

# SERVICIOS DE RED E INTERNET

**VICEN MORALES**

UD5 - FTP



2012

# INDICE UD 5: Instalación y administración de servicios de transferencia de ficheros

- **Funcionalidad del servicio de transferencia de archivos.**

- Características. Componentes y funcionamiento.

- Protocolo FTP.

- Tipos de usuarios y accesos al servicio: Acceso anónimo y acceso autorizado.

- Configuración del servicio de transferencia de archivos. Permisos y cuotas.

- Conexiones y modos: Conexión de control y conexión de datos. Modos activo y pasivo.

- Tipos de transferencia de archivos: ASCII y Binario.

- Clientes FTP : en línea de comandos, entornos “gráficos” y navegadores / exploradores.

- Monitorización y registro del servicio de transferencia de archivos.

- Seguridad en FTP.

- FTPS (FTP/SSL): FTPS Implícito. FTPS Explícito (FTPES)

- Protocolo FXP (File eXchange Protocol).

- Servicio TFTP (Trivial File Transfer Protocol).

- Servicios SFTP/SCP.

- **Transferencia o distribución de archivos entre iguales (peer-to-peer).**

- Características. Protocolos. Software. Configuración.

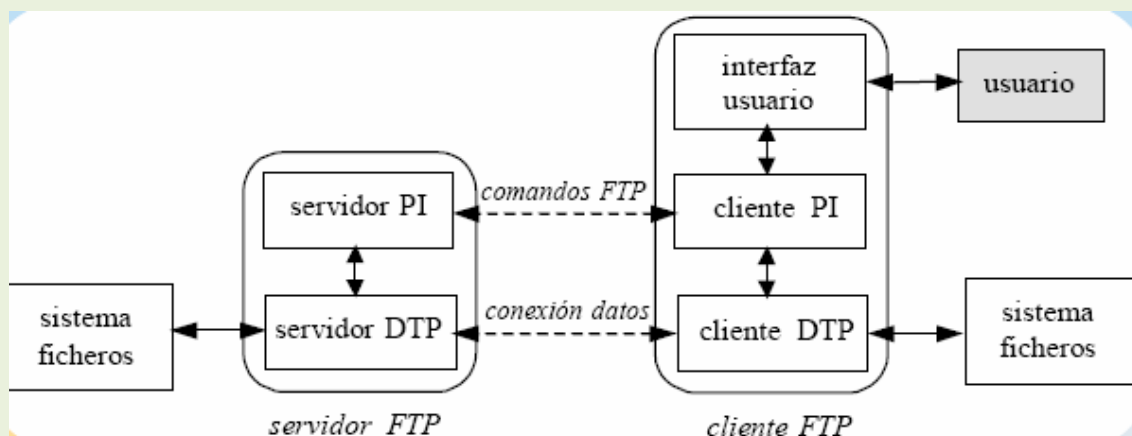
## UD 5: “Instalación y administración de servicios de transferencia de ficheros”

### Funcionalidad del servicio de transferencia de archivos.

#### - Características. Componentes y funcionamiento.

FTP es un programa que se utiliza para transferir información, almacenada en ficheros, de una máquina remota a otra local, o viceversa (RFC 959). Para poder realizar esta operación es necesario conocer la dirección IP (o el "nombre") de la máquina a la que nos queremos conectar para realizar algún tipo de transferencia. Al igual que HTTP, FTP se basa en el envío de comandos codificados mediante ASCII, es decir, en texto plano.

FTP es un servicio orientado a conexión concurrente que funciona sobre dos puertos 21 para el intercambio de comandos y 20 para los datos. La estructura general de funcionamiento es la que se muestra en la siguiente figura.



Los elementos que componen el sistema son los siguientes:

- **Servidor FTP:** Máquina a la que nos queremos conectar y que debe aceptar sesiones FTP. Debe ser una máquina en la que esté activo el servicio FTP. A su vez se compone de:

- o **Servidor PI (Protocol Interpreter):** El intérprete de protocolo del servidor “escucha” en el puerto 21 los comandos que le envía el intérprete de protocolo del cliente y controla el proceso de transferencia de datos del servidor.

- o **Servidor DTP (Data Transfer Protocol):** El protocolo de transferencia de datos del servidor se utiliza para transmitir los datos entre el servidor y el protocolo

de transferencia de datos del cliente. Puede estar en modo “pasivo” a la escucha de conexiones en el puerto 20 de datos.

- **Cliente FTP:** Máquina con la que nos conectamos al servidor FTP. Está compuesta por los siguientes elementos:

- o **Interfaz de usuario:** conjunto de comandos de “alto nivel” que el usuario puede memorizar más fácilmente que los comandos FTP que se envían entre cliente y servidor.

- o **Cliente PI:** El intérprete de protocolo de usuario inicia el control de la conexión a través del puerto 21 con el servidor FTP, envía los comandos FTP una vez codificados por la interfaz de usuario y los envía al intérprete de protocolo del servidor, y controla el proceso de transferencia de los archivos (DTP).

- o **Cliente DTP:** El proceso de transferencia de datos “escucha” el puerto de datos (20) aceptando conexiones para la transferencia de ficheros. En el modelo descrito en la figura anterior, el PI del cliente inicia la conexión TCP por el puerto 21. Al iniciarse, se envían los comandos mediante dicho PI al PI del servidor y si éste acepta la conexión, solicita una identificación al usuario, pudiéndose realizar un acceso anónimo (no aceptado por todos los servidores). Cuando se solicita un archivo del servidor, se establece una conexión TCP por el puerto 20 para entre el DTP del cliente y el servidor para la transmisión de datos.

### **Conectarse al servidor de FTP**

En la máquina local lanzamos el cliente FTP.

Una vez hecho esto nos preguntará el nombre de usuario y la palabra clave. Si tenemos cuenta en el servidor introducimos la pareja username / password que tenemos asignada. Si no tenemos cuenta en el servidor podemos entrar como un usuario anónimo.

Si nos hemos autenticado con éxito aparecerá el prompt de FTP.

FTP>

A partir de este momento ya se pueden utilizar los comandos específicos del FTP.

### **Desconectarse del servidor de FTP**

Para salir de una sesión de FTP, se pueden utilizar los siguientes comandos:

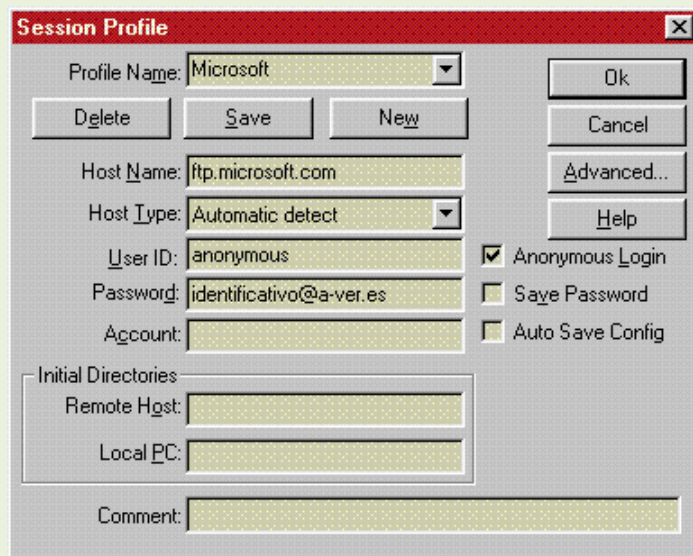
**close:** termina la sesión de FTP, pero no sale del programa.

**bye o quit:** termina la sesión de FTP y sale del programa.

De los directorios de una máquina remota, se puede tomar de ella la información que necesita, o guardar en ella la información que desea compartir. El protocolo FTP (File Transfer Protocol) permite:

- La conexión a un sistema remoto. De los directorios de una máquina remota, se puede tomar de ella la información que necesita, o guardar en ella la información que desea compartir. El protocolo FTP (File Transfer Protocol) permite:

- La conexión a un sistema remoto.



- Observar los directorios remotos.
- Cambiar de directorio remoto.
- Copiar uno o varios archivos hacia el directorio local.
- Copiar uno o varios archivos hacia el directorio remoto.

De los directorios de una máquina remota, se puede tomar de ella la información que necesita, o guardar en ella la información que desea compartir. El protocolo FTP (File Transfer Protocol) permite:

- La conexión a un sistema remoto.
- Observar los directorios remotos.
- Cambiar de directorio remoto.
- Copiar uno o varios archivos hacia el directorio local.
- Copiar uno o varios archivos hacia el directorio remoto.

Se realiza sobre directorios pertenecientes a una cuenta en la máquina remota. Para acceder dicho directorio se requiere conocer el password de la cuenta en cuestión.

- Ftp dirección.- Indica que se desea realizar la conexión a dirección. El sistema remoto solicitará información sobre la cuenta y password remotos.
- Cd directorio.- Indica que se desea entrar en el directorio.
- Cd .. -.- Salir al directorio padre.
- Bin .- Definir que las siguientes transferencias sean binarias (a 8 bits)
- ascii .- Definir que las siguientes transferencias sean en ascii (a 7 bits)
- getarchivo .- Transferir archivo del directorio remoto al local.
- Mget expresión.-Transferir archivos que cumplan con la expresión regular expresión, hacia el directorio local.
- Put archivo.-Transferir archivo del directorio local, hacia el directorio remoto.
- Mput expresión.-Transferir los archivos que cumplan con la expresión regular expresión, hacia el directorio local.
- Bye.- Concluir sesión.

- Observar los directorios remotos.
- Cambiar de directorio remoto.
- Copiar uno o varios archivos hacia el directorio local.
- Copiar uno o varios archivos hacia el directorio remoto.
  - Put archivo.-Transferir archivo del directorio local, hacia el directorio remoto.
  - Mput expresión.-Transferir los archivos que cumplan con la expresión regular expresión, hacia el directorio local.
  - Bye.- Concluir sesión.

### Comandos FTP

Ahora vamos a ver algunos comandos útiles para las sesiones de FTP separados por categorías.

#### Ayuda

FTP posee varios comandos para obtener ayuda de cómo utilizarlo.

#### Comando Acción

? help Muestra una lista de los comandos del FTP de la máquina local.

**help**comando

? comando

Muestra información sobre el comando especificado, correspondiente a la máquina local.

#### Archivos y directorios

A continuación se da una relación de comandos del FTP referentes al manejo de archivos y directorios.

#### Comando Acción

**lcd**Para moverse de un directorio a otro en la máquina local

**lcd**Para cambiar de una unidad de disco a otra, en el caso particular de que la máquina local esa un PC

**cd**Para moverse de un directorio a otro en la máquina remota

**lls**Para listar el contenido de un directorio en la máquina local

**diró ls**Para listar el contenido de un directorio en la máquina remota

**! comando**Para ejecutar un comando en la máquina local

**delete**Para borrar un fichero en la máquina remota

**rmdir**Para borrar un directorio en la máquina remota

**mkdir**Para crear un directorio en la máquina remota

**pwd**Para saber el directorio en el que se está, en la máquina remota

#### Transferencia de información

Con FTP se puede realizar la transferencia de información en dos formatos diferentes: ascii y binario. Por defecto, la transferencia se hace en modo ascii.

**Comando Acción**

**binary** Establece la transmisión en modo binario (para ficheros binarios).

**ascii** Establece la transmisión en modo texto.

**type** Indica el tipo de transmisión activa en éste momento.

**delete** Borra algún archivo existente.

**rename** Renombra algún archivo o directorio.

**rmdir** Borra algún directorio existente.

**put** Transmite un determinado archivo desde nuestro directorio local al remoto.

**mput** Transmite al servidor múltiples ficheros.

**get** Transmite un determinado archivo desde el servidor remoto al directorio local.

**mget** Transmite desde el servidor múltiples ficheros.

**Ejemplo de uso de FTP**

Como ejemplo de uso del protocolo FTP usaremos el programa ftp de que dispone Windows,

para ello abrimos una consola de terminal y escribimos lo que en negrita se muestra a continuación (el resto de líneas son respuestas del servidor):

**C:\>ftp ftp.rediris.es**

Conectado a zeppo.rediris.es.

220-=(<\*>)=-..: (( Welcome to ftp.rediris.es )) ..-=(<\*>)=-

220-You are user number 660 of 1500 allowed

220-<<

220-Bienvenido al FTP anónimo de RedIRIS.

... ..

Usuario (zeppo.rediris.es:(none)): **anonymous**

331- RedIRIS - Red Académica e Investigadora Española

331-

331- ftp://ftp.rediris.es -- http://sunsite.rediris.es

331-

331-

331--- Se puede dejar toda la información o programas que se estimen de --

331--- interés público en el directorio incoming con una nota aclarativa. --

... ..

331 Any password will work

Contraseña:

230 Any password will work

**ftp> type**

Usandomodoascii paratransferirarchivos.

**ftp>helps**

Is Mostrar el contenido del directorio remoto

**ftp>ls**

200 PORT command successful

150 Connecting to port 12014

.

..

.banner

debian

```
debian-non-US
docs
... ..
software
sun
welcome.msg
226-Options: -a
226 24 matches total
ftp: 196 bytes recibidos en 0,01 segundos 13,07 a KB/s.
ftp> cd docs
250 OK. Current directory is /docs
ftp> cd rfc
250 OK. Current directory is /sites/ftp.ietf.org/rfc
ftp> get rfc959.txt
200 PORT command successful
150-Connecting to port 12012
150 143.9 kbytes to download
226-File successfully transferred
226 1.860 seconds (measured here), 77.35 Kbytes per second
ftp: 151249 bytes recibidos en 3,00 segundos 50,42 a KB/s.
ftp> close
221 Goodbye. You uploaded 0 and downloaded 144 kbytes.
ftp>bye
C:\>
```

### - Protocolo FTP.

**FTP** (siglas en inglés de *File Transfer Protocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.



## - Tipos de usuarios y accesos al servicio: Acceso anónimo y acceso autorizado.

Un servidor FTP nos permite dos formas de acceso:

Mediante acceso privado: requiere que el cliente se autentique para poder acceder a él. Es decir, necesitará introducir su nombre de usuario y contraseña. Previamente la cuenta del usuario se deberá haber creado en el servidor.

Mediante acceso público: el cliente no dispone de usuario ni contraseña en el servidor y utiliza una cuenta de tipo genérico denominada "anonymous". Como contraseña suele indicarse la dirección de correo electrónico, no siendo obligatorio.

## - Configuración del servicio de transferencia de archivos. Permisos y cuotas.

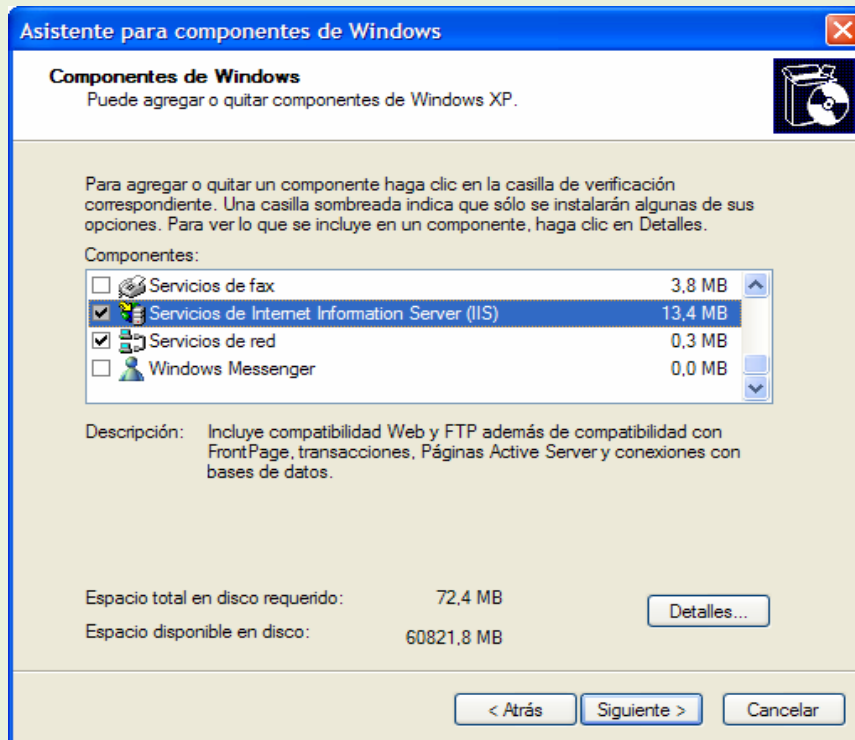
### **Servicio FTP de Internet Information Services (IIS)**

Aunque muchas de las transferencias de archivos que se transmiten por Internet tienen lugar a través de HTTP (recordad los comandos GET y PUT), FTP sigue siendo un protocolo importante si estamos administrando un sitio web público, sencillamente debido a su compatibilidad con el cliente.

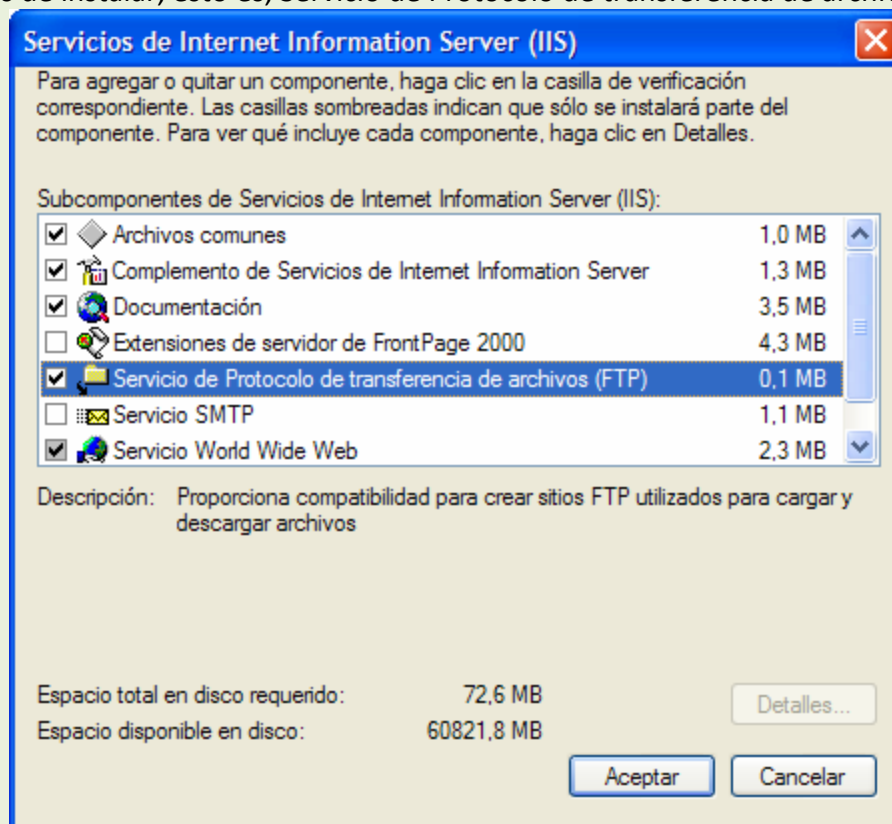
### **Instalación**

La instalación y configuración de este servicio tiene gran similitud con la del servicio HTTP. Principalmente consiste en determinar el directorio que ejercerá de raíz del sitio y establecer toda la estructura de ficheros y directorios a ofertar a los clientes. También podremos establecer otros parámetros adicionales como aquellos que determinen la forma de acceso al sitio FTP por los usuarios (Público o privado), determinar los privilegios que estos tendrán sobre el sitio FTP, si cada usuario tendrá restringido el acceso a su directorio particular o si tendrá acceso al sitio de otros usuarios, limitaciones respecto a la tasa de transferencia, número de conexiones o el tiempo de conexión e incluso asegurar la conexión mediante conexiones seguras. La gestión de espacio en disco o cuotas suele gestionarse a través del sistema de operativo, estableciéndose de forma individual para cada usuario del servicio que necesite alojamiento en el servidor.

Para instalar el servicio HTTP de IIS hay que ir al Panel de Control dentro del menú Inicio y hacer clic en Agregar o quitar componentes de Windows. En la lista de componentes se debe seleccionar Servicios de Internet Information Server (IIS), tal como se muestra a continuación.



Como vemos tenemos instalados los servicios por defecto y el servidor HTTP de la clase anterior (en caso de no estarlo no es necesario instalar el servicio HTTP, pero si los servicios por defecto). En la siguiente figura vemos que componente es el que debemos de instalar, esto es, Servicio de Protocolo de transferencia de archivos (FTP).



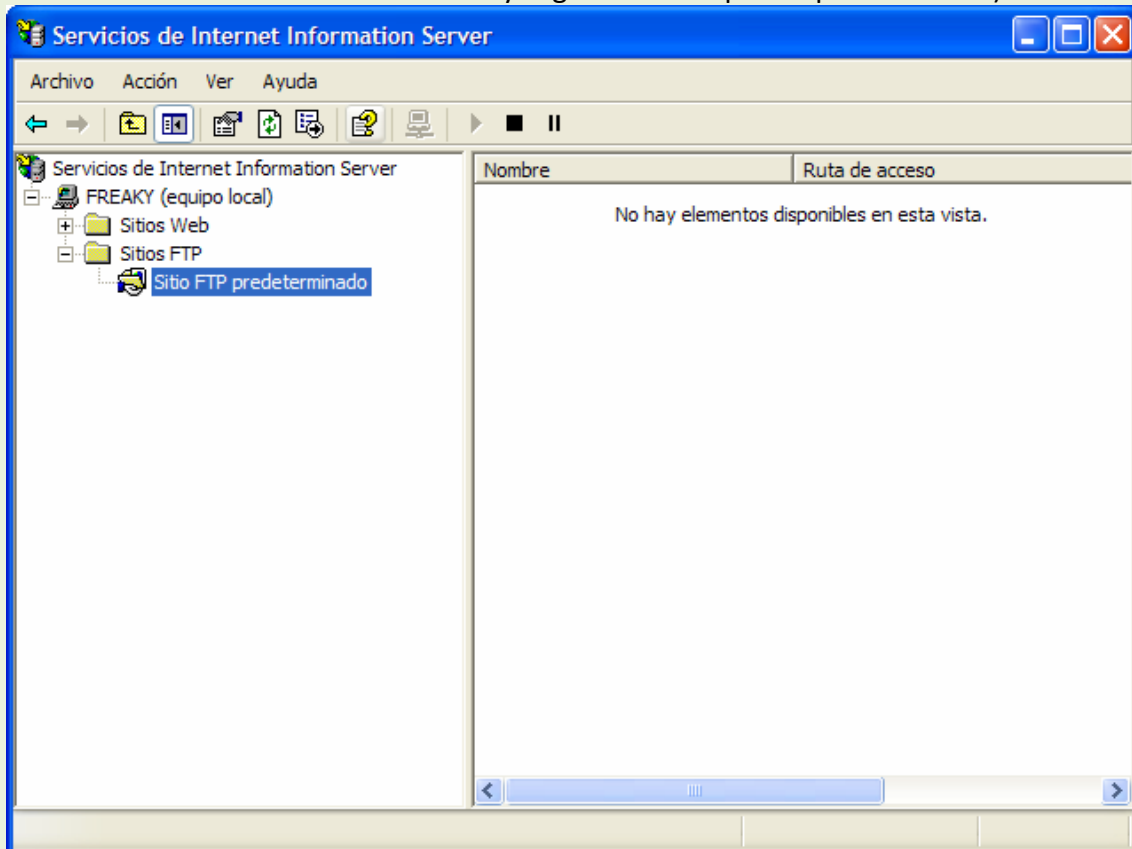
### Creación de un nuevo sitio FTP

Para configurar los servicios FTP en IIS debemos tener la siguiente información preparada.

- Dirección IP a la que debe responder FTP (o si debe responder a todas las direcciones disponibles).
- Número de puerto TCP en que debe responder (por defecto el 21).
- Si se va a permitir acceso de lectura, escritura o ambos.
- Directorio del sistema en el que se alojarán los archivos FTP.

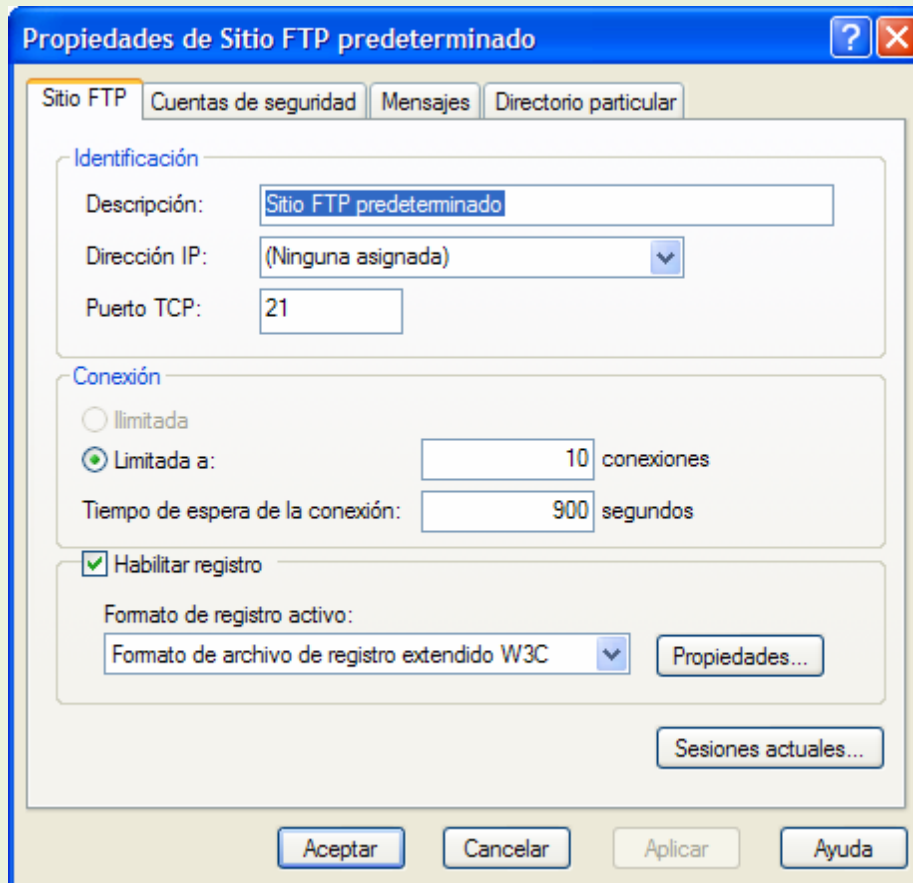
Una vez tengamos claros estos puntos podemos crear un nuevo sitio FTP.

Comenzaremos abriendo la Consola de Gestión de Microsoft, más conocida por MMC. Lo encontraremos en Inicio-Panel de Control-Herramientas Administrativas-Servicios de Internet Information Server. Al abrirla veremos (igual que en la figura siguiente) que se ha creado un nuevo sitio FTP (en caso de que queramos crear uno nuevo, Acción-Nuevo-Sitio FTP se abrirá un asistente y seguiremos los pasos que nos indica).



### Modificación de las propiedades del sitio FTP

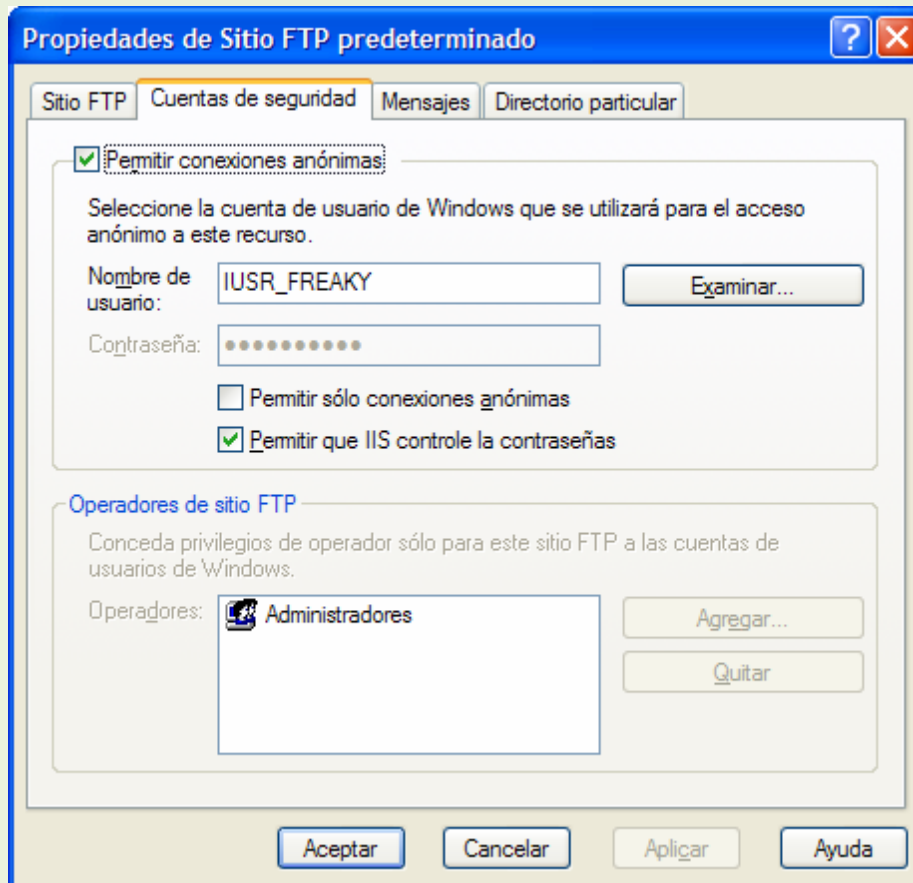
Al igual que hicimos en su momento con las propiedades de un sitio Web, haremos ahora con las de un sitio FTP. Encima de Sitio FTP predeterminado clic derecho-Propiedades.



En la figura anterior vemos una ventana en la que podemos cambiar las *opciones principales* del sitio FTP:

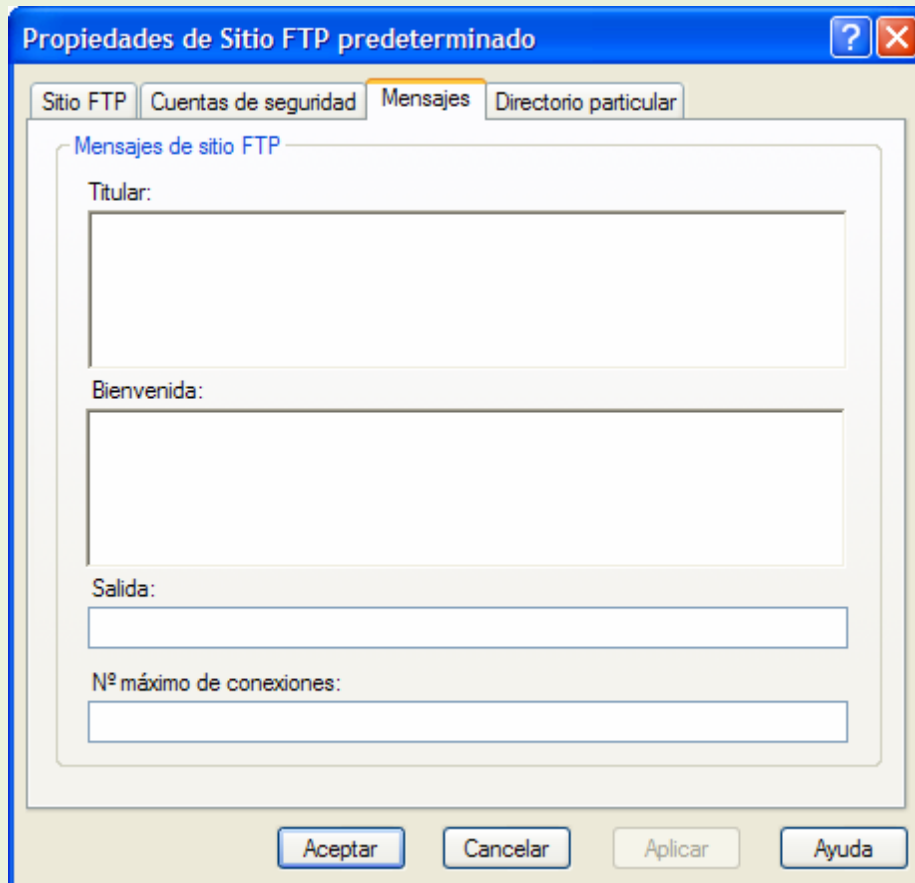
- **Identificación:** Cambiar la descripción del sitio, la dirección IP y el puerto de escucha. El número de puerto puede cambiarse como medio de protección de nuestro sitio.
- **Conexión:** Número de conexiones del servidor y tiempo máximo de estas conexiones.
- **Habilitar registro:** Habilita los logs del sistema que recogen información sobre incidencias.
- **Sesiones actuales:** Técnicamente no se trata de un parámetro que tengamos que ajustar, es más bien una forma de controlar quienes están conectados actualmente a nuestro servidor FTP. Aquí podemos desconectar a los usuarios manualmente si lo deseamos.

La siguiente pestaña nos muestra las *cuentas de seguridad* del sistema, que no se trata más que de los usuarios que pueden acceder al sistema:



En un servidor FTP, los usuarios generalmente hacen dos tipos de conexiones: conexiones anónimas o conexiones de usuario. Las conexiones anónimas son las más comunes en Internet y es así como funcionan la mayoría de los servidores con acceso público.

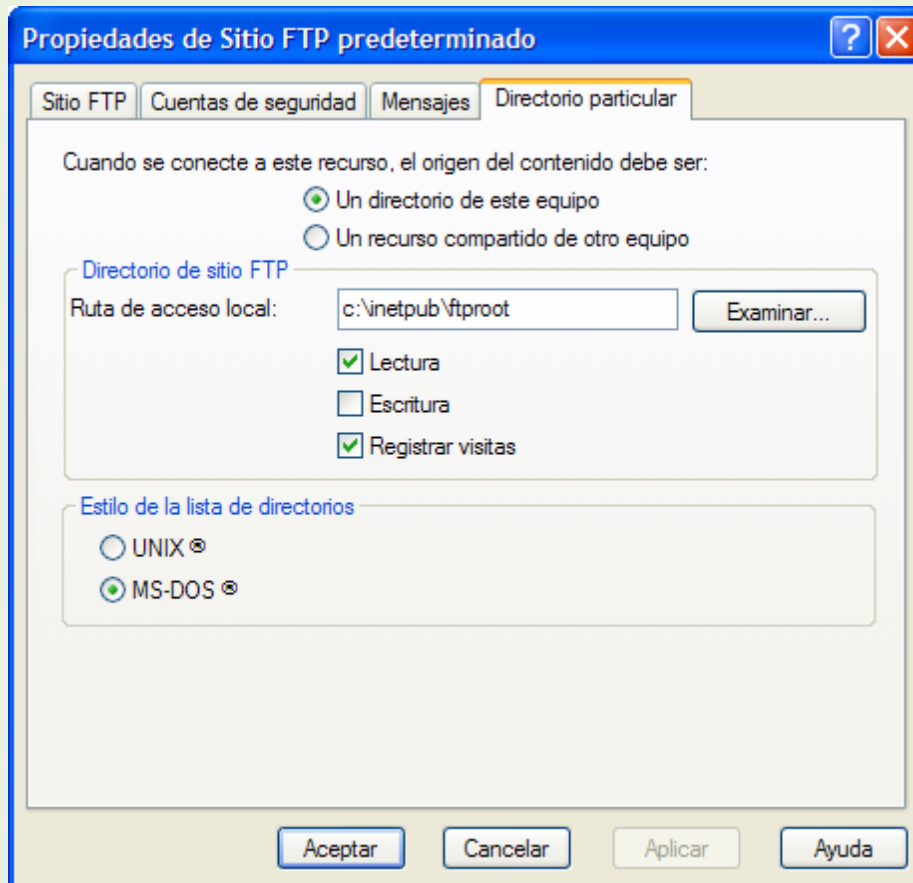
La siguiente pestaña es la de *propiedades de mensaje*, utilizada para configurar los mensajes que queremos que se muestren al cliente cuando se realiza la conexión y se cierra.



Esta opción es muy útil de cara a mostrar mensajes con advertencias legales, sobre colocación de nuevos archivos en el sitio FTP, y cualquier mensaje que el administrador quiera poner.

El mensaje de bienvenida se muestra cuando un cliente se conecta por primera vez al servidor, y en caso de estar usando un navegador como cliente FTP, en cada pantalla del subdirectorio por debajo de la raíz. Si el servidor ha alcanzado el máximo número de conexiones permitidas, se mostrará el mensaje que hayamos establecido en Nº máximo de conexiones. En cuanto a la Salida, si un usuario se desconecta, este será el mensaje que se mostrará. Los navegadores no muestran el mensaje de salida, por lo que si tenemos algo importante que decir, deben hacerse en el de bienvenida.

La última pestaña es la del *directorio particular*, o lo que es lo mismo, la localización de los archivos de FTP y los permisos de seguridad para esta ubicación.



Los parámetros que podemos configurar los describimos a continuación:

- **Localización del contenido:** Directorio en el que se inicia la sesión FTP.
- **Configuración de la seguridad:** Permisos de seguridad adicionales.
- **Registrar visitas:** Si está activa se realiza un seguimiento de las visitas al servidor.
- **Estilo de la lista de directorios:** Formato de Unix o formato de MS-DOS.

#### Directorios virtuales

La definición de directorios virtuales FTP es la misma que para HTTP, el modo de crearlos es el mismo que con el servidor Web. Acción-Nuevo-Directorio Virtual. Aparecerá un asistente en el que tenemos que indicar el alias o nombre del directorio virtual, la localización física del directorio y los permisos de lectura y escritura. Una vez completado podemos modificar las propiedades como siempre.

### Montar servidor FTP en Linux

Un servidor FTP (File Transfer Protocol) nos permite básicamente el compartir o alojar archivos de cualquier tipo en un espacio virtual donde nosotros mismos u otros usuarios de cualquier parte del mundo podrán descargarlos mientras estos sigan dentro del servidor.

#### Modos de un servidor FTP:

**FTP Anónimo:** Es un servidor FTP abierto a todo el público, donde a pesar que se sigue pidiendo un usuario y contraseña, estos serían anonymous y su correo electrónico para poder ingresar, estos usuarios tendrán tanto el privilegio de leer, subir o descargar archivos del servidor.

FTP Privado: Este servidor realiza las mismas funciones que el anónimo pero los usuarios que pueden ingresar al mismo son únicamente los que se encuentran dentro de la base de datos del sistema local sin excepción alguna.

Para montar nuestro servidor FTP vamos a utilizar VSFTPD ( VerySecure File Transfer ProtocolDaemon ) que actualmente se sitúa como el servidor más seguro y más utilizado en el mundo, además de contar con un método de configuración bastante fácil.

### Instalación

Debian/Ubuntu: apt-getinstallvsftpd

RedHat/Fedora: yum -y installvsftpd

\*Genérico: Descargamos el archivo desde <http://vsftpd.beasts.org/> . Lo descomprimos, configuramos y compilamos con las opciones predeterminadas e instalamos.

```
tarxvf vsftpd-2.0.5.tar.gz && cd vsftpd-2.0.5/ && make && make install
```

### Archivos de Configuración

/etc/vsftpd.user\_list : Es la lista que va a establecer que usuarios pueden o no utilizar el servicio.

/etc/vsftpd/vsftpd.conf : Archivo de configuración.

### Configuración

Vamos a abrir el archivo /etc/vsftpd/vsftpd.conf con permisos de administrador( root ) utilizando nuestro editor de texto

preferido; puede ser mediante gedit, vi, pico, nano, etc... ( Podemos utilizar el comando sudo para abrir el editor con permiso de administrador)

-Opción anonymous\_enable.

Esta opción nos permite establecer si el servidor aceptará o no acceso anónimos, se establece como valor "YES" o "NO".

```
anonymous_enable=NO
```

-Opción local\_enable.

Esta opción nos permite establecer si el servidor se combinará con la función de jaula o chroot, de esta manera se define si se permitirán accesos a los usuarios locales del sistema, los valores son "YES" o "NO".

```
local_enable=NO
```

-Opción write\_enable.

Con esto establecemos si se va a permitir escribir en el servidor. Los valores son "YES" o "NO".

```
write_enable=YES
```

-Opción ftpd\_banner.

Aquí podemos establecer un mensaje de bienvenida que se mostrará al usuario cada vez que se conecte.

```
ftpd_banner=Bienvenido al servidor FTP.
```

### Control de Ancho de Banda

-Opción anon\_max\_rate.

Se utiliza para establecer el máximo de bytes por segundo para usuarios anónimos, el ejemplo muestra un máximo de

5kbps.



anon\_max\_rate=5120

-Opción local\_max\_rate

Igual que la opción anterior pero para usuarios locales.

local\_max\_rate=5120

-Opción max\_clientes.

Establece el número de conexiones simultaneas al servidor.

max\_clients=10

-Opción max\_per\_ip.

Establece el número de conexiones que se aceptarán al servidor desde la misma

ip

max\_per\_ip=3

### Inicialización del Servidor

Para ejecutar el servicio por primera vez ejecutamos con permisos de administrador (root):

```
/etc/init.d/vsftpdstart
```

Si hemos hecho algunos cambios a la configuración mientras el servidor está activo lo reiniciamos con:

```
/etc/init.d/vsftpdrestart
```

Para detenerlo usamos:

```
/etc/init.d/vsftpd stop
```

### PERMISOS Y CUOTAS

El protocolo FTP se desarrolló en entornos de tipo UNIX similares a los populares GNU/Linux.

Por eso tenemos los permisos de ejecución, lectura y escritura, estableciéndose tres tipos de usuarios:

- **Propietario:** Es normalmente la persona que ha creado o que ha subido el archivo al servidor FTP.
- **Grupo:** Se refiere a un grupo de usuarios al que probablemente pertenece el propietario.
- **Otros:** Son todos los demás usuarios anónimos o que no pertenecen al grupo indicado.

Para establecer los permisos de escritura existe un algoritmo, el cual asigna valores al tipo de acceso que se quiere otorgar a cada tipo de usuario.

- 4=lectura
- 2= escritura
- 1= ejecución

Los permisos se asignan acorde con la suma de los tipos ya descritos. Por ejemplo:

- 6 (4+2) = lectura y escritura
- 5 (4+1) = lectura y ejecución
- 3 (2+1) = escritura y ejecución

- 7 (4+2+1) = lectura, escritura y ejecución

Las combinaciones se dan en el siguiente orden: propietario, grupo y usuarios.

Por ejemplo: 755, otorga lectura, escritura y ejecución al propietario, y al grupo y otros le otorga los permisos de ejecución y lectura.

Para cambiar los permisos, en Windows XP, basta con enviar el comando literal `chmod 755 /`, lo que permite que la carpeta raíz tenga los permisos descritos.

**Más información sobre asignar permisos en:**

<http://www.ignside.net/man/ftp/chmod.php>

Para establecer permisos con el FileZilla, se hace lo siguiente:

1. Clic con el botón derecho del mouse sobre la(s) carpeta(s) y/o archivo(s) que desees establecer permisos, recuerda que para seleccionar más de un archivo o carpeta, selecciónalos manteniendo pulsada la tecla Ctrl o Alt; haces clic en atributos del archivo o File Attributes, dependiendo el idioma en que lo tengas.



2. Nos aparecerá una ventana, seleccionaremos los valores que deseemos cambiar, o bien, escribir en el cuadro de abajo los dígitos.



3. Presionamos el botón OK, y si nuestras modificaciones fueron procesadas exitosamente, en la parte de arriba aparecerá un mensaje diciendo Directorylistingsuccessful.

```
Comando: PASV
Respuesta: 200 Type set to A
Comando: LIST
Respuesta: 150 Opening ASCII mode data connection for file list
Comando: PASV
Respuesta: 226 Transfer complete.
Estado: Directory listing successful
```

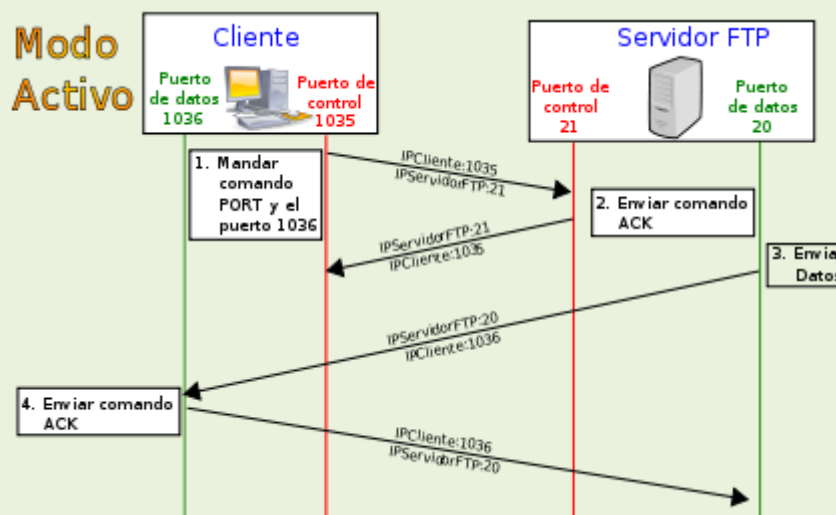
## - Conexiones y modos: Conexión de control y conexión de datos. Modos activo y pasivo.

Para lograr su objetivo, el protocolo FTP establece una doble conexión TCP entre el cliente y el servidor:

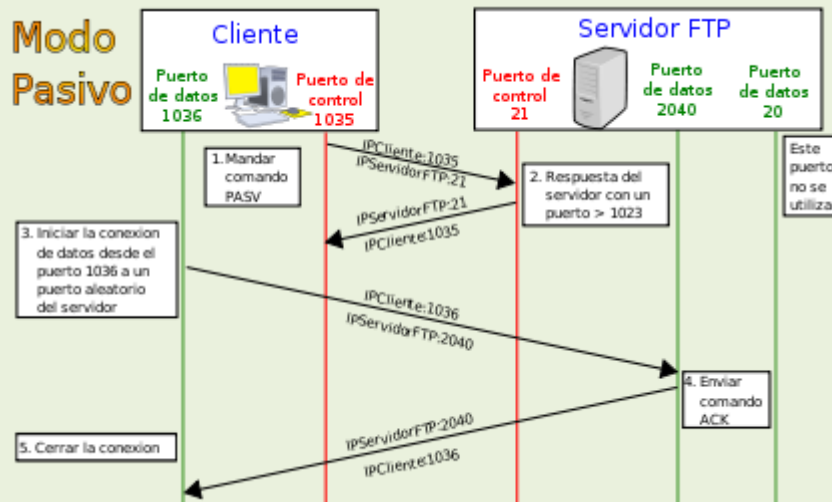
-Conexión de control: suele utilizar el puerto 21 del servidor y es la que sirve para acceder a éste e indicarle las operaciones que el cliente desea realizar.

-conexión de datos: habitualmente se utiliza el puerto 20 del servidor y es la que sirve para la transferencia de archivos hacia o desde el servidor. El cliente puede negociar con el servidor un puerto distinto para establecer esta conexión, distinguiéndose dos modos:

Modo activo: el cliente establece una conexión con el puerto habitual de datos para realizar la transferencia. Es el modo por defecto.



Modo Pasivo: el cliente utiliza la conexión de control para solicitar al servidor la utilización de un puerto distinto al habitual para la transferencia de datos. El servidor comunicará al cliente el puerto por encima del 1024 por donde atenderá la conexión de datos. El cliente utiliza un puerto aleatorio para establecer la conexión de control y habitualmente el puerto inmediatamente superior para establecer la conexión de datos. Por ejemplo el cliente podría utilizar su puerto 1045 para la conexión de control con el puerto 21 del servidor y el 1056 para la conexión de datos con el puerto 20 del servidor, siempre y cuando el cliente no requiera un modo pasivo.



### - Tipos de transferencia de archivos: ASCII y Binario.

Para transferir un archivo puede determinarse su tipo: texto o binario. Esto evitará, por ejemplo, que al obtener un fichero ejecutable (binario) transferido como texto, no se ejecute. Si no lo indicamos, la transferencia se realizará según la configuración por defecto del servidor. Hoy en día, la utilización de programas específicos auto detectan el tipo de fichero a transmitir y no requiere que se especifique su tipo.

Es importante conocer cómo debemos transportar un archivo a lo largo de la red. Si no utilizamos las opciones adecuadas podemos destruir la información del archivo. Por eso, al ejecutar la aplicación FTP, debemos acordarnos de utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica):

- tipo ascii

Adecuado para transferir archivos que sólo contengan caracteres imprimibles (archivos ASCII, no archivos resultantes de un procesador de texto), por ejemplo páginas HTML, pero no las imágenes que puedan contener.

- tipo binario

Este tipo es usado cuando se trata de archivos comprimidos, ejecutables para PC, imágenes, archivos de audio...

Ejemplos de cómo transferir algunos tipos de archivo dependiendo de su extensión:

#### Extensión de Archivo Tipo de Transferencia

txt (texto)                      ascii

html (página WEB)	ascii
doc (documento)	binario
ps (postscript)	ascii
hqx (comprimido)	ascii
Z (comprimido)	binario
ZIP (comprimido)	binario
ZOO (comprimido)	binario
Sit (comprimido)	binario
pit (comprimido)	binario
shar (comprimido)	binario
uu (comprimido)	binario
ARC (comprimido)	binario
tar (empaquetado)	binario

## - Clientes FTP : en línea de comandos, entornos “gráficos” y navegadores / exploradores.

Previo a la utilización de un cliente FTP, es necesario asegurarse de tener configurada correctamente la red TCP/IP para que, a través de nuestro interfaz de red o módem, se disponga de acceso a distintos servidores de Internet. Si el equipo pertenece a una organización que dispone de proxy, se puede configurar el equipo del usuario o su navegador para indicar el dispositivo o equipo que ejerce de proxy.

La configuración de los parámetros del cliente consistirá básicamente en indicar el servidor al que se quiere acceder, bien con su dirección IP o mediante su nombre FQDN. En función del tipo de usuarios que acepte el servidor, podremos autenticarnos como usuario anónimo o usuario del servidor. Indicaremos si el modo de transferencia que deseamos realizar es activa o pasiva, así como el tipo de ficheros que deseamos transferir. Adicionalmente podemos establecer otros parámetros como el directorio local y remoto por defecto. El establecimiento de estos parámetros del cliente se realizará de la forma escogida para acceder al servidor remoto.

Un **cliente FTP** emplea el protocolo FTP para conectarse a un servidor FTP para transferir archivos.

Algunos clientes de FTP básicos vienen integrados en los sistemas operativos, incluyendo Windows, DOS, Linux y Unix. Sin embargo, hay disponibles clientes con más funcionalidades, habitualmente en forma de shareware/freeware para Windows y como software libre para sistemas de tipo Unix. Muchos navegadores recientes también llevan integrados clientes FTP (aunque un cliente FTP trabajará mejor para FTP privadas que un navegador).

Algunos sistemas operativos, incluyendo los Windows más recientes y Mac OS X pueden montar servidores FTP como unidades virtuales directamente dentro del sistema operativo, como puede ser fireftp[1] para firefox, pues es un plugin que se puede añadir al navegador, solo si se necesita. lo que puede resultar más fácil o más conveniente para algunos usuarios, que emplear un cliente especializado.

Establecida la conexión entre el cliente y el servidor, el cliente tendrá acceso al sistema de ficheros del servidor mediante cualquiera de los siguientes métodos: línea de órdenes, navegador o programas específicos. Las partes del sistema de ficheros a las que el usuario tendrá acceso y las operaciones que podrá realizar en él, dependerá de los privilegios que al usuario se le hayan otorgado al configurar el servicio FTP, así como de los privilegios que el usuario tenga sobre cada una de las partes del sistema de ficheros en el servidor.


## - Monitorización y registro del servicio de transferencia de archivos.


Monitorizando conexiones con el servicio FTP


Para saber quién está conectado a tu servidor vía FTP, en qué directorios se encuentra y qué archivos está cargando o descargando del servidor:


1. Vete a **Sesiones** > y haz clic en **Sesiones FTP**. Se mostrarán todas las sesiones, incluida la tuya, así como los siguientes detalles:


- **Tipo**. El tipo de usuario de panel de control que estableció la sesión:

 para usuarios no registrados en el panel de control.

 para usuarios de FTP anónimo.

 para administradores de sitio web o de dominio.

 para administradores de subdominio.

 para usuarios web (propietarios de páginas web personales sin nombres de dominio individuales).

- **Estado**. Estado actual de la conexión FTP.
- **Nombre de usuario FTP**. Nombre de usuario usado para acceder a la cuenta FTP.
- **Nombre de dominio**. Dominio en el que el usuario FTP está conectado.
- **Ubicación actual**. Directorio donde se encuentra el usuario FTP.
- **Nombre del Archivo**. El nombre de archivo con el que se opera.
- **Velocidad**. Velocidad de transferencias en kilo bites.
- **Progreso, %**. Progreso de la operación de transferencia de archivo en porcentaje.
- **Dirección IP**. Dirección IP desde la que se accede a la cuenta FTP.
- **Hora de acceso**. Tiempo transcurrido desde que el usuario se conectó.
- **Tiempo de inactividad** . Tiempo en que el usuario no estaba realizando ninguna acción en el panel de control aún y estando conectado.



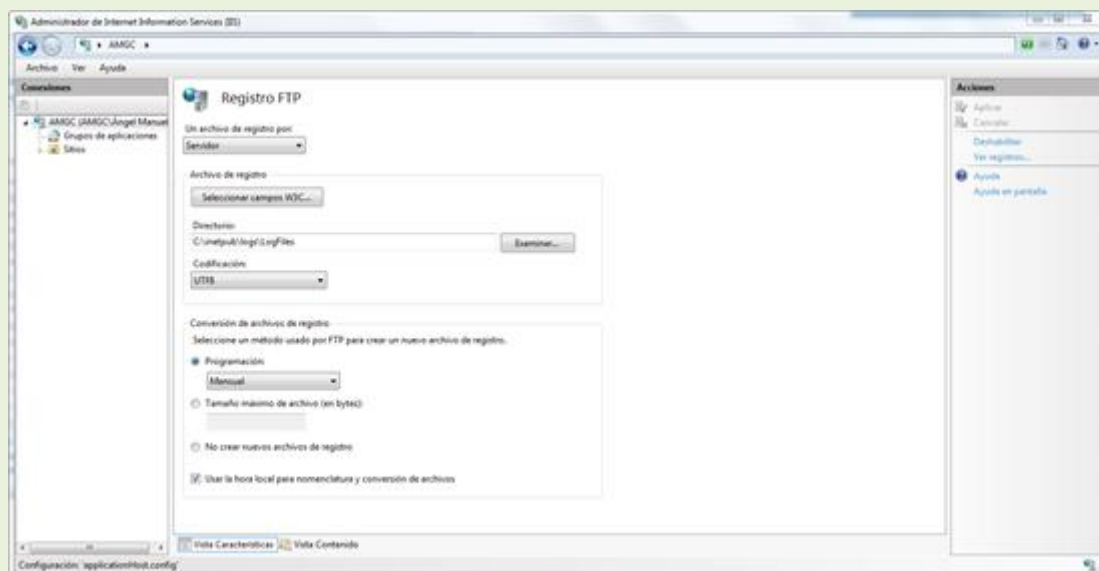
2. Para actualizar la lista de sesiones FTP haz clic en **Actualizar**
3. Para finalizar la sesión marque la casilla respectiva y haz clic en **Eliminar Seleccionados**.

Registro del servicio de transferencia de archivos.

Si tenemos configurado un servidor FTP en IIS, es posible habilitar un registro de conexiones, el cual puede ser útil para informarnos acerca de la cantidad de usuarios que se conectan, tener pruebas útiles en caso de que el sitio haya sido hackeado o sabotado, etc.

Vamos a configurarlo nosotros de modo que se cree un archivo de registro por servidor y no por cada sitio y para ello debemos hacer lo siguiente:

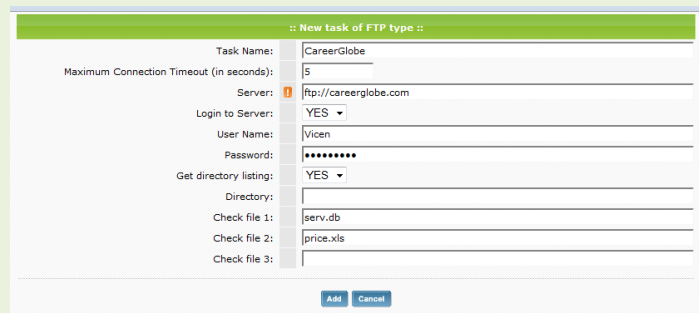
1. Abramos IIS y vayamos al nivel de servidor.
2. Ahí, hacemos clic en "Registro FTP" dentro de la sección FTP y podemos configurar si se generará un archivo de registro por servidor o por cada sitio además de indicar cada cuánto tiempo se generará un nuevo archivo. Una vez finalizado esto, hacemos clic en aplicar y todo listo. Recordemos que tenemos que seleccionar los campos a mostrar en "Seleccionar campos W3C", pero dichos campos vendrán acompañados de un nombre, por ejemplo el campo "Fecha" irá guiado de "(date)", pudiendo obtener más información sobre éstos en <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/librar y/iis/676400bc-8969-4aa7-851a-9319490a9bbb.mspx>.



Podemos también tener el control mediante la instalación de software especializado para tal fin, un ejemplo de ello es el siguiente:

**Servicio de monitorización FTP****Monitorización de servidores de protocolo de transferencia de archivos (FTP).**

Nuestro servicio de monitorización de red se conecta al servidor FTP especificado. Una vez conectado, accederá al servidor FTP utilizando un nombre de usuario y una contraseña introducida por usted y se solicitará un listado de directorios para un directorio específico. Después de listar los contenidos de ese directorio, el servicio de monitorización comprobará si existen los archivos especificados en el servidor, y en ese directorio concreto. Si nuestros agentes de monitorización remota detectan un problema en cualquier punto del proceso, Dotcom-Monitor se lo notificará por medio del proceso de notificación.



:: New task of FTP type ::	
Task Name:	CareerGlobe
Maximum Connection Timeout (in seconds):	5
Server:	ftp://careerglobe.com
Login to Server:	YES
User Name:	Vicen
Password:	*****
Get directory listing:	YES
Directory:	
Check file 1:	serv.db
Check file 2:	price.xls
Check file 3:	

### - Seguridad en FTP.

FTP es un servicio no seguro, ya que tanto la autenticación del usuario como la transferencia de información se realizan sin encriptar, pudiendo ser interceptado por usuarios malintencionados y hacer mal uso de ella. Para realizar transferencias de información que comprometan la seguridad, es recomendable utilizar servicios más seguros como SSH, el cual implementa el protocolo SFTP (Secure Shell File Transfer Protocol o Shell Seguro para protocolo de Transferencia de ficheros) proporcionando un canal seguro en la transferencia de ficheros entre cliente y servidor.

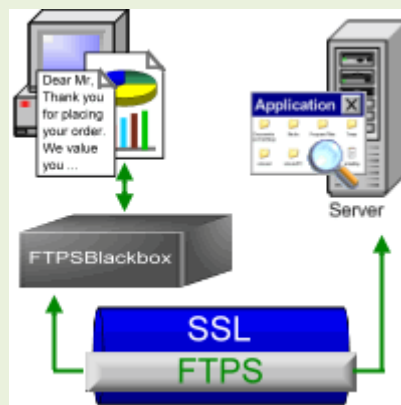
Otra forma de asegurar la transferencia de ficheros es utilizar el servicio FTP apoyándose sobre una conexión segura, como por ejemplo mediante la utilización de SSL (Secure Socket Layer o Capa de conexión Segura) o TLS (Transport Layer Security o Seguridad de la Capa de Transporte). Requiere mecanismos de cifrado, como por ejemplo de clave pública y la utilización de certificados.

### - FTPS (FTP/SSL): FTPS Implícito. FTPS Explícito (FTPES)

La utilización conjunta del protocolo FTP y SSL o TLS tiene dos modos de funcionamiento:

Explícito o FTPES: el cliente se conecta al puerto habitual FTP (21) y explícitamente cambia a un modo seguro utilizando TLS o SSL, para transferir la información.

Implícito o FTPS: el cliente asume el modo seguro con TLS o SSL, desde el inicio de la conexión, antes de transferir la información. Habitualmente se utiliza el puerto 990 en vez del habitual puerto 21.



### - Protocolo FXP (File eXchangeProtocol).

**File eXchangeProtocol (FXP)** es un método de transferencia de datos, a través del cual los datos se envían de un servidor FTP a otro sin pasar por un cliente intermedio. La comunicación convencional FTP consiste en un solo servidor y un solo cliente. Toda la transferencia de datos se realiza entre los dos. Durante una sesión FXP, un cliente mantiene conexiones estándares con dos servidores, dirigiendo cualquiera de los dos servidores que se conecte al otro para iniciar una transferencia de datos. Este método permite a un cliente con poco ancho de banda intercambiar datos entre dos servidores con mas ancho de banda sin el retraso asociado con la comunicación convencional FTP. A lo largo de este proceso, sólo el cliente es capaz de acceder a los recursos de los dos servidores.



### Riesgos

Sin embargo, algunos de los servidores que soportan el FXP son vulnerables a un exploit conocido como el ataque FTP Bounce, por el cual un usuario malicioso puede superar algunos cortafuegos.<sup>1</sup>

### FXP a través de SSL

Algunos servidores FTP como gFTPd, RaidenFTPd y wzdfpd soportan la negociación de un canal de dato seguro entre dos servidores mediante cualquiera de las dos

órdenes de extensión del protocolo FTP: CPSV o SSCN. Normalmente, un cliente realiza esto enviando CPSV en lugar de la orden PASV (modo pasivo), o enviando SSCN antes de iniciar las transferencias pasivas. No obstante, ambos métodos aún son susceptibles a los ataques Man-in-the-middle, pues los dos servidores FTP no comprueban sus respectivos certificados SSL.

### •Servicio TFTP (Trivial File Transfer Protocol).

Existe una versión del protocolo FTP denominada TFTP (trivial file Transfer Protocol o Protocolo Trivial de transferencias de Archivos) cuyo funcionamiento es similar a FTP aunque no requiere autenticación del usuario antes de la conexión, simplemente lleva a cabo la transferencia de archivos.

Este protocolo es utilizado para clonar equipos en una red, para una instalación por red o para obtener los archivos del sistema operativo de un servidor en estaciones sin disco duro. Algunos ejemplos donde TFTP es utilizado lo tenemos en proyectos como TCOS (ThinClientOperatingSystem o Sistema Operativo de cliente Ligero) o LTSP (Linux Terminal Server Project o Proyecto de Servidor de Terminales Linux) para la obtención del sistema operativo en equipos antiguos con pocos recursos hardware. Otro ejemplo lo tenemos con WDM (Windows DeploymentServices o Servicios de Despliegue de Windows), anteriormente RIS (RemoteInstallationServices o Servicios de Instalación Remota), utilizado en sistemas operativos Windows de servidor como 2008 ó 2003 para instalaciones desatendidas de sistemas operativos cliente Windows. TFTP se limita a la transferencia de información, por tanto para lograr dicho objetivo, se debe utilizar de forma conjunta con otros protocolos, como por ejemplo:

UDP (User Datagram Protocol o Protocolo de Datagramas de Usuario): permite a la máquina cliente enviar un mensaje de petición a los equipos de la red solicitando una dirección IP.

DHCP o BOOTP (BootstrapProtocol o Protocolo Autosuficiente): permite a lamáquina cliente obtener su dirección IP del servidor que alberga el núcleo o los ficheros de instalación del sistema operativo.

IP (Internet Protocol o Protocolo de Internet: para establecer comunicación con el servidor a través de la red.

## •Servicios SFTP/SCP.

**SFTP (SSH File Transfer Protocol)** es un protocolo que provee funcionalidad de transferencia y manipulación de ficheros a través de un flujo confiable de datos. Comúnmente se utiliza con **SSH** para proveer a éste de transferencia segura de ficheros.

**SCP (SecureCopy, o Copia Segura)** es un protocolo seguro para transferir ficheros entre un anfitrión local y otro remoto, a través de **SSH**. Básicamente, es idéntico a **RCP (RemoteCopy, o Copia Remota)**, con la diferencia de que los datos son cifrados durante la transferencia para evitar la extracción potencial de información a través de programas de captura de las tramas de red (**packetsniffers**). **SCP** solo implementa la transferencia de ficheros, pues la autenticación requerida es realizada a través de **SSH**.

## •Transferencia o distribución de archivos entre iguales (peer-to-peer).

### - Características. Protocolos. Software. Configuración

Una **red peer-to-peer, red de pares, red entre iguales, red entre pares o red punto a punto (P2P)**, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

Normalmente este tipo de redes se implementan como redes superpuestas construidas en la capa de aplicación de redes públicas como Internet.

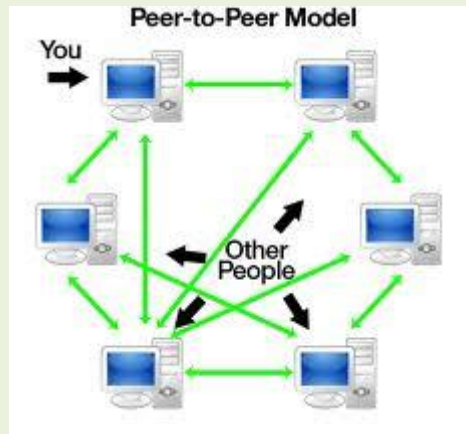
El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que parte de los usuarios lo utilicen para intercambiar archivos cuyo contenido está sujeto a las leyes de copyright, lo que ha generado una gran polémica entre defensores y detractores de estos sistemas.

Las redes *peer-to-peer* aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.

Dichas redes son útiles para diversos propósitos. A menudo se usan para compartir ficheros de cualquier tipo (por ejemplo, audio, vídeo o software). Este tipo de red

también suele usarse en telefonía VoIP para hacer más eficiente la transmisión de datos en tiempo real.

La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local (cortafuegos, NAT, ruteadores, etc.), velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco.



### Características

Seis características deseables de las redes P2P:

- **Escalabilidad.** Las redes P2P tienen un alcance mundial con cientos de millones de usuarios potenciales. En general, lo deseable es que cuantos más nodos estén conectados a una red P2P, mejor será su funcionamiento. Así, cuando los nodos llegan y comparten sus propios recursos, los recursos totales del sistema aumentan. Esto es diferente en una arquitectura del modo servidor-cliente con un sistema fijo de servidores, en los cuales la adición de clientes podría significar una transferencia de datos más lenta para todos los usuarios. Algunos autores advierten que, si proliferan mucho este tipo de redes, cliente-servidor, podrían llegar a su fin, ya que a cada una de estas redes se conectarán muy pocos usuarios.
- **Robustez.** La naturaleza distribuida de las redes *peer-to-peer* también incrementa la robustez en caso de haber fallos en la réplica excesiva de los datos hacia múltiples destinos, y —en sistemas **P2P** puros— permitiendo a los *peers* encontrar la información sin hacer peticiones a ningún servidor centralizado de indexado. En el último caso, no hay ningún punto singular de falla en el sistema.
- **Descentralización.** Estas redes por definición son descentralizadas y todos los nodos son iguales. No existen nodos con funciones especiales, y por tanto ningún nodo es imprescindible para el funcionamiento de la red. En realidad, algunas redes comúnmente llamadas P2P no cumplen esta característica, como Napster, eDonkey o BitTorrent.

- **Distribución de costes entre los usuarios.** Se comparten o donan recursos a cambio de recursos. Según la aplicación de la red, los recursos pueden ser archivos, ancho de banda, ciclos de proceso o almacenamiento de disco.
- **Anonimato.** Es deseable que en estas redes quede anónimo el autor de un contenido, el editor, el lector, el servidor que lo alberga y la petición para encontrarlo, siempre que así lo necesiten los usuarios. Muchas veces el derecho al anonimato y los derechos de autor son incompatibles entre sí, y la industria propone mecanismos como el DRM para limitar ambos.
- **Seguridad.** Es una de las características deseables de las redes P2P menos implementada. Los objetivos de un P2P seguro serían identificar y evitar los nodos maliciosos, evitar el contenido infectado, evitar el espionaje de las comunicaciones entre nodos, creación de grupos seguros de nodos dentro de la red, protección de los recursos de la red... La mayor parte de los nodos aún están bajo investigación, pero los mecanismos más prometedores son: cifrado multiclave, cajas de arena, gestión de derechos de autor (la industria define qué puede hacer el usuario; por ejemplo, la segunda vez que se oye la canción se apaga), reputación (permitir acceso sólo a los conocidos), comunicaciones seguras, comentarios sobre los ficheros, etc.