

EXAMEN REDES

PREGUNTA 1:

Según el enunciado de este acertijo interpreto este modelo como el actual modelo OSI el cual se divide en capas, cada una con una función específica para asegurar que un mensaje llegue correctamente a su destino. Este modelo se divide en 7 capas:

Capa Física – Representa la infraestructura básica de comunicación, como cables y señales eléctricas. En el mural, sería la base del mensaje, la forma más primitiva de la comunicación.

Capa de Enlace de Datos – Garantiza la transmisión libre de errores entre dispositivos. Se relaciona con cómo los sabios aseguraban que los símbolos fueran entendidos sin errores.

Capa de Red – Maneja el direccionamiento y el encaminamiento del mensaje. En el mural, esto representaría el proceso de guiar el mensaje a su destino correcto.

Capa de Transporte – Garantiza que los datos lleguen completos y en orden. Se asemeja a cómo el mensaje se refina para mantener su integridad a medida que avanza.

Capa de Sesión – Administra las interacciones entre emisores y receptores. Podría representar la estructura del ritual de comunicación en la civilización antigua.

Capa de Presentación – Traduce y adapta los datos para que sean comprensibles. Esto refleja la interpretación y conversión de símbolos en el mural.

Capa de Aplicación – Es la interacción final con el usuario. En el mural, es el mensaje en su forma final, listo para ser comprendido por su destinatario.

PREGUNTA 2:

Los dos pergaminos del mensajero se pueden interpretar como los protocolos TCP y UDP siendo el protocolo TCP el Mensajero confiable y el protocolo UDP el Mensajero veloz. Comparando los anteriores protocolos encunto a sus ventajas y desventajas podemos decir que:

PROTOCOLO TCP:

- **Ventajas de TCP:**
 - Garantiza la entrega de los datos en orden y sin errores.
 - Es ideal para aplicaciones como navegación web, correos electrónicos y transferencia de archivos, donde la precisión es clave.
- **Desventajas de TCP:**
 - Introduce latencia debido a su mecanismo de confirmación y reenvío.
 - Consume más recursos porque mantiene la conexión y el control de errores.

PROTOCOLO UDP:

- **Ventajas de UDP:**
 - Es rápido y eficiente, ya que no tiene sobrecarga de control.
 - Se usa en aplicaciones donde la velocidad es más importante que la fiabilidad, como transmisión de video en vivo, juegos en línea y VoIP.
- **Desventajas de UDP:**
 - No garantiza que los mensajes lleguen ni que lo hagan en orden.
 - Puede generar pérdida de paquetes en redes congestionadas.

PREGUNTA 3:

1: Identifico la máscara base

La dirección 192.168.50.0 pertenece a la clase C, que por defecto usa la máscara 255.255.255.0 (/24), lo que equivale a 256 direcciones (0-255).

2: Determino cuántos bits se necesitan para dividir en 4 subredes

Para crear 4 subredes, se necesitan 2 bits adicionales en la parte de la subred, porque:

$$2^2=4 \text{ subredes}$$

Esto significa que extendemos la máscara original /24 a /26, lo que da una nueva máscara:

255.255.255.192

(porque 192 en binario es 11000000, reservando 2 bits para la subred).

3: Calculo el tamaño de cada subred

Con /26, cada subred tiene un bloque de 64 direcciones:

$$2^{(32-26)}=64$$

De estas, 2 direcciones no son utilizables (una para la red y otra para el broadcast), lo que deja:

$$64-2=62 \text{ direcciones de host utilizables por subred.}$$

Resultado

Los antiguos habrían usado la máscara /26 (255.255.255.192) para dividir la red en 4 subredes, cada una con 62 direcciones de host utilizables.

Las subredes serían:

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 civilización digital antigua habría usado /26 (255.255.255.192) para

dividir su reino en 4 distritos iguales, asegurando 62 direcciones de host por subred.

PREGUNTA 4:

El tótem de la encrucijada representa una tabla de enrutamiento.

¿Qué es una tabla de enrutamiento?

Una tabla de enrutamiento es un conjunto de reglas que los routers usan para decidir cómo enviar los paquetes de datos a su destino, es como un mapa que le indica al router qué camino tomar para alcanzar diferentes redes. Contiene entradas con:

- Red de destino (hacia dónde enviar el paquete).
- Máscara de subred (para identificar el tamaño de la red).
- Próximo salto (otro router si el destino no está en la misma red).
- Interfaz de salida (por dónde enviar el paquete).

Cuando un router recibe un paquete, consulta su tabla de enrutamiento y sigue la mejor ruta posible.

Diferencia entre las flechas talladas en piedra y las móviles

- Flechas Talladas en Piedra - Enrutamiento Estático
 - Son caminos fijos definidos manualmente.
 - No cambian automáticamente si un camino deja de estar disponible.
 - Son confiables en redes pequeñas pero poco flexibles ante cambios.
 - Ejemplo: un administrador configura una ruta fija para alcanzar una red específica.
- Flechas Móviles - Enrutamiento Dinámico
 - Se adaptan automáticamente si las condiciones de la red cambian.
 - Usan protocolos como RIP, OSPF o BGP para actualizar rutas en tiempo real.

- Son esenciales en redes grandes y cambiantes.
- Ejemplo: si un camino se cierra (fallo de enlace), el router encuentra otra ruta sin intervención manual.

PREGUNTA 5:

El Guardián de la máscara única representa la técnica NAT.

LA NAT:

NAT (Traducción de Direcciones de Red) es un mecanismo en los routers que sustituye las direcciones IP privadas de los dispositivos internos por una única dirección IP pública al salir de la red. Luego, cuando las respuestas regresan, NAT recuerda qué dispositivo interno originó cada solicitud y le reenvía la respuesta adecuadamente.

Este proceso se asemeja al Guardián de la Máscara, quien oculta la identidad de los mensajeros y gestiona sus respuestas correctamente.

¿Cómo funciona la NAT?

1. Un dispositivo dentro de la red interna (por ejemplo, 192.168.1.10) envía una solicitud a Internet.
2. El router con NAT cambia la dirección de origen por la dirección IP pública de la red (por ejemplo, 203.0.113.1).
3. Cuando el servidor externo responde a la IP pública, el router traduce la dirección de regreso y envía la respuesta al dispositivo correcto.

2beneficios de NAT en redes modernas

- Ahorro de direcciones IP:

Permite que muchos dispositivos usen una sola IP pública, lo cual es crucial debido a la escasez de direcciones IPv4.

- Seguridad y privacidad:

Ocultar las direcciones IP internas, dificultando que dispositivos externos accedan directamente a los equipos dentro de la red.