Definiciones Clave de Redes:

1. Tipos de Conexión a Internet:

**ISP (Proveedor de Servicios de Internet):**

- Acceso a Internet (no especifica la tecnología).

**DSL (Línea de Suscriptor Digital):**

- Internet por cables de cobre (líneas telefónicas).

2. Identificadores de Red:

**SSID (Service Set Identifier - Identificador del Conjunto de Servicios):**

- Nombre de la red Wi-Fi.

3. Tipos de Redes:

**LAN (Local Area Network - Red de Área Local):**

- Red en área limitada (casa, oficina). Conexión por cable (Ethernet).

**WLAN (Wireless Local Area Network - Red de Área Local Inalámbrica):**

- LAN inalámbrica (Wi-Fi).

**MAN (Metropolitan Area Network):**

- Red en área metropolitana (ciudad).

**WAN (Wide Area Network):**

- Red en área extensa (país, mundo). Internet es la WAN más grande.

**Servidor DNS (Domain Name System):**

- "Guía telefónica" de Internet: Nombre de dominio (google.com) -> Dirección IP (142.250.184.142).

Modelos de Comunicación de Red (Síntesis Funcional):

- **Objetivo:** Comunicación entre dispositivos en la red.
- **Protocolos de Red (Fundamentos):**
    - **Definición:** Reglas para que las computadoras se comuniquen correctamente.
    - **Elementos Clave:**
        - Formato del mensaje.
        - Tamaño del mensaje.
        - Sincronización (velocidad de transmisión).
        - Codificación (conversión a bits).
        - Encapsulación (agregar encabezados con direcciones).
        - Patrón de mensaje (ej: Request/Response).
- **Modelos:**
    - **TCP/IP:** Estándar de Internet (práctico).
    - **TCP (Transmission Control Protocol):** Protocolo de control de transmisión (protocolo confiable).
        - **Protocolos Clave:** * **TCP:** Entrega confiable. * **IP:** Enrutamiento.
    - **OSI:** Modelo conceptual (cómo *debería* funcionar).
    - **OSI (Open Systems Interconnection):** Interconexión de sistemas abiertos (modelo de referencia para redes).*
- **Tabla Comparativa de Capas TCP/IP vs. OSI:**

| Nº | Capa TCP/IP | Capa OSI | Función Principal | Detalles Clave y Ejemplos Prácticos | ¿Cómo Recordarlo Fácil? |
|---|---|---|---|---|---|
| 7 | Aplicación | Aplicación | **(Usuario y Servicios)**: Proporciona la interfaz para que las aplicaciones de red interactúen con el usuario y ofrezcan servicios. | * Define la forma en que las aplicaciones acceden a la red. Incluye protocolos para correo electrónico (SMTP, POP3, IMAP), web (HTTP, HTTPS), transferencia de archivos (FTP), acceso remoto (SSH), nombres de dominio (DNS), etc. * **Ejemplo:** Usar Outlook para enviar un correo (la aplicación interactúa con los protocolos SMTP para enviar y POP3/IMAP para recibir). | **El programa que usas:** ¡El navegador, el correo, el juego en línea! |
| 6 | Aplicación | Presentación | **(Formato y Cifrado)**: Garantiza que los datos sean presentados de manera comprensible para la aplicación receptora, manejando formatos, cifrado y compresión. | * Convierte los datos a un formato común, cifra datos sensibles para seguridad (SSL/TLS), y comprime para eficiencia. * **Ejemplo:** Un navegador web entendiendo una imagen JPEG (formato) o una página web segura con HTTPS (cifrado). | **Traduce y Protege:** ¡Como un intérprete y guardaespaldas de la información! |
| 5 | Aplicación | Sesión | **(Conexiones y Diálogos)**: Establece, gestiona y finaliza las conexiones (sesiones) entre aplicaciones. | * Define cómo comenzar, controlar y terminar "conversaciones" entre aplicaciones. Sincroniza la comunicación y maneja interrupciones. * **Ejemplo:** Mantener una sesión activa en un juego en línea o una videoconferencia sin que se interrumpa constantemente. | **La Conversación Continua:** ¡Asegura que no te corten la llamada a mitad de la frase! |
| 4 | Transporte | Transporte | **(Comunicación Confiable o Rápida)**: Proporciona una comunicación confiable (TCP) o rápida (UDP) entre aplicaciones, segmentando datos y controlando el flujo. | * **TCP:** Orientado a conexión, entrega confiable, control de flujo, reordenamiento de paquetes, corrección de errores. Confirma la recepción de datos mediante **ACK (acuse de recibo)** para verificar la entrega o, en caso de error, puede enviar un **NACK (acuse de no recibo o recibo mal)** para solicitar la retransmisión. * **UDP:** Sin conexión, más rápido, sin garantías de entrega. * **Ejemplo:** Descargar un archivo grande (TCP) para asegurar que no se corrompa vs. ver una transmisión en vivo (UDP) donde perder algunos paquetes es aceptable. | **Elige el Mensajero:** ¡Confianza (TCP) o Velocidad (UDP)! |
| 3 | Internet | Red | **(Enrutamiento Global)**: Enruta los paquetes de datos entre diferentes redes, definiendo el direccionamiento IP y encontrando la mejor ruta. | * Define el direccionamiento lógico (IP) para identificar dispositivos en la red. Enruta paquetes a través de múltiples redes hasta su destino final. * **Ejemplo:** Un paquete de datos viajando desde tu casa a un servidor en otro país, pasando por múltiples routers. | **El Mapa de la Red:** ¡Encuentra el camino a casa! |

| Nº | Capa TCP/IP | Capa OSI | Función Principal | Detalles Clave y Ejemplos Prácticos | ¿Cómo Recordarlo Fácil? |
|---|---|---|---|---|---|
| 2 | Acceso a la Red | Enlace de Datos | **(Enlace Local y Direccionamiento Físico)**: Transfiere datos entre dos nodos directamente conectados, definiendo el formato de las **tramas** y las direcciones MAC. | * **Creación de Tramas:** Los datos de la capa de Red se encapsulan en tramas en esta capa. Si faltan datos para completar la trama, se puede usar padding. * Controla el acceso al medio (MAC), maneja notificación de errores, la topología de red, control de flujo y direccionamiento físico (MAC). *Tu computadora, Tablet, PS5 comunicándose directamente con tu router a través de Ethernet o Wi-Fi gracias a su NIC inalámbrica con dirección MAC*. * **Ejemplo:** Switches y bridges conectando dispositivos en una red local. * **Subcapas (clave):** MAC (Media Access Control) y LLC (Logical Link Control). * **Ejemplo:** Tu computadora comunicándose directamente con tu router a través de Ethernet o Wi-Fi. * **Protocolos/Tecnologías:** CSMA/CD (en redes Ethernet antiguas, detección de colisión). | **La Calle Local:** ¡Entre tu casa y la avenida principal! |
| 1 | Acceso a la Red | Física | **(Transmisión Física de Bits)**: Transmite los datos brutos (bits) a través del medio físico, definiendo voltajes, tasas de datos y conectores. | * Implementación en hardware, codificación de canal, representación de bits, voltaje, frecuencia, sincronización, conectores físicos, distancias y cableado. Medios de transmisión: Cables (Ethernet, UTP, FTP, SFTP), Radiofrecuencias (Wi-Fi, Bluetooth, ZigBee) *Ejemplo: Redes Wi-Fi unificadas que operan en 2.4 GHz y 5 GHz*, F.O. (Fibra Óptica), AP (Puntos de Acceso), Hubs. La capa física define las características de la transmisión, incluyendo el tipo de antena (direccional, omnidireccional, sectorial) Transmisión Simplex, Half-Duplex, Full-Duplex. * **Tecnologías:** SONET (con WDM "espacio" y TDMA "tiempo"), Ethernet, Wi-Fi, Bluetooth, ZigBee, USB. * **Componentes:** Activos (amplificadores, repetidores), Pasivos (cables, conectores). **Verifica la cantidad de bits, no la calidad.** * **Ejemplo:** Un cable Ethernet conectando tu computadora al router o las ondas de radio transmitiendo datos Wi-Fi. | **El Cable y las Ondas:** ¡La autopista de los bits! |

### Diseño de Red: Redes Jerárquicas

En la tecnología de redes, un diseño jerárquico implica dividir la red en niveles independientes. Cada nivel en la jerarquía proporciona funciones específicas que definen su rol dentro de la red general. Un diseño típico de red jerárquica incluye los siguientes niveles de switches:

- **Switches de Core (Núcleo):** Situados en la parte superior de la jerarquía, los switches de core son responsables de transportar grandes cantidades de tráfico de manera confiable y rápida. Su propósito es mover el tráfico lo más rápido posible. En este nivel, la velocidad y la latencia son preocupaciones primordiales.
- **Switches de Distribución (Distribution Layer):** Es el punto de comunicación entre los switches de acceso y los de core. Su función es proporcionar enrutamiento, filtrado y acceso a la WAN, y determinar cómo los paquetes pueden acceder al core. Aquí se implementan las políticas de red.
- **Switches de Acceso (Access Layer):** Controlan el acceso de usuarios y grupos de trabajo a los recursos de la red interna. Los recursos de red que la mayoría de los usuarios necesitan se encuentran disponibles localmente en este nivel. Aquí se maneja cualquier tráfico para servicios remotos.

Tipos de Medios de Red

| Medio | Tipo de Datos | Distancia Máxima | Entorno de Instalación | Ancho de Banda/Velocidad | Costo | Funcionalidad | Ejemplo de Uso |
|---|---|---|---|---|---|---|---|

| Medio | Tipo de Datos | Distancia Máxima | Entorno de Instalación | Ancho de Banda/Velocidad | Costo | Funcionalidad | Ejemplo de Uso |
|---|---|---|---|---|---|---|---|
| **Par Trenzado (Cat5/5e/6/6a)** | Impulsos Eléctricos | Hasta 100 metros (Ethernet) | Interior (oficinas, hogares) | Moderado a Alto | Bajo a Moderado | Conexión de dispositivos en redes Ethernet (LAN). Base de la mayoría de redes locales. | Conectar una PC a un router en casa o en la oficina. |
| **Coaxial** | Impulsos Eléctricos | Media (depende de la frecuencia) | Interior/Exterior | Moderado | Moderado | Transmisión de señales de TV, conexión satelital. Como cables de cobre de compañías de TV. | Conexión de un televisor a un servicio de cable, conexión satelital. |
| **Fibra Óptica** | Pulsos de Luz | Varios kilómetros o más | Interior/Exterior (subterráneo, submarino) | Muy Alto | Alto | Transmisión de datos a alta velocidad, inmune a interferencia. | Redes troncales, conexión de ciudades, centros de datos, compañías telefónicas. |
| **Inalámbrico** | Ondas Electromagnéticas | Variable (depende del estándar y entorno) | Interior/Exterior | Bajo a Moderado | Bajo a Moderado | Conexión de dispositivos sin cables mediante modulación de frecuencias. | Conexión de laptops, smartphones, tablets a redes Wi-Fi; Bluetooth; redes celulares. |

### Encapsulación y la Trama de Ethernet

Este módulo explica el concepto de encapsulación y la estructura de la trama Ethernet:

**Encapsulación:** Es el proceso de envolver datos en un formato específico (trama) para su transmisión a través de la red. Similar a poner una carta dentro de un sobre.

**Trama Ethernet:** Actúa como un "sobre" para los datos, conteniendo información de origen y destino. El formato de la trama está determinado por el tipo de mensaje y el canal de transmisión.

**Dirección MAC:** Cada tarjeta de interfaz de red (NIC) tiene una dirección MAC única que se utiliza para identificar el origen y el destino de la trama Ethernet.

**Protocolo IP:** Similar al sobre en la analogía, el protocolo IP (ej. IPv6) es responsable de enviar el mensaje desde el origen al destino a través de la red.

# Propósito de una dirección IPv4

## La Dirección IPv4

Una dirección IPv4 es necesaria para que un host pueda comunicarse en Internet y en redes LAN. Es una dirección lógica que debe ser única y configurarse correctamente tanto a nivel local como remoto para permitir la comunicación.

Cada interfaz de red (como una tarjeta NIC) en un dispositivo final, como PC, servidores, impresoras de red o teléfonos IP, requiere una dirección IPv4. Los enrutadores también tienen direcciones IPv4 en sus interfaces para conectarse a redes IP.

Cada paquete enviado en Internet incluye una dirección IPv4 de origen y destino, lo que garantiza que los datos lleguen al destino correcto y las respuestas sean enviadas al origen.

## 8.1.2 Octetos y notación decimal con puntos

Una dirección IPv4 tiene 32 bits, agrupados en cuatro bloques de 8 bits llamados octetos. Para facilitar su lectura y configuración, se convierten de binario a formato decimal separado por puntos.

**Ejemplo:**

- Binario: `11010001101001011100100000000001`
- Octetos: `11010001.10100101.11001000.00000001`
- Decimal con puntos: `209.165.200.1`

## IPs en Resumen: Máscara y Redondeo a Cero

**Concepto Clave:** IP = RED + HOST. La MÁSCARA define la división.

**Los Dos Trucos:**

1. **Máscara -> IP: Coordenadas RED/HOST:**
   - `255` en la máscara: El número correspondiente en la IP es RED.
   - `0` en la máscara: El número correspondiente en la IP es HOST.
2. **Calcular la Dirección de RED:**
   - Toma la parte de RED de la IP.
   - Redondea a cero la parte del HOST. Ej: si el HOST era .50, ahora es .0

**Ejemplo Rápido:**

- IP: `192.168.1.50`
- Máscara: `255.255.255.0`
- RED: `192.168.1`
- Dirección de RED: `192.168.1.0`

**Misma Red?** Compara las Direcciones de RED. Si coinciden, ¡están en la misma red!

**Redes Domésticas/Oficinas Pequeñas:**

1. **Internet Entra:** El ISP te da Internet. El "ancho de banda" de tu plan define la velocidad.
2. **Red Local (LAN/WLAN):** Tu router crea una red local (LAN = cable, WLAN = Wi-Fi) para que tus dispositivos se conecten y compartan Internet.
3. **Direcciones:** Cada dispositivo *activo* en la red necesita una dirección IP (y tiene una MAC). Pero periféricos (mouse, teclado, webcam) no necesitan IP.
4. **IPs y Máscaras (Lo Crucial):**
   - La Máscara define qué parte de la IP es la RED y cuál el HOST.
   - Para encontrar la Red, "redondea" la parte HOST a cero.
   - Si dos IPs tienen la misma dirección de RED, están en la misma LAN.
5. **Más Cables?**: Si necesitas conectar más dispositivos con cable, usa un switch Ethernet (amplía los puertos de tu router).
6. **Redes Virtuales (VLANs - Opcional):** Un switch avanzado puede crear VLANs. Esto divide la red en "subredes virtuales". Dispositivos en diferentes VLANs no se ven, aunque estén conectados al mismo switch. Útil para separar redes de invitados o dispositivos inseguros.

## IPv4: Unidifusión, Difusión y Multidifusión (Resumen)

- **Unidifusión (1 a 1):** Envío a un host específico. (excluyendo reservados)
- **Difusión (1 a Todos):** Envío a todos en la red. (Los routers *no* reenvían difusiones limitadas 255.255.255.255).
- **Multidifusión (1 a Grupo):** Envío a un grupo de hosts suscritos.

## Tipos de Direcciones IPv4: Públicas vs. Privadas (y el Truco!)

### Direcciones IPv4: Tipos y Rangos (¡Identifícalas Fácil!)

- **Públicas:** Para Internet. (¡Si no está en los siguientes rangos, es pública!)

- **Privadas:** Para redes internas.
    - **10.x.x.x**
    - **172.16.x.x - 172.31.x.x**
    - **192.168.x.x**
- **NAT:** Convierte IPs privadas a una IP pública.
- **Especiales:**
    - **Loopback (bucle invertido)(127.0.0.0/8):** Para probar la propia conexión. *Comienza con 127* (ej: 127.0.0.1, 127.255.255.255)
    - **APIPA / Link-Local (169.254.0.0/16):** Windows las usa si no obtiene IP automáticamente. *Comienza con 169.254* (ej: 169.254.0.1, 169.254.255.254)
    - **Experimental (240.0.0.0 - 255.255.255.254):** Para investigación. *Comienza con 240 a 255* (ej: 240.0.0.1, 255.255.255.0). No deben usarse en redes públicas.
    - **Multidifusión (224.0.0.0 - 239.255.255.255):** Envío a un grupo específico de hosts. *Comienza con 224 a 239* (ej: 224.0.0.5).
- **Unidifusión y Difusión:** No tienen rangos específicos fijos. Las de unidifusión son todas las IPs que *no* son privadas, loopback, APIPA, experimentales o multidifusión. Las de difusión dependen de la máscara de subred.
- **Quién Asigna las IPs?** IANA da bloques de IPs a los **RIRs**, quienes las asignan a los ISPs.

  La *Internet Assigned Numbers Authority* (IANA) es responsable de administrar globalmente el espacio de direcciones IP. IANA delega bloques de direcciones IP a los *Registros Regionales de Internet* (RIRs), que son organizaciones responsables de la asignación y registro de direcciones IP dentro de una región geográfica específica. Los RIRs, a su vez, asignan bloques más pequeños de direcciones a los *Proveedores de Servicios de Internet* (ISPs) y a otras organizaciones dentro de su región.

  **Los cinco RIRs son:**

    - **AfriNIC:** Para África.
    - **APNIC:** Para Asia-Pacífico.
    - **ARIN:** Para Norteamérica.
    - **LACNIC:** Para Latinoamérica y el Caribe.
    - **RIPE NCC:** Para Europa, Oriente Medio y partes de Asia Central.

  Esta estructura jerárquica asegura una gestión eficiente y organizada del espacio de direcciones IP en todo el mundo.

## Segmentación de la Red: Dominios de Difusión y Subredes

Esta sección explora cómo dividir una red en segmentos más pequeños para mejorar el rendimiento y la seguridad.

**Dominios de Difusión:**

- **Difusión:** Un mensaje enviado a *todos* los dispositivos en una red.
- **Switches:** Propagan difusiones a *todas* las interfaces excepto la que recibió la difusión.
- **Routers:** *No* propagan difusiones, limitando el dominio.

**Problemas con los Dominios de Difusión Grandes:**

- Tráfico de difusión excesivo -> red lenta.
- **Solución: Subredes:** Dividir la red en dominios de difusión más pequeños.

**Razones para la Segmentación de Redes (Subredes):**

- Mejora el rendimiento y la seguridad.

# Abreviando Direcciones IPv6 (4x el Tamaño de IPv4)

Las direcciones IPv6, que tienen 128 bits (cuatro veces el tamaño de una dirección IPv4 de 32 bits), se componen de 8 hextetos (grupos hexadecimales de 16 bits) separados por dos puntos. Para simplificar su representación, se aplican dos reglas de abreviación:

**1. Regla 1: Omitir Ceros Iniciales (por Hexteto, en Toda la Dirección):**

- **Aplicación:** A *cada* hexteto individual dentro de la dirección IPv6, lo que significa que se puede aplicar hasta en los 8 hextetos de la dirección.
- **Acción:** Eliminar cualquier cero(s) que aparezca al comienzo de cada hexteto.

- **Cobertura:** Al aplicarse a cada hexteto, esta regla afecta *hasta* los 128 bits (todos los dígitos) de la dirección completa y permite la eliminación de ceros *en cualquier parte* de la dirección, siempre y cuando estén al inicio de un hexteto. Es, en ese sentido, más "invasiva" porque afecta a una mayor cantidad de dígitos individuales.
- **Ejemplo:** `2001:0DB8:000A:0001` se simplifica a `2001:DB8:A:1` (ceros iniciales removidos en 4 hextetos distintos).

**2. Regla 2: Compresión con "::" (por Dirección IPv6):**

- **Aplicación:** A la *dirección IPv6 completa*.
- **Acción:** Reemplazar una *única* secuencia contigua de *uno o más* hextetos *completamente cero* por `::`.
- **Restricción:** Solo puede usarse *una vez* por dirección IPv6.
- **Cobertura:** Aunque puede reemplazar múltiples hextetos a la vez, solo se aplica en una *única* ubicación dentro de la dirección.
- **Ejemplo:** `2001:0DB8:0000:0000:0000:0000:0000:0200` se simplifica a `2001:DB8::200`

**Importante:** La regla 2 (compresión con ":😊 se aplica a cada dirección IPv6 de forma *independiente*. Esto significa que puedes usar `::` en *múltiples direcciones IPv6 diferentes*, siempre y cuando cada una de esas direcciones cumpla con la condición de tener una secuencia contigua de hextetos cero, y solo se aplique una vez *dentro de esa dirección específica*.

## Síntesis: Direccionamiento IPv4 Estático vs. Dinámico, Límites de Red y NAT

El direccionamiento IPv4 puede ser estático o dinámico.

- **Estático:** El administrador de red configura manualmente la dirección IP, máscara de subred y puerta de enlace predeterminada en cada host. Es útil para dispositivos que necesitan una dirección IP consistente (servidores, impresoras). Ofrece mayor control, pero es propenso a errores, requiere una gestión cuidadosa de las direcciones, y es lento de implementar en grandes redes.

- **Dinámico (DHCP):** El protocolo DHCP asigna automáticamente la dirección IP, máscara de subred, puerta de enlace predeterminada y otra información de configuración a los hosts. Es preferible en redes grandes porque reduce la carga administrativa, minimiza los errores y permite la reutilización de direcciones IP a través del **arrendamiento (lease)**.

  El proceso de asignación DHCP involucra mensajes **DORA (Discover, Offer, Request, Acknowledge)**. Este proceso asegura que cada dispositivo que necesite una dirección IP la obtenga de manera única y automatizada. DHCP es el método preferido para asignar direcciones en redes grandes por que reduce la carga del equipo de soporte y elimina errores de configuracion.

  - **DHCP Discover:** El cliente (recién conectado o reiniciado) difunde un mensaje (broadcast) a la dirección **255.255.255.255** para encontrar servidores DHCP. Este mensaje indica que el cliente *busca* un servidor DHCP.
  - **DHCP Offer:** El servidor DHCP responde con un **DHCP Offer**, *ofreciendo* una dirección IP disponible, máscara de subred, puerta de enlace predeterminada y tiempo de arrendamiento.
  - **DHCP Request:** El cliente responde al servidor *solicitando* la dirección IP ofrecida. El cliente difunde una `DHCPREQUEST` al servidor que le ha ofertado.
  - **DHCP Acknowledge (ACK):** El servidor DHCP confirma la asignación de la dirección IP al cliente con un **DHCPACK**. Este mensaje indica que el cliente es capaz de usar la información IP proporcionada.

**Límites de Red y Puertas de Enlace:**

Los enrutadores actúan como puertas de enlace que permiten que hosts en diferentes redes se comuniquen. Cada interfaz del enrutador está conectada a una red diferente. La dirección IP de la interfaz del enrutador sirve como la puerta de enlace predeterminada para los hosts en su red. En redes domésticas, el router inalámbrico, además de ser servidor DHCP, sirve como conexión entre la red interna y la red del proveedor de internet.

**Traducción de Direcciones de Red (NAT):**

Dado que las direcciones IPv4 públicas son limitadas, **NAT** permite que múltiples dispositivos en una red privada (con direcciones IP privadas, ej. 192.168.x.x) compartan una única dirección IP pública para acceder a Internet. El enrutador, actuando como servidor NAT, traduce las direcciones IP privadas internas a la dirección IP pública proporcionada por el ISP. Cuando el tráfico regresa de Internet, el enrutador utiliza información de puerto para determinar a qué dispositivo interno debe reenviar el tráfico. NAT es una parte fundamental de la funcionalidad de la mayoría de los enrutadores domésticos y de pequeñas empresas.

## Síntesis: Direcciones MAC e IP y la Comunicación en Redes - Proceso de Comunicación y Resolución de Direcciones

Esta sección explica cómo las direcciones MAC (Media Access Control) y las direcciones IP trabajan juntas para permitir la comunicación en redes, y cómo se usan para enviar datos dentro de una red local y a través de Internet. Entender este proceso es fundamental para comprender cómo los dispositivos se encuentran y se comunican entre sí.

- **Direcciones Primarias: Dos Tipos de "Destino" para los Datos (Capas 2 y 3)**
    - **Dirección MAC (Dirección Física - Capa 2):** Imagina que solo necesitas enviar un mensaje al edificio de al lado. Necesitas su dirección *física*: "Casa número 12". La dirección MAC se usa en la *Capa de Enlace de Datos (Capa 2)* para que los dispositivos se encuentren *directamente* dentro de la misma red local (LAN). Es el "destino" para la comunicación *local*.
    - **Dirección IP (Dirección Lógica - Capa 3):** Ahora imagina que necesitas enviar un paquete a otro país. Necesitas su dirección *postal completa*: "Calle Falsa, 123, Ciudad Imaginaria, País Lejano". La dirección IP se usa en la *Capa de Red (Capa 3)* para que los dispositivos se encuentren *a través de Internet*, pasando por múltiples redes. Es el "destino" para la comunicación *global*.
- **El Proceso de Entrega: Dos Rutas, Dos Direcciones**
    - **Ruta Local (Misma Red):** Cuando envías datos al "edificio de al lado", solo necesitas saber su dirección MAC. Tu dispositivo crea un "paquete" que incluye:
        - Dirección MAC del destino (el edificio de al lado)
        - Tu propia dirección MAC (para que sepan quién lo envió)
        - El contenido del mensaje (los datos que quieres enviar).
    - **Ruta Global (Otra Red):** Cuando envías datos a "otro país", no puedes simplemente enviarlo directamente. Necesitas enviarlo primero a la oficina de correos *local* (el enrutador). Tu dispositivo crea un paquete que incluye:
        - Dirección MAC de la *oficina de correos local* (el enrutador)
        - Tu propia dirección MAC
        - El contenido del mensaje (que incluye la dirección postal completa del destino final).
- **Conectar las Dos Direcciones: Los Traductores que Solicitan la MAC (ARP y ND)**
    - ¿Cómo sabe tu dispositivo la dirección MAC del "edificio de al lado" o de la "oficina de correos local" si solo conoce la dirección IP? Aquí es donde entran en juego los "traductores", que *solicitan* la dirección MAC a partir de la dirección IP:
        - **ARP (Address Resolution Protocol):** Para redes IPv4. Es como preguntar: "¿Quién vive en la dirección IP 192.168.1.10? Necesito su dirección MAC".
        - **ICMPv6 Neighbor Discovery (ND):** Para redes IPv6. Es lo mismo que ARP, pero para la nueva generación de direcciones de Internet.
- **¿Qué NO Hacen ARP/ND?** Es importante entender que **ARP/ND no hacen lo mismo que NAT o DHCP**.
    - **NAT** permite que multiples dispositivos compartan una dirección IP pública para acceder a Internet.
    - **DHCP** asigna direcciones IP a los dispositivos.

  ARP/ND son para *descubrir la dirección MAC asociada a una dirección IP dentro de la red local*.
- **PDUs (Protocol Data Units):**
    - Una PDU es simplemente un "paquete" de datos que se envía a través de la red, y la visualización de PDUs en Packet Tracer es una simplificación para fines didácticos.

**En resumen:** La comunicación en red requiere saber a *dónde* enviar la información (dirección IP) y *cómo* llegar allí (dirección MAC). El proceso de comunicación cambia dependiendo si el destino es local o remoto, y protocolos como ARP y ND se encargan de traducir direcciones IP a MAC cuando es necesario, pero no realizan las mismas funciones que NAT o DHCP. Packet Tracer te ayuda a ver este proceso en acción.

## Síntesis: Dominios de Difusión y ARP - Encontrando Dispositivos en la Red Local

Esta sección explica cómo los dispositivos se encuentran en la red local (LAN) y cómo se gestionan los "anuncios" (difusiones) para evitar problemas de rendimiento.

- **Difusiones: Anuncios para Todos**

  Una *difusión* es un mensaje enviado a *todos* los dispositivos en la red local. Una red con conmutadores (LAN) es un *dominio de difusión*: todos los dispositivos escuchan todas las difusiones.
- **Contención: El Problema del Ruido**

  *Demasiadas* difusiones hacen que la red se vuelva lenta (contención). Para solucionar esto, se dividen las redes grandes en dominios más pequeños usando enrutadores.
- **ARP: Preguntando por la MAC (el "Nombre") conociendo la IP (el "Apellido")**

Si un dispositivo (Host A) quiere enviar un mensaje *directamente* a otro (Host B) en la LAN, necesita la dirección MAC de Host B. ARP permite a Host A encontrar la MAC de Host B conociendo su IP.

- **El Proceso ARP: Preguntar, Escuchar, Recordar**

    1. **ARP Request:** Host A *difunde* una pregunta: "¿Quién tiene la IP X.X.X.X (Host B)?". La dirección MAC destino es `FF-FF-FF-FF-FF-FF` (difusión).
    2. **ARP Reply:** *Solo* Host B responde *directamente* a Host A con su dirección MAC.
    3. **Tabla ARP:** Host A guarda la IP y la MAC de Host B en su tabla ARP para uso futuro.

**En resumen:** Las difusiones permiten que todos se encuentren, pero ARP ayuda a los dispositivos a encontrar a alguien específico (su MAC), y los enrutadores limitan el alcance de las difusiones para evitar la congestión.

## Tabla de Enrutamiento - El "Mapa" del Enrutador para Enviar Datos

Los enrutadores dirigen el tráfico usando la *tabla de enrutamiento*, que es como su "mapa".

- **Tabla de Enrutamiento: ¿Qué contiene?**
    - Redes de destino.
    - Interfaces de salida (puertos).
- **¿Cómo se llena?**
    - Redes conectadas directamente (automáticamente).
    - Configuración manual.
    - Intercambio dinámico con otros enrutadores.
- **¿Cómo decide el enrutador?**
    - Examina la dirección IP de destino del paquete.
    - Busca en la tabla la mejor ruta a esa red.
- **Ruta Predeterminada: El "Plan B"**
    - Si no encuentra la red en la tabla, usa la ruta predeterminada.
- **El host envía información al Gateway Predeterminado de su LAN**

**En resumen:** La tabla de enrutamiento permite al enrutador dirigir el tráfico. Contiene redes e interfaces de salida, y la decisión se basa en la IP destino. Sin una ruta específica, usa la predeterminada y el host usará para contactar otras redes fuera de su dominio local el Gateway.

**LAN (Red de Área Local):**

- Red(es) bajo un mismo control administrativo.
- Varía en tamaño (hogar a edificios múltiples).
- Usa Ethernet/inalámbrico, alta velocidad.
- Intranet: LAN privada para una organización.

## TCP y UDP

- **TCP (Transmission Control Protocol):**
    - Entrega confiable de datos.
    - Divide mensajes en segmentos numerados.
    - Realiza seguimiento de segmentos enviados y retransmite los perdidos.
    - Utilizado donde la integridad de los datos es crucial.
- **UDP (User Datagram Protocol):**
    - Entrega "mejor esfuerzo" sin confirmación de recepción.
    - Rápido, pero no garantiza la entrega.
    - Adecuado para audio y VoIP (transmisión en tiempo real).

## Números de Puerto

- Identifican protocolos y servicios en la capa de transporte (TCP/UDP).
- Cada mensaje tiene puerto de origen y destino.
- El cliente se preconfigura para usar un puerto de destino ya registrado en Internet para cada servicio.
- Asignados y administrados por ICANN.
    - **Puertos Conocidos (1-1023):** Servicios comunes (FTP: 21, TFTP: 69, HTTP: 80 - web, SMTP: 25 - mensajes, DNS: 53 - traductor de nombres de dominio a IP).

    - **Puertos Registrados (1024-49151):** Usados por organizaciones para aplicaciones específicas (ej: IM).
    - **Puertos Privados/Dinámicos/Efímeros (49152-65535):** Generalmente puerto origen, uso libre por aplicaciones.
- Puerto origen: Generado dinámicamente (puerto efímero) para identificar una conversación.
- Puerto destino: Indica al servidor el servicio solicitado.

## Sockets

- Combinación de una dirección IP y un número de puerto (origen o destino).
- Generalmente, el puerto de origen es un puerto efímero (asignado dinámicamente).
- Permiten distinguir entre diferentes procesos en un cliente o conexiones a un servidor.

## El Comando `netstat`

- Muestra conexiones TCP activas.
- Informa: protocolos, direcciones (local/externa), puertos, estado. Permite identificar conexiones y seguridad.
- Se usa para enumerar: protocolos, dirección local y puertos, dirección extranjera y puertos, y el estado de la conexión.

# 16.2 Servicios de Aplicaciones de Red

### 16.2.1 Servicios de Aplicaciones de Red Comunes

- Servicios comunes: búsquedas, redes sociales, video/audio, compras, correo, mensajería.
- Dependen de TCP/IP para transmisión confiable.

**Servicios Comunes y sus Protocolos:**

- **DNS (Sistema de Nombres de Dominio):** Resuelve nombres de dominio a direcciones IP.
- **SSH (Secure Shell):** Acceso remoto seguro a servidores y dispositivos de red.
- **SMTP (Protocolo Simple de Transferencia de Correo):** Envía correos electrónicos y archivos adjuntos.
- **POP (Protocolo de Oficina de Correos):** Recupera correos electrónicos y archivos adjuntos.
- **IMAP (Protocolo de Acceso a Mensajes de Internet):** Recupera correos electrónicos y archivos adjuntos.
- **DHCP (Protocolo de Configuración Dinámica de Host):** Configura automáticamente la información IP.
- **HTTP (Protocolo de Transferencia de Hipertexto):** Solicita y transfiere páginas web.
- **FTP (Protocolo de Transferencia de Archivos):** Transferencia interactiva de archivos.

A continuación, una tabla que resume los protocolos más comunes y sus respectivos puertos y protocolos de transporte:

| Número de Puerto | Transporte | Protocolo de Aplicación |
|---|---|---|
| 20 | TCP | Protocolo de Transferencia de Archivos (FTP) - Datos |
| 21 | TCP | FTP - Control |
| 22 | TCP | Secure Shell (SSH) |
| 23 | TCP | Telnet |
| 25 | TCP | Protocolo Simple de Transferencia de Correo (SMTP) |
| 53 | UDP, TCP | Servicio de Nombres de Dominio (DNS) |
| 67 | UDP | Protocolo de Configuración Dinámica de Host (DHCP): Servidor |
| 68 | UDP | DHCP - Cliente |
| 69 | UDP | Protocolo Trivial de Transferencia de Archivos (TFTP) |
| 80 | TCP | Protocolo de Transferencia de Hipertexto (HTTP) |
| 110 | TCP | Protocolo de Oficina de Correos, versión 3 (POP3) |
| 143 | TCP | Protocolo de Acceso a Mensajes de Internet (IMAP) |
| 161 | UDP | Protocolo Simple de Administración de Redes (SNMP) |
| 443 | TCP | Protocolo Seguro de Transferencia de Hipertexto (HTTPS) |

# 16.3 Sistema de Nombres de Dominio (DNS)

- Los clientes DNS solicitan la dirección IP correspondiente a un nombre de dominio a los servidores DNS.
- DHCP usualmente configura el servidor DNS en redes domésticas a través del router.

### 16.3.3 Comprobador de Sintaxis — El Comando `nslookup`

- `nslookup` se utiliza para consultar servidores DNS y obtener la dirección IP asociada a un nombre de dominio.
- Ejemplo: Para obtener la dirección IP de www.cisco.com, un cliente DNS solicita al servidor DNS la dirección IP antes de enviar su solicitud HTTP.

## 16.4 HTTP y HTML

### 16.4.2 HTTP y HTML

- **HTTP (Hypertext Transfer Protocol):** Protocolo de transferencia de hipertexto para solicitar servicios web utilizando la dirección IP y el puerto 80.
- **HTML (Hypertext Markup Language):** Lenguaje de marcado utilizado para codificar el contenido de las páginas web, indicando al navegador cómo formatear la página, qué gráficos y fuentes usar.
- **HTTPS (HTTP Secure):** Versión segura de HTTP que utiliza protocolos de transporte seguros, enviando solicitudes al puerto 443.

## 16.5 Clientes y Servidores FTP

### 16.5.1 Protocolo de Transferencia de Archivos

- **FTP (File Transfer Protocol):** Método sencillo para transferir archivos entre computadoras. Permite subir y descargar archivos, y administrar archivos de forma remota (eliminar, renombrar).
- Utiliza dos puertos para la comunicación:
  - Puerto 21 (TCP): Conexión de control (solicitudes).
  - Puerto 20 (TCP): Transferencia de datos.
- El software cliente FTP viene incorporado en los sistemas operativos y en la mayoría de los exploradores Web.

## 16.6 Terminales Virtuales

### 16.6.2 Telnet

- **Telnet:** Protocolo para emulación de terminales basados en texto a través de la red.
  - Utiliza el puerto 23 (TCP).
  - Permite ejecutar comandos remotamente como si estuviera conectado localmente.
  - **Inseguro:** Transmite datos sin cifrar.

### 16.6.3 Problemas de Seguridad con Telnet

- **SSH (Secure Shell):** Alternativa segura a Telnet que proporciona:
  - Inicio de sesión remoto seguro.
  - Autenticación más sólida.
  - Transporte de datos cifrados.
- **Recomendación:** Usar SSH en lugar de Telnet siempre que sea posible.

## 16.7 Correo Electrónico y Mensajería

### 16.7.1 Clientes y Servidores de Correo Electrónico

- El correo electrónico es una aplicación cliente/servidor popular en Internet.
- Los buzones se identifican como: `usuario@empresa.dominio`
- Protocolos utilizados: SMTP, POP3 e IMAP4

### 16.7.2 Protocolos de Correo Electrónico

- **SMTP (Simple Mail Transfer Protocol):**
  - Utilizado para enviar correos electrónicos del cliente al servidor local y entre servidores.
  - Puerto 25.
- **POP3 (Post Office Protocol version 3):**
  - Recibe y almacena mensajes para sus usuarios.
  - Descarga los mensajes al cliente.

    - Puerto 110.
- **IMAP4 (Internet Message Access Protocol version 4):**
    - Recibe y almacena los mensajes.
    - Conserva los mensajes en el servidor a menos que el usuario los elimine.
    - Puerto 143.

### 16.7.3 Mensajería de Texto

- La mensajería de texto (mensajería instantánea, mensajes directos, etc.) permite la comunicación en tiempo real a través de Internet.

### 16.7.4 Llamadas Telefónicas por Internet

- La telefonía por Internet (VoIP) convierte señales de voz analógicas en datos digitales.
- Utiliza tecnología entre pares similar a la mensajería instantánea.
- Para llamadas a teléfonos convencionales (PSTN) se requiere una puerta de enlace.

## 17.1 Comandos de solución de problemas

### 17.1.1 Descripción General de los Comandos de Solución de Problemas

- Utilidades de software para identificar problemas de red, generalmente proporcionadas como comandos de línea de comandos (CLI).
- Sintaxis puede variar según el sistema operativo.
- **Utilidades comunes:**
    - `ipconfig`: Muestra información de configuración IP.
    - `ping`: Prueba conexiones con otros hosts IP.
    - `netstat`: Muestra las conexiones de red.
    - `tracert`: Muestra la ruta exacta recorrida hasta el destino.
    - `nslookup`: Solicita información sobre un dominio directamente a un servidor de nombres.

### 17.1.2 El comando `ipconfig`

- Permite visualizar la configuración IP actual de un host.
- **Opciones y uso:**

    - `ipconfig`: Muestra información básica: Dirección IP, máscara de subred y gateway predeterminado. Útil para verificar rápidamente la configuración IP actual.

```
C:\> ipconfig

Configuración IP de Windows


Ethernet adaptador Ethernet:

   Estado de los medios . . . . . . . . . . . : Medios desconectados
   Sufijo DNS específico de la conexión. :

Adaptador LAN inalámbrico Wi-Fi:

   Sufijo DNS específico de la conexión. : lan
   Dirección IPv6 de enlace local. . . . . : fe80::a1cc:4239:d3ab:2675%6
   Dirección IPv4. . . . . . . . . . . . . : 10.10.10.130
   Máscara de subred . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . . . . . : 10.10.10.1

C:\>
```

    - `ipconfig /all`: Muestra información detallada: Dirección MAC, direcciones IP de gateway y DNS, si DHCP está activado (e información relacionada). Útil para verificar si el DHCP asignó correctamente la configuración IP.

```
C:\> ipconfig/all
```

```
Configuración IP de Windows

  Host Name . . . . . . . . . . . . : your-a9270112e3
  Primary Dns Suffix . . . . . . . :
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No
  DNS Suffix Search List. . . . . . : lan

Ethernet adaptador Ethernet:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
  Physical Address. . . . . . . . . : 00-16-D4-02-5A-EC
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes

Adaptador LAN inalámbrico Wi-Fi:

  Connection-specific DNS Suffix . : lan
  Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
  Physical Address. . . . . . . . . : 00-13-02-47-8C-6A
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6(Preferred)
  IPv4 Address. . . . . . . . . . . : 10.10.10.130(Preferred)
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . . . . : Wednesday, September 2, 2020 10:03:43 PM
  Lease Expires . . . . . . . . . . : Friday, September 11, 2020 10:23:36 AM
  Default Gateway . . . . . . . . . : 10.10.10.1
  DHCP Server . . . . . . . . . . . : 10.10.10.1
  DHCPv6 IAID . . . . . . . . . . . : 98604135
  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-21-A5-84-44-A8-42-FC-0D-6F
  DNS Servers . . . . . . . . . . . : 10.10.10.1
  NetBIOS over Tcpip. . . . . . . . : Enabled

C:\>
```

- `ipconfig /release`: Libera la configuración DHCP actual (si la hay). Útil cuando un dispositivo necesita obtener una nueva configuración IP del servidor DHCP.
- `ipconfig /renew`: Solicita una nueva configuración IP del servidor DHCP. Útil cuando un dispositivo tiene una configuración IP incorrecta u obsoleta y necesita renovarla.

```
C:\> ipconfig/release

Configuración IP de Windows

No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adaptador Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :

Adaptador LAN inalámbrico Wi-Fi:

   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   Default Gateway . . . . . . . . . :

C:\> ipconfig /renew

Configuración IP de Windows
```

```
No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adaptador Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . :

Adaptador LAN inalámbrico Wi-Fi:

   Connection-specific DNS Suffix . : lan
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   IPv4 Address. . . . . . . . . . . : 10.10.10.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1

C:\>
```

- Si después de la configuración IP el host no puede obtener información actualizada del servidor DHCP, verifique la conexión física (luz de enlace).

### 17.1.4 El comando `ping`

- La mayoría de los dispositivos habilitados para IP admiten el comando `ping`.
- Prueba la conectividad de red, indicando si un host es accesible o no.
- Sintaxis: `ping` [dirección IP] o `ping` [nombre de host]
- Si el host de destino recibe la solicitud de eco (ICMP), responde con una respuesta de eco. La recepción de la respuesta de eco indica conectividad.
- Si se hace `ping` a un nombre, primero se resuelve la dirección IP con un servidor DNS. Un `ping` a la dirección IP sin resolución de DNS indica que la resolución de nombre está fallando.
- Si funciona el `ping` a la dirección IP, pero no funciona el `ping` al nombre, es muy probable que exista un problema con DNS.
- Si los comandos de `ping` enviados tanto al nombre como a la dirección IP son exitosos, pero el usuario aún no puede acceder a la aplicación, lo más probable es que el problema resida en la aplicación en el host de destino (no se está ejecutando, puerto bloqueado, etc.).
- Si no funciona ninguno de los dos comandos `ping`, el problema es la conectividad de red en la ruta hacia el destino. Probar el gateway predeterminado ayuda a aislar si el problema es local o externo.
- Un `ping` puede fallar debido a cortafuegos en el origen, destino o en la ruta.

## 17.1.5 Resultados de ping

- El comando `ping` básico suele enviar cuatro ecos.

## 17.2.1 ¿Qué aprendí en este módulo?

- `nslookup`: Directamente solicita al servidor de nombres información sobre un dominio de destino.
- `netstat`: Muestra las conexiones de red activas. Ayuda a identificar si una conexión es activa o no.

Glosario de Acrónimos y Siglas:

- **Servicios y Protocolos de Red:**
  - **UDP (User Datagram Protocol):** Protocolo de datagramas de usuario (protocolo rápido, no confiable).
  - **IP (Internet Protocol):** Protocolo de Internet (para enrutamiento).
- **Organizaciones y Estándares de Internet:**
  - **IANA (Internet Assigned Numbers Authority):** Asigna direcciones IP, números de sistema autónomo, etc.
  - **IEEE (Institute of Electrical and Electronics Engineers):** Instituto de Ingenieros Eléctricos y Electrónicos.
  - **IETF (Internet Engineering Task Force):** Fuerza de Tarea de Ingeniería de Internet.
  - **RFC (Request for Comments):** Petición de Comentarios (documentos técnicos de la IETF).
- **Interferencias de Medios de Red:**
  - **EMI (Electromagnetic Interference):** Interferencia Electromagnética.

- **RFI (Radio Frequency Interference):** Interferencia de Radiofrecuencia.