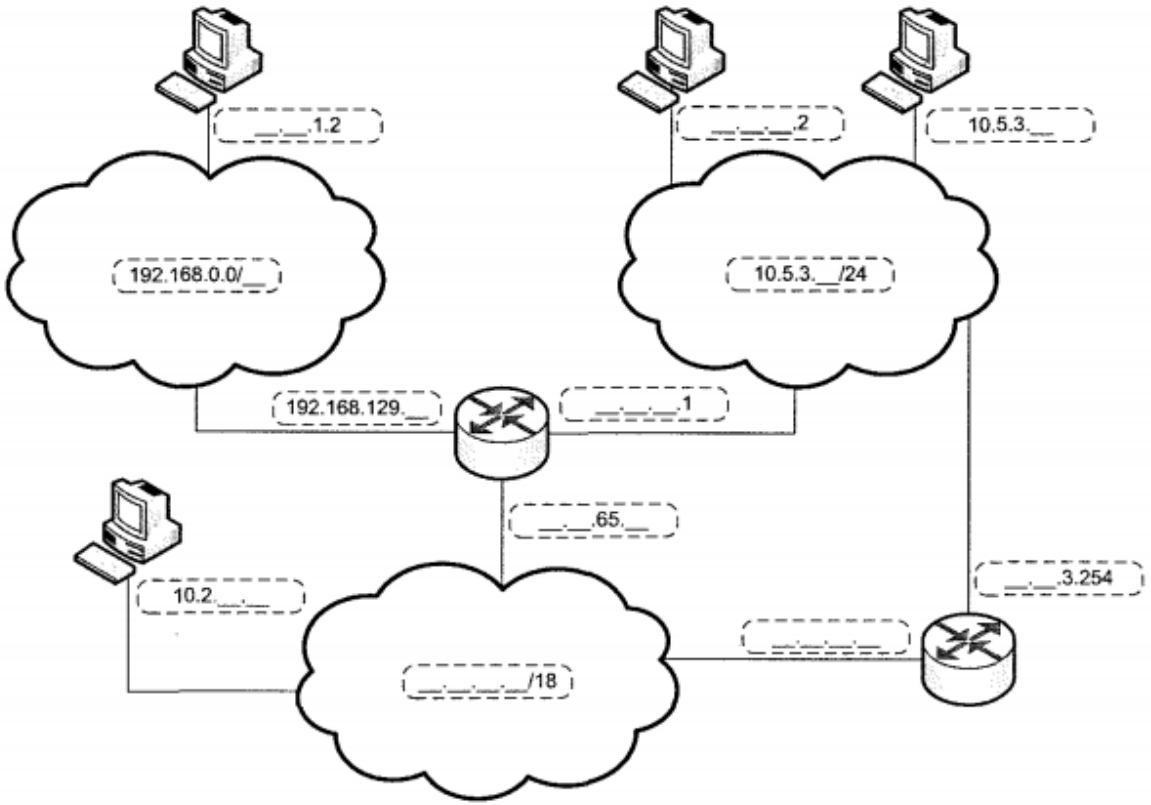


Figura 1.6: Red a direccionar

Segmentación de redes

- Dada la red 200.5.2.0 /24
- ¿Cuántos bits se necesitan para tener 2 subredes?
- 1 solo bit
- Como sólo necesito un bit, la máscara de red /24 pasa a ser una máscara de subred /25 Máscara de subred:
- 11111111.11111111.1111111.10000000 (/25)

Segmentación de redes

	Identificativo de red (24 bits)			Identificativo de subred (1 bit)	Identificativo de host (7 bits)
Máscara de subred (binario)	11111111	11111111	11111111	1	0000000
Máscara de subred (decimal)	255	255	255	128	

Segmentación de redes

	Identificativo de red (24 bits)			Identificativo de subred (1 bit)	Identificativo de host (7 bits)
Máscara de subred (binario)	11111111	11111111	11111111	1	0000000
Dirección de subred1 (binario)	11001000	00000101	00000010	0	0000000
Dirección de subred1 (decimal)	**200**	**5**	**2**	**0**	
Dirección de subred2 (binario)	11001000	00000101	00000010	1	0000000
Dirección de subred2 (decimal)	**200**	**5**	**2**	**128**	

Solución: Las dos subredes serían la 200.5.2.0/25 y la 200.5.2.128/25

Asignación de direcciones públicas

- Las direcciones públicas las asigna la IANA y se componen de un identificador de red basado en clases o bloques de direcciones basadas en CIDR (denominados bloques CIDR), y tienen la garantía de que son exclusivas en Internet en todo el mundo. El número de direcciones públicas que pueden asignarse es limitado.
- Cuando se asignan direcciones públicas, se programan rutas en los enrutadores de Internet para que el tráfico enviado a las direcciones públicas asignadas pueda llegar a esas ubicaciones. El tráfico enviado a direcciones públicas de destino se transmite a través de Internet.

Enrutadores

- En una red interconectada, un enrutador conecta las subredes entre sí y facilita la conexión con otras redes. Si se sabe cómo el enrutador reenvía paquetes de datos a las direcciones de destino IP, podrá garantizar que los equipos host de su red estén correctamente configurados para transmitir y recibir datos.
- Los enrutadores operan en la capa de red del modelo de referencia de interconexión de sistemas abiertos (OSI), de modo que pueden conectar redes con diferentes protocolos de la capa de vínculo de datos y medios de red.

Enrutadores

- En una red interconectada pequeña, el trabajo de un enrutador puede ser muy sencillo. Cuando dos LAN están conectadas mediante un enrutador, éste se limita a recibir paquetes de una red y reenviar sólo los que van destinados a la otra red.
- En una red interconectada grande, los enrutadores conectan varias redes diferentes y, en muchos casos, estas tienen más de un enrutador conectado. Esto permite que los paquetes sigan rutas diferentes a un destino determinado. Si un enrutador de la red falla, los paquetes pueden sortearlo y llegar a su destino.

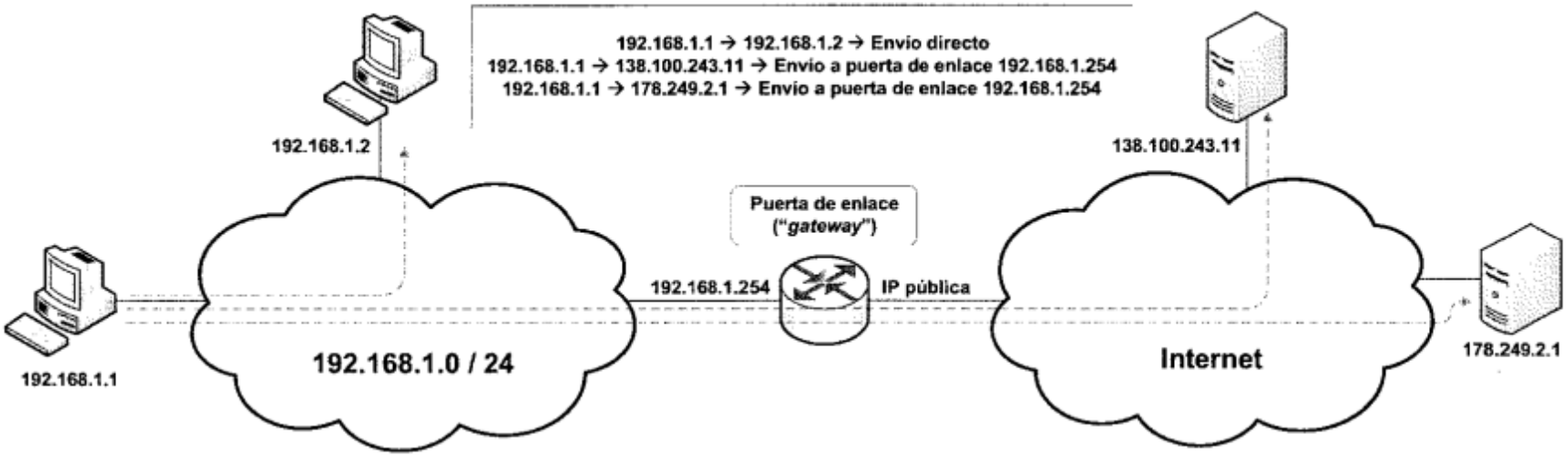
Enrutadores

- Los enrutadores utilizan las direcciones IP de destino contenidas en los paquetes junto con las tablas de enrutamiento, para reenviar los paquetes entre las redes. La tabla de enrutamiento debe contener todas las direcciones y rutas posibles de la red, además del costo que implica llegar a cada una. En definitiva, los enrutadores enrutan los paquetes de acuerdo con las rutas disponibles y su costo.

Enrutadores

- Cuando un equipo desee poner un datagrama en la red debe decidir si la dirección IP de destino está en su misma red, con lo que el **envío** sería **directo** y sin intermediación ninguna.
- O bien, no está en su misma red y en este caso se enviaría a un encaminador(puerta de enlace),para que lo encamine hacia su **destino(envío indirecto**)

Envío directo / envío indirecto



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 del protocolo de encaminamiento concreto empleado pero en general, son:

Tablas de encaminamiento

- Destino(D): dirección IP de una red o host.
- Máscara de red (MR): asociada al Destino anterior sirve para determinar exactamente todas las direcciones 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 la que hay que enviar el datagrama a la Dirección de salto.

Tablas de encaminamiento

- 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 host o equipo.
- Ruta por defecto:cuando ninguna entrada de los tipos anteriores es aplicable, se puede disponer de una ruta por defecto para todas las redes no consideradas previamente,

Tablas de encaminamiento

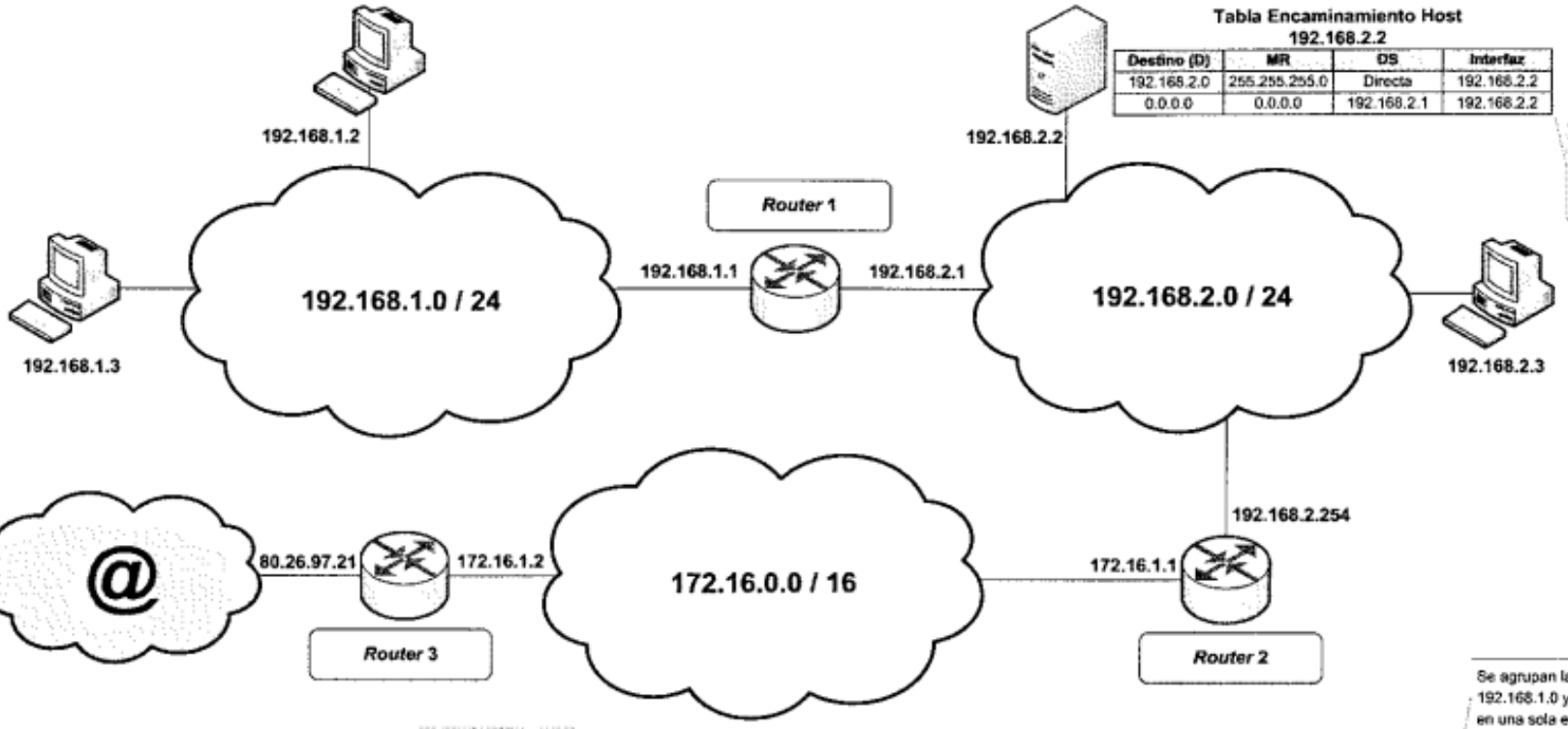


Tabla Encaminamiento Host 192.168.2.2

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)

Tabla Encaminamiento *Router 1*

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

Ruta de red (directa)

Ruta de red (indirecta)

Ruta por defecto

Tabla Encaminamiento *Router 2*

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

Tabla Encaminamiento *Router 3*

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

Se agrupan las redes 192.168.1.0 y 192.168.2.0 en una sola entrada

La dirección de salto se encuentra ya en Internet

Actividad 2

- Consulta la tabla de encaminamiento de tu ordenador con el comando *route* ejecutado desde un terminal. Estudia sus diversas opciones y comprueba cómo se encaminan los datagramas hacia la puerta de enlace o bien son entregados directamente a su destino.
- Si te encuentras en *Linux*, puedes ejecutar el comando *route -C* que mostrará la *caché* de encaminamiento con los últimos datagramas encaminados.

Protocolos de encaminamiento

- **Encaminamiento estático**: la configuración de las tablas de encaminamiento se hace de forma manual. Es una estrategia no adaptativa, es decir, que cualquier cambio que se produzca en la topología de la red debe ser supervisado por el administrador para evitar rutas imposibles o bucles indeseados. Por esto mismo es muy sensible a fallos y solo recomendable en redes de pequeño tamaño y topología fija.
- **Encaminamiento dinámico**: el propio encaminador actualiza sus tablas gracias a la utilización 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 posibles.

Nivel de transporte

- El nivel de transporte nos provee de elementos para diferenciar y gestionar, de forma simultánea, múltiples orígenes y destinos en una comunicación y múltiples comunicaciones en cada equipo
- También permite identificar los extremos finales en la comunicación y nuevos servicios orientados a conexión.

Puertos de comunicaciones

- Cada proceso del nivel de aplicación tiene asociado uno ovarios puertos a través de los cuales es accesible. Cada puerto se identifica por un número binario de 16 bits que en notación decimal pueden variar entre O y 2 elevado a 16-1= 65535

Tipos de puertos

- Existen varias clases de puertos en función del uso que se hace de ellos:
- Puertos conocidos (O - 1023): se conocen como wellk nown ports y están reservados para aplicaciones y servicios estándar como HTTP, FTP, etc. Las aplicaciones clientes se conectan a estos puertos para acceder a los servicios.
- Puertos registrados (1024 - 49151): para aplicaciones no estándar instaladas por el usuario que no tienen un puerto well known preasignado. Estos puertos pueden asignarse dinámicamente a clientes si ningún servicio está haciendo uso de ellos.
- Puertos dinámicos(49152 - 65535): habitualmente se emplean para iniciar conexiones desde el cliente. No suelen emplearse en procesos servidores.

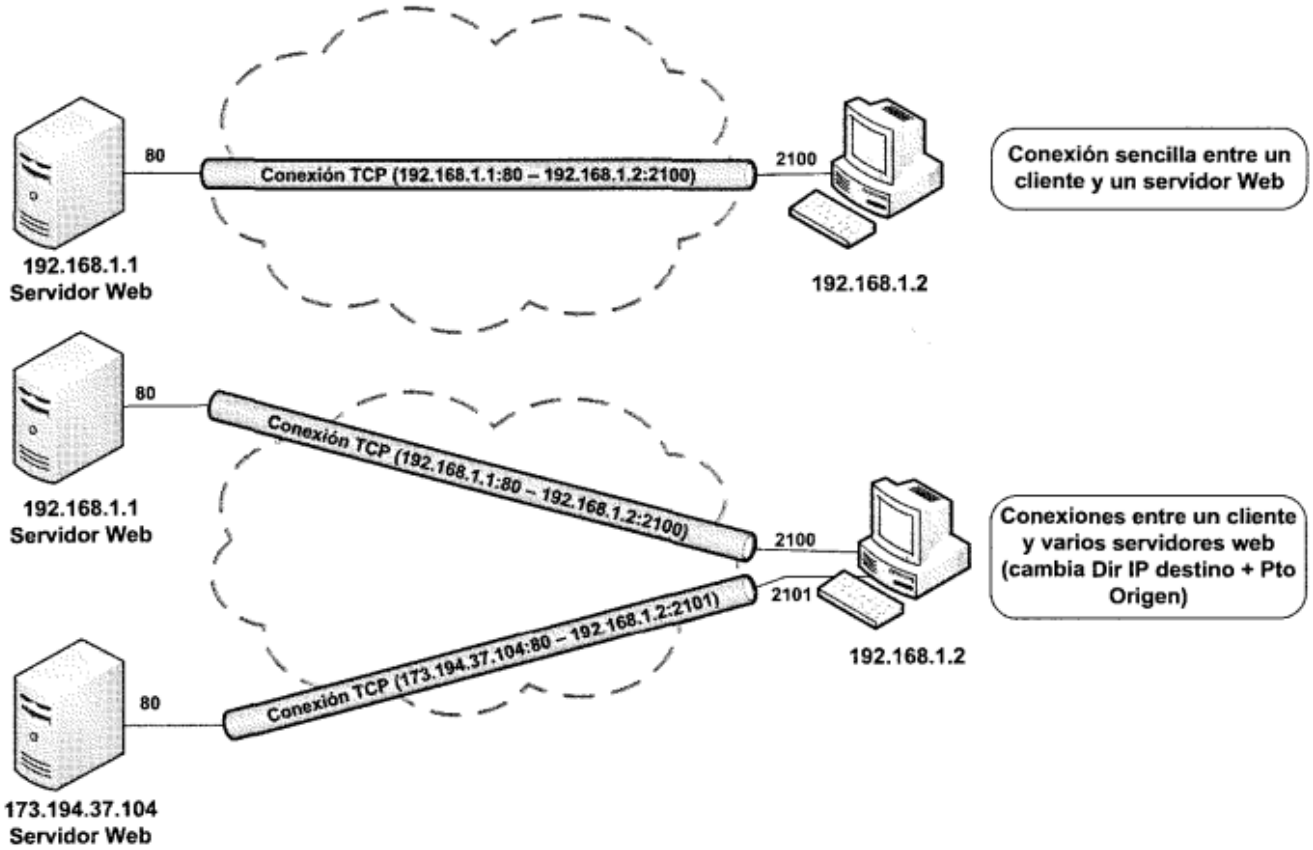
Tipos de puertos

- La correspondencia entre procesos y puertos se hace de dos formas distintas:
  - Asignación estática: los well known ports están reservados para aplicaciones estándar y solo pueden ser empleados por estos procesos.
  - Asignación dinámica: cuando un proceso necesita un puerto y este no se asigna estáticamente, el sistema operativo le asigna uno que esté disponible(1024-65535).
- Los puertos TCP y UDP son totalmente independientes entre sí.

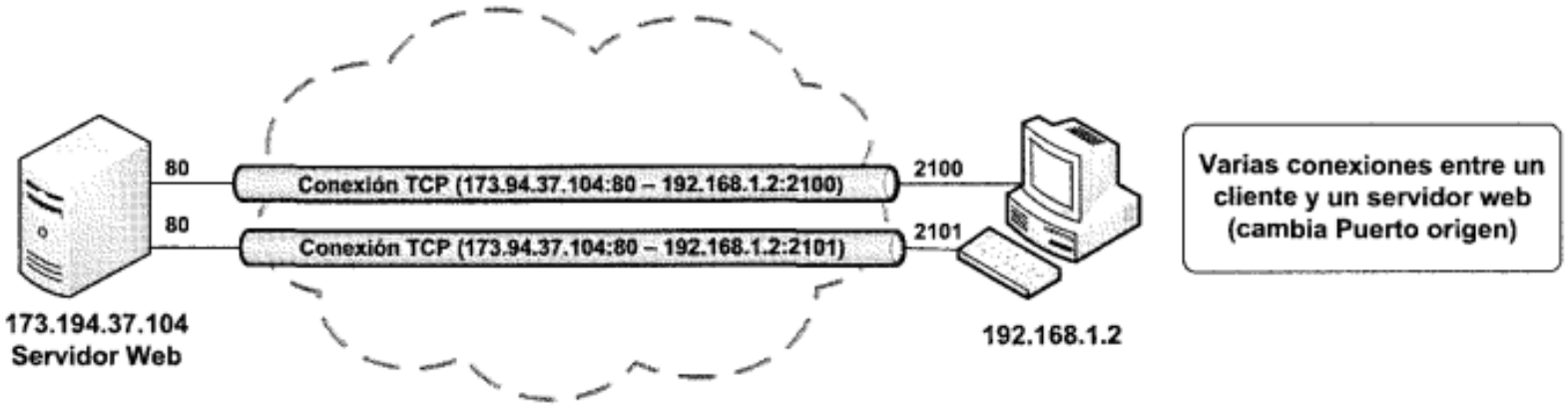
Conexiones TCP

- La conexión TCP se define de forma única por los datos relativos a los puntos extremos de la comunicación, es decir, por estos cuatro elementos:
  (Dirección IP origen, Puerto TCP origen)=>(Dirección IP destino,Puerto TCP destino).
- No puede haber dos conexiones TCP que tengan en común estos cuatro elementos.

Ejemplos de conexiones TCP



Ejemplos de conexiones TCP



Actividad 3

- Emplea el comando netstat para averiguar información sobre las conexiones TCP/IP y los puertos de escucha de tu ordenador. Utilizala ayuda con netstat-h.
- Abre en un navegador la página www.google.es y consulta las conexiones TCP establecidas. ¿Reconoces la conexión a la página anterior? Comenta todo lo que sepas de ella.
- Consulta por un lado los puertos UDP abiertos y por otro todas las conexiones TCP establecidas. ¿Qué diferencias aprecias en la información mostrada referente a UDPyTCP?¿A qué se debe?
- Muestra las aplicaciones que han creado cada una de las conexionesTCP.

Actividad 4

Emplea la utilidad *Nmap* para averiguar información sobre las conexiones TCP/IP y los puertos de escucha de **otros** ordenadores. Descarga la utilidad desde `http://nmap.org/download.html`. Hay disponibles versiones de línea de comandos y de interfaz gráfica (*Zenmap*).

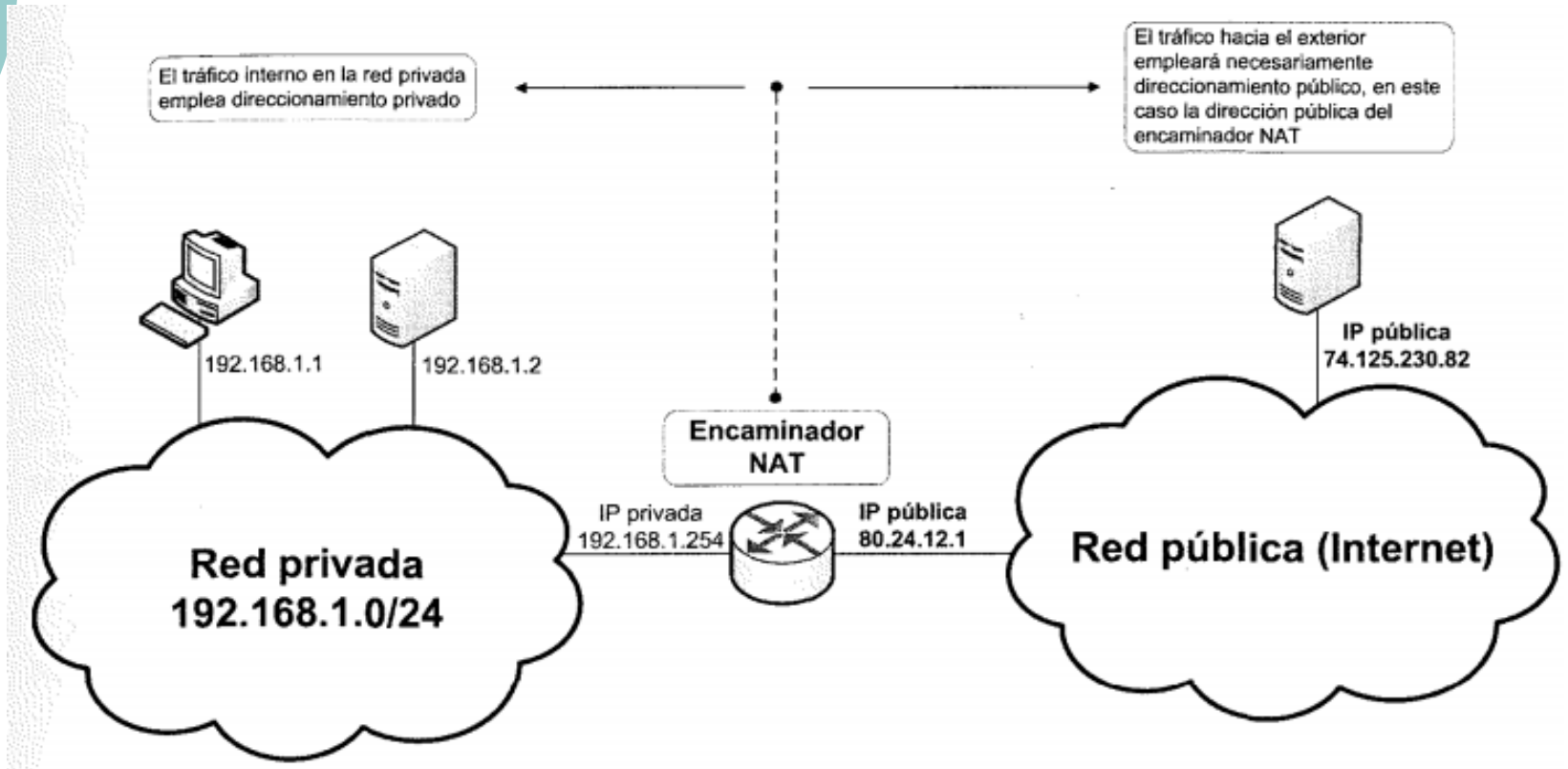
- Consulta los puertos TCP y UDP abiertos de tu propio ordenador (*localhost*) y contrástalo con lo obtenido mediante *netstat*.
- Averigua los puertos TCP y UDP abiertos en **la puerta de enlace** de tu red. Comenta la utilidad de todos los puertos conocidos, *well known ports*, que hayas encontrado.
- Averigua los puertos TCP y UDP abiertos en `www.google.es` y en `asterix.fi.upm.es`.

NAT

- El uso más habitual de NAT (Network Address Translation) es que una red privada pueda emplear direcciones IP privadas internamente y tener una o varias direcciones IP globales (IP'spúblicas) que estarán 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 comunes. 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

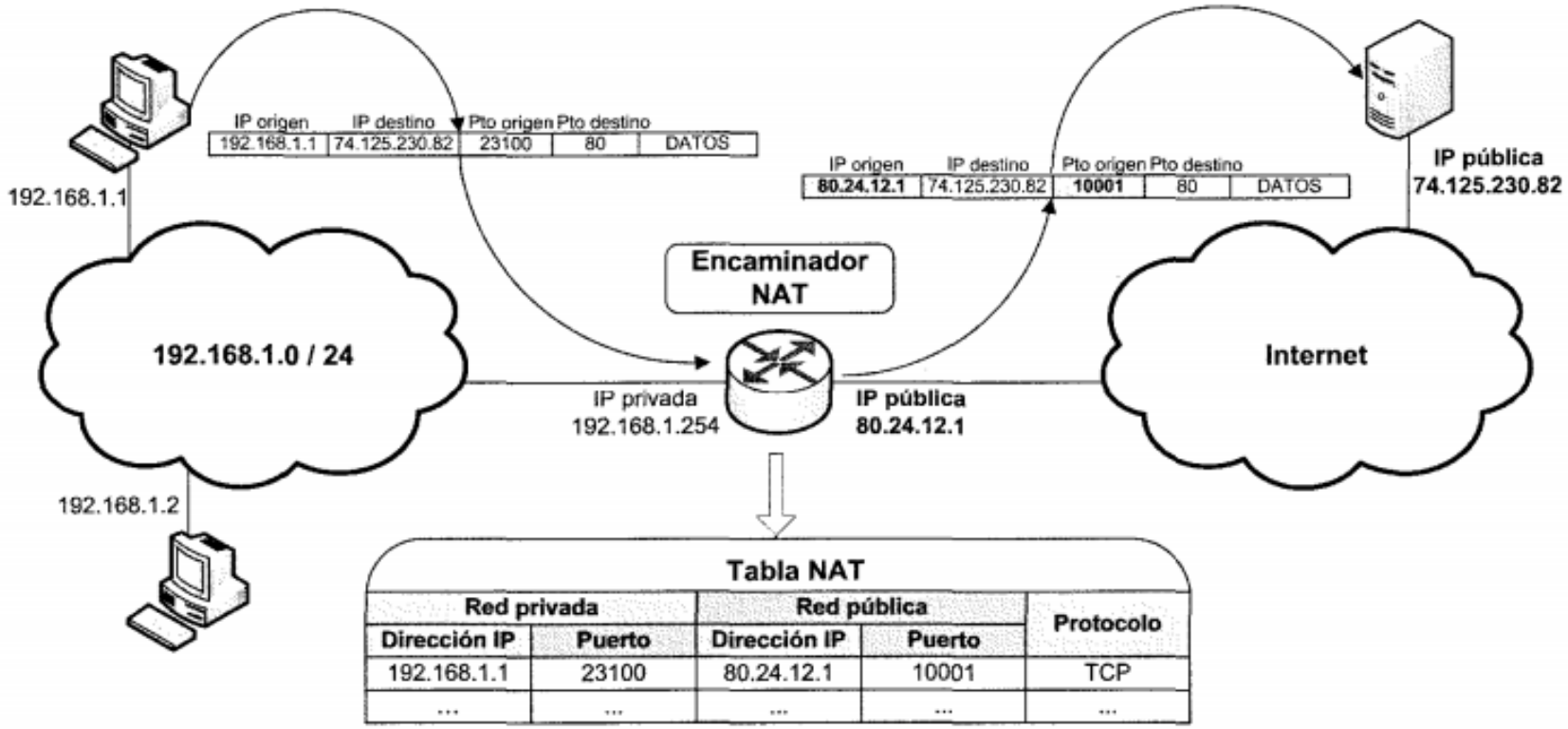
- NAT básico: únicamente se modifica la dirección IP



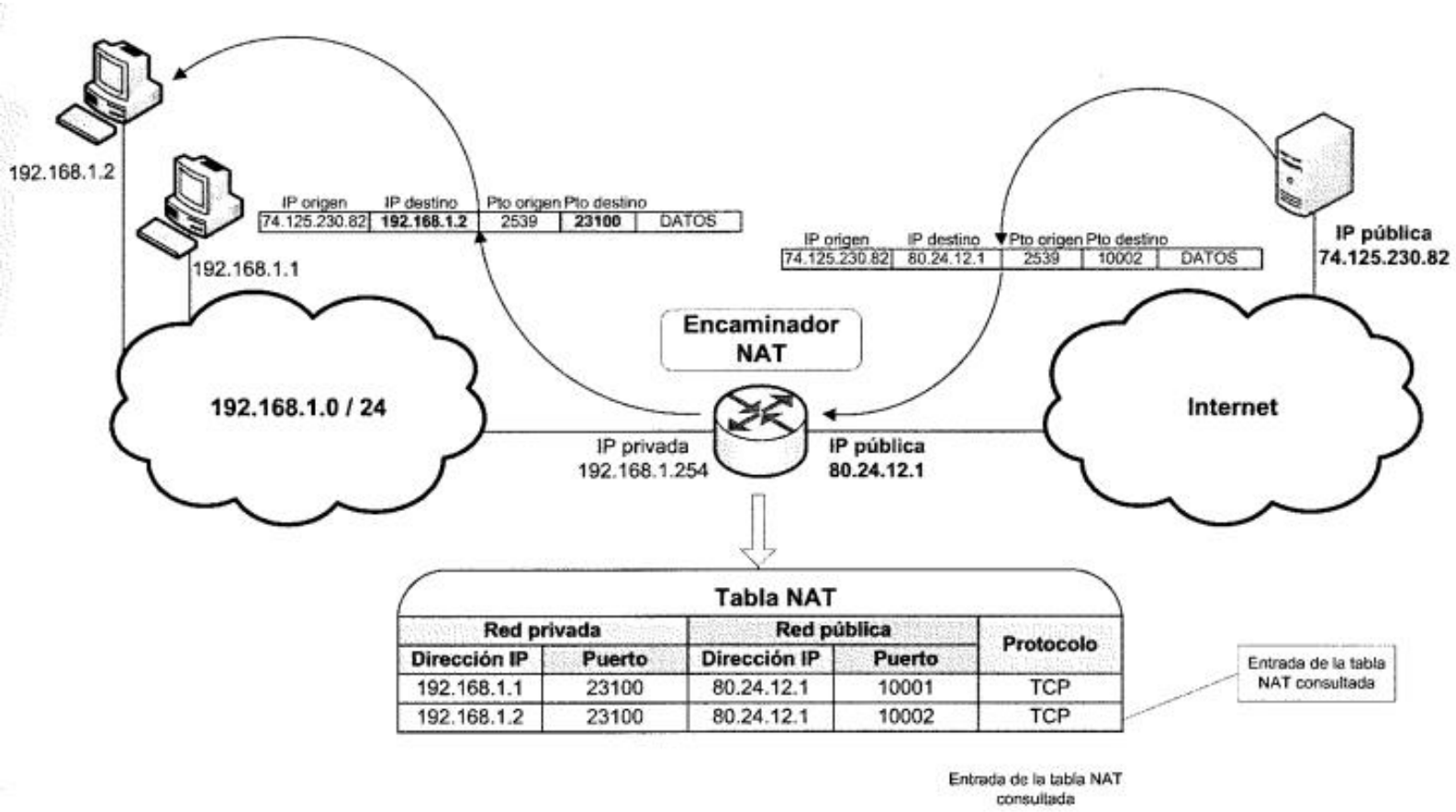
NAT

- NAPT (Network Address Port Translation)/ PAT(Port Address Translation): además de la dirección IP también se modifican los puertos empleados en la comunicación a nivel de transporte. También se conoce como NAT a nivel de transporte. Ha sustituido de hecho a NAT y ahora se le denomina indistintamente NAT o NAPT.
  - Se modifica la dirección IP de origen y el puerto deorigen en el tráfico saliente de la red privada.
  - Se modifica la dirección IP de destino y el puerto de destino en el tráfico entrante en la red privada.

NAT – tráfico saliente



NAT – respuestas al tráfico saliente



NAT – tráfico entrante nuevo

- Si en cambio, el datagrama que le llega al encaminador NAT no se corresponde con un datagrama saliente previo (tráfico entrante nuevo), el encaminador NAT no sabrá a que dirección interna y puerto redirigirlo y, en general, descartará el datagrama.
- De esta manera no se podrían alojar servidores dentro de la red, para subsanarlo, a pesar del peligro potencial que supone dejar que se inicien conexiones desde la red exterior, es posible permitir las conexiones entrantes nuevas mediante el mecanismo de redirección de puertos.

NAT – tráfico entrante nuevo

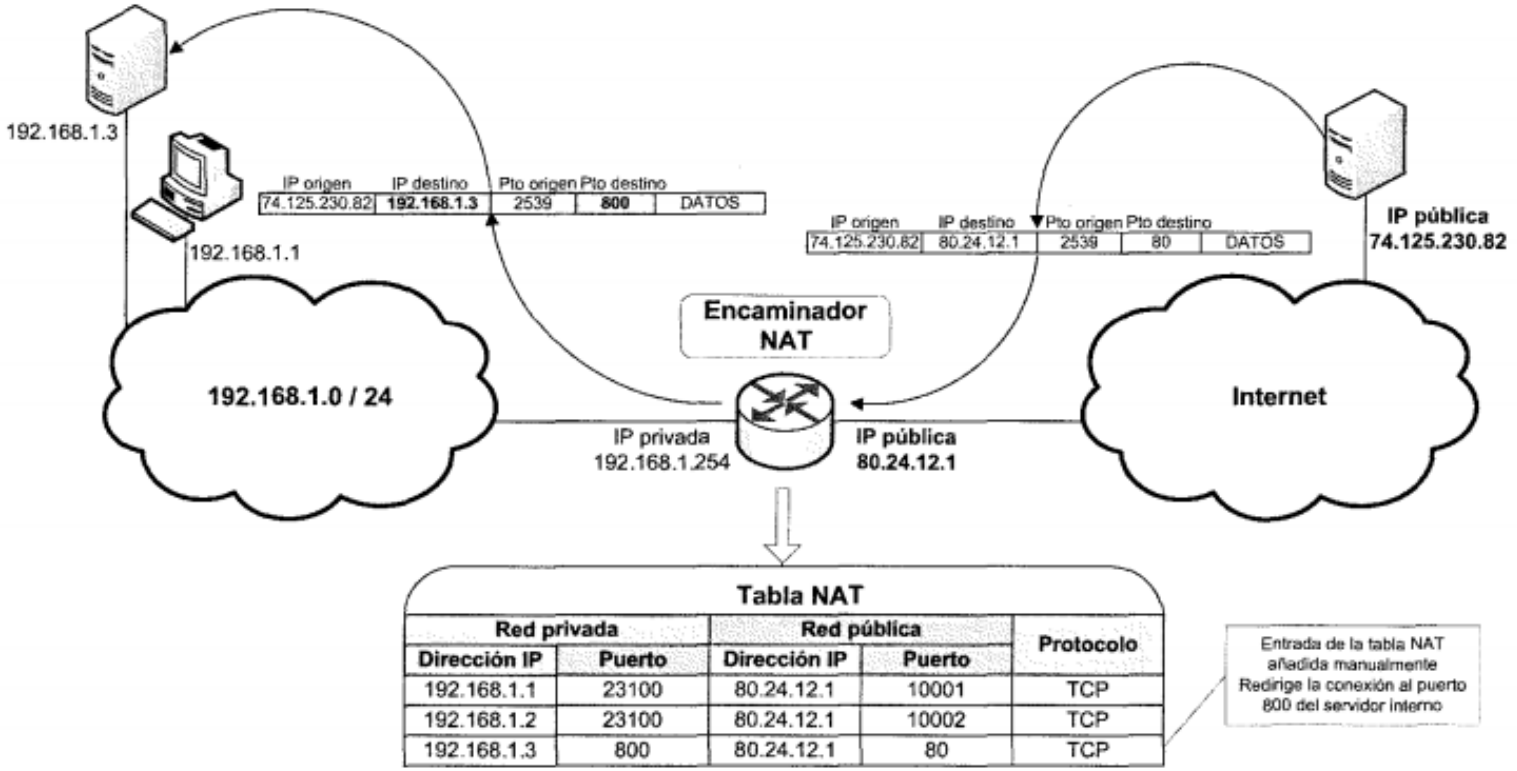


Tabla NAT

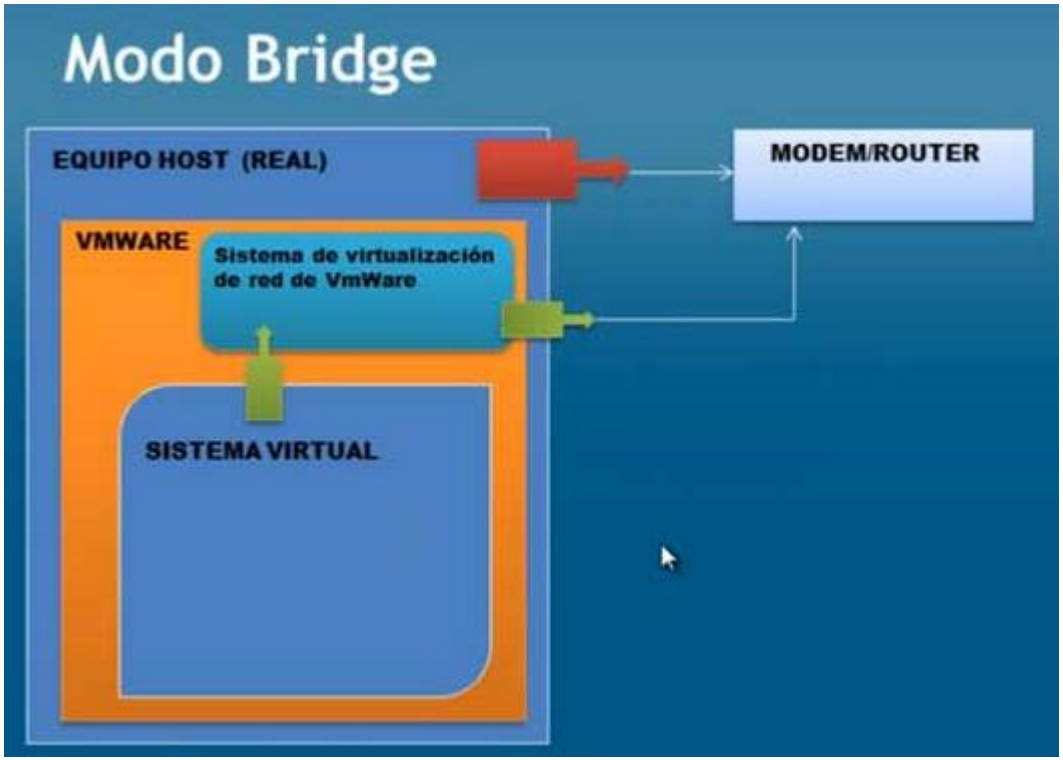
Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
192.168.1.2	23100	80.24.12.1	10002	TCP
192.168.1.3	800	80.24.12.1	80	TCP

Entrada de la tabla NAT añadida manualmente
Redirige la conexión al puerto 800 del servidor interno

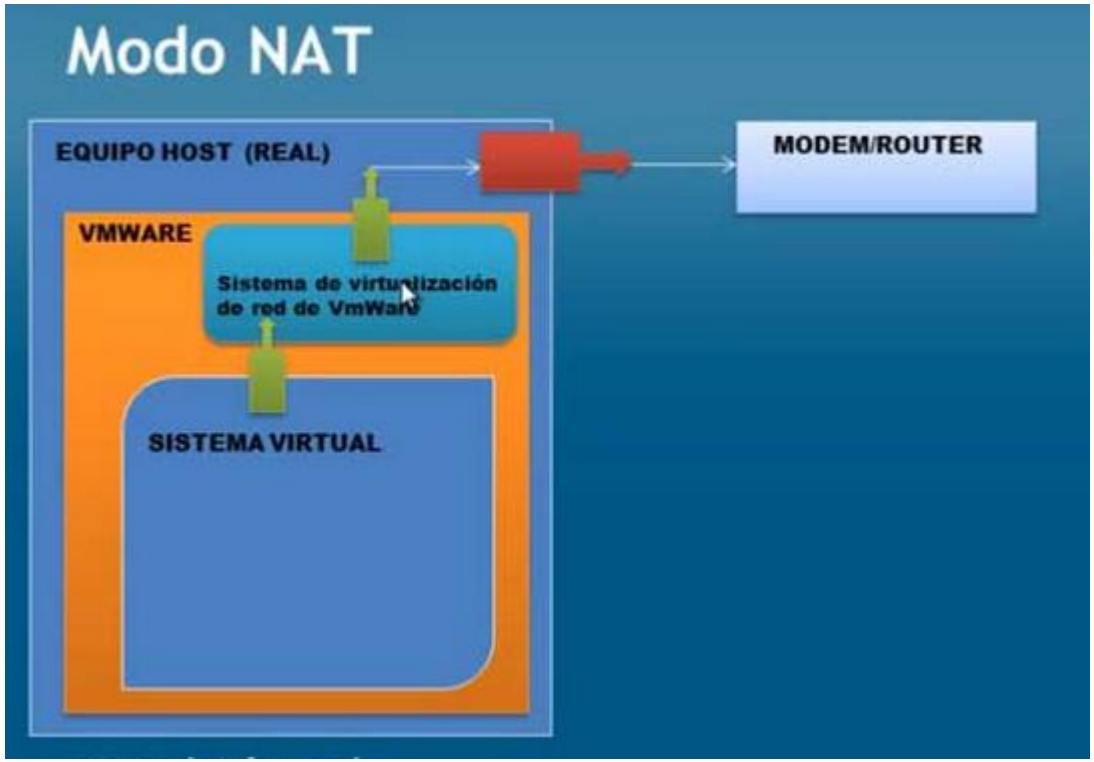
NAT y WMware

- Modo Bridge: Tiene su propia IP en la red local y es como si tuvieras otro equipo físico en la red.
- Modo NAT: Sale a internet emulando un DHCP y utilizando la misma IP del equipo host.

NAT y WMware


Modo Bridge
EQUIPO HOST (REAL)
MODEM/ROUTER
VMWARE
Sistema de virtualización de red de VmWare
SISTEMA VIRTUAL

NAT y WMware


Modo NAT
EQUIPO HOST (REAL)
MODEM/ROUTER
VMWARE
Sistema de virtualización de red de VmWare
SISTEMA VIRTUAL