Protocolo FTP

Viviana Zambrano, Byron Herrera, Santiago Viñan, Diego Macas,
Students Member, Universidad Nacional de Loja,
viviana.zambrano@unl.edu.ec, byron.herrera@unl.edu.ec,
diego.a.macas@unl.edu.ec, santiago.vinan@unl.edu.ec

***Resumen*—**El Protocolo de Transferencia de Archivos (FTP) es un protocolo ampliamente utilizado para la transferencia de archivos entre un cliente y un servidor. El FTP se basa en una arquitectura cliente-servidor, donde el cliente se conecta al servidor a través de los puertos 20 y 21. Durante el funcionamiento del FTP, se establece una conexión de control en el puerto 21 para enviar comandos y recibir respuestas. Los datos se transfieren a través del puerto 20 en el modo de transferencia de datos activo. Las consideraciones de seguridad que deben abordarse se basan en riesgos asociados, como la exposición de credenciales y la falta de cifrado. Para mitigar estos riesgos, se recomienda el uso de las mejoras de FTP que contemplan una autenticación segura al utilizar protocolos como FTPS o SFTP que proporcionan cifrado para la transferencia de datos. Dentro de su uso, encontramos el compartir archivos, respaldar datos y realizar intercambios de archivos punto a punto. Además, existen herramientas y clientes FTP populares, como FileZilla o WinSCP, que facilitan la gestión de conexiones y la transferencia de archivos.

I. Introducción

En la era digital actual, los protocolos de comunicación juegan un papel fundamental en el intercambio eficiente y seguro de información a través de redes de computadoras. Los protocolos son quienes establecen reglas y estándares que permiten a diferentes dispositivos y sistemas comunicarse de manera coherente y confiable. Dentro de este contexto, el estudio y comprensión en profundidad de protocolos específicos, como el protocolo de transferencia de archivos (FTP), se vuelve crucial para garantizar una transferencia de datos.

El presente artículo tiene como objetivo principal investigar y analizar el protocolo FTP. Como uno de los protocolos más antiguos en la transferencia de archivos, comprender sus características fundamentales, su funcionamiento y las consideraciones de seguridad asociadas al mismo. A través de esta investigación, buscamos proporcionar una visión completa del protocolo FTP, desde su arquitectura cliente-servidor hasta sus aplicaciones prácticas y recomendaciones de seguridad.

II. Desarrollo

El protocolo de transferencia de archivos (FTP) fue desarrollado en la década de 1970 por Abhay Bhushan del MIT(Massachusetts Institute of Technology), con el propósito de facilitar la transferencia de archivos entre sistemas conectados en red. FTP se convirtió rápidamente en un estándar, permitiendo a los usuarios transferir archivos de manera eficiente a través de una arquitectura cliente-servidor.

Debido al gran crecimiento del internet, FTP se volvió esencial en la infraestructura de red, proporcionando una forma simple y compatible de compartir datos. Aunque han surgido alternativas más seguras, FTP sigue siendo ampliamente utilizado en diversas industrias y aplicaciones.

FUNDAMENTOS

FTP se basa en una arquitectura cliente-servidor, donde un cliente FTP realiza solicitudes a un servidor FTP para acceder, enviar o recibir archivos. Esta arquitectura permite establecer una comunicación bidireccional entre el cliente y el servidor, facilitando la transferencia de datos de manera eficiente. El cliente FTP envía comandos al servidor FTP para solicitar acciones, como listar directorios, descargar o subir archivos, entre otras. Por otro lado, el servidor FTP responde a estas solicitudes proporcionando las respuestas correspondientes.

Como parte de transferencia FTP establece dos tipos: activo y pasivo. En la transferencia activa, el servidor establece una conexión de datos directa con el cliente para enviar los datos solicitados. En cambio, en la transferencia pasiva, el cliente establece una conexión de datos con el servidor para recibir los datos solicitados. La elección entre el modo activo o pasivo depende de la configuración de los firewalls y las restricciones de la red.

Los modos de transferencia de archivos, como ASCII se utilizan para transferir archivos de texto y convierte los caracteres especiales según la codificación utilizada. Por otro lado, el modo binario se utiliza para transferir archivos binarios, como imágenes o programas, y mantiene la estructura y el contenido del archivo sin cambios.

FTP se basa en una serie de comandos básicos que permiten a los usuarios interactuar con el servidor FTP. Estos comandos incluyen la autenticación del usuario, la navegación por los directorios, la transferencia de archivos y la administración de la conexión. Algunos ejemplos de comandos FTP comunes son "USER" para ingresar el nombre de usuario, "PASS" para ingresar la contraseña, "LIST" para listar los archivos en un directorio y "GET" para descargar un archivo desde el servidor.

Finalmente, el servidor FTP proporciona respuestas a los comandos enviados por el cliente. Estas respuestas contienen códigos numéricos y mensajes descriptivos que indican el estado y el resultado de la operación solicitada. Los códigos de respuesta se dividen en categorías, como respuestas positivas, respuestas de error y respuestas de información, y proporcionan información importante para el cliente sobre el resultado de su solicitud y cualquier posible problema o error que pueda haber ocurrido durante la operación**.**

FUNCIONAMIENTO

FTP se basa en una secuencia de pasos para establecer la conexión entre el cliente y el servidor. Mismo que trabaja exclusivamente con el protocolo de transporte TCP (Transmission Control Protocol). FTP utiliza TCP para establecer una conexión confiable entre el cliente y el servidor, garantizando que los datos se transmitan de manera segura y sin pérdida de información. TCP proporciona mecanismos de control de flujo, segmentación y retransmisión de paquetes, lo que es fundamental para una transferencia de archivos confiable a través de FTP.

Cuando el cliente inicia la comunicación enviando una solicitud de conexión al servidor a través del puerto de control TCP 21. Después de que se establece la conexión, se lleva a cabo la autenticación y autorización, donde el cliente proporciona su nombre de usuario y contraseña al servidor para acceder a los recursos como se aprecia en la Fig 1.

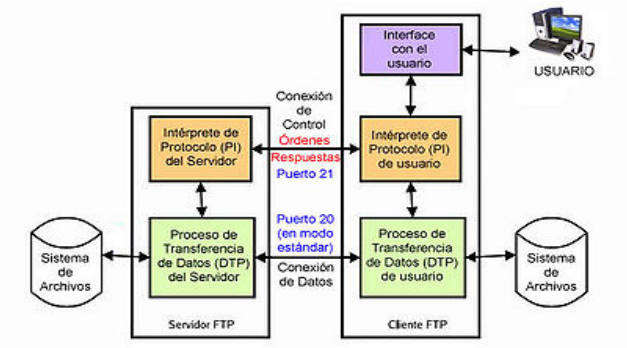


Fig 1. Funcionamiento de FTP

Por otro lado el puerto 20, se utiliza como puerto de datos. FTP utiliza el puerto 20 para enviar los datos al cliente o para recibir datos del cliente. Es importante destacar que el puerto 20 se utiliza solo en el modo de transferencia de datos activo de FTP. En el modo de transferencia de datos pasivo, se utilizan otros puertos dinámicos y aleatorios. Estos mecanismos aseguran un flujo adecuado de datos y permiten la recuperación de errores, como retransmisiones o reconexiones interrumpidas. Al finalizar la transferencia o cuando el cliente decide cerrar la conexión, se utiliza el comando "QUIT" para solicitar el cierre de la conexión y el servidor responde con un mensaje de despedida**.**

SEGURIDAD

Uno de los principales riesgos es la exposición de credenciales de autenticación, ya que el nombre de usuario y la contraseña se transmiten en texto plano, lo que los hace susceptibles a ser interceptados y comprometidos por atacantes. Además, FTP no proporciona cifrado por defecto, lo que significa que los datos transferidos, incluyendo archivos y comandos, también se transmiten en texto plano, lo que facilita el acceso no autorizado y la manipulación de la información.

Para enfrentar estas vulnerabilidades, es importante implementar medidas de autenticación seguras en FTP. Esto implica utilizar métodos de autenticación más robustos, como la autenticación basada en certificados, que proporciona una capa adicional de seguridad al verificar la identidad de los usuarios. Además, es recomendable habilitar el cifrado en la transferencia de datos utilizando protocolos seguros como FTPS (FTP sobre SSL/TLS) o SFTP (SSH File Transfer Protocol). Estos protocolos cifran tanto la autenticación como los datos transferidos, proporcionando una capa adicional de protección.

Las alternativas seguras al FTP incluyen protocolos como SFTP (SSH File Transfer Protocol) y FTPS (FTP sobre SSL/TLS). SFTP utiliza SSH (Secure Shell) para encriptar tanto la autenticación como la transferencia de datos, mientras que FTPS utiliza SSL/TLS para proporcionar cifrado de extremo a extremo. Ambos protocolos ofrecen una mayor seguridad en comparación con FTP estándar y son ampliamente adoptados en entornos donde la seguridad es una prioridad.

APLICACIONES y USOS

El protocolo FTP tiene una amplia gama de aplicaciones y usos en diferentes contextos. Uno de los casos de uso típicos es la transferencia de archivos entre un cliente y un servidor, lo que permite a los usuarios compartir archivos de manera eficiente y conveniente. Esto es especialmente útil en entornos de desarrollo web, donde los archivos del sitio web se cargan y descargan a través de FTP para actualizar y mantener la presencia en línea.

Otro de los usos de FTP se utiliza en entornos de respaldo y almacenamiento, donde los archivos se transfieren de manera regular y automatizada para crear copias de seguridad y mantener la integridad de los datos.

Existen varias herramientas y clientes FTP populares que facilitan la utilización y gestión de conexiones FTP. Algunas de las herramientas más comunes incluyen FileZilla, Cyberduck, WinSCP y Transmit. Estas herramientas proporcionan una interfaz gráfica de usuario intuitiva que permite a los usuarios navegar, cargar, descargar y administrar archivos en servidores FTP de manera eficiente.

III. CONCLUSIONES

Es uno de los protocolos más antiguos y más utilizado desde 1970, es por ello que la seguridad en este protocolo es débil, ya que la transferencia se basa en texto plano, tanto para la autenticación como para la transferencia de datos.

FTP es un protocolo de transferencia de archivos que trabaja mediante TCP, mismo que se maneja bajo una arquitectura cliente-servidor

Las mejoras o actualizaciones para combatir problemas de seguridad en FTP fueron la creación de SFTP y FTPS protocolos que llevan un mejor control de seguridad, como la encriptación de datos o el uso de certificados SSL.

El FTP tiene diversas aplicaciones prácticas, como compartir archivos, respaldar datos y realizar intercambios de archivos punto a punto. Además, existen herramientas y clientes FTP populares, como FileZilla o WinSCP, que facilitan la gestión de conexiones y la transferencia de archivos.

IV. Referencias

[1] R. Bassett, “Aligning India in the Cold War era: Indian technical elites, the Indian Institute of Technology at Kanpur, and computing in India and the United States,” Technology and Culture, vol. 50, no. 4, pp. 783–810, 2009.

[2] M. S. Al-Hakeem, S. M. Zeki, and S. Y. Yousif, “Development of Fast Reliable Secure File Transfer Protocol (FRS-FTP),” Al-Mansour Journal, vol. 19, no. 1, pp. 1–15, 2013.

[3]]J. Andreu, Servicios FTP (Servicios en red). Editex, 2011.

[4] D. Cardoso[1], L. Januário, and L. G. Labegalini, “Protocolo FTP”.

[5] M. Gien, “A file transfer protocol (FTP),” Computer Networks (1976), vol. 2, no. 4–5, pp. 312–319, 1978.

[6]]J. Postel and J. Reynolds, RFC0959: File Transfer Protocol. RFC Editor, 1985.

FTP (File Transfer Protocol)
Protocolo de Transferencia de Archivos

PROTOCOLO FTP

GESTORES DE FTP MAS UTILIZADOS

- **FileZilla**
  - Transferir archivos en segundo plano
- **WinSCP**
  - WedDAV, Amason S**3**
- **Cyberduck**
  - FTP y SFTP
- **Transmit**
  - Mac
  - Amazon s3
  - Google drive

FTP fue desarrollado en la década de 1970 por Abhay Bhushan, como parte del proyecto ARPANET. Desde entonces, ha evolucionado y se ha convertido en un estándar ampliamente utilizado para la transferencia de archivos en redes.

FTP no es un protocolo seguro por defecto, ya que transmite los datos y las credenciales en texto plano. Sin embargo, existen variantes más seguras, como FTPS (FTP sobre SSL/TLS) y SFTP (SSH File Transfer Protocol), que cifran la comunicación y autenticación para mayor seguridad. Es recomendable utilizar estas variantes en lugar del FTP estándar cuando se requiera una mayor protección de los datos.

CARACTERISTICAS

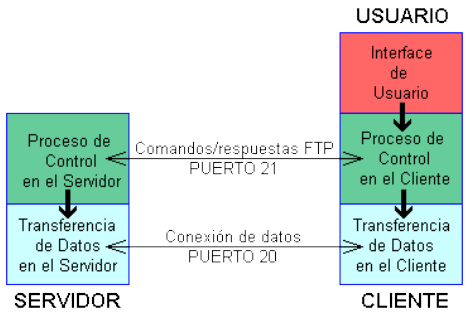
- Permite la transferencia de archivos de un servidor a un cliente y viceversa.(paralelizacion)
- Permite la autenticación de usuarios con nombre de usuario y contraseña.
- Permite la administración remota de archivos en servidores.(carpetas y subcarpetas)

HISTORIA

SEGURIDAD

VELOCIDAD

La velocidad de transferencia en FTP depende de varios factores, incluyendo:
- Velocidad de conexión a Internet,.
- Carga de tráfico en la red,.
- La distancia entre el cliente y el servidor.
- La capacidad de los servidores y la eficiencia de los sistemas de almacenamiento subyacentes.



Puertos 21 (control)

Puertos 20 (datos)

PUERTOS

TIPOS DE TRANSFERENCIA

Modo ASCII

Se encarga de convertir los caracteres según la codificación estándar ASCII. Este modo es adecuado para archivos de texto legibles por humanos, como archivos HTML o scripts.

Modo Binario

Se utiliza para la transferencia de archivos binarios, como imágenes, archivos comprimidos o ejecutables. En este modo, los datos se transfieren byte a byte sin realizar ninguna conversión o interpretación.

COMUNICACIÓN

- Utiliza comandos y respuestas en texto plano.(encriptacion)
- Mantiene un tipo de comunicación cliente y servidor.
- Los comandos en el cliente suelen ser:
  - iniciar sesión
  - listar directorios,
  - transferir archivos, entre otros.
- Las respuestas del servidor indican el estado de las operaciones solicitadas.(codigos estandarizados(exito,fracaso, error)

Servicios

Acceso Anónimo:
Ofrecen sus servicios libremente a todos los usuarios, permitiendo acceder a sus archivos sin necesidad de disponer de ningún identificador

Acceso de usuario
Con este tipo de usuarios, se dispondrá de un usuario y una clave para poder acceder al contenido, pudiendo así subir y bajar información.

Acceso de invitado
Se trata de permitir que cada usuario conecte a la máquina mediante su login y su password, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo

VENTAJAS

- Amplia compatibilidad con diferentes sistemas operativos y plataformas.
- Estándar y protocolo establecido para la transferencia de archivos.
- Soporte para múltiples modos de transferencia y tipos de archivos.
- Amplia disponibilidad de clientes y servidores FTP.

DESVENTAJAS

- Falta de encriptación y seguridad en la versión estándar de FTP.
- Problemas de compatibilidad con cortafuegos y NAT (Traducción de Direcciones de Red).
- Puede ser vulnerable a ataques de interceptación de datos o robo de credenciales.
- No es eficiente en la transferencia de grandes cantidades de archivos o archivos muy grandes debido a la falta de compresión integrada

ERRORES COMUNES

Problemas de conexión, como tiempo de espera agotado o incapacidad para establecer una conexión.
Fallos de autenticación debido a credenciales incorrectas o permisos insuficientes.
Errores de transferencia de archivos, como archivos dañados o interrupciones durante la transferencia.

MODOS DE CONEXIÓN

Modo Activo

El cliente FTP establece una conexión de datos saliente con el servidor FTP. El servidor acepta esta conexión y utiliza un puerto de datos específico para la transferencia de archivos.

Modo Pasivo

El servidor FTP abre un puerto de datos y espera a que el cliente establezca una conexión de datos entrante. El cliente acepta esta conexión y utiliza el puerto de datos del servidor para la transferencia de archivos.

INTEGRANTES:
Byron Herrera
Viviana Zambrano
Diego Macas
Santiago Viñan

DOCENTE:
John Jossimar Tucker Yepez

ASIGNATURA:
Fundamentos de Redes de Datos