CAPÍTULO 5
Servidores Archivos

FTP – Introducción

FTP es un protocolo de capa de aplicación que ofrece un servicio estándar de **transferencia de ficheros** entre sistemas conectados a redes TCP/IP.

- Su funcionamiento se basa en el modelo **cliente/servidor**
- **Abstrae** a los usuarios de los detalles de los **S.O.**
- Es **sencillo** de mantener y configurar.
- Ofrece **rapidez** en la transferencia de ficheros.

FTP – Funcionalidad

FTP permite a los usuarios:

- **Acceder** a sistemas remotos y listar directorios y ficheros.
- Subir (**upload**) o bajar (**download**) ficheros a/desde el sistema remoto.
- Realizar acciones adicionales en el sistema remoto como renombrar, borrar, crear archivos y carpetas (**comandos**).

Servidor FTP

- Un servidor FTP es un programa que **atiende y procesa las conexiones** de los clientes FTP. Puede **acceder al sistema de ficheros** del equipo donde está instalado para la subida y bajada de archivos.
- Ofrecen **opciones de configuración** para los privilegios de los usuarios, limitaciones de subida y descarga, tiempos de conexión y espera, etc.
- Existen **múltiples servidores FTP** libres o propietarios (pago)
  - vsftpd (http://vsftpd.beasts.org/)
  - proftpd (http://www.proftpd.org/)
  - Fillezilla Server (http.//filezilla-project.org/)
  - IIS (http://www.iis.net/) para Windows

Cliente FTP

- Programas que **acceden al sistema de ficheros** del equipo donde están y **establecen conexiones** con los servidores FTP para subir o descargar archivos.
- Existen **múltiples clientes** FTP tanto para sistemas libres como para sistemas propietarios (de pago)
- Se pueden **clasificar** según el **interfaz de usuario** que ofrecen:
  - Clientes en línea de comandos
  - Clientes "gráficos“
  - Navegadores/exploradores

Cliente FTP – Gráficos

- Ofrecen al usuario un interfaz gráfico que facilita la conexión al servidor y la transferencia de ficheros.
- Suelen integrar múltiples funciones adicionales.
- Algunos de los más utilizados son:
  - Filezilla client (http://filezilla-project.org/).
  - WinSCP (http://winscp.net).
  - Gftp (http://www.gftp.org/).
  - SmartFTP (http://www.smartftp.com/).
  - CuteFTP (http://www.global.scape.com/products/ftp_clients.aspx)

ftp

Cliente FTP – Navegadores

- Los navegadores y los exploradores de archivos actuales pueden actuar como clientes ftp con una **funcionalidad limitada.**
- Hay que indicar en la dirección que se realizará la conexión a un servidor FTP
- Ofrecen un cliente FTP limitado pero sencillo de usar.
- Permiten instalar **complementos adicionales** que incluyen clientes FTP más completos

FTP – Tipos de Acceso

Anónimo

- Se usa en el servidor un usuario especial
- Solo permite descargas y acceder a un directorio (se puede parametrizar)
- El id viaja el blanco o con la palabra “anonymous” y sin contraseña

Autorizado

- El cliente FTP se loga con las credenciales de un usuario existente en el servidor
- Este usuario puede ser del SO del servidor, o propio del servicio
- En el servidor se configuran los accesos y privilegios

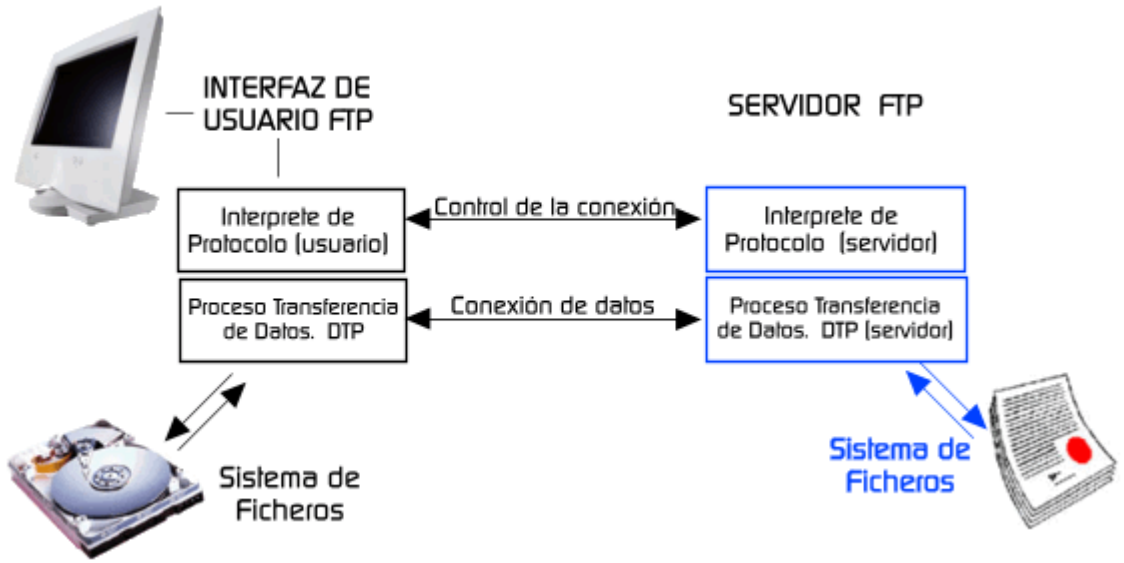
FTP – Doble Conexión

Control

- Intercambio de comandos y respuestas
- Se mantiene activa durante toda la sesión

Datos

- Se utilizan para intercambiar los contenidos de los ficheros
- Puede haber varias simultáneas (configurable)



FTP – Modalidad Conexión

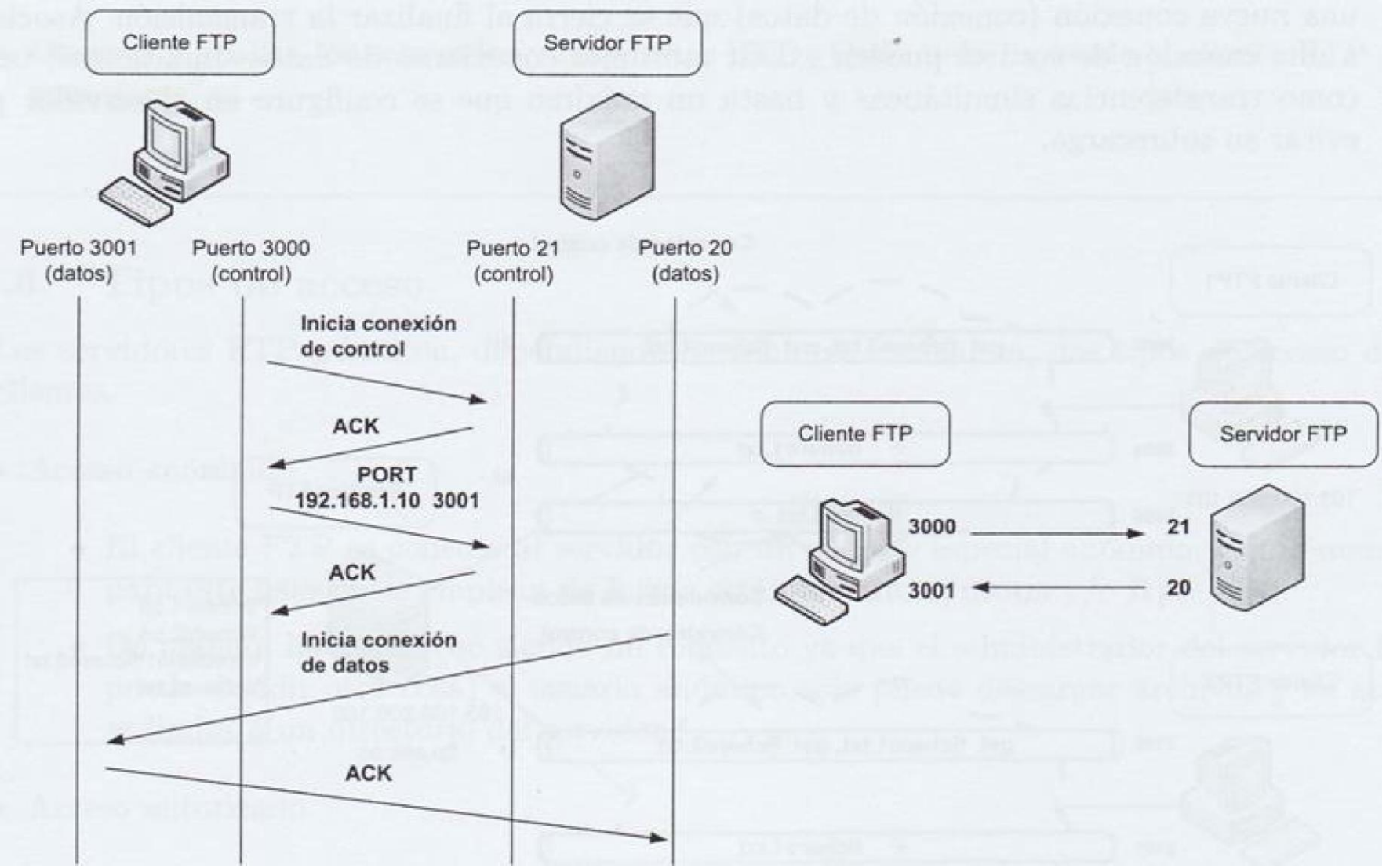
Activa

- El cliente que establece una conexión de control contra el puerto 21 del servidor
- El cliente le indica al servidor el puerto al que conectarse para el intercambio (>1023)
- El servidor utiliza su puerto 20 para enviar la información
- Es más fácil configurar y administrar el servidor FTP pero presenta problemas de seguridad y acceso

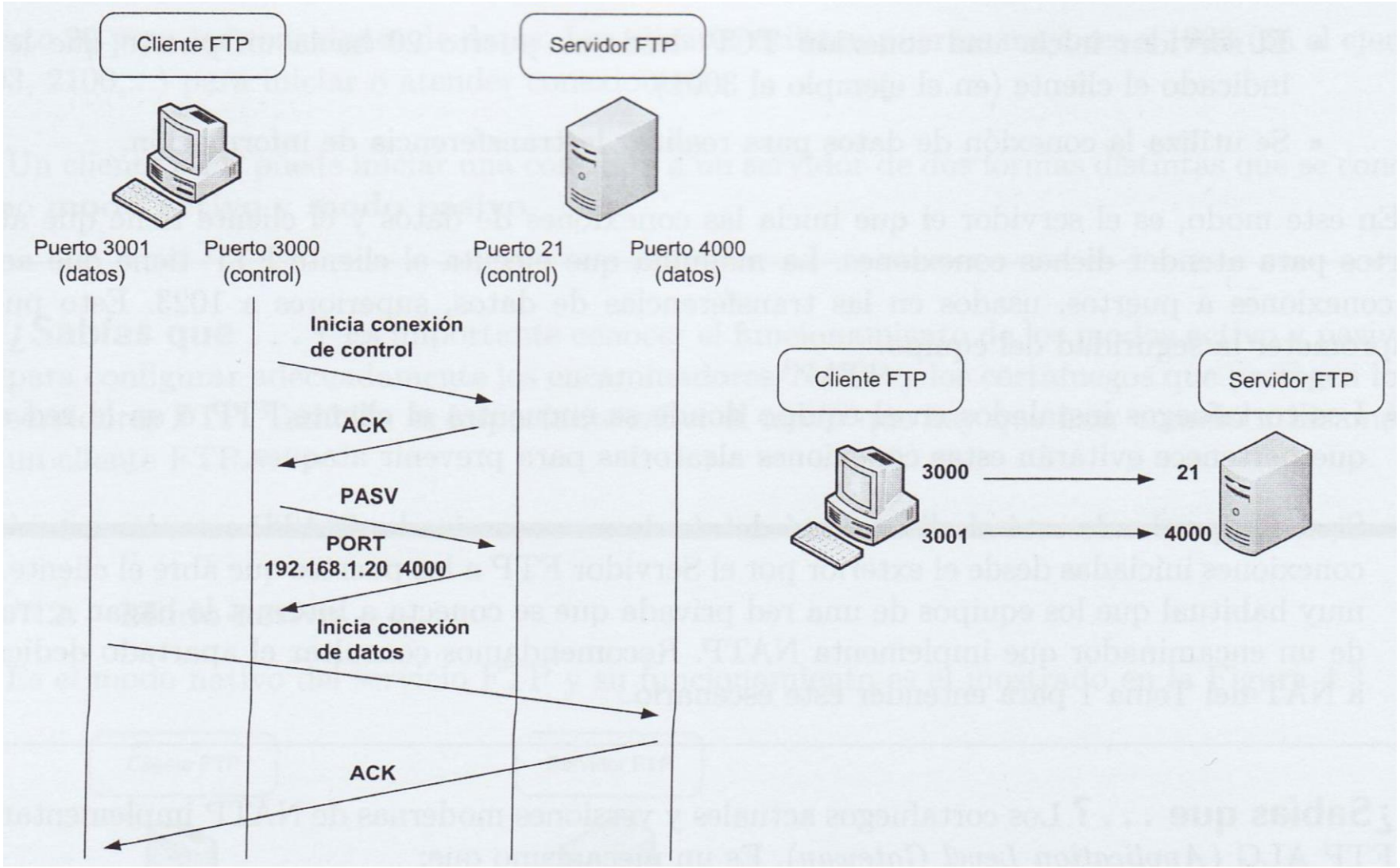
Pasiva

- El cliente que establece una conexión de control contra el puerto 21 del servidor
- (igual que en el modo activo)
- El cliente pregunta por el puerto que debe abrir (>1023) para el intercambio
- El Servidor utiliza un puerto cualquiera (>1023) para intercambiar la información
- Favorece al cliente pero implica configuración más compleja en el servidor.

FTP - Activo


Cliente FTP
Servidor FTP
Puerto 3001
(datos)
Puerto 3000
(control)
Puerto 21
(control)
Puerto 20
(datos)
Inicia conexión
de control
ACK
PORT
192.168.1.10 3001
ACK
Inicia conexión
de datos
ACK
Cliente FTP
Servidor FTP
3000
21
3001
20

FTP - Pasivo


Cliente FTP
Servidor FTP
Puerto 3001
(datos)
Puerto 3000
(control)
Puerto 21
(control)
Puerto 4000
(datos)
Inicia conexión
de control
ACK
PASV
PORT
192.168.1.20 4000
Inicia conexión
de datos
ACK
Cliente FTP
Servidor FTP
3000
21
3001
4000

FTP – Modalidad Transferencia

- Existen dos modos de transferencia de archivos
  - ASCII (type ascii). Se transmite byte a byte. Para archivos de texto (txt, html, java,...)
  - Binario (type bin). Se transmite bit a bit. Para archivos que no son de texto (ejecutables, imágenes, videos,...)
- Los clientes FTP permiten definir el formato de transmisión (ascii o bin) a utilizar en función el tipo de archivo a transferir.
- Algunos clientes ofrecen modo automático que detecta el tipo de archivo y establece el tipo de transferencia adecuado

FTP – Seguridad

- FTP 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 (spoofing).
  - Todo el intercambio de información, incluyendo el usuario y password y la transferencia de cualquier archivo, se realiza en **"texto plano"** sin ningún tipo de cifrado. Es vulnerable a ataques de análisis de tráfico de red (sniffing).
- Los clientes y servidores FTP pueden tener **vulnerabilidades** y ser aprovechadas por potenciales atacantes.

FTPS - Implícito

FTPS son un conjunto de especificaciones que determinan cómo encapsular FTP en SSL o en TLS para ofrecer comunicaciones seguras. Existen dos métodos para implementar FTPS. En el método 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.
- Por compatibilidad con los clientes FTP que no soporten SSL/TLS se utilizan otros puertos para las peticiones FTPS (el 990/TCP para control y el 989/TCP para datos)

FTPS - Explícito

- El cliente establece una conexión de control al puerto 21, solicita una comunicación segura enviando el comando AUTH SSL o AUTH TTL y si el servidor lo soporta se establece una conexión SSL/TLS.
- 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/o conexiones de datos serán cifradas.
- Es el método recomendado porque permite mayor control sobre la comunicación.