***Parte I: Conceptos y Teoría***

***1. El Mural de las Siete Capas***

Diagrama

El contenido generado por IA puede ser incorrecto.

***Capa 1: Física***

La **capa física** es el nivel más bajo del modelo OSI. Se encarga de la **transmisión de bits crudos** (0 y 1) a través de un medio físico. No entiende de estructuras lógicas ni de significado; su único objetivo es enviar y recibir señales eléctricas, ópticas o electromagnéticas que representen los datos.

* Define características como: voltajes, tipos de cables (coaxial, par trenzado, fibra óptica), conectores, duración de los impulsos, sincronización, etc.
* Establece los medios y normas para conectar dispositivos (hardware).
* No realiza verificación de errores.

**Ejemplos**: cables Ethernet, conectores RJ-45, señales de radio Wi-Fi, transmisiones de fibra óptica.

***Capa 2: Enlace de Datos***

La **capa de enlace de datos** crea una conexión directa entre dos dispositivos conectados físicamente. Su misión principal es **encapsular bits en tramas**, detectar errores en la transmisión y controlar el acceso al medio compartido (como una red Ethernet).

* Utiliza **direcciones MAC** para identificar dispositivos dentro de la misma red.
* Gestiona la detección y corrección de errores simples.
* Controla cuándo un dispositivo puede transmitir, evitando colisiones.

**Ejemplos**: protocolos Ethernet, Wi-Fi (IEEE 802.11), PPP, HDLC.

***Capa 3: Red***

La **capa de red** es responsable del **direccionamiento lógico y del encaminamiento de datos** entre redes distintas. Decide por qué camino deben viajar los datos para llegar de un punto A a un punto B, incluso si están en redes diferentes.

* Introduce el concepto de **direcciones IP**.
* Gestiona tablas de enrutamiento.
* Puede fragmentar paquetes grandes para adaptarlos al tamaño máximo de transmisión de cada red.

**Ejemplos**: IP (Internet Protocol), ICMP, IPsec, routers.

***Capa 4: Transporte***

La **capa de transporte** garantiza una **comunicación fiable de extremo a extremo** entre dispositivos, sin importar cuántas redes intermedias haya. Controla la integridad y el orden de los datos.

* Se encarga de la **segmentación** y **reensamblaje** de datos.
* Implementa mecanismos de **control de flujo** y **retransmisión en caso de pérdida**.
* Puede operar de forma fiable (TCP) o no fiable (UDP), según lo requiera la aplicación.

**Ejemplos**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

***Capa 5: Sesión***

La **capa de sesión** gestiona las **conexiones activas (sesiones)** entre aplicaciones. Es la encargada de establecer, mantener y finalizar sesiones de comunicación, permitiendo la sincronización y control de los datos que viajan entre ambas partes.

* Administra el inicio y cierre de sesiones.
* Permite múltiples sesiones simultáneas sin interferencia.
* Sincroniza el diálogo entre dispositivos (por ejemplo, videollamadas).

**Ejemplos**: NetBIOS, RPC (Remote Procedure Call), PPTP.

***Capa 6: Presentación***

La **capa de presentación** actúa como el **intérprete** del modelo OSI. Su objetivo es **traducir, cifrar o comprimir** los datos para que las capas superiores e inferiores se entiendan entre sí.

* Traduce entre diferentes formatos de datos (por ejemplo, de ASCII a binario).
* Realiza cifrado para seguridad (SSL/TLS).
* Comprime datos para mejorar la eficiencia de la transmisión.

**Ejemplos**: JPEG, MPEG, SSL/TLS, codificaciones de caracteres (ASCII, UTF-8).

***Capa 7: Aplicación***

La **capa de aplicación** es la más cercana al usuario. Proporciona **servicios y protocolos de red directamente a las aplicaciones** (como el navegador o el correo).

* Permite a los usuarios interactuar con la red.
* Utiliza protocolos que permiten transferencias de archivos, navegación web, envío de correos, etc.
* Es la única capa que **interactúa directamente con el software del usuario**.

**Ejemplos**: HTTP, FTP, SMTP, DNS, POP3.

***2. Los Dos Pergaminos del Mensajero***

Imagen que contiene Diagrama

El contenido generado por IA puede ser incorrecto.

***TCP (Transmission Control Protocol)***

Este protocolo es **orientado a conexión**, lo que significa que antes de comenzar a transmitir datos, el emisor y el receptor deben establecer una conexión mediante un proceso llamado **"three-way handshake"** (saludo de tres pasos: SYN, SYN-ACK, ACK).

Durante la comunicación:

* Cada mensaje enviado espera una confirmación del receptor (ACK).
* Si el emisor no recibe respuesta, **retransmite** el mensaje.
* TCP también realiza el **reordenamiento** de los datos y **control de flujo** para evitar saturar al receptor.

**Ventajas de TCP**:

* Alta fiabilidad: garantiza que los datos lleguen completos y en orden.
* Reintentos automáticos ante pérdida.
* Control de congestión y flujo.

**Desventajas de TCP**:

* **Mayor latencia**: por las confirmaciones y el establecimiento de conexión.
* **Mayor carga** por la cabecera y el control adicional.

**Usos comunes**: navegación web (HTTP/HTTPS), transferencia de archivos (FTP), correos electrónicos (SMTP, IMAP), bases de datos.

***UDP (User Datagram Protocol)***

El protocolo **UDP** es **no orientado a conexión**. El emisor envía los datos **sin esperar confirmación**, sin handshake previo, ni control de errores ni de flujo.

Este protocolo se caracteriza por ser extremadamente **rápido y ligero**, aunque sacrifica la fiabilidad.

**Ventajas de UDP**:

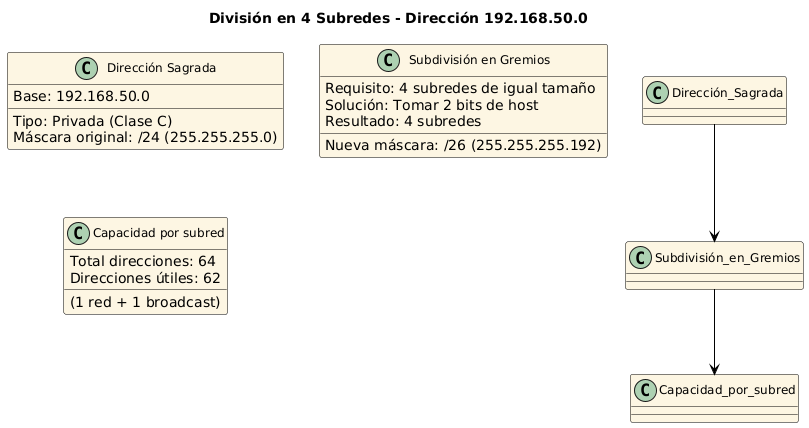
* **Baja latencia**: ideal para comunicaciones en tiempo real.
* **Menor carga**: por no tener cabeceras complejas ni gestión de conexión.
* Permite una mayor velocidad de transmisión en aplicaciones que pueden tolerar cierta pérdida de datos.

**Desventajas de UDP**:

* **No garantiza entrega**: los paquetes pueden perderse sin aviso.
* **No hay orden**: los datos pueden llegar desordenados.
* **No hay control de congestión**.

**Usos comunes**: llamadas por voz (VoIP), streaming de video en vivo, videojuegos online, DNS.

***3. El Enigma de las Subredes***



***Cálculo de la máscara de subred***

Para dividir en 4 subredes necesitamos encontrar cuántos bits extra debemos "pedir prestados" a la parte de host:

* 2² = 4 subredes → Necesitamos tomar **2 bits del campo de host**.
* La nueva máscara será:  
  24 (original) + 2 (prestados) = /26

Esto nos da una máscara **/26**, es decir:

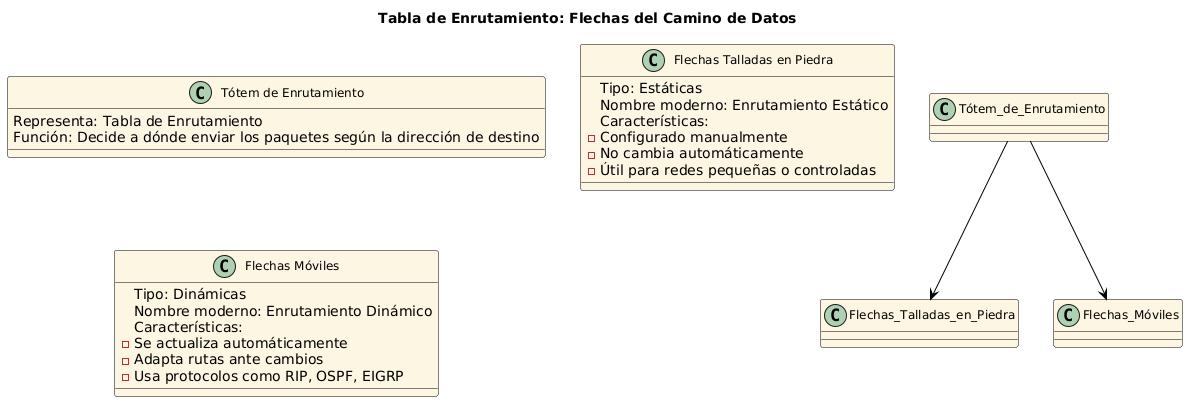
* **255.255.255.192**  
  (porque los 2 bits nuevos valen: 11000000 = 192 en decimal)

***Cálculo de direcciones por subred***

Con una máscara /26 tenemos **6 bits para hosts** (32 – 26):

* **2⁶ = 64 direcciones por subred**
* Pero recordemos que:
  + 1 dirección es para la red (ej. 192.168.50.0)
  + 1 dirección es para broadcast (ej. 192.168.50.63)
* Por tanto, quedan **62 direcciones utilizables por subred**.

***4. La Encrucijada de las Rutas***



***El tótem: una tabla de enrutamiento***

El tótem en el centro de la encrucijada representa de forma simbólica una **tabla de enrutamiento**, un componente esencial en **routers modernos**. Esta tabla contiene información sobre las posibles rutas que un paquete de datos puede tomar para llegar a su destino.

Cada entrada en la tabla incluye:

* Una **dirección de destino** (red o subred)
* Una **máscara de red**
* La **puerta de enlace siguiente** (next hop)
* La **interfaz de salida**
* Y, en el caso del enrutamiento dinámico, una **métrica o costo** asociado

Cuando un router recibe un paquete, consulta su tabla de enrutamiento y **elige la mejor ruta disponible** según los datos del encabezado IP.

***Flechas talladas en piedra: Enrutamiento Estático***

Estas flechas representan rutas configuradas manualmente. En el mundo actual, se conocen como rutas estáticas.

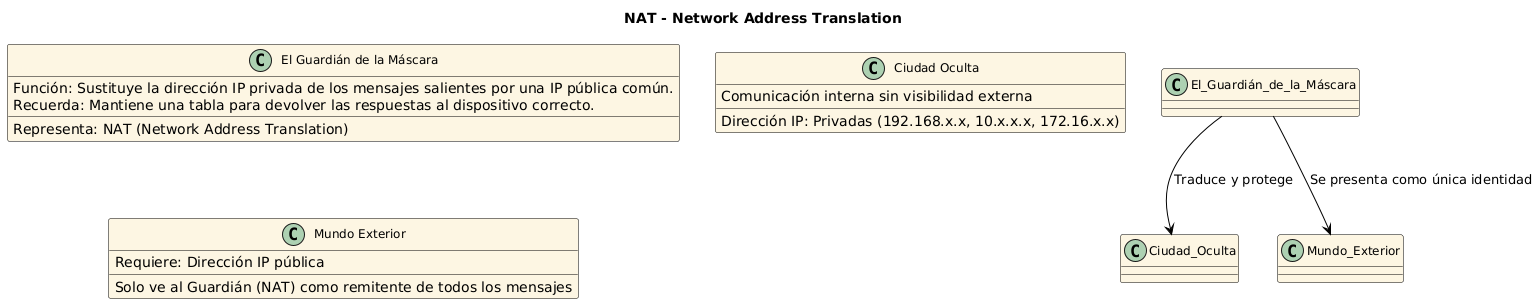
* Características:
  + No cambian automáticamente si una ruta falla.
  + Son ideales para entornos pequeños, seguros y predecibles.
  + El administrador debe agregar, cambiar o eliminar las rutas manualmente.
* Ventajas:
  + Predecibles y seguras.
  + Sin sobrecarga de procesamiento.
* Desventajas:
  + No se adaptan a cambios en la red.
  + Difíciles de mantener en redes grandes.

***Flechas móviles: Enrutamiento Dinámico***

Estas flechas representan **rutas que pueden cambiar automáticamente** si hay un cambio en la topología. Se trata del **enrutamiento dinámico**, gestionado por **protocolos de enrutamiento**.

* **Características**:
  + La tabla de enrutamiento se actualiza de forma **automática y continua**.
  + Los routers comparten información con otros routers.
  + Se ajustan a **fallos de enlaces o cambios de red**.
* **Protocolos comunes**:
  + **RIP** (Routing Information Protocol)
  + **OSPF** (Open Shortest Path First)
  + **EIGRP** (Enhanced Interior Gateway Routing Protocol)
* **Ventajas**:
  + Adaptación automática ante cambios.
  + Ideal para **redes grandes y complejas**.
* **Desventajas**:
  + Mayor complejidad.
  + Requiere procesamiento adicional.

***5. El Guardián de la Máscara Única***



***¿Qué representa el Guardián de la Máscara?***

El guardián con dos caras de la leyenda representa la técnica moderna llamada **NAT (Network Address Translation)**, o **Traducción de Direcciones de Red**.

Esta técnica permite que múltiples dispositivos dentro de una **red privada** (la ciudad oculta) compartan una **única dirección IP pública** al comunicarse con el exterior (el mundo más allá de las murallas).

***¿Cómo funciona NAT?***

1. **Al salir un mensaje**:
   * El router NAT sustituye la **IP privada** del dispositivo por la **IP pública** del router.
   * Además, guarda un **registro (tabla NAT)** de qué puerto privado generó la solicitud.
2. **Al llegar la respuesta**:
   * El router NAT **consulta su tabla** para saber a qué IP privada y puerto debe reenviar la respuesta.
   * Así, cada mensaje vuelve a su verdadero origen dentro de la red.

**Ejemplo**:

* Dispositivo A (192.168.1.10) quiere acceder a un servidor web externo.
* NAT cambia su IP a la pública (ej. 80.80.80.1) y le asigna un puerto (ej. 5001).
* El servidor responde a 80.80.80.1:5001, y NAT sabe que debe enviarlo de vuelta a 192.168.1.10.

***¿Qué beneficios brinda NAT?***

1. **Ahorro de direcciones IPv4**
   * Gracias a NAT, **cientos de dispositivos** pueden compartir **una sola IP pública**.
   * Esto es crucial dada la escasez de direcciones IPv4 disponibles.
2. **Seguridad adicional**
   * Los dispositivos con IP privada **no son accesibles directamente** desde Internet.
   * Esta capa de ocultamiento actúa como un **filtro o escudo** frente a ataques externos.