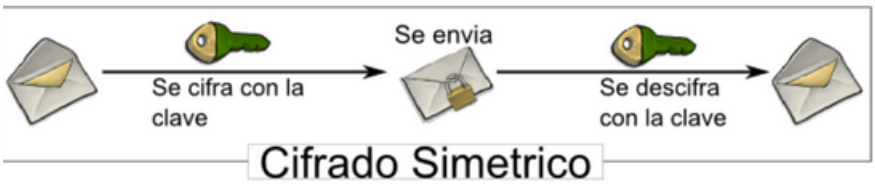
Resumen teoria

Fecha de realización: 01 - 12 - 22

Telnet (Telecommunication Network), es un protocolo de red que sirve para conectarse a una máquina de una red desde otra para manejarla remotamente, como si estuviésemos sentados delante de ella. Es un protocolo cliente-servidor que se comunica por el puerto 23. Antiguamente este tipo de acceso tenía mucho sentido, cuando los terminales o clientes eran máquinas muy lentas y los servidores máquinas muy potentes. Telnet solo se usa en redes locales (de hecho la mayoría de sistemas operativos ya no lo permiten ni en LAN, como por ejemplo Windows), esto se debe a que las comunicaciones no están cifradas, es decir, no son seguras y se pueden descifrar con cualquier programa de sniffer. Además, permite conexión como root.



El cifrado mediante clave simétrica significa que dos o más usuarios, tienen una única clave secreta, esta clave será la que cifrará y descifrará la información transmitida a través del canal inseguro. Es decir, la clave secreta la debe tener los dos usuarios, y con dicha clave, el usuario A cifrará la información, la mandará a través del canal inseguro, y a continuación el usuario B descifrará esa información con la MISMA clave que ha usado el usuario A.

Para que un algoritmo de claves simétricas sea fiable deberemos tener en cuenta que no deberá ser posible obtener la clave de cifrado/descifrado o el texto en claro cuando el mensaje está cifrado.

La clave será segura mientras que esta quede entre el emisor y el receptor, ya que de caer en otras manos, deberá generarse otra clave.

Algoritmos destacados en encriptación simétrica.

DES (Data Encryption Standard): Algoritmo desarrollado por IBM EN LOS AÑOS 70 usa una clave simétrica de 64bits, los 56 primeros bits son empleados para el cifrado, y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, tenemos 256 combinaciones posibles, por lo que la fuerza bruta se hace casi imposible.

3DES (Triple Data Encryption Standard): Se basa en aplicar 3 veces el algoritmo DES, la clave tiene una longitud de 128 bits. Consiste en cifrar el mismo bloque de datos tres veces con 2 llaves diferentes (64 bits cada una).

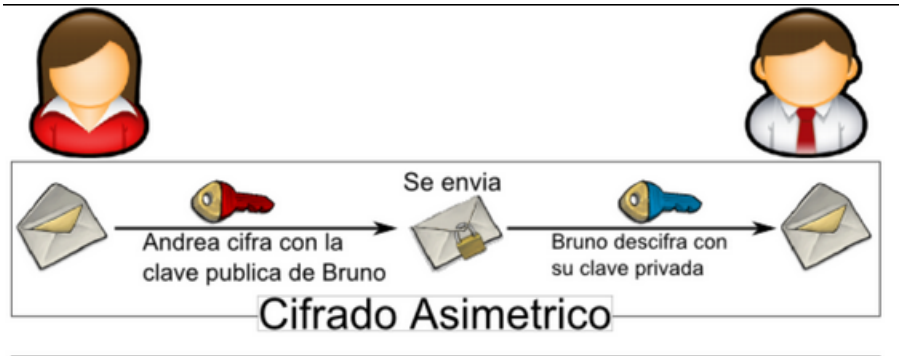
Información -> Cifrado con clave A -> Cifrado con clave B -> Cifrado con clave A

Aumenta de manera muy significativa la seguridad del sistema DES pero requiere más recursos del ordenador. Hay una variante de este algoritmo llamada DES-EDE3 el cual en vez de usar 2 claves usa 3, consiguiendo así una longitud de clave de 192 bits.

IDEA (International Data Encriptión Algorithm): Desarrollado por la escuela politécnica de Zurich en 1990 aplica una clave de 128 bits sin paridad a bloques de datos de 64 bits y se usa tanto para cifrar como para descifrar. Según distintos expertos es el mejor algoritmo de cifrado debido a que existen 2^{128} claves posibles.

AES (Advanced Encryption Standard): Estandarizado por el gobierno de EEUU en el 2001. Es el algoritmo que usa el protocolo WPA como método de cifrado. Este sistema criptográfico puede operar con bloques y claves de distintas longitudes, hay claves AES de 128 bits, 192 bits y 256 bits.

Criptografía de clave asimétrica.



Se basa en dos claves distintas (por eso es asimétrica). Una de las claves es la pública y la otra es la privada. La clave pública puede ser revelada, mientras que la privada solo la conoce su propietario. Para cifrar un mensaje se usa la clave pública de un usuario, este usuario puede desencriptarla con su clave privada para así ver el contenido de su mensaje.

- Algoritmos de clave asimétrica RSA y DSA: La principal diferencia entre usar RSA y DSA es que RSA te permite encriptar documentos y firmas de archivos, mientras DSA permite generar claves para firmar documentos solamente y tiene un tamaño de clave como máximo de 1024 bits, si necesitas una clave mayor o cifrar las firmas de archivo, deberás usar una clave RSA.

SSH (Secure Shell)

Es la evolución segura de Telnet, cifra las conexiones (normalmente a través de claves RSA pero también se puede hacer mediante DSA).

Características:

- Autentica al usuario en la máquina mediante usuario y contraseña.
- Se cifran las conexiones.
- Se verifica la integridad de los paquetes y si se ha alterado se detectará, otras ventajas de este sistema de verificación son:

- No rechazo: al contestar a la comunicación se verifica la identidad.
- Evita la recolección de información mediante sniffers ya que el tráfico va encriptado.
- Evita ataques Man in The Middle (Para poder hacerlo tendrían que usar también técnicas de spoofing ARP).
- Permite tunelizar tráfico FTP, SMTP, etc...
- Permite comprimir los paquetes.

Funcionamiento del protocolo:

- El cliente se conecta a través del puerto 22 al servidor.
- El servidor y el cliente negocian la versión, el tipo de cifrado y otros parámetros.
- El servidor envía su clave pública al cliente.
- El cliente la compara con las claves que tiene y si es la primera vez, el cliente indica si es válida o no. En esta fase, un atacante podría suplantar el servidor.
- El cliente genera una clave de sesión aleatoria que se envía al servidor dentro de un paquete cifrado con el algoritmo seleccionado y la clave pública.
- A partir de este momento, las comunicaciones están encriptadas.

Tunelización SSH

Los túneles pueden encriptar otros protocolos y los convierten en más seguros o los centralizan para poder pasarlos por el cortafuegos.
Podemos crear uno desde la línea de comandos desde la siguiente manera:

```
ssh -L puertolocal:servidor:puertoservidor [usuario]@servidor
```

Ejemplo:

```
ssh -L 10443:smtp.gmail.com:443 usuario@smtp.gmail.com
```

Transferencia segura de archivos usando SSH (sftp y scp)

Para conectarnos a un servidor FTP de manera segura podremos usar la herramienta sftp, se usa de la siguiente forma:

```
sftp [usuario]@servidor
```

Para copiar archivos de manera segura entre servidor y cliente podremos usar scp de la siguiente forma:

```
scp origen destino
```

Ejemplo:

```
scp ~/Imágenes/juan/*.jpg juan@iesruizgijon.com:/imagenes
```

El VNC o programa de Computación en Red Virtual es otro programa de administración remota de código libre. El servidor utiliza el puerto 5900, los clientes de Windows el puerto 5800, y los de Linux y Mac OS el terminal que no estén usando (por ejemplo, si solo hemos activado un terminal, el siguiente puede acceder desde el puerto 5801, si tenemos activados cuatro debemos conectarnos por el puerto 5804, etc.).

Las características más importantes de VNC son:

- Permite crear pantallas virtuales en Linux y Mac OS, pero solo puede compartir la pantalla actual en Windows.
- En algunas versiones puede compartir la pantalla con varios clientes a la vez.
- Permite codificación IDEA de hasta 128 bits para encriptar y RSA de hasta 2048 bits para autenticar.
- Permite compartir impresoras.
- Permite FTP seguro.
- Permite chat seguro.
- Puede compartir aplicaciones con servidores Windows.

Remote Desktop Protocol (RDP) es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado). El modo de funcionamiento del protocolo es sencillo. La información gráfica que genera el servidor es convertida a un formato propio RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal. Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de windows, no se verá lo que el usuario está realizando de forma remota.

Los clientes de escritorio remoto son programas que se conectan a un servidor para administrarlo, ejecutar programas en máquinas más potentes, etc. Se suelen utilizar para la administración remota y así evitar desplazamientos, para acceder a servidores que no tienen pantalla, para teleformación, para solucionar problemas de configuración, etc.

FTP (File Transfer Protocol)

El protocolo de transferencia de archivos (File Transfer Protocol, FTP para abreviar) es un protocolo el cual se emplea para transferir archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, en el modelo OSI se encontraría en la capa de aplicación. Usa dos puertos: el puerto 20 que se encarga de transferir datos y el puerto 21 que sirve para comunicarnos con el servidor.

FTP está pensado para ser rápido pero no seguro, ya que las conexiones con el servidor no están cifradas, pudiendo ver incluso las credenciales de inicio de sesión al acceder al servidor usando programas de esnifado de red. Este problema se soluciona con aplicaciones como SCP o SFTP las cuales vienen incluidas en el paquete SSH, el cual permite las mismas funciones pero cifrando los archivos.

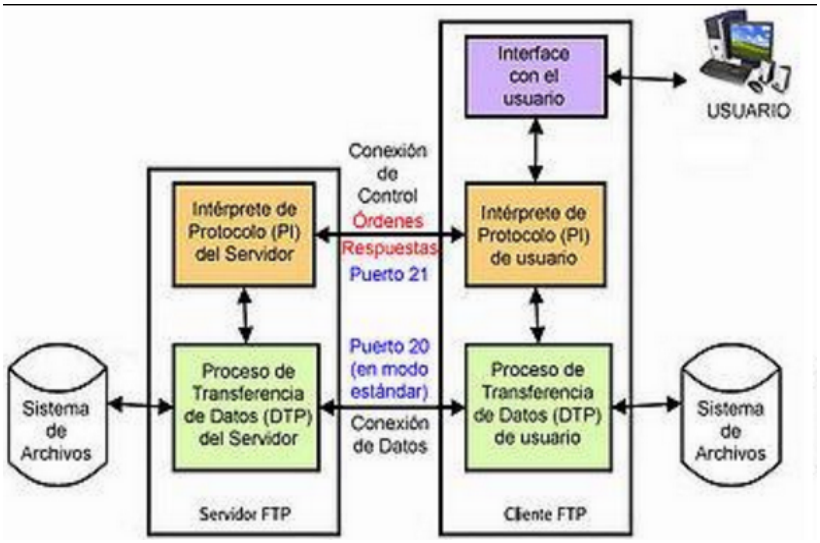
El protocolo FTP se empezó a usar en abril de 1971 y fue publicado bajo el RFC 114 antes de TCP/IP. Fue modificado varias veces al añadir nuevos comandos y funcionalidades. Acabó publicándose bajo el RFC 959 en 1885.

Protocolo de transferencia de archivos	
Familia	Familia de protocolos de Internet
Función	Transferencia de archivos
Puertos	20/TCP DATA Port 21/TCP Control Port
Ubicación en la pila de protocolos	
Aplicación	**FTP**
Transporte	TCP
Red	IP
Estándares	
FTP: RFC 959 (1985) Extensiones de FTP para IPv6 y NATs: RFC 2428 (1998)	

El protocolo FTP se empezó a utilizar en abril de 1971, publicado como el RFC 114, antes de que existiera la pila TCP/IP. La estructura general fue establecida en 1973. Fue modificado varias veces, añadiendo nuevos comandos y funcionalidades. Al final se publicó el RFC 959 en octubre de 1985, que es la que se utiliza actualmente.

El intérprete de protocolo del cliente inicia la conexión de control en el puerto 21. Las órdenes FTP las genera el intérprete de protocolo (PI) y se transmiten al proceso servidor por la conexión de control, las respuestas se envían del intérprete de protocolo del servidor hasta la del cliente por la conexión de control en respuesta a las órdenes.

.



También hay que destacar que la conexión de datos es bidireccional, es decir, se puede usar simultáneamente para enviar y para recibir, y no tiene por qué existir todo el tiempo que dura la conexión FTP.

Características Generales:

- Diferentes formas de acceso al servidor: Por medio de usuario y contraseña, el usuario debe existir en el servidor, de manera anónima usando el usuario anonymous y de manera virtual por medio de usuarios virtuales.
- Limitaciones de acceso al sistema de archivos acorde al usuario: El usuario anonymous solo accede a un directorio en específico, los usuarios locales acceden al sistema de archivos que comienza en su directorio de conexión. Los usuarios FTP acceden a los directorios en los que tienen permiso.
- Comunicación con el servidor: Se pueden usar distintas órdenes o comandos FTP para realizar tareas distintas como subir/descargar archivos, borrarlos, crear/borrar directorios, moverse entre directorios ver el tamaño de archivos, cerrar la conexión, etc…

- SERVIDOR FTP: Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores. Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él. Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol). Hay dos modos de ejecución del servidor.

1) Modo Standalone. El servidor se ejecuta como un proceso autónomo e independiente del sistema y siempre está activo esperando peticiones. Es el modo Recomendado.

2) Modo Supervisor. El proceso del servidor FTP se ejecuta por el inetd como si se tratara de un proceso hijo. El proceso del servidor debe iniciarse cada vez que hay una nueva conexión

- CLIENTE FTP: Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesitará utilizar un programa cliente FTP. Un cliente FTP es un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos. Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra. Algunos clientes de FTP básicos en modo consola vienen integrados en los sistemas operativos, incluyendo Microsoft Windows, DOS, GNU/Linux y Unix. Sin embargo, hay disponibles clientes con opciones añadidas e interfaz gráfica. Aunque muchos navegadores tienen ya integrado FTP, es más confiable a la hora de conectarse con servidores FTP no anónimos utilizar un programa cliente.

Acceso anónimo

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permiten acceder a sus archivos sin necesidad de tener un 'USER ID' o una cuenta de usuario. Es la manera más cómoda fuera del servicio web de permitir que todo el mundo tenga acceso a cierta información sin que para ello el administrador de un sistema tenga que crear una cuenta para cada usuario. Si un servidor posee servicio 'FTP anonymous' solamente con teclear la palabra «anonymous», cuando pregunte por tu usuario tendrás acceso a ese sistema. No se necesita ninguna contraseña preestablecida, aunque tendrás que introducir una sólo para ese momento, normalmente se suele utilizar la dirección de correo electrónico propia. Solamente con eso se consigue acceso a los archivos del FTP,

aunque con menos privilegios que un usuario normal. Normalmente solo podrás leer y copiar los archivos que sean públicos, así indicados por el administrador del servidor al que nos queramos conectar. Normalmente, se utiliza un servidor FTP anónimo para depositar grandes archivos que no tienen utilidad si no son transferidos a la máquina del usuario, como por ejemplo programas, y se reservan los servidores de páginas web (HTTP) para almacenar información textual destinada a la lectura en línea.

Acceso de usuario

Si se desea tener privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes, y de posibilidad de subir nuestros propios archivos, generalmente se suele realizar mediante una cuenta de usuario. En el servidor se guarda la información de las distintas cuentas de usuario que pueden acceder a él, de manera que para iniciar una sesión FTP debemos introducir una autentificación (en inglés: login) y una contraseña (en inglés: password) que nos identifica unívocamente.

Cliente FTP basado en Web

Un «cliente FTP basado en Web» no es más que un cliente FTP al cual podemos acceder a través de nuestro navegador web sin necesidad de tener otra aplicación para ello. El usuario se conecta mediante HTTP a un servidor web, y el servidor web se conecta mediante FTP al servidor de archivos. El servidor web actúa de intermediario haciendo pasar la información desde el servidor FTP en los puertos 20 y 21 hacia el puerto 80 HTTP que ve el usuario. Siempre hay momentos en que nos encontramos fuera de casa, no llevamos el ordenador portátil encima y necesitamos realizar alguna tarea urgente desde un ordenador de acceso público, de un amigo, del trabajo, la universidad, etc. Lo más común es que no estén instaladas las aplicaciones que necesitamos y en muchos casos hasta carecemos de los permisos necesarios para realizar su instalación. Otras veces estamos detrás de un proxy o cortafuegos que no nos permite acceder a servidores FTP externos. Al disponer de un cliente FTP basado en Web podemos acceder al servidor FTP remoto como si estuviéramos realizando cualquier otro tipo de navegación web. A través de un cliente FTP basado en Web podrás, crear, copiar, renombrar y eliminar archivos y directorios. Cambiar permisos, editar, ver, subir y descargar archivos, así como cualquier otra función del protocolo FTP que el servidor FTP remoto permita.

Acceso de invitado

El acceso sin restricciones al servidor que proporcionan las cuentas de usuario implica problemas de seguridad, lo que ha dado lugar a un tercer tipo de acceso FTP

denominado invitado (guest), que se puede contemplar como una mezcla de los dos anteriores. La idea de este mecanismo es la siguiente: se trata de permitir que cada usuario conecte a la máquina mediante su login y su password, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo, de esta forma accederá a un entorno restringido, algo muy similar a lo que sucede en los accesos anónimos, pero con más privilegios. Ejemplos de Clientes FTPs: Entre los varios clientes FTP que existen, se pueden mencionar los siguientes: Free FTP Upload Manager, F->IT , net2ftp , Web FTP.co.uk ,Web-Ftp, Jambai FTP ,ftp4net , PHP FTP Client , ,Asuk PHP FTP, Weeble File Manager ,FileZilla

MODOS DE CONEXIÓN

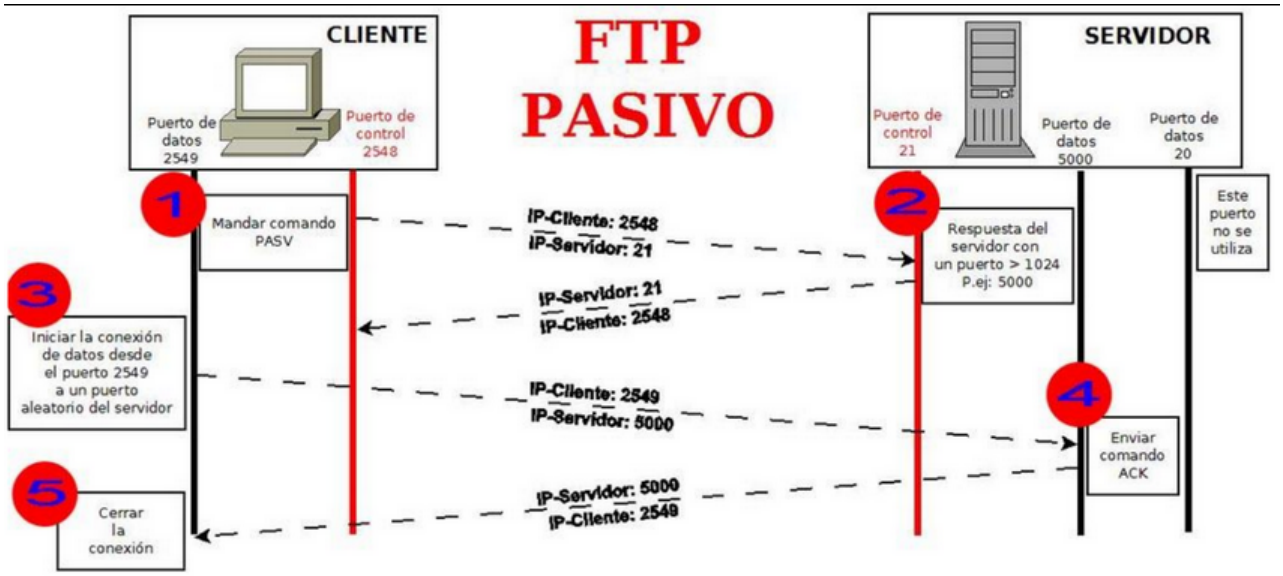
FTP admite dos modos de conexión del cliente. Estos modos se denominan activo (o Estándar, o PORT, debido a que el cliente envía comandos tipo PORT al servidor por el canal de control al establecer la conexión) y pasivo (o PASV, porque en este caso envía comandos tipo PASV). Tanto en el modo Activo como en el modo Pasivo, el cliente establece una conexión con el servidor mediante el puerto 21, que establece el canal de control.

Modo activo.

En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicando ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado. Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias. Para solucionar esto se desarrolló el modo pasivo

Modo pasivo

Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1024 del servidor. Ejemplo:2040) al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control (Ejemplo: 1036) hacia el puerto del servidor especificado anteriormente (Ejemplo: 2040). Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, según el modo en el que haya conectado), y el servidor recibirá esa conexión de datos en un nuevo puerto (aleatorio si es en modo pasivo o por el puerto 20 si es en modo activo).



Tipos de transferencia de archivos en FTP

En el protocolo FTP existen 2 tipos de transferencia en ASCII y en binarios. 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 solo contengan caracteres imprimibles (archivos ASCII, no archivos resultantes de un procesador de texto), por ejemplo páginas HTML, pero no las imágenes que puedan contener. Se transforman algunos símbolos de control para mantenerlos compatibles entre diferentes sistemas, por ejemplo, si el archivo está alojado sobre un servidor linux, el salto de línea para los archivos de texto es "\n" (byte 10 en decimal). Si el cliente es un sistema Mac, el salto de línea es "\r" (byte 13 en decimal), este modo cambia estos símbolos de control para que el archivo sea legible en ambos lados, al igual que si se envía a un sistema windows, el salto de línea es "\r\n" (dos bytes, 13 y 10). Si se usa este modo en archivos que no son de texto plano, en el caso de intercambiarse entre diferentes sistemas, ese archivo quedará corrupto.

Tipo Binario

Este tipo es usado cuando se trata de archivos comprimidos, ejecutables para PC, imágenes, archivos de audio, entre otros. 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 (poscript)	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

En la red existen diversas soluciones de software que desarrolla este tipo de tecnología, los más conocidos, son Filezilla (software libre) y CuteFTP (shareware).