Protocolos básicos en redes

Los **protocolos de red** son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

Protocolos de la capa de acceso al medio

ARP (Address Resolution Protocol)

El protocolo ARP para redes IPv4 es uno de los protocolos fundamentales de Internet y de las redes locales. Este protocolo también trabaja junto con el protocolo IP para mapear direcciones IP en relación a las direcciones de hardware utilizados por un protocolo de enlace datos. A estas direcciones de hardware se las denominan **direcciones MAC**. Estas direcciones sirven de código de identificación para cada una de las interfaces de red de los dispositivos. ARP opera en el medio de la capa de red y la capa de acceso al medio (si consideramos al modelo TCP/IP). Este protocolo se aplica cuando se utiliza el protocolo IP sobre Ethernet.

Protocolos de la capa de red

Internet Protocol (IP)

Los protocolos de Internet son un conjunto de reglas que determinan la manera en que se transmiten los datos a través de la red. El protocolo de IP es un estándar con especificaciones respecto a cómo deben funcionar los dispositivos conectados que se encuentran en Internet. Por un par de razones: el **direccionamiento** y el **routing**.

El **direccionamiento** consiste en asegurar que cualquier dispositivo conectado a una determinada red cuente con una **dirección de IP** única. Así, se podrá conocer al origen y el destino de los datos en tránsito. Por otro, lado el **routing** determina el camino por el cual el tráfico debe transitar teniendo como base la dirección IP. La tarea de routing es realizada mediante los routers, no solamente el que tenemos en nuestro hogar, sino los routers de los operadores. A su vez, varios protocolos interactúan con IP para posibilitar la comunicación en cualquier red.

Internet Control Message Protocol (ICMP)

Este protocolo apoya al proceso de control de errores. Esto es así ya que el protocolo IP, por defecto, no cuenta con un mecanismo para la gestión de errores en general. ICMP es utilizado para el reporte de errores y consultas de gestión. Es un protocolo utilizado por dispositivos como routers para enviar mensajes de errores e información relacionada a las operaciones. Por ejemplo, puede informar que el servicio solicitado no se encuentra disponible o que un *host* o router no pudo ser alcanzado/localizado. Este protocolo se encuentra justo por encima del protocolo IP en la capa de protocolos TCP/IP.

.

Protocolos de la capa de transporte

Transmission Control Protocol (TCP)

TCP es el aliado de IP para garantizar que los datos se transmiten de manera adecuada a través de Internet. Su función principal es asegurar que el tráfico llegue a destino de una manera confiable. Esta característica de confiabilidad no es posible lograrla únicamente mediante IP. Otras funciones de TCP son:

- Que no se pierdan los paquetes de datos.
- Control del orden de los paquetes de datos.
- Control de una posible saturación que se llegue a experimentar.
- Prevención de duplicado de paquetes.

User Datagram Protocol (UDP)

A diferencia del protocolo TCP, **UDP** no es tan confiable. Este no cuenta con posibilidad de realizar revisiones en búsqueda de errores o correcciones de transmisiones de datos. Sin embargo, hay ciertas aplicaciones en donde **UDP es más factible de utilizar** en vez de TCP. Un ejemplo de esto es una sesión de juegos en línea, en donde UDP permite que los paquetes de datos se descarten sin posibilidad de reintentos.

Lo malo es que este protocolo no es recomendado para realizar transferencia de datos. Ya que si algunos paquetes se pierden durante el proceso de transferencia, el resultado final es que el archivo se corrompe, y las capas superiores (capa de aplicación) es quien debe realizar la solicitud para que se vuelva a enviar el datagrama de nuevo. Un archivo corrupto no puede ser utilizado para el fin por el cual fue enviado. Igualmente, para este escenario de juegos en línea o sesiones de streaming de vídeos, UDP es el protocolo recomendado porque es más rápido al no tener que realizar el típico handshake.

Os recomendamos visitar nuestro completo artículo de TCP vs UDP donde encontraréis las principales diferencias entre ellos, y por qué los dos son importantes.

Protocolos de la capa de aplicación

Hypertext Transfer Protocol (HTTP)

Es el protocolo que permite que los navegadores y servidores web se comuniquen adecuadamente. Este es utilizado por navegadores web para solicitar archivos HTML de parte de los servidores remotos. Así, los usuarios podrán interactuar con dichos archivos mediante la visualización de las páginas web que cuentan con imágenes, música, vídeos, texto, etc.

El protocolo HTTP tiene como base a TCP, el cual implementa un modelo de comunicación cliente-servidor. Existen tres tipos de mensajes que HTTP utiliza:

- **HTTP GET:** Se envía un mensaje al servidor que contiene una URL con o sin parámetros. El servidor responde retornando una página web al navegador, el cual es visible por el usuario solicitante.
- **HTTP POST:** Se envía un mensaje al servidor que continee datos en la sección «body» de la solicitud. Esto es hecho para evitar el envío de datos a través de la propia URL. Así como sucede con el HTTP GET.
- **HTTP HEAD:** Aquí se hace énfasis en la respuesta por parte del servidor. Este mensaje restringe lo que el servidor responde para que solamente responda con la información de la cabecera.

No debemos olvidar el protocolo HTTPS, el cual nos proporciona seguridad punto a punto (entre el cliente y el servidor web). El protocolo HTTPS utiliza el protocolo TLS (Transport Layer Security) que también utiliza TCP por encima.

Domain Name System (DNS)

Es el servicio encargado de **traducir/interpretar nombres de dominio** a direcciones IP. Recordemos que los nombres de dominio se constituyen en base a caracteres alfabéticos (letras), los cuales son más fáciles de recordar. Para el usuario, es más fácil recordar un nombre que una serie numérica de cierta longitud. Sin embargo, Internet en general funciona en gran parte mediante las direcciones de IP. Siempre y cuando introduzcas un nombre de dominio en tu navegador, un servicio DNS recibe esa información para interpretarla y permitir la visualización de la página web deseada.

Tengamos presente que cuando contratamos un servicio de Internet, este nos provee la conectividad mediante sus propios servidores DNS. Sin embargo, es posible optar por DNS alternativos tanto para conectarnos desde el ordenador como nuestro móvil. ¿No estás seguro acerca de cuáles son las mejores alternativas? Echa un vistazo a la guía de DNS alternativos para el ordenador y esta otra guía para el móvil. También os recomendamos visitar los mejores servidores DNS over TLS (DoT) y DNS over HTTPS (DoH) para tener seguridad y privacidad a la hora de navegar por Internet.

File Transfer Protocol (FTP)

El **protocolo FTP** es utilizado para compartir archivos entre dos ordenadores. Así como el protocolo HTTP, FTP implementa el modelo cliente-servidor. Para que se pueda ejecutar FTP, se debe lanzar el cliente FTP y conectar a un servidor remoto que cuente con un software del mismo protocolo. Una vez que la conexión se ha establecido, se deben descargar los archivos elegidos de parte del servidor FTP. En RedesZone hemos hablado sobre servidores FTP y FTPES (la versión segura) para Windows, también hemos hablado sobre los mejores servidores FTP y FTPES para Linux, e incluso os hemos recomendado una gran cantidad de clientes FTP incluyendo un completo tutorial de FilleZilla Client.

Por otro lado, el **protocolo TFTP** fue diseñado para dispositivos con menor capacidad. Sus siglas corresponden a **Trivial File Transfer Protocol**. Este provee un uso básico que contiene solamente las operaciones elementales de FTP. Este protocolo se suele utilizar para cargar los firmwares en routers y switches gestionables, ya que es un protocolo muy simple de comunicación.

Los protocolos que citaremos a continuación, también interactúan con IP y con TCP. Una de las razones de ser del mundo corporativo es el correo electrónico. Día tras día, nos llegan mensajes, los respondemos y ese ciclo se repite un gran número de veces. Sin embargo, ¿tenemos idea de cómo se llevan a cabo las conexiones? ¿Cómo es posible visualizar los correos y a su vez, mantener una copia de los mismos en nuestro ordenador? Te comentamos al respecto:

Post-Office Protocol Version 3 (POP3)

Es un protocolo estándar de Internet es utilizado por los distintos clientes de correo electrónico. se utiliza para poder recibir correos de parte de un servidor remoto a través de una conexión TCP/IP. Haciendo un poco de historia, POP3 ha sido concebido por primera vez en el año 1984 y se ha vuelto uno de los más populares. Es utilizado por prácticamente el total de los clientes de correo electrónico conocidos, es simple de configurar, operar y mantener.

En la mayoría de los casos, los servidores de correo electrónico son ofrecidos y alojados por parte de los ISP. Si fuese así, dicho proveedor debe de facilitarte los datos para poder configurar correctamente tu cliente de correo electrónico. A parte de visualizar los mensajes, es posible descargar una copia de los mismos y mantenerlos en nuestro ordenador. Una vez que se descargan los mensajes, estos ya desaparecen de parte del servidor remoto. Sin embargo, existen casos en los que los usuarios configuran que los correos se mantengan en el servidor por un período determinado de tiempo.

El número de puerto TCP utilizado normalmente por parte de POP3 es el **110**. Si es que la comunicación cifrada está disponible, los usuarios pueden escoger conectarse mediante el comando **STLS (TLS seguro)** o bien, utilizando **POP3S (POP3 seguro)**. Este último puede valerse de **TLS** o **SSL** en el puerto **TCP 995** para conectarse al servidor de correo.

Internet Message Access Protocol (IMAP)

Es un estándar para el acceso a correos electrónicos alojados en un servidor web, mediante un cliente de correo electrónico local. Para establecer las conexiones de comunicación, utiliza el protocolo de la capa de transporte TCP. Lo cual permite el uso de un servidor remoto de correo electrónico. Ahora bien, el puerto utilizado para IMAP es el **143**. Tiene utilidades y características similares a POP3.

Una consideración importante es que IMAP es protocolo para servidores remotos de archivos, a diferencia de aquellos que se valen del protocolo POP3, el cual permite el almacenamiento de dichos mensajes. En otras palabras, gracias a IMAP los mensajes de correo electrónico **se mantienen en el servidor hasta que el usuario decide borrarlos**. Por otro lado, este protocolo permite la administración de una sola cuenta de correo electrónico de parte de más de un cliente.

Cuando un usuario solicita el acceso a un mensaje de correo electrónico, dicha solicitud se encamina a través de un servidor central. Algunos de los beneficios del protocolo IMAP consisten en la posibilidad de borrar los mensajes del servidor y la búsqueda mediante palabras clave entre los mensajes que se encuentran en nuestro buzón. Por tanto, se puede crear y administrar múltiples buzones y/o carpetas, y la visualización de vistas previas de los mensajes.

Simple Mail Transfer Protocol (SMTP)

Este protocolo, así como los que hemos citado anteriormente, es considerado como uno de los servicios más valiosos de Internet. La mayoría de los sistemas que funcionan a través de Internet se valen de SMTP como un método para enviar/transferir correos electrónicos.

El cliente que quiere enviar un correo electrónico, establece una conexión TCP al servidor SMTP. Después, envía el mensaje a través de dicha conexión. El servidor siempre está en modo *listening*. Tan pronto se hace eco de una conexión TCP, el proceso SMTP inicia una conexión mediante su puerto asignado que es el número 25. Una vez que se haya establecido exitosamente una conexión TCP, el cliente procede al envío automático del correo electrónico.

Podemos toparnos con dos esquemas de funcionamiento SMTP:

- Método Extremo a Extremo (End-to-End)
- Método Almacenamiento y Envío (Store-and- forward)

Primeramente, el **método Extremo a Extremo** es utilizado para la comunicación entre distintas organizaciones. Por otro lado, el **método Almacenamiento y Envío** es utilizado para las comunicaciones entre los hosts que se encuentran en una misma organización. Un cliente SMTP que quiere enviar un mensaje de correo electrónico va a establecer un contacto con su destino para poder enviar el mensaje. El servidor SMTP se va a quedar con la copia del mensaje de correo hasta que el mismo haya llegado a destino.