Fundamentos de Redes

1. Introducción: La Red como Ecosistema Conectado

1.1. Propósito y Alcance del Documento

El presente documento ha sido redactado con la finalidad de establecer una base sólida y bien estructurada en los fundamentos de las redes de computadoras. Se reconoce que, para un aprendizaje efectivo, es esencial partir de los conceptos más elementales y avanzar de manera lógica, evitando la confusión que surge al entrelazar principios básicos con aplicaciones prácticas específicas. Este informe se centrará, por lo tanto, en desmitificar los componentes y protocolos fundamentales de las redes, con una atención particular al direccionamiento IP y la subnetización. Se espera que este material sirva como un cimiento robusto para futuras exploraciones en temas de mayor complejidad, sentando las bases necesarias para una comprensión profunda del campo.

1.2. ¿Qué es una Red de Computadoras? (Redefinición)

Una red de computadoras es, en su esencia, un conjunto de dispositivos de computación interconectados, como ordenadores, servidores, impresoras y dispositivos móviles, que pueden intercambiar datos y compartir recursos entre sí.[1] Esta interconexión no es arbitraria; se rige por un conjunto de reglas y directrices, conocidos como protocolos de comunicación, que dictan cómo se transmite la información a través de los diversos medios físicos o inalámbricos.[1]
Para que una red funcione, se requiere de varios componentes clave. Entre ellos se encuentran los nodos (los dispositivos finales que se conectan a la red, como un PC o un servidor), los medios de transmisión (los canales físicos por donde viajan los datos, ya sean cables de fibra óptica, coaxiales, pares trenzados o medios inalámbricos como ondas de radio) y los dispositivos de interconexión (hardware especializado como *hubs*, *switches* y *routers*) que gestionan el flujo de información entre los nodos.[2]

1.3. Clasificación de Redes por Alcance Geográfico

La forma más común de clasificar las redes es por su alcance geográfico. Aunque existen otras taxonomías, esta es la más útil para contextualizar la conectividad en la mayoría de los escenarios.

- **Red de Área Local (LAN):** Una LAN es una red que se limita a un área geográfica pequeña y delimitada, como una casa, una oficina o un campus escolar.[3] Su principal característica es la alta velocidad de transmisión de datos y la baja latencia, lo que la hace ideal para compartir recursos cercanos, como impresoras o archivos.[4] Las LANs suelen ser de propiedad y gestión privada por la entidad que las opera.[6]
- **Red de Área Amplia (WAN):** Una WAN conecta múltiples LANs que están geográficamente separadas.[3] Por ejemplo, la red de una empresa que tiene sedes en diferentes ciudades o países se considera una WAN. La conectividad a larga distancia en una WAN se logra a menudo a través de infraestructuras de red de terceros, como líneas alquiladas a un proveedor de servicios de telecomunicaciones.[3] Las WANs están diseñadas para ofrecer conectividad segura y confiable a través de distancias significativas.[5]
- **Internet: La Red de Redes:** Internet es, en esencia, la WAN más grande del mundo. Es una vasta colección de redes públicas y privadas interconectadas globalmente que permite la comunicación entre dispositivos de cualquier lugar.[3] Cuando un dispositivo en una LAN doméstica se conecta a un servidor en otro continente, el tráfico viaja a través del
  router local, pasa por la WAN del proveedor de servicios de Internet (ISP) y, finalmente, se enruta a través de la red global de Internet hasta su destino.[4]

1.4. Arquitecturas de Red (Modelo Lógico)

Más allá de su tamaño, las redes también se definen por su arquitectura lógica, que determina cómo los dispositivos se comunican y comparten recursos.

- **Arquitectura Cliente-Servidor:** En este modelo, los dispositivos se dividen en dos categorías: servidores y clientes.[7] Los servidores son nodos que proporcionan recursos, como datos, aplicaciones o capacidad de procesamiento. Los clientes son dispositivos que solicitan y utilizan estos recursos. Esta arquitectura es dominante en entornos empresariales, donde los clientes acceden a datos y aplicaciones centralizadas en servidores.[2]
- **Arquitectura Punto a Punto (P2P):** A diferencia del modelo cliente-servidor, en una arquitectura P2P, los nodos tienen los mismos privilegios y pueden actuar tanto como clientes como servidores.[6] No existe un servidor central. Cada dispositivo puede compartir sus propios recursos, como archivos o potencia de procesamiento, con otros dispositivos de la red. Este modelo es común en redes domésticas o en aplicaciones que distribuyen la carga de trabajo entre múltiples ordenadores.[6]

La evolución de las redes, particularmente con la aparición de la computación en la nube, no

es solo un avance tecnológico, sino un cambio en la arquitectura. Las menciones a conceptos como VPC (Nube Privada Virtual) en el contexto de AWS y SD-WAN (WAN Definida por Software) revelan que la interconexión ya no se limita a la conexión de hardware físico. Estas tecnologías crean capas lógicas y virtuales que permiten construir redes sobre redes preexistentes. Por ejemplo, una SD-WAN utiliza software para gestionar una WAN, y una VPN crea una red privada virtual sobre la red pública de Internet.[3] Esta transición subraya que la comprensión de los fundamentos de redes es el primer paso para dominar la complejidad de las infraestructuras modernas que son inherentemente flexibles, escalables y, a menudo, virtuales. El usuario, al buscar una explicación de redes y AWS, está intuyendo esta evolución hacia un ecosistema digital más abstracto y configurable.

2. Modelos de Comunicación: El Lenguaje de las Redes (OSI y TCP/IP)

2.1. El Modelo de Referencia OSI: Un Marco Conceptual

El modelo de interconexión de sistemas abiertos (OSI) es un marco conceptual creado por la Organización Internacional de Normalización (ISO) que estandariza las funciones de red en siete capas jerárquicas.[4] Su principal valor reside en ser una herramienta pedagógica que permite visualizar y entender cómo los datos se mueven a través de una red, desde la aplicación del usuario hasta el medio físico.[9] Cada capa realiza tareas específicas y se comunica con las capas adyacentes, tanto la que está "encima" como la que está "debajo".[10]

- **Capa 1 - Física:** Esta es la capa más baja y se encarga de la transmisión de bits puros a través de un medio físico, como cables de cobre, fibra óptica o señales de radio.[9] Se ocupa de aspectos como el voltaje de la señal, la sincronización de los bits y las especificaciones de los conectores. Dispositivos como los *hubs* y los repetidores operan en esta capa, simplemente amplificando o repitiendo la señal eléctrica.[4]
- **Capa 2 - Enlace de datos:** La capa de enlace de datos organiza los bits de la capa física en unidades lógicas llamadas tramas.[4] Su función principal es gestionar la conectividad entre dos nodos directamente conectados y asegurar la entrega sin errores de la información a través del medio físico. Utiliza direcciones de control de acceso al medio (MAC) para identificar de forma única los dispositivos dentro de un mismo segmento de red.[4] Los *switches* son los dispositivos clave en esta capa, ya que reenvían las tramas basándose en las direcciones MAC de destino.[4]
- **Capa 3 - Red:** Esta capa es fundamental para el enrutamiento. Su tarea es mover paquetes de datos entre redes diferentes, utilizando direcciones lógicas como las

direcciones IP.[4] Un
router, el dispositivo principal de esta capa, examina la dirección IP de destino de un paquete y determina la mejor ruta para enviarlo a su próxima parada en el camino hacia su destino final, permitiendo que un equipo en una LAN se comunique con otro en una red externa como Internet.[4]

- **Capa 4 - Transporte:** La capa de transporte se encarga de la comunicación de extremo a extremo, dividiendo los datos en unidades más pequeñas llamadas segmentos.[10] Esta capa es donde entran en juego los protocolos clave de la red: el **Protocolo de Control de Transmisión (TCP)** y el **Protocolo de Datagramas de Usuario (UDP)**.[4] Se discute su función en detalle en la sección 5.1.
- **Capa 5 - Sesión:** Esta capa establece, administra y finaliza las sesiones o diálogos entre aplicaciones en dispositivos diferentes.[4] La sesión es única para el usuario y garantiza que la transferencia de datos se mantenga durante el tiempo necesario y que se pueda reanudar si se interrumpe.[10]
- **Capa 6 - Presentación:** La capa de presentación se ocupa del formato y la sintaxis de los datos. Se asegura de que la información sea legible para la capa de aplicación de destino. Esto incluye la codificación y decodificación, la compresión y descompresión, y el cifrado y descifrado de los datos.[4]
- **Capa 7 - Aplicación:** Esta es la capa superior, la más cercana al usuario. Proporciona la interfaz para que las aplicaciones de *software* accedan a la red. Los protocolos de aplicación, como HTTP (para navegadores web) o SMTP (para correo electrónico), operan en esta capa.[4]

2.2. El Modelo de Protocolos TCP/IP: La Práctica de Internet

Aunque el modelo OSI es una excelente herramienta conceptual, el modelo que realmente rige la operación de Internet es el modelo de protocolos TCP/IP.[11] Este modelo, más simple y funcional, consolida las siete capas de OSI en cuatro, reflejando de manera más precisa cómo los protocolos se implementan en la práctica.

- **Capa de Acceso a la Red:** Combina las capas Física y de Enlace de datos de OSI.
- **Capa de Internet:** Equivale a la capa de Red de OSI. Es responsable del direccionamiento lógico y el enrutamiento de paquetes, usando principalmente el protocolo IP.[6]
- **Capa de Transporte:** Coincide con la capa de Transporte de OSI, gestionando la entrega de datos de extremo a extremo a través de protocolos como TCP y UDP.[8]
- **Capa de Aplicación:** Combina las capas de Sesión, Presentación y Aplicación de OSI. Incluye los protocolos con los que interactúan directamente las aplicaciones de usuario.[8]

2.3. Comparativa Detallada y el Proceso de Encapsulación

La relación entre los modelos OSI y TCP/IP no es de sustitución, sino de complemento. Mientras que el modelo OSI se utiliza a menudo con fines educativos para proporcionar una perspectiva holística de la red, el modelo TCP/IP es el estándar de facto utilizado en la práctica.[9] Curiosamente, la funcionalidad de protocolos clave de TCP/IP, como IP y TCP, se describe casi de forma universal en términos de las capas 3 (Red) y 4 (Transporte) del modelo OSI.[8] Esto demuestra que el marco conceptual de OSI no es solo una teoría, sino que ha influido de forma fundamental en la arquitectura real de los protocolos de red, proporcionando un lenguaje común que los desarrolladores y arquitectos han adoptado a lo largo de los años.

Para entender cómo funcionan estos modelos, es crucial comprender el proceso de **encapsulación**. Cuando los datos se preparan para ser enviados, pasan por cada capa, de arriba hacia abajo. En la capa de aplicación, los datos se empaquetan y se les añade una cabecera. A medida que este paquete desciende por la pila, cada capa añade su propia información de cabecera, encapsulando el paquete de la capa superior dentro de su propia unidad de datos. Por ejemplo, la capa de transporte añade una cabecera para formar un segmento, la capa de red añade otra para formar un paquete, y la capa de enlace añade la última para formar una trama.[4] Este proceso es análogo a colocar una carta dentro de un sobre, luego ese sobre dentro de otro, y así sucesivamente, con cada sobre añadiendo la información de enrutamiento necesaria para la siguiente etapa del viaje. En el destino, el proceso se invierte (desencapsulación), con cada capa retirando su cabecera y pasando el paquete a la capa superior hasta que los datos originales llegan a la aplicación final.

Tabla 1: Comparación de los Modelos OSI y TCP/IP

Capa del modelo OSI	Nombre de la Capa	Función Principal	Capa del modelo TCP/IP
Capa 7	Aplicación	Interfaz con la aplicación; protocolos de usuario (HTTP, SSH) [4]	
Capa 6	Presentación	Formato, cifrado, compresión de datos [10]	**Capa de Aplicación** (Capa 4)
Capa 5	Sesión	Inicia, administra y finaliza sesiones [10]	
Capa 4	Transporte	Segmentación de datos; entrega confiable (TCP) o rápida (UDP) [9]	**Capa de Transporte** (Capa 3)
Capa 3	Red	Direccionamiento lógico y enrutamiento	**Capa de Internet** (Capa 2)

		de paquetes (IP) [4]	
Capa 2	Enlace de datos	Formato de tramas y direcciones MAC [9]	
Capa 1	Física	Transmisión de bits a través de medios físicos [9]	**Capa de Acceso a la Red** (Capa 1)

3. Direccionamiento: El DNI de los Dispositivos

3.1. Direcciones IPv4: La Anatomía Digital

Una dirección IP es un identificador numérico único asignado a un dispositivo en una red.[4] En la versión 4 del Protocolo de Internet (IPv4), esta dirección se compone de 32 bits, que se representan típicamente como cuatro números decimales (octetos) separados por puntos, con cada número en el rango de 0 a 255.[4] Por ejemplo,
192.168.1.100.
Una dirección IPv4 se divide en dos partes principales: la **porción de red** y la **porción de host**.[4] La porción de red identifica la red específica a la que pertenece el dispositivo, mientras que la porción de host identifica al dispositivo individual dentro de esa red.[13] El número de bits asignados a cada parte no es fijo y depende de la estructura de la red.[14]

3.2. La Máscara de Subred: La Frontera Lógica

La máscara de subred es una combinación de 32 bits que funciona como un filtro para indicar a los dispositivos cuál es la porción de red y cuál es la de host de una dirección IP.[15] En su representación binaria, los bits de la máscara que están en
1 corresponden a la parte de red de la dirección IP, y los bits que están en 0 corresponden a la parte de host.[16]
Para determinar la dirección de red de cualquier IP, se realiza una operación lógica **AND** bit a bit entre la dirección IP del dispositivo y su máscara de subred.[15] El resultado de esta operación es la dirección de red, que es una dirección con la porción de host en ceros, y es la misma para todos los dispositivos en el mismo segmento de red.
Por ejemplo, si la dirección IP es 192.168.1.100 y la máscara es 255.255.255.0, al convertirlos a binario y aplicar la operación AND, el resultado será la dirección de red 192.168.1.0.

- 192.168.1.100 en binario es: 11000000.10101000.00000001.01100100
- 255.255.255.0 en binario es: 11111111.11111111.11111111.00000000
- Resultado (AND lógico): 11000000.10101000.00000001.00000000

- Lo cual se traduce a: 192.168.1.0 (Dirección de Red)

La notación más común en la actualidad es la notación **CIDR** (*Classless Inter-Domain Routing*), que simplifica la máscara de subred a un simple número precedido por una barra inclinada (/). Este número representa la cantidad de bits que forman la porción de red.[18] Por ejemplo, la máscara
255.255.255.0 tiene 24 bits a 1 en su forma binaria, por lo que se representa como /24.

3.3. Puerta de Enlace Predeterminada (Gateway): El Camino de Salida

La puerta de enlace predeterminada o *gateway* es la dirección IP del dispositivo (generalmente un *router*) que sirve como punto de salida de la red local para conectarse a otras redes, como Internet.[15] Cuando un dispositivo en una red necesita enviar un paquete a un destino fuera de su propia red, envía el paquete al
gateway. Es responsabilidad del *router* enrutar el paquete a su destino final.[17] La dirección IP del
gateway debe estar obligatoriamente dentro de la misma subred que los dispositivos a los que sirve.[15]

3.4. Direcciones IP Públicas vs. Privadas

Las direcciones IP se dividen en dos categorías, según su alcance en la red global:

- **Direcciones IP Públicas:** Son direcciones únicas a nivel mundial que son enrutables en Internet. Un dispositivo que posee una IP pública puede ser accedido directamente desde cualquier lugar de Internet.[4] Son asignadas por la Internet Assigned Numbers Authority (IANA) y los proveedores de servicios de Internet (ISP) para garantizar su unicidad.
- **Direcciones IP Privadas:** Estas direcciones están reservadas para su uso exclusivo dentro de redes locales y no son enrutables en Internet. Cualquier paquete con una IP privada como destino será descartado por los *routers* de Internet.[4] Esta práctica permite que miles de redes privadas en todo el mundo utilicen los mismos rangos de direcciones sin conflicto, al tiempo que preserva el espacio limitado de direcciones IPv4 públicas. Los rangos de IP privadas están definidos por el RFC 1918 [4]:

Tabla 2: Rangos de Direcciones IP Privadas (RFC 1918)

Clase	Rango de Direcciones IPv4	Prefijo CIDR
A	10.0.0.0 a 10.255.255.255	10.0.0.0/8
B	172.16.0.0 a 172.31.255.255	172.16.0.0/12
C	192.168.0.0 a 192.168.255.255	192.168.0.0/16

3.5. El Concepto Histórico de Clases de Red (Clase A, B y C)

El sistema de direccionamiento IPv4 se diseñó originalmente en un modelo de clases, donde la clase de una dirección estaba determinada por el valor de su primer octeto.[14] Cada clase venía con una máscara de subred por defecto predefinida, lo que fijaba el tamaño de la porción de red y host.

- **Clase A:** Rango de 1.0.0.0 a 126.255.255.255. Su máscara por defecto es 255.0.0.0 (/8). Estas redes eran para organizaciones muy grandes, con la capacidad de albergar hasta 16.777.214 hosts por red, lo que representaba un enorme desperdicio de direcciones.[21]
- **Clase B:** Rango de 128.0.0.0 a 191.255.255.255. Su máscara por defecto es 255.255.0.0 (/16). Ofrecía hasta 65.534 hosts por red y estaba destinada a redes de tamaño mediano.[21]
- **Clase C:** Rango de 192.0.0.0 a 223.255.255.255. Su máscara por defecto es 255.255.255.0 (/24). Con solo 254 hosts disponibles por red, era adecuada para redes pequeñas a medianas.[21]

El modelo de clases se abandonó en gran medida a medida que Internet crecía. La rigidez de las máscaras por defecto condujo a un uso ineficiente del espacio de direcciones.[19] Por ejemplo, una organización que necesitaba 500 hosts no cabía en una red de Clase C, pero se veía obligada a tomar una Clase B, desperdiciando miles de direcciones.[17] Esta ineficiencia en la asignación de recursos condujo a la escasez de direcciones IPv4. La respuesta directa a este problema fue el desarrollo de la notación CIDR y la técnica de subnetting, que permitieron una distribución de direcciones más flexible y adaptada a las necesidades reales de cada red.[18] El estudio de las clases de red no es solo un dato histórico; es la clave para entender por qué la subnetización es una práctica tan crítica en la actualidad.

Tabla 3: Clases de Red IPv4 (Histórico)

Clase	Rango de Primer Octeto	Máscara por Defecto	Prefijo	Hosts por Red
A	1-126	255.0.0.0	/8	224−2
B	128-191	255.255.0.0	/16	216−2
C	192-223	255.255.255.0	/24	28−2

4. Subnetting: El Arte de Segmentar Redes

4.1. Propósito y Beneficios de Subnetting

La subnetización es la práctica de dividir una red grande en una o más subredes más

pequeñas y lógicas.[4] Este proceso, habilitado por el uso de máscaras de subred de longitud variable (CIDR), ofrece múltiples beneficios clave:

- **Optimización del espacio de direcciones IP:** Al dividir una red grande en subredes más pequeñas, se evita el desperdicio de direcciones que ocurría con el sistema de clases.[19]
- **Reducción del tráfico de red:** Los *broadcasts* (mensajes enviados a todos los dispositivos en una red) se contienen dentro de su subred, lo que reduce la congestión y el tráfico innecesario en la red principal.[19]
- **Mejora de la seguridad:** Las subredes permiten aislar segmentos de la red, de manera que el tráfico entre ellos debe pasar a través de un *router* o un *firewall*, lo que facilita la implementación de políticas de seguridad.[19]
- **Administración simplificada:** La segmentación lógica de una red facilita la gestión y el diagnóstico de problemas, ya que los administradores pueden centrarse en segmentos de red más manejables.[16]

4.2. Cálculos Fundamentales: El Proceso Matemático

El subnetting es una habilidad analítica que implica la aplicación de dos fórmulas matemáticas básicas para determinar el número de subredes y el número de hosts en cada una:

1. **Número de subredes:** 2^n donde n es el número de bits que se toman prestados de la porción de host de la máscara original. Es importante destacar que la antigua práctica de reservar dos subredes (la primera y la última) y calcular el número de subredes como $2^n - 2$ ha sido abandonada en favor de la notación CIDR, que permite el uso de todas las subredes disponibles.[22]
2. **Número de hosts por subred:** $2^h - 2$ donde h es el número de bits restantes en la porción de host. Se restan dos direcciones: la dirección de red (donde todos los bits de host son 0) y la dirección de *broadcast* (donde todos los bits de host son 1).[13]

A continuación, se presentan dos ejemplos prácticos que ilustran los dos enfoques más comunes en subnetting: dividir una red en un número específico de subredes y dividirla para que cada subred albergue un número mínimo de hosts.

4.3. Ejemplo Práctico 1: Subnetting de una Red Clase C (/24)

Problema: Subdividir la red 192.168.10.0/24 para crear 8 subredes.
Solución Paso a Paso:

1. **Identificar la máscara original:** La red es /24, lo que significa que la máscara por defecto es 255.255.255.0, y la porción de host tiene 8 bits (32−24=8).
2. **Calcular los bits a prestar (n):** Se necesita crear 8 subredes. Usando la fórmula $2^n \geq 8$, se determina que $2^3 = 8$. Por lo tanto, se necesitan tomar prestados 3 bits de la porción de host.[23]

3. **Calcular la nueva máscara:** La nueva máscara tendrá 24+3=27 bits a 1. La máscara /27 se traduce a 255.255.255.224 en decimal (11100000 en el último octeto).[24]
4. **Calcular el número de hosts por subred (h):** Quedan 5 bits para la porción de host (8−3=5). Usando la fórmula 2h−2, se obtiene 25−2=32−2=30 hosts utilizables por subred.
5. **Calcular el salto de red:** El salto se calcula restando el último octeto de la nueva máscara al valor 256. En este caso, 256−224=32. Esto significa que cada subred comenzará en un múltiplo de 32.[22]
6. **Enumerar las subredes:** Se genera una tabla que lista cada subred con su dirección de red, rango de hosts y dirección de *broadcast*.

Tabla 4: Subredes de la Red 192.168.10.0/24 con Prefijo /27

Subred	Dirección de Red	Rango de Hosts Válidos	Dirección de Broadcast
1	192.168.10.0	192.168.10.1 a 192.168.10.30	192.168.10.31
2	192.168.10.32	192.168.10.33 a 192.168.10.62	192.168.10.63
3	192.168.10.64	192.168.10.65 a 192.168.10.94	192.168.10.95
4	192.168.10.96	192.168.10.97 a 192.168.10.126	192.168.10.127
5	192.168.10.128	192.168.10.129 a 192.168.10.158	192.168.10.159
6	192.168.10.160	192.168.10.161 a 192.168.10.190	192.168.10.191
7	192.168.10.192	192.168.10.193 a 192.168.10.222	192.168.10.223
8	192.168.10.224	192.168.10.225 a 192.168.10.254	192.168.10.255

4.4. Ejemplo Práctico 2: Subnetting de una Red Clase B (/16)

Problema: Dividir la red 172.16.0.0/16 para que cada subred pueda albergar al menos 1000 hosts.

Solución Paso a Paso:

Este problema requiere un enfoque diferente, ya que la restricción no es el número de subredes, sino el número de hosts por subred. Esto es un ejemplo de cómo la ingeniería de redes no siempre sigue una sola dirección y requiere un pensamiento adaptable, como señalan los expertos en el campo.[25]

1. **Identificar la máscara original:** La red es /16, lo que significa que tiene 16 bits para la porción de host.
2. **Calcular los bits de host (h) necesarios:** Se necesita un mínimo de 1000 hosts. Usando la fórmula $2^h - 2 \geq 1000$, se busca el valor de h que satisfaga esta condición.
    - $2^{10} - 2 = 1024 - 2 = 1022$ hosts.
    - Por lo tanto, se necesitan 10 bits para la porción de host.
3. **Calcular los bits prestados (n):** El número total de bits en una dirección IPv4 es 32. La máscara original tiene 16 bits de red. El número de bits de host es 10. Por lo tanto, el número de bits prestados es $32 - 16 - 10 = 6$.
4. **Calcular la nueva máscara:** La nueva máscara tendrá $16 + 6 = 22$ bits a 1. La máscara /22 se traduce a 255.255.252.0 en decimal.
5. **Calcular el salto de red:** El cambio en la máscara ocurrió en el tercer octeto (el bit prestado cayó en este octeto). Por lo tanto, el salto se calcula sobre el tercer octeto: $256 - 252 = 4$. Esto significa que las subredes se incrementarán en 4 en el tercer octeto.
6. **Enumerar las primeras subredes:**
    - Subred 1: 172.16.0.0/22. (Hosts: 172.16.0.1 a 172.16.3.254, Broadcast: 172.16.3.255)
    - Subred 2: 172.16.4.0/22. (Hosts: 172.16.4.1 a 172.16.7.254, Broadcast: 172.16.7.255)
    - Subred 3: 172.16.8.0/22. (Hosts: 172.16.8.1 a 172.16.11.254, Broadcast: 172.16.11.255)

Este ejemplo demuestra que la subnetización es una herramienta versátil. La capacidad de un administrador de red para determinar la lógica del cálculo, ya sea por el número de subredes o por el número de hosts, es una de las habilidades más importantes en la ingeniería de sistemas. La flexibilidad del subnetting permite una asignación estratégica de los recursos de red, asegurando un crecimiento ordenado y eficiente en el futuro.

5. Protocolos Complementarios y Servicios Fundamentales

5.1. TCP vs. UDP: Fiabilidad vs. Velocidad

En la capa de transporte, la comunicación de red se gestiona a través de dos protocolos principales: TCP y UDP.[4]

- **Protocolo de Control de Transmisión (TCP):** Es un protocolo orientado a la conexión y fiable. Antes de enviar datos, TCP establece una conexión segura entre el origen y el destino a través de un proceso conocido como "saludo de tres vías" (*three-way handshake*).[10] Una vez establecida la conexión, TCP garantiza que los datos se entreguen en el orden correcto y sin errores, retransmitiendo cualquier segmento que se pierda en el camino. Los servicios que requieren una entrega de datos precisa, como la navegación web (HTTP/HTTPS), el acceso remoto (SSH) y la transferencia de archivos

(FTP), utilizan TCP.[4] La existencia de
puertos lógicos permite a los servicios distinguirse dentro de una misma IP, como el puerto 80 para HTTP o el 22 para SSH.[4]

- **Protocolo de Datagramas de Usuario (UDP):** A diferencia de TCP, UDP es un protocolo sin conexión y no fiable. Envía datagramas de datos sin establecer una conexión previa ni confirmar su recepción.[9] Debido a esta falta de garantías, UDP es mucho más rápido y eficiente. Se utiliza en aplicaciones donde la velocidad es más importante que la fiabilidad y se pueden tolerar pequeñas pérdidas de datos, como en el
streaming de vídeo, las llamadas de voz sobre IP (VoIP) o las consultas DNS.[4]

Tabla 5: Puertos y Protocolos Comunes

Servicio	Puerto	Protocolo	Descripción
SSH	22	TCP	Acceso seguro a la línea de comandos de un servidor [4]
HTTP	80	TCP	Protocolo de navegación web no cifrada [4]
HTTPS	443	TCP	Protocolo de navegación web cifrada [4]
DNS	53	UDP	Resuelve nombres de dominio a direcciones IP [4]
RDP	3389	TCP	Protocolo de escritorio remoto de Windows [4]
MySQL	3306	TCP	Base de datos relacional [4]
PostgreSQL	5432	TCP	Base de datos relacional [4]
SMTP	25	TCP	Envío de correo electrónico [4]

5.2. NAT y PAT: El Ahorro de Direcciones IPv4

Para que los dispositivos en una red privada (con IPs no enrutables) puedan acceder a Internet, se necesita una técnica de traducción de direcciones. La **Traducción de Direcciones de Red (NAT)** es el concepto que permite a un *router* o *firewall* actuar como intermediario, reescribiendo la dirección IP de origen de un paquete saliente.[26]

La forma más común de NAT es la **Traducción de Direcciones de Puerto (PAT)**, también conocida como NAT de sobrecarga (*NAT overloading*). Este método es crucial para la conservación de IPs públicas, ya que permite que múltiples dispositivos en una red privada compartan una única dirección IP pública.[28] PAT funciona aprovechando los puertos lógicos de los protocolos de transporte (TCP/UDP). Cuando un dispositivo interno (ej. 192.168.1.10:1024) envía una solicitud a un servidor en Internet, el *router* NAT sustituye la IP privada del dispositivo por su propia IP pública (20.35.50.10) y le asigna un número de puerto único para esa sesión (ej. 20.35.50.10:55000).[28] Cuando la respuesta del servidor regresa a la IP pública del
router, este consulta una tabla interna de mapeo de sesiones para saber a qué IP privada y puerto interno debe reenviar el paquete. Este proceso permite que un solo *router* con una única IP pública sirva de puerta de enlace a docenas o incluso cientos de dispositivos internos.[4] Es importante distinguir entre NAT como término genérico para la traducción de direcciones y PAT como la técnica específica que utiliza los puertos para compartir una única IP pública.

5.3. Servicios de Automatización y Nombres

Para que la conectividad funcione de manera fluida, se requieren servicios de red que automatizan procesos y facilitan el acceso:

- **DHCP (Dynamic Host Configuration Protocol):** Es un protocolo que asigna automáticamente una dirección IP, una máscara de subred, una puerta de enlace predeterminada y un servidor DNS a los dispositivos que se conectan a una red.[4] Esto elimina la necesidad de configurar manualmente cada dispositivo y asegura que no haya conflictos de direcciones.
- **DNS (Domain Name System):** Conocido como la "guía telefónica de Internet", el DNS traduce los nombres de dominio legibles para humanos (ej. google.com) a las direcciones IP numéricas que los ordenadores usan para comunicarse.[4] Sin el DNS, un usuario tendría que recordar la IP de cada sitio web, como 142.250.187.164, para acceder a él.

6. Conclusión y Diagnóstico de Red (Resumen para la Práctica)

6.1. Recapitulación de los Fundamentos Clave

A lo largo de este documento, se han revisado los principios esenciales que rigen la operación

de las redes de computadoras. Se ha establecido una comprensión de los modelos de referencia OSI y TCP/IP, que ofrecen una visión teórica y práctica de la comunicación en capas. Se ha profundizado en la anatomía de una dirección IPv4, la función de la máscara de subred y la puerta de enlace, y se ha explorado el concepto crucial de las IPs públicas y privadas. El subnetting se ha presentado no solo como una técnica de cálculo, sino como una solución vital a los problemas de conservación de direcciones que surgieron del obsoleto modelo de clases de red. Finalmente, se han cubierto protocolos de transporte clave como TCP y UDP, y servicios fundamentales como NAT/PAT, DHCP y DNS.

6.2. Herramientas de Diagnóstico Básico

Antes de abordar cualquier problema de conectividad, es esencial utilizar herramientas de diagnóstico básicas para identificar la ubicación de la falla.

- **Ping:** Envía un paquete de prueba (*ICMP echo request*) a un destino IP y espera una respuesta.[4] Si el destino responde, se confirma que existe conectividad IP. Es importante recordar que muchos
  firewalls bloquean las peticiones ping por defecto, por lo que una falla en el *ping* no siempre indica un problema de conectividad.[4]
- **Traceroute:** Muestra la ruta completa que toma un paquete desde el origen hasta el destino, listando cada salto (*router*) intermedio.[4] Si la comunicación se detiene en un punto determinado, puede ayudar a identificar dónde se interrumpe la conexión.

6.3. Un Enfoque Metódico para la Solución de Problemas

La percepción de que los conceptos de red están "mezclados" es un problema común para los principiantes, ya que las fallas en el mundo real rara vez se limitan a una sola capa. Un problema de conectividad es, casi siempre, la manifestación de una falla en la interconexión de varias capas de la red. Por lo tanto, un experto no aborda un problema de forma aislada, sino que sigue un enfoque metódico basado en los "cuatro pilares" de la conectividad [4]:

1. **IP:** ¿Tiene el dispositivo una dirección IP válida? ¿Es la IP de destino correcta?
2. **Rutas:** ¿Existe una ruta para que el tráfico saliente llegue a su destino? ¿Está el *gateway* configurado correctamente?
3. **Puertos:** ¿Está el servicio que se intenta contactar escuchando en el puerto correcto?
4. **Firewall:** ¿Hay alguna regla en el *firewall* local o de la red (como un grupo de seguridad en AWS) que bloquee el tráfico entrante o saliente en el puerto requerido? [4]

Por ejemplo, si un usuario no puede conectarse por SSH a un servidor (timeout), el problema no es solo la falta de un *firewall* abierto. Podría ser que el servidor no tenga una IP pública, que la subred no tenga una puerta de enlace a Internet, que el servicio SSH esté inactivo o que un *firewall* local lo esté bloqueando, incluso si la regla de seguridad a nivel de red lo permite.[4]

Este enfoque integrado, que evalúa la interdependencia de los conceptos a través de un diagnóstico estructurado, es el que diferencia a un experto de un novato. Este documento ha proporcionado la base teórica para que el usuario pueda empezar a desarrollar esta forma de pensar, sentando el terreno para el éxito en su aprendizaje y la solución de problemas complejos en el futuro.