Introducción (I)

- Intercambiar archivos entre ordenadores, teóricamente sencillo, presenta problemas debido a:
  - Convenciones diferentes para nombrar archivos:
    - Limitaciones diferentes en el tamaño del nombre de archivos.
  - Reglas diferentes para recorrer los directorios:
    - Unidades en Windows.
    - Directorios representados como \ en Windows y / en Linux.
  - Restricciones de acceso a archivos.
  - Diferentes formas de representar texto y datos dentro de los archivos.
    - Fin de línea: \r\n en Windows y \n en Linux.

Introducción (II)

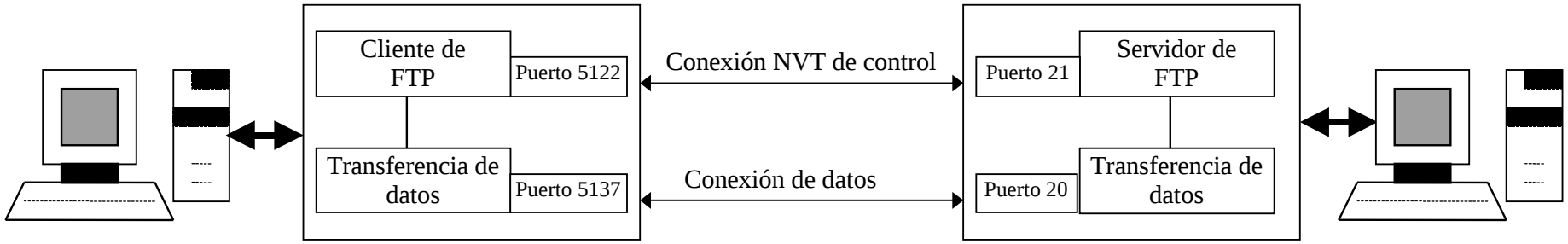
- Para solventar estos problemas se desarrollo File Transfer Protocol.
- En FTP:
  - Un cliente establece una conexión con un servidor a través de una **conexión de control**.
  - La conexión de control es una sesión de Network Virtual Terminal (NVT).
  - Por la conexión de control el cliente envía comandos al servidor y el servidor las respuestas.
  - Por la conexión de control **nunca se envían datos** (incluidos listados de directorios).

Introducción (III)

- El conjunto de comandos es muy grande y no todo cliente o servidor debe soportar todos.
- La respuesta a un comando del cliente por parte del servidor es un código numérico:
  - 1xx: Comienzo de acción.
  - 2xx: Comando ejecutado correctamente.
  - 3xx: Punto intermedio alcanzado con éxito.
  - 4xx: Error temporal recuperable.
  - 5xx: Error permanente irrecuperable.

Introducción (IV)

- Cuando se solicita la transferencia de un archivo o un listado de un directorio:
  - Se establece una **conexión de datos**.
  - Por ella se envían datos, **nunca comandos**.



Transferencia de datos

- El principal problema en la transferencia de archivos es el diferente formato de los datos en función del:
  - Hardware.
  - Sistema operativo.
- Ambos ordenadores necesitan conocer el formato y tipo de datos que se transmiten.
- FTP utiliza tres atributos:
  - Tipo de los datos.
  - Estructura de los datos.
  - Modo de transmisión.

Tipo de los datos

- Se indica con el comando TYPE.
- Tres tipos fundamentales:
  - Texto ASCII (A).
  - Texto EBCDIC (E).
  - Binario (B).
- Los datos de texto ASCII se convierten desde el formato local a NVT en el emisor y viceversa en el receptor.
- Los datos de texto EBCDIC no se convierten, pues solo suele suceder entre computadores IBM.
- Los datos binarios se transfieren sin ninguna conversión y sin tener en cuenta diferencias hardware (little-endian o big-endian).

Estructura de los datos

- Se indica con el comando STRU.
- Existen dos tipos de estructura:
  - Archivo (F).
  - Registro (R).
- La estructura de archivo supone que los datos son una secuencia de bytes a enviar.
- La estructura de registro indica que el archivo esta formado por registros de datos.

Modo de transmisión (I)

- Se indica con el comando MODE.
- Tres modos:
  - Flujo (S).
  - Bloque (B).
  - Comprimido (C).
- Determinan, junto con la estructura de los datos, como se transmiten estos.

Modo de transmisión (II)

- Modo flujo:
  - Estructura archivo:
    - Se transmite como un flujo de bytes.
    - El final del archivo se indica cerrando la conexión de datos.
  - Estructura registro:
    - Cada registro termina con End Of Record (0xFF 0x01).
    - El final del archivo con End Of File (0xFF 0x02).
    - EOR y EOF seguidos pueden ponerse como 0xFF 0x03.
    - Si el archivo contiene 0xFF este debe duplicarse antes de enviarse.

Modo de transmisión (III)

- Modo bloque:
  - El archivo se transmite como bloques con una cabecera de 3 bytes.
    - 1er byte contiene la bandera del descriptor (fin de bloque, fin de archivo, etc.).
    - 2º y 3er byte indican el número de bytes que siguen.
  - Si la estructura de los datos es registro pueden transmitirse varios archivos sin cerrar la conexión de datos.
- Modo comprimido: Comprime la información a enviar, es una compresión deficiente.

El cliente de FTP (I)

- El cliente de FTP se ejecuta como:

```
> ftp [nombre del ordenador]
```

- Ejemplo:

```
> ftp glup.irobot.uv.es
Connected to glup.irobot.uv.es (147.156.222.65).
220 Bienvenido al servicio de FTP del Instituto de Robotica
Name (glup.irobot.uv.es: quique): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /dist/ssh
250 Directory successfully changed.
ftp> get putty.zip
local: putty.zip remote: putty.zip
227 Entering Passive Mode (147,156,222,65,19,244)
150 Opening BINARY mode data connection for putty.zip (190784 bytes).
226 File send OK.
190784 bytes received in 0.0122 secs (1.5e+04 Kbytes/sec)
ftp> quit
221 Goodbye.
```

El cliente de FTP (II)

- Si se llama sin especificar el servidor:

```
> ftp
ftp> help
Commands may be abbreviated.  Commands are:
!               debug           mdir            sendport        site
$               dir             mget            put             size
account         disconnect      mkdir           pwd             status
append          exit            mls             quit            struct
ascii           form            mode            quote           system
bell            get             modtime         recv            sunique
binary          glob            mput            reget           tenex
bye             hash            newer           rstatus         tick
case            help            nmap            rhelp           trace
cd              idle            nlist           rename          type
cdup            image           ntrans          reset           user
chmod           lcd             open            restart         umask
close           ls              prompt          rmdir           verbose
cr              macdef          passive         runique         ?
delete          mdelete         proxy           send
ftp> help quote
quote           send arbitrary ftp command
```

El servidor de FTP

- El servidor de FTP:
  - Recibe las peticiones de los clientes y las procesa.
  - Se ejecuta de forma normal en el puerto 21 TCP para la conexión de control.
- Existen distintos servidores de FTP:
  - in.ftpd.
  - wu-ftpd.
  - vsftpd.
  - ...
- Escogemos vsftpd (Very Secure FTPD) por:
  - Características añadidas de seguridad.
  - Permite definir diferentes servidores para distintos interfaces de red.

VSFTPD

- Sus ficheros de configuración se encuentran en /etc/vsftpd y deben terminar con la extensión .conf.
- La sintaxis de los ficheros es:
  - Las líneas que empiezan con # son comentarios.
  - El resto de líneas tiene el formato opción=valor, sin espacios entre opción, el igual y el valor.
- Existen tres tipos de opciones:
  - Booleanas.
  - Numéricas.
  - Opciones de cadena.

Opciones booleanas (I)

- Solo pueden tomar valores YES o NO.
- Podemos dividirlas en:
  - Opciones de configuración del servidor.
  - Opciones generales.
  - Opciones de los usuarios del sistema.
  - Opciones de los usuarios anónimos.
  - Otras opciones.

Opciones booleanas (II)

- Las opciones de configuración del servidor son:

Opción	Descripción	Defecto	Dependencia
listen	Habilita la ejecución del servidor como un demonio independiente en lugar de ser ejecutado por xinetd. Es excluyente con *listen_ipv6*.	NO	listen_ipv6
listen_ipv6	Igual que *listen*, excepto que escucha conexiones en cualquier dirección IPv6 (::), por lo que también escucha conexiones IPv4. Es excluyente con *listen*.	NO	listen
pasv_enable	Habilita el modo pasivo del servidor.	YES	Ninguna.
port_enable	Habilita el modo activo del servidor.	YES	Ninguna.
connect_from_port_20	Permite al servidor iniciar conexiones activas utilizando el puerto 20, en caso contrario las conexiones activas se inician en un puerto no privilegiado.	NO	Ninguna.
tcp_wrappers	Indica que el servidor compruebe las reglas de los envolventes de acceso. Requiere que el servidor haya sido compilado para soportar los envolventes de acceso.	NO	Ninguna.

Opciones booleanas (III)

- Las opciones generales son:

Opción	Descripción	Defecto	Dependencia
download_enable	Permite la descarga de ficheros desde el servidor.	YES	Ninguna.
write_enable	Habilita el uso de los comandos que modifican el sistema de ficheros, permitiendo crear, borrar, etc., directorios y ficheros.	NO	Ninguna.
ascii_download_enable	Permite descargar ficheros en formato ASCII.	NO	Ninguna.
ascii_upload_enable	Permite subir ficheros en formato ASCII.	NO	Ninguna.
dirlist_enable	Permite el listado de los directorios.	YES	Ninguna.
use_localtime	Devuelve la hora de los ficheros y directorios en la hora local.	NO	Ninguna.
hide_ids	Oculta la información sobre usuarios y grupos mostrando estos datos como ftp.	NO	Ninguna.
dirmessage_enable	Permite que se muestre a los usuarios un mensaje cuando acceden a los directorios. El mensaje a mostrar se encuentra, por defecto, en el fichero *.message* de cada directorio, pero puede modificarse con la opción *message_file*.	NO	message_file
xferlog_enable	Habilita la escritura en el fichero de "log" de los ficheros que son descargados o subidos.	NO	vsftpd_log_file xferlog_file
xferlog_std_format	Especifica que el fichero de "log" se escriba en formato de vsftpd, en el fichero indicado por *vsftpd_log_file* si su valor es NO, o bien se escriba en el formato de xferlog, en el fichero indicado por *xferlog_file* si su valor es YES.	NO	Ninguna.

Opciones booleanas (IV)

- Las opciones de los usuarios del sistema son:

Opción	Descripción	Defecto	Dependencia
local_enable	Permite el acceso a los usuarios locales, los cuales se especifican en */etc/passwd*.	NO	Ninguna.
check_shell	Para los usuarios locales, verifica que la shell que tienen asignada se encuentra en una lista de shells autorizadas que se indica en */etc/shells*.	YES	Ninguna.
chmod_enable	Permite a los usuarios locales ejecutar el comando chmod para cambiar los permisos de un fichero.	YES	Ninguna.
chroot_list_enable	Habilita la lista de usuarios que serán “encerrados” en su directorio raíz al acceder por FTP. La lista por defecto se encuentra en */etc/vsftpd.chroot_list*, pero puede modificarse con la opción *chroot_list_file*.	NO	chroot_local_user chroot_list_file
chroot_local_user	Invierte el funcionamiento de la opción *chroot_list_enable* y hace que los usuarios sean “encerrados” en su directorio raíz excepto los especificados en la lista.	NO	Ninguna.
passwd_chroot_enable	Si se encuentra habilitada la opción *chroot_local_user*, permite redirigir el directorio donde se encuentra “encerrado” el usuario. La aparición de /./ en el directorio que especifica el directorio raíz indica la localización donde se “encerrara” al usuario.	NO	chroot_local_user
text_userdb_names	Habilita que se muestren los nombres de los usuarios y grupos en lugar de sus números identificadores.	NO	Ninguna.
tilde_user_enable	Permite que se resuelvan las localizaciones indicadas como ~usuario como el directorio raíz del usuario indicado.	NO	Ninguna.
userlist_deny	Indica si la lista contiene los usuarios locales cuyo acceso esta permitido (valor NO) o si la lista contiene los usuarios locales cuyo acceso esta denegado (valor YES). En cualquier caso, la denegación se produce antes de que el usuario pueda introducir su contraseña.	YES	userlist_enable userlist_file
userlist_enable	Indica si esta habilitado el uso de la lista de usuarios permitidos o denegados que se encuentra en el fichero especificado por la opción *userlist_file*.	NO	userlist_file

Opciones booleanas (V)

- Las opciones de los usuarios anónimos son:

Opción	Descripción	Defecto	Dependencia
anonymous_enable	Permite el acceso de usuarios anónimos, que son reconocidos por “anonymous” y “ftp”.	YES	Ninguna.
anon_mkdir_write_enable	Permite a los usuarios anónimos crear directorios si esta habilitada la opción de escribir.	NO	write_enable
anon_other_write_enable	Permite a los usuarios anónimos realizar otras operaciones diferentes de crear directorios y ficheros, tales como borrar y renombrar ficheros.	NO	write_enable.
anon_upload_enable	Permite a los usuarios anónimos subir ficheros si esta habilitada la opción de escribir.	NO	write_enable
anon_world_readable_only	Permite a los usuarios anónimos descargar ficheros solo si estos tienen permisos para ser leídos por todo el mundo.	YES	Ninguna.
chown_uploads	Habilita el cambio del propietario de los ficheros subidos por los usuarios anónimos al indicado en la opción *chown_username*.	NO	chown_username
deny_email_enable	Habilita una lista de correos a los que se les deniega el acceso al servidor con el usuario anónimo. La lista por defecto se encuentra en */etc/vsftpd.banned_emails*, pero puede modificarse con la opción *banned_email_file*.	NO	banned_email_file
secure_email_list_enable	Habilita que solo los usuarios anónimos cuya dirección de correo se encuentre en el fichero indicado por *email_password_file* puedan acceder como anónimos.	NO	email_password_file

Opciones numéricas (I)

- Pueden tomar valores enteros no negativos.
  - El valor 0 indica sin limite.
  - Se pueden especificar en formato octal, anteponiendo al número un 0, por ejemplo 0666.

Opciones numéricas (II)

Opción	Descripción	Defecto
accept_timeout	Número de segundos que se espera el establecimiento de una conexión en modo pasivo.	60
anon_max_rate	Máximo número de bytes por segundo que se transmiten a un usuario anónimo.	0
anon_umask	Valor de la máscara de usuario para la creación de ficheros por los usuarios anónimos.	077
connect_timeout	Número máximo de segundos que se espera la aceptación de una conexión en modo activo.	60
data_connection_timeout	Número máximo de segundos que permanece abierta una conexión de datos sin que se transmita ningún dato.	300
file_open_mode	Modo por defecto en el que son creados los ficheros subidos al servidor. A este modo por defecto se le aplica siempre la máscara del usuario.	0666
ftp_data_port	Puerto desde el que se establece la conexión de datos en modo activo.	20
idle_session_timeout	Número máximo de segundos que permanece abierta una conexión de control en espera de nuevos comandos.	300
listen_port	Puerto en el que se encuentra a la escucha el servidor si no es lanzado por el servidor de xinetd.	21
local_max_rate	Máximo número de bytes por segundo que se transmiten a un usuario local.	0
local_umask	Valor de la máscara de usuario para la creación de ficheros por usuarios locales.	077
max_clients	Número máximo de conexiones que acepta el servidor, siempre que no sea lanzado por el servidor de xinetd. Las conexiones que exceden dicho número reciben un mensaje de error.	0
max_per_ip	Número máximo de conexiones por dirección IP que acepta el servidor de forma simultanea. Solo es valido si no es lanzado por el servidor de xinetd.	0
pasv_max_port	Indica el valor máximo del puerto que puede usarse para la transmisión de datos en modo pasivo.	0
pasv_min_port	Indica el valor mínimo del puerto que puede usarse para la transmisión de datos en modo pasivo.	0
trans_chunk_size	Limite de ancho de banda que puede ocupar el servidor.	0

Opciones de cadena (I)

- Permiten especificar la localización de:
  - Ficheros de log.
  - Ficheros con listas de acceso.
  - Ficheros con mensajes a mostrar.
  - Etc.

Opciones de cadena (II)

Opción	Descripción	Defecto
anon_root	Directorio donde acceden los usuarios anónimos.	Ninguno.
banned_email_file	Fichero con la lista de correos a los que se les deniega el acceso al servidor con el usuario anónimo	/etc/vsftpd/banned_email
banner_file	Fichero con el texto a mostrar cuando accede un usuario al servidor. Esta opción prevalece sobre la opción *ftpd_banner*.	Ninguno.
chown_username	Nombre del usuario al que se asignan los ficheros subidos por los usuarios anónimos.	root
chroot_list_file	Fichero que contiene la lista de usuarios a los que afectarán las opciones de ser “encerrados”.	/etc/vsftpd/chroot_list
cmds_allowed	Lista de comandos, separados por comas, que aceptará el servidor de FTP.	Ninguno.
deny_file	Patrón que especifica los ficheros que no deben ser accesibles por los usuarios virtuales.	Ninguno.
dsa_cert_file	Localización del certificado DSA para conexiones SSL.	Ninguno.
dsa_private_key_file	Localización de la clave privada del certificado DSA para conexiones SSL.	La misma localización que el certificado DSA.
email_password_file	Fichero con las direcciones de correo a las que se autoriza el acceso.	/etc/vsftpd/email_passwords
ftp_username	Nombre del usuario al que se asignan los accesos anónimos. Su directorio de acceso es el directorio raíz de los usuarios anónimos.	ftp
ftpd_banner	Texto a mostrar cuando accede un usuario al servidor.	Ninguno.
guest_username	Nombre del usuario al que se asignan los accesos virtuales si la opción *guest_enable* los ha habilitado.	ftp

Opciones de cadena (III)

Opción	Descripción	Defecto
hide_file	Patrón que especifica los ficheros que deben ser ocultados a los usuarios virtuales.	Ninguno.
listen_address	Dirección IP en la que escucha el servidor si se ha lanzado directamente, esto es, sin el servidor xinetd.	Ninguno.
listen_address6	Dirección IPv6 en la que escucha el servidor si se ha lanzado directamente, esto es, sin el servidor xinetd.	Ninguno
local_root	Directorio donde el servidor coloca al usuario en caso de acceso por parte de un usuario local.	Ninguno
message_file	Nombre del fichero que contiene el mensaje a mostrar cuando se cambia de directorio.	.message
nopriv_user	Nombre del usuario con el que se ejecuta el servidor para no tener los privilegios de administrador.	nobody
pam_service_name	Nombre del servicio PAM que debe utilizar el servidor	ftp
pasv_address	Cambia la dirección IP que envía el servidor ante una transferencia de datos en modo pasivo.	Ninguno.
rsa_cert_file	Localización del certificado RSA para conexiones SSL.	/usr/share/ssl/certs/vsftpd.pem
rsa_private_key_file	Localización de la clave privada del certificado RSA para conexiones SSL.	La misma localización que el certificado RSA.

Opciones de cadena (IV)

Opción	Descripción	Defecto
secure_chroot_dir	Nombre del directorio vacío y sin permisos de escritura donde se pueden “encerrar” las conexiones que no requieran acceso al sistema de ficheros.	/usr/share/empty
ssl_ciphers	Selecciona el tipo de cifrado que se utilizará para las conexiones cifradas.	DES-CBC3-SHA
user_config_dir	Especifica el directorio donde se escribirán las opciones de acceso particulares para cada usuario, y que pueden sobrescribir las opciones del fichero de configuración por defecto.	Ninguno
user_sub_token	Genera un directorio para los usuarios virtuales en el cual son “encerrados”.	Ninguno
userlist_file	Nombre del fichero que contiene los usuarios a los que se les deniega el acceso si la opción *userlist_enable* está activada.	/etc/vsftpd/user_list
vsftpd_log_file	Nombre del fichero donde se escribe el “log” del servidor	/var/log/vsftpd.log
xferlog_file	Nombre del fichero donde se escribe el “log” del servidor.	/var/log/xferlog

Ejemplo de fichero de configuración (I)

```
# Ejecutamos el servidor como demonio
# Podriamos poner listen_ipv6=YES para escuchar en IPv4 e IPv6.
listen=YES
# Permitimos las conexiones activas desde el puerto 20
connect_from_port_20=YES
# Habilitamos el uso de los envolventes de acceso
tcp_wrappers=YES
# Indicamos el servicio PAM que utiliza el servidor
pam_service_name=vsftpd
# Habilitamos la escritura del fichero de log
xferlog_enable=YES
# Indicamos el modo de log deseado
xferlog_std_format=NO
# Habilitamos la muestra de mensajes al cambiar de directorio
dirmessage_enable=YES
# Permitimos la escritura de ficheros
write_enable=YES
# Permitimos el acceso a usuarios locales
local_enable=YES
# Denegamos el acceso a los usuarios no deseados (root, etc.)
userlist_enable=YES
# Especificamos la mascara de escritura de los ficheros
local_umask=022
# Permitimos el acceso de usuarios anonimos
anonymous_enable=YES
```

Ejemplo de fichero de configuración (II)

```
# Ejecutamos el servidor como demonio
# Podriamos poner listen_ipv6=YES para escuchar en IPv4 e IPv6
listen=YES
# Permitimos las conexiones activas desde el puerto 20
connect_from_port_20=YES
# Habilitamos el uso de los envolventes de acceso
tcp_wrappers=YES
# Indicamos el servido PAM que utiliza el servidor
pam_service_name=vsftpd
# Habilitamos la escritura del fichero de log
xferlog_enable=YES
# Indicamos el modo de log deseado
xferlog_std_format=YES
# Indicamos el fichero donde el log se almacenará
xferlog_file=/var/log/vsftpd.log
# Habilitamos la muestra de mensajes al cambiar de directorio
dirmessage_enable=YES
# Mostramos un mensaje en el acceso al servidor
ftpd_banner=Bienvenido al servicio de FTP
# Ocultamos los usuarios y grupos de los ficheros
hide_ids=YES
# Permitimos el acceso de usuarios anónimos
anonymous_enable=YES
# Limitamos el numero máximo de clientes a 1000
max_clients=1000
# Limitamos el numero máximo de conexiones por cliente a 1
max_per_ip=1
```

Servidores virtuales (I)

- Podemos especificar servidores distintos para cada interfaz de red de un ordenador.
- Crear un fichero de configuración para cada interfaz:
  - Ejecutándose como demonio propio.
  - Indicando la dirección IP que escucha.

Servidores virtuales (II)

- Servidor con interfaces público y privado.
- Fichero publico.conf.

```
# Servidor publico
# Aqui no es posible usar listen_ipv6 al indicar una IPv4
# en listen_address
listen=YES
listen_address=147.156.222.65
ftpd_banner=Bienvenido al servidor FTP publico
...
```

- Fichero privado.conf

```
# Servidor privado
# Aqui no es posible usar listen_ipv6 al indicar una IPv4
# en listen_address
listen=YES
listen_address=192.168.1.1
ftpd_banner=Bienvenido al servidor FTP privado
...
```

Seguridad del servidor de FTP

- En modo activo:
  - El cliente indica un puerto al servidor.
  - El servidor inicia la conexión al puerto indicado.
  - El cortafuegos del cliente debe permitir que el servidor establezca la conexión.
- En modo pasivo:
  - El servidor indica un puerto al cliente.
  - El cliente inicia la conexión al puerto indicado.
  - El cortafuegos del servidor debe permitir que el cliente establezca la conexión.

TFTP (I)

- En determinadas circunstancias:
  - Configuración de un router.
  - Ordenadores sin disco.
  - Etc.
- Se necesita un protocolo sencillo para transferir ficheros: TFTP.
- TFTP utiliza protocolo de transporte UDP.

TFTP (II)

- Las características de TFTP son:
  - Envío de bloques de datos de 512 bytes (excepto el último).
  - Añade una cabecera de 4 bytes a cada bloque.
  - Número los bloques empezando en 1.
  - Admite transferir archivos ASCII o binarios.
  - Permite leer o escribir archivos.
  - No contempla la autenticación de usuarios.

TFTP (III)

- Funcionamiento:
  - El cliente envía un paquete al puerto 69 UDP del servidor con un mensaje de lectura o escritura.
  - El servidor obtiene otro puerto y desde él responde al cliente, será el puerto usado a partir de ese momento.
  - Se intercambian bloques de datos numerados empezando en 1 y ACKs de reconocimiento.
    - El emisor espera el ACK antes de enviar el siguiente bloque.
    - Si el emisor no recibe el ACK en un cierto tiempo reenvía el bloque de datos.
    - Si el receptor no recibe un nuevo bloque de datos en un cierto tiempo reenvía el ACK.

TFTP (IV)

- Existen cinco tipos de mensajes (PDU):

Petición de lectura (RRQ):

2 bytes	Cadena	1 byte	Cadena	1 byte
Código de op.=1	Nombre de archivo	0	Modo	0

Petición de escritura (WRQ):

2 bytes	Cadena	1 byte	Cadena	1 byte
Código de op.=2	Nombre de archivo	0	Modo	0

Datos (DATA):

2 bytes	2 bytes	
Código de op.=3	Nº de bloque	Datos

Confirmación (ACK):

2 bytes	2 bytes
Código de op.=4	Nº de bloque

Error (ERROR):

2 bytes	2 bytes	Cadena	1 byte
Código de op.=5	Código de error	Mensaje de error	0

El cliente de TFTP (I)

- Se ejecuta como:

```
>tftp [nombre del servidor]
```

- Ejemplo:

```
>tftp glup.irobot.uv.es
tftp> verbose
tftp> get X86PC/UNDI/linux-install/linux.0
Received 12498 bytes in 0.1 seconds
tftp> quit
```

El cliente de TFTP (II)

- Si se llama sin especificar el servidor:

```
> tftp
(to)
usage: connect host-name [port]
tftp> help
tftp-hpa 0.49
Commands may be abbreviated.  Commands are:
connect  connect to remote tftp
mode     set file transfer mode
put      send file
get      receive file
quit     exit tftp
verbose  toggle verbose mode
trace    toggle packet tracing
literal  toggle literal mode, ignore ':' in file name
status   show current status
binary   set mode to octet
ascii    set mode to netascii
rexmt    set per-packet transmission timeout
timeout  set total retransmission timeout
?        print help information
help     print help information
```

El servidor de TFTP (I)

- Es ejecutado de forma normal por el servidor xinetd.
- No posee fichero de configuración.
  - Su configuración por defecto debe ser modificada desde la línea de comandos.
- Por defecto considera que puede:
  - Leer los ficheros que pueden ser leídos por cualquier usuario.
  - Escribir los ficheros que pueden ser escritos por cualquier usuario.
- Al no autenticar al usuario debe usarse con mucha precaución.

El servidor de TFTP (II)

- Opciones del servidor:

Opción	Descripción
-l	Ejecuta el servidor directamente, sin ser ejecutado por el servidor xinetd.
-a [dirección][:puerto]	Si el servidor escucha directamente el puerto sin ser lanzado por el servidor xinetd, especifica la dirección IP y el puerto en que permanece a la escucha.
-c	Permite la creación de nuevos ficheros. Por defecto tftp solo permite escribir en ficheros ya existentes.
-s	Especifica el directorio raíz al que accede el servidor, limitando el acceso a ficheros fuera de ese directorio raíz.
-u usuario	Especifica el usuario como el que se ejecuta el servidor.
-U mascara de usuario	Especifica la máscara con que se crearán los ficheros. La máscara por defecto es cero (nadie puede leerlos o escribir en ellos).
-p	Indica que no se ejecute ninguna comprobación de seguridad adicional excepto las normales para el usuario especificado por la opción –u.
-t timeout	Cuando se ejecuta desde el servidor xinetd, especifica el tiempo que permanece en espera de posteriores conexiones antes de terminar su ejecución.
-m fichero	Especifica un fichero que contiene una serie de operaciones, que pueden ser condicionales, que deben ser ejecutadas.
-v	Incrementa la información facilitada por el servidor.
-r opción de tftp	Indica que la opción de tftp especificada no debe ser admitida. Las opciones que es posible especificar se encuentran en el RFC 2347.
-V	Muestra la versión y configuración por defecto del servidor.