Tecnológico Nacional de México
Tecnológico de Mérida Yucatán
Ingeniería en sistemas

←Programación web→

Grupo 7SB

Investigación de protocolos de la web

Alumna: Ana Laura Ayil Angulo
Fecha de entrega: 31 de agosto del 2022

Contenido

¿Qué son y para qué sirven los protocolos de comunicación de redes?

La interconexión de sistemas o redes de computadoras son la base de las comunicaciones hoy en día y están diseñadas bajo múltiples protocolos de comunicación. Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red.

Estos protocolos permiten la transmisión de datos desde nuestros dispositivos para navegar a través de los sitios, enviar correos electrónicos, escuchar música online, etc. Entre los varios tipos de protocolos de red se encuentran los protocolos de comunicación de red, el cual contiene protocolos de comunicación de paquetes básicos como TCP / IP y HTTP, de los cuales se hablará más adelante.

Cuando se lleva a cabo la comunicación entre ordenadores conectados a una misma red, los datos se parten en paquetes de datos más pequeños, normalmente tienen una longitud de 1500 bytes, ya que es el típico MTU (Maximum Transfer Unit) que se suele utilizar en las redes.

Explica las características y funcionamiento de los siguientes tipos de protocolos:

Protocolo TCP/IP

TCP/IP define cómo se mueve la información desde el remitente hasta el destinatario. En primer lugar, los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, UDP o TCP. Estos protocolos reciben los datos de la aplicación, los dividen en partes más pequeñas llamadas paquetes, añaden una dirección de destino y, a continuación, pasan los paquetes a la siguiente capa de protocolo, la capa de red de Internet, la cual pone el paquete en un datagrama de IP, pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (si es directamente a un destino o por una pasarela) y pasa el datagrama a la capa de interfaz de red.

La capa de interfaz de red acepta los datagramas IP y los transmite como tramas a través de un hardware de red específico, por ejemplo, redes Ethernet o de Red en anillo. Las tramas recibidas por un sistema principal pasan a través de las capas de protocolo en sentido inverso. Cada capa quita la información de cabecera correspondiente, hasta que los datos regresan a la capa de aplicación.

La capa de interfaz de red (en este caso, un adaptador Ethernet) recibe las tramas. La capa de interfaz de red quita la cabecera Ethernet y envía el datagrama hacia arriba hasta la capa de red. En la capa de red, Protocolo Internet quita la cabecera IP y envía el paquete hacia arriba hasta la capa de transporte. En la capa de transporte, TCP (en este caso) quita la cabecera TCP y envía los datos hacia arriba hasta la capa de aplicación.

Protocolo HTTP y HTTPS

Funcionamiento del protocolo HTTP

HTTP se encuentra ubicado en la capa de Aplicación: “HyperText Transfer Protocol” (o “Protocolo de Transferencia de HiperTexto” en español), este protocolo permite las transferencias de información a través de archivos que se encuentra bajo la World Wide Web (WWW). HTTP es un protocolo sin estado, por lo que no guarda ninguna información sobre conexiones anteriores.

Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web. Así, una página web completa resulta de la unión de distintos sub-documentos recibidos, como, por ejemplo: un documento que especifique el estilo de maquetación de la página web (CSS), el texto, las imágenes, vídeos, scripts, etc...

Cuando el cliente quiere comunicarse con el servidor, tanto si es directamente con él, o a través de un proxy intermedio, realiza los siguientes pasos: Abre una conexión TCP, hace una petición HTTP, lee la respuesta enviada por el servidor y finalmente hace el cierre o reúso de la conexión para futuras peticiones.

Funcionamiento del protocolo HTTPS

Al igual que HTTP, HTTPS se encuentra ubicado en la capa de Aplicación: “HyperText Transfer Protocol Secure” (o “Protocolo Seguro de Transferencia de HiperTexto” en español), este es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. Normalmente utiliza SSL o TLS para cifrar toda la comunicación entre un cliente y un servidor. Esta conexión segura permite a los clientes intercambiar datos confidenciales de forma segura con un servidor, por ejemplo, para actividades bancarias o compras en línea.

En el protocolo HTTP las URLs comienzan con "http://" y utilizan por omisión el puerto 80, las URLs de HTTPS comienzan con "https://" y utilizan el puerto 443 por omisión.

HTTP es inseguro y está sujeto a ataques man-in-the-middle (ataque de intermediario) y eavesdropping (escuchadores secretos) que pueden permitir al atacante obtener acceso a bancos y a cuentas de un sitio web e información confidencial. HTTPS está diseñado para resistir esos ataques y ser más seguro.

Características del protocolo HTTP y HTTPS

HTTP es sencillo: Incluso con el incremento de complejidad, que se produjo en el desarrollo de la versión del protocolo HTTP/2, en la que se encapsularon los mensajes, HTTP está pensado y desarrollado para ser leído y fácilmente interpretado por las personas, haciendo de esta manera más fácil la depuración de errores, y reduciendo la curva de aprendizaje para las personan que empieza a trabajar con él.

HTTP es extensible: Presentadas en la versión HTTP/1.0, las cabeceras de HTTP, han hecho que este protocolo sea fácil de ampliar y de experimentar con él. Funcionalidades nuevas pueden desarrollarse, sin más que un cliente y su servidor, comprendan la misma semántica sobre las cabeceras de HTTP.

HTTP es un protocolo con sesiones, pero sin estados: HTTP no guarda ningún dato entre dos peticiones en la misma sesión. Pero el uso de HTTP cookies, si permite guardar datos con respecto a la sesión de comunicación.

HTTP y conexiones: Una conexión se gestiona al nivel de la capa de trasporte, y por tanto queda fuera del alcance del protocolo HTTP. Aún con este factor, HTTP no necesita que el protocolo que lo sustenta mantenga una conexión continua entre los participantes en la comunicación, solamente necesita que sea un protocolo fiable o que no pierda mensajes

HTTPS y los accesos controlados: El sistema puede también ser usado para la autenticación de clientes con el objetivo de limitar el acceso a un servidor web a usuarios autorizados.

HTTPS y las claves privadas: Un certificado puede ser revocado si este ya ha expirado, por ejemplo, cuando el secreto de la llave privada ha sido comprometido. Los navegadores más nuevos como son Firefox,7 Opera,8 e Internet Explorer sobre Windows Vista9 implementan el Protocolo de Estado de Certificado Online (OCSP) para verificar que ese no es el caso.

Explica que es el SSL

SSL se encuentra ubicado en la capa de Sesión: "Secure Sockets Layer" (o "Capa de Sockets Seguros" en español) es un protocolo criptográfico y la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

Desde el punto de vista técnico, el protocolo SSL es un método transparente para establecer una sesión segura que requiere una intervención mínima por parte del usuario final. En el caso de los navegadores, es posible determinar si un sitio web usa SSL cuando se muestra el candado o la barra de direcciones presenta la URL como HTTPS, en lugar de HTTP.

Nota: el protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL.

Características del protocolo SSL

Cifrado: protege la transmisión de datos.

Autenticación: garantiza que el servidor al que se conecta es, en efecto, el servidor correcto.

Integridad de los datos: garantiza que los datos solicitados o enviados son realmente los datos legítimos.

Protocolo SMPT

Funcionamiento del protocolo SMTP

SMPT se encuentra ubicado en la capa de Aplicación: "Simple Mail Transport Protocol" (o "Protocolo Simple de Transferencia de Correo" en español) este protocolo se encarga de proporcionar servicios de correo electrónico en las redes Internet e IP. Es, en otras palabras, un protocolo de conexión de Internet.

El protocolo SMTP utiliza el protocolo de la capa de transporte TCP, y hace uso de diferentes puertos dependiendo de si el tráfico va cifrado o no va cifrado: Puerto 25 TCP para tráfico sin

cifrar, puerto 465 TCP para tráfico cifrado SSL (SMTPS) o puerto 587 TCP como puerto alternativo para SMTPS con TLS.

El funcionamiento del protocolo SMTP es bastante sencillo, lo primero que debemos tener en cuenta es que SMTP es un protocolo orientado a conexión basado en texto, por tanto, es un protocolo fiable al utilizar el protocolo de la capa de transporte TCP. El cliente de correo se comunica con el servidor a través de una serie de secuencias de comandos para realizar la autenticación, el envío de los mensajes y para cerrar la conexión, por supuesto, el servidor de correo también le responderá con una serie de secuencias de comandos a modo de contestación. En la misma sesión de SMTP se pueden incluir cero o más transacción, en cada una de estas transacciones tendremos un total de tres secuencias de comandos/respuesta que son:

1. MAIL: establece la dirección de retorno.
2. RCPT: establece un destinatario del mensaje, puede emitirse varias veces dependiendo del número de destinatarios.
3. DATA: es el mensaje de texto del correo electrónico, es decir, el contenido del propio correo electrónico. Se compone de la cabecera y también del cuerpo del mensaje.

Una vez que configuramos el cliente de correo correctamente, el email se redacta directamente en el propio cliente de correo, cuando se le da al botón de «Enviar» es cuando empieza todo el proceso:

1. El cliente establecerá la conexión con el servidor SMTP esperando contestación de HELO para recibir la identificación del servidor.
2. El cliente empieza la comunicación con la orden MAIL FROM con la dirección de email, a continuación, el servidor comprobará que el origen es válido.
3. El cliente le enviará un mensaje RCPT TO incorporando el email de destino del correo electrónico, dependiendo de los destinatarios tendremos un mensaje RCPT TO o varios. A continuación, se envía una orden DATA para indicar que viene el cuerpo del mensaje línea a línea.
4. El cliente si no va a enviar más emails, enviará una orden QUIT para terminar la sesión SMTP.

En el caso de enviar posteriormente un email, empezaría todo el proceso nuevamente.

Características del protocolo SMTP

Comandos fáciles: Tiene comandos de textos que son muy fáciles de usar que posee líneas de texto en donde se especifican las instrucciones de este sistema.

Correos electrónicos: Es un protocolo de red que se usa para los mensajes electrónicos y ayuda a que los usuarios se mantengan comunicados mediante un servidor, ya que se envía y reciben mensajes.

Host: Brindan la opción de poder intercambiar mensajes de correo electrónico mediante "hosts TCP/IP hosts" y mediante él existe la opción de poder sincronizar un servidor Smart host.

Está conformado por 3 protocolos que son estándar: estos 3 protocolos se aplican a los correos, dentro de los cuales están: el MAIL, DATA y RCPT

Puede configurarse conjuntamente con otros protocolos: un ejemplo de esto son POP3 o IMAP, pues en ocasiones el SMTP es sólo usado para los correos de salida, mientras que para los de entrada se utilizan los POP3 o IMAP.

Protocolo POP

Funcionamiento del protocolo POP

POP se encuentra ubicado en la capa de Aplicación: "Post Office Protocol" (o "Protocolo de Oficina de Correo" en español) este protocolo se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP. POP3 está diseñado para recibir correo, que en algunos casos no es para enviarlo. El protocolo POP 3 es la última versión del protocolo POP que se actualizó en 1988. Este protocolo se ha ido actualizando a lo largo del tiempo, pero ha seguido manteniendo su nombre POP3

El protocolo POP3 es muy fácil de implementar y la conexión a un servidor POP3 funciona de manera sencilla. El servidor de correo recibe los mensajes y a través del protocolo POP3 los envía al cliente local, es decir, al usuario que utiliza el correo. Estos mensajes pueden enviarse al cliente de dos formas, dejando una copia en el servidor, o moviendo el correo hacia el cliente (por lo que desaparece del servidor).

Mediante el protocolo POP solo un cliente puede conectarse al correo al mismo tiempo, y a la hora de descargar un mensaje se hará de forma completa.

Para conectarse a un servidor POP son necesarios varios datos: Nombre del host, nombre de usuario, contraseña de usuario y un puerto de acceso (normalmente el protocolo POP3 utiliza el puerto 110 para conexiones no cifradas y el puerto 995 con conexiones cifradas).

Características del protocolo POP

Dejar mensajes en el servidor POP: Para poder mantener los mensajes en el servidor, el cliente de correo emplea la orden UIDL (Unique IDentification Listing o "Listado de identificación Única" en español). Para la identificación de los mensajes en el servidor POP3 utiliza el numero ordinal del mensaje.

Órdenes del protocolo POP: Técnicamente hablando, para un cliente de correo con el protocolo POP establecer conexión con el servidor POP abre una conexión TCP en el puerto 110. Una vez establecida la conexión, el cliente envía órdenes al servidor y espera respuestas a estas órdenes. Este flujo de órdenes y respuestas entre el cliente de correo y el servidor POP ocurre mientras la conexión esté establecida.

Seguridad del protocolo POP: En principio el protocolo POP no era muy de fiar. Esto se debía a que las credenciales eran transmitidas entre el cliente de correo y el servidor mediante texto plano, sin ningún cifrado. Actualmente POP3 ha implementado diversos mecanismos de autenticación y cifrado para mantener la seguridad en la comunicación.

Modo de desconexión: La principal ventaja del protocolo POP es la posibilidad de trabajar en modo de desconexión. Ya que el protocolo no requiere estar conectado todo el tiempo al servidor para poder visualizar o eliminar los correos.

Protocolo SSH

Funcionamiento del protocolo SSH

SSH se encuentra ubicado en la capa de Aplicación: "Secure Shell" es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además, permite copiar datos de forma segura, gestionar claves RSA, etc…

En la práctica, el SSH ofrece un mecanismo para que haya la autenticación de ese usuario remoto, garantizando que esa persona tenga autorización para comunicarse con el servidor.

El SSH es accedido vía terminal, independientemente del sistema operacional usado, y entonces es desarrollada la criptografía que va a proteger las informaciones. Por medio de la ventana es hecha la conexión con el servidor remoto, y entonces el proceso se desarrolla.

La criptografía es lo que garantiza, además de la seguridad del sitio, la protección de conexión entre el cliente y el servidor remoto. Sin embargo, hay diferentes estructuras de criptografía que pueden ser aplicadas a la hora de usar el protocolo SSH en esa demanda.

Son, básicamente, tres alternativas:

- Simétrica: Esta es una forma de criptografía que es realizada por medio de una clave secreta, esa que es compartida apenas entre el servidor y el usuario. Su papel es encriptar o des encriptar el mensaje que es transferido en ese proceso, sin embargo, el Secure Shell solo ofrece la lectura del contenido mediante la presentación de esa clave.
- Asimétrica: Ese modelo es el opuesto al anterior: son usadas dos claves, una para el cliente y otra para el servidor, para que haya la criptografía de los datos transferidos. Las claves son llamadas públicas y privadas, formando entonces la combinación necesaria para generar el SSH y su protocolo de seguridad.
- Hashing.: Es un método unidireccional de criptografía usado en el SSH. Esta práctica consiste en crear un hash, por medio de un algoritmo, para garantizar que el mensaje será protegido en una forma específica de criptografía y códigos de autenticación.

Características del protocolo SSH

Verificación de conexión a servidor: Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.

Autenticación segura: El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.

Encriptación robusta y confiable: Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

Reenvió por X11: El cliente tiene la posibilidad de reenviar aplicaciones X11 [1] desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Protocolo FTP y SFTP

Funcionamiento del protocolo FTP

FTP se encuentra ubicado en la capa de Aplicación: “File Transfer Protocol” (o “Protocolo de Transferencia de Archivos” en español) este protocolo proporciona una interfaz y servicios para la transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.

El servidor FTP, en esencia, es un software que está instalado en una computadora con conexión a Internet. Este protocolo tiene como objetivo principal brindar acceso y permitir el intercambio controlado de los archivos que estén dentro de la computadora con otro equipo.

El cliente FTP es el software de cliente es la aplicación que el usuario de un protocolo FTP deberá instalar en su equipo para poder acceder al servidor para poder descargar y cargar archivos. El cliente FTP es el programa que los usuarios deben tener instalado en su equipo computacional para poder subir y bajar archivos. Se le llama “cliente” porque es el cliente (usuario) que se conecta al servidor, aplicando el modelo cliente-servidor de Internet.

Funcionamiento del protocolo FTPS

Al igual que HTTS con HTTP, el protocolo FTPS es la versión segura del protocolo FTP. En esencia, FTPS (FTP sobre SSL) es un protocolo seguro de transferencia de archivos que le permite conectarse de forma segura con sus socios de Negocio, clientes y usuarios. Cuando se envían transferencias de archivos, se utiliza FTPS para el intercambio y se pueden autenticar con métodos que FTPS soporta, como contraseñas, certificados de cliente y certificados de servidor.

FTPS es mucho más seguro, fiable y flexible que las soluciones básicas de transferencia de archivos por FTP o desarrolladas a medida.

Características de los protocolos FTP y FTPS

FTP en subida de archivos: El protocolo FTP es idóneo para subir muchos o pocos archivos, según lo que necesite el usuario.

FTP es bidireccional: El servidor FTP permite subir y bajar archivos de forma bidireccional.

FTP multiplataforma: El FTP se caracteriza por ser multiplataforma, esto quiere decir que funciona bien en cualquier sistema operativo (Windows, Linux y Mac).

FTP y conexiones encriptadas: Este servidor es que soporta conexiones encriptadas, con certificados SSL. En el protocolo de FTP no hay un SSL de por medio así que los datos de usuario, contraseña y la información que se carga y se descarga se envía sin ningún tipo de encriptación.

FTPS y TSL: FTPS utiliza TLS para encriptar las conexiones de los servidores. También utiliza SSL, aunque PCI DSS y la mayoría de los estándares de la industria ahora consideran que SSL no es seguro.

FTPS y los firewalls: puede ser difícil conectar con él a través de firewalls con niveles de Seguridad elevados. FTPS utiliza múltiples números de puerto para los tipos de conexión implícitos y explícitos, lo que significa que se abre otro puerto cada vez que se realiza una transferencia de archivos.

Referencias bibliográficas

KIO Networks 2022. (s. f.). *¿Qué son y para qué sirven los protocolos de comunicación de redes?* kionetworks. Recuperado 30 de agosto de 2022, de https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes#:%7E:text=Estos%20protocolos%20permiten%20la%20transmisi%C3%B3n,como%20TCP%20%2F%20IP%20y%20HTTP.

© Copyright IBM Corporation 2020. (2021, 12 abril). *Protocolos TCP/IP*. IBM. Recuperado 30 de agosto de 2022, de https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols

Individual mozilla.org contributors. (2022, 14 agosto). *Generalidades del protocolo HTTP - HTTP | MDN*. Moz://A. Recuperado 30 de agosto de 2022, de https://developer.mozilla.org/es/docs/Web/HTTP/Overview

colaboradores de Wikipedia. (2022, 27 agosto). *Protocolo seguro de transferencia de hipertexto*. Wikipedia, la enciclopedia libre. Recuperado 30 de agosto de 2022, de https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto

© 2022 GlobalSign. (2020, 27 abril). *¿Qué es SSL?* GlobalSign. Recuperado 30 de agosto de 2022, de https://www.globalsign.com/es/ssl-information-center/what-is-ssl

de Luz, S. (2021, 24 septiembre). *Aprende cómo funciona el protocolo SMTP para correo saliente*. RedesZone. Recuperado 30 de agosto de 2022, de https://www.redeszone.net/tutoriales/internet/que-es-protocolo-smtp-email-configuracion/

HostingPlus Mexico. (2021, 8 marzo). *Protocolo POP: qué es y cómo funciona | Blog | Hosting Plus Mexico*. Hosting Plus. Recuperado 30 de agosto de 2022, de https://www.hostingplus.mx/blog/protocolo-pop-que-es-y-como-funciona/

Gomez, Y. L. (2021, 29 diciembre). *El uso del correo electrónico es uno de los medios de comunicación Leer más*. LovTechnology. Recuperado 30 de agosto de 2022, de https://lovtechnology.com/todo-lo-que-necesita-saber-sobre-el-protocolo-pop/#caracteristicas-del-protocolo-pop

Souza, I. (2020, 16 abril). *Descubre qué es SSH (Secure Shell) y para qué sirve ese protocolo*. Rockcontent. Recuperado 30 de agosto de 2022, de https://rockcontent.com/es/blog/ssh/#:%7E:text=El%20funcionamiento%20del%20protocolo%20SSH&text=El%20SSH%20es%20accedido%20v%C3%ADa,entonces%20el%20proceso%20se%20desarrolla.

Protocolo SSH. (s. f.). MTI. Recuperado 30 de agosto de 2022, de https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html#:%7E:text=El%20protocolo%20SSH%20proporciona%20los,encriptaci%C3%B3n%20robusta%20de%20128%20bits.

U. (2020, 13 abril). *Todo sobre servidores FTP: Qué es, tipo, ventajas, desventajas y más*. HDLider - Servicios profesionales en la nube. Recuperado 30 de agosto de 2022, de https://www.hdlider.com/ftpsftp/todo-sobre-servidores-ftp/#:%7E:text=El%20FTP%20se%20caracteriza%20por,conexiones%20encriptadas%2C%20con%20certificados%20SSL.