

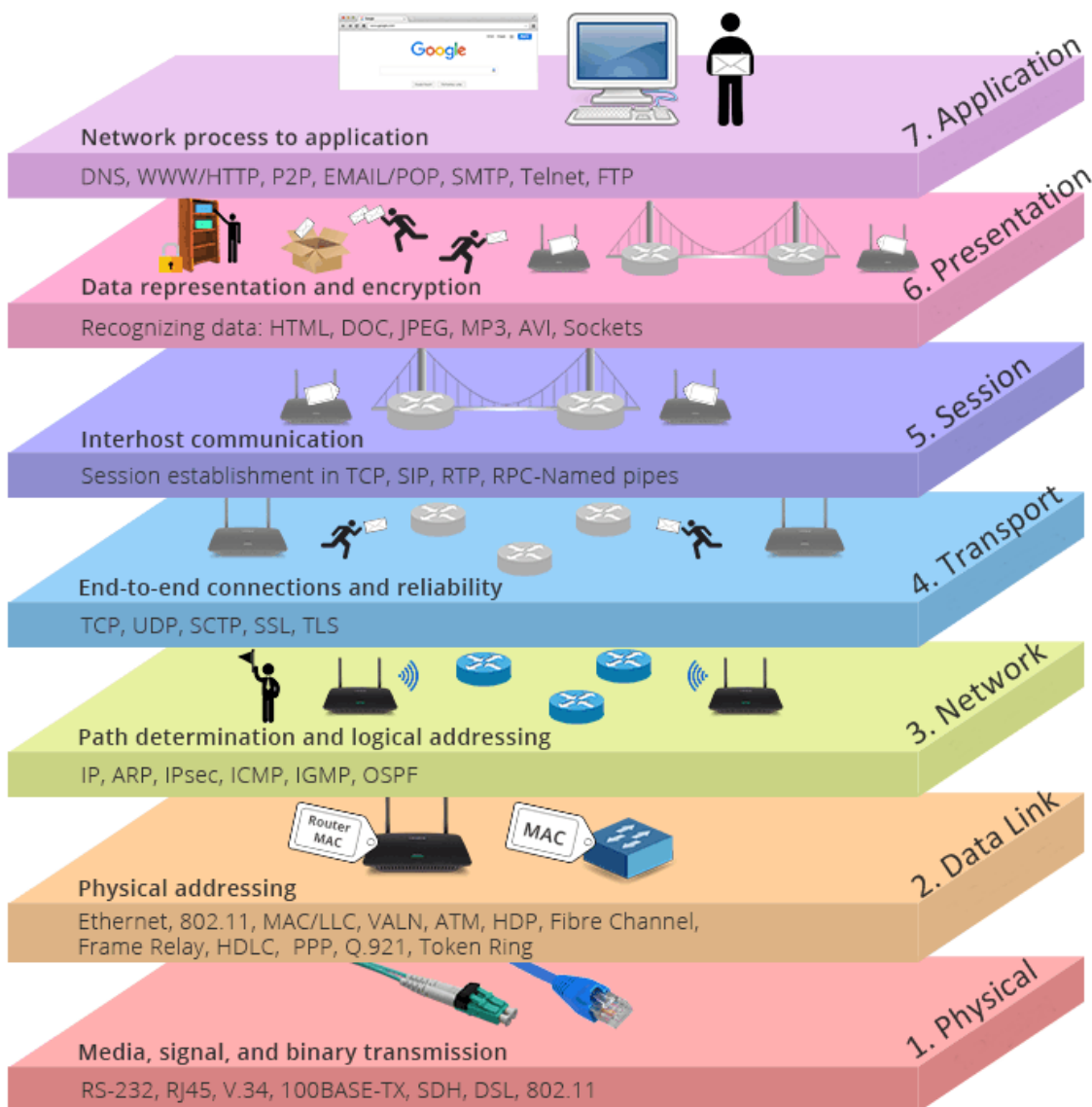
OSI vs. TCP/IP

CAPAS DEL MODELO OSI

Cuando hablamos de switches de capa 2 y capa 3, en realidad nos referimos a las capas de un modelo de protocolo genérico: el modelo de interconexión de sistemas abiertos (OSI), el cual es comúnmente utilizado para la descripción de las comunicaciones de red. La comunicación de datos entre redes diferentes no sería posible si no existiesen reglas compartidas para su transmisión y recepción. Estas reglas se conocen como protocolos, entre los cuales se distingue el Protocolo de control de transmisión (TCP)/Protocolo de internet (IP) por ser uno de los más utilizados. Este se usa popularmente en la descripción de la red y es más antiguo que el modelo OSI, ambos con muchas capas. A continuación, explicaremos cuál es la diferencia entre ellos.

Capas del modelo OSI

El modelo OSI, de siete capas, es un modelo conceptual que caracteriza y estandariza la manera en la que los diferentes componentes de software y hardware involucrados en una comunicación de red deben dividir la mano de obra e interactuar entre sí. En la siguiente figura podrá ver los nombres y funciones básicas de cada una de las capas.



Capa 7: Capa de aplicación

La capa de aplicación del modelo OSI interactúa directamente con las aplicaciones de software para proporcionar funciones de comunicación según sea necesario, y es la más cercana a los usuarios finales. Las funciones de la capa de aplicación generalmente incluyen la verificación de la disponibilidad de los socios de comunicación y los recursos para respaldar cualquier transferencia de datos. Esta capa también define protocolos para aplicaciones finales, como sistema de nombres de dominio (DNS), protocolo de transferencia de archivos (FTP), protocolo de transferencia de hipertexto (HTTP), protocolo de acceso a mensajes de Internet (IMAP), protocolo de oficina postal (POP), transferencia de correo simple. Protocolo (SMTP), Protocolo simple de administración de red (SNMP) y Telnet (una emulación de terminal).

Capa 6: Capa de presentación

La capa de presentación verifica los datos para asegurarse de que sean compatibles con los recursos de comunicaciones. Traduce los datos a la forma que aceptan el nivel de aplicación y los niveles inferiores. La sexta capa también maneja cualquier formato de datos necesario o conversión de código, como convertir un archivo de texto codificado con código de intercambio decimal codificado en binario extendido (EBCDIC) en un archivo de texto codificado con código estándar americano para el intercambio de información (ASCII). También funciona para la compresión y el cifrado de datos. Por ejemplo, las video llamadas se comprimirán durante la transmisión para que se puedan transmitir más rápido y los datos se recuperarán en el lado receptor. Para los datos que tienen altos requisitos de seguridad, como un mensaje de texto que contiene su contraseña, se cifrarán en esta capa.

Capa 5: Capa de sesión

La capa de sesión controla los diálogos (conexiones) entre computadoras. Establece, gestiona, mantiene y, en última instancia, finaliza las conexiones entre la aplicación local y remota. El software de capa 5 también maneja las funciones de autenticación y autorización. También verifica que se entreguen los datos. La capa de sesión se implementa comúnmente de forma explícita en entornos de aplicaciones que utilizan llamadas a procedimientos remotos.

Capa 4: Capa de transporte

La capa de transporte proporciona las funciones y los medios para transferir secuencias de datos desde una fuente a un host de destino a través de una o más redes, mientras mantiene las funciones de calidad de servicio (QoS) y asegura la entrega completa de los datos. La integridad de los datos se puede garantizar mediante la corrección de errores y funciones similares. También puede proporcionar una función de control de flujo explícita. Aunque no se ajusta estrictamente al modelo OSI, TCP y los protocolos de datagramas de usuario (UDP) son protocolos esenciales en la capa 4.

Capa 3: Capa de red

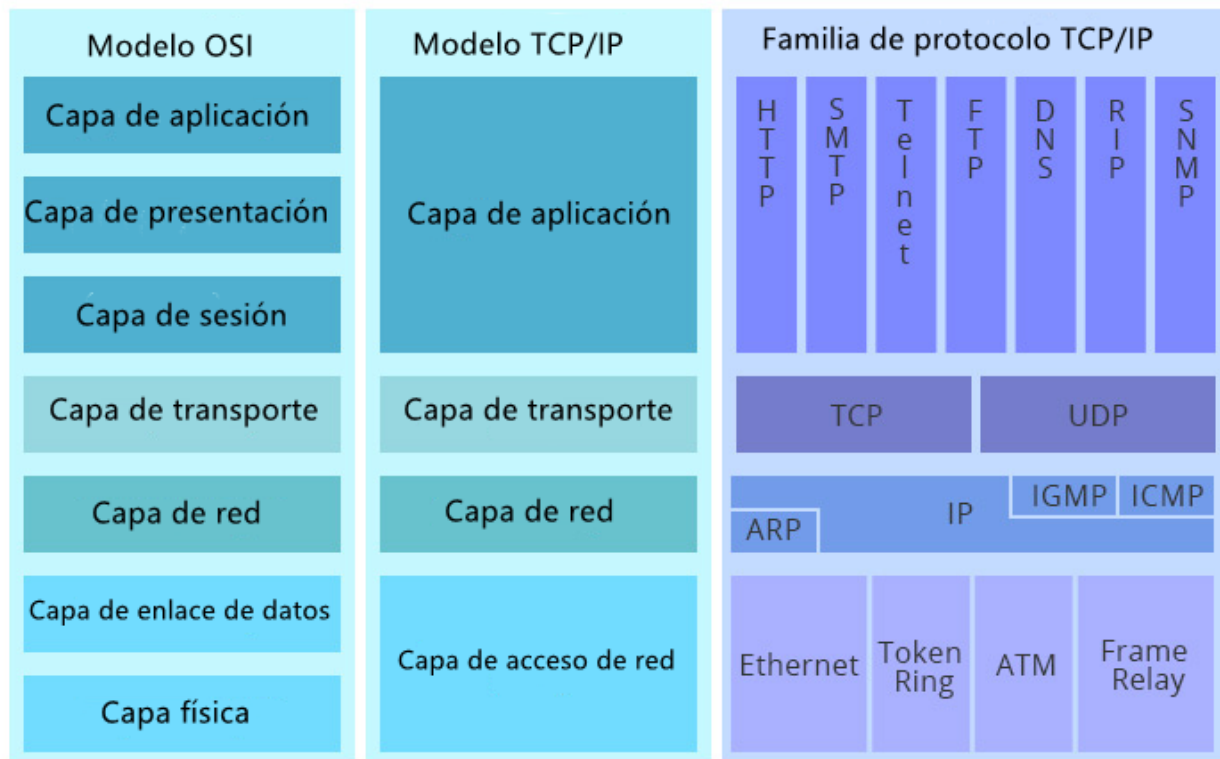
La capa de red maneja el enrutamiento de paquetes a través de funciones de conmutación y direccionamiento lógico. Una red es un medio al que se pueden conectar muchos nodos. Cada nodo tiene una dirección. Cuando un nodo necesita transferir un mensaje a otros nodos, simplemente puede proporcionar el contenido del mensaje y la dirección del nodo de destino, luego la red encontrará la manera de entregar el mensaje al nodo de destino, posiblemente enrutándolo a través de otros nodos. Si el mensaje es demasiado largo, la red puede dividirlo en varios segmentos en un nodo, enviarlos por separado y volver a ensamblar los fragmentos en otro nodo.

Capa 2: Capa de enlace de datos

La capa de enlace de datos proporciona transferencia de nodo a nodo, un enlace entre dos nodos conectados directamente. Maneja el empaquetado y desempaquetado de datos en marcos. Define el protocolo para establecer y terminar una conexión entre dos dispositivos conectados físicamente, como el Protocolo punto a punto (PPP). La capa de enlace de datos generalmente se divide en dos subcapas: capa de control de acceso a medios (MAC) y capa de control de enlace lógico (LLC). La capa MAC es responsable de controlar cómo los dispositivos en una red obtienen acceso a un medio y permiso para transmitir datos. La capa LLC es responsable de identificar y encapsular los protocolos de la capa de red y controla la verificación de errores y la sincronización de tramas.

Capa 1: Capa física

La capa física define las especificaciones eléctricas y físicas de la conexión de datos. Por ejemplo, la disposición de las clavijas del conector, los voltajes de funcionamiento de un cable eléctrico, las especificaciones del cable de fibra óptica y la frecuencia de los dispositivos inalámbricos. Es responsable de la transmisión y recepción de datos brutos no estructurados en un medio físico. El control de la tasa de bits se realiza en la capa física. Es la capa del equipo de red de bajo nivel y nunca se ocupa de los protocolos u otros elementos de la capa superior.



CAPAS DEL MODELO TCP/IP

El modelo TCP/IP solamente tiene cuatro capas y es conocido generalmente como TCP/IP, ya que estos son sus dos protocolos más importantes.

Capa de aplicación

La capa de aplicación del modelo TCP/IP ofrece a las aplicaciones la capacidad de acceder a los servicios de las otras capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. Los protocolos de la capa de aplicación más conocidos son HTTP, FTP, SMTP, Telnet, DNS, SNMP y el Protocolo de información de enrutamiento (RIP).

Capa de transporte

La capa de transporte se encarga de proporcionar comunicación de sesión y datagrama a la capa de aplicación de servicios. Los protocolos principales de esta capa son TCP y UDP. TCP proporciona un servicio de comunicaciones individual, fiable y orientado a la conexión. Es responsable de la secuenciación y detección de los paquetes enviados y de la recuperación de los paquetes perdidos en la transmisión. UDP proporciona un servicio de comunicaciones individual o grupal, sin conexión y poco fiable. Este se utiliza normalmente cuando la cantidad de datos a transferir es pequeña, como por ejemplo cuando estos caben en un solo paquete.

Capa de red

La capa de red es responsable de las funciones de direccionamiento, empaquetado y enrutamiento del host. Los protocolos centrales de la capa de Internet son IP, Protocolo de resolución de direcciones (ARP), Protocolo de mensajes de control de Internet (ICMP) y Protocolo de administración de grupos de Internet (IGMP). En esta capa, el IP agrega la cabecera a los paquetes, lo que se conoce como dirección IP. En la actualidad existen tanto dirección IPv4 (32 bits) como dirección IP IPv6 (128 bits). Más información: ¿Cómo podemos entender lo que significa la dirección IP y la máscara de subred?

Capa de acceso a la red

La capa de acceso a la red (o capa de enlace) es responsable de colocar los paquetes TCP/IP en el portador de datos de la red y recibir los paquetes TCP/IP situados fuera del mismo. El protocolo TCP/IP está diseñado para ser independiente del método de acceso a la red, el formato de la trama de red y el portador. En otras palabras, este protocolo es independiente de cualquier tecnología de red específica, lo que hace que este se pueda utilizar para conectar diferentes tipos de red, como Ethernet, TokenRing y Modo de transferencia asíncrono (ATM).

¿Cómo se procesan los datos durante la transmisión?

En un sistema de capas, los dispositivos de una capa intercambian datos en un formato diferente, lo que se conoce como unidad de datos de protocolo (PDU).

Por ejemplo, cuando un usuario solicita navegar por un sitio web en su ordenador, el software del servidor remoto primero entrega los datos solicitados a la capa de aplicación, donde se procesa de capa a capa con cada capa realizando sus funciones designadas. Los datos posteriormente se transmiten a través de la capa física de la red hasta ser recibidos por el servidor de destino u otro dispositivo. En este punto, los datos pasan nuevamente a través de las capas, cada capa realiza sus operaciones asignadas hasta que finalmente el software receptor utilice los datos.

Durante la transmisión, cada capa agrega una cabecera, pie de página o ambos a la PDU proveniente de la capa superior, el cual dirige e identifica el paquete. Este proceso se llama encapsulación. La cabecera (y el pie de página) y el cuerpo forman la PDU para la siguiente capa. El proceso continúa hasta llegar a la capa de nivel más bajo (capa física o capa de acceso a la red), desde la cual los datos se transmiten al dispositivo receptor. El dispositivo receptor invierte el proceso, desencapsulando los datos en cada capa con la información de la cabecera y pie de página que dirige las operaciones. Finalmente, la aplicación utiliza los datos y el proceso continúa hasta que todos los datos son transmitidos y recibidos.

Gracias a que se conoce el funcionamiento de la división de capas, es posible diagnosticar el problema cuando una conexión falla. La clave es comprobar el funcionamiento desde el nivel más bajo, en lugar de desde el nivel más alto, ya que cada capa atiende a su capa inmediatamente superior, por lo que será más fácil tratar los problemas de la capa inferior. Por ejemplo, si su ordenador no puede conectarse a Internet, lo primero que debe hacer es verificar si el cable de red está conectado al mismo o si el punto de acceso inalámbrico (WAP) está conectado al switch.

Las diferencias entre modelo OSI y modelo TCP/IP

La capa de aplicación del modelo TCP/IP es similar a las capas 5, 6, 7 combinadas del modelo OSI, el modelo TCP/IP no tiene una capa de sesión. La capa de transporte de TCP/IP abarca las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI. La capa de acceso a la red del modelo TCP/IP abarca el enlace de datos y las capas físicas del modelo OSI.

Considerando los significados de los dos modelos de referencia, el modelo OSI es solo un modelo conceptual. Se utiliza principalmente para describir, discutir y comprender funciones de red individuales. Sin embargo, TCP/IP está diseñado en primer lugar para resolver un conjunto específico de problemas, no para funcionar como una descripción de generación para todas las comunicaciones de red como modelo OSI. El modelo OSI es genérico, independiente del protocolo, pero la mayoría de los protocolos y sistemas se adhieren a él, mientras que el modelo TCP/IP se basa en protocolos estándar que Internet ha desarrollado. Otra cosa que debe tenerse en cuenta en el modelo OSI es que no todas las capas se utilizan en aplicaciones más simples. Si bien las capas 1, 2, 3 son obligatorias para cualquier comunicación de datos, la aplicación puede usar alguna capa de interfaz única para la aplicación en lugar de las capas superiores habituales en el modelo.

Importancia de TCP/IP y OSI para la resolución de problemas

Si tenemos en cuenta los significados de los dos modelos de referencia, el modelo OSI sería solo un modelo conceptual; este se utiliza principalmente para describir, discutir y comprender funciones de red individuales. Sin embargo, TCP/IP está diseñado para resolver un conjunto específico de problemas y no para funcionar como una descripción de generación para todas las comunicaciones de red, tal y como lo hace el modelo OSI. El modelo OSI es genérico e independiente del protocolo, aunque la mayoría de los protocolos y sistemas se adaptan a él, mientras que el modelo TCP/IP se basa en protocolos estándar desarrollados por Internet. Otro factor a tener en cuenta en el modelo OSI es que, para las aplicaciones más simples, no todas las capas son utilizadas. Si bien las capas 1, 2, 3 son obligatorias para cualquier comunicación de datos, también existen aplicaciones que pueden usar ciertas capas de interfaz específicas en lugar de las capas superiores habituales del modelo.

Resumen

El modelo TCP/IP y el modelo OSI son modelos conceptuales utilizados para la descripción de todas las comunicaciones de la red, a su vez, TCP/IP también es un protocolo importante que se utiliza en todas las operaciones de Internet. Generalmente, cuando hablamos de capa 2, capa 3 o capa 7 en las que funciona un dispositivo de red, nos referimos al modelo OSI. El modelo TCP/IP se usa tanto para modelar la arquitectura actual de Internet como para proporcionar un conjunto de reglas seguidas por todas las formas de transmisión a través de la red.