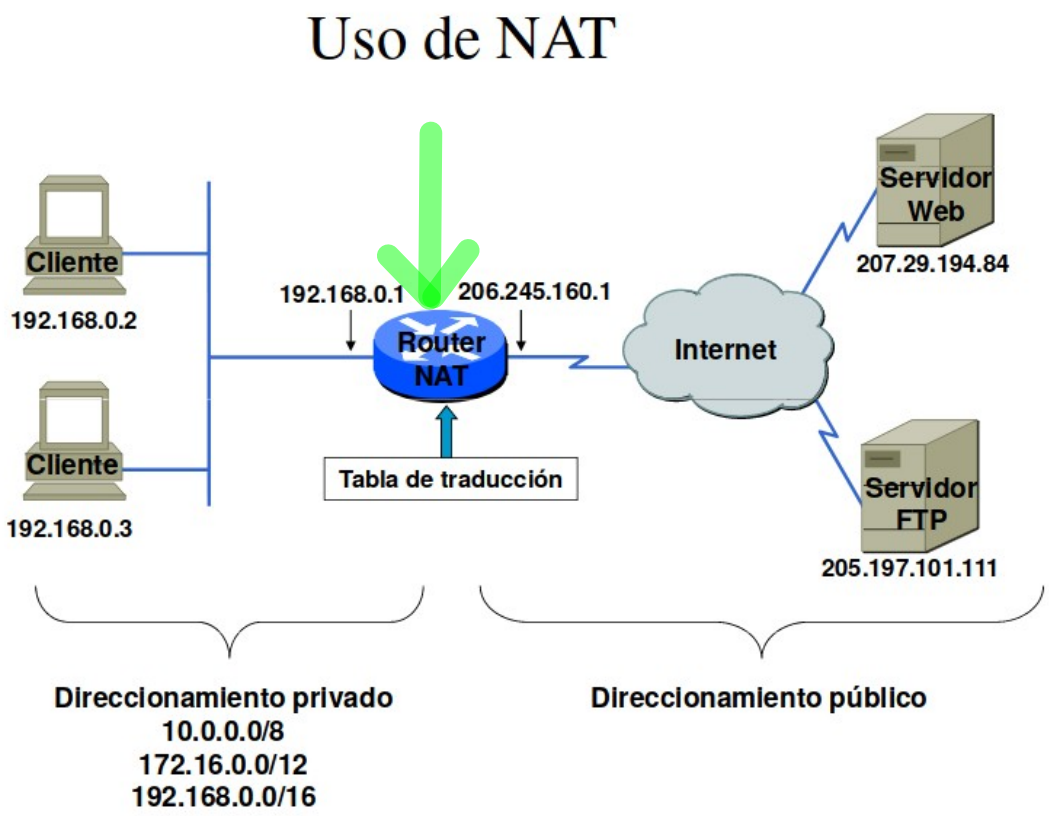
NAT - PAT

NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al ISP.

Esto surgió como consecuencia del agotamiento de Direcciones IPV4. El uso mas frecuente es el de utiliza NAT para conectar a Internet redes IP que utilizan rangos privados (RFC 1918). Esto se realiza en el Modem/Router o Gateway.



RFC 3022 , RFC 1631 y RFC 2663 se refieren a NAT y su Terminología.

En este tipo de NAT sólo necesitan cambiar y recalcularse:

- las direcciones IP
- cabecera de comprobación IP
- las sumas de comprobación de nivel superior que incluyen la dirección IP.

Trabajo del Router!

El NAT solo se aplica a TCP, UDP e ICMP. TCP y UDP con UDP de Capa 4-

Sin embargo, NAT presenta desventajas en términos de sus efectos negativos en el rendimiento de los dispositivos, la seguridad, la movilidad y la conectividad de extremo a extremo, y se debe considerar como una implementación a corto plazo para el agotamiento de direcciones, cuya solución a largo plazo es IPv6.

1. Tipos de NAT

Existen tres tipos de traducción NAT:

- **Traducción estática de direcciones (NAT estática)**: asignación de direcciones uno a uno entre una dirección local y una global.
- **Traducción dinámica de direcciones (NAT dinámica)**: asignación de varias direcciones a varias direcciones entre direcciones locales y globales.
- **Traducción de la dirección del puerto (PAT)**: asignación de varias direcciones a una dirección entre direcciones locales y globales. Este método también se conoce como "sobrecarga" (NAT con sobrecarga).

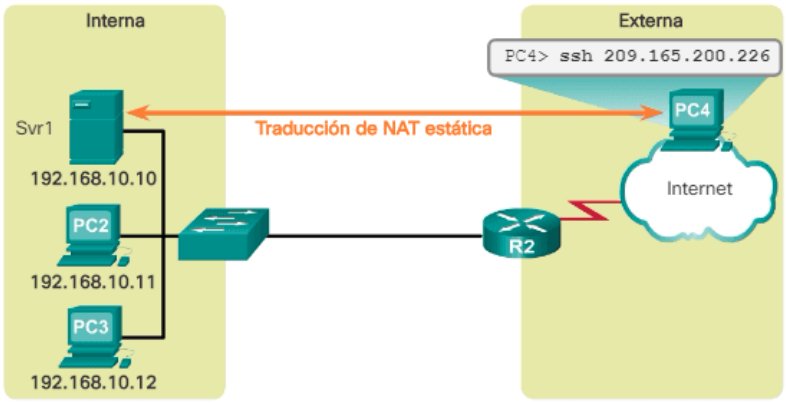
1.1. NAT estática

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes.

En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.

Tabla de NAT estática

Dirección local interna	Dirección global interna: direcciones a las que se puede llegar a través del R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



La NAT estática resulta útil, en especial **para los servidores web** o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa.

También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando no está en su lugar de trabajo, pero no el público en general en Internet. Por ejemplo, un administrador de red puede acceder a la dirección global interna del Svr1 (209.165.200.226) desde la PC4

mediante SSH. El R2 traduce esta dirección global interna a la dirección local interna y conecta la sesión del administrador al Svr1.

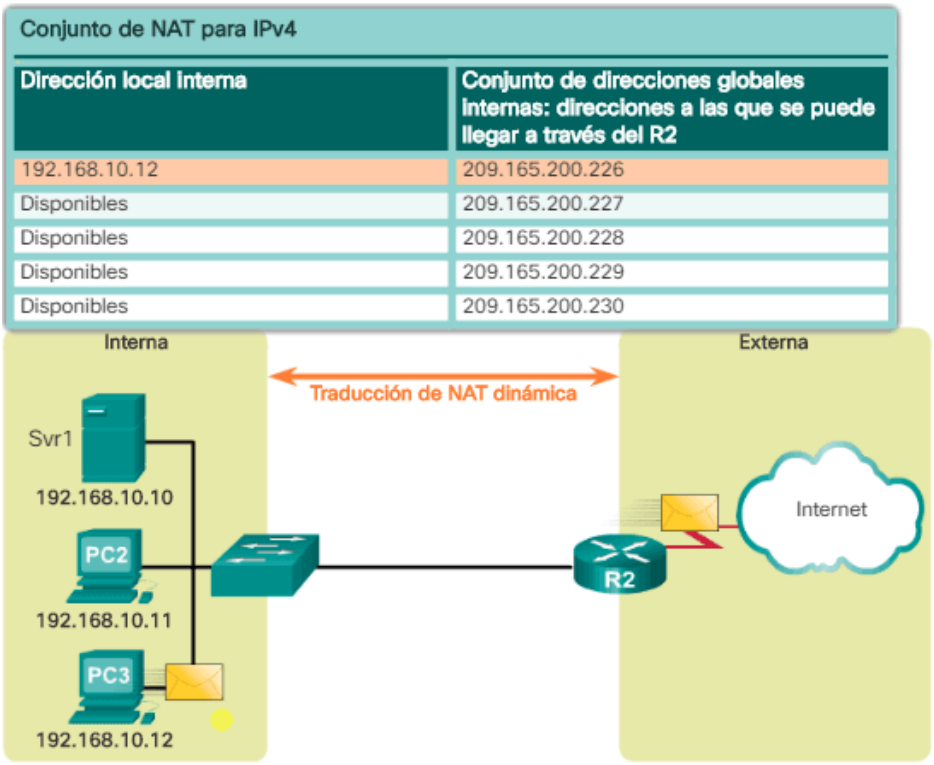
> "La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas."

1.2. NAT dinámica

varios a varios.

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.

Ver que SOLO hay IPs!!

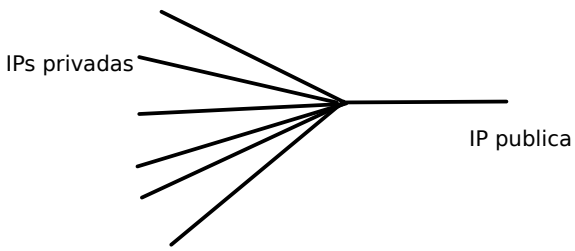


En la ilustración, la PC3 accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámica. Las demás direcciones siguen disponibles para utilizarlas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

1.3. Traducción de la dirección del puerto (PAT)

esto es lo que usan los modem o ont!!

La traducción de la dirección del puerto (PAT), también conocida como "**NAT con sobrecarga**" o Overlading, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones. Esto es lo que hace la mayoría de los routers domésticos. El ISP asigna una dirección al router, no obstante, varios miembros del hogar pueden acceder a Internet de manera simultánea. Esta es la forma más común de NAT.



Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto. Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva. Cuando el router NAT recibe un paquete del cliente, utiliza su número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.

PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.

Proceso de PAT

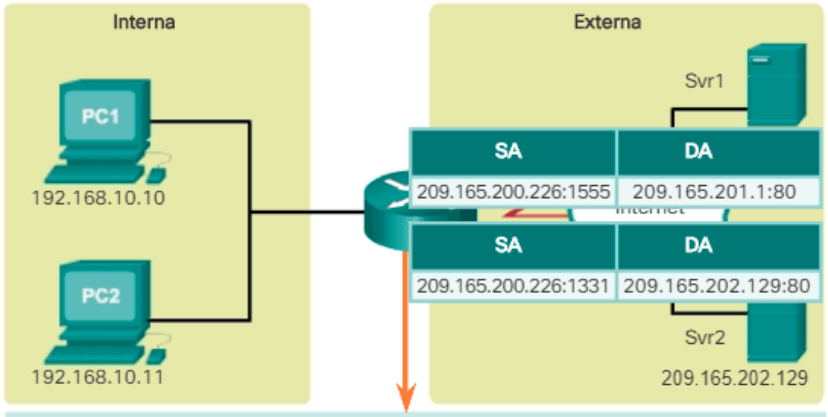


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.10:1331	209.165.202.129:80	209.165.202.129:80

En la Ilustración, se muestra el proceso de PAT. PAT agrega números de puerto de origen únicos a la dirección global interna para distinguir las traducciones.

A medida que el R2 procesa cada paquete, utiliza un número de puerto (1331 y 1555, en este ejemplo) para identificar el dispositivo en el que se originó el paquete. La dirección de origen (SA) es la dirección local interna a la que se agregó el número de puerto TCP/IP asignado. La dirección de destino (DA) es la dirección local externa a la que se agregó el número de puerto de servicio. En este ejemplo, el puerto de servicio es 80, que es HTTP.

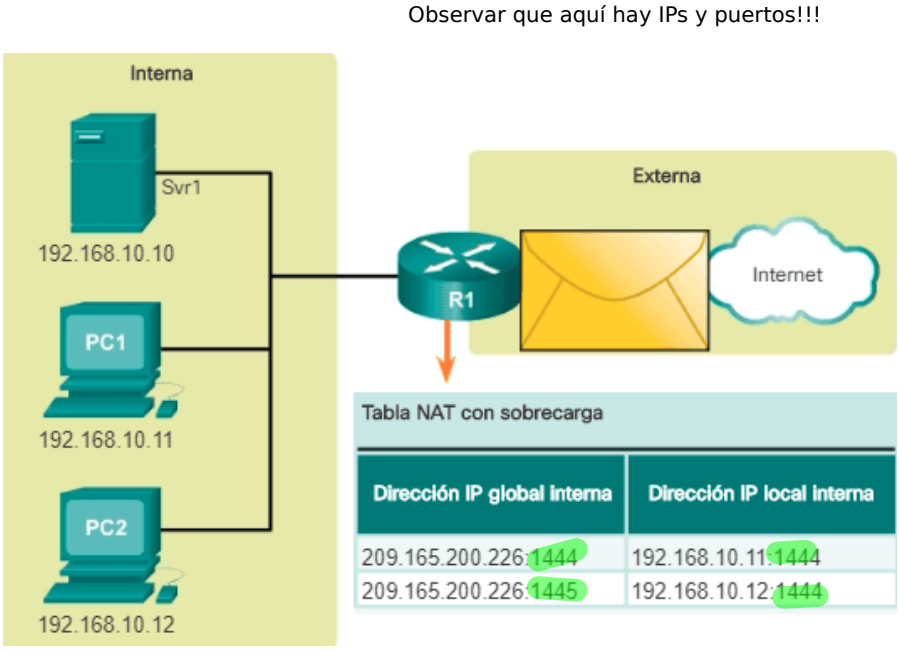
Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado. La dirección de destino no se modifica, pero ahora se la denomina “dirección IP global externa”. Cuando el servidor web responde, se invierte la ruta.

Siguiente puerto disponible ¿Que pasa si el nro. de puerto esta usado?

En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen inicial ya está en uso, PAT asigna el primer número de puerto disponible desde el comienzo del grupo de puertos correspondiente de 0 a 511, 512 a 1023 o 1024 a 65 535.

Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial. Este proceso continúa hasta que no haya más direcciones IP externas o puertos disponibles.



En la Ilustración, los hosts eligieron el mismo número de puerto 1444. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IP privadas únicas. Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen. En este ejemplo, PAT asignó el siguiente puerto disponible (1445) a la segunda dirección host.

2. Comparación entre NAT y PAT

Hacer un resumen de las diferencias entre NAT y PAT contribuye a la comprensión de ambas.

Como se muestran en la ilustración, NAT traduce direcciones IPv4 en una relación de 1:1 entre direcciones IPv4 privadas y direcciones IPv4 públicas. Sin embargo, PAT modifica la dirección y el número de puerto.

NAT reenvía los paquetes entrantes a su destino interno mediante la dirección IPv4 de origen de entrada proporcionada por el host en la red pública. En general, con PAT hay solo una o muy pocas direcciones IPv4 públicamente expuestas. Los paquetes entrantes de la red pública se enrutan a sus destinos en la red privada consultando una tabla en el router NAT. Esta tabla hace un seguimiento de los pares de puertos públicos y privados. Esto se denomina “**seguimiento de conexiones**“.

NAT

Conjunto de direcciones globales internas	Dirección local interna
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

No existen Puertos !!

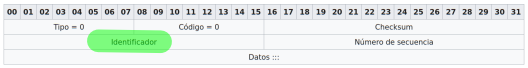
PAT

Dirección global interna	Dirección local interna
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

2.1. Paquetes sin segmento de capa 4

¿Qué sucede con los paquetes IPv4 que transportan datos que no son segmentos TCP o UDP? Estos paquetes no contienen un número de puerto de capa 4. ---> como ser ICMP!

PAT traduce la mayoría de los protocolos comunes transmitidos mediante IPv4 que no utilizan TCP o UDP como protocolo de la capa de transporte. El más común de ellos es ICMPv4. PAT maneja cada uno de estos tipos de protocolos de manera diferente.



Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta. ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta. La ID de consulta aumenta con cada solicitud de eco enviada. PAT utiliza la ID de consulta en lugar de un número de puerto de capa 4.

Nota: otros mensajes ICMPv4 no utilizan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían.

3.Ventajas de NAT

NAT proporciona muchos beneficios, incluido lo siguiente:

- **Conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets.** NAT conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto. Con la NAT con sobrecarga, los hosts internos pueden compartir una única dirección IPv4 pública para todas las comunicaciones externas. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir varios hosts internos.
- **Aumenta la flexibilidad de las conexiones a la red pública.** Se pueden implementar varios conjuntos y conjuntos de respaldo y de equilibrio de carga para asegurar conexiones de red pública confiables.

- **Proporciona coherencia a los esquemas de direccionamiento de red interna.** Para cambiar el esquema de direcciones IPv4 públicas en una red que no utiliza direcciones IPv4 privadas ni NAT, se requiere redireccionar todos los hosts en la red existente. Los costos de redireccionamiento de hosts pueden ser considerables. NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público. Esto significa que una organización podría cambiar los ISP sin necesidad de modificar ninguno de sus clientes internos.
- **NAT proporciona seguridad de red**. Debido a que las redes privadas no anuncian sus direcciones ni su topología interna, son razonablemente seguras cuando se utilizan en conjunto con NAT para obtener acceso externo controlado. Sin embargo, **NAT no reemplaza a los firewalls**.

4. Desventajas de la NAT

NAT presenta algunas desventajas. El hecho de que los hosts en Internet parezcan comunicarse de forma directa con el dispositivo con NAT habilitada, en lugar de hacerlo con el host real dentro de la red privada, genera una serie de inconvenientes.

- **Se deteriora el rendimiento:** en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo.
- **Se deteriora la funcionalidad de extremo a extremo**. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. Algunas aplicaciones no funcionan con NAT. Por ejemplo, algunas aplicaciones de seguridad, como las firmas digitales, fallan porque la dirección IPv4 de origen cambia antes de llegar a destino.
- **Se reduce el seguimiento IP de extremo a extremo.** El seguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de NAT se torna mucho más difícil y, en consecuencia, dificulta la resolución de problemas.
- **El tunneling se torna más complicado**. El uso de NAT también genera complicaciones para los protocolos de tunneling como IPsec, ya que NAT modifica los valores en los encabezados que interfieren en las verificaciones de integridad que realizan IPsec y otros protocolos de tunneling.
- **El inicio de las conexiones TCP puede interrumpirse**. Los servicios que requieren que se inicie una conexión TCP desde la red externa, o "protocolos sin estado", como los servicios que utilizan UDP, pueden interrumpirse. A menos que el router NAT esté configurado para admitir dichos protocolos, los paquetes entrantes no pueden llegar a su destino.

Resumen de Diferencias

NAT	PAT
*Se usa para permitir utilizar direcciones privadas y aun asi proveer conectividad con el resto de internet.	* Se usa para compartir a varias máquinas de la intranet una sola dirección IP en Internet.

*Basta tener una sola dirección IP publica para poder conectar multiples dispositivos.	*PAT utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones.
*Permite la reutilización de direcciones privadas.	*Protege la seguridad de la red. Debido a que las redes privadas no publican sus direcciones o topología interna
* Preserva el escaso direccionamiento público y abaratar coste.	
*Funciona como mecanismo de seguridad ya que esconde al exterior nuestra red privada.	
*Evita que los hackers o intrusos conozcan el direccionamiento interno.	