

## Unidad Didáctica 3

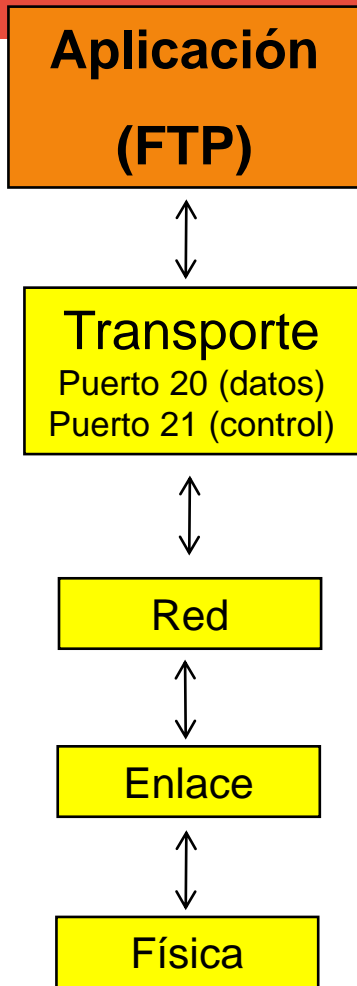
### Servicio de transferencia de ficheros

- 1.- ¿En que consiste el servicio de transferencia de ficheros?
- 2.- Funcionamiento del servicio de transferencia de ficheros. Modo activo y pasivo.
- 3.- Acceso a un servidor FTP.
- 4.- Usuarios y modos de transferencia.
- 5.- Clientes y servidores FTP.
- 6.- Deficiencias de seguridad. Protocolo seguro.
- 7.-FTPS (FTP/SSL)
- 8.- SSH: Secure FTP (SFTP) y SCP
- 9.- El servicio con ... Puesta en marcha.

# ¿Qué es el servicio de transferencia de archivos?

- El servicio de transferencia de archivos permite transferir archivos desde una máquina local a un servidor FTP remoto (“Subir” archivos) y transferir archivos desde el servidor a la máquina local (“Descargar” archivos) *(es posible subir o descargar varios archivos simultáneamente)*
- FTP es el protocolo que regula la transferencia de archivos entre sistemas a través de redes TCP/IP.
- Para utilizarlo hay que disponer de una cuenta en la máquina que va a recibir o enviar los archivos (*servidor FTP*). Numerosos servidores FTP en Internet permiten el uso de sus sistemas utilizando una cuenta anónima validando el password con la dirección de correo.
- El servicio FTP ha evolucionado a lo largo del tiempo y hoy día es muy utilizado en Internet, en redes corporativas, Intranets, etc.
- Utilidad de los servidores FTP:
  - Para manejar sitios web y blogs
  - Para acceder a repositorios de programas de código libre.
- En la actualidad, cuando el usuario se descarga un archivo a partir de un enlace de una página Web no llega ni a saber que lo está haciendo desde un servidor FTP.
- Soportado por cualquier sistema operativo, existe gran cantidad de software basado en el protocolo FTP que permite implementar este servicio.
- Ejemplos servidores FTP públicos:
  - Rediris (<ftp://ftp.rediris.es/>) *(RedIRIS es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional).*

# Funcionamiento del servicio de transferencia de archivos



- El servicio de transferencia de archivos es un servicio basado en la arquitectura cliente/servidor.
- El servidor FTP que proporciona el servicio utiliza dos puertos *por defecto*:
  - El puerto 20 para la transferencia de datos.
  - El puerto 21 para la transferencia de órdenes (control y autenticación).
- El cliente FTP utiliza un puerto aleatorio para establecer la conexión de control (mayor que 1024) y, habitualmente el puerto inmediatamente superior para establecer la conexión de datos (modo activo).
- El cliente puede solicitar al servidor durante la conexión de control que la transferencia de datos se realice por un puerto distinto al 20 (modo pasivo).
- Este protocolo está descrito en el RFC 959 y en él se establecen los objetivos de dicho protocolo.

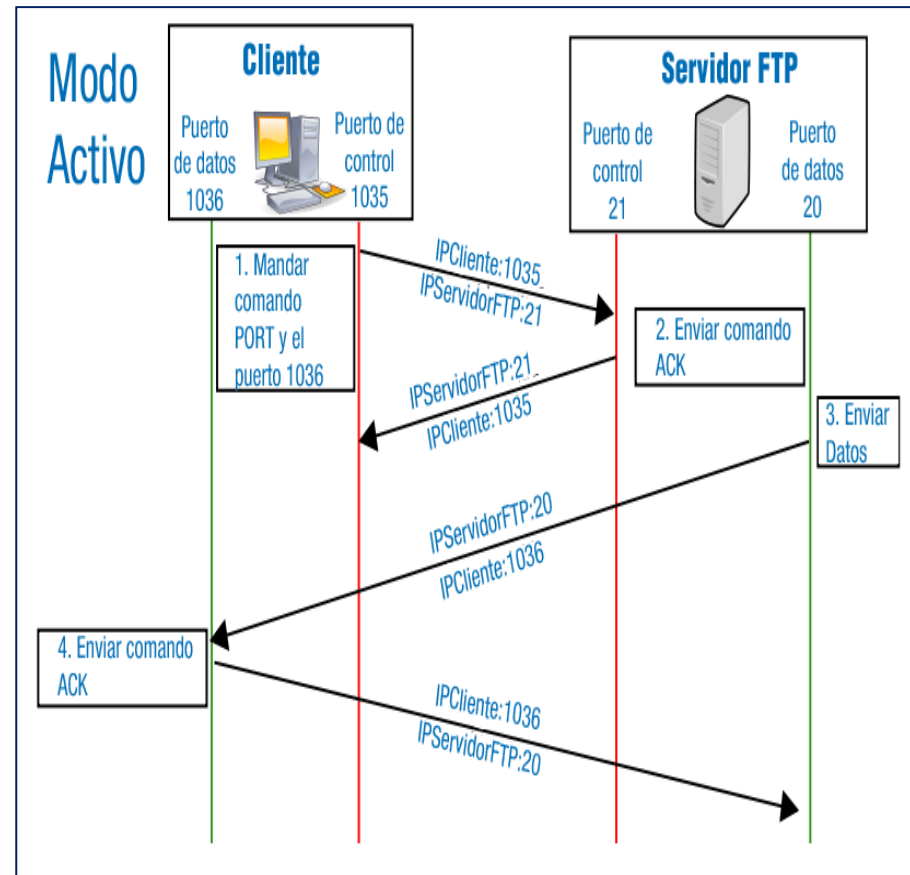
# Funcionamiento FTP. Modo activo.

.Se establece una conexión para la transmisión de comandos por un puerto mayor que 1024 en el cliente y el puerto 21 del servidor.

.Con el comando PORT se indica al servidor el puerto del cliente que está a la escucha de los datos.

.En modo activo, la conexión de datos es iniciada desde el servidor por el puerto 20, hacia el puerto indicado del cliente.

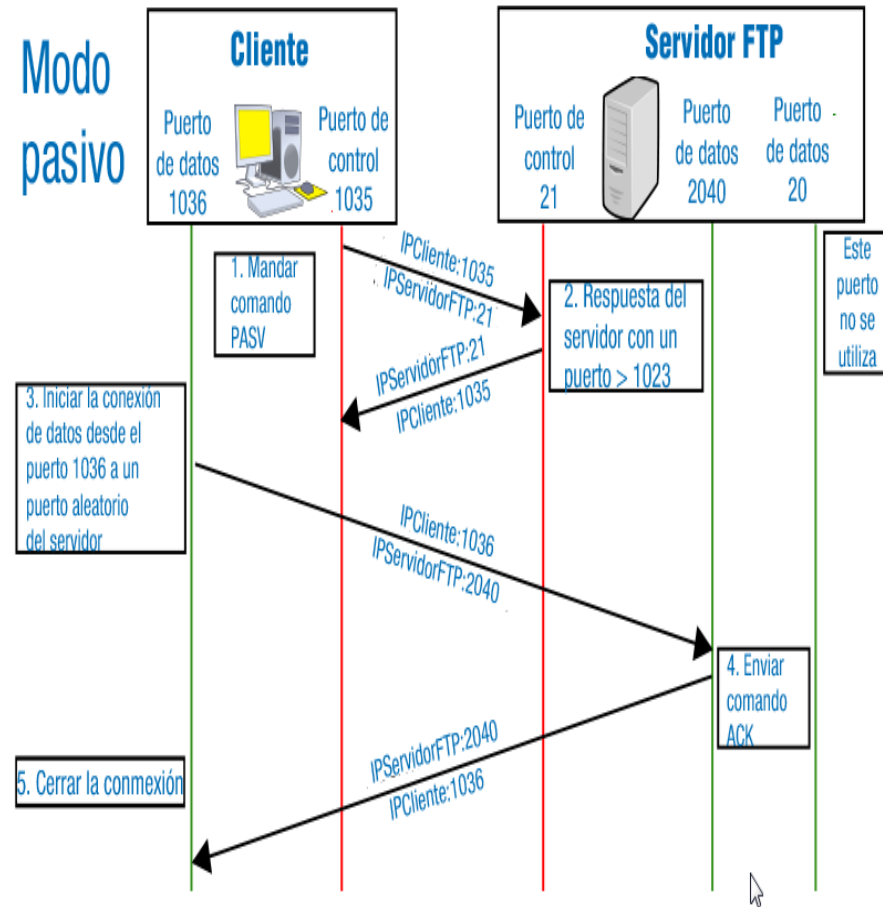
.Inconveniente: la seguridad. El cliente ftp debe estar dispuesto a aceptar cualquier conexión de entrada en un puerto superior al 1024.



# Funcionamiento FTP.

## Modo pasivo. *(recomendado)*

- El cliente envía un comando PASV sobre el canal de control.
- El servidor FTP abre un puerto efímero (mayor que 1024) e informa de ello al cliente FTP
- El cliente conecta con ese puerto del servidor y así no será necesario aceptar conexiones aleatorias inseguras para realizar la transferencia de datos.
- En modo pasivo, es el cliente FTP quien inicia la conexión de datos con el servidor.
- El servidor utiliza un puerto distinto al puerto 20 para la transferencia de datos



# Acceso a un servidor FTP

## Formas de acceso:

- Acceso privado: el cliente se autentifica (nombre de usuario y contraseña).
- Acceso público o anónimo: el cliente no se autentifica (no dispone de cuenta de usuario ni de contraseña). En este caso se utiliza una cuenta de tipo genérico denominada “anonymous o ftp”.
- El acceso al sistema de archivos del servidor FTP está limitado, dependiendo del tipo de usuario que se conecta.

# Usuarios de FTP

Con respecto a los usuarios disponibles desde FTP, existen dos tipos de usuarios:

- **Usuarios FTP:** disponen de una cuenta en la máquina que ofrece el servicio FTP. Se conectan vía FTP mediante su nombre de usuario y una contraseña, y tienen acceso a aquellas partes del sistema de archivos para las que tienen permisos.
- **Usuarios anónimos:** usuarios cualesquiera que, al conectarse al servidor FTP, sólo introducen una contraseña simbólica (dirección de correo electrónico) y sólo tienen acceso a una parte limitada del sistema de archivos.

# Modos de transferencia: texto y binaria.

- Modo texto: transferencia de archivos ASCII (*texto plano*).
- Modo binario: todo lo que no son archivos de texto, como archivos con extensiones .exe, .bin, imágenes, archivos de audio y vídeo, etcétera.

*\*Hoy en día los programas específicos para la transferencia de archivos autodetectan el tipo de fichero a transmitir.*



# Servidores FTP

## –En Windows:

Instalar el servicio FTP Internet Information Server (<http://www.iis.net/>.)

## –En Linux:

- [vsftpd](http://vsftpd.beasts.org/) - Secure, fast FTP server for UNIX-like systems [vsftpd.beasts.org/](http://vsftpd.beasts.org/)
- The *ProFTPD* Project [www.proftpd.org/](http://www.proftpd.org/)
- *Pure-FTPd* - [www.pureftpd.org/](http://www.pureftpd.org/)

## –Filezilla Server (en Windows)

# Cientes FTP. Tipos.

• **Cliente FTP:** aplicación que permite al usuario, desde su máquina local, conectarse a un servidor FTP remoto para solicitar (“descargar”) o transferirle (“subir”) archivos.

• **Tipos de clientes FTP**

– *Modo texto o línea de comandos:* `ftp IP_o_nombre`; utilizando comandos u órdenes definidos para la transferencia de archivos (*get “para descargar” y put “para subir”*)

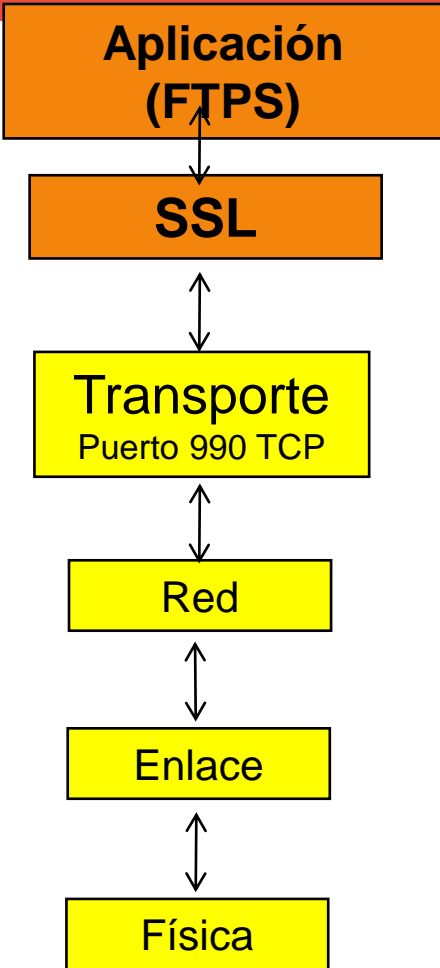
– *Modo web* utilizando el navegador Web como cliente: `ftp://IP_o_nombre`

– *Modo gráfico* utilizando un programa cliente específico, como *FileZilla client*, *WinSCP*,...

# Deficiencias de seguridad

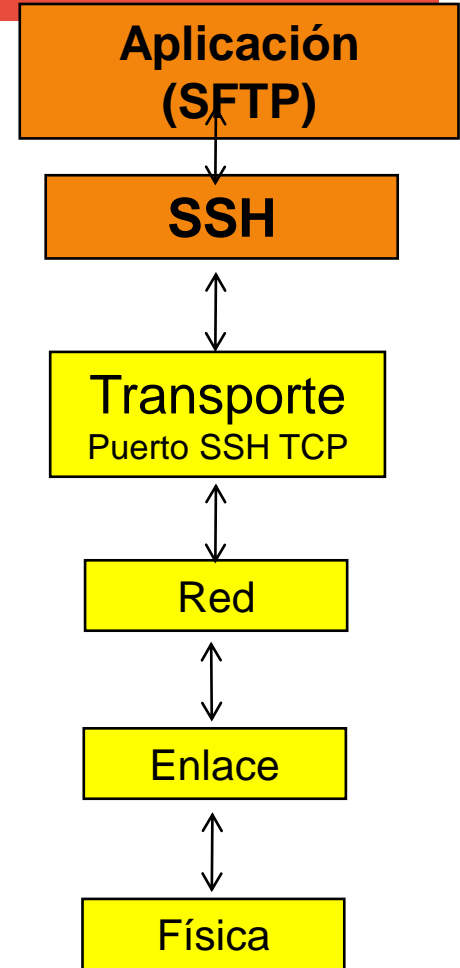
- El protocolo FTP utiliza el mecanismo 'normal' de autenticación de usuarios a través de nombre de usuario (login) y contraseña (password), con lo que el servidor no puede garantizar que el usuario es quien dice ser.
- Transfiere las contraseñas en texto plano, por lo que cualquier herramienta del tipo 'sniffer', como Wireshark podría capturarlas.
- No cifra la propia sesión FTP en sí misma, por lo que las transferencias de archivos también son en texto plano.

# FTP seguro



• Hay dos formas de hacer el protocolo FTP seguro:

- Usando el protocolo SSL
- Usando el protocolo SSH



## FTPS ( o FTP/SSL)

Conjunto de especificaciones que determinan cómo encapsular FTP en SSL (Secure Sockets Layer ) o TLS (Transport Layer Security) 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.

## SSH: Secure FTP / SCP

SSH (Secure Shell Protocol) es un protocolo de capa de aplicación diseñado para ofrecer servicio de acceso a terminales de equipos remotos. Está basado en el modelo cliente/servidor. El cliente SSH permite establecer conexiones a terminales de equipo donde ejecuta el servidor SSH. Los servidores SSH usan el puerto 22/TCP como puerto estándar.

SSH ofrece autenticación, confidencialidad e integridad.

Se autentica a los dos extremos de la conexión

Se cifran los datos intercambiados.

- ✓ Nombres de usuarios y passwords viajan cifrados.
- ✓ La información transmitida viaja también cifrada.

# SSH: Secure FTP / SCP

SSH, además de otras funcionalidades, integra mecanismos de transferencia de ficheros garantizado igualmente autenticación, confidencialidad e integridad. Se basa en los protocolos SFTP (SSH File Transfer Protocol) y SCP (Secure Copy Protocol) Permite la transferencia de ficheros entre sistemas remotos.

- ✓ Permite listar ficheros y directorios del servidor.
- ✓ Permite realizar funciones adicionales en el servidor como renombrar, borrar, crear archivos y carpetas, cambiar permisos, descomprimir,...

## SCP

- ✓ Permite la copia de ficheros entre sistemas remotos.
- ✓ Hay clientes SCP gráficos que integran funcionalidades adicionales como listar, borrar, etc. No son clientes scp "puros".

Los **servidores SSH** atienden peticiones de transferencia de ficheros desde clientes SFTP Y/O SCP. Ejemplos de servidores SSH con OpenSSH (<http://www.openssh.com/>) y WinSSHD (<http://www.bitvise.com/winsshd>).

Existen múltiples **clientes SFTP/SCP** se pueden clasificar según el interfaz de usuario que ofrecen:

- ✓ Clientes en línea de comandos
  - Clientes que se pueden invocar desde la línea de comandos.
  - Clientes scp y sftp (este último ofrece comandos similares a los clientes ftp como get, put, mget, ...)
- ✓ Clientes gráficos
  - La mayoría de los clientes gráficos FTP también pueden actuar como clientes SFTP/SCP.

# El servicio con *vsftpd*. Puesta en marcha.

VerySecure FTP Daemon (*vsftpd*) (<http://vsftpd.beasts.org/>) es un servidor FTP rápido, seguro y fácil de configurar que se distribuye con licencias GNU (General PublicLicense) para sistemas Unix y Linux. Está disponible en los repositorios de software de las principales distribuciones de Linux.

Pasos para su puesta en funcionamiento.

Instalación. (`Apt-get update // Apt-get install vsftpd`. Ello conlleva la creación de:

—Los archivos de configuración.

- `/etc/vsftpd.conf`. contiene un conjunto de directivas que determinan el comportamiento del servidor ftp.
- `/etc/ftpusers`
- `/etc/vsftpd.user_list` (no está creado por defecto; listado de usuarios que pueden acceder al servidor ftp)
- `/etc/vsftpd.chroot_list` (no está creado por defecto; listado de usuarios no enjaulados)
- `/var/log/vsftpd.log`, es el fichero de logs por defecto

—El usuario ftp que se incluye en el grupo ftp.

—El directorio `/srv/ftp` (directorio predeterminado de los usuarios anónimos)

Notas:

- con `ps -ef|grep vsftpd`, comprobarás que el servicio está correctamente iniciado
- para comprobar la creación del usuario ftp y ver que su directorio home es el usuario es `/srv/ftp` se puede ejecutar `cat /etc/passwd` y `cat /etc/group`
- para comprobar que se ha creado el directorio `/srv/ftp` y que su propietario es el usuario root y su grupo es ftp se puede ejecutar `ls -l/srv`

Configurar el servicio ftp.

Para ello es necesario editar archivos de configuración principalmente el archivo *vsftpd.conf* (**consultar *man vsftpd.conf* para tener información sobre las directivas**)

Notas:

- antes de modificar un archivo de configuración debes realizar una copia (ej: `cp vsftpd.conf vsftpd.conf.copia`)
- cualquier cambio en los ficheros de configuración requiere de la reiniciación del servicio a través del comando `/etc/init.d/vsftpd restart` o `service vsftpd restart`