Examen de Redes II – *En Busca de la Red Perdida*

Parte I: Conceptos y Teoría

Rodrigo Yepes Rubio

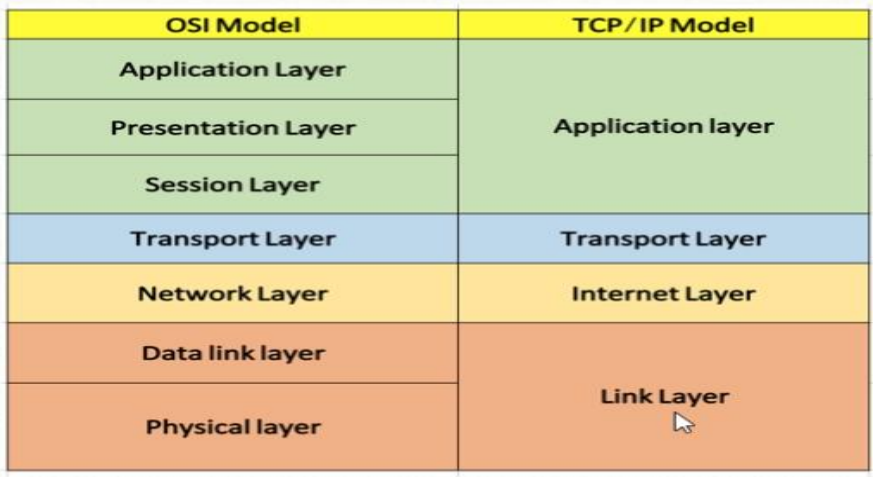
Pregunta 1:

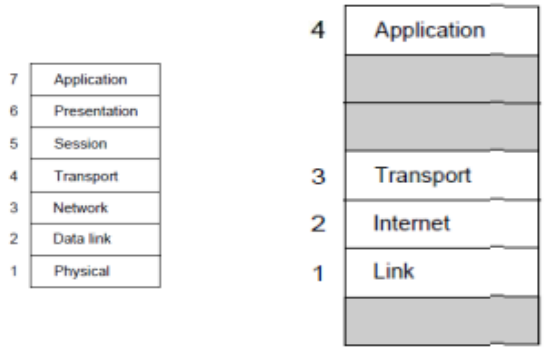
El mural de las siete capas representa el Modelo OSI (Open Systems Interconnection), un esquema conceptual que describe cómo los datos viajan desde un dispositivo a otro a través de una red. Este modelo es fundamental en la teoría de las redes de comunicación modernas, aunque en la práctica, el Modelo TCP/IP es el más utilizado hoy en día.

Cada franja del mural simboliza una capa del Modelo OSI, donde un mensaje se transforma y refina hasta llegar a su destino. Aquí están las siete capas y su relación con la comunicación de datos actual:

1. Capa Física – Representa el medio físico (cables, ondas de radio) por el cual viajan los datos en forma de señales eléctricas, ópticas o inalámbricas.
2. Capa de Enlace de Datos – Asegura que los datos viajen sin errores entre dos nodos conectados en la misma red, usando direcciones MAC.
3. Capa de Red – Determina la ruta que seguirán los datos para llegar a su destino, utilizando direcciones IP y protocolos como el ICMP.
4. Capa de Transporte – Garantiza que los datos lleguen de manera confiable y en el orden correcto, empleando protocolos como TCP o UDP.
5. Capa de Sesión – Establece, mantiene y finaliza sesiones de comunicación entre dispositivos.
6. Capa de Presentación – Se encarga de la codificación y cifrado de los datos para que puedan ser interpretados correctamente por la capa de aplicación.
7. Capa de Aplicación – Es la interfaz entre el usuario y la red, donde operan protocolos como HTTP, FTP o SMTP.

El modelo TCP/IP, usado en Internet, simplifica estas capas en cuatro niveles funcionales: Acceso a red, Internet, Transporte y Aplicación, pero sigue la misma lógica del mural: transformar y transmitir información eficazmente. Así, esta antigua civilización entendía un principio esencial de la comunicación de datos moderna: la transmisión de información requiere procesos estructurados para asegurar su correcto envío, recepción y comprensión. A continuación, muestro una tablan que relaciona las capas de ambos modelos:





Como podemos observar el modelo TCP/IP optimiza las capas de aplicación donde incluye la capa de presentación y de sesión, y la capa de acceso a red que incluye las capas física y de enlace de datos. Por lo que el modelo TCP/IP se utiliza más actualmente porque es el que realmente funciona en el internet y las redes modernas, al ser más simple, eficiente y práctico. Y el modelo OSI se ha quedado como referencia para aprender sobre el funcionamiento de las redes de manera teórica.

Pregunta 2:

El mensajero confiable lo podemos relacionar con el TCP (Transmission Control Protocol), mientras que el mensajero veloz lo podemos relacionar con el UDP (User Datagram Protocol).

Los protocolos TCP y UDP son protocolos de transporte que permiten la comunicación entre dispositivos en una red, como Internet.

- TCP: Es un protocolo fiable que garantiza que los datos lleguen completos y en orden. Se usa en aplicaciones como navegación web, correos electrónicos y transferencias de archivos, donde la precisión es clave.
- UDP: Es un protocolo rápido, pero sin garantía de entrega, ideal para aplicaciones en tiempo real como videollamadas, streaming y videojuegos en línea, donde la velocidad es más importante que la exactitud.

A continuación, comparo y contrasto ambos protocolos en términos de:

- Orientación a conexión:
    - TCP: Orientado a conexión: Establece una conexión antes de transmitir datos, asegurando que ambos extremos están listos para la comunicación.
    - UDP: No orientado a conexión: No establece una conexión previa, simplemente envía los datos sin verificar si el receptor está listo.
- Fiabilidad y control de errores:
    - TCP: Fiable: Garantiza la entrega de datos sin errores, en el orden correcto y sin pérdidas. Utiliza mecanismos de control de flujo y retransmisión de paquetes perdidos.
    - UDP: No fiable: No garantiza la entrega de datos ni el orden. No tiene mecanismos de control de flujo ni retransmisión de paquetes perdidos.
- Velocidad y orden de entrega:
    - TCP: Velocidad: Más lento debido a los mecanismos de control de errores y la necesidad de establecer una conexión. Orden de entrega: Garantiza que los datos se entreguen en el orden correcto.
    - UDP: Velocidad: Más rápido porque no establece conexión ni realiza control de errores. Orden de entrega: No garantiza el orden de entrega de los datos.

En resumen, TCP es adecuado para aplicaciones que requieren fiabilidad y orden en la entrega de datos, mientras que UDP es preferido para aplicaciones que necesitan velocidad y pueden tolerar cierta pérdida de datos.

Pregunta 3:

Para dividir la red 192.168.50.0 en 4 subredes de igual tamaño, debemos determinar la máscara de subred adecuada.

Paso 1: Identificar la red original

La dirección 192.168.50.0 pertenece a la clase C, cuya máscara predeterminada es /24 (255.255.255.0). Esto significa que la red original tiene 256 direcciones disponibles (2^8 = 256).

Paso 2: Determinar la máscara necesaria para 4 subredes

Para crear 4 subredes, necesitamos dividir el rango original en 4 partes iguales.

- En binario, esto se logra tomando bits prestados de la parte de host.
- Con 2 bits adicionales en la máscara de subred, obtenemos 2^2 = 4 subredes.
- Esto cambia la máscara de /24 a /26, lo que equivale a 255.255.255.192.

Paso 3: Calcular el tamaño de cada subred

Con una máscara /26, quedan 6 bits para hosts en cada subred.

- El total de direcciones por subred es 2^6 = 64.
- Sin embargo, cada subred debe reservar:
    - 1 dirección para la red (primera dirección).
    - 1 dirección para el broadcast (última dirección).
- Por lo tanto, las direcciones de host utilizables en cada subred son:

  64 - 2 = 62

Paso 4: Verificar las subredes resultantes

Las cuatro subredes con máscara /26 son:

1. 192.168.50.0/26 → Hosts: 192.168.50.1 - 192.168.50.62 / Broadcast: 192.168.50.63
2. 192.168.50.64/26 → Hosts: 192.168.50.65 - 192.168.50.126 / Broadcast: 192.168.50.127
3. 192.168.50.128/26 → Hosts: 192.168.50.129 - 192.168.50.190 / Broadcast: 192.168.50.191
4. 192.168.50.192/26 → Hosts: 192.168.50.193 - 192.168.50.254 / Broadcast: 192.168.50.255

Conclusión

La máscara de subred adecuada es /26 (255.255.255.192).
Cada subred resultante tiene 62 direcciones de host utilizables, asegurando una misma distribución entre los cuatro gremios.

Pregunta 4:

El tótem con flechas que apuntas hacia los caminos de las aldeas representa un concepto moderno de redes: una tabla de enrutamiento. Esta tabla es utilizada por los routers para dirigir el tráfico de datos a través de la red, seleccionando la mejor ruta hacia el destino.

Una tabla de enrutamiento es una base de datos que contiene información sobre cómo llegar a diferentes redes o destinos dentro de una red. Esta tabla incluye detalles sobre las direcciones IP de destino y las máscaras de subred correspondientes, así como la interfaz o puerta de enlace por la cual el tráfico debe ser enviado para llegar a ese destino.

Cuando un router recibe un paquete de datos, consulta su tabla de enrutamiento para determinar cuál es la mejor ruta hacia el destino del paquete. Esto le permite reenviar el paquete en la ruta correcta.

Enrutamiento Estático vs. Enrutamiento Dinámico:

Las flechas fijas en el tótem tallado representan el concepto de enrutamiento estático. En el enrutamiento estático, las rutas son configuradas manualmente por el administrador de la red y no cambian automáticamente. Son fijas y no se actualizan a menos que el administrador modifique la tabla. Esto es útil en redes pequeñas y simples donde las rutas no cambian frecuentemente.

Las flechas móviles representan el enrutamiento dinámico, en el cual el router puede cambiar las rutas automáticamente basándose en la información recibida de otros routers a través de protocolos de enrutamiento dinámico, como RIP (Routing Information Protocol), OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol). Estas rutas se ajustan automáticamente en función de la carga de la red, la congestión, o la disponibilidad de enlaces, permitiendo que el tráfico se redirija por las rutas más eficientes en tiempo real.

Diferencias entre enrutamiento estático y dinámico:

1. Enrutamiento Estático (Flechas Fijas):
    - Las rutas son configuradas manualmente.
    - No cambian a menos que el administrador las modifique.
    - Es adecuado para redes pequeñas y predecibles.
2. Enrutamiento Dinámico (Flechas Móviles):
    - Las rutas se ajustan automáticamente en función de las condiciones de la red.
    - Se utilizan protocolos de enrutamiento para actualizar las rutas.
    - Es adecuado para redes grandes y complejas que requieren adaptabilidad.

Conclusión:

El tótem con flechas representa una tabla de enrutamiento moderna, que dirige el tráfico de datos hacia el destino adecuado. La diferencia entre las flechas fijas y móviles simboliza las diferencias entre enrutamiento estático (fijo) y enrutamiento dinámico (móvil), donde el enrutamiento estático es más rígido y predefinido, mientras que el dinámico permite flexibilidad y adaptabilidad ante cambios en la red.

Pregunta 5:

La leyenda del Guardián de la Máscara refleja una NAT (Network Address Translation), específicamente una técnica llamada NAT sobrecargado o PAT (Port Address Translation).

NAT es una técnica que permite a una red privada compartir una única dirección IP pública cuando se comunica con redes externas, como Internet. En lugar de asignar una dirección IP única a cada dispositivo dentro de una red privada, el router o dispositivo de red reemplaza las direcciones IP internas de los dispositivos por la dirección IP pública del router cuando los mensajes salen. Además, mantiene un registro de qué dispositivo interno envió cada mensaje para que las respuestas puedan ser reenviadas correctamente a la máquina adecuada dentro de la red.

En el caso de la leyenda, el Guardián reemplaza la "máscara" del mensajero con la suya propia, asegurándose de que todas las comunicaciones externas parezcan provenir de una única fuente (el Guardián, o en términos de red, la dirección IP pública), mientras mantiene la correspondencia interna para reenviar las respuestas al destinatario correcto.

Beneficios de esta estrategia:

1. Seguridad y anonimato: NAT oculta las direcciones IP internas de los dispositivos, lo que aumenta la seguridad evitando que los dispositivos dentro de la red sean accesibles desde el exterior. Solo la IP pública es visible para los dispositivos externos.
2. Conservación de direcciones IP: Al permitir que varios dispositivos de una red privada compartan una sola dirección IP pública, NAT ayuda a conservar direcciones IP, algo muy valioso, dado que las direcciones IPv4 son limitadas.

Conclusión:

La leyenda del Guardián de la Máscara es una representación de NAT, que permite a una red interna ocultar la identidad de sus dispositivos y compartir una única dirección IP al comunicarse con el mundo exterior. Esta técnica proporciona beneficios como mayor seguridad y conservación de direcciones IP, lo que es necesario en las redes modernas.

Referencias

Pregunta 1:

- Tema 1 – Introducción a las redes de ordenadores, Tema 1 – Introducción a las redes de ordenadores, Redes, Ingeniería Informática UAX
- Curso_Redes_Ordenadores, rubences, Github

Pregunta 2:

- Tema 5 – Capa de Transporte, Tema 5 – Capa de Transporte, Redes, Ingeniería Informática UAX

Pregunta 3:

- Tema 4 – Capa de Red, Tema 4 – Capa de Red, Redes, Ingeniería Informática UAX
- Curso_Redes_Ordenadores, rubences, Github

Pregunta 4:

- Tema 4 – Capa de Red, Tema 4 – Capa de Red, Redes, Ingeniería Informática UAX
- Tema 4 – Capa de Red, Encaminamiento Dinámico, Redes, Ingeniería Informática UaX

Pregunta 5:

- Tema 4 – Capa de Red, NAT, Redes Ingeniería Informática UAX