

PROTOCOLO DE TRANSFERENCIA DE FICHEROS

DESPLIEGUE DE APLICACIONES



JOEL CAPAPE HERNÁNDEZ
2º DESARROLLO DE APLICACIONES WEB

ÍNDICE

Resumen -----	2
Fundamentación Teórica -----	7
Reflexión Personal-----	10

Portfolio 2 - Protocolo de Transferencia de Ficheros

1. Resumen

- a. Haz un resumen con los contenidos del tema
Protocolo de Transferencia de Ficheros

→ Servicios de Transferencia

Transmitir información en este caso ficheros entre los distintos equipos utilizan el protocolo de red TCP/IP

Correo Electrónico - Adjuntos

Http

P2P

Recursos Compartidos como por ejemplo SAMBA/SMB/CIFS

FTP

→ FTP - Características

Es uno de los servicios más longevos que hay. Tiene las siguientes características:

- Acceder a sistemas remotos y listar directorios y ficheros
- Transferir ficheros desde o hacia el sistema remoto lo que se conoce comúnmente como subir archivos o descargar archivos
- Realizar acciones extras que están relacionadas con la gestión de ficheros y directorios como puede ser: renombrar, borrar y crear archivos y carpetas, cambiar permisos, etc.

Además, tiene fácil mantenimiento y también es fácil de configurar por lo que aporta rapidez a la hora de transferir ficheros.

→ Componentes

Trabaja bajo un modelo cliente/servidor y formado por los siguientes componentes:

- ❖ Clientes FTP: Tienen acceso al sistema de ficheros local, establecen conexiones con servidores FTP para subir o descargar ficheros.
- ❖ Servidores FTP: Tienen acceso al sistema de ficheros del servidor y gestionan las conexiones de los clientes permitiendo a los clientes FTP la subida o descarga de ficheros en función de los permisos que estos últimos tienen
- ❖ Protocolo FTP: Normas y Reglas en base a las cuales trabajan los clientes y servidores FTP. Usan TCP como protocolo de transporte

→ Servidores - FTP

Un servidor FTP es un software que gestiona las conexiones de los clientes FTP y que puede acceder al sistema de ficheros del equipo donde está instalado permitiendo la descarga o subida de archivos. Estos tipos de servidores ofrecen un montón de opciones de configuración como por ejemplo para establecer privilegios a los usuarios, limitaciones en cuanto a la subida o descarga, los tiempos de conexión y espera, entre muchos otros tipos de opciones.

→ Clientes - FTP

Software que accede al sistema de ficheros del equipo donde está instalado y establece conexiones con los servidores FTP para subir o descargar archivos. Existen diferentes tipos de clientes FTP entre los que se encuentran:

- Clientes por líneas de comandos: Los sistemas operativos suelen integrar un cliente FTP que se accede a él a partir de línea de comandos con la orden ftp. Para iniciar la conexión se emplea la sintaxis ftp servidor, cuando se establece la conexión el cliente ofrece al usuario una serie de comandos para realizar diferentes acciones. Con el comando help o ? podemos consultar los comandos disponibles según el S.O. Para ejecutar comandos en local se procede con el símbolo ! salvo con el comando cd que se usa |cd de vez de !cd.
- Clientes gráficos: Estos tipos de clientes ofrecen al usuario una interfaz gráfica que facilita la conexión con el servidor y la transferencia de ficheros.
- Navegadores y Exploradores: Los navegadores y exploradores actuales pueden actuar como clientes FTP. Para poder utilizar los así en la barra de búsqueda tienes que poner ftp, tiene limitaciones, pero tiene un fácil manejo. Ejemplo: ftp://ftp.rediris.es, ftp://alumno@192.168.100.100.

→ Protocolo FTP

La comunicación se basa en el envío de mensajes de texto que contienen comandos y respuestas. Se utiliza TCP como transporte

- Los comandos FTP son cadenas de caracteres que finalizan con el código de final de línea (< CR > + < LF >).
- Las respuestas FTP son enviadas por el servidor como consecuencia de la acción ejecutada al recibir un comando. Están compuestas por un código de 3 dígitos que indican cómo se ha procesado el comando y un mensaje de descripción. Que indican los dígitos:
 - El primer dígito indica si la acción solicitada por comando fue exitosa o fallida
 - El segundo se refiere a la respuesta
 - El tercero ofrece información más específica relacionada sobre el segundo

→ Tipos de Acceso

Para acceder a un servidor FTP existen diferentes tipos de acceso como pueden ser:

- Acceso Anónimo: Te permite, sin tener un usuario o cuenta en un ordenador, poder acceder a sus ficheros. El usuario anónimo solo puede descargar archivos y su acceso se limita a un directorio del servidor.
- Acceso Autorizado: El cliente FTP se conecta con un usuario registrado. Estos a su vez pueden ser:
 - Usuarios locales del sistema operativo donde está el servidor
 - Usuarios virtuales creados para el acceso FTP. Sus datos se pueden guardar en una BBDD, servicios de directorio, ficheros txt, etc.

Una vez el usuario se verifica puede acceder a un directorio del servidor en el que puede estar limitado o no a un directorio, es decir, no puede subir a directorios superiores

En el servidor se configuran los privilegios que tiene cada usuario

→ Conexiones

Servidor y cliente mantienen conexiones FTP separadas para control y transferencia de datos

- **Conexión de Control:** El cliente realiza una conexión con el servidor, le envía comandos y este recibe unas respuestas del servidor que le informan de cómo atiende las peticiones. La conexión permanece activa hasta que el usuario cierra sesión o el servidor la cierre por timeout. Los servidores pueden atender múltiples conexiones dependiendo de cómo se haya configurado el servidor
- **Conexión de Transferencia de Datos:** Cuando el cliente solicita una transferencia de información se crea una nueva conexión de datos que se cierra al finalizar la transmisión. Asociadas a una conexión de control pueden existir múltiples conexiones de datos simultáneas, tantas como transferencias simultáneas y hasta el tope que se haya configurado en el servidor para evitar la sobrecarga.

Para las conexiones de control nunca se envían datos y para las conexiones de datos nunca se envían comandos de control.

Los servidores FTP al principio usaban el puerto 21 para atender las conexiones de control y el puerto 20 para iniciar las conexiones de datos. En la actualidad, debido a una serie de problemas para las conexiones de datos los clientes utilizan puertos mayores a 1023 para iniciar o atender conexiones.

→ Modos de Conexión - Modo Activo

El primer modo de conexión

1. Se inicia el cliente y establece una conexión de control
 - a. Abre un puerto superior al 1023
 - b. Establece una conexión TCP con el puerto 21 del servidor
2. Cuando solicita una transferencia de ficheros

El cliente lanza el comando PORT al servidor en el que se especifica su dirección IP y un número de puerto que abrirá para usar la conexión de datos

 - a. El servicio inicializa una conexión TCP desde el puerto 20 hacia el puerto del cliente
 - b. Se realiza conexión de datos para realizar la transferencia de la información

En este tipo de modo el servidor es el que inicializa las conexiones de datos y el cliente tiene que abrir los puertos para atender dichas conexiones

La máquina que ejecuta el cliente tiene que aceptar las conexiones a puertos, usando para la transferencia de datos, puertos superiores al 1023. Esto puede traer problemas de seguridad al sistema

- ◆ Los cortafuegos donde se encuentra el cliente o en la red a la que pertenece cortaran este tipo de conexiones aleatorias para evitar ataques, y así evitar problemas de seguridad
- ◆ Si el equipo donde está el cliente está detrás de un encaminador/NATP este cortara las conexiones.

Si un NATP implementa ALG, los clientes de la red interna podrán iniciar conexiones FTP utilizando el modo activo. Hay que tener en cuenta que no todos los encaminadores/NATP implementan ALG

→ Modos de Conexión - Modo Pasivo

Este modo de conexión se creó después de observar que el modo activo traía problemas de seguridad

En el modo pasivo es siempre el cliente el que inicia las conexiones con el servidor. No se utiliza el puerto 20

1. El cliente inicia la comunicación y establece una conexión de control
 - a. Abre un puerto local superior a 1023.
 - b. Establece una conexión TCP con el puerto 21 del servidor.
 - c. Esto es igual que el modo activo.
2. Cuando se solicita una transferencia de ficheros
 - a. El cliente envía el comando PASV para activar el modo pasivo. Como respuesta a este comando, el servidor retorna un número de puerto que tenga disponible.
 - b. El cliente inicia una conexión TCP, abre un puerto local superior al 1023 hacia el puerto que le envió el servidor.
 - c. Se utiliza la conexión de datos para realizar la transferencia de información.

El modo pasivo resuelve el problema de que el cliente tiene que aceptar conexiones en puertos mayores a 1023 pero lo traslada al servidor.

La máquina donde se ejecuta el servidor FTP tiene que aceptar conexiones en múltiples puertos y esto es una amenaza para la seguridad del equipo. Los cortafuegos actuales permiten realizar un seguimiento de las conexiones pasivas de datos, comprobando que el cliente que solicita la conexión al puerto especificado por el servidor se corresponde con el cliente al que se le indicó ese puerto y que por tanto la conexión se establece para el envío o recepción de datos.

Si el servidor está detrás de un NATP hay que:

- Configurar en el servidor la IP externa que usa el NATP y un rango de puertos para aceptar conexiones de datos.
- Redirigir el rango de puertos del encaminador que hace NATP al equipo donde está el servidor FTP

→ Tipos de transferencia de archivos

En los servidores FTP existen 2 tipos de transferencia de archivos:

1. Tipo de Transferencia ASCII: Se transmite byte a byte. Se utiliza en archivos de texto
2. Tipo de Transferencia Binario: Se transmite bit a bit. Se utiliza para archivos que no son de texto

Los clientes FTP pueden decidir en qué formato de transmisión se va a en función del archivo a transferir. Algunos clientes detectan automáticamente el tipo de archivo que se va a transferir

→ Seguridad

FTP no es un protocolo seguro. Fue diseñado para ofrecer velocidad, pero no seguridad. Se utilizan mecanismos de autenticación de usuarios para determinar los privilegios de acceso y transferencia en el servidor, pero:

- No se usan mecanismos para garantizar que los equipos involucrados en la transferencia son quienes dicen ser. Es vulnerable a ataques de suplantación de identidad.
- Todo el intercambio de información, incluyendo el usuario y contraseña y la transferencia de cualquier archivo, se realiza en sin ningún tipo de cifrado. Es vulnerable a ataques de análisis de tráfico de red.

→ FTPS

Conjunto de especificaciones que determinan cómo encapsular FTP en SSL o en TLS para ofrecer comunicaciones seguras.

Gracias a la utilización de algoritmos criptográficos y certificados digitales se puede garantizar la confidencialidad y la integridad de la información transmitida, así como la autenticidad de los servidores.

◆ FTPS Implícito

El cliente establece una conexión de control y se establece la conexión SSL/TLS.

Si el servidor no soporta FTPS se cierra la conexión.

Todas las comunicaciones, conexión de control y conexiones de datos, **son cifradas**. El cliente y el servidor no negocian.

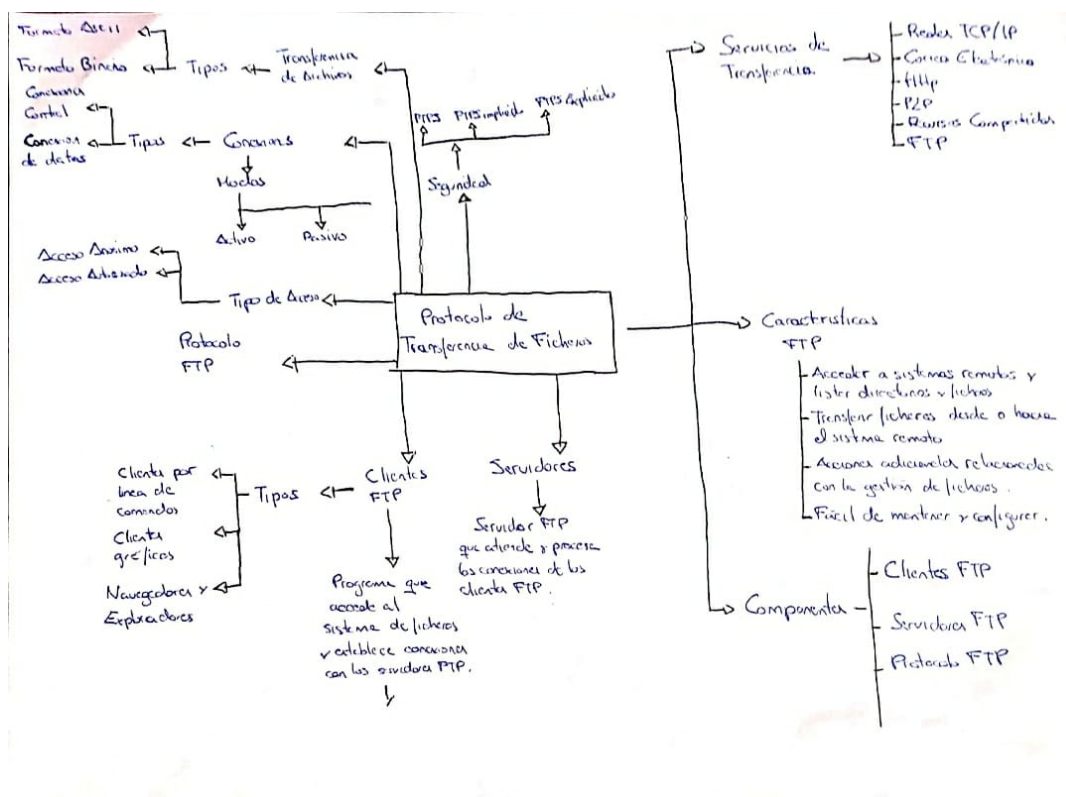
Para mantener la compatibilidad con los clientes FTP que no soportan SSL/TLS se utilizan otros puertos para atender las peticiones FTPS

◆ FTPS Explícito

El cliente establece una conexión de control al puerto 21, solicita que la comunicación sea segura enviando el comando AUTH SSL o AUTH TLS y si el servidor lo soporta se establece una conexión SSL/TLS basándose en algoritmos criptográficos y certificados digitales.

Si el servidor no soporta FTPS le ofrece al cliente la posibilidad de usar FTP no seguro. El cliente y el servidor pueden negociar qué parte de las comunicaciones, conexión de control y conexiones de datos serán cifradas. Permite mayor control sobre la comunicación

b. Realiza un mapa conceptual sobre el tema



2. Fundamentación Teórica

a. Investiga, explica cómo funcionan y las diferencias que tienen los servicios p2p, SMB y FTP.

- P2P

Cada ordenador trabaja como un nodo, es decir, puede ser un cliente o un servidor. De esta forma los usuarios pueden colocar un archivo para compartir y todos los usuarios que quieran ese archivo pueden acceder a ese archivo, creándose varias conexiones hacia este tipo de archivo, de modo que todos los usuarios puedan descargar o subir el archivo por partes. Así, podremos obtener una rápida descarga o subida de archivos, y podremos pausar o parar la descarga a nuestro gusto.

- SMB

SMB es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red como impresoras, enrutadores o interfaces abiertas a la red. El intercambio de información entre los diferentes procesos de un sistema se puede manejar en base al protocolo SMB.

Es un protocolo de red que permite a los usuarios comunicarse con computadoras y servidores remotos para usar sus recursos o compartir, abrir y editar archivos.

- FTP

El funcionamiento de este protocolo es bastante sencillo. Simplemente, un ordenador A se conecta directamente a un ordenador B, y podrá ver los archivos que tiene disponible para compartir. Al verlos, simplemente podrá descargarlos directamente en el equipo que se ha conectado al otro.

Las conexiones FTP tienen una relación de cliente y servidor. Esto quiere decir que un ordenador tiene que estar configurado como servidor FTP, ese en el que se aloja el contenido, y luego tú te conectas a él como un cliente

A partir de cómo funcionan los diferentes servicios explicados en el punto anterior las diferencias que he encontrado entre los 3 servicios son las siguientes:

1. El servicio p2p los usuarios pueden ser cliente o servidor mientras que en el ftp están muy diferenciados los roles
2. El p2p no trabaja bajo una arquitectura cliente-servidor sino una serie de nodos que se comportan como iguales entre sí. Mientras que el ftp y el smb trabajan bajo la arquitectura cliente-servidor.
3. El Bloque de mensajes del servidor (SMB) es un protocolo cliente-servidor para compartir archivos. A diferencia del protocolo para compartir archivos FTP, los clientes establecen una conexión a largo plazo con los servidores.
4. A la hora de descargar en un servidor ftp debe estar el archivo que quieres descargar, necesitas permisos para descargarlo y en ocasiones un usuario y una contraseña mientras que en el p2p los archivos no están en el servidor, los archivos los tienen los usuarios conectados a esa red, descargas de todos los usuarios que tienen ese archivo, trozo por trozo, aunque el usuario de donde estás descargando no lo tenga entero. y el SMB Es un protocolo de red que permite a los usuarios comunicarse con computadoras y servidores remotos para usar sus recursos o compartir, abrir y editar archivos.
5. p2p solo pueden descargar los archivos los nodos que están conectados a esa red, mientras que ftp ofrece una descarga más directa en la cual tu tienes que conectarte directamente al servidor

b. Investiga y realiza una comparativa entre distintos servidores(software) FTP

Filezilla	Proftpd	WinSCP	Cyberduck	Commander one	Forklift
Es compatible con los principales S.O (Windows, Mac, Linux)	Es compatible con MacOS y distribuciones de Linux	Es compatible con Windows	Es compatible con Windows y MacOS	es compatible con macOS,	Es compatible con macOS
Admite encriptación SSL y SSH	Permite la configuración de varios servidores FTP virtuales.	Soporta el cifrado SSL, SSH, SCP	Encriptación SSL y SSH	ofrece diferentes opciones de configuración visual	El software de pago no solo soporta varios protocolos , como FTP, SFTP, SMB, AFP y NFS
Las tasas de transferencia de datos se pueden configurar	Diseñado para funcionar tanto como un servidor independiente o desde inetd / xinetd, dependiendo de la carga del sistema.	Permite la conexión a FTP y a SFTP	conexión a servidores FTP, SFTP, WebDav y servicios en la nube como puede ser Amazon S3	cuenta con gestor de procesos integrado	conexión a servidores FTP, SFTP, WebDav y servicios en la nube como puede ser Amazon S3
Permite la conexión a servidores proxy FTP	Diseñado para funcionar tanto como un servidor independiente o desde inetd / xinetd, dependiendo de la carga del sistema.	La sincronización de directorios se hace de manera completa o semiautomática	regulación del número de transferencias simultáneas	conexión a servidores FTP, SFTP, WebDav y servicios en la nube como puede ser Amazon S3	protección con contraseña para la información del servidor
Tiene mucha documentación	Su diseño es modular, permitiendo ampliar su funcionalidad. Algunos de los principales módulos son; para bases de datos SQL, servidores LDAP, cifrado TLS	El editor de texto está integrado	SSH para guardar y expandir archivos .tar y .zip	Almacena todos los ajustes del servidor y la información de inicio de sesión automáticamente en el llavero de macOS.	organización de archivos simple mediante etiquetas

Usa mecanismos de mantenimiento o de conexión de red	Es compatible con IPv6.	La versión móvil permite su uso sin necesidad de instalación.	encriptación del lado del cliente con cryptonator	Se puede utilizar como FTP client en la versión Pro, de pago	sincronización de directorios y vista previa de imágenes, PDF, texto o función de reproducción (archivos de video, audio).
--	-------------------------	---	---	---	--

c. ¿Qué son los RFCs?

RFC en español como Respuesta de comentarios. Es un documento numérico en el que se describen y definen protocolos, conceptos, métodos y programas de Internet. Algunos RFCs se describen como documentos de información mientras que otros describen protocolos Internet. El organismo IAB mantiene una lista de los RFCs que describen la familia de protocolos. Cada uno de estos tiene asignado un *estado* y un *status*.

No hay nunca versiones diferentes de un RFCs. Por ejemplo, el RFC 1521 que describe el protocolo MIME es una "segunda edición", siendo una revisión del RFC 1341 y RFC 1590 es una corrección al RFC 1521. RFC 1521 es por tanto etiquetada como "Obsoleto RFC 1341; Actualizado por RFC 1590".

d. ¿Qué ventajas ofrece el modo activo en FTP?

Según lo que he investigado el modo activo tiene más inconvenientes que ventajas debido a que es demasiado inseguro y por eso se creo el modo pasivo, pero desde mi punto de vista las ventajas que he encontrado son las siguientes:

1. Favorece la configuración y administración del servidor
2. Las conexiones son abiertas
3. El servidor es él quien inicia la conexión de datos
4. Modo predeterminado de las conexiones, por lo que no hay que configurar otras
5. No hay que abrir un rango de puertos, por lo que no hay riesgo de error

3. Reflexión Personal

a. ¿Qué mecanismos de transferencia de archivos has utilizado? Cuenta tu experiencia.

● FTP

Aquí no tengo ninguna experiencia negativa, más bien la primera vez que use un protocolo de transferencia de archivos como el FTP fue el año pasado y me sorprendió bastante, cuando tuve que subir una página web a internet y tuve que subir la carpeta de la página web para que se viera en internet, me resultó bastante útil a la hora de hacer el mantenimiento de dicha página ya que solo tenía que subir el archivo modificado, y como hay clientes con interfaz gráfica es bastante intuitivo y rápido de utilizar y aprender y esta es la única experiencia que tengo sobre este tipo de transferencia de archivos.

Ahora mismo lo utilizo diariamente en el trabajo y me gusta bastante este tipo de mecanismo

- P2P
Las experiencias que puedo contar sobre este protocolo y que posiblemente le haya pasado a más gente.
Una vez me quería descargar una película y la descarga era muy lenta y mire si era problema de mi internet y no era, el problema era por la velocidad en la que otros usuarios compartían su versión del torrent conmigo.
- SMTP
Una vez utilizando este protocolo tuve un problema en el que mande un trabajo y pensaba que el trabajo se había enviado, al día siguiente el profesor me dijo que no recibió el trabajo y yo le dije que, si se lo había enviado, de hecho a mi me salía que el trabajo se había enviado y se lo enseñe y eso es lo única experiencia destacable que puedo contar sobre este protocolo.
- SMB
Cuando quería compartir archivos entre mi ordenador y una máquina virtual utilizaba este tipo de mecanismo de transferencia de ficheros
- HTTPs
Es el que uso diariamente para transmitir todo tipo de archivos y para hacer aplicaciones web

b. ¿Qué utilidad crees que puede tener para los desarrolladores que tu servidor web sea también servidor FTP? ¿Y para los usuarios?

Yo creo que es bastante útil para un desarrollador web que sea también FTP por los siguientes motivos que expongo a continuación

- Realiza una conexión rápida con el servidor
- Es muy útil a la hora de realizar los mantenimientos de las páginas web si las tienes alojadas en un servidor ftp ya que solo tendrás que subir al servidor los archivos modificados
- Para desplegar páginas web rápidamente ya que solo tendrás que subir la carpeta de la página web
- Tiene interfaces gráficas por lo que es fácil de utilizar, sin la necesidad de utilizar comandos
- Bajar archivos rápidamente
- Soporta conexiones SSL

Para un usuario casual creo que es útil en estos dos casos que expongo a continuación:

- Para un usuario normal puede ser útil para aquellos que aún lo usan de vez en cuando para compartir archivos: una persona puede cargar uno en un servidor FTP y luego compartir un enlace con otra persona. Este tipo de uso se ha vuelto menos usable debido a los servicios en la nube que son más fáciles de usar, pero algunas personas aún prefieren mantener sus archivos alojados en un servidor doméstico y usar FTP para habilitarlo.
- Como pasatiempo o recurso didáctico