

Tabla de contenido

OBJETIVOS	3
Objetivo general	3
Objetivos específicos	3
ANTECEDENTES	3
La Trama IP y TCP	3
TCP y sus Características	3
Puertos y Servicios en Redes	3
DP, Telefonía y Ping	4
¿Qué es TCP?	4
¿Qué caracteriza a TCP?	4
¿Cómo funciona?	5
1. Establecimiento de la Conexión (Saludo de Tres Vías)	5
2. Transferencia de Datos	5
3. Terminación de la Conexión	5
Tipos de TCP	5
1. TCP Tahoe y Reno	5
2. TCP New Reno	5
3. TCP Vegas	5
4. TCP CUBIC	6
¿Cuáles servicios utilizan TCP? ¿Cuáles no?	6
Servicios que utilizan TCP	6
Servicios que NO utilizan TCP (generalmente usan UDP)	6
Puertos Conocidos y Puertos Privados	6
Clasificación de servicios entorno a puertos	7
UDP, telefonía o ping	7
CONCLUSIONES	8
RECOMENDACIONES	8
BIBLIOGRAFÍA	9

OBJETIVOS

Objetivo general

- Comprender el funcionamiento y la importancia de los formatos de trama IP y el protocolo TCP como pilares fundamentales de las redes de comunicación de datos.

Objetivos específicos

- Definir y diferenciar los conceptos clave de trama IP y el protocolo TCP.
- Identificar las características, el funcionamiento y los tipos de TCP.
- Clasificar los servicios de red según su uso de TCP o protocolos alternativos.
- Distinguir entre puertos de red conocidos y privados y su relevancia en la clasificación de servicios.

ANTECEDENTES

La Trama IP y TCP

El Protocolo de Internet (IP) es un componente crucial para la transmisión de datos en redes, y su formato de trama asegura que los datos lleguen a su destino correcto. Además, el Protocolo de Control de Transmisión (TCP) proporciona una conexión confiable para la transmisión de datos.

Según Kurose & Ross (2017), "IP proporciona una dirección para cada dispositivo en la red, mientras que TCP se encarga de garantizar la entrega correcta de los datos" (p. 45).

TCP y sus Características

TCP es fundamental en la capa de transporte del modelo OSI, asegurando que los datos lleguen en orden y sin errores. De acuerdo con Tanenbaum & Wetherall (2013), "TCP establece una conexión entre el emisor y el receptor antes de transmitir los datos, garantizando fiabilidad" (p. 232).

Puertos y Servicios en Redes

La clasificación de puertos en redes es esencial para la correcta asignación y gestión de servicios, lo que permite a los sistemas de red funcionar correctamente y evitar

conflictos. Según Stallings (2016), "los puertos son claves para diferenciar los diferentes servicios que se ejecutan en un dispositivo de red" (p. 208).

DP, Telefonía y Ping

Las **PDU (Unidades de Datos de Protocolo)** son esenciales en la capa de transporte para asegurar la transmisión adecuada. El ping, por otro lado, es una herramienta utilizada para verificar la conectividad de los dispositivos en la red, y la telefonía sobre IP (VoIP) utiliza protocolos específicos como SIP y RTP. Según Forouzan (2017), "el ping se utiliza como una prueba simple para verificar la conectividad, mientras que VoIP facilita las llamadas a través de redes IP" (p. 72).

¿Qué es TCP?

El Protocolo de Control de Transmisión (TCP, por sus siglas en inglés *Transmission Control Protocol*) es uno de los protocolos fundamentales de la suite de protocolos de Internet. Opera en la capa de transporte y su principal objetivo es proporcionar una comunicación fiable, ordenada y con control de errores sobre una red IP, que por su naturaleza no es fiable.

¿Qué caracteriza a TCP?

- **Orientado a la conexión:** Antes de que se pueda intercambiar datos, se debe establecer una conexión entre los dos dispositivos a través de un proceso conocido como "saludo de tres vías" (three-way handshake).
- **Fiabilidad:** Garantiza que los datos lleguen sin errores, en el orden correcto y sin duplicados. Para ello, utiliza números de secuencia y acuses de recibo (ACKs). Si un segmento de datos no es acusado, se retransmite.
- **Control de Flujo:** Evita que un remitente rápido sature a un receptor lento. El receptor puede indicar al remitente la cantidad de datos que está dispuesto a aceptar.
- **Control de Congestión:** Ayuda a prevenir y mitigar la congestión en la red. TCP ajusta la velocidad de transmisión en función de la congestión detectada en la red.
- **Segmentación:** Divide grandes cantidades de datos de la capa de aplicación en segmentos más pequeños para su transmisión a través de la capa de red.

¿Cómo funciona?

1. Establecimiento de la Conexión (Saludo de Tres Vías)

- El cliente envía un segmento SYN (sincronizar) al servidor.
- El servidor responde con un segmento SYN-ACK (sincronizar-acuse de recibo).
- El cliente responde con un segmento ACK (acuse de recibo), estableciendo la conexión.

2. Transferencia de Datos

- Los datos se envían en segmentos. Cada segmento tiene un número de secuencia. El receptor envía ACKs para confirmar la recepción de los segmentos.

3. Terminación de la Conexión

- Se realiza a través de un "saludo de cuatro vías" donde ambas partes acuerdan cerrar la conexión.

Tipos de TCP

TCP es un estándar único, pero existen diferentes implementaciones y variantes que optimizan el control de la congestión. Algunos ejemplos incluyen:

1. TCP Tahoe y Reno

- De las primeras implementaciones, introdujeron algoritmos básicos de control de congestión.

2. TCP New Reno

- Una mejora sobre Reno que es más eficiente en la recuperación de múltiples pérdidas de paquetes.

3. TCP Vegas

- Estima el ancho de banda disponible para ajustar la velocidad de transmisión.

4. TCP CUBIC

- El algoritmo de control de congestión por defecto en muchos sistemas operativos Linux, diseñado para ser más escalable en redes de alta velocidad y larga distancia (redes "largas y anchas").

¿Cuáles servicios utilizan TCP? ¿Cuáles no?

Servicios que utilizan TCP

- **World Wide Web (HTTP/HTTPS):** Para la transferencia fiable de páginas web, imágenes y otros recursos.
- **Correo Electrónico (SMTP, POP3, IMAP):** Para el envío y recepción de correos electrónicos de manera fiable.
- **Transferencia de Archivos (FTP, SFTP):** Para garantizar que los archivos se transfieran sin errores.
- **Acceso Remoto Seguro (SSH):** Para una conexión segura y fiable a sistemas remotos.
- **Sistemas de Bases de Datos:** Para la comunicación fiable entre clientes y servidores de bases de datos.

Servicios que NO utilizan TCP (generalmente usan UDP)

- **Sistema de Nombres de Dominio (DNS):** Las consultas suelen ser pequeñas y se prefiere la rapidez de UDP.
- **Streaming de video y audio en vivo:** Se prioriza la velocidad sobre la fiabilidad. La pérdida de algunos paquetes es preferible a los retrasos causados por las retransmisiones de TCP.
- **Juegos en línea:** La baja latencia es crucial, por lo que se utiliza UDP.
- **Voz sobre IP (VoIP):** Al igual que el streaming, la velocidad es fundamental para una conversación fluida.
- **Protocolo de Tiempo de Red (NTP):** Para la sincronización de relojes en la red.

Puertos Conocidos y Puertos Privados

Los puertos son números de 16 bits (del 0 al 65535) que se utilizan para identificar aplicaciones y servicios específicos en un host. La IANA (Autoridad de Asignación de Números de Internet) los clasifica de la siguiente manera:

- **Puertos Conocidos (Well-Known Ports):** Rango del 0 al 1023. Están reservados para servicios y protocolos del sistema. Por ejemplo, el puerto 80 para HTTP, el 443 para HTTPS y el 22 para SSH.
- **Puertos Registrados:** Rango del 1024 al 49151. Pueden ser registrados por organizaciones para sus aplicaciones.
- **Puertos Privados o Dinámicos:** Rango del 49152 al 65535. Son utilizados por las aplicaciones cliente para establecer conexiones temporales.

Clasificación de servicios entorno a puertos

Los servicios de red se pueden clasificar según el puerto conocido que utilizan. Esta asociación permite a los sistemas operativos y al software de red dirigir el tráfico entrante a la aplicación correcta.

- **Servicios Web:** Puerto 80 (HTTP), Puerto 443 (HTTPS).
- **Servicios de Correo:** Puerto 25 (SMTP), Puerto 110 (POP3), Puerto 143 (IMAP).
- **Servicios de Transferencia de Archivos:** Puerto 20 y 21 (FTP), Puerto 22 (SFTP).
- **Servicios de Acceso Remoto:** Puerto 22 (SSH), Puerto 23 (Telnet - inseguro), Puerto 3389 (RDP).

UDP, telefonía o ping

- **UDP (User Datagram Protocol):** Es un protocolo de la capa de transporte sin conexión y no fiable. Es más rápido que TCP porque no tiene la sobrecarga del establecimiento de conexión, control de flujo ni retransmisiones. Es ideal para aplicaciones donde la velocidad es más importante que la fiabilidad.
- **Telefonía (VoIP):** Utiliza predominantemente UDP para la transmisión de paquetes de voz en tiempo real. La baja latencia es crítica para la calidad de la llamada.
- **Ping:** Es una utilidad de diagnóstico de red que utiliza el protocolo ICMP (Internet Control Message Protocol), que se encapsula directamente en IP (no usa TCP ni UDP). Sirve para comprobar la conectividad y medir el tiempo de ida y vuelta de los paquetes a un host de destino.

CONCLUSIONES

- El formato de la trama IP es la estructura esencial que permite el enrutamiento de datos a través de Internet, conteniendo la información de direccionamiento y control necesaria.
- TCP es un protocolo de transporte fundamental que añade fiabilidad, orden y control de errores a la comunicación sobre redes IP, siendo indispensable para una amplia gama de servicios críticos como la web, el correo electrónico y la transferencia de archivos.
- La elección entre TCP y un protocolo no orientado a conexión como UDP depende de los requisitos de la aplicación, principalmente de la necesidad de fiabilidad frente a la velocidad y la baja latencia.
- El sistema de puertos es un mecanismo crucial que permite a un único dispositivo ejecutar múltiples servicios de red simultáneamente, dirigiendo el tráfico entrante a la aplicación correspondiente.

RECOMENDACIONES

- Para exposiciones futuras, se recomienda el uso de diagramas visuales para ilustrar el formato de la trama IP y el proceso del "saludo de tres vías" de TCP, facilitando así una mejor comprensión por parte de la audiencia.
- Es importante enfatizar la diferencia práctica entre TCP y UDP mediante ejemplos cotidianos, como la diferencia entre cargar una página web (TCP) y realizar una videollamada (UDP).
- Se sugiere realizar una demostración práctica simple utilizando herramientas como ping y netstat para mostrar la actividad de red y los puertos en uso en un sistema, lo que puede ayudar a solidificar los conceptos teóricos.

BIBLIOGRÁFIA

Forouzan, B. A. (2017). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.

Stallings, W. (2016). *Data and Computer Communications* (10th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer Networks* (5th ed.). Prentice Hall.