¿Qué diferencia hay entre TCP e IP?

TCP e IP son protocolos distintos para redes informáticas. La diferencia entre TCP (protocolo de control de transmisión) e IP (protocolo de Internet) es su papel en el proceso de transmisión de datos. IP obtiene la dirección a la que se envían los datos (su ordenador tiene una dirección IP). TCP garantiza la entrega correcta de los datos una vez hallada dicha dirección IP. En combinación, ambos forman el protocolo TCP/IP.

En otras palabras, IP clasifica el correo y TCP lo envía y recibe. Aunque los dos protocolos suelen considerarse una entidad, otros protocolos, como UDP (protocolo de datagrama de usuario), pueden enviar datos en el sistema IP sin usar TCP. Aun así, TCP requiere una dirección IP para enviar datos. Esa es otra diferencia entre IP y TCP.

¿Cuáles son las capas del modelo TCP/IP?

Hay cuatro capas en el modelo TCP/IP: acceso a la red, Internet, transporte y aplicación. Conjuntamente, estas capas son un conjunto de protocolos. El modelo TCP/IP pasa los datos por estas capas en un orden concreto cuando un usuario envía información y después en el orden inverso cuando se reciben los datos.

Capa 1: capa de acceso a la red
La capa de acceso a la red, también conocida como la capa de enlace a los datos, gestiona la infraestructura física que permite a los ordenadores comunicarse entre sí por Internet. Esto abarca, entre otros elementos, cables Ethernet, redes inalámbricas, tarjetas de interfaz de red y controladores de dispositivos en el ordenador.

La capa de acceso a la red también incluye la infraestructura técnica, como el código que convierte datos digitales en señales transmisibles, que hacen posible una conexión.

Capa 2: Capa de Internet
La capa de Internet, también llamada la capa de red, controla el flujo y el enrutamiento de tráfico para garantizar que los datos se envían de forma rápida y correcta. Esta capa también es responsable de volver a juntar el paquete de datos en el destino. Si hay mucho tráfico en Internet, esta capa puede tardar un poco más en enviar un archivo, pero es menos probable que el archivo se dañe.

Capa 3: Capa de transporte
La capa de transporte es la que proporciona una conexión de datos fiable entre dos dispositivos de comunicación. Es como enviar un paquete asegurado: la capa de transporte divide los datos en paquetes, confirma los paquetes que ha recibido del remitente y se asegura de que el destinatario confirme los paquetes recibidos por su parte.

Capa 4: Capa de aplicaciones
La capa de aplicaciones es el grupo de aplicaciones que permite al usuario acceder a la red. Para la mayoría de nosotros, esto significa el correo electrónico, las aplicaciones de mensajería y los programas de almacenamiento en la nube. Esto es lo que el usuario final ve y con lo que interactúa al recibir y enviar datos.

¿Con qué direcciones IP funciona TCP/IP?

Ya tenga una dirección IPv4 o IPv6, es muy probable que ya esté usando el modelo TCP/IP. Este es el modelo estándar para la mayor parte de la infraestructura de Internet. Hay distintas categorías de direcciones IP que pueden afectar a su privacidad o a cómo funciona el protocolo (por ejemplo, direcciones IP públicas frente a locales o estáticas frente a dinámicas), pero todas siguen el modelo TCP/IP estándar.

TCP/IP: el protocolo más habitual

TCP/IP es el conjunto de protocolos usado más habitualmente en Internet. Es tan habitual que la mayoría de la gente no se da cuenta de que lo está usando. La mayor parte de los ordenadores incluyen TCP/IP como estándar, así que no se requiere una configuración manual. Basta con conectarse a su red inalámbrica local y listo.

No obstante, aunque es el protocolo más habitual, no es el más seguro. Por ese motivo, nuestros expertos en seguridad han diseñado AVG Secure VPN, que proporciona un cifrado seguro en el protocolo OpenVPN (en Windows y Android) y el protocolo IKEv2 (para Mac OS y dispositivos iOS). Ambos son más seguros que los protocolos estándar TCP o IP.

AVG Secure VPN protege su dispositivo esté donde esté, ya sea conectado a una red Wi-Fi pública o a la red doméstica.

HTTP y FTP. Mientras que el primero nos permite acceder a una página web, el segundo se utiliza para comunicarse con el servidor y descargar o subir archivos al mismo.

Cada vez que un usuario utiliza un navegador para conectarse a Internet, el navegador se conecta con el servidor a través del protocolo HTTP, o HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto).

Al introducir una URL en nuestro navegador, éste interpreta y distingue entre tres partes. Pondremos como ejemplo https://www.arsys.es/mapa-web, donde:

HTTP es el protocolo utilizado

www.arsys.es es el nombre del servidor

mapa-web es el nombre del directorio especificado

Una vez que las tres partes han sido analizadas, el navegador entra en comunicación con un servidor DNS o de nombres y se conecta al servidor. Este proceso se suele realizar mediante el uso del protocolo HTTP. Este protocolo fue creado básicamente para la publicación de páginas en HTML, pertenece al grupo TCP/IP y es uno de los protocolos más extendidos en la actualidad.

El mecanismo del protocolo es sencillo: primero un navegador envía una solicitud GET al servidor pidiendo un archivo; posteriormente el servidor responde enviando al navegador el código perteneciente a ese archivo, que finalmente descifra el navegador.

Para intercambiar la información con el servidor HTTP se pueden utilizar tres tipos diferentes de mensajes:

GET: es un mensaje que lleva los datos de una manera visible al cliente, a través de la URL.
POST: envía los datos de una manera oculta para el cliente, mediante formularios.
PUT: lo utiliza el servidor para enviar información al servidor, cargando el contenido en éste.
Aunque muy extendido, HTTP es un protocolo que ofrece poca seguridad, puesto que la información con la que trabaja se puede extraer y leer fácilmente. Como evolución de este protocolo se creó HTTPS, que aunque es muy similar, ofrece mayor seguridad al encriptar la información que maneja, haciéndola menos accesible.

Protocolo FTP

El protocolo FTP ("File Transfer Protocol", o "Protocolo de Transferencia de Archivos") se usa para intercambiar archivos entre el cliente y el servidor. Para que dicha transferencia de archivos sea posible es necesario un cliente FTP y un servidor FTP.

Para que pueda funcionar, FTP necesita establecer dos conexiones diferentes entre las partes, una de ellas para poder transferir los archivos y la otra para las respuestas y los comandos. Es el cliente el que realiza ambas conexiones, una que se abre y se cierra cada vez que se envían los archivos y otra sola y permanente utilizada para los comandos.

Cabe recordar que la transferencia de archivos es bidireccional, puesto que ambas partes pueden actuar como cliente o servidor, siempre dependiendo de quién sirva el archivo y quién lo solicite.