MANUAL PRÁCTICO

# IP ADDRESSING & SUBNETTING PARA PENTESTERS DE CERO A PRO

*MIGUEL ANGEL VILLALOBOS GARCIA*

# IP Addressing & Subnetting para Pentesters: de cero a PRO




Autor: **Miguel Ángel Villalobos García** | https://www.linkedin.com/in/m7villalobos/

# Introducción

Este manual está diseñado para proporcionar a los profesionales de la seguridad ofensiva, específicamente a los pentesters, un conocimiento profundo y práctico del direccionamiento IP en sus versiones IPv4 e IPv6. La comprensión del direccionamiento IP va más allá de la teoría; es fundamental para interpretar cómo se estructuran las redes, cómo fluye el tráfico y, lo más importante desde la perspectiva de un pentester, cómo estos sistemas pueden ser reconocidos, enumerados, eludidos y potencialmente explotados durante una evaluación de riesgos de seguridad.

El dominio del direccionamiento IP es una habilidad esencial en el arsenal de un pentester. Permite definir con precisión el alcance de las pruebas, identificar activos críticos, comprender la segmentación de la red, interpretar los resultados de las herramientas de escaneo como Nmap, y analizar el tráfico capturado con herramientas como Wireshark para extraer inteligencia valiosa. Además, un conocimiento sólido de los mecanismos de asignación como DHCP y SLAAC, así como de las tecnologías de traducción como NAT y PAT, revela vectores de ataque específicos y las contramedidas que se pueden encontrar.[1]
Con la progresiva adopción de IPv6 junto al omnipresente IPv4, la competencia en ambos protocolos ya no es opcional, sino una necesidad.[4] Este manual abordará ambos protocolos, cubriendo desde los conceptos fundamentales hasta las técnicas avanzadas y consideraciones de seguridad relevantes para la práctica del pentesting, asegurando que el lector esté equipado para navegar y evaluar las redes modernas.

# 1. Fundamentos de Direccionamiento IPv4 para Pentesters

El Protocolo de Internet versión 4 (IPv4) ha sido la columna vertebral de la comunicación en Internet durante décadas. Aunque enfrenta limitaciones de espacio de direcciones, su comprensión sigue siendo crucial para cualquier pentester, ya que la gran mayoría de las redes internas y muchas redes externas todavía dependen en gran medida de él.

## Estructura IPv4: 32 Bits y Notación Decimal Punteada

Una dirección IPv4 es fundamentalmente un número de 32 bits.[7] Esta estructura binaria es la que utilizan las máquinas para identificar de forma única a los hosts (como computadoras, servidores, impresoras o routers) dentro de una red TCP/IP.[10] Para facilitar la lectura y el manejo por parte de los humanos, esta secuencia de 32 bits se divide en cuatro secciones de 8 bits cada una, conocidas como octetos o bytes.[10]
Cada octeto se convierte a su valor decimal equivalente, que puede variar de 0 a 255. Estas cuatro cifras decimales se separan por puntos, dando lugar a la familiar **notación decimal punteada**, como por ejemplo, 192.168.1.1.[7] Es vital recordar que aunque vemos la notación

decimal, la representación subyacente que utilizan los dispositivos de red es binaria. Por ejemplo, 192.168.1.1 en binario es 11000000.10101000.00000001.00000001.[9] Conceptualmente, cada dirección IPv4 se divide en dos partes principales: el **Identificador de Red (Network ID)** y el **Identificador de Host (Host ID)**.[10] El Network ID identifica la red específica a la que pertenece el dispositivo, mientras que el Host ID identifica de forma única a ese dispositivo dentro de esa red. La línea divisoria exacta entre estas dos partes no es inherente a la dirección IP en sí misma, sino que es definida por un valor complementario: la máscara de subred.[10]

- **Relevancia para Pentesters:** La comprensión precisa de la estructura de 32 bits y la notación decimal punteada es la base absoluta para cualquier actividad de pentesting. Permite interpretar correctamente los resultados de las herramientas de escaneo (como Nmap), definir los rangos de objetivos con precisión, analizar el tráfico de red capturado (con Wireshark) y, en fases más avanzadas, construir paquetes personalizados para técnicas de evasión o explotación. Un error en la interpretación de un octeto o su equivalente binario puede llevar a escanear redes incorrectas, violar el alcance definido o fallar en la explotación de vulnerabilidades dependientes de la red.

## Contexto Histórico: Direccionamiento con Clases (A, B, C) y Sus Limitaciones

Originalmente, entre 1981 y 1993, la asignación de direcciones IPv4 se regía por un sistema conocido como **direccionamiento con clases**.[13] Este método dividía el espacio total de direcciones IPv4 en cinco clases (A, B, C, D y E), aunque solo las clases A, B y C se utilizaban comúnmente para la asignación a redes de hosts.[1] La clase de una dirección se determinaba por los primeros bits del primer octeto:

- **Clase A:** El primer bit es 0. Rango: 1.0.0.0 a 126.255.255.255. Máscara por defecto: 255.0.0.0 (/8). Diseñada para redes muy grandes, permitiendo hasta 224−2 (más de 16 millones) de hosts por red, pero solo 126 redes de este tipo.[1]
- **Clase B:** Los primeros dos bits son 10. Rango: 128.0.0.0 a 191.255.255.255. Máscara por defecto: 255.255.0.0 (/16). Para redes medianas a grandes, permitiendo 216−2 (65,534) hosts por red, con 16,384 redes posibles.[1]
- **Clase C:** Los primeros tres bits son 110. Rango: 192.0.0.0 a 223.255.255.255. Máscara por defecto: 255.255.255.0 (/24). Para redes pequeñas, permitiendo 28−2 (254) hosts por red, pero con más de 2 millones de redes posibles.[1]

Las **limitaciones** de este sistema se hicieron evidentes rápidamente con el crecimiento de Internet [1]:

1. **Ineficiencia y Desperdicio de Direcciones:** Las clases A y B asignaban bloques

enormes que a menudo eran subutilizados por las organizaciones, desperdiciando millones de direcciones IP. Por el contrario, la Clase C era frecuentemente demasiado pequeña para las necesidades de muchas organizaciones, forzándolas a solicitar un bloque de Clase B (desperdiciando aún más direcciones) o múltiples bloques de Clase C (fragmentando su espacio de direcciones).[1]

2. **Agotamiento del Espacio IPv4:** Esta ineficiencia aceleró drásticamente el agotamiento del limitado espacio de direcciones IPv4.[1] La demanda superó rápidamente la oferta disponible bajo este esquema rígido.
3. **Crecimiento de las Tablas de Enrutamiento:** La asignación de bloques fijos y, a veces, múltiples bloques de Clase C no contiguos a una sola organización, contribuyó a un crecimiento explosivo de las tablas de enrutamiento globales en los routers de Internet, lo que afectaba el rendimiento y la gestión.[1]

Además, existían las **Clases D y E**:

- **Clase D:** Primeros cuatro bits 1110. Rango: 224.0.0.0 a 239.255.255.255. Reservada para direccionamiento **multicast**.[1]
- **Clase E:** Primeros cuatro bits 1111. Rango: 240.0.0.0 a 255.255.255.255. Reservada para **uso experimental o futuro**, no utilizada en la práctica en la Internet pública.[1]
- **Relevancia para Pentesters:** Aunque el direccionamiento por clases está obsoleto para la asignación moderna, comprenderlo sigue siendo útil. Ayuda a interpretar documentación de red antigua, configuraciones heredadas o el comportamiento predeterminado de algunas herramientas o sistemas operativos más antiguos. Reconocer una dirección y su máscara de clase predeterminada (por ejemplo, ver una IP 150.100.x.x e inferir inicialmente una máscara /16) puede ofrecer una pista inicial sobre el tamaño potencial de una red antes de descubrir un subnetting más específico. Proporciona el contexto histórico esencial para entender por qué se desarrollaron y son omnipresentes las técnicas de CIDR y subnetting (Sección 2), que superaron estas limitaciones.

## Rangos Esenciales: IP Públicas vs. Privadas (RFC 1918) y Direcciones de Uso Especial

No todas las direcciones IPv4 son iguales en términos de su alcance y propósito. Una distinción fundamental para cualquier pentester es entre direcciones IP públicas y privadas.

- **Direcciones IP Públicas:** Son direcciones asignadas por autoridades de registro de Internet (IANA y los Registros Regionales de Internet o RIRs como ARIN, RIPE NCC, APNIC, etc.).[2][3] Son **globalmente únicas** y **enrutables** a través de la Internet pública.[4] Cualquier dispositivo que necesite ser directamente accesible desde Internet (como servidores web, servidores de correo, etc.) debe tener una dirección IP pública.
- **Direcciones IP Privadas (RFC 1918):** Para conservar el limitado espacio de direcciones

IPv4 públicas y proporcionar un nivel básico de separación de red, el RFC 1918 [23] definió tres bloques de direcciones reservadas exclusivamente para uso en redes internas (privadas).[4] Estas direcciones **no son enrutables** en la Internet pública; los routers de los proveedores de servicios de Internet (ISP) están configurados para descartar cualquier tráfico con origen o destino en estos rangos.[4] La principal ventaja es que cualquier organización puede utilizar estas direcciones internamente sin necesidad de coordinación externa, y pueden ser reutilizadas por innumerables redes privadas en todo el mundo.[4]

**Tabla: Rangos de Direcciones IPv4 Privadas (RFC 1918)**

| Rango de Direcciones | Bloque CIDR Más Grande | Descripción Clásica | Número de Direcciones |
|---|---|---|---|
| 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 | Una red de Clase A | 16,777,216 |
| 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 | 16 redes Clase B contiguas | 1,048,576 |
| 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 | 256 redes Clase C contiguas | 65,536 |

La identificación de si una dirección IP es pública o privada es un primer paso crítico en la fase de reconocimiento de un pentest. Si el objetivo asignado o descubierto cae dentro de uno de los rangos RFC 1918, indica inmediatamente que se está tratando con un host interno, lo que generalmente implica que se requiere acceso a la red interna (ya sea físico, a través de una VPN, o mediante la explotación de un sistema perimetral y posterior pivoting) para interactuar directamente con él. La comunicación desde redes privadas hacia Internet es posible gracias a Network Address Translation (NAT), que se discute en la Sección 5.[4]

Además de los rangos públicos y privados estándar, existen otros bloques de direcciones IPv4 reservados para usos especiales, cuyo reconocimiento es vital para un pentester:

- **Loopback (127.0.0.0/8):** Este bloque está reservado para la comunicación interna dentro del propio host. La dirección más comúnmente utilizada es 127.0.0.1, a menudo asociada con el nombre de host localhost. Se utiliza para probar servicios que se ejecutan localmente o para la comunicación entre procesos en la misma máquina.[20] *Relevancia para Pentesters:* El tráfico hacia o desde este rango indica actividad local en el host. Descubrir servicios escuchando en 127.0.0.1 puede revelar aplicaciones o interfaces de administración no expuestas a la red externa, pero potencialmente accesibles si se obtiene acceso local o mediante vulnerabilidades de redirección.
- **Link-Local (APIPA/Zeroconf) (169.254.0.0/16):** Automatic Private IP Addressing (APIPA) en Windows, o Zeroconf en otros sistemas, utiliza este rango. Las direcciones en este bloque se autoasignan cuando un dispositivo configurado para DHCP no puede

contactar a un servidor DHCP.[20] Estas direcciones solo son válidas en el segmento de red local (enlace) y no son enrutables.[20] *Relevancia para Pentesters:* Encontrar dispositivos con direcciones APIPA durante un escaneo interno sugiere problemas de configuración de red (fallo del servidor DHCP, problemas de conectividad del cliente). Estos hosts pueden ser más fáciles de atacar si están aislados o mal configurados. También puede ser un indicador útil en escenarios de respuesta a incidentes.

- **Carrier-Grade NAT (CGNAT) (100.64.0.0/10):** Definido en RFC 6598, este espacio de direcciones está reservado para que los proveedores de servicios de Internet (ISPs) lo utilicen *entre* su infraestructura y los equipos de los clientes (CPE).[35] Permite a los ISPs compartir un número limitado de direcciones IPv4 públicas entre muchos clientes, implementando NAT a gran escala.[29] Aunque técnicamente no es parte del RFC 1918, se trata como espacio privado dentro del contexto del ISP y no es globalmente enrutable desde la Internet pública.[22] *Relevancia para Pentesters:* Desde una perspectiva externa, complica la identificación y el seguimiento de usuarios individuales, ya que múltiples clientes comparten la misma IP pública vista desde Internet. Puede dificultar ciertos ataques que dependen de conexiones directas o correlación de IP. Para un pentester que opera *desde* una red detrás de CGNAT, puede haber limitaciones en el establecimiento de conexiones entrantes (como shells inversos) sin técnicas de traversal adicionales.
- **Documentación (TEST-NET) (192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24):** Estos bloques están reservados explícitamente para ser utilizados en documentación y ejemplos (RFC 5737).[20] Nunca deben asignarse a dispositivos reales ni aparecer en tablas de enrutamiento globales. *Relevancia para Pentesters:* Si se detecta tráfico hacia o desde estas redes durante un pentest, es una señal clara de una posible mala configuración, un entorno de prueba expuesto accidentalmente o incluso un intento de ofuscación.
- **Reservado (240.0.0.0/4):** Este rango corresponde a la antigua Clase E y está reservado para uso futuro o experimental.[1] No debe verse en redes operativas. *Relevancia para Pentesters:* Similar a las direcciones de documentación, su presencia indica anomalías o configuraciones inusuales.
- **"Esta Red" (0.0.0.0/8):** La dirección 0.0.0.0 se utiliza como dirección de origen por un host que aún no ha obtenido una dirección IP, típicamente durante el proceso de descubrimiento DHCP.[20] También puede usarse en tablas de enrutamiento para indicar una ruta predeterminada o en configuraciones de escucha de servicios para indicar "cualquier interfaz". *Relevancia para Pentesters:* Ver 0.0.0.0 como origen en el tráfico capturado indica procesos de arranque o adquisición de direcciones. En configuraciones de servicios, puede indicar que un servicio está escuchando en todas las interfaces disponibles.

**Tabla: Otros Rangos IPv4 de Uso Especial (No RFC 1918)**

| Rango | Nombre | Uso Clave / Relevancia para Pentesters | RFC(s) Principales |
|---|---|---|---|
| 127.0.0.0/8 | Loopback | Representa el host local (127.0.0.1). Indica servicios/comunicación local. | [20] |
| 169.254.0.0/16 | Link-Local (APIPA) | Autoasignada si falla DHCP. Indica problemas de configuración de red. Hosts potencialmente aislados/vulnerables. No enrutable. | [20] |
| 100.64.0.0/10 | Carrier-Grade NAT (CGNAT) | Usado por ISPs entre su red y clientes. Complica rastreo externo. No globalmente enrutable. | [20] |
| 192.0.2.0/24 | Documentación (TEST-NET-1) | Reservado para ejemplos. Su presencia en tráfico real es una anomalía/mala configuración. | [20] |
| 198.51.100.0/24 | Documentación (TEST-NET-2) | Reservado para ejemplos. Su presencia en tráfico real es una anomalía/mala configuración. | [20] |
| 203.0.113.0/24 | Documentación (TEST-NET-3) | Reservado para ejemplos. Su presencia en tráfico real es una anomalía/mala configuración. | [20] |
| 240.0.0.0/4 | Reservado (Antigua Clase E) | Reservado para uso futuro. No debería verse en redes operativas. | [1] |
| 0.0.0.0/8 | "Esta Red" | Usado como origen antes de tener IP | [20] |

| | | | |
|---|---|---|---|
| | | (DHCP Discover). Indica procesos de arranque o servicios escuchando en todas las interfaces (0.0.0.0). | |

El reconocimiento de estos rangos especiales proporciona un contexto crucial durante las pruebas. APIPA puede señalar debilidades en la configuración de DHCP, Loopback confirma servicios locales, CGNAT explica ciertos comportamientos de conectividad externa, y la aparición de rangos de Documentación o Reservados en tráfico real son fuertes indicadores de malas configuraciones o entornos de prueba expuestos. Un pentester no los ve como meros datos triviales, sino como pistas sobre la salud y configuración de la red.

## Función de la Máscara de Subred

La **máscara de subred** es un número de 32 bits indispensable que acompaña a cada dirección IPv4.[37] Su función primordial es definir la división entre la porción de **Network ID** y la porción de **Host ID** dentro de una dirección IP.[37] Estructuralmente, una máscara de subred consiste en una secuencia contigua de bits puestos a '1', seguida por una secuencia contigua de bits puestos a '0'.[38] Los bits '1' corresponden a la parte de la dirección IP que identifica la red (y la subred), mientras que los bits '0' corresponden a la parte que identifica al host específico dentro de esa red (o subred).[38]
El propósito fundamental de la máscara de subred es permitir que un dispositivo determine si una dirección IP de destino se encuentra en su **misma red local (o subred)** o en una **red remota**.[40] Para ello, el dispositivo realiza una operación lógica **AND bit a bit** entre su propia dirección IP y su máscara de subred. El resultado es el Network ID de su propia red.[38] Luego, realiza la misma operación AND entre la dirección IP de *destino* y su *propia* máscara de subred. Si los Network IDs resultantes coinciden, el destino está en la red local. Si no coinciden, el destino está en una red remota.

Esta determinación es crucial para las decisiones de enrutamiento [37]:

- Si el destino es **local**, el dispositivo buscará la dirección física (MAC) del host de destino utilizando el Protocolo de Resolución de Direcciones (ARP) y enviará el paquete directamente a través de la capa de enlace de datos (Layer 2).[40]
- Si el destino es **remoto**, el dispositivo enviará el paquete a la dirección IP de su **gateway por defecto** (router), que será el responsable de encaminar el paquete hacia la red remota (Layer 3 routing).[40]

Históricamente, las clases de direcciones tenían máscaras de subred por defecto (Clase A:

255.0.0.0, Clase B: 255.255.0.0, Clase C: 255.255.255.0).[13] Sin embargo, con la introducción del subnetting y CIDR (que se detallan en la siguiente sección), estas máscaras por defecto ya no son la norma, y se utilizan máscaras de longitud variable para crear subredes de tamaños personalizados.

- **Relevancia para Pentesters:** La máscara de subred define los límites lógicos de un segmento de red local desde la perspectiva de un dispositivo. Es un dato crítico que un pentester debe obtener o inferir durante el reconocimiento. Define el alcance de los escaneos locales (por ejemplo, un escaneo ARP con nmap -PR solo funcionará dentro de la subred local definida por la máscara). Permite interpretar correctamente el tráfico de red capturado (¿por qué este paquete va al gateway y este otro no?). Ayuda a identificar posibles límites de segmentación de red o configuraciones erróneas (máscaras inconsistentes en la misma red). Sin conocer la máscara de subred correcta, es imposible determinar con precisión el tamaño y los límites de la red local que se está evaluando.

La transición desde el rígido sistema de clases hacia la necesidad de rangos privados (RFC 1918) y, finalmente, a CIDR, ilustra una tensión central en las redes: la necesidad de conectividad universal frente a la limitación práctica del espacio de direcciones. Este contexto histórico explica por qué las redes modernas suelen estructurarse con IPs privadas internamente y dependen de NAT para la conectividad externa, un factor clave en la planificación de ataques por parte de un pentester.

# 2. Dominando Subnetting IPv4 y CIDR

La incapacidad del sistema de direccionamiento por clases para asignar eficientemente el espacio de direcciones IPv4 llevó al desarrollo de Classless Inter-Domain Routing (CIDR) y la práctica del subnetting. Estas técnicas son fundamentales para la gestión moderna de redes IPv4 y, por lo tanto, esenciales para que los pentesters comprendan la estructura y segmentación de las redes objetivo.

## Definición de CIDR (Classless Inter-Domain Routing) y Notación (/xx)

**Classless Inter-Domain Routing (CIDR)** se introdujo en 1993 (RFC 1519, posteriormente actualizado) para reemplazar el sistema de direccionamiento por clases.[3] Sus objetivos principales eran ralentizar el agotamiento de las direcciones IPv4 y mejorar la eficiencia del enrutamiento en Internet, reduciendo el tamaño de las tablas de enrutamiento globales.[45]
La innovación clave de CIDR es la eliminación de las clases fijas (A, B, C) y la introducción de **máscaras de subred de longitud variable (Variable Length Subnet Masks - VLSM)**.[3] Esto significa que la división entre la porción de red y la porción de host de una dirección IP ya no está predeterminada por el primer octeto, sino que puede definirse de manera flexible utilizando una máscara de subred de cualquier longitud (dentro de los 32 bits).

Para representar esta flexibilidad de forma compacta, CIDR introdujo una nueva notación: la **notación CIDR** o **notación de prefijo**. Consiste en la dirección IP seguida de una barra diagonal (/) y un número decimal (xx) que indica la **longitud del prefijo de red**, es decir, el número de bits contiguos iniciales que constituyen la porción de red de la dirección.[45] Por ejemplo, 192.168.1.0/24:

- 192.168.1.0 es la dirección de red.
- /24 indica que los primeros 24 bits (los tres primeros octetos en este caso) representan el prefijo de red.
- Los 32−24=8 bits restantes son para identificar hosts dentro de esa red.

La relación entre la longitud del prefijo y el tamaño de la subred es inversa:

- Un **valor /xx más alto** (ej. /27, /30) significa un prefijo de red más largo, menos bits para hosts y, por lo tanto, una **subred más pequeña** (menos hosts posibles).
- Un **valor /xx más bajo** (ej. /16, /20) significa un prefijo de red más corto, más bits para hosts y, por lo tanto, una **subred más grande** (más hosts posibles).[45]
- **Relevancia para Pentesters:** La notación CIDR es el estándar de facto para definir rangos de red en el mundo real. Se utiliza en documentos de alcance de pentesting, configuraciones de firewall, listas de control de acceso (ACLs), y como entrada para herramientas de escaneo como Nmap (ej. nmap 192.168.1.0/24). Un pentester debe ser completamente fluido en la lectura, interpretación y cálculo de rangos a partir de la notación CIDR para definir con precisión los objetivos, comprender la segmentación de la red y evitar salirse del alcance autorizado.

## El Proceso de Subnetting: Tomar Bits Prestados, Calcular Subredes y Hosts

El **subnetting** (o subredes) es el proceso de tomar un bloque de direcciones IP (definido por un prefijo CIDR) y dividirlo lógicamente en múltiples segmentos de red más pequeños, llamados subredes.[37] Esto se hace para mejorar la organización de la red, la eficiencia, la seguridad y la gestión del tráfico.[37]
El mecanismo central del subnetting consiste en **"tomar prestados" bits** de la porción de host original de la dirección IP y reasignarlos a la porción de red.[44] Cada bit que se toma prestado de la porción de host se convierte en un bit de subred, extendiendo efectivamente la longitud del prefijo de red original.

Este proceso tiene dos consecuencias directas que se pueden calcular mediante fórmulas:

1. Número de Subredes Creadas: Cada bit prestado duplica el número de subredes que se pueden crear a partir del bloque original. La fórmula es:

Número de Subredes=2s
donde 's' es el número de bits prestados.[44]

2. Número de Hosts por Subred: Al tomar prestados bits para crear subredes, quedan menos bits disponibles para identificar hosts dentro de cada nueva subred. La fórmula para calcular el número de direcciones IP utilizables para hosts en cada subred es:

   Número de Hosts Utilizables por Subred=$2^h-2$

   donde 'h' es el número de bits que quedan en la porción de host después de tomar prestados los bits de subred.[21]

Es crucial entender por qué se restan 2 direcciones:

- La **primera dirección** de la subred (donde todos los bits de host restantes son '0') se reserva como la **Dirección de Red** (o Network ID) y no puede asignarse a un host. Identifica la subred en sí misma.
- La **última dirección** de la subred (donde todos los bits de host restantes son '1') se reserva como la **Dirección de Broadcast** y no puede asignarse a un host. Se utiliza para enviar paquetes a todos los hosts dentro de esa subred específica.[13]

**Ejemplo:** Consideremos el bloque 192.168.1.0/24. Este bloque tiene 8 bits de host (h=8). Si decidimos **tomar prestados 2 bits** (s=2) para crear subredes:

- La nueva longitud del prefijo será 24+2=26 (/26).
- El número de subredes creadas será 2s=2x2=4 subredes.
- El número de bits de host restantes será h=8−2=6 bits.
- El número de hosts utilizables por cada subred será $2^h-2=2^6-2=64-2=62$ hosts.[44]
- **Relevancia para Pentesters:** Comprender el mecanismo de "préstamo de bits" permite a un pentester deducir la estructura potencial de una red a partir de información limitada. Por ejemplo, si se descubre un host con una máscara /27 dentro de lo que parece ser un rango 192.168.x.0, el pentester sabe que se tomaron prestados 3 bits (27−24=3), lo que implica que podrían existir hasta $2^3=8$ subredes de ese tamaño en el bloque /24 original, y que cada una tiene $2^{(8-3)}-2=30$ hosts utilizables. Esto guía la fase de descubrimiento y enumeración de redes adyacentes.

## Ejemplos Prácticos de Cálculo: Direcciones de Red, Rango de Hosts, Broadcast

La capacidad de calcular rápidamente la dirección de red, la dirección de broadcast y el rango de hosts utilizables para cualquier prefijo CIDR es una habilidad fundamental y no negociable para un pentester. Estos cálculos definen los límites exactos de una subred.

**Metodología General:**

1. **Identificar la longitud del prefijo (/xx)**: Esto determina cuántos bits son para la red y cuántos para el host (h=32−xx).
2. **Calcular el tamaño del bloque (incremento)**: El tamaño de cada subred es $2^h$. Este valor es el "número mágico" o incremento entre direcciones de red consecutivas.
3. **Encontrar la Dirección de Red**:
    - **Método 1 (AND binario):** Convierte la dirección IP dada y la máscara de subred (derivada del /xx) a binario. Realiza una operación AND bit a bit. El resultado es la dirección de red en binario, que luego se convierte a decimal.[38]
    - **Método 2 (Número Mágico):** Encuentra el múltiplo del tamaño del bloque (calculado en el paso 2) que sea menor o igual al valor del octeto donde ocurre la división red/host. Coloca ceros en todos los bits de host. Por ejemplo, para /27, el tamaño del bloque es 32. Si la IP es 192.168.1.100, el último octeto es 100. Los múltiplos de 32 son 0, 32, 64, 96, 128... El múltiplo menor o igual a 100 es 96. La dirección de red es 192.168.1.96.[69]
4. **Encontrar la Dirección de Broadcast**:
    - **Método 1 (Bits de host a 1):** Toma la dirección de red en binario y cambia todos los bits de la porción de host (los h bits finales) a '1'. Convierte el resultado a decimal.[50]
    - **Método 2 (Siguiente Red - 1):** Calcula la dirección de red de la *siguiente* subred (Dirección de Red Actual + Tamaño del Bloque). La dirección de broadcast es la dirección inmediatamente anterior a la siguiente dirección de red.[59] Para 192.168.1.96/27, la siguiente red es 192.168.1.128. La broadcast es 192.168.1.127.
5. **Determinar el Rango de Hosts Utilizables**:
    - El primer host utilizable es la Dirección de Red + 1.
    - El último host utilizable es la Dirección de Broadcast - 1.[50]

**Ejemplo 1: Prefijo /27**

Dado: IP 192.168.1.100/27

1. **Longitud Prefijo:** /27. Bits de host $h=32-27=5$.[44]
2. **Tamaño Bloque:** $2^h=2^5=32$.[49]
3. **Dirección de Red:** Múltiplo de 32 <= 100 es 96. Dirección de Red = 192.168.1.96.[38]
4. **Dirección de Broadcast:** Siguiente red = 192.168.1.(96+32) = 192.168.1.128. Broadcast = 192.168.1.127.[50]
5. **Rango de Hosts Utilizables:** 192.168.1.97 a 192.168.1.126.[50]
6. **Número de Hosts Utilizables:** $25-2=32-2=30$.[44]

**Ejemplo 2: Prefijo /29**

Dado: IP 10.10.10.29/29

1. **Longitud Prefijo:** /29. Bits de host h=32−29=3.[44]
2. **Tamaño Bloque:** $2^h=2^3=8$.[76]
3. **Dirección de Red:** Múltiplo de 8 <= 29 es 24. Dirección de Red = 10.10.10.24.[38]
4. **Dirección de Broadcast:** Siguiente red = 10.10.10.(24+8) = 10.10.10.32. Broadcast = 10.10.10.31.[50]
5. **Rango de Hosts Utilizables:** 10.10.10.25 a 10.10.10.30.[50]
6. **Número de Hosts Utilizables:** $2^3-2=8-2=6$.[44]

Aunque existen numerosas calculadoras de subredes en línea [38], es imperativo que un pentester domine el proceso manual para comprender verdaderamente la estructura de la red y poder realizar cálculos rápidos en situaciones donde las herramientas no estén disponibles o no sean prácticas.

- **Relevancia para Pentesters:** Esta es una habilidad operativa diaria. Al recibir un alcance (ej. "probar la red 10.50.100.0/26"), el pentester debe calcular inmediatamente:
    - Dirección de Red: 10.50.100.0
    - Dirección de Broadcast: 10.50.100.63
    - Rango Utilizable: 10.50.100.1 a 10.50.100.62 Esto define exactamente qué IPs escanear. Si durante un escaneo interno en 192.168.5.77/28, se encuentra un servicio interesante en 192.168.5.90, el cálculo rápido (Bloque /28 = 16 IPs; Redes: 0, 16, 32, 48, 64, **80**, 96...) revela que 192.168.5.90 está en la subred 192.168.5.80/28 (rango 81-94), que es *diferente* de la subred inicial (192.168.5.64/28, rango 65-78). Esto informa que se necesita enrutamiento (o pivoting si hay firewalls) para alcanzar ese objetivo.

## Impacto del Subnetting en el Pentesting: Segmentación, Escaneo y VLSM

El subnetting no es solo un ejercicio de asignación de direcciones; tiene implicaciones directas y significativas en cómo se planifica y ejecuta una prueba de penetración.

- **Segmentación de Red:** El propósito principal del subnetting es dividir una red grande en segmentos lógicos más pequeños y manejables.[37] Estos segmentos a menudo se alinean con divisiones funcionales u organizativas (departamentos de ventas, ingeniería, recursos humanos), tipos de dispositivos (servidores, estaciones de trabajo, VoIP, IoT) o zonas de seguridad (red interna, DMZ, red de gestión).[38] Desde la perspectiva de un pentester, esta segmentación crea barreras lógicas. El acceso a una subred no garantiza automáticamente el acceso a otras. Los routers actúan como guardianes entre subredes, y a menudo se colocan firewalls en estos puntos de interconexión para filtrar el tráfico.[77] Una segmentación eficaz limita significativamente la superficie de

ataque interna visible desde un único punto comprometido y puede dificultar el movimiento lateral.[77]

- **Estrategias de Escaneo:** La segmentación obliga a los pentesters a adoptar estrategias de escaneo más matizadas que simplemente escanear un gran bloque de direcciones.[77] La fase de reconocimiento debe centrarse en identificar los diferentes rangos de subredes en uso.[79] Esto puede lograrse analizando configuraciones de routers (si se comprometen), examinando tráfico de red capturado, consultando registros DNS, realizando OSINT o incluso infiriendo a partir de las máscaras de subred observadas en los hosts descubiertos. Una vez identificada una subred (ej. 10.1.50.64/27), las herramientas de escaneo como Nmap deben dirigirse específicamente a ese rango CIDR (nmap 10.1.50.64/27).[80] El pentester debe planificar escaneos para cada subred descubierta dentro del alcance, teniendo en cuenta que las reglas de firewall entre subredes pueden variar, requiriendo potencialmente técnicas de pivoting para escanear subredes no directamente accesibles.[77]
- **VLSM (Variable Length Subnet Mask):** Como ya se mencionó, CIDR permite VLSM, donde se utilizan máscaras de subred de *diferentes* longitudes dentro del mismo bloque de red original.[16] Esto contrasta con el antiguo método FLSM (Fixed Length Subnet Mask), donde todas las subredes creadas a partir de un bloque tenían el mismo tamaño, lo que a menudo resultaba ineficiente.[49] VLSM permite a los administradores adaptar el tamaño de cada subred a sus necesidades específicas de hosts (por ejemplo, una subred grande para usuarios, una mediana para servidores y varias muy pequeñas para enlaces punto a punto), optimizando así el uso del espacio de direcciones.[48]
    - *Relevancia de VLSM para Pentesters:* Encontrar máscaras de subred de diferentes longitudes (ej. /25, /27, /30) dentro de lo que parece ser un bloque original coherente (ej. un antiguo Clase B) durante el reconocimiento es un fuerte indicador de un diseño de red VLSM. Esto sugiere una planificación de red más compleja que FLSM. Si bien es más eficiente, esta complejidad también puede introducir más oportunidades para errores de configuración (como subredes superpuestas [99] o ACLs mal definidas entre subredes de diferentes tamaños). El pentester debe ser meticuloso al calcular los límites de cada subred de tamaño diferente descubierta para asegurar una cobertura completa dentro del alcance y para identificar posibles relaciones o errores entre ellas. La no uniformidad requiere una validación de alcance más cuidadosa que en un entorno FLSM simple.

En resumen, CIDR y el subnetting resultante no son meros mecanismos de asignación; son la base de la estrategia de segmentación de la red. Esto impacta directamente en la metodología del pentester, exigiendo un reconocimiento cuidadoso para descubrir los segmentos, cálculos precisos para definir los rangos de escaneo y, a menudo, técnicas de pivoting para navegar las barreras creadas por la segmentación. La presencia de VLSM añade una capa de complejidad que requiere aún más atención al detalle durante el reconocimiento

y la validación del alcance.

# 3. Fundamentos de Direccionamiento IPv6 para Pentesters

Con el agotamiento del espacio de direcciones IPv4, IPv6 se ha convertido en el sucesor designado y su adopción está en constante crecimiento. Para un pentester moderno, la competencia en IPv6 es indispensable. Aunque comparte algunos principios con IPv4, introduce cambios significativos en la estructura de direcciones, tipos y mecanismos asociados.

## Estructura IPv6: 128 Bits, Notación Hexadecimal y Reglas de Abreviación

La diferencia más fundamental entre IPv4 e IPv6 es el tamaño de la dirección. Una dirección IPv6 consta de **128 bits**, en comparación con los 32 bits de IPv4.[6] Este aumento exponencial (de $2^{32}$ a $2^{128}$ direcciones) proporciona un espacio de direcciones prácticamente ilimitado para el futuro previsible, eliminando la necesidad de mecanismos como NAT para la conservación de direcciones en la mayoría de los casos.[6]
Dada su longitud, las direcciones IPv6 no se representan en notación decimal punteada. En su lugar, se utiliza una **notación hexadecimal**. La dirección de 128 bits se divide en ocho grupos de 16 bits cada uno. Cada grupo de 16 bits se representa mediante cuatro dígitos hexadecimales (0-9, a-f). Estos grupos, a veces llamados hextetos, se separan por dos puntos (:).[6]

Un ejemplo de una dirección IPv6 completa sería:
2001:0db8:85a3:0000:0000:8a2e:0370:7334 [101]

Para simplificar esta notación larga y a menudo repetitiva, RFC 4291 [104] y RFC 5952 [104] (que recomienda usar minúsculas para los dígitos hexadecimales a-f) definen dos reglas principales de abreviación:

1. **Omisión de Ceros Iniciales:** Dentro de cualquier grupo de cuatro dígitos hexadecimales (hexteto), los ceros iniciales pueden omitirse. Sin embargo, si un grupo consta de cuatro ceros, debe dejarse al menos un cero.[101]
    - Ejemplo: 0db8 se convierte en db8.
    - Ejemplo: 0000 se convierte en 0.
    - Ejemplo: 0370 se convierte en 370.
2. **Compresión de Ceros Consecutivos:** Una secuencia *única* (la más larga, o la primera si hay varias de igual longitud) de grupos consecutivos compuestos enteramente de ceros puede reemplazarse por dos puntos dobles (::).[101] Esta regla sólo puede aplicarse

**una vez** por dirección para evitar ambigüedades. No se usa :: para reemplazar un solo grupo de ceros.
    - Ejemplo: 2001:0db8:0000:0000:0000:ff00:0042:8329 se convierte en 2001:db8::ff00:42:8329.
    - Ejemplo: fe80:0000:0000:0000:a299:9bff:fe18:50d1 se convierte en fe80::a299:9bff:fe18:50d1.
    - Ejemplo: 2001:db8:0:0:1:0:0:1 se convierte en 2001:db8::1:0:0:1 (se comprime la primera secuencia más larga de ceros).

Aplicando ambas reglas:

- La dirección de loopback 0000:0000:0000:0000:0000:0000:0000:0001 se abrevia como ::1.[101]
- La dirección no especificada 0000:0000:0000:0000:0000:0000:0000:0000 se abrevia como ::.[101]

Al igual que en IPv4, los rangos de red IPv6 se especifican utilizando la notación CIDR, indicando la longitud del prefijo en bits después de una barra diagonal. Por ejemplo, 2001:db8:cafe::/48 representa una red donde los primeros 48 bits son fijos.[101]

- **Relevancia para Pentesters:** La maestría en la lectura, escritura, expansión y compresión de direcciones IPv6 es absolutamente esencial. Un error al interpretar una dirección abreviada, especialmente la posición y longitud de la sección omitida por ::, conducirá a la identificación incorrecta de objetivos, rangos de escaneo erróneos y fallos en el uso de herramientas. Todas las herramientas de pentesting (Nmap, Metasploit, Wireshark, etc.) y los sistemas operativos modernos utilizan y muestran direcciones IPv6 en su forma (potencialmente) abreviada.

## Tipos Principales de Direcciones Unicast: GUA, ULA, Link-Local

Las direcciones unicast identifican una única interfaz de red. IPv6 define varios tipos de direcciones unicast, cada una con un alcance y propósito específicos.[101] Las tres más importantes para un pentester son:

1. **Global Unicast Addresses (GUA):**
    - **Propósito:** Equivalentes a las direcciones IPv4 públicas. Son globalmente únicas y enrutables en la Internet IPv6.[101] Se utilizan para la comunicación a través de Internet.
    - **Prefijo:** Actualmente, IANA asigna GUAs del bloque 2000::/3 (direcciones que comienzan con los bits 001).[101] Las asignaciones típicas a organizaciones o sitios finales suelen ser prefijos /48 o /56, dejando 16 o 8 bits respectivamente para la creación de subredes internas.[101]
    - **Alcance (Scope):** Global.[101]

- **Estructura Típica:** Se divide generalmente en: Prefijo de Enrutamiento Global (asignado por el RIR/ISP, típicamente 48 bits) + ID de Subred (definido por la organización, típicamente 16 bits) + ID de Interfaz (identifica al host en la subred, 64 bits).[6]
- *Relevancia para Pentesters:* Las GUAs son los objetivos principales en pruebas de penetración externas de IPv6. Identificar los rangos GUA asignados a una organización es fundamental para definir el alcance externo del pentest.

2. **Unique Local Addresses (ULA):**
   - **Propósito:** Diseñadas para comunicaciones locales *dentro* de un sitio o entre un número limitado de sitios cooperantes. Son análogas a las direcciones privadas RFC 1918 de IPv4.[32] **No están destinadas a ser enrutadas en la Internet global**.[116] Los routers de borde deben filtrar estas direcciones.
   - **Prefijo:** El bloque reservado es fc00::/7.[26] Este se subdivide:
     - fd00::/8: Se utiliza para direcciones asignadas localmente. La idea es generar un Identificador Global (Global ID) pseudoaleatorio de 40 bits, que se combina con el prefijo fd para crear un prefijo /48 único para el sitio (con alta probabilidad).[101] Esto minimiza la posibilidad de colisiones si dos organizaciones que usan ULA se fusionan o interconectan.[116]
     - fc00::/8: Está reservado para una posible asignación futura gestionada centralmente, pero actualmente no está definido su uso.[101]
   - **Alcance (Scope):** Tienen alcance *global* según RFC 4007 [101], pero su dominio de enrutamiento es *limitado* (efectivamente, sitio-local o entre sitios cooperantes).[101] No deben ser anunciadas ni filtradas por los routers de borde de Internet.[116]
   - **Estructura:** fd (8 bits) + Global ID (40 bits) + ID de Subred (16 bits) + ID de Interfaz (64 bits).[29]
   - *Relevancia para Pentesters:* Detectar direcciones ULA (fácilmente identificables por empezar con fd) indica la presencia de una red IPv6 interna, similar a encontrar rangos RFC 1918 en IPv4. El pentesting de estos rangos requiere acceso a la red interna o técnicas de pivoting. La probabilidad de unicidad del Global ID reduce el riesgo de solapamiento si se comprometen múltiples redes, pero no lo elimina por completo.

3. **Link-Local Addresses:**
   - **Propósito:** Se utilizan **exclusivamente** para la comunicación entre nodos dentro del **mismo segmento de red local (enlace)**. Son fundamentales para el funcionamiento del Neighbor Discovery Protocol (NDP), que realiza funciones como la resolución de direcciones (similar a ARP en IPv4) y el descubrimiento de routers.[101] **Nunca son enrutadas** fuera del enlace local por los routers.[102]
   - **Prefijo:** Utilizan el prefijo reservado fe80::/10.[101] Aunque el prefijo es /10, en la práctica, los siguientes 54 bits suelen ser cero, resultando en un prefijo efectivo de fe80::/64 para cada enlace.[101]
   - **Alcance (Scope):** Link-Local.[101]

    - **Generación:** Cada interfaz habilitada para IPv6 **debe** tener al menos una dirección link-local.[104] Esta dirección se configura automáticamente al iniciar la interfaz (autoconfiguración), generalmente combinando el prefijo fe80::/64 con un ID de Interfaz generado mediante EUI-64 o extensiones de privacidad.[101]
    - *Relevancia para Pentesters:* Las direcciones link-local son cruciales para el reconocimiento y los ataques en la red local. Un pentester conectado al mismo segmento puede:
        - Descubrir otros nodos en el enlace enviando paquetes a direcciones multicast link-local (ej. ff02::1).
        - Identificar routers locales (gateways) escuchando sus Router Advertisements (RAs) que se originan desde sus direcciones link-local.
        - Realizar ataques de Neighbor Discovery (NDP spoofing, Rogue RA) que operan a nivel link-local (ver Sección 7).
        - Interactuar directamente con servicios que puedan estar escuchando solo en direcciones link-local.

La introducción de ámbitos específicos (Link-Local, Unique Local, Global) en IPv6 crea fronteras de comunicación y superficies de ataque distintas que los pentesters deben reconocer y abordar de manera diferente. A diferencia de IPv4, donde la distinción principal es pública vs. privada, IPv6 introduce el ámbito Link-Local como un espacio operativo crítico pero no enrutable, fundamental para los protocolos de descubrimiento y, por lo tanto, para los ataques locales. Las ULAs actúan como el espacio privado, mientras que las GUAs son el objetivo para el reconocimiento y ataque externo. Identificar el ámbito de una dirección descubierta es clave para determinar su alcanzabilidad y los vectores de ataque aplicables.

## Otros Tipos Importantes: Loopback, No Especificada, Multicast, Anycast

Además de las direcciones unicast principales, existen otros tipos de direcciones IPv6 con funciones especiales:

- **Loopback (::1/128):** Al igual que 127.0.0.1 en IPv4, la dirección ::1 representa al propio host local.[101] Se utiliza para pruebas de la pila TCP/IP local y para que las aplicaciones en el host se comuniquen entre sí. Tiene alcance de nodo (node-local scope) pero se considera link-local en la práctica.[130] *Relevancia:* Útil para identificar servicios que escuchan localmente en un host comprometido.
- **No Especificada (::/128):** La dirección compuesta completamente por ceros (::) se utiliza como dirección de origen cuando un host aún no conoce su propia dirección IP.[101] Esto ocurre típicamente durante el proceso de Detección de Direcciones Duplicadas (DAD) o al iniciar una solicitud DHCPv6. Nunca se asigna a una interfaz ni se utiliza como dirección de destino.[104] *Relevancia:* Ver esta dirección como origen en el tráfico capturado indica procesos de autoconfiguración o adquisición de direcciones en curso.

- **Multicast (ff00::/8):** Las direcciones multicast se utilizan para enviar un paquete a un *grupo* de interfaces, que pueden pertenecer a diferentes nodos (comunicación uno-a-muchos).[101] IPv6 no utiliza direcciones de broadcast; la funcionalidad de broadcast se implementa mediante direcciones multicast específicas.[104] Las direcciones multicast tienen una estructura que incluye flags y un campo de alcance (scope) que define los límites de enrutamiento del grupo (ej., link-local, site-local, organization-local, global).[108]
    - **Direcciones Multicast Bien Conocidas:** Definidas para grupos estándar. Ejemplos clave para pentesters:
        - ff02::1: Grupo All-Nodes (alcance link-local). Todos los nodos IPv6 en el enlace local escuchan en esta dirección. Usado para anuncios generales en el enlace.[108]
        - ff02::2: Grupo All-Routers (alcance link-local). Todos los routers IPv6 en el enlace local escuchan aquí. Usado por hosts para enviar Router Solicitations (RS).[108]
    - **Solicited-Node Multicast Address (ff02::1:ffxx:xxxx/104):** Un tipo especial de dirección multicast con alcance link-local, utilizada por NDP para la resolución de direcciones (reemplaza a ARP).[108] Se genera automáticamente para cada dirección unicast y anycast configurada en una interfaz. Se forma tomando los últimos 24 bits de la dirección unicast/anycast y añadiéndolos al prefijo ff02::1:ff00:0/104. Un nodo escucha en las direcciones solicited-node correspondientes a sus direcciones configuradas. Cuando un nodo necesita resolver la dirección MAC de un vecino, envía una Neighbor Solicitation (NS) a la dirección solicited-node del vecino. Solo el nodo objetivo (y potencialmente otros con los mismos últimos 24 bits de dirección, aunque es raro) procesará eficientemente esta solicitud. *Relevancia:* Fundamental para entender NDP y sus vulnerabilidades (Sección 7). Permite ataques de DoS o MitM si se pueden inyectar respuestas falsas a estas direcciones. El tráfico multicast puede ser utilizado en ataques de amplificación si no se filtra adecuadamente.
- **Anycast:** Una dirección anycast identifica a un *conjunto* de interfaces (generalmente en nodos diferentes), pero un paquete enviado a una dirección anycast se entrega a *una sola* de esas interfaces: la más "cercana" según la métrica del protocolo de enrutamiento (comunicación uno-a-más-cercano).[101] Las direcciones anycast se toman del espacio de direcciones unicast y no son sintácticamente distinguibles de ellas; su naturaleza anycast se configura en los routers.[101] Se utilizan para redundancia y descubrimiento de servicios (ej., encontrar el servidor DNS o 6to4 relay más cercano). *Relevancia:* Puede complicar el pentesting de servicios, ya que el pentester podría estar interactuando con diferentes instancias del servicio en diferentes momentos sin darse cuenta. Identificar si una dirección unicast es en realidad anycast requiere un análisis más profundo del enrutamiento o del comportamiento del servicio.

**Tabla: Resumen de Tipos de Direcciones IPv6**

| Tipo | Prefijo/Ejemplo Común | Alcance (Scope) Típico | Propósito Principal | Relevancia para Pentesters |
|---|---|---|---|---|
| **Unicast** | | | Identifica una única interfaz | |
| Global (GUA) | 2001:db8::/32 (ej.) | Global | Comunicación en Internet pública | Objetivo primario para pentesting externo. |
| Unique Local (ULA) | fd00::/8 | Global (Enrut. Limitado) | Comunicación interna/privada (similar a RFC 1918) | Indica red interna; requiere acceso local/pivoting. |
| Link-Local | fe80::/10 | Link-Local | Comunicación en el enlace local; esencial para NDP | Crucial para reconocimiento local, ataques NDP. |
| Loopback | ::1/128 | Node-Local | Pruebas locales, comunicación inter-proceso | Identifica servicios locales en host comprometido. |
| Unspecified | ::/128 | Node-Local | Usado como origen antes de tener IP (DAD, DHCPv6) | Indica procesos de adquisición de dirección. |
| **Multicast** | ff00::/8 | Variable | Comunicación uno-a-muchos (reemplaza broadcast) | |
| All-Nodes (Link) | ff02::1 | Link-Local | Alcanza todos los nodos en el enlace | Útil para descubrimiento local; vector potencial DoS. |
| All-Routers (Link) | ff02::2 | Link-Local | Alcanza todos los routers en el enlace | Usado para Router Solicitation (RS). |
| Solicited-Node | ff02::1:ffxx:xxxx | Link-Local | Resolución de direcciones (NDP) | Fundamental para ataques NDP (cache poisoning). |
| **Anycast** | (Tomado de Unicast) | Variable | Comunicación uno-a-más-cercano (redundancia/servicio) | Puede complicar la identificación del objetivo real; requiere análisis de enrutamiento. |

*Fuentes:* [101]

Esta tabla sirve como referencia rápida para que los pentesters identifiquen el tipo, alcance y propósito probable de una dirección IPv6 encontrada durante el reconocimiento, lo cual es crítico para determinar la alcanzabilidad y las técnicas de ataque aplicables.

## Identificador de Interfaz (64 bits): EUI-64 y Extensiones de Privacidad

Una característica distintiva de la arquitectura de direccionamiento IPv6 más común es la división fija de la dirección de 128 bits en dos mitades: los primeros 64 bits para el **prefijo de red** (que incluye el prefijo de enrutamiento global y el ID de subred) y los últimos 64 bits para el **Identificador de Interfaz (IID)**.[6] El IID identifica de forma única una interfaz dentro de una subred específica (definida por el prefijo de 64 bits). Existen varios métodos para generar este IID:

1. **EUI-64 Modificado (Extended Unique Identifier):** Este método, definido originalmente como el estándar para interfaces con direcciones de capa de enlace (como Ethernet MAC), genera un IID de 64 bits a partir de la dirección MAC de 48 bits de la interfaz.[105] El proceso es el siguiente:
    - Se toma la dirección MAC de 48 bits (ej. 39:A7:94:07:CB:D0).
    - Se divide en dos mitades de 24 bits (39:A7:94 y 07:CB:D0).
    - Se insertan los 16 bits hexadecimales FFFE en el medio (39:A7:94:FF:FE:07:CB:D0).
    - Se invierte el séptimo bit del primer octeto (el bit U/L - Universal/Local). Si es 0 (universalmente administrado, como la mayoría de los MACs), se cambia a 1. Si es 1 (localmente administrado), se cambia a 0. En el ejemplo, 39 (binario 00111001) se convierte en 3B (binario 00111011).
    - El IID resultante es 3BA7:94FF:FE07:CBD0.[132]
    - **Ventajas:** Genera automáticamente un IID que es (con alta probabilidad) globalmente único, simplificando la configuración inicial.
    - **Desventajas:** Expone directamente la dirección MAC del fabricante del hardware en la dirección IP. Esto crea importantes **preocupaciones de privacidad**, ya que permite rastrear un dispositivo específico a medida que se mueve entre diferentes redes IPv6 (el IID permanece constante aunque cambie el prefijo de red). También puede revelar el fabricante del hardware, lo que podría ayudar a un atacante a seleccionar exploits.[132]
2. **Extensiones de Privacidad (RFC 4941 / RFC 8981):** Para mitigar las preocupaciones de privacidad asociadas con EUI-64, se desarrollaron las extensiones de privacidad.[133]
    - **Propósito:** Generar IIDs temporales y aleatorios que cambian periódicamente, dificultando el rastreo de un host a través de diferentes redes o a lo largo del

tiempo.[136]

- **Mecanismo:** Cuando están habilitadas, un sistema operativo genera una dirección "pública" estable (que puede ser EUI-64 u otro método como RFC 7217) y una o más direcciones "temporales" con IIDs aleatorios. Las direcciones temporales se utilizan preferentemente para iniciar conexiones salientes.[140] Estas direcciones temporales tienen una vida útil preferida y una vida útil válida; una vez que la preferida expira, se genera una nueva dirección temporal, y la antigua se deprecia (solo se usa para conexiones existentes) hasta que expira su vida útil válida.[140] El intervalo de regeneración suele ser de un día por defecto en muchos sistemas operativos.[137]
- **Ventajas:** Mejora significativamente la privacidad del usuario al dificultar la correlación de actividades y el rastreo basado en direcciones IP.[137]
- **Desventajas:** Las direcciones cambiantes pueden complicar la resolución de problemas de red, el registro (logging) y la auditoría. Algunas aplicaciones que esperan direcciones IP estables pueden tener problemas. Aunque raro, la generación aleatoria puede teóricamente llevar a colisiones de DAD con mayor frecuencia que EUI-64.[137] RFC 8981 actualizó RFC 4941 para abordar algunas debilidades algorítmicas y permitir el uso exclusivo de direcciones temporales.[148]
- **Estado Actual:** La mayoría de los sistemas operativos modernos (Windows, macOS, Linux, iOS, Android) habilitan las extensiones de privacidad por defecto.[137]

3. **Otros Métodos:**
   - **Identificadores Opacos Estables (RFC 7217):** Genera un IID estable *por prefijo de red*, utilizando un hash que incluye el prefijo, un secreto local y otros parámetros. El IID cambia al cambiar de red, pero permanece estable dentro de la misma red, ofreciendo un compromiso entre la estabilidad de EUI-64 y la privacidad entre redes de las extensiones de privacidad.[139]
   - **Direcciones Generadas Criptográficamente (CGA - RFC 3972):** Utilizadas principalmente por SEND (Secure Neighbor Discovery), generan el IID a partir de un hash de la clave pública del nodo, vinculando criptográficamente la dirección a la clave.[144]
   - **Asignación Manual o DHCPv6 Stateful:** Aunque SLAAC es común, los IIDs también pueden asignarse manualmente o mediante un servidor DHCPv6 en modo stateful.

- **Relevancia para Pentesters:** El método de generación del IID tiene un impacto directo en el reconocimiento y el rastreo de hosts.
  - Si se usa **EUI-64**, el pentester puede extraer la dirección MAC (y por ende, el fabricante del hardware) directamente de la dirección IPv6. Esto proporciona información valiosa sobre el host y permite rastrearlo si se mueve entre redes (siempre que el prefijo cambie pero la interfaz sea la misma).
  - Si se usan **Extensiones de Privacidad**, el rastreo a largo plazo y la correlación de actividades se vuelven mucho más difíciles. El pentester no puede confiar en que

la dirección IP de un host permanezca constante. Las técnicas de reconocimiento deben adaptarse, enfocándose más en el escaneo activo periódico, el análisis de tráfico NDP en el enlace local o la identificación de servicios en lugar de hosts individuales basados en IPs estables. La aleatoriedad también hace que el escaneo de fuerza bruta de IIDs dentro de un /64 sea aún menos práctico.
    - Comprender qué método es el predeterminado para diferentes sistemas operativos (la mayoría ahora usa extensiones de privacidad por defecto [137]) ayuda a formular hipótesis sobre la red objetivo y a seleccionar las herramientas y técnicas de enumeración adecuadas.

La inmensidad del espacio de direcciones IPv6 transforma radicalmente las estrategias de escaneo y reconocimiento en comparación con IPv4. El escaneo exhaustivo de subredes es impracticable, lo que obliga a los pentesters a depender de técnicas de descubrimiento más dirigidas, como el análisis del protocolo Neighbor Discovery (NDP), la enumeración a través de DNS, la inteligencia de fuentes abiertas (OSINT) y la explotación de patrones predecibles (o aleatorios, en el caso de las extensiones de privacidad) en la asignación de direcciones.

# 4. Asignación y Configuración de Direcciones IP: Perspectivas del Pentester

La forma en que se asignan y configuran las direcciones IP en una red tiene implicaciones significativas tanto para la administración de la red como para la seguridad. Los pentesters deben comprender estos métodos para identificar posibles debilidades, realizar reconocimientos efectivos y ejecutar ciertos tipos de ataques.

## Comparación de Métodos de Asignación: Estática vs. Dinámica (DHCP, DHCPv6, SLAAC)

Existen dos enfoques principales para asignar direcciones IP a los dispositivos de red: estático y dinámico.

- **Asignación Estática:**
    - **Descripción:** La configuración IP (dirección IP, máscara de subred, gateway por defecto, servidores DNS) se introduce manualmente en cada dispositivo de red.[152] La dirección asignada no cambia a menos que un administrador la modifique manualmente.[152]
    - **Ventajas:**
        - **Previsibilidad:** Las direcciones son fijas y conocidas, lo que facilita el acceso a servicios alojados en esos dispositivos (como servidores web, de archivos o impresoras) y la configuración de reglas de firewall o listas de control de acceso (ACLs) basadas en IP.[152]

        - **Control:** Proporciona un control granular sobre la asignación de direcciones.
    - **Desventajas:**
        - **Gestión:** Requiere un esfuerzo administrativo considerable para configurar cada dispositivo y mantener un registro preciso para evitar conflictos de IP (asignar la misma IP a dos dispositivos).[152]
        - **Errores:** Propensa a errores manuales (dirección IP incorrecta, máscara de subred errónea, gateway equivocado, duplicados) que pueden causar problemas de conectividad.[152]
        - **Escalabilidad:** Difícil de gestionar en redes grandes o con dispositivos que cambian con frecuencia.[152]
    - *Relevancia para Pentesters:* Las direcciones IP estáticas son más fáciles de rastrear y perfilar a lo largo del tiempo durante fases de reconocimiento prolongadas. Los servidores, la infraestructura de red crítica (routers, firewalls) y las impresoras suelen tener direcciones IP estáticas. Una mala configuración manual (máscara incorrecta, gateway incorrecto) puede ser una vulnerabilidad explotable.
- **Asignación Dinámica:**
    - **Descripción:** La configuración IP se asigna automáticamente a los dispositivos cuando se conectan a la red, utilizando protocolos específicos.[152] Las direcciones suelen asignarse por un período limitado (lease o concesión) y pueden cambiar con el tiempo.
    - **Métodos Principales:**
        - **DHCP (Dynamic Host Configuration Protocol) para IPv4:** Un servidor DHCP centralizado gestiona un grupo (pool) de direcciones IP y las "presta" a los clientes que las solicitan, junto con otras opciones de configuración (máscara, gateway, DNS, etc.).[152] Es el método predominante en redes IPv4.
        - **DHCPv6 (DHCP para IPv6):** Puede operar en dos modos principales [161]:
            - **Stateful:** Similar a DHCPv4, el servidor DHCPv6 asigna direcciones IPv6 completas del pool y realiza un seguimiento del estado de estas asignaciones (quién tiene qué dirección y por cuánto tiempo). También puede proporcionar otras opciones de configuración.
            - **Stateless:** El servidor DHCPv6 *no* asigna direcciones IPv6 (se asume que el host las obtiene mediante SLAAC), pero sí proporciona otra información de configuración útil que SLAAC no ofrece de forma estándar, como las direcciones de los servidores DNS o el nombre de dominio.
        - **SLAAC (Stateless Address Autoconfiguration) para IPv6:** Un método específico de IPv6 donde el host genera su propia dirección IP.[126] Utiliza los mensajes de Router Advertisement (RA) enviados por los routers locales para obtener el prefijo de red y otra información básica (como el gateway por defecto). Combina este prefijo con un Identificador de Interfaz (IID)

generado localmente (usando EUI-64 o Extensiones de Privacidad). No requiere un servidor central para asignar direcciones y no mantiene un registro del estado de las asignaciones.

- **Ventajas (Dinámica):**
  - **Administración Simplificada:** Reduce enormemente la carga administrativa, especialmente en redes grandes.[152]
  - **Menos Errores:** Minimiza los errores de configuración manual y los conflictos de IP.[152]
  - **Uso Eficiente de IP:** Las direcciones se reutilizan cuando expiran las concesiones o los dispositivos se desconectan.[152]
  - **Escalabilidad y Flexibilidad:** Facilita la adición, eliminación o movimiento de dispositivos.[152] Ideal para entornos con muchos dispositivos móviles o invitados (BYOD, Wi-Fi público).[155]
- **Desventajas (Dinámica):**
  - **IPs Cambiantes:** Las direcciones pueden cambiar, lo que dificulta el acceso directo a un dispositivo específico por IP o el seguimiento a largo plazo.[153]
  - **Dependencia:** Requiere que el servidor DHCP (para DHCP/DHCPv6 stateful) o el router local (para SLAAC y DHCPv6 stateless) estén operativos y correctamente configurados.
  - **Menos Control Centralizado (SLAAC):** SLAAC ofrece menos control administrativo centralizado sobre qué direcciones se asignan en comparación con DHCP/DHCPv6 stateful.[161]
- *Relevancia para Pentesters:* Los entornos dinámicos implican que las direcciones IP de los objetivos (especialmente estaciones de trabajo) pueden cambiar entre escaneos o incluso durante una sesión. El reconocimiento debe ser un proceso continuo. La infraestructura de asignación dinámica (servidores DHCP, routers que emiten RAs) se convierte en un objetivo en sí misma, ya que su compromiso o manipulación puede permitir ataques de denegación de servicio (DoS) o de intermediario (Man-in-the-Middle - MitM). Comprender qué método (DHCP, DHCPv6 stateful/stateless, SLAAC) se utiliza ayuda a predecir el comportamiento de la red y a seleccionar los vectores de ataque adecuados.

La elección entre asignación estática y dinámica a menudo refleja un equilibrio entre la necesidad de previsibilidad y control (favoreciendo la estática para servidores e infraestructura) y la eficiencia administrativa y escalabilidad (favoreciendo la dinámica para los puntos finales de los usuarios). Un pentester puede inferir prácticas potenciales de gestión de red y tipos de objetivos basándose en el esquema de direccionamiento probable encontrado durante el reconocimiento.

## Inmersión Profunda en Asignación Dinámica: DHCP DORA y SLAAC

## (RA/ND)

Para explotar o evaluar adecuadamente los mecanismos de asignación dinámica, es crucial comprender sus procesos subyacentes.

- Proceso DORA de DHCP (IPv4 - RFC 2131):
  El proceso de obtención de una dirección IP mediante DHCPv4 implica una conversación de cuatro pasos entre el cliente y el servidor, conocida como DORA 157:
  1. **Discover (Descubrir):** El cliente DHCP, al conectarse a la red y necesitar una configuración IP, envía un mensaje DHCPDISCOVER. Este mensaje es un **broadcast** (Destino IP: 255.255.255.255, Destino MAC: FF:FF:FF:FF:FF:FF) ya que el cliente no conoce la dirección de ningún servidor DHCP. El mensaje utiliza una dirección IP de origen de 0.0.0.0 porque aún no tiene una asignada.[157] El cliente incluye su dirección MAC para que los servidores puedan responderle.
  2. **Offer (Ofrecer):** Uno o más servidores DHCP en la red que reciben el DHCPDISCOVER pueden responder con un mensaje DHCPOFFER. Este mensaje contiene una propuesta de dirección IP para el cliente, la duración de la concesión (lease time) y otras opciones de configuración (máscara de subred, gateway, DNS, etc.).[157] La oferta se envía típicamente como broadcast a nivel de IP (255.255.255.255) pero dirigida a la dirección MAC específica del cliente a nivel de enlace de datos.[158]
  3. **Request (Solicitar):** El cliente recibe una o más ofertas y selecciona una (normalmente la primera que llega). Para aceptar la oferta, envía un mensaje DHCPREQUEST. Este mensaje también es un **broadcast**.[157] Se envía como broadcast para informar a todos los servidores DHCP cuál oferta ha sido aceptada; los servidores cuyas ofertas no fueron seleccionadas pueden entonces liberar las direcciones IP que habían reservado.[157] El DHCPREQUEST incluye un identificador del servidor elegido y repite la dirección IP solicitada.
  4. **Acknowledge (Confirmar):** El servidor DHCP cuya oferta fue seleccionada finaliza el proceso enviando un mensaje DHCPACK. Este mensaje confirma que la dirección IP y los parámetros de configuración han sido asignados al cliente y establece formalmente la concesión.[157] Este mensaje también suele enviarse como broadcast a nivel IP pero unicast a nivel MAC.[160] Una vez que el cliente recibe el DHCPACK, configura su interfaz de red con la información recibida y puede comenzar a comunicarse en la red.
  - *Relevancia para Pentesters:* Cada paso de DORA es una oportunidad para el reconocimiento pasivo (sniffing) o ataques activos. Sniffing DHCPDISCOVER y DHCPREQUEST revela las direcciones MAC de los clientes. Sniffing DHCPOFFER y DHCPACK revela la dirección del servidor DHCP, los rangos de IP ofrecidos y opciones de configuración valiosas (gateway, DNS, dominios de búsqueda). Los ataques de DHCP Spoofing interceptan el DHCPDISCOVER y envían un DHCPOFFER malicioso antes que el servidor legítimo. Los ataques de DHCP

Starvation inundan la red con DHCPDISCOVER o DHCPREQUEST falsos.

- Proceso SLAAC (IPv6 - RFC 4861/4862):
  SLAAC permite a los hosts IPv6 autoconfigurarse sin depender de un servidor DHCPv6 para la asignación de direcciones. Se basa en el Protocolo de Descubrimiento de Vecinos (Neighbor Discovery Protocol - NDP), que utiliza mensajes ICMPv6.126 Los pasos clave son:
  1. **Generación de Dirección Link-Local:** Al activarse una interfaz IPv6, el host primero genera su dirección Link-Local. Combina el prefijo estándar fe80::/64 con un Identificador de Interfaz (IID) de 64 bits, típicamente derivado de la dirección MAC mediante EUI-64 modificado o generado aleatoriamente mediante Extensiones de Privacidad.[126]
  2. **Detección de Direcciones Duplicadas (DAD):** Antes de usar la dirección Link-Local (y cualquier otra dirección unicast), el host debe verificar que sea única en el enlace local. Envía un mensaje ICMPv6 **Neighbor Solicitation (NS)** a la dirección solicited-node multicast correspondiente a su dirección tentativa, usando la dirección no especificada (::) como origen. Si otro nodo ya está usando esa dirección, responderá con un **Neighbor Advertisement (NA)**, indicando un conflicto. Si no se recibe respuesta NA después de un corto período, la dirección se considera única.[126]
  3. **Descubrimiento de Routers:** Para obtener información de red (prefijos para direcciones globales, gateway), el host envía un mensaje ICMPv6 **Router Solicitation (RS)** a la dirección multicast all-routers (ff02::2).[127]
  4. **Anuncio de Router (Router Advertisement - RA):** Los routers IPv6 en el enlace responden a los RS (y también envían RAs periódicamente) con mensajes ICMPv6 **Router Advertisement (RA)**.[126] Estos mensajes contienen información crucial:
     - Uno o más prefijos de red on-link (ej. 2001:db8:cafe:1::/64) que el host puede usar para autoconfigurar direcciones globales (GUAs o ULAs).
     - Tiempos de vida para los prefijos (válido y preferido).
     - La dirección Link-Local del router emisor (que el host usará como gateway por defecto).
     - Flags como el flag 'M' (Managed address configuration) y 'O' (Other configuration) que indican si el host debe usar DHCPv6 stateful (M=1) o stateless (O=1) para obtener direcciones adicionales u otras opciones (como DNS).[166]
  5. **Configuración de Dirección Global:** Si el RA contiene prefijos con el flag 'A' (Autoconfiguration) activado, el host combina el prefijo recibido con su IID (EUI-64 o de privacidad) para formar una o más direcciones globales (GUA o ULA). Luego realiza DAD para cada nueva dirección global generada.[126]
  - *Relevancia para Pentesters:* SLAAC depende completamente de los mensajes NDP (NS, NA, RS, RA) que viajan por el enlace local. Un pentester en el mismo segmento puede:
    - **Pasivamente:** Capturar RAs para descubrir prefijos de red, direcciones de

gateway (link-local del router) y flags M/O que indican el uso de DHCPv6. Capturar NS/NA para mapear direcciones IPv6 a direcciones MAC (similar a ARP).
        - **Activamente:** Enviar RS para provocar RAs de los routers. Enviar NS para resolver direcciones o verificar la presencia de hosts. Explotar la falta de autenticación inherente a NDP para realizar ataques de Rogue RA o NDP cache poisoning (ver Sección 7).

La introducción de SLAAC junto a DHCPv6 en IPv6 crea un panorama de configuración dinámica más complejo que en IPv4. Mientras que DHCPv4 es el principal mecanismo dinámico, IPv6 permite que SLAAC gestione la asignación de direcciones mientras DHCPv6 (en modo stateless) proporciona opciones adicionales, o que DHCPv6 (en modo stateful) gestione todo. Esta dualidad presenta más vectores potenciales de ataque (ataques a NDP/RA además de ataques a DHCPv6) y más puntos de posible mala configuración que un pentester debe investigar.

## Implicaciones de Seguridad y Reconocimiento: DHCP Snooping, Ataques a SLAAC

Tanto DHCP como SLAAC, al ser protocolos fundamentales para la configuración de red, presentan superficies de ataque que los pentesters deben evaluar.

- **Seguridad DHCP (IPv4/IPv6):**
    - **Vulnerabilidades:**
        - **DHCP Spoofing (Suplantación):** Un atacante en la red local configura un servidor DHCP falso (rogue). Cuando un cliente legítimo envía un DHCPDISCOVER (o Solicit en DHCPv6), el servidor rogue responde con una oferta maliciosa (DHCPOFFER/Advertise) más rápido que el servidor legítimo. Si el cliente acepta esta oferta (DHCPREQUEST/Request), el atacante puede proporcionar información de configuración falsa, como su propia dirección IP como gateway por defecto o servidor DNS. Esto le permite interceptar todo el tráfico del cliente (ataque Man-in-the-Middle) o redirigirlo a sitios maliciosos.[177]
        - **DHCP Starvation (Agotamiento):** El atacante envía una gran cantidad de mensajes DHCPDISCOVER/Solicit utilizando direcciones MAC de origen falsificadas (spoofed). El servidor DHCP legítimo responde con ofertas y reserva direcciones IP de su pool para cada solicitud falsa. Si el atacante también falsifica los DHCPREQUEST/Request, puede agotar rápidamente todo el pool de direcciones IP disponibles. Esto provoca una Denegación de Servicio (DoS), ya que los clientes legítimos no pueden obtener una dirección IP al conectarse a la red.[177]
    - **Mitigación - DHCP Snooping:** Es una característica de seguridad implementada

en switches de red (Capa 2).[177] Funciona de la siguiente manera:
    - **Puertos Confiables vs. No Confiables:** Los puertos del switch se clasifican. Los puertos conectados a servidores DHCP legítimos (o enlaces ascendentes hacia ellos) se configuran como *confiables* (trusted). Todos los demás puertos (conectados a hosts finales) se consideran *no confiables* (untrusted) por defecto.
    - **Filtrado de Mensajes del Servidor:** El switch bloquea los mensajes de *respuesta* DHCP (Offer, Ack, Advertise, Reply) que llegan por puertos no confiables. Esto impide que un servidor DHCP rogue conectado a un puerto de usuario pueda distribuir configuraciones falsas.
    - **Base de Datos de Vinculación (Binding Database):** El switch construye una tabla que mapea la dirección MAC del cliente, la dirección IP asignada, el ID de VLAN y el puerto del switch por el que se realizó la transacción DHCP legítima.
    - **Verificación de Mensajes del Cliente:** (Opcional) El switch puede verificar los mensajes DHCP de los clientes (como DHCPRELEASE o DHCPDECLINE) contra la base de datos de vinculación para asegurar que la dirección MAC y la IP coincidan con una entrada válida para ese puerto.
    - **Limitación de Tasa (Rate Limiting):** Se puede configurar un límite en la cantidad de paquetes DHCP por segundo permitidos en puertos no confiables para mitigar los ataques de DHCP Starvation.
  - *Relevancia para Pentesters:* Durante una prueba interna, se debe intentar realizar ataques de DHCP spoofing y starvation para verificar si DHCP Snooping está habilitado y configurado correctamente. Hay que comprobar si los puertos troncales o los conectados a servidores están marcados como confiables. El reconocimiento pasivo implica capturar tráfico DHCP para identificar servidores y clientes.
- **Seguridad SLAAC (IPv6):**
  - **Vulnerabilidades:**
    - **Rogue Router Advertisements (RA):** Dado que los RAs son mensajes ICMPv6 no autenticados por defecto, un atacante en el enlace local puede enviar RAs falsos.[151] Estos RAs maliciosos pueden:
      - Anunciar prefijos de red falsos, haciendo que los hosts configuren direcciones IP incorrectas y pierdan conectividad (DoS).
      - Anunciar prefijos legítimos pero con la dirección link-local del atacante como gateway por defecto, interceptando todo el tráfico saliente del host (MitM).
      - Anunciar tiempos de vida muy cortos para los prefijos o routers, causando inestabilidad en la red (DoS).
      - Manipular los flags M/O para forzar o impedir el uso de DHCPv6.
      - Inundar la red con RAs falsos para agotar los recursos de los hosts (DoS).[151]

        - **Neighbor Discovery (ND) Spoofing/Poisoning:** Como se detallará en la Sección 7, la falta de autenticación en los mensajes NS/NA permite a un atacante falsificar estos mensajes para redirigir el tráfico entre dos víctimas (envenenamiento de caché ND, similar a ARP poisoning) o realizar DoS.[150]
    - **Mitigaciones:**
        - **RA Guard (RFC 6105/7113):** Similar a DHCP Snooping, es una característica de seguridad de Capa 2 implementada en switches.[175] Los puertos se clasifican como confiables (conectados a routers legítimos) o no confiables (conectados a hosts). RA Guard inspecciona los RAs entrantes en puertos no confiables y los filtra (descarta) si no cumplen con una política definida (ej., permitir RAs solo de ciertas direcciones MAC/IP de origen, bloquear todos los RAs, verificar la consistencia de los prefijos anunciados, etc.). **Importante:** Implementaciones tempranas de RA Guard eran vulnerables a técnicas de evasión usando cabeceras de extensión IPv6 o fragmentación (documentado en RFC 7113).[188]
        - **SEND (Secure Neighbor Discovery - RFC 3971):** Un enfoque más robusto que utiliza Direcciones Generadas Criptográficamente (CGAs) y certificados para autenticar y proteger la integridad de los mensajes NDP (incluidos RAs).[150] Sin embargo, su despliegue es complejo y requiere una infraestructura de clave pública (PKI), por lo que su adopción no es generalizada.[151]
    - *Relevancia para Pentesters:* Los ataques de Rogue RA son una de las amenazas más significativas en redes IPv6 locales no aseguradas. Los pentesters deben probar activamente esta vulnerabilidad utilizando herramientas como thc-ipv6 [175] o Scapy. Es crucial verificar si RA Guard está implementado, si la política es adecuada y si es susceptible a las técnicas de evasión conocidas (fragmentación, cabeceras de extensión). El reconocimiento implica capturar y analizar mensajes RA y otros mensajes NDP.

Los mecanismos de seguridad como DHCP Snooping y RA Guard son defensas esenciales de Capa 2 contra ataques comunes de asignación dinámica. Sin embargo, su eficacia depende de una configuración correcta y de implementaciones robustas. No son infalibles y deben ser específicamente evaluados durante una prueba de penetración para confirmar su presencia, correcta configuración y resistencia a técnicas de evasión conocidas.

# 5. Navegando por la Traducción de Direcciones de Red (NAT)

Network Address Translation (NAT) es una tecnología omnipresente en las redes IPv4, nacida principalmente de la necesidad de conservar el limitado espacio de direcciones públicas. Aunque IPv6 con su vasto espacio de direcciones reduce la necesidad de NAT para la conservación, NAT sigue siendo relevante y los pentesters deben comprender cómo funciona

y sus implicaciones para la seguridad.

## Conceptos Centrales: NAT vs. PAT (NAT Overload) Explicados

**Network Address Translation (NAT)** es un proceso, generalmente realizado por un router o firewall en el borde de una red, que consiste en modificar la información de la dirección IP en las cabeceras de los paquetes mientras transitan entre una red (típicamente privada) y otra (típicamente la Internet pública).[34]
El principal impulsor histórico de NAT fue la **conservación de direcciones IPv4 públicas**.[4] Permite que múltiples dispositivos en una red local, utilizando direcciones IP privadas (RFC 1918), compartan una o unas pocas direcciones IP públicas para acceder a Internet.[202]
Existen varios tipos de NAT, pero los más relevantes son:

1. **Static NAT (NAT Estático):** Establece un mapeo **uno a uno** permanente entre una dirección IP privada interna y una dirección IP pública externa.[34] Cada vez que el dispositivo interno envía tráfico, se traduce a la misma IP pública. El tráfico entrante a esa IP pública se traduce siempre a la misma IP privada. Se utiliza comúnmente para hacer accesibles servidores internos (web, correo) desde Internet.
2. **Dynamic NAT (NAT Dinámico):** Mapea una dirección IP privada interna a una dirección IP pública disponible de un **grupo (pool)** predefinido de direcciones públicas.[34] El mapeo es temporal y dura mientras la conexión está activa o por un tiempo determinado. Requiere tener un pool de direcciones públicas al menos tan grande como el número de hosts internos que necesiten acceder a Internet simultáneamente. Sigue siendo un mapeo uno a uno mientras está activo.
3. **PAT (Port Address Translation) o NAT Overload (Sobrecarga NAT):** Es una forma de NAT dinámico que permite que **múltiples** direcciones IP privadas internas se mapeen a **una única** dirección IP pública.[34] Logra esto no sólo traduciendo la dirección IP de origen, sino también el **puerto de origen**. El dispositivo NAT asigna un puerto de origen único (del rango de puertos efímeros) en la IP pública para cada conexión saliente iniciada desde un host interno diferente (o incluso desde el mismo host pero con un puerto de origen diferente). Mantiene una tabla de estado que rastrea la correspondencia entre {IP_privada:Puerto_privado} y {IP_pública:Puerto_público_asignado}. Cuando llega una respuesta a la IP pública y al puerto asignado, utiliza la tabla para traducir de vuelta a la IP y puerto privados originales. Este es, con diferencia, el tipo de NAT más común utilizado en hogares y pequeñas empresas para el acceso a Internet.[207]

Todos los tipos de NAT (excepto quizás el estático más simple) dependen de **tablas de traducción de estado (stateful translation tables)**. Estas tablas almacenan información sobre las conexiones activas que atraviesan el dispositivo NAT, incluyendo las direcciones y puertos internos y externos mapeados, y a menudo información del protocolo de transporte (TCP/UDP) y temporizadores.[34] Esta naturaleza stateful es clave para permitir que el tráfico de

respuesta regrese al host interno correcto.

- **Relevancia para Pentesters:** Identificar el tipo de NAT implementado es crucial. PAT es la barrera más común para el escaneo externo directo de hosts internos. Si se detecta Static NAT (por ejemplo, una IP pública que siempre responde con los servicios de un servidor específico), ese servidor interno se convierte en un objetivo directo desde el exterior (aunque probablemente protegido por un firewall). Dynamic NAT dificulta el seguimiento a largo plazo de un host interno desde el exterior, pero todavía expone un conjunto de IPs públicas.

## Cómo NAT Permite la Comunicación Privada-a-Pública (Contexto RFC 1918)

El escenario de uso más común para NAT/PAT es permitir que los hosts de una red interna que utilizan direcciones privadas RFC 1918 (como 192.168.1.0/24) se comuniquen con hosts en la Internet pública.[4] El proceso funciona de la siguiente manera, asumiendo un dispositivo NAT (router/firewall) en el borde de la red con una interfaz interna (ej. 192.168.1.1) y una interfaz externa con una IP pública (ej. 203.0.113.1) [4]:

- **Tráfico Saliente (Desde Privado hacia Público):**
  1. Un host interno (ej. 192.168.1.100) quiere conectarse a un servidor en Internet (ej. 8.8.8.8 en el puerto 53 - DNS). Envía un paquete con:
     - Origen IP: 192.168.1.100
     - Puerto Origen: (un puerto efímero, ej. 51000)
     - Destino IP: 8.8.8.8
     - Puerto Destino: 53
  2. El paquete llega al dispositivo NAT (router) en su interfaz interna.
  3. El dispositivo NAT consulta su configuración. Reconoce que el tráfico va desde la red interna a la externa y necesita traducción.
  4. Modifica la cabecera IP del paquete:
     - Reemplaza la IP Origen privada (192.168.1.100) por su IP pública (203.0.113.1).[34]
     - Si usa PAT, reemplaza el Puerto Origen privado (51000) por un puerto público único de su pool (ej. 62001).[199]
  5. Crea (o actualiza) una entrada en su tabla de estado NAT: {192.168.1.100:51000} <-> {203.0.113.1:62001} (mapeando la tupla interna a la externa para esta conexión específica).[34]
  6. Recalcula las sumas de comprobación (checksums) de las cabeceras IP y TCP/UDP si es necesario.
  7. Envía el paquete traducido hacia Internet. El servidor en 8.8.8.8 ve el paquete como si viniera de 203.0.113.1:62001.
- **Tráfico Entrante (Respuesta desde Público hacia Privado):**
  1. El servidor en 8.8.8.8 responde. Envía un paquete con:

        - Origen IP: 8.8.8.8
        - Puerto Origen: 53
        - Destino IP: 203.0.113.1
        - Puerto Destino: 62001
    2. El paquete llega al dispositivo NAT en su interfaz externa.
    3. El dispositivo NAT examina la IP y puerto de destino (203.0.113.1:62001).
    4. Busca esta tupla en su tabla de estado NAT y encuentra la entrada correspondiente: {192.168.1.100:51000} <-> {203.0.113.1:62001}.[34]
    5. Modifica la cabecera IP del paquete de respuesta:
        - Reemplaza la IP Destino pública (203.0.113.1) por la IP privada (192.168.1.100).
        - Reemplaza el Puerto Destino público (62001) por el Puerto privado original (51000).
    6. Recalcula checksums si es necesario.
    7. Envía el paquete traducido hacia el host interno 192.168.1.100.

Este proceso stateful es la razón por la que NAT/PAT permite la comunicación iniciada desde el interior, pero generalmente bloquea las conexiones iniciadas desde el exterior: si un paquete llega a la IP pública del NAT desde Internet sin una entrada preexistente en la tabla de estado (es decir, no es una respuesta a una conexión saliente), el NAT no sabe a qué host interno dirigirlo y lo descarta.[206]

- **Relevancia para Pentesters:** Este mecanismo explica por qué los escaneos externos estándar fallan contra hosts internos detrás de NAT/PAT. El dispositivo NAT actúa como un guardián stateful. Para alcanzar un host interno desde el exterior, se necesita una excepción explícita (port forwarding) o se debe inducir al host interno a iniciar una conexión hacia el exterior (reverse shell).

## Desafíos y Oportunidades de NAT para Pentesters

La presencia de NAT/PAT en el perímetro de una red objetivo presenta tanto obstáculos como posibles puntos de interés para un pentester.

- **Dificultad para Escanear Hosts Internos Directamente:** Como se ha explicado, el principal desafío que impone NAT/PAT es que bloquea las conexiones entrantes no solicitadas.[206] Esto significa que un pentester que realiza un escaneo desde Internet no puede "ver" ni interactuar directamente con los hosts internos que utilizan direcciones RFC 1918, a menos que existan reglas específicas que permitan el tráfico entrante.[215] El escaneo de puertos estándar contra la IP pública del dispositivo NAT solo revelará los puertos abiertos en el propio dispositivo NAT o aquellos que han sido explícitamente reenviados (forwarded) a hosts internos.
- **Necesidad de Pivoting:** Para superar la barrera del NAT y evaluar la seguridad de la red interna, los pentesters a menudo necesitan emplear técnicas de **pivoting**.[215] El

pivoting consiste en utilizar un sistema comprometido *dentro* de la red objetivo como punto de apoyo o relevo para lanzar ataques o escaneos contra otros sistemas internos que no son accesibles directamente desde el exterior.[215] Una vez que se obtiene acceso a un host interno (por ejemplo, a través de un exploit en un servicio expuesto o mediante phishing), ese host comprometido puede usarse para escanear otros rangos de IP internas (RFC 1918), acceder a recursos compartidos internos o intentar explotar otras vulnerabilidades dentro de la red local. Herramientas como Metasploit tienen módulos específicos para facilitar el pivoting a través de sesiones comprometidas (Meterpreter, SSH).[216]

- **Reverse Shells (Conexiones Inversas):** Dado que NAT/PAT permite el tráfico saliente iniciado desde el interior, una técnica fundamental para obtener control interactivo de un host comprometido detrás de NAT es la **reverse shell**.[215] En lugar de que el atacante se conecte *hacia* el host comprometido (lo cual sería bloqueado por NAT), el host comprometido inicia una conexión *hacia fuera*, hacia una máquina controlada por el atacante que está escuchando en un puerto específico. Una vez establecida esta conexión saliente (que NAT permite y traduce), el atacante puede enviar comandos al host comprometido a través de este túnel inverso. Esta es la forma estándar de obtener un shell interactivo en un sistema detrás de NAT después de una explotación exitosa.
- **Descubrimiento de Port Forwarding (Reenvío de Puertos):** Aunque NAT bloquea el tráfico entrante no solicitado por defecto, los administradores a menudo necesitan exponer servicios internos (como un servidor web, un servidor de correo o un servidor VPN) a Internet. Esto se logra mediante **port forwarding**, que es una configuración en el dispositivo NAT (una forma de Destination NAT o DNAT) que mapea un puerto específico en la dirección IP pública externa a una dirección IP y puerto privados internos.[206] Por ejemplo, se podría configurar para que todo el tráfico que llegue a public_IP:80 sea redirigido a private_IP_WebServer:80.
    - *Oportunidad para Pentesters:* Los puertos reenviados son **visibles y escaneables** desde Internet.[217] Durante el reconocimiento externo, un escaneo de puertos contra la IP pública del NAT revelará estos puertos abiertos. Identificar los servicios que se ejecutan en estos puertos reenviados es crucial, ya que representan la superficie de ataque externa directa hacia la red interna. Cualquier vulnerabilidad en estos servicios expuestos puede ser una puerta de entrada a la red privada.
- **Técnicas de Traversal de NAT:** Existen protocolos diseñados específicamente para ayudar a establecer conexiones directas (peer-to-peer) entre dispositivos que se encuentran detrás de diferentes dispositivos NAT. Estos son comunes en aplicaciones como VoIP, videoconferencia (WebRTC), juegos en línea y compartición de archivos P2P.[223] Los más conocidos incluyen:
    - **STUN (Session Traversal Utilities for NAT):** Permite a un cliente detrás de NAT descubrir su dirección IP pública y el tipo de NAT que tiene.[223] Funciona bien con algunos tipos de NAT pero no con todos (falla con NAT simétrico).[225]
    - **TURN (Traversal Using Relays around NAT):** Utiliza un servidor intermediario

(relay) en Internet. Cuando una conexión directa falla, los clientes envían su tráfico al servidor TURN, que lo retransmite al otro par.[223] Funciona con más tipos de NAT pero introduce latencia y requiere infraestructura de servidor.

- **ICE (Interactive Connectivity Establishment):** Un framework que utiliza STUN y TURN (y direcciones locales) para encontrar la mejor ruta de comunicación posible entre dos pares, intentando primero una conexión directa y recurriendo a TURN si es necesario.[223] Es la base de WebRTC.
- **UPnP (Universal Plug and Play) / NAT-PMP (NAT Port Mapping Protocol):** Permiten a las aplicaciones dentro de la red local solicitar al dispositivo NAT que abra puertos automáticamente para permitir conexiones entrantes.[223] UPnP es común en routers domésticos pero a menudo se considera un riesgo de seguridad si no está debidamente asegurado.[223]
- *Relevancia para Pentesters (Traversal):* Aunque estos protocolos están diseñados para uso legítimo, pueden presentar vectores de ataque. Un servidor STUN/TURN mal configurado o vulnerable podría filtrar información sobre la red. UPnP, si está habilitado en el router NAT y no está restringido, podría ser abusado por malware dentro de la red para abrir puertos no deseados hacia Internet, o por un atacante externo (si la interfaz de administración UPnP está expuesta) para mapear puertos hacia hosts internos. Los pentesters deben verificar la presencia y seguridad de estos mecanismos.

En esencia, NAT/PAT redefine el campo de batalla para los pentesters. Transforma la evaluación externa de una tarea de escaneo directo de hosts a una de identificación de servicios expuestos a través de port forwarding. Para evaluar la red interna "detrás" del NAT, el compromiso inicial de un sistema expuesto o interno se vuelve primordial, seguido por técnicas de pivoting y el establecimiento de canales de comando y control inversos (reverse shells) que aprovechen la permisividad inherente de NAT para las conexiones salientes. Aunque NAT ofrece una capa de ocultación para los hosts internos, no debe considerarse una barrera de seguridad robusta por sí misma. Las reglas de port forwarding mal configuradas, los servicios vulnerables expuestos a través de esas reglas, o las debilidades en los mecanismos de traversal de NAT pueden proporcionar puntos de entrada a la red interna. Un pentester debe evaluar NAT no como un muro infranqueable, sino como una capa de traducción con sus propias configuraciones y protocolos asociados que pueden ser vulnerables.

# 6. Técnicas de Reconocimiento y Enumeración de IP

La fase de reconocimiento y enumeración es fundamental en cualquier prueba de penetración. El objetivo es descubrir hosts activos, identificar los servicios que ejecutan, mapear la topología de la red y recopilar tanta información como sea posible sobre el entorno objetivo utilizando las direcciones IP como punto de partida.

### Descubrimiento de Hosts Activos (Ping Sweeps y Otras Sondas)

El primer paso suele ser determinar qué direcciones IP dentro de un rango objetivo corresponden a sistemas activos ("vivos"). Varias técnicas, a menudo implementadas en herramientas como **Nmap**, se utilizan para este propósito [80]:

- **ICMP Echo Ping Sweep (nmap -sn -PE <target_range>):**
    - **Mecanismo:** Envía paquetes ICMP Echo Request (tipo 8) a cada dirección IP en el rango objetivo. Los hosts activos que no bloquean ICMP responderán con un ICMP Echo Reply (tipo 0).[235]
    - **Ventajas:** Rápido y sencillo si ICMP

Pero esto lo tratamos en profundidad en otro manual:

**Nmap para pentesters: de cero a pro**[252]

https://www.linkedin.com/posts/m7villalobos_nmap-para-pentesters-de-cero-a-pro-activity-7319330458247356417-DptO

# Obras citadas


1. What Is IPv4? What Are the Limitations of IPv4? - Huawei Technical Support, https://info.support.huawei.com/info-finder/encyclopedia/en/IPv4.html
2. IPv4 address exhaustion - Wikipedia, https://en.wikipedia.org/wiki/IPv4_address_exhaustion
3. A Linux networking guide to CIDR notation and configuration - Opensource.com, https://opensource.com/article/16/12/cidr-network-notation-configuration-linux
4. What is an RFC1918 Address? - NetBeez, https://netbeez.net/blog/rfc1918/
5. Private IP Addresses (RFC 1918) Tutorial - FlackBox, https://www.flackbox.com/cisco-private-ip-addresses-rfc-1918
6. Preparing an IPv6 Address Plan, https://www.ipv6forum.com/dl/presentations/IPv6-addressing-plan-howto.pdf
7. www.geoplugin.com, https://www.geoplugin.com/resources/ip-address-format-everything-you-need-to-know/#:~:text=IPv4%20address%20format%20consists%20of,0.1.
8. Understanding IPv4 and IPv6 Protocol Families | Junos OS - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-ipv4-ipv6-protocol.html
9. IP address - Wikipedia, https://en.wikipedia.org/wiki/IP_address
10. Understand TCP/IP addressing and subnetting basics - Learn Microsoft, https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting
11. IP Address Format: Everything You Need To Know - GeoPlugin,

https://www.geoplugin.com/resources/ip-address-format-everything-you-need-to-know/
12. What is IPv4? - GeeksforGeeks, https://www.geeksforgeeks.org/what-is-ipv4/
13. Introduction of Classful IP Addressing | GeeksforGeeks, https://www.geeksforgeeks.org/introduction-of-classful-ip-addressing/
14. IPv4 Addressing - IBM, https://www.ibm.com/docs/en/zvm/7.4?topic=addressing-ipv4
15. Classful network - Wikipedia, https://en.wikipedia.org/wiki/Classful_network
16. Classful and Classless Addressing Explained - Auvik Networks, https://www.auvik.com/franklyit/blog/classful-classless-addressing/
17. Classful vs Classless Addressing | GeeksforGeeks, https://www.geeksforgeeks.org/classful-vs-classless-addressing/
18. History of the Internet - APNIC, https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-internet/
19. Classful Addressing Limitations - TCP/IP Implementation and Operations Guide, https://public.support.unisys.com/aseries/docs/ClearPath-MCP-20.0/37877693-226/section-000021665.html
20. IPv4 - Wikipedia, the free encyclopedia, http://cs.indstate.edu/~jkinne/cs473-s2015/ipv4.html
21. How to Calculate Network Addresses with ipcalc - Linux.com, https://www.linux.com/topic/networking/how-calculate-network-addresses-ipcalc/
22. IANA IPv4 Special-Purpose Address Registry - Internet Assigned Numbers Authority, https://www.iana.org/assignments/iana-ipv4-special-registry
23. RFC 1918 - Address Allocation for Private Internets - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc1918
24. Understanding IP Addressing and CIDR Charts — RIPE Network Coordination Centre, https://www.ripe.net/about-us/press-centre/understanding-ip-addressing/
25. RFC 1918 - CyberHoot Cyber Library, https://cyberhoot.com/cybrary/rfc-1918/
26. Understanding Public and Private IP Addresses | pfSense Documentation, https://docs.netgate.com/pfsense/en/latest/network/addresses.html
27. IT - Use of RFC 1918 "Private Addresses" on the UC Berkeley Campus Network, https://berkeley.service-now.com/kb_view.do?sysparm_article=KB0011961
28. IPv4 Private Address Space and Filtering - American Registry for Internet Numbers - ARIN, https://www.arin.net/reference/research/statistics/address_filters/
29. Private network - Wikipedia, https://en.wikipedia.org/wiki/Private_network
30. Prevent IPv4 exhaustion in Azure - Azure Architecture Center - Learn Microsoft, https://learn.microsoft.com/en-us/azure/architecture/networking/guide/ipv4-exhaustion
31. Special IP Address Ranges and When to Use Them | Auvik, https://www.auvik.com/franklyit/blog/special-ip-address-ranges/
32. Private and Reserved IP Addresses - WintelGuy.com,

https://wintelguy.com/2009/20090220_private_ip.html
33. Reserved IP addresses - Wikipedia, https://en.wikipedia.org/wiki/Reserved_IP_addresses
34. Network Address Translation (NAT) - GeeksforGeeks, https://www.geeksforgeeks.org/network-address-translation-nat/
35. RFC 6598 - IANA-Reserved IPv4 Prefix for Shared Address Space - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc6598
36. Can I Use Shared (RFC 6598) IPv4 Address Space Within My Network? - ipSpace.net blog, https://blog.ipspace.net/2013/08/can-i-use-shared-rfc-6598-ipv4-address/
37. What is an IPv4 Subnet Mask? - Explainer - Brander Group, https://brandergroup.net/2021/02/what-is-ipv4-subnet-mask/
38. What is a Subnet Mask? Examples, Uses and Benefits - Auvik Networks, https://www.auvik.com/franklyit/blog/what-is-subnet-mask/
39. What Is a Subnet Mask? 2024 Updated Guide - IPXO, https://www.ipxo.com/blog/what-is-subnet-mask/
40. What does a subnet mask really do? : r/CompTIA - Reddit, https://www.reddit.com/r/CompTIA/comments/1d78zvc/what_does_a_subnet_mask_really_do/
41. I'm mildly confused what the purpose of a subnet mask is : r/CompTIA - Reddit, https://www.reddit.com/r/CompTIA/comments/n6h7og/im_mildly_confused_what_the_purpose_of_a_subnet/
42. Role of Subnet Mask | GeeksforGeeks, https://www.geeksforgeeks.org/role-of-subnet-mask/
43. Why do we need subnet mask? - Super User, https://superuser.com/questions/394385/why-do-we-need-subnet-mask
44. How to Calculate Number of Host in a Subnet? - GeeksforGeeks, https://www.geeksforgeeks.org/how-to-calculate-number-of-host-in-a-subnet/?ref=rp
45. What is CIDR? - CIDR Blocks and Notation Explained - AWS, https://aws.amazon.com/what-is/cidr/
46. Classless Inter-Domain Routing - Wikipedia, https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing
47. Classless Inter Domain Routing (CIDR) - GeeksforGeeks, https://www.geeksforgeeks.org/classless-inter-domain-routing-cidr/?ref=rp
48. VLSM: A Complete Guide to Variable Length Subnet Masking - Netmaker, https://www.netmaker.io/resources/vlsm
49. Introduction of Variable Length Subnet Mask (VLSM) - GeeksforGeeks, https://www.geeksforgeeks.org/introduction-of-variable-length-subnet-mask-vlsm/
50. Understanding CIDR Notation in IP Subnets - NetworkCalc, https://networkcalc.com/articles/cidr-notation/
51. Understanding CIDR Subnet Mask Notation | pfSense Documentation, https://docs.netgate.com/pfsense/en/latest/network/cidr.html
52. CIDR to Subnet Mask Explained: Simplify IP Addressing - Netmaker,

https://www.netmaker.io/resources/cidr-to-subnet-mask
53. CIDR Full Form | GeeksforGeeks, https://www.geeksforgeeks.org/cidr-full-form/
54. About Slash Notation - WatchGuard, http://www.watchguard.com/help/docs/help-center/en-US/content/en-us/Firewar e/overview/networksecurity/slash_about_c.html
55. Understanding CIDRs and Public vs Private IPs - DZone, https://dzone.com/articles/understanding-cidrs-classless-inter-domain-routing
56. Subnetting: What It Is and How It Works | Auvik, https://www.auvik.com/franklyit/blog/subnetting-primer/
57. Introduction To Subnetting | GeeksforGeeks, https://www.geeksforgeeks.org/introduction-to-subnetting/
58. Subnetting Tutorial Guide – What is Subnet? - DNSstuff, https://www.dnsstuff.com/subnet-ip-subnetting-guide
59. 4 Examples | IP Subnetting Overview - IPCisco, https://ipcisco.com/lesson/ip-subnetting-and-subnetting-examples/
60. Variable Length Subnet Mask (VLSM) Tutorial - Fully Explained - Comparitech, https://www.comparitech.com/net-admin/variable-length-subnet-mask-vlsm-tut orial/
61. Subnetting in Binary - NetworkLessons.com, https://networklessons.com/subnetting/subnetting-in-binary
62. Subnetting Tutorial – Subnetting Made Easy - CCNA Training, https://www.9tut.com/subnetting-tutorial
63. Subnetting an IP Address - cloudfront.net, https://d12vzecr6ihe4p.cloudfront.net/media/966010/wp-subnetting-an-ip-addre ss.pdf
64. Understanding Variable Length Subnet Masks (VLSM) - Study CCNA, https://study-ccna.com/variable-length-subnet-mask-vlsm/
65. Calculating IPv4 Subnets and Hosts - CompTIA Network+ N10-007 - 1.4 - YouTube, https://www.youtube.com/watch?v=qQEaAb_p8_E
66. Calculating IPv4 Subnets and Hosts - CompTIA Network+ N10-009 - 1.7 - YouTube, https://www.youtube.com/watch?v=cYQOMifDIKI
67. What is VLSM? | NetworkAcademy.io, https://www.networkacademy.io/ccna/ip-subnetting/what-is-vlsm
68. VLSM in Networking || Variable Length Subnet Mask - PyNet Labs, https://www.pynetlabs.com/what-is-vlsm-variable-length-subnet-mask/
69. Subnet Mask Cheat Sheet - A Tutorial and Thorough Guide to Subnetting! - Websentra, https://www.websentra.com/subnet-mask-cheat-sheet-guide/
70. Subnetting Tricks Subnetting Made Easy with Examples - Computer Networking Notes, https://www.computernetworkingnotes.com/ccna-study-guide/subnetting-tricks-subnetting-made-easy-with-examples.html
71. Ip Addressing and Subnetting Workbook - Instructors Version v1_5.pmd, https://dce.telkomuniversity.ac.id/wp-content/uploads/2014/09/49445184-IP-Addr essing-and-Subnetting-Workbook-Instructors-Version-1-5.pdf
72. 4 Ways to Calculate the Network and Broadcast Address - wikiHow,

https://www.wikihow.com/Calculate-Network-and-Broadcast-Address
73. A Beginners Guide to Subnetting - Packet Coders, https://www.packetcoders.io/a-beginners-guide-to-subnetting/
74. IP Calculator / IP Subnetting, https://jodies.de/
75. Calculate Network, Broadcast and host addresses - YouTube, https://www.youtube.com/watch?v=hb2yTNT2rBU&pp=0gcJCdgAo7VqN5tD
76. Easy IPv4 Subnetting and Mask Calculation Method - Interlir networks marketplace, https://interlir.com/2024/02/19/easy-ipv4-subnetting-and-mask-calculation-method/
77. What's an Internal Network Segmentation Penetration Test? - RSI Security, https://blog.rsisecurity.com/whats-an-internal-network-segmentation-penetration-test/
78. Subnetting != Segmentation - LMG Security, https://www.lmgsecurity.com/pentest-subnetting-segmentation/
79. Penetration Testing | Pen Testing - Akto, https://www.akto.io/devsecops/what-is-penetration-testing-a-step-by-step-guide
80. Nmap Subnet Scanning Tutorial: Network Reconnaissance for Beginners - DEV Community, https://dev.to/labex/nmap-subnet-scanning-tutorial-network-reconnaissance-for-beginners-8n4
81. Network Penetration Testing Checklist - 2025 - GBHackers, https://gbhackers.com/network-penetration-testing-checklist-examples/
82. A COMPREHENSIVE ANALYSIS OF NETWORK SCANNING AND SECURITY ASSESSMENT TOOL - Aircc Digital Library, https://aircconline.com/ijnsa/V16N6/16624ijnsa07.pdf
83. What Is Nmap? A Comprehensive Tutorial For Network Mapping - Simplilearn.com, https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-nmap
84. Network Scanning With Nmap Commands: Definitive Guide - Netmaker, https://www.netmaker.io/resources/nmap-commands
85. Network Mapper: Purpose, Devices, and Security Insights - Fynd Academy, https://www.fynd.academy/blog/network-mapper
86. nmap - How do I find subnets on the network in order to scan them for hosts?, https://security.stackexchange.com/questions/266513/how-do-i-find-subnets-on-the-network-in-order-to-scan-them-for-hosts
87. Learn About The Five Penetration Testing Phases | Pentesting - EC-Council, https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/
88. Penetration Testing Phases: Steps in the Process - Compass IT Compliance, https://www.compassitc.com/blog/penetration-testing-phases-steps-in-the-process
89. Web Application Penetration Testing: Steps, Methods, & Tools - PurpleSec, https://purplesec.us/learn/web-application-penetration-testing/

90. 7 Penetration Testing Phases Explained: Ultimate Guide - Astra Security, https://www.getastra.com/blog/security-audit/penetration-testing-phases/
91. Pentesting Reconnaissance: Gathering information about the target - 4Geeks, https://4geeks.com/lesson/pentesting-reconnaissance-gathering-information-about-the-target
92. Penetration Test Steps: 7 Pentesting Process Phases - Datami Cybersecurity, https://datami.ee/blog/penetration-test-steps-7-pentesting-process-phases/
93. The Essential Guide to Network Enumeration: Tools and Techniques | Fidelis Security, https://fidelissecurity.com/cybersecurity-101/learn/network-enumeration/
94. eJPTv2-Notes/README/assessment-methodologies-and-auditing/1.1-information-gathering.md at main - GitHub, https://github.com/dev-angelist/eJPTv2-Notes/blob/main/README/assessment-methodologies-and-auditing/1.1-information-gathering.md
95. The 4 Phases of Penetration Testing - RSI Security, https://blog.rsisecurity.com/the-4-phases-of-penetration-testing/
96. Nmap | darkcybe, https://darkcybe.github.io/posts/ETH_Tools_Nmap/
97. How to scan and ip range in nmap - Ask Ubuntu, https://askubuntu.com/questions/1226310/how-to-scan-and-ip-range-in-nmap
98. Nmap cheat sheet: From discovery to exploits - Part 1 - Infosec, https://www.infosecinstitute.com/resources/hacking/nmap-cheat-sheet/
99. Variable-Length Subnet Masks - Cisco Community, https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/4461-docs-network-infrastructure/4932/1/9781587205804_ch22_0.pdf
100. Variable-Length Subnet Masks > Foundation Topics | Cisco Press, https://www.ciscopress.com/articles/article.asp?p=2731924
101. IPv6 address - Wikipedia, https://en.wikipedia.org/wiki/IPv6_address
102. IPv6 Address Types - RIPE NCC, https://www.ripe.net/participate/member-support/lir-basics/ipv6_reference_card.pdf
103. IPv6 Address Representation | NetworkAcademy.io, https://www.networkacademy.io/ccna/ipv6/ipv6-address-representation
104. RFC 4291 - IP Version 6 Addressing Architecture - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc4291
105. IPv6 - Wikipedia, https://en.wikipedia.org/wiki/IPv6
106. SLAAC Prefixes with Variable Interface ID (IID) - IETF, https://www.ietf.org/archive/id/draft-mishra-v6ops-variable-iids-problem-statement-00.html
107. IPv6 - Wikipedia, the free encyclopedia, https://www.cs.odu.edu/~salam/wsdl/inforet/wikihtml/IPv6_fdb7.html
108. IP Addressing - RouterOS - MikroTik Documentation - Support, https://help.mikrotik.com/docs/spaces/ROS/pages/328247/IP+Addressing
109. Hierarchical IPv6 addressing plan - GestióIP IPAM, http://www.gestioip.net/docu/ipv6_address_examples.html
110. Glowing in the Dark: Uncovering IPv6 Address Discovery and Scanning

Strategies in the Wild - USENIX, https://www.usenix.org/system/files/usenixsecurity23-bin-tanveer.pdf
111. IPv6 Address Types - Cisco Press, https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=3
112. Benefits of IPv6: A Free Multi-Chapter Tutorial | Catchpoint, https://www.catchpoint.com/benefits-of-ipv6
113. IPv6 Address Representation and Address Types - Cisco Press, https://www.ciscopress.com/articles/article.asp?p=2803866
114. Intro to IPv6 Addressing - Wireshark SharkFest, https://sharkfest.wireshark.org/retrospective/sfus/presentations13//PA-02_Introduction-to-IPv6-Addressing_Nalini-Elkins.pdf
115. 5- IPv6 Address Types - Googleapis.com, https://academy-training-wiki-media.storage.googleapis.com/_media/ipv620200228-ph/5-_ipv6_address_types.pdf
116. RFC 4193 - Unique Local IPv6 Unicast Addresses - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc4193
117. IPv6 Address Types | NetworkAcademy.io - Learn Networking for Free, https://www.networkacademy.io/ccna/ipv6/ipv6-address-types
118. IPv6 Address Types - NetworkLessons.com, https://networklessons.com/ipv6/ipv6-address-types
119. IPv6 Addressing | OpenThread, https://openthread.io/guides/thread-primer/ipv6-addressing
120. Back to Basics – The IPv6 Address Types - Infoblox Blog, https://blogs.infoblox.com/ipv6-coe/back-to-basics-the-ipv6-address-types/
121. Understanding IPv6 addressing on AWS and designing a scalable addressing plan, https://aws.amazon.com/blogs/networking-and-content-delivery/understanding-ipv6-addressing-on-aws-and-designing-a-scalable-addressing-plan/
122. Unicast Addresses > IPv6 Address Representation and Address Types | Cisco Press, https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4
123. 3 Ways to Ruin Your Future Network with IPv6 Unique Local Addresses (Part 1 of 2), https://blogs.infoblox.com/ipv6-coe/3-ways-to-ruin-your-future-network-with-ipv6-unique-local/
124. Unique local address - Wikipedia, https://en.wikipedia.org/wiki/Unique_local_address
125. Manual:IPv6/Address - MikroTik Wiki, https://wiki.mikrotik.com/Manual:IPv6/Address
126. IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io, https://www.networkacademy.io/ccna/ipv6/stateless-address-autoconfiguration-slaac
127. IPv6 Neighbor Discovery | Junos OS - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/neighbor-discovery/topics/topic-map/ipv6-neighbor-discovery.html
128. Introducing IPv6: Neighbor Discovery & SLAAC - Chris Grundemann,

https://chrisgrundemann.com/index.php/2012/introducing-ipv6-neighbor-discovery-slaac/
129. IPv6 Neighbor Discovery and Stateless Address Autoconfiguration - GeeksforGeeks, https://www.geeksforgeeks.org/ipv6-neighbor-discovery-and-stateless-address-autoconfiguration/
130. RFC 5156: Special-Use IPv6 Addresses, https://www.rfc-editor.org/rfc/rfc5156.html
131. IPv6 cheat-sheet, part 3: IPv6 multicast - BlueCat Networks, https://www.menandmice.com/blog/ipv6-reference-multicast
132. How EUI-64 Works in IPv6 - Catchpoint, https://www.catchpoint.com/benefits-of-ipv6/eui-64
133. Summary of Stateless Address Auto-Configuration for Ipv6 - Atlantis Press, https://www.atlantis-press.com/php/download_paper.php?id=25870957
134. SLAAC : What's wrong with this generated IPv6 address?, https://networkengineering.stackexchange.com/questions/41105/slaac-whats-wrong-with-this-generated-ipv6-address
135. The Good, the Bad, the IPv6 | IT Security Office, https://security.vt.edu/docs/The_Good_the_Bad_the_IPv6.pdf
136. RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6, https://datatracker.ietf.org/doc/html/rfc4941
137. Privacy Extensions for IPv6 SLAAC - Internet Society, https://www.internetsociety.org/resources/deploy360/2014/privacy-extensions-for-ipv6-slaac/
138. RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6, https://datatracker.ietf.org/doc/rfc4941/
139. IPv6 Addresses, Security and Privacy - RIPE Labs, https://labs.ripe.net/author/johanna_ullrich/ipv6-addresses-security-and-privacy/
140. Back to the Future: Revisiting IPv6 Privacy Extensions - USENIX, https://www.usenix.org/system/files/login/articles/105438-Barrera.pdf
141. RFC 4862 - IPv6 Stateless Address Autoconfiguration - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc4862
142. IPv6 Privacy Extensions (RFC 4862) are disabled by default - Fedora Discussion, https://discussion.fedoraproject.org/t/ipv6-privacy-extensions-rfc-4862-are-disabled-by-default/117274
143. How is a link-local address created when duplicate address detection fails in IPv6 Stateless Address Autoconfiguration (SLAAC)? - Super User, https://superuser.com/questions/1532974/how-is-a-link-local-address-created-when-duplicate-address-detection-fails-in-ip
144. IPv6 Duplicate Address Detection - The Internet Protocol Blog - WordPress.com, https://theinternetprotocolblog.wordpress.com/2021/02/21/ipv6-duplicate-address-detection/
145. IPv6 and Internet Privacy - Infoblox Blog,

https://blogs.infoblox.com/ipv6-coe/ipv6-and-internet-privacy/
146. IPv6 Privacy Addresses Provide Protection Against Surveillance And Tracking, https://www.internetsociety.org/blog/2014/12/ipv6-privacy-addresses-provide-protection-against-surveillance-and-tracking/
147. Privacy Extensions for Stateless Address Autoconfiguration in IPv6 - ResearchGate, https://www.researchgate.net/publication/242627069_Privacy_Extensions_for_Stateless_Address_Autoconfiguration_in_IPv6
148. RFC 8981: Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6, https://www.rfc-editor.org/rfc/rfc8981.html
149. RFC 4862: IPv6 Stateless Address Autoconfiguration, https://www.rfc-editor.org/rfc/rfc4862.html
150. Secure IPv6 Neighbor Discovery | Junos OS - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/neighbor-discovery/topics/topic-map/ipv6-secure-neighbor.html
151. An Analysis of Neighbor Discovery Protocol Attacks - MDPI, https://www.mdpi.com/2073-431X/12/6/125
152. DHCP vs Static IP: What's the Difference? - FS.com, https://www.fs.com/blog/dhcp-vs-static-ip-which-one-is-better-1155.html
153. Static vs. Dynamic IP Address: A Comprehensive Guide - IPXO, https://www.ipxo.com/blog/static-vs-dynamic-ip-address/
154. The Difference Between Dynamic and Static IP Address Assignments - LARUS, https://larus.net/blog/difference-between-dynamic-static-ip-address-assignments/
155. DHCP vs. static allocation: Understanding the difference | ManageEngine OpUtils, https://www.manageengine.com/products/oputils/tech-topics/dhcp-vs-static.html
156. Static vs. Dynamic IP Addresses: What's the Difference? | Security.org, https://www.security.org/vpn/static-vs-dynamic-ip-address/
157. Dynamic Host Configuration Protocol - Wikipedia, https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
158. DHCP DORA Process Explained: Discover How It Works - SynchroNet, https://synchronet.net/dhcp-dora/
159. DHCP (Dynamic Host Configuration Protocol) Basics - Learn Microsoft, https://learn.microsoft.com/en-us/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics
160. How DORA Works? | GeeksforGeeks, https://www.geeksforgeeks.org/how-dora-works/
161. SLAAC Vs DHCPv6: A Comprehensive Analysis - Tolu Michael, https://tolumichael.com/slaac-vs-dhcpv6-a-comprehensive-analysis/
162. dhcpv6 - stateful VS stateless, what is difference between it?, https://networkengineering.stackexchange.com/questions/47829/dhcpv6-stateful-vs-stateless-what-is-difference-between-it
163. DHCPv6Auth: a mechanism to improve DHCPv6 authentication and privacy -

Indian Academy of Sciences, https://www.ias.ac.in/public/Volumes/sadh/045/00/0033.pdf
164. DHCPv6 - Wikipedia, https://en.wikipedia.org/wiki/DHCPv6
165. RFC 8415 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6) - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc8415
166. DHCP and DHCPv6: Options Differences - Hogg Networking, https://hoggnet.com/blogs/news/dhcp-and-dhcpv6-options-differences
167. Information on RFC 8415 - » RFC Editor, https://www.rfc-editor.org/info/rfc8415
168. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) - IETF Datatracker, https://datatracker.ietf.org/doc/html/draft-ietf-dhc-rfc8415bis-05
169. The Pros and Cons of SLAAC in Modern Networks | NSC - NetSecCloud, https://netseccloud.com/the-pros-and-cons-of-slaac-in-modern-networks
170. Exploring DHCP DORA Process in Network Configurations | NSC - NetSecCloud, https://netseccloud.com/dhcp-dora-process
171. DHCP and DHCPv6: Commonalities and Differences - Infoblox Blog, https://blogs.infoblox.com/ipv6-coe/dhcp-and-dhcpv6-commonalities-and-differences/
172. Why are DHCP request and acknowledgment messages broadcasted and not unicasted?, https://serverfault.com/questions/714930/why-are-dhcp-request-and-acknowledgment-messages-broadcasted-and-not-unicasted
173. RFC 4861: Neighbor Discovery for IP version 6 (IPv6), https://www.rfc-editor.org/rfc/rfc4861.html
174. Junos® OS IPv6 Neighbor Discovery User Guide - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/neighbor-discovery/neighbor-discovery.pdf
175. Why You Must Use ICMPv6 Router Advertisements (RAs) - Infoblox Blog, https://blogs.infoblox.com/ipv6-coe/why-you-must-use-icmpv6-router-advertisements-ras/
176. Understanding IPv6 Router Advertisement Guard | Junos OS - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-ra-guard.html
177. Layer 2 Attacks and Mitigation Techniques: DHCP Snooping for Network Protection - Adex, https://adex.ltd/layer-2-attacks-vulnerabilities-and-mitigation-with-dhcp-snooping
178. Attacks and Mitigation Techniques, https://cs-coe.iisc.ac.in/wp-content/uploads/2020/08/Attacks-and-Mitigation-Techniques.pdf
179. Understanding and Preventing DHCP Spoofing Attacks - Pentera, https://pentera.io/blog/dhcp-spoofing-101/
180. DHCP SNOOPING ATTACKS PREVENTION METHOD WITH LAB, https://linuxtiwary.com/2015/12/01/dhcp-snooping-attacks-prevention-method-w

ith-lab/
181. DHCP exploitation guide - WhiteWinterWolf.com, https://www.whitewinterwolf.com/posts/2017/10/30/dhcp-exploitation-guide/
182. 10 Critical Network Pentest Findings IT Teams Overlook - The Hacker News, https://thehackernews.com/2025/03/10-critical-network-pentest-findings-it.html
183. Understanding DHCP Snooping: Enhancing Network Security - Emplus Technologies, Inc., https://www.emplustech.com/blog_post_20.html
184. RFC 6105 - IPv6 Router Advertisement Guard - IETF Datatracker, https://datatracker.ietf.org/doc/html/rfc6105
185. MITM-cheatsheet/README.md at master - GitHub, https://github.com/frostbits-security/MITM-cheatsheet/blob/master/README.md
186. Holding IPv6 Neighbor Discovery to a Higher Standard of Security - Infoblox Blog, https://blogs.infoblox.com/ipv6-coe/holding-ipv6-neighbor-discovery-to-a-higher-standard-of-security/
187. Review of Security Vulnerabilities in the IPv6 Neighbor Discovery Protocol - ResearchGate, https://www.researchgate.net/publication/297313818_Review_of_Security_Vulnerabilities_in_the_IPv6_Neighbor_Discovery_Protocol
188. RFC 7113 - Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard), https://datatracker.ietf.org/doc/rfc7113/
189. The IPv6 Router Advertisement Guard - Barracuda Campus, https://campus.barracuda.com/product/networkaccessclient/doc/168101485/the-ipv6-router-advertisement-guard/
190. Cut Me Some SLAAC, Or Why You Need RA Guard | The Networking Nerd, https://networkingnerd.net/2011/05/09/cut-me-some-slaac-or-why-you-need-ra-guard/
191. IPv6 Security in the Local Area with First - Cisco Live, https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2023/pdf/BRKENT-3002.pdf
192. IPv6 Neighbor Discovery Inspection | Junos OS - Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-nd-inspection.html
193. What is ARP Spoofing | ARP Cache Poisoning Attack Explained - Imperva, https://www.imperva.com/learn/application-security/arp-spoofing/
194. An Analysis of Neighbor Discovery Protocol Attacks - ResearchGate, https://www.researchgate.net/publication/371694125_An_Analysis_of_Neighbor_Discovery_Protocol_Attacks
195. IPv6 Neighbor Discovery: Keep Calm and IPv6 On! | Zivaro, https://zivaro.com/ipv6-neighbor-discovery-keep-calm-and-ipv6-on/
196. Securing ARP/NDP From the Ground Up - Patrick McDaniel, https://patrickmcdaniel.org/pubs/tkc17.pdf
197. SLAAC Attack Detection Mechanism - DergiPark, https://dergipark.org.tr/en/download/article-file/2160169
198. Operational Security Considerations for IPv6 Networks,

https://www.potaroo.net/ietf/all-ids/draft-ietf-opsec-v6-16.html
199. NAT vs PAT Networking: Unraveling the Differences - Wix.com, https://seoaryan97.wixsite.com/pynetlabs/post/nat-vs-pat-networking-unraveling-the-differences
200. Difference Between Network Address Translation (NAT) and Port Address Translation (PAT) | GeeksforGeeks, https://www.geeksforgeeks.org/difference-between-network-address-translation-nat-and-port-address-translation-pat/
201. NAT and PAT - What's the Difference? - Boson Blog, https://blog.boson.com/bid/53313/nat-and-pat-what-s-the-difference
202. Network Address Translation Definition | How NAT Works - CompTIA, https://www.comptia.org/content/guides/what-is-network-address-translation
203. NAT vs PAT - Two Sides of a Coin | Orhan Ergun, https://orhanergun.net/nat-vs-pat
204. CS402: Network Address Translation (NAT) - Saylor Academy, https://learn.saylor.org/mod/page/view.php?id=72231
205. What is Network Address Translation? - VMware, https://www.vmware.com/topics/network-address-translation
206. Network address translation - Wikipedia, https://en.wikipedia.org/wiki/Network_address_translation
207. NAT - Network Address Translation - NETWORX SECURITY, https://www.networxsecurity.org/members-area/glossary/n/nat.html
208. Network Address Translation (NAT) - CCNA Practice Tests - learncisco.net, https://www.learncisco.net/courses/cisco-ccna/nat-network-address-translation/network-address-translation.html
209. 7. Network Address Translation - Nokia Documentation Center, https://infocenter.nokia.com/public/7750SR140R4/topic/com.sr.msisa/html/nat.html
210. About NAT and Azure VPN Gateway - Learn Microsoft, https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-overview
211. Chapter 6. Network Address Translation - SmallWall, https://smallwall.org/docs/handbook/nat.html
212. NAT vs PAT? : r/networking - Reddit, https://www.reddit.com/r/networking/comments/87fof0/nat_vs_pat/
213. Introduction to NAT and PAT - NetworkLessons.com, https://networklessons.com/cisco/ccnp-encor-350-401/introduction-to-nat-and-pat
214. NAT Overload (PAT) | NetworkAcademy.io - Learn Networking for Free, https://www.networkacademy.io/ccna/network-services/nat-overload-pat
215. The Difference Between Pivoting vs. Lateral Movement - TrueFort, https://truefort.com/pivoting-vs-lateral-movement/
216. Tunneling, Pivoting, and Web Application Penetration Testing - GIAC Certifications, https://www.giac.org/paper/gwapt/4686/tunneling-pivoting-web-application-penetration-testing/120229

217. How to Perform Internal Network Scanning with Pentest-Tools.com, https://pentest-tools.com/blog/internal-network-scanning
218. Pivoting in Metasploit, https://docs.metasploit.com/docs/using-metasploit/intermediate/pivoting-in-metasploit.html
219. PTES Technical Guidelines - The Penetration Testing Execution Standard, http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
220. Your goal is to access an internal webserver (10.0.4.3), https://www.cs.utep.edu/CFIA/files/outreach/PivotingExploitation/PivotingExploitation_Exercise.pdf
221. Fun With SSH Reverse Shells in 2021 - Pivot Point Security, https://www.pivotpointsecurity.com/fun-with-ssh-reverse-shells/
222. The Basics of Hacking and Penetration Testing - GitHub Pages, https://wqreytuk.github.io/Patrick+Engebretson+The+Basics+of+Hacking+and+Penetration+Testing,+Second+Edition+%282013%29.pdf
223. NAT Traversal Techniques for Peer-to-Peer Connections: A Comprehensive Guide, https://www.checkmynat.com/posts/nat-traversal-techniques-for-peer-to-peer-connections/
224. Metasploitable 2 Exploitability Guide - Docs @ Rapid7, https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
225. ICE TURN and STUN for NAT Traversal Explained for CLCEI Exam - Cisco Learning Network, https://learningnetwork.cisco.com/s/question/0D56e0000CgaKXvCQM/ice-turn-and-stun-for-nat-traversal-explained-for-clcei-exam
226. NAT, STUN, TURN, and ICE | Thirdlane.com, https://www.thirdlane.com/blog/nat-stun-turn-and-ice
227. STUN, TURN, and ICE NAT Traversal Protocols - AnyConnect, https://anyconnect.com/stun-turn-ice/
228. NAT Traversal using STUN TURN and ICE, https://aptsoftware.com/nat-traversal-using-stun-turn-and-ice/
229. Demystifying NAT Traversal with STUN TURN and ICE - Cisco Community, https://community.cisco.com/t5/collaboration-knowledge-base/demystifying-nat-traversal-with-stun-turn-and-ice/ta-p/4766853
230. NAT Traversal Techniques For Programming-TechnoGumbo, https://www.technogumbo.com/2010/01/NAT-Traversal-Techniques-For-Programming/
231. How NAT traversal works - Tailscale, https://tailscale.com/blog/how-nat-traversal-works
232. Implement ICE / TURN / STUN for forwarding packets through NAT · Issue #434 · godotengine/godot-proposals - GitHub, https://github.com/godotengine/godot-proposals/issues/434
233. Tailscale for Offensive Security - 0xd33r.com, https://0xd33r.com/article/2024/tailscale-for-offsec
234. Discovering network hosts with 'TCP SYN' and 'TCP ACK' ping scans in

Nmap[Tutorial], https://www.packtpub.com/en-us/learning/how-to-tutorials/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial
235. Host Discovery Techniques in Ethical Hacking | ARP, ICMP, TCP, UDP, and IP Protocol Scans Explained with Nmap Commands and Real-Time Use Cases - Web Asha Technologies, https://www.webasha.com/blog/host-discovery-techniques-in-ethical-hacking-arp-icmp-tcp-udp-and-ip-protocol-scans-explained-with-nmap-commands-and-real-time-use-cases
236. Nmap Host Discovery: The Ultimate Guide - Device42, https://www.device42.com/blog/2023/03/29/nmap-host-discovery-the-ultimate-guide/
237. Chapter 3. Host Discovery ("Ping Scanning") - Nmap, https://nmap.org/book/host-discovery.html
238. Host Discovery | Nmap Network Scanning, https://nmap.org/book/man-host-discovery.html
239. Nmap Cheat Sheet: Commands, Flags, Switches & Examples (2024) - HighOn.Coffee, https://highon.coffee/blog/nmap-cheat-sheet/
240. Host Discovery Techniques | Nmap Network Scanning, https://nmap.org/book/host-discovery-techniques.html
241. Host Discovery in Nmap Network Scanning | GeeksforGeeks, https://www.geeksforgeeks.org/host-discovery-in-nmap-network-scanning/
242. nmap - How to find live hosts on my network? - Information Security Stack Exchange, https://security.stackexchange.com/questions/36198/how-to-find-live-hosts-on-my-network
243. Discovery Scan | Metasploit Documentation - Docs @ Rapid7, https://docs.rapid7.com/metasploit/discovery-scan/
244. Subverting Intrusion Detection Systems | Nmap Network Scanning, https://nmap.org/book/subvert-ids.html
245. ICMP Protocol (Internet Control Message Protocol): A Guide - Okta, https://www.okta.com/identity-101/icmp/
246. Ping, traceroute, and netstat: The network troubleshooting trifecta - Red Hat, https://www.redhat.com/en/blog/ping-traceroute-netstat
247. What is ICMP? - ICMP Protocol Explained - AWS, https://aws.amazon.com/what-is/icmp/
248. ICMP (Internet Control Message Protocol) - NetworkLessons.com, https://networklessons.com/cisco/ccie-routing-switching-written/icmp-internet-control-message-protocol
249. Internet Control Message Protocol (ICMP) | GeeksforGeeks, https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/
250. Internet Control Message Protocol - Wikipedia, https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
251. Basics of ICMP: What You Need to Know - Orhan Ergun, https://orhanergun.net/icmp-guide

252. Nmap para pentesters: de cero a pro | Miguel Ángel Villalobos García, https://www.linkedin.com/posts/m7villalobos_nmap-para-pentesters-de-cero-a-pro-activity-7319330458247356417-DptO