MODULO 2
PROTOCOLOS Y MODELOS DE COMUNICACION
Direcciones IP

REDES INFORMATICAS

Ing. Yarisol A. Castillo Q.

yarisol.castillo@utp.ac.pa

Introducción

¿Qué es una dirección IP?
Es como una dirección postal para tu dispositivo en internet. Permite que otros dispositivos y sitios web te encuentren.

Una **dirección IP (Internet Protocol)** es un **número único que identifica a cada dispositivo en una red**.

Versión	**Ejemplo**	**Características**
IPv4	192.168.1.15	32 bits → 4 números (0–255) separados por puntos.
IPv6	2001:0db8:85a3::8a2e:0370:7334	128 bits → más larga, usa números y letras hexadecimales.

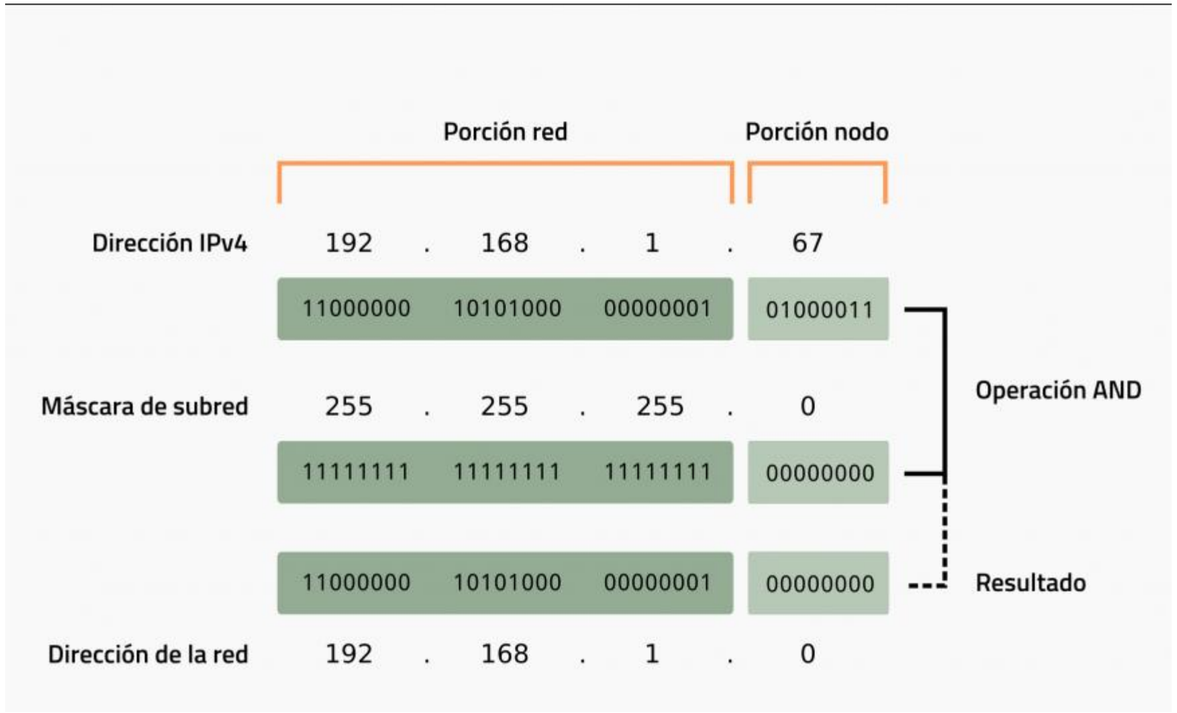
Partes de una dirección IPv4
Parte de red → identifica a la red a la que pertenece el dispositivo.
Parte de host → identifica al dispositivo dentro de esa red.

Máscara de red

La máscara de red (o máscara de subred) es un conjunto de números que se utiliza en redes informáticas para dividir una dirección IP en dos partes:

- **La parte de red, que identifica a la red a la que pertenece el dispositivo.**
- **La parte de host, que identifica a un dispositivo específico dentro de esa red.**

Por medio de una máscara de 32 bits, definiremos los bits que identifican la red (bits en 1) y los que identifican la estación (bits en 0).



Cómo funciona:

Una dirección IP (como 192.168.123.132) siempre se acompaña de una máscara de red (como 255.255.255.0).

La máscara indica qué bits de la IP corresponden a la red y cuáles al host.

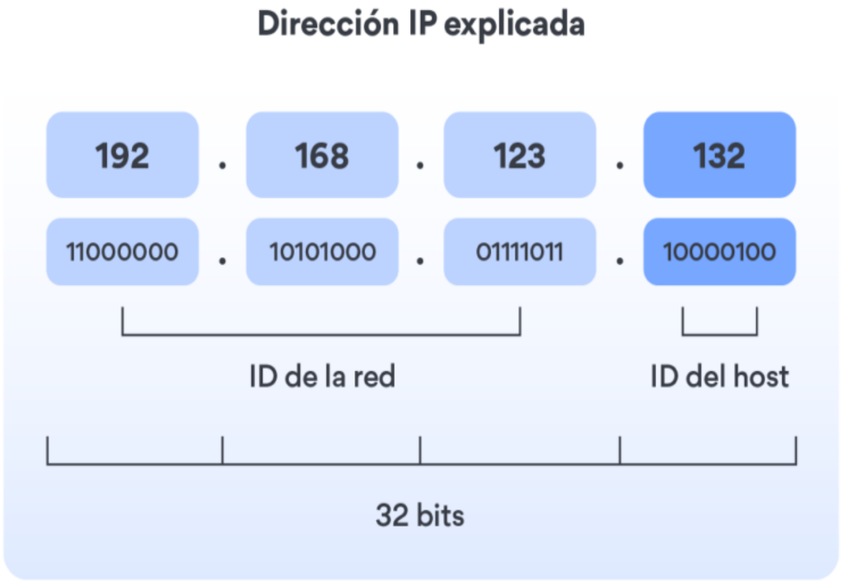
Ejemplo:
Dirección IP 192 . 168 . 123 . 132

Máscara de red 255 . 255 . 255 . 0

Los primeros 24 bits (255.255.255) indican la red → 192.168.123

El último 8 bits (0) indican el host → 132

Entonces todos los dispositivos que tengan direcciones 192.168.123.x con esa misma máscara están en la misma red local.



Notación CIDR (Classless Inter-Domain Routing)

Método de asignación y agregación de direcciones IP que permite una mayor flexibilidad en la división de rangos de direcciones IP en redes separadas.

Se representa mediante una dirección IP seguida de una barra diagonal (/) y un número que indica el tamaño de la máscara de subred.

- **Ayuda a optimizar el uso de direcciones IP**
- **Evita el agotamiento de las direcciones IPv4 disponibles.**

Notación: /número (CIDR), donde el número indica cuántos bits son para la red.

Ejemplos: **255.255.255.0 = /24**
255.255.0.0 = /16
255.0.0.0 = /8

CIDR: obtención de la dirección de red

- Para obtener la dirección de red a partir de la dirección IP de uno de sus hosts hay que hacer el AND lógico de la dirección IP con la máscara de red

Recuerda ....

Operaciones AND
1 AND 1 = 1
1 AND 0 = 0
0 AND 1 = 0
0 AND 0 = 0

10

Video para complementar→ https://youtu.be/f3bwe88iBHQ

Si tenemos dos estaciones con las direcciones
147.83.153.100
147.83.153.200,

podemos deducir que están interconectadas directamente (por una LAN) si la máscara de su red es 255.255.255.0, así como deduciríamos que no están conectadas con la misma LAN si la máscara fuese, por ejemplo, 255.255.255.128.

Máscaras de red

Por norma general, los bits 1 y los 0 son consecutivos, pero no necesariamente.

A continuación, definimos de nuevo el concepto identificador de red, adaptándolo a la máscara: el identificador de red es la porción de dirección IP que encaja con los bits 1 de la máscara.

El concepto máscara es capital para la comprensión del funcionamiento de las redes IP, permite a una estación decidir si el destino al que debe transmitir un paquete se encuentra dentro de la misma red de área local que este último o si, por el contrario, se encuentra en una LAN remota y, por tanto, debe delegar su transmisión a algún equipo de su misma LAN (el direccionador) para que se encargue de hacer llegar el paquete a su destino.

En resumen la máscara:
Define el tamaño de la red.
Permite a los dispositivos saber si otro equipo está en su misma red o en otra.
Es esencial para el enrutamiento de paquetes en redes IP.

Direcciones de propósito especial

DIRECCIÓN DE RED:

Las direcciones de red se expresan con la dirección que tendría cualquier estación suya y con todos los bits de identificador de estación a cero.

Por ejemplo, la red en que se encuentra la estación 147.83.153.100/24 es la 147.83.153.0/24

147.83.153.200/25 es la 147.83.153.128/25.

DIRECCIÓN 0.0.0.0.:

Esta dirección señala al mismo ordenador que la envía.
Tiene dos funciones básicas:

- Aparecer como dirección origen en paquetes IP generados por estaciones sin dirección IP asignada.
  Normalmente sólo aparece mientras la estación intenta averiguar su dirección mediante protocolos como:
  - **RARP (reverse address resolution protocol),**
  - **BOOTP (bootstrap protocol)**
  - **o DHCP (dynamic host configuration protocol).**

- Servir al software de gestión de direccionamiento para indicar la ruta por defecto.

Direcciones de propósito especial

DIRECCIÓN 127.0.0.1 (loopback) (en IPv6 es ::1):

La dirección de loopback es una dirección IP especial que permite que un dispositivo se comunique consigo mismo.
También se le llama localhost.

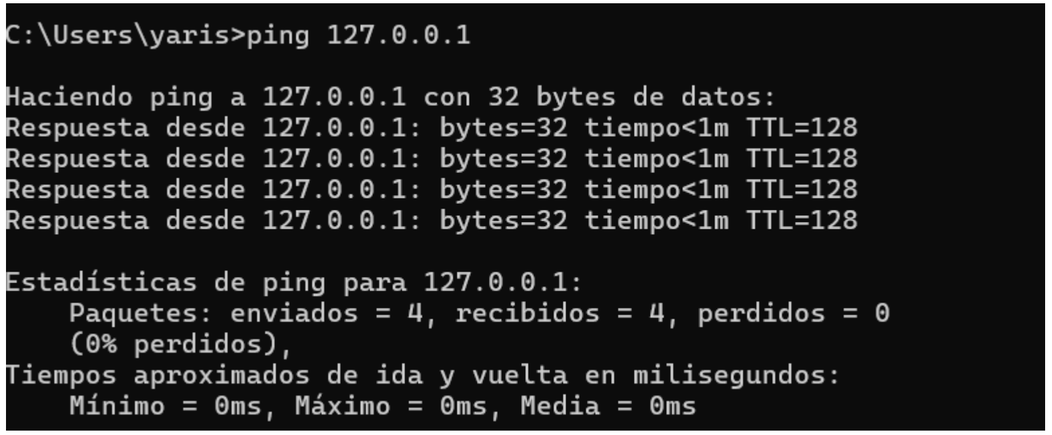
Pertenece a la red reservada 127.0.0.0/8, pero normalmente solo se usa la 127.0.0.1.

El software de red la utiliza para transmitir paquetes a la máquina local (de hecho, los paquetes no son enviados, sino que son entregados al destino por el mismo sistema operativo).

En realidad, los tres bytes del identificador de estación son irrelevantes. Esta dirección sólo tiene interés para programar aplicaciones; los sistemas de red no verán nunca que ningún paquete viaje por la red con esta dirección como origen o destino.

Ejemplo: ping 127.0.0.1

Ningún paquete enviado a 127.0.0.1 viajará por la red; todo se queda dentro del mismo dispositivo.



En resumen la dirección de loopback sirve para:

- **Probar la pila de red local:** Permite verificar que el software de red de tu computadora funciona, incluso sin estar conectado a Internet o a otra red.
- **Desarrollo y pruebas:** Los programadores la usan para ejecutar servidores y clientes en el mismo equipo.
- **Evitar tráfico externo:** Los datos enviados a 127.0.0.1 nunca salen de tu computadora.

Direcciones de propósito especial

DIRECCIÓN 255.255.255.255 (BROADCAST).

- **Es una dirección IP especial dentro de cada red.**
- **Se usa cuando un dispositivo necesita comunicarse con todos los demás dispositivos de su misma red local.**
- **Se utiliza para transmitir paquetes a todas las estaciones localizadas dentro de la misma LAN que la máquina de origen.**

Existe una versión equivalente, que es el broadcast dirigido.

En este segundo caso, el paquete es recibido por todas las máquinas de una LAN especificada por el identificador de red. El identificador de estación debe ser todo 1.

Por lo tanto, para enviar un broadcast a la red 147.83.153.0 con la máscara 255.255.255.0 (o 147.83.153.0/24)

podemos utilizar la dirección 255.255.255.255 si estamos dentro de la red 147.83.153.0, o bien la 147.83.153.255 si estamos en una estación remota.

El primer caso, lo llamaremos broadcast local, y el segundo, broadcast remoto.

Para qué se usa el broadcast

- Descubrir dispositivos en la red (por ejemplo, cuando un equipo busca el servidor DHCP).
- Para enviar anuncios o mensajes simultáneos a todos los hosts locales.
- Para sincronizar o actualizar información de red entre dispositivos.

Ejemplo:

Red: 192.168.1.0

Máscara: 255.255.255.0 → /24

Dirección de broadcast: 192.168.1.255

Esto significa que cualquier paquete enviado a 192.168.1.255 será recibido por todos los dispositivos en la red 192.168.1.x.

Recomendación:
Los routers normalmente no reenvían paquetes de broadcast a otras redes, porque solo deben circular dentro de la red local.
Usarlos en exceso puede saturar la red (por eso se usan con cuidado).

Direcciones de propósito especial

DIRECCIÓN IP PÚBLICA: dirección de tu casa en internet. Visible para todos y es asignada por tu proveedor de internet. Sirve para que otros dispositivos en internet puedan comunicarse contigo.
Son únicas en todo el mundo (no pueden repetirse).

Ejemplo: 8.8.8.8, 201.150.45.2, 190.168.1.10

Se usan en: servidores web, routers que conectan tu red a Internet, páginas web, etc.

DIRECCIÓN IP PRIVADA: dirección de una habitación dentro de tu casa. Es única dentro de tu red local (tu hogar, oficina, etc.) y no es visible desde internet. Sirve para que los dispositivos dentro de tu red se comuniquen entre sí.

Se usan dentro de redes locales (LAN).
Se pueden repetir en redes distintas porque solo funcionan internamente.
Los dispositivos locales (PC, impresoras, celulares, etc.) suelen usar este tipo.

Diferencias clave:

Alcance: Las públicas son visibles en todo internet, mientras que las privadas solo son visibles dentro de tu red.

Asignación: Las públicas las asigna tu proveedor de internet, mientras que las privadas las asigna tu router a cada dispositivo.

Seguridad: Las públicas son más fáciles de rastrear, mientras que las privadas ofrecen más privacidad dentro de tu red.

¿Por qué es importante saber esto?

Privacidad: Si te preocupa que te rastreen en línea, puedes usar una VPN para ocultar tu dirección IP pública.

Seguridad: Entender cómo funcionan las direcciones IP te ayuda a proteger tus dispositivos de ataques cibernéticos.

Rangos reservados para IP privadas:

Clase	Rango privado	Notación CIDR
A	10.0.0.0 – 10.255.255.255	/8
B	172.16.0.0 – 172.31.255.255	/12
C	192.168.0.0 – 192.168.255.255	/16

Ejemplos:
192.168.1.15,
10.0.0.5,
172.16.20.10

¿Se pueden rastrear las direcciones IP públicas?

Sí. Las direcciones IP públicas se pueden rastrear hasta el ISP, lo que podría revelar su ubicación geográfica general. Cuando los anunciantes, gobiernos o hackers saben desde dónde se conecta, les resulta más sencillo seguir sus actividades en línea.

Los sitios web también utilizan el seguimiento IP para analizar patrones de comportamiento en línea, por lo que les resulta más fácil determinar si la misma persona visita un sitio de forma repetida. Los sitios web emplean estos patrones para predecir sus preferencias.

¿Se pueden rastrear las direcciones IP privadas?
Sí, las direcciones IP privadas se pueden rastrear, pero solo por parte de otros dispositivos en su red local.

En resumen:

Dirección IP pública: Tu identidad en internet.
Dirección IP privada: Tu identidad dentro de tu red local.

¿Como podemos proteger nuestra dirección ip?

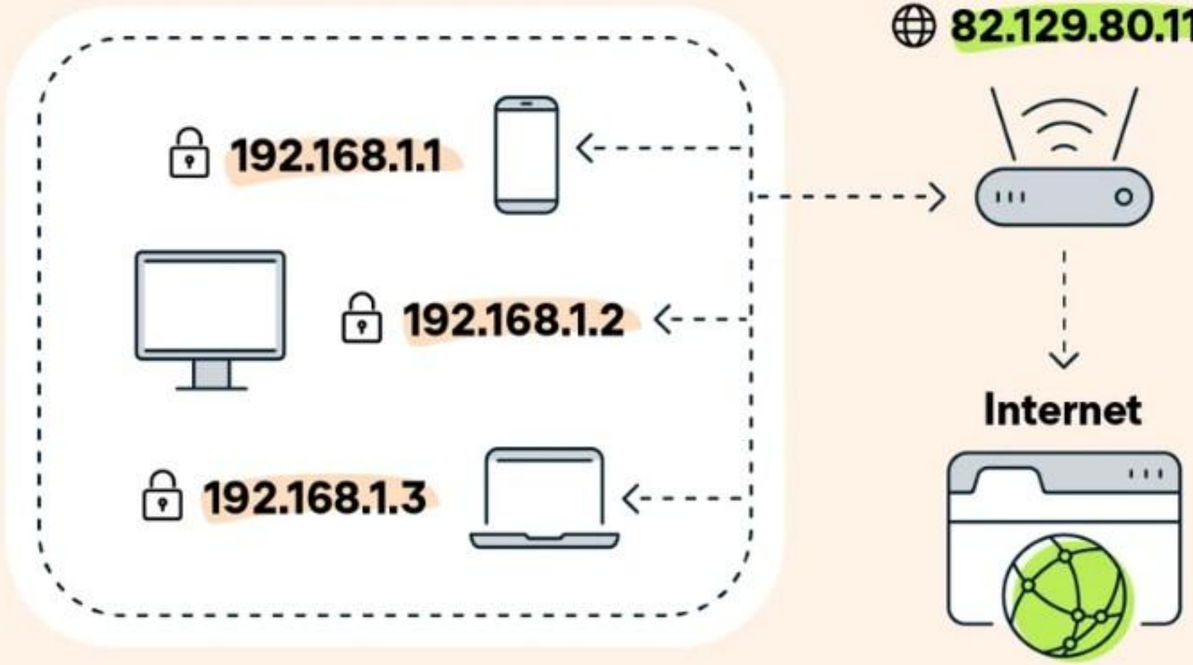
La dirección IP pública es útil pero también puede causar un problema:

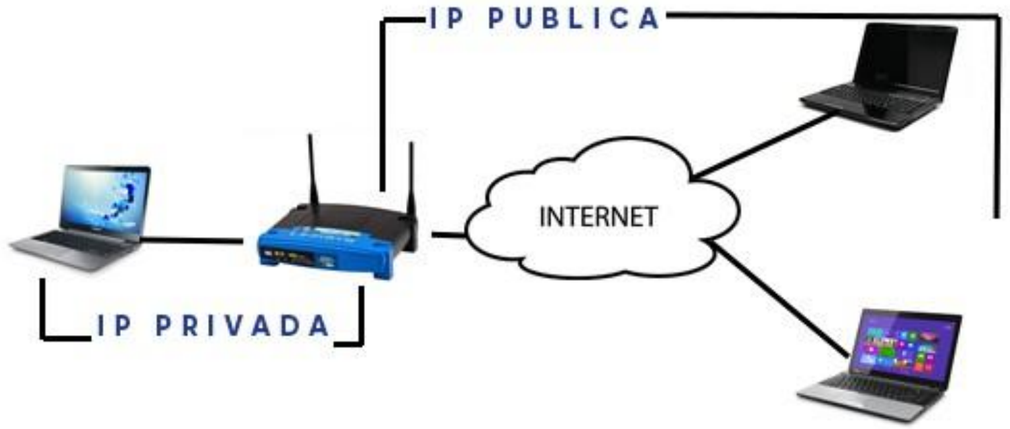
Porque es totalmente visible en línea. El mejor modo de proteger su auténtica dirección IP es utilizar una VPN, que redirige todo el tráfico en línea a través de un servidor independiente y muy alejado de su ubicación real.

Ejemplo Ilustrativo

Privada / Local / Interna
- generada automáticamente

Pública / Externa
- asignada por el ISP



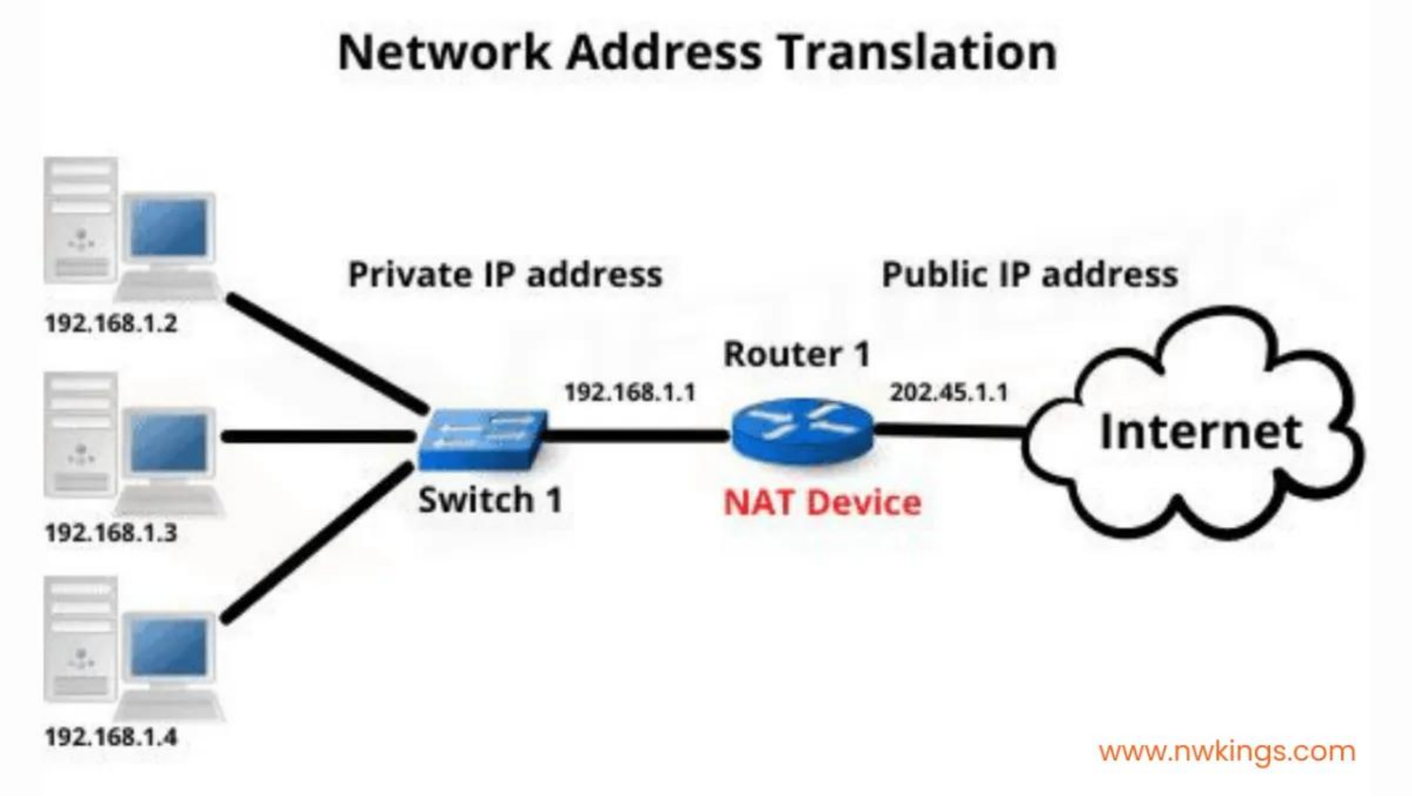


Se encuentra en la configuración interna del dispositivo

Se encuentra escribiendo en Google: «¿Cuál es mi dirección IP?»

Cómo muchas direcciones privadas comparten una pública?

NAT (Network Address Translation) / Traducción de Direcciones de Red



Lo hace el router (o firewall).

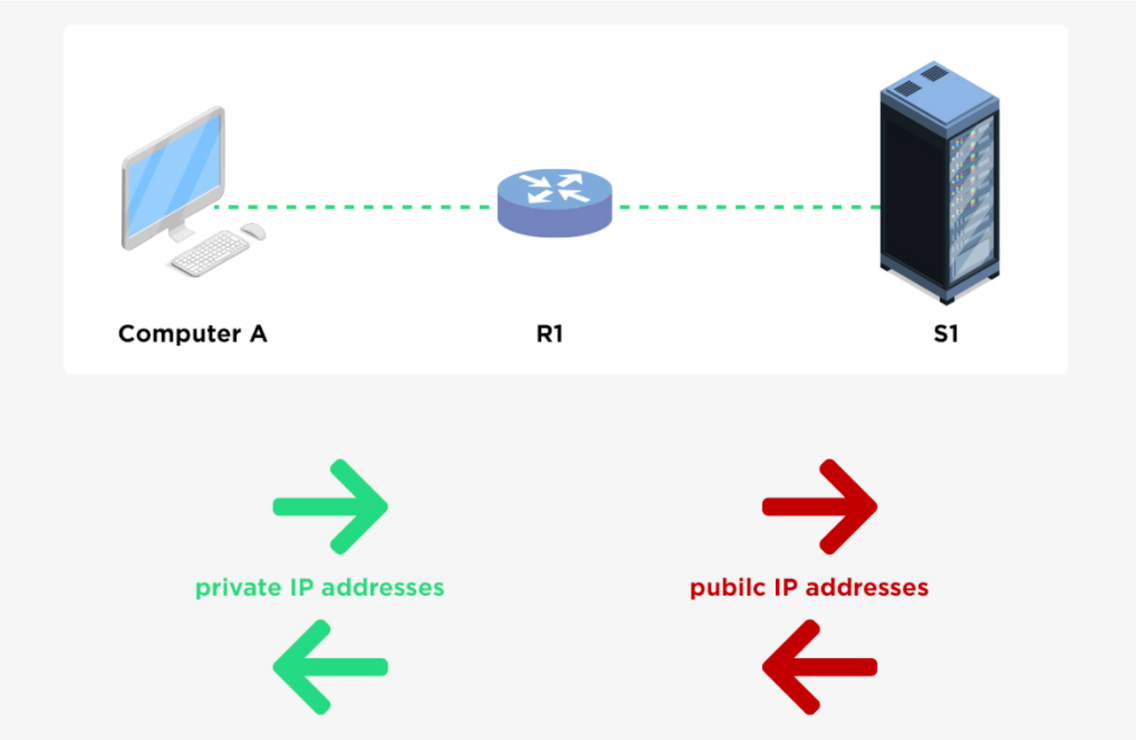
Traduce las direcciones IP privadas de tu red local en una sola IP pública cuando los dispositivos salen a Internet.

También traduce las respuestas de vuelta a la IP privada correcta.

Ejemplo1:

Tres dispositivos en casa con IP privadas:
PC → 192.168.1.2
Celular → 192.168.1.3
Tablet → 192.168.1.4

Tu router tiene:
IP privada en tu red local: 192.168.1.1
IP pública: 190.45.60.10



Para ver Internet:

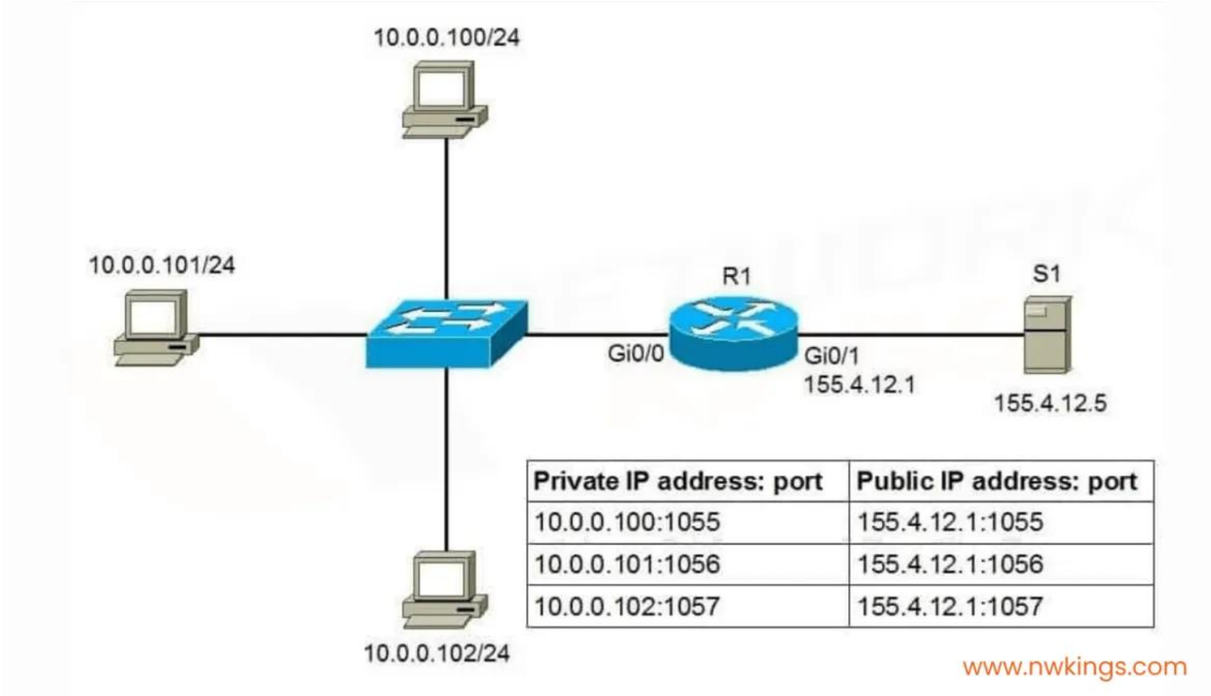
1. Cada dispositivo envía su tráfico al router.
2. El router cambia (traduce) la IP de origen por su IP pública 190.45.60.10.
3. El router lleva un registro de qué conexión pertenece a qué dispositivo (tabla NAT).
4. Cuando llega la respuesta de Internet, el router la envía al dispositivo correcto usando esa tabla.

¿Cuales son los tipos de NAT?

- **NAT Estático:** traduce una dirección IP privada a una pública. La dirección IP pública siempre es la misma. Esta NAT solo se aplica si solo una persona accede a Internet a la vez en un edificio. Este no es un caso real.

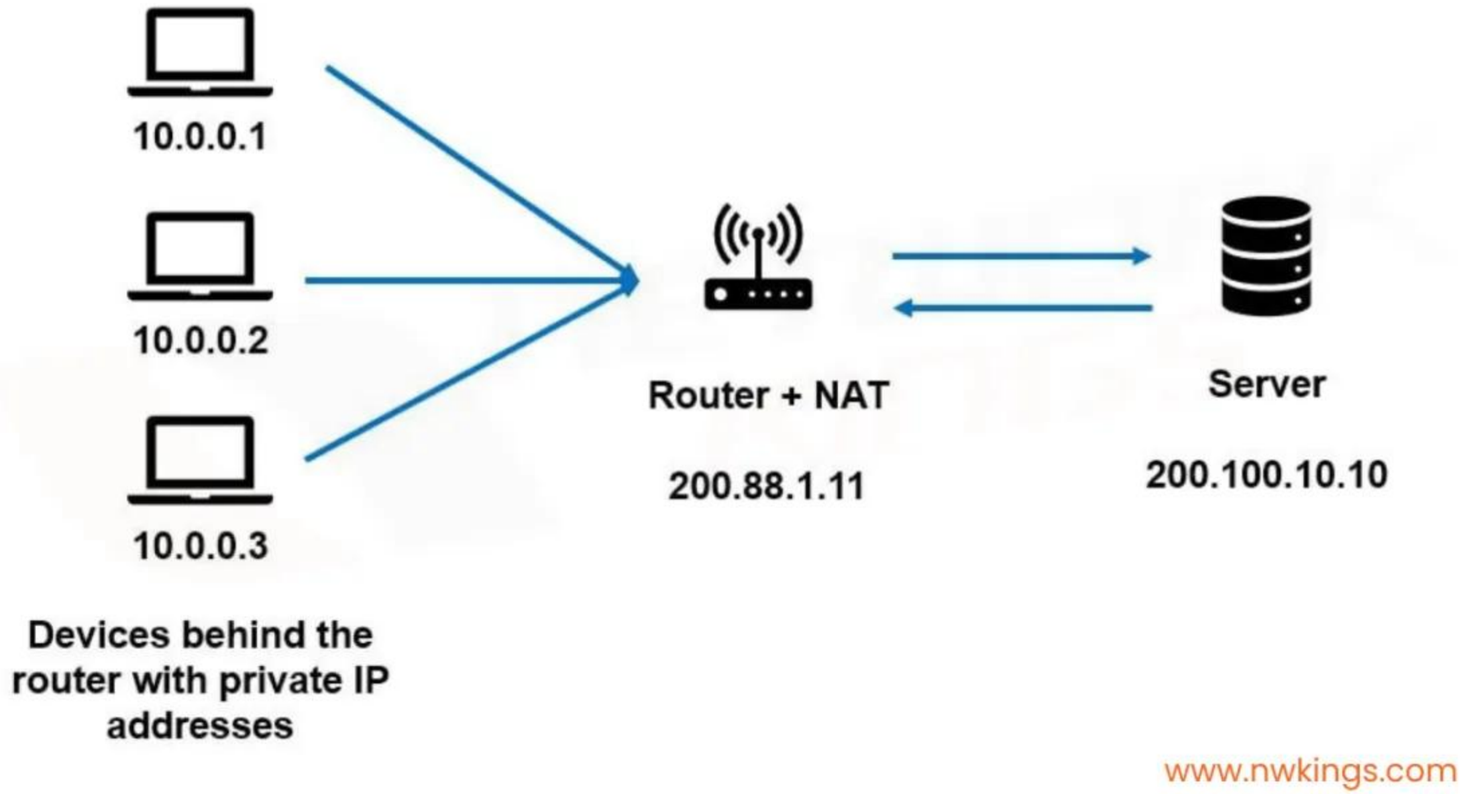
- **NAT Dinámico:** se mapean las direcciones IP privadas al pool de direcciones públicas. La IP pública puede variar. Asigna direcciones públicas disponibles de un grupo.

- **Port Address Translation (PAT):** se usa una sola dirección IP pública para todos los dispositivos internos, pero se asigna un puerto distinto a cada dirección privada. Este método nos proporciona más flexibilidad para utilizar direcciones IP registradas públicamente.
  Traduce varias IP privadas a una sola IP pública usando puertos distintos. Es el más usado en casas.



Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Cómo es la arquitectura NAT?



El **dominio interno** está compuesto por los hosts o dispositivos con direcciones IP privadas. El **dominio externo** está compuesto por el servidor.

La solicitud del host se envía desde el origen con una dirección IP privada y se convierte a una dirección IP pública al llegar a la dirección IP de destino mediante NAT. Por lo tanto, el NAT funciona en línea recta.

En resumen:

- **Cada dispositivo conectado a una red necesita una IP.**
- **Sirven para identificar y localizar dispositivos.**
- **Hay diferentes tipos (pública, privada, loopback, broadcast) y versiones (IPv4, IPv6).**
- Enrutamiento de la información. Los routers usan las direcciones IP para decidir por dónde enviar los paquetes de datos.
- Sin direccionamiento, no se podría mover información entre redes diferentes (como Internet).
- Comunicación entre redes. Permite que millones de redes diferentes se conecten entre sí y funcionen como una sola gran red (Internet).
- Administración y seguridad. Ayuda a controlar el acceso a la red (qué dispositivos pueden conectarse).Permite aplicar políticas de seguridad, filtrado y control de tráfico.

NAT TIENE ALGUNAS VENTAJAS:

- **Permite ahorrar direcciones IPv4 públicas.**
- **Protege la red interna (las IP privadas no son visibles desde fuera).**
- **Facilita la administración de redes domésticas.**