

GUÍA DE ESTUDIO: NETWORK LAYER

Martín Gómez Caicedo

1. ¿Cuáles son las dos funciones básicas de la capa de red? Explique brevemente cada una de ellas.

Las dos funciones básicas de la capa de red son el enrutamiento y el reenvío. El enrutamiento implica determinar la mejor ruta para enviar datos desde el origen al destino a través de una red. El reenvío implica tomar los datos recibidos y enviarlos al destino basado en la información de enrutamiento.

2. ¿Qué define un modelo de servicio de red?

Un modelo de servicio de red define las características y comportamientos que proporciona una red a las aplicaciones y usuarios que la utilizan. Esto incluye aspectos como la calidad de servicio, la confiabilidad, la seguridad y la disponibilidad.

3. ¿Cuáles servicios puede prestar la red a un PAQUETE?

La red puede proporcionar servicios como enrutamiento, conmutación, encapsulación, fragmentación y desfragmentación de paquetes, entre otros.

4. ¿Cuáles servicios puede prestar la red a un FLUJO DE PAQUETES?

La red puede proporcionar servicios como la gestión de la congestión, la calidad de servicio (QoS), la priorización del tráfico, la segmentación y el reensamblaje de paquetes, entre otros.

5. ¿En qué consiste el servicio de MEJOR ESFUERZO que presta IP?

El servicio de mejor esfuerzo que presta IP implica que la red hará todo lo posible para entregar los paquetes, pero no garantiza ningún tipo de calidad de servicio o priorización.

6. Averigüe la estructura del encabezado de un datagrama IP. ¿Cuántos y cuáles campos tiene?

El encabezado de un datagrama IP consta de varios campos, incluyendo versión, longitud de encabezado, tipo de servicio, longitud total, identificación, banderas, desplazamiento de fragmento, tiempo de vida, protocolo, suma de comprobación, dirección IP de origen, dirección IP de destino, opciones (variable) y datos.

7. ¿En cuántas y cuáles partes se divide una dirección IPv4?

Una dirección IPv4 se divide en dos partes: la parte de red y la parte de host.

Parte de red:

Esta parte de la dirección IPv4 identifica la red a la que pertenece un dispositivo. Los bits en esta sección son consistentes para todos los dispositivos en la misma red. La longitud de esta parte de red depende del tamaño de la red y está determinada por la máscara de subred.

Parte de host:

Esta parte de la dirección IPv4 identifica de manera única a un dispositivo dentro de una red específica. Los bits en esta sección pueden variar entre diferentes dispositivos dentro de la misma red, ya que se utilizan para identificar los hosts individuales en esa red.

8. ¿Por qué el identificador de host no puede ser 0, ni 255?

El identificador de host no puede ser 0 ni 255 porque 0 se reserva para la dirección de red y 255 se reserva para la dirección de difusión.

9. ¿Cuántas redes clase A hay? ¿Cuántos hosts puede tener una red clase A?

Las redes clase A van desde 1.0.0.0 hasta 126.0.0.0. Hay un total de 126 redes clase A. Una red clase A utiliza un octeto para la parte de red y tres octetos para la parte de host. Esto da lugar a $2^{24} - 2$ direcciones de host por red, ya que se reservan una dirección para la red y otra para la difusión. Por lo tanto, una red clase A puede tener hasta 16,777,214 hosts.

10. ¿Cuántas redes clase B hay? ¿Cuántos hosts puede tener una red clase B?

Las redes clase B van desde 128.0.0.0 hasta 191.255.0.0. Hay un total de 16,384 redes clase B. Una red clase B utiliza dos octetos para la parte de red y dos octetos para la parte de host. Esto da lugar a $2^{16} - 2$ direcciones de host por red, ya que se reservan una dirección para la red y otra para la difusión. Por lo tanto, una red clase B puede tener hasta 65,534 hosts.

11. ¿Cuántas redes clase C hay? ¿Cuántos hosts puede tener una red clase C?

Las redes clase C van desde 192.0.0.0 hasta 223.255.255.0. Hay un total de 2,097,152 redes clase C. Una red clase C utiliza tres octetos para la parte de red y un octeto para la parte de host. Esto da lugar a $2^8 - 2$ direcciones de host por red, ya que se reservan una dirección para la red y otra para la difusión. Por lo tanto, una red clase C puede tener hasta 254 hosts.

12. ¿Cuáles son las dos razones para emplear subnetting?

Las dos razones principales para emplear subnetting son la conservación de direcciones IP y la segmentación de redes para mejorar el rendimiento y la seguridad.

Conservación de direcciones IP:

El subnetting permite asignar direcciones IP de manera más eficiente. En lugar de asignar una gran red a una organización, se pueden asignar múltiples subredes más pequeñas, lo que permite

un uso más eficiente de las direcciones IP disponibles. Esto es particularmente útil en entornos donde las direcciones IP son limitadas, como en organizaciones grandes o proveedores de servicios de Internet.

Segmentación de redes:

El subnetting permite segmentar una red en subredes más pequeñas con el fin de mejorar la gestión y el rendimiento de la red. Al dividir una red en subredes más pequeñas, se puede mejorar el rendimiento al reducir el tráfico de broadcast y aumentar la eficiencia del enrutamiento. Además, la segmentación de redes puede proporcionar un mejor control de acceso y seguridad al limitar la comunicación entre subredes específicas y al implementar políticas de seguridad a nivel de subred.

13. ¿Cuál es la función de la máscara de subred?

La máscara de subred se utiliza para identificar qué parte de una dirección IP se refiere a la red y qué parte se refiere al host.

14. ¿Cómo funciona la notación de prefijo para especificar la máscara de subred?

La notación de prefijo indica cuántos bits se utilizan para la parte de red de una dirección IP. Por ejemplo, /24 indica que los primeros 24 bits se utilizan para la parte de red y los últimos 8 bits para la parte de host.

15. ¿Para qué se emplean las direcciones privadas?

Las direcciones privadas se utilizan para redes internas dentro de organizaciones y no están directamente conectadas a Internet. Permiten a las organizaciones utilizar direcciones IP únicas dentro de sus redes internas sin conflicto con direcciones IP públicas en Internet.

16. Determine la dirección IP que su computador adquiere en su casa. Determine también la dirección IP que su computador adquiere cuando se conecta a la red PÚBLICA de la universidad.

17. ¿Para qué se emplea la técnica de NAT?

La técnica de NAT (Network Address Translation) se emplea para traducir direcciones IP privadas en una red interna a una dirección IP pública utilizada en Internet. Esto permite que múltiples dispositivos en una red privada compartan una única dirección IP pública para acceder a Internet. Además, NAT proporciona una capa adicional de seguridad al ocultar las direcciones IP internas de la red privada.