







DHCP, DNS, NAT y PAT: Fundamentos de Redes

Conceptos clave para la ciberseguridad en redes

Índice


-  **DHCP**: Asignación dinámica de IPs
-  **DNS**: Traducción de nombres en IPs
-  **NAT**: Network Address Translation
-  **PAT**: Port Address Translation
-  Ataques y defensas
-  Conclusiones


DHCP: Asignación Dinámica de IPs

¿Qué es DHCP?

El **Protocolo de Configuración Dinámica de Host (DHCP)** es un protocolo de red que permite a los dispositivos de una red obtener automáticamente sus parámetros de configuración de red, como la dirección IP, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS, de un servidor DHCP. Esto simplifica enormemente la administración de la red, eliminando la necesidad de configurar manualmente cada dispositivo.

Características Clave

 **Capa de Aplicación (Capa 7):** DHCP opera en la capa de aplicación del modelo OSI.

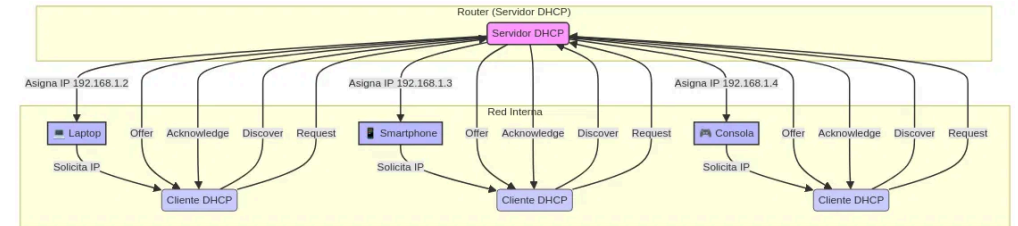
 **Protocolo de Transporte UDP:** Utiliza el Protocolo de Datagramas de Usuario (UDP) para sus comunicaciones, específicamente los puertos 67 (para el servidor) y 68 (para el cliente).

 **Automatización:** Facilita la gestión de direcciones IP en redes grandes y pequeñas, reduciendo errores de configuración y conflictos de IP.

DHCP: Proceso DORA

El proceso de asignación de una dirección IP por DHCP sigue cuatro pasos fundamentales, conocidos como DORA:

- 1 Discover (Descubrimiento):** El cliente DHCP envía un mensaje de difusión (broadcast) para encontrar servidores DHCP disponibles en la red.
- 2 Offer (Oferta):** Los servidores DHCP responden con un mensaje Offer, proponiendo una dirección IP disponible y otros parámetros de configuración.
- 3 Request (Solicitud):** El cliente DHCP selecciona una oferta y envía un mensaje Request al servidor elegido, solicitando formalmente la dirección IP ofrecida.
- 4 Acknowledge (Reconocimiento):** El servidor DHCP confirma la asignación de la dirección IP al cliente con un mensaje Acknowledge, completando el proceso.




DNS: Traducción de Nombres en IPs


¿Qué es DNS?

El **Sistema de Nombres de Dominio (DNS)** es un sistema de nomenclatura jerárquico y descentralizado para dispositivos conectados a redes IP, como Internet. Su función principal es traducir nombres de dominio legibles por humanos (por ejemplo, `www.ejemplo.com`) a direcciones IP numéricas (por ejemplo, `192.0.2.1`), que son las que las computadoras utilizan para identificarse entre sí.

Características Clave

 **Capa de Aplicación (Capa 7):** DNS opera en la capa de aplicación del modelo OSI.

 **Protocolo de Transporte UDP/TCP:** Utiliza UDP en el puerto 53 para consultas rápidas y TCP en el puerto 53 para transferencias de zona (sincronización de bases de datos DNS entre servidores).

 **Esencial para la Navegación:** Sin DNS, los usuarios tendrían que recordar direcciones IP numéricas para acceder a sitios web y otros recursos en línea.

DNS: Funcionamiento

El proceso de resolución DNS comienza cuando un usuario intenta acceder a un recurso en la red utilizando un nombre de dominio. El navegador o la aplicación cliente envía una consulta DNS a un servidor DNS, que se encarga de encontrar la dirección IP correspondiente al nombre de dominio solicitado.

Flujo de Resolución DNS

- 1 **Usuario escribe:** http://miportal
- 2 **Servidor DNS responde:** 192.168.1.5 (la dirección IP asociada a miportal)
- 3 **Navegador conecta:** El navegador utiliza la dirección IP 192.168.1.5 para establecer una conexión con el servidor web alojado en la laptop.

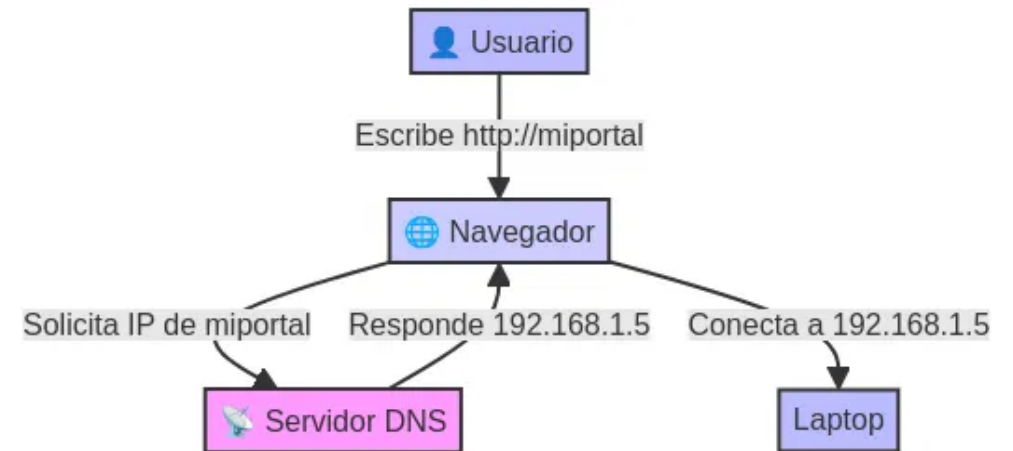


Diagrama del proceso de resolución DNS

NAT: Network Address Translation

¿Qué es NAT?

Network Address Translation (NAT) es un método de reasignación de un espacio de direcciones IP a otro, modificando la información de dirección de red en el encabezado IP de los paquetes mientras están en tránsito a través de un dispositivo de enrutamiento de tráfico. Su principal función es permitir que múltiples dispositivos en una red privada compartan una única dirección IP pública para acceder a Internet, conservando así el limitado espacio de direcciones IPv4.

Características Clave



Capa de Red (Capa 3): NAT opera en la capa de red del modelo OSI.



Conservación de IPs: Ayuda a mitigar el agotamiento de direcciones IPv4 al permitir que una red privada utilice un conjunto de direcciones IP internas que no son enrutables en Internet.



Tipos de NAT: Static NAT (1:1), Dynamic NAT (grupo a grupo) y NAT Overload/PAT (muchos a uno con puertos).

NAT: Funcionamiento

Cuando un dispositivo en la red interna inicia una conexión hacia Internet, el router con NAT intercepta el paquete. Antes de reenviarlo a la red externa, el router reemplaza la dirección IP privada de origen del paquete con su propia dirección IP pública.

Ejemplo Práctico

Pequeña empresa con varias PCs en una red privada:

Interno: 192.168.1.2, 192.168.1.3, 192.168.1.4

Externo: 203.0.113.1 (única IP pública)

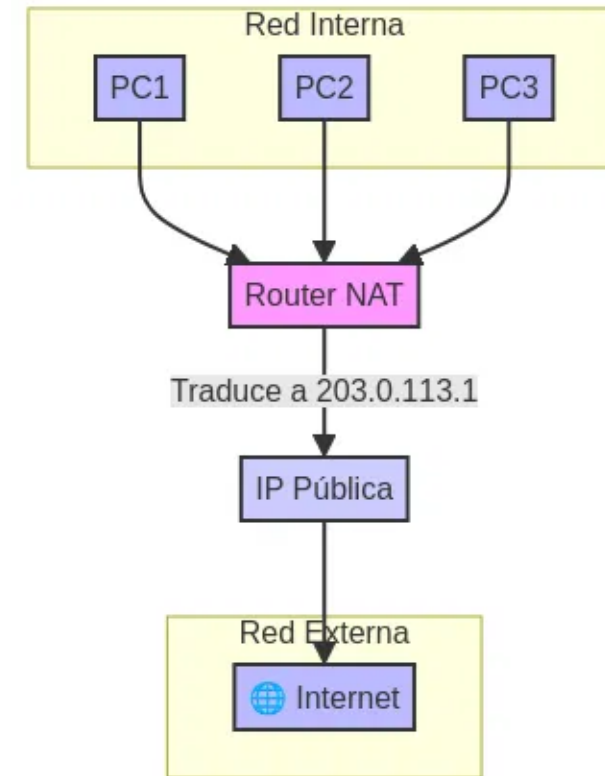
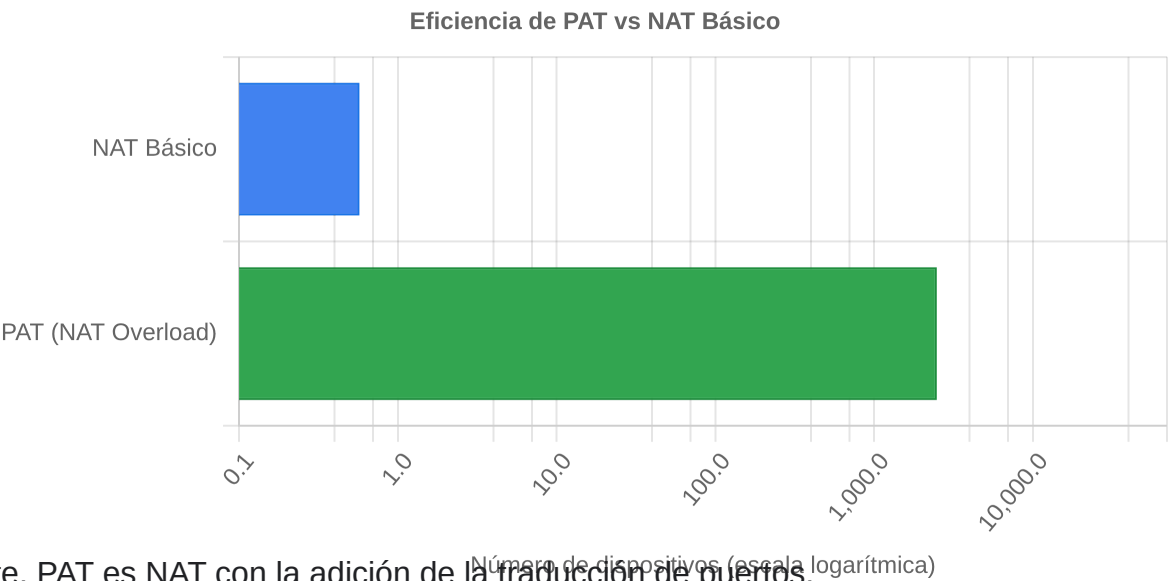


Diagrama de funcionamiento de NAT: Múltiples dispositivos internos comparten una IP pública

PAT: Port Address Translation

¿Qué es PAT?

Port Address Translation (PAT), también conocido como NAT Overload, es una forma específica de Network Address Translation (NAT) que permite que múltiples dispositivos en una red privada compartan una única dirección IP pública. A diferencia de otros tipos de NAT, PAT logra esto asignando un número de puerto de origen único a cada conexión saliente. Cuando el tráfico regresa, el router PAT utiliza el número de puerto de destino para dirigir el paquete al dispositivo interno correcto.



Características Clave

- + PAT = NAT + Puertos:** Esencialmente, PAT es NAT con la adición de la traducción de puertos.
- Alta Eficiencia:** Permite que un gran número de dispositivos (decenas o cientos) compartan una sola dirección IP pública, maximizando el uso de las direcciones IPv4 disponibles.
- Mapeo de Sesiones:** El router mantiene una tabla de mapeos que asocia la combinación de IP privada y puerto de origen con la IP pública y el puerto asignado para cada sesión de comunicación.

PAT: Funcionamiento

El router PAT asigna un puerto único a cada conexión saliente de los dispositivos internos. Esto permite diferenciar el tráfico de cada dispositivo cuando las respuestas regresan de Internet, todo a través de una única dirección IP pública.

Ejemplo de Tráfico

PC1 (192.168.1.2) pide una web → El router traduce a **203.0.113.1:10001**

PC2 (192.168.1.3) juega online → El router traduce a **203.0.113.1:10002**

PC3 (192.168.1.4) hace streaming → El router traduce a **203.0.113.1:10003**

Cuando un servidor externo responde a 203.0.113.1:10001, el router sabe que debe reenviar esa respuesta a PC1.

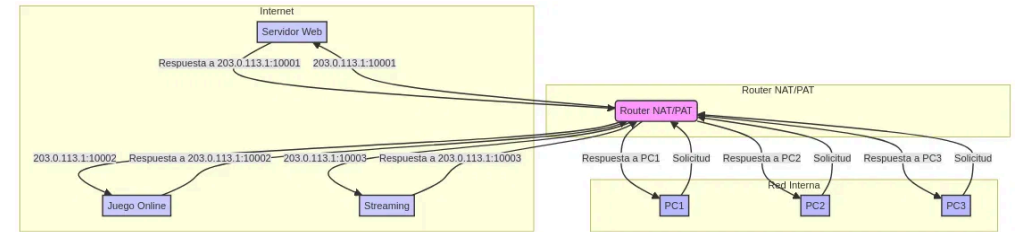


Diagrama de funcionamiento de PAT: Asignación de puertos únicos a cada dispositivo

Ataques y Defensas en DHCP, DNS, NAT y PAT

La implementación de estos servicios de red conlleva riesgos de seguridad que deben ser mitigados con defensas adecuadas. A continuación, se presenta un resumen de los ataques comunes y sus respectivas contramedidas:

Servicio	Ataques Comunes	Defensas Recomendadas
DHCP	<ul style="list-style-type: none">⚠️ DHCP Starvation (agotamiento de direcciones)⚠️ Rogue DHCP (servidor DHCP falso)	<ul style="list-style-type: none">🛡️ DHCP Snooping🛡️ Rangos limitados de IP🛡️ Reservas de IP por MAC
DNS	<ul style="list-style-type: none">⚠️ DNS Spoofing (suplantación)⚠️ Cache Poisoning (envenenamiento de caché)⚠️ DNS Tunneling (túneles DNS)	<ul style="list-style-type: none">🛡️ DNSSEC (DNS Security Extensions)🛡️ Filtrado de dominios🛡️ Monitorización de tráfico DNS
NAT/PAT	<ul style="list-style-type: none">⚠️ NAT Traversal (evasión de NAT)⚠️ Port Scanning (escaneo de puertos)⚠️ Session Hijacking (secuestro de sesión)	<ul style="list-style-type: none">🛡️ Firewalls NGFW🛡️ IDS/IPS (Sistemas de detección/prevención)🛡️ Segmentación de red🛡️ VPN/IPsec

Es crucial implementar una estrategia de seguridad en capas que combine estas defensas para proteger la infraestructura de red de manera efectiva.

Conclusiones



DHCP

Simplifica la administración de la red al automatizar la asignación de direcciones IP, reduciendo la carga de trabajo manual y minimizando errores de configuración.



DNS

Actúa como la "guía telefónica" de Internet, traduciendo nombres de dominio legibles por humanos a direcciones IP, esencial para la navegación web.



NAT

Permite la optimización del uso de direcciones IP públicas, posibilitando que múltiples dispositivos en una red privada compartan una única IP pública.



PAT

Extiende las capacidades de NAT mediante el uso de puertos, permitiendo que cientos de dispositivos compartan una sola dirección IP pública.



La correcta configuración y protección de estos servicios es vital para mantener la integridad, disponibilidad y seguridad de la red.