Redes de comunicaciones

Una red de comunicaciones es un conjunto de dispositivos (a menudo llamados nodos) conectados por enlaces de comunicación. Estos enlaces pueden ser cableados (como cable de cobre o fibra óptica) o inalámbricos (como WiFi o enlaces de satélite). El propósito de una red es permitir que los dispositivos compartan recursos e información.

Algunos beneficios clave de las redes incluyen:

- Compartir recursos: Los usuarios pueden acceder y compartir recursos como impresoras, escáneres y almacenamiento de archivos.
- Compartir información: Las redes permiten que la información se transfiera fácilmente entre dispositivos, ya sea a través de correo electrónico, mensajería instantánea, bases de datos compartidas, etc.
- Soporte para servicios distribuidos: Las aplicaciones y servicios pueden distribuirse entre varios dispositivos conectados en red para mejorar el rendimiento, la escalabilidad y la confiabilidad.
- Ahorro de costos: El uso compartido de recursos puede reducir los costos al minimizar los requisitos de equipos y dispositivos redundantes.

Las redes pueden variar en tamaño desde pequeñas redes locales (LAN) que abarcan una oficina o edificio hasta grandes redes de área amplia (WAN) que se extienden por ciudades, países o incluso globalmente, como Internet.

Arquitectura de las redes

La arquitectura de una red define su estructura en términos de componentes, sus funciones y cómo interactúan. Proporciona un marco para el diseño, implementación y operación de una red.

Modelos de arquitectura de red

Hay dos modelos principales utilizados para describir las arquitecturas de red:

1. Modelo OSI (Open Systems Interconnection)
2. Modelo TCP/IP (que es la base de las redes modernas de Internet)

Modelo OSI

El modelo OSI es un marco conceptual que describe las funciones de un sistema de red. Divide las tareas de comunicación en siete capas distintas:

7. Capa de Aplicación
8. Capa de Presentación
9. Capa de Sesión
10. Capa de Transporte
11. Capa de Red
12. Capa de Enlace de Datos

13. Capa Física

Cada capa tiene un propósito específico y se comunica con las capas de arriba y abajo. Esta segregación de tareas en capas permite la interoperabilidad entre diferentes productos y software.

- Capa Física: Se encarga de la transmisión de bits crudos a través de un canal de comunicación. Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico.

- Capa de Enlace de Datos: Proporciona transferencia confiable de datos entre dos nodos conectados directamente. Divide los datos de entrada en tramas de datos y envía las tramas de forma secuencial. Es decir, estiona la transmisión de datos entre dos nodos directamente conectados. Asegura que los datos lleguen sin errores. El switch es un ejemplo de un dispositivo que opera en esta capa. Ejemplos de protocolos de capa 2 son Ethernet para LAN y Point-to-Point Protocol (PPP) para conexiones WAN y como HW es el Switch

- Capa de Red: Maneja el direccionamiento y enrutamiento de datos entre nodos en redes diferentes. Permite que los datos atraviesen múltiples enlaces de red para viajar de la fuente al destino. El protocolo más significativo de capa 3 es IP (Internet Protocol).

- Capa de Transporte: Proporciona transferencia confiable de datos entre puntos finales. Divide los datos en segmentos más pequeños y puede proporcionar transporte confiable asegurando que los datos lleguen sin errores y en la secuencia correcta. Los protocolos clave de capa 4 son TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). Por ejemplo

- Capa de Sesión: Establece, administra y termina sesiones entre dos hosts que se comunican. Sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos.

- Capa de Presentación: Proporciona independencia de las diferencias en la representación de datos (sintaxis) traduciendo entre formatos de aplicación y de red. Por ejemplo, codificación, compresión, cifrado/descifrado de datos.

- Capa de Aplicación: Interactúa con aplicaciones de software que implementan un componente de comunicación. Funciones como la identificación de socios de comunicación, determinación de disponibilidad de recursos y sincronización de comunicación.

Algunas ventajas del modelo OSI incluyen:

- Estandarización de los componentes de red, lo que permite múltiples proveedores.
- Evita que los cambios en una capa afecten a otras.
- Ayuda en el diseño de protocolos al dividir la funcionalidad de red.

Sin embargo, el modelo OSI a menudo se considera demasiado complejo y rígido para implementaciones reales. Más bien se usa como una herramienta de enseñanza y referencia.

Modelo TCP/IP

El modelo TCP/IP es la base de Internet y se usa ampliamente en las redes modernas. Es un modelo simplificado con sólo 4 capas:

4. Capa de Aplicación. Equivalente a las capas física y de enlace de datos del modelo OSI.

5. Capa de Transporte. Igual que en el modelo OSI, gestiona la entrega confiable o no confiable de datos.
6. Capa de Internet. Equivalente a la capa de red del modelo OSI, esta capa gestiona el enrutamiento de los paquetes.
7. Capa de Acceso a la Red. Equivalente a las capas de presentación y aplicación del modelo OSI.

El modelo TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación, y la capa física y de enlace de datos del modelo OSI en la capa de acceso a la red.

- Capa de Acceso a la Red: Especifica cómo se transmiten físicamente los datos a través de la red, incluyendo los detalles de cómo los bits se señalizan eléctricamente y las técnicas de corrección de errores de bajo nivel.

- Capa de Internet: Permite que los hosts inyecten paquetes en cualquier red y que viajen de forma independiente a su destino (potencialmente a través de múltiples redes). Define el formato de paquete y el protocolo oficial - IP.

- Capa de Transporte: Permite la comunicación peer-to-peer entre hosts. Los dos protocolos clave son TCP (proporciona entrega confiable, ordena y verifica errores) y UDP (entrega sin conexión, mínima).

- Capa de Aplicación: Contiene todos los protocolos de nivel más alto como HTTP (web), SMTP (correo electrónico), FTP (transferencia de archivos), DNS (resolución de nombres), etc.

El modelo TCP/IP tiene varias ventajas:

- Es un estándar abierto, no controlado por una sola compañía.
- Es independiente del hardware de red subyacente.
- No necesita capas estrictas; un protocolo puede realizar funciones de múltiples capas.
- Es el modelo usado por Internet, probado ampliamente y escalable.

Comunicación entre capas

En ambos modelos, cada capa se comunica con su capa par en el otro sistema. Esta comunicación se logra a través de información de encabezado añadida a los datos en cada capa.

Por ejemplo, cuando se envía un mensaje desde la capa de aplicación (como un correo electrónico), pasa por cada capa inferior hasta que se transmite a través de la capa física. Cada capa añade su propia información de encabezado que es utilizada por la capa correspondiente en el sistema receptor. A esto se le llama encapsulación.

En el sistema receptor, el mensaje sube por la pila de protocolos, y cada capa elimina el encabezado correspondiente usado por su capa par en el lado emisor, hasta que el mensaje llega a la capa de aplicación.

Topologías en LAN

La topología de una red se refiere a la disposición de los nodos de red y los enlaces que los conectan. Afecta a factores como el costo, la confiabilidad y el rendimiento de la red. Aquí nos centraremos en tres topologías comunes para redes de área local (LAN): Bus, Estrella y Anillo.

Topología en BUS

En una topología de bus, todos los nodos se conectan a un único cable llamado el bus o backbone. Este cable actúa como un medio compartido para que los nodos se comuniquen.

Ventajas:

- Fácil de instalar y extender. Los nodos pueden conectarse o desconectarse al bus sin interrumpir la red.
- Requiere menos cableado en comparación con otras topologías, reduciendo el costo.

Desventajas:

- Si el cable del bus falla, toda la red se cae (único punto de fallo).
- Difícil de solucionar problemas. Una falla en cualquier parte del cable puede interrumpir toda la red.
- El rendimiento de la red se degrada a medida que se añaden más nodos debido a colisiones de datos. Dado que los nodos comparten el medio, si dos nodos transmiten simultáneamente, sus paquetes chocarán. Entonces tendrán que esperar un tiempo aleatorio antes de retransmitir.

Las topologías de bus se usaban comúnmente en las primeras Ethernets (10Base2 y 10Base5), pero ahora son raras debido a sus limitaciones.

Topología en estrella

En una topología en estrella, cada nodo se conecta a un hub o switch central con su propio cable. Toda la comunicación entre nodos pasa a través del dispositivo central.

Ventajas:

- Fácil de instalar y reconfigurar. Los nodos pueden añadirse, quitarse o trasladarse simplemente moviendo los cables de conexión en el hub/switch.
- Confiable. Si un cable individual falla, sólo ese nodo se ve afectado. El resto de la red sigue funcionando.
- Mejor rendimiento. Las transmisiones de cada nodo están recibidas sólo por el hub/switch y luego dirigidas sólo al nodo de destino. Así no hay problemas de colisión.

Desventajas:

- Requiere más cableado que otras topologías, lo que puede aumentar el costo.
- Si el dispositivo central falla, toda la red se cae (punto único de fallo).
- La instalación y el cableado pueden ser complejos y caros.

La topología en estrella es la más común en redes Ethernet modernas utilizando interruptores.

Topología en anillo

En una topología de anillo, cada nodo se conecta a exactamente otros dos nodos, formando un camino cerrado para que los mensajes pasen en una dirección alrededor del anillo.

Ventajas:

- Toda la red puede manejar altas carga de tráfico porque cada nodo sólo necesita pasar los datos al siguiente nodo. No hay problemas de colisión como en la topología de bus.
- Fácil de instalar y reconfigurar. Para añadir o quitar un nodo, sólo hay que mover dos conexiones.

Desventajas:

- Si un nodo o enlace falla, toda la red se cae a menos que haya algún mecanismo de redundancia (como un anillo doble).
- Los datos deben pasar a través de cada nodo intermediario para llegar a su destino, lo que puede causar retrasos.
- Solucionar problemas puede ser difícil ya que un problema en cualquier nodo puede afectar a toda la red.

Los anillos son relativamente raros en las LAN debido a sus limitaciones, pero la topología se usa en redes de fibra óptica como SONET/SDH y en algunas implementaciones de redes de área local de alta velocidad como FDDI (Fiber Distributed Data Interface).

Hardware y Software de un sistema en red

Para construir y mantener una red funcional se requiere una combinación de hardware y software.

Componentes de Hardware de Red

- Adaptador de red (NIC): permite que un dispositivo se conecte a la red. Cada NIC tiene una dirección MAC única que identifica el dispositivo. Ejemplos son tarjetas Ethernet para LAN cableadas y tarjetas WiFi para redes inalámbricas.

- Cable: el medio por el cual viajan los datos entre dispositivos en una red cableada. Los tipos comunes incluyen par trenzado (por ejemplo, Cat5/Cat6 Ethernet), coaxial y fibra óptica. Cada tipo tiene sus propias ventajas en términos de costo, velocidad y distancia soportada.

- Conectores: Se utilizan para terminar los extremos de los cables y permitir que se conecten a dispositivos. Ejemplos son RJ45 para cables Ethernet, BNC para coaxial y LC para fibra óptica.

- Hub: Un simple dispositivo que conecta múltiples dispositivos en una red LAN. Cuando un paquete llega a un puerto, se copia a todos los demás puertos. Esto puede conducir a colisiones y no es muy eficiente.

- Switch: Un dispositivo inteligente que filtra y reenvía paquetes entre segmentos de LAN. Los switches aprenden qué dispositivos están conectados a qué puertos observando las direcciones MAC de origen, y luego sólo envían un paquete al puerto de destino necesario en lugar de a todos los puertos como un hub.

- Router: Un dispositivo que reenvía paquetes entre redes diferentes. Los routers usan direcciones IP para tomar decisiones sobre la mejor ruta para que un paquete llegue a su destino. Son cruciales para conectar redes LAN a una WAN o Internet.

- Punto de acceso inalámbrico: conecta dispositivos inalámbricos a una red cableada. Convierte entre señales cableadas e inalámbricas y a menudo sirve como un hub central para la parte inalámbrica de la red.

Software de Red

- Sistema operativo: casi todos los sistemas operativos modernos incluyen soporte de software para redes. Esto incluye controladores para hardware de red, así como implementaciones de protocolos de

red como TCP/IP.

- Software de protocolo: implementaciones de varios protocolos de red. Estos pueden ser parte del sistema operativo o software separado. Ejemplos incluyen el conjunto de protocolos TCP/IP, protocolos de enrutamiento como OSPF o BGP, el sistema de nombres de dominio (DNS), etc.

- Utilidades y herramientas de red: programas usados para configurar, gestionar y solucionar problemas de redes. Algunos ejemplos comunes:

    - ping: comprueba la conectividad entre dispositivos enviando paquetes ICMP y esperando una respuesta.
    - traceroute: muestra la ruta y mide los retrasos de tránsito de los paquetes a través de una red IP.
    - ipconfig/ifconfig: muestra y configura los parámetros de la interfaz de red.
    - nslookup: consulta el DNS para obtener información de mapeo entre nombres de dominio y direcciones IP.

- Servidores de red: hosts que proporcionan recursos a otros dispositivos en la red. Algunos ejemplos comunes incluyen servidores web (que alojan páginas web), servidores de archivos (que almacenan y permiten el acceso a los archivos), servidores de correo (para enviar y recibir correo elect