¿Cuál es una de las funciones principales de la información de tráiler que agrega la encapsulación de la capa de enlace de datos?

Seleccione una:

a. Asegura el arribo ordenado de datos

X b. Admite la detección de errores.

c. Identifica los servicios en la red local.

d. Proporciona el envío al destino correcto.

Una de las funciones principales de la información de tráiler que agrega la encapsulación de la capa de enlace de datos es la identificación de los servicios en la red local. La información de tráiler se agrega al final de cada trama en la capa de enlace de datos, y esta información incluye campos que identifican el tipo de trama, la dirección del destinatario y la dirección del remitente, entre otros detalles. Esto permite que los dispositivos en la red local puedan identificar a qué servicio o dispositivo está dirigida una trama y reenviarla al destino correcto.

Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios, seleccione la respuesta correcta

Seleccione una:

a. Rendimiento, confiabilidad, baja latencia y seguridad

X b. tolerancia a fallas, escalabilidad, calidad del servicio y seguridad

c. Confiabilidad, baja latencia, tolerancia a fallas y seguridad

La respuesta correcta es la (b) tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

Estas son las cuatro características básicas que la arquitectura subyacente de las redes necesita para cumplir con las expectativas de los usuarios en la actualidad.

Tolerancia a fallas: la capacidad de la red para mantener el funcionamiento y la disponibilidad en caso de fallas o interrupciones.

Escalabilidad: la capacidad de la red para crecer y adaptarse a medida que aumenta el tráfico y el número de dispositivos conectados.

Calidad del servicio: la capacidad de la red para garantizar un cierto nivel de rendimiento y experiencia de usuario para diferentes tipos de tráfico y aplicaciones.

Seguridad: la capacidad de la red para protegerse contra ataques y asegurar la privacidad y la integridad de la información transmitida

¿Cuáles son los dos servicios o protocolos que usan el protocolo UDP preferido para obtener transmisiones veloces y baja sobrecarga? Elija dos opciones.

Seleccione una o más de una:

X a. DNS

b. FTP

X c. VoIP

d. POP3

e. HTTP

Los dos servicios o protocolos que usan el protocolo UDP preferido para obtener transmisiones veloces y baja sobrecarga son:

a. DNS (Domain Name System)

c. VoIP (Voice over Internet Protocol)

DNS utiliza UDP en lugar de TCP porque UDP es más rápido y tiene una sobrecarga menor que TCP. VoIP también utiliza UDP debido a su capacidad para ofrecer transmisiones veloces con una sobrecarga menor, lo que es importante en las comunicaciones en tiempo real como las llamadas de voz y videoconferencias.

Las otras opciones mencionadas, FTP, POP3 y HTTP, generalmente utilizan TCP en lugar de UDP debido a la necesidad de una transmisión de datos confiable y ordenada.

¿Qué entidad de capa de transporte se utiliza para garantizar el establecimiento de la sesión?

Seleccione una:

X a. Protocolo de enlace TCP de 3 vías

b. Número de secuencia UDP

c. Indicador ACK UDP

d. Número de puerto TCP

La entidad de capa de transporte que se utiliza para garantizar el establecimiento de la sesión es el protocolo de enlace TCP de 3 vías (opción a).

El protocolo de enlace TCP de 3 vías es utilizado por el protocolo de control de transmisión (TCP) para establecer una conexión confiable entre dos dispositivos en una red. La secuencia de 3 vías se refiere a tres mensajes intercambiados entre los dispositivos para establecer y confirmar la conexión:

El dispositivo solicitante envía un mensaje de sincronización (SYN) al dispositivo remoto, indicando que desea establecer una conexión.

El dispositivo remoto responde con un mensaje SYN-ACK, que indica que está dispuesto a establecer una conexión y está esperando la confirmación del dispositivo solicitante.

El dispositivo solicitante responde con un mensaje ACK, confirmando la conexión y estableciendo la sesión.

El protocolo TCP utiliza este proceso de 3 vías para asegurar que la conexión se establezca correctamente antes de que se inicie la transmisión de datos.

Un administrador de red trata de resolver un problema de falla para acceder a www.unicauca.edu.co. Al escribir la dirección IP del servidor en el explorador, la pagina web se abre exitosamente. ¿Qué protocolo de la capa de aplicación es el responsable de la falla?

Seleccione una:

a. DHCP

b. HTTP

X c. DNS

d. CDP

e. SSL

La falla parece estar relacionada con el protocolo DNS (Sistema de Nombres de Dominio) (opción c).

El protocolo DNS se utiliza para traducir los nombres de dominio, como www.unicauca.edu.co, en direcciones IP numéricas, que son necesarias para acceder a los servidores web correspondientes. Al escribir la dirección IP en el navegador, el servidor web se puede acceder directamente, lo que sugiere que el problema puede estar en el proceso de resolución de nombres de dominio.

Es posible que el servidor DNS utilizado por el administrador de red esté caído o no esté configurado correctamente, lo que hace que la resolución de nombres de dominio no funcione correctamente. Por lo tanto, el administrador de red puede necesitar investigar la configuración del servidor DNS y solucionar cualquier problema allí.

Cuáles son los tres problemas comunes que presenta una red de gran tamaño? (Elija tres).

Seleccione una o más de una:

a. Responsabilidad limitada de la administración

X b. Identificación del host

X c. Degradación del rendimiento

X d. Problemas de seguridad

e. Muy pocos broadcasts

Los tres problemas comunes que presenta una red de gran tamaño son:

c. Degradación del rendimiento: A medida que una red se hace más grande, el tráfico de red aumenta, lo que puede resultar en congestión y latencia, lo que puede degradar el rendimiento de la red.

d. Problemas de seguridad: Una red de gran tamaño puede presentar más vulnerabilidades de seguridad y puede ser más difícil de administrar y proteger contra ataques maliciosos.

e. Muy pocos broadcasts: En una red grande, el uso excesivo de transmisiones de difusión (broadcasts) puede abrumar la red y reducir el rendimiento general. Por lo tanto, es importante limitar y controlar el uso de broadcasts en una red grande.

Las opciones a, b no son problemas comunes que presentan una red de gran tamaño. La responsabilidad limitada de la administración depende más del enfoque y la estructura de la organización, mientras que la identificación del host es un problema que puede resolverse con la implementación de un sistema de nombres de dominio adecuado o un protocolo de descubrimiento de host.

¿Cuáles son los factores externos que afectan el éxito de las comunicaciones? (elija dos)

Seleccione una o más de una:

X a. la cantidad de mensajes adicionales que se transmiten simultáneamente en la red de comunicación

b. el tamaño del mensaje

X c. la importancia del mensaje

d. la complejidad del mensaje

e. la cantidad de veces que el mensaje tiene que cambiar la forma

Los dos factores externos que afectan el éxito de las comunicaciones son:

a. La cantidad de mensajes adicionales que se transmiten simultáneamente en la red de comunicación: A medida que aumenta la cantidad de mensajes que se transmiten simultáneamente en la red de comunicación, aumenta la competencia por los recursos de la red y disminuye el rendimiento de la red.

c. La importancia del mensaje: La importancia del mensaje puede afectar su éxito en la comunicación, ya que los mensajes importantes pueden requerir priorización sobre otros mensajes menos importantes para asegurarse de que lleguen a su destino de manera oportuna.

Las opciones b, d, y e se refieren a factores internos que pueden afectar el éxito de las comunicaciones, tales como el tamaño, la complejidad y la forma de los mensajes transmitidos.

¿Cuáles son los factores clave que se deben tener en cuenta al agrupar hosts en una red común? (Elija tres).

Seleccione una o más de una:

a. propiedad

X b. direccionamiento físico

X c. gateways

X d. propósito

e. versión del software

f. ubicación geográfica

Los tres factores clave que se deben tener en cuenta al agrupar hosts en una red común son:

b. Direccionamiento físico: Al agrupar hosts en una red común, es importante tener en cuenta su direccionamiento físico, ya que esto afectará cómo se enrutan los paquetes en la red.

c. Gateways: El acceso a otras redes, incluyendo Internet, se realiza a través de gateways. Al agrupar hosts en una red común, es importante tener en cuenta los gateways necesarios para que los hosts se comuniquen con otras redes.

d. Propósito: Agrupar hosts en una red común según su propósito es importante para optimizar el tráfico y garantizar la seguridad. Por ejemplo, puede ser necesario agrupar hosts en subredes separadas para garantizar que los servidores críticos no se vean afectados por el tráfico de usuarios.

Las opciones a, e, y f no son factores clave que se deben tener en cuenta al agrupar hosts en una red común. La propiedad, la versión del software y la ubicación geográfica son factores que pueden ser relevantes en ciertos casos, pero no son factores clave que se deben tener en cuenta al agrupar hosts en una red común en general.

¿Qué factor determina el tamaño de la ventana TCP?

Seleccione una:

a. El número de servicios incluidos en el segmento TCP

X b. La cantidad de datos de destino que puede procesar a la vez

c. La cantidad de datos a transmitir

d. La cantidad de datos que la fuente es capaz de enviar de una sola vez

El factor que determina el tamaño de la ventana TCP es:

b. La cantidad de datos de destino que puede procesar a la vez.

La ventana TCP se refiere al número de bytes que el receptor puede recibir y procesar sin necesidad de enviar un acuse de recibo (ACK) al remitente. El tamaño de la ventana TCP se determina por la capacidad del receptor para procesar datos y se comunica al remitente a través del campo de ventana en el encabezado TCP. Esto permite que el remitente ajuste la cantidad de datos que envía en un momento dado para evitar la congestión en la red.

¿Cómo utiliza la capa de red el valor de MTU?

Seleccione una:

a. La capa de red depende de la capa de enlace de datos para establecer la MTU y ajusta la velocidad de transmisión para admitirla.

X b. La capa de red depende de las capas de niveles superiores para determinar la MTU

c. La capa de enlace de datos pasa la MTU a la capa de red.

d. Para aumentar la velocidad de entrega, la capa de red ignora la MTU

La capa de red utiliza el valor de MTU (Maximum Transmission Unit) para fragmentar y reensamblar los paquetes de datos que se transmiten a través de la red. La MTU es el tamaño máximo de un paquete que puede transmitirse sin fragmentación.

Por lo tanto, la respuesta correcta es:

b. La capa de red depende de las capas de niveles superiores para determinar la MTU.

La MTU se determina en gran medida por las características de la capa física y de enlace de datos de la red, pero también puede ser influenciada por las aplicaciones que generan los datos. Por lo tanto, la capa de red no establece la MTU directamente, sino que utiliza el valor de MTU proporcionado por las capas superiores para fragmentar y reensamblar los paquetes de datos de manera que puedan ser transmitidos a través de la red de manera eficiente.

¿Cuáles son los factores que identifican una red de área local? (elija dos)

Seleccione una o más de una:

X a. el tamaño del área cubierta

b. la cantidad de conexiones WAN

X c. la cantidad de usuarios conectados

d. la cantidad de redes extranet configuradas en la red

e. las políticas dentro de la red del proveedor del servicio de comunicaciones son

controladas por el TSP

Las opciones a y c son las respuestas correctas. Los factores que identifican una red de área local son el tamaño del área cubierta y la cantidad de usuarios conectados. Las otras opciones no están relacionadas con la definición de una red de área local.

¿Qué protocolos TCP/IP se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red?

Seleccione una:

a. HTTP

X b. TELNET

c. SMTP

d. DHCP

e. DNS

El protocolo TCP/IP que se utiliza para proporcionar acceso remoto a servidores y dispositivos de red es TELNET. La respuesta correcta es la opción b.

¿Cuál es el propósito de la ventana deslizante de TCP?

Seleccione una:

a. finalizar la comunicación cuando se completa la transmisión de datos.

b. asegurar que los segmentos lleguen en orden al destino.

X c. informar a un origen que debe retransmitir datos desde un punto específico en adelante

d. solicitar a un origen que reduzca la velocidad de transferencia de datos.

La ventana deslizante de TCP tiene el propósito de regular el flujo de datos en una comunicación TCP. Permite que el emisor transmita un número de segmentos específico antes de esperar una confirmación del receptor. De esta manera, se puede lograr un mejor rendimiento de la red y evitar la congestión de la red. La ventana deslizante también puede ajustarse en tiempo real según las condiciones de la red, lo que permite una transferencia de datos más eficiente y confiable. La opción c) puede ser una situación que se presente en una comunicación TCP, pero no es el propósito principal de la ventana deslizante.

Durante una sesión TCP, un dispositivo de destino envía un número de confirmación al dispositivo de origen. ¿Qué representa el número de acuse de recibo?

Seleccione una:

a. El número total de bytes que se han recibido

b. El último número de secuencia enviado por el origen

X c. El siguiente byte que el destino espera recibir

d. Un número más que el número de secuencia

El número de acuse de recibo en una sesión TCP representa el siguiente byte que el destino espera recibir.

Aplicaciones como bases de datos, e-mails, solicitudes web. ¿Que protocolo de la capa de transporte usan?

Seleccione una:

a. ICMP

X b. TCP

c. UDP

d. IP

Las aplicaciones como bases de datos, correos electrónicos y solicitudes web utilizan el protocolo TCP de la capa de transporte.

Cual de los siguientes procesos no esta descrito por la suite de protocolos de networking

Seleccione una:

a. el método por el cual los dispositivos de networking comparten información sobre rutas con otras redes

X b. la cantidad de mensajes de error enviados en una ventana de tiempo

c. cómo y cuándo se pasan los mensajes de error y del sistema entre dispositivos

d. el inicio y terminación de las sesiones de transferencia de datos

e. El formato o estructura del mensaje

La cantidad de mensajes de error enviados en una ventana de tiempo no está descrito por la suite de protocolos de networking.

¿Cuáles son las dos características que comúnmente se relacionan con los protocolos de enrutamiento dinámico? (Elija dos).

Seleccione una o más de una:

a. requieren menos potencia de procesamiento que las rutas estáticas

X b. consumen ancho de banda para intercambiar información de la ruta

c. impiden la configuración manual y el mantenimiento de la tabla de enrutamiento

X d. proporcionan routers con tablas de enrutamiento actualizadas

e. no requieren ningún tipo de configuración de dispositivos

Las dos características que comúnmente se relacionan con los protocolos de enrutamiento dinámico son:

b. Consumen ancho de banda para intercambiar información de la ruta.

d. Proporcionan routers con tablas de enrutamiento actualizadas.

Cuando la red de destino no se encuentra en la lista de la tabla de enrutamiento de un router Cisco, ¿cuáles son las dos acciones posibles que el router podría realizar? (Elija dos).

Seleccione una o más de una:

a. El router envía una solicitud de ARP (Protocolo de resolución de direcciones) para determinar la dirección del siguiente salto requerido.

X b. El router descarta el paquete

c. El router reenvía el paquete a la interfaz indicada por la dirección de origen

X d. El router reenvía el paquete a la interfaz indicada por la entrada de ruta por defecto

e. El router reenvía el paquete hacia el siguiente salto indicado en la tabla ARP.

Seleccione una o más de una:

b. El router descarta el paquete

d. El router reenvía el paquete a la interfaz indicada por la entrada de ruta por defecto

Qué campo del paquete ip evitara los bucles sin fin?

Seleccione una:

a. Identificación

b. Checksum del encabezado

c. Tipo de servicio

X d. Tiempo de vida

e. Señaladores

El campo del paquete IP que evitará los bucles sin fin es el campo "Tiempo de vida" o TTL (Time to Live).

¿Cuál de las siguientes opciones describe la dirección IP 172.16.134.64/27?

Seleccione una:

a. Ésta es una dirección de broadcast

X b. Ésta es una dirección de red

c. Esta dirección no es válida.

d. Ésta es una dirección host utilizable.

La dirección IP 172.16.134.64/27 es una dirección de red. La notación "/27" indica que los primeros 27 bits de la dirección IP son la parte de red, dejando los últimos 5 bits para la parte de host.

Si la gateway por defecto está configurada de forma incorrecta en el host, ¿cuál es el impacto sobre las comunicaciones?

Seleccione una:

a. El host puede comunicarse con otros hosts en redes remotas, pero no se puede comunicar con hosts de la red local.

b. El host no puede comunicarse en la red local.

c. No hay impacto sobre las comunicaciones

X d. El host puede comunicarse con otros hosts en la red local pero no se puede comunicar con hosts de redes remotas.

d. El host puede comunicarse con otros hosts en la red local pero no se puede comunicar con hosts de redes remotas. La gateway por defecto es la dirección IP del router utilizado para acceder a redes remotas. Si esta configuración es incorrecta en el host, entonces el host no podrá enviar paquetes a redes remotas a través del router. Sin embargo, aún puede comunicarse con hosts en la misma red local, ya que no necesita un router para hacerlo.

A partir de la dirección IP 192.168.85.129/26, ¿cuál es la dirección de subred (DS) y la dirección de Broadcast (DB) a la que pertenece el host?

Seleccione una:

a. DS=192.168.84.0, DB=192.168.92.255

X b. DS=192.168.85.128, DB=192.168.85.191

c. DS=192.168.85.129, DB= 192.168.85.224

d. DS=192.168.85.128, DB= 192.168.85.255

La dirección de subred se obtiene aplicando la máscara de subred a la dirección IP y la dirección de broadcast se obtiene cambiando los bits de host a 1 en la parte de host de la dirección de subred.

En este caso, la máscara de subred es /26, lo que significa que los primeros 26 bits son 1 y los últimos 6 bits son 0. Aplicando la máscara de subred a la dirección IP, se obtiene la dirección de subred:

192.168.85.129 AND 255.255.255.192 = 192.168.85.128 (dirección de subred)

Para obtener la dirección de broadcast, se cambian los últimos 6 bits de host a 1 en la dirección de subred:

192.168.85.128 + (2^6 - 1) = 192.168.85.191 (dirección de broadcast)

Por lo tanto, la dirección de subred (DS) es 192.168.85.128 y la dirección de Broadcast (DB) es 192.168.85.191. La opción correcta es b.

Cuando un servidor responde a una solicitud Web, ¿qué ocurre a continuación en el proceso de encapsulación después de que los datos de la página web se formatean y separan en segmentos TCP?

Seleccione una:

a. El cliente agrega las direcciones físicas correspondientes a los segmentos para que el servidor pueda enviar los datos

X b. El servidor agrega la dirección IP de origen y destino a cada encabezado de segmento para entregar los paquetes al destino

c. El cliente Desencapsula el segmento y abre la página web

d. El servidor agrega las direcciones físicas de origen y destino al encabezado del paquete

e. El servidor convierte los datos en bits para transportarlos a través del medio

La opción b es la correcta: El servidor agrega la dirección IP de origen y destino a cada encabezado de segmento para entregar los paquetes al destino. Después de que los datos de la página web se formatean y se separan en segmentos TCP, el servidor agrega la información de encabezado necesaria, incluyendo las direcciones IP de origen y destino, a cada segmento para que pueda ser entregado al destino. A partir de ahí, el proceso de encapsulación continúa a través de la red a medida que los paquetes se enrutan a través de diferentes dispositivos hasta que llegan al destino final.

3 principales características de ipv4

Las tres principales características de IPv4 son las siguientes:

Direcciones de 32 bits: IPv4 utiliza direcciones de 32 bits, lo que significa que puede haber hasta 4.3 billones de direcciones únicas en el espacio de direcciones IPv4. Sin embargo, debido a la rápida expansión de Internet, el espacio de direcciones IPv4 se ha agotado y ha surgido la necesidad de una nueva versión de IP, conocida como IPv6.

Protocolo sin conexión: IPv4 es un protocolo sin conexión, lo que significa que no establece una conexión dedicada entre dos hosts antes de que comience la transmisión de datos. En su lugar, los paquetes de datos se envían individualmente y cada paquete se enruta de manera independiente.

Enrutamiento jerárquico: IPv4 utiliza un enrutamiento jerárquico, lo que significa que las direcciones IP se dividen en redes más pequeñas, conocidas como subredes. Cada subred está conectada a una red más grande, y estas redes más grandes a su vez están conectadas a otras redes aún más grandes, creando una jerarquía de redes interconectadas que permite la comunicación a través de Internet.

Smtp

SMTP (Simple Mail Transfer Protocol) es un protocolo estándar de Internet para la transferencia de correo electrónico desde un servidor de correo a otro. SMTP es utilizado por programas de correo electrónico para enviar mensajes de correo electrónico desde un servidor de correo saliente (también conocido como servidor SMTP) a un servidor de correo entrante (también conocido como servidor POP o IMAP).

SMTP utiliza el puerto 25 como su puerto predeterminado para la comunicación. Cuando un usuario envía un correo electrónico, el programa de correo electrónico se comunica con el servidor SMTP para enviar el mensaje. El servidor SMTP se encarga de enrutar el mensaje a través de Internet a través de servidores SMTP intermedios hasta que llega al servidor de correo del destinatario.

SMTP también utiliza el concepto de autenticación de correo electrónico para garantizar que solo los usuarios autorizados puedan enviar correo electrónico a través del servidor SMTP. Los servidores SMTP pueden estar configurados para aceptar o rechazar los mensajes de correo electrónico basados en diversas reglas y filtros, como la dirección IP del remitente o el contenido del mensaje.

Smb

SMB (Server Message Block) es un protocolo de red que se utiliza para compartir archivos, impresoras y otros recursos entre dispositivos en una red. Es el protocolo de red principal utilizado en sistemas operativos Windows.

SMB se utiliza para permitir que un dispositivo comparta archivos e impresoras con otros dispositivos de la red, así como para acceder a archivos e impresoras compartidos en otros dispositivos de la red. SMB utiliza el puerto 445 como su puerto predeterminado para la comunicación.

Además de la compartición de archivos e impresoras, SMB también se utiliza para proporcionar otros servicios, como la autenticación y la autorización de usuarios en una red, el acceso remoto a archivos y la replicación de archivos entre servidores.

SMB ha sido ampliamente adoptado por la industria y se ha convertido en uno de los protocolos de red más utilizados en todo el mundo. Sin embargo, ha habido algunos problemas de seguridad asociados con SMB, y se han desarrollado nuevas versiones del protocolo para abordar estos problemas.

Dirección de red y su objetivo

La dirección de red es un término utilizado en redes informáticas para referirse a la dirección IP utilizada para identificar una red específica en la que se encuentran los dispositivos conectados a ella. La dirección de red se utiliza para dirigir el tráfico de datos entre diferentes redes y para enrutar los paquetes de datos a su destino correcto.

El objetivo principal de la dirección de red es proporcionar un mecanismo para identificar una red específica en una red más grande y permitir que los dispositivos en la red se comuniquen entre sí. Sin una dirección de red, los dispositivos no podrían conectarse y comunicarse en una red, lo que haría que la red fuera inútil.

La dirección de red se utiliza en combinación con la dirección IP de un dispositivo para proporcionar una forma de enrutar los datos a través de la red. La dirección IP identifica un dispositivo específico en una red, mientras que la dirección de red identifica la red en la que se encuentra el dispositivo. Juntos, estos dos componentes permiten que los dispositivos se comuniquen y compartan datos en una red de manera efectiva.

Dirección de Broadcast y su objetivo

La dirección de broadcast es una dirección especial utilizada en redes informáticas para enviar datos a todos los dispositivos conectados a una red en particular. Cuando se envía un mensaje a la dirección de broadcast, todos los dispositivos en la red reciben el mensaje.

El objetivo principal de la dirección de broadcast es permitir que un dispositivo envíe un mensaje a todos los dispositivos en una red sin tener que conocer las direcciones IP individuales de cada dispositivo. Esto es especialmente útil en situaciones donde se necesita enviar un mensaje a todos los dispositivos en una red al mismo tiempo, como en una red de difusión o para enviar actualizaciones o anuncios.

La dirección de broadcast se representa por la dirección IP más alta en una red determinada. Por ejemplo, si una red tiene la dirección IP 192.168.1.0 y una máscara de subred de 255.255.255.0, la dirección de broadcast será 192.168.1.255.

Es importante tener en cuenta que enviar un mensaje a la dirección de broadcast puede consumir mucho ancho de banda de red y hacer que la red sea lenta o inestable. Por lo tanto, es importante usar la dirección de broadcast con precaución y solo cuando sea necesario.

Dirección de host y su objetivo

La dirección de host es una dirección IP única que se asigna a cada dispositivo en una red. Esta dirección se utiliza para identificar de manera única un dispositivo dentro de la red y permitir que otros dispositivos se comuniquen con él.

El objetivo principal de la dirección de host es proporcionar una forma de identificar y comunicarse con un dispositivo en una red. Cuando un dispositivo en la red quiere comunicarse con otro dispositivo, utiliza la dirección de host del dispositivo de destino para enrutar los datos a través de la red hasta el dispositivo adecuado.

La dirección de host se compone de dos partes: la dirección de red y la dirección de host. La dirección de red identifica la red en la que se encuentra el dispositivo, mientras que la dirección de host identifica el dispositivo individual en esa red.

Por ejemplo, si la dirección de red es 192.168.1.0 y la dirección de host de un dispositivo es 192.168.1.10, entonces ese dispositivo se encuentra en la red 192.168.1.0 y su dirección de host es 10.

Es importante tener en cuenta que la dirección de host no es necesariamente la misma en todas las redes. Si un dispositivo se mueve de una red a otra, su dirección de host puede cambiar para reflejar la nueva red en la que se encuentra.

3 aplicaciones que usan tcp

TCP (Transmission Control Protocol) es un protocolo de comunicación utilizado para establecer conexiones de red confiables y sin errores. A continuación se presentan tres aplicaciones que utilizan TCP:

Navegador web: Los navegadores web, como Chrome, Firefox y Safari, utilizan TCP para comunicarse con los servidores web y solicitar páginas web. TCP asegura que todas las partes de la página web se carguen correctamente y sin errores.

Correo electrónico: El correo electrónico es otro ejemplo de una aplicación que utiliza TCP. Cuando se envía un correo electrónico, TCP se encarga de dividir el mensaje en paquetes y enviarlos a través de la red de manera confiable, asegurándose de que el mensaje llegue al destinatario completo y sin errores.

Transferencia de archivos: TCP se utiliza ampliamente en aplicaciones de transferencia de archivos, como FTP y SFTP, para enviar archivos grandes de manera confiable. TCP divide el archivo en paquetes y los envía a través de la red, y se asegura de que todos los paquetes lleguen al destino sin errores ni pérdidas.

Cuál es el objetivo de la configuración de un host como dirección de gateway por defecto

El objetivo de configurar la dirección de un host como dirección de gateway por defecto es permitir que el host se comunique con dispositivos en redes remotas que no están directamente conectados a él.

Cuando un host envía un paquete a una dirección IP que no está en su red local, envía el paquete al gateway por defecto. El gateway por defecto es el dispositivo que actúa como puerta de enlace para otras redes, y se utiliza para enrutar los paquetes hacia la red de destino.

Por lo tanto, al configurar la dirección de un host como dirección de gateway por defecto, se permite al host comunicarse con dispositivos en otras redes y acceder a recursos como servidores de correo electrónico, servidores web y otros dispositivos en la red.