TEMA 5-FTP INSTALACIÓN Y ADMINISTRACIÓN DE SERVICIOS DE TRANSFERENCIA DE FICHEROS

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- 2º ASIR- TEMA 4 HTTP-SRI

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.

Funcionalidad del servicio de transferencia de archivos.

Características. Componentes y funcionamiento.

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.

Este protocolo está descrito en el RFC 959 y en él se establecen los objetivos de dicho protocolo, qué básicamente son los siguientes:

- Promover que se compartan archivos entre máquinas remotas a través de la red.
- Como consecuencia de lo anterior, fomentar el acceso a máquinas remotas.
- Independizar las necesidades de los usuarios de diferentes sistemas de archivos utilizados en las diferentes máquinas.
- Conseguir una transferencia de datos rápida y fiable

El servicio FTP presenta una serie de deficiencias importantes en cuanto a seguridad:

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

FTP es un servicio basado en la arquitectura cliente/servidor, y su funcionamiento es el siguiente: existe un servidor FTP en la red (local o en Interet), que es el que proporciona el servicio, utilizando para ello dos puertos:

- Puerto 20 para transferencia de datos.
- Puerto 21 para transferencia de órdenes (control) .

Características de los servidores FTP

Con respecto al diseño del servicio:

- La conexión de un usuario remoto al servidor FTP puede hacerse como inicio de una sesión de un usuario que existe en el sistema o también como un usuario genérico que se llama anónimo
- El acceso al sistema de archivos del servidor FTP está limitado, dependiendo del tipo de usuario que se conecta.
- Una vez se ha establecido la conexión con el servidor FTP, el usuario tiene disponible el conjunto de órdenes FTP que permiten realizar las operaciones básicas de descarga(get) o subida(put) de archivos, junto con otras órdenes.

Con respecto a tipos de usuarios:

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

Protocolo FTP

El protocolo FTP (Protocolo de transferencia de archivos) es, como su nombre lo indica, un protocolo para transferir archivos.

La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos (descrito en RFC141) entre equipos del Instituto Tecnológico de Massachusetts (MIT, Massachusetts Institute of Technology). Desde entonces, diversos documentos de RFC (petición de comentarios) han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973.

Actualmente, el protocolo FTP está definido por RFC 959 (Protocolo de transferencia de archivos (FTP) - Especificaciones).

La función del protocolo FTP

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

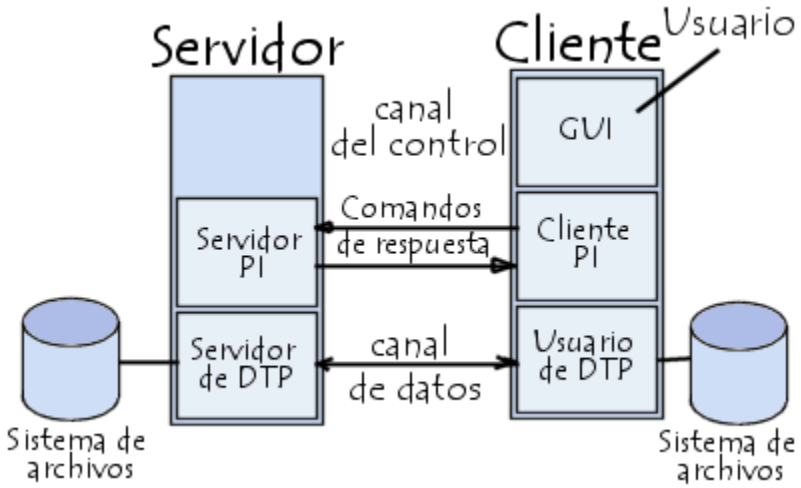
- permitir que equipos remotos puedan compartir archivos
- permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- permitir una transferencia de datos eficaz

El modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control)
- Un canal de datos



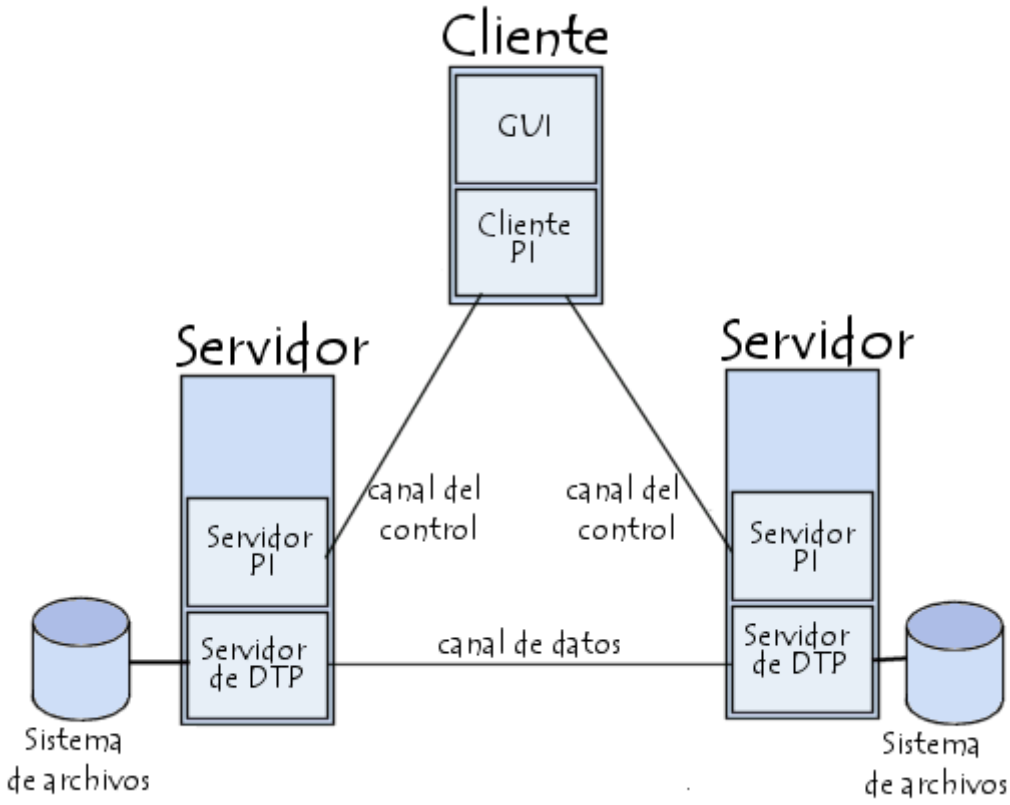
Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- DTP (Proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina SERVIDOR DE DTP y el DTP del lado del cliente se denomina USUARIO DE DTP.
- PI (Intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control.

Esto es diferente en el cliente y el servidor:

- El SERVIDOR PI es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del USUARIO PI a través de éste, de responderles y de ejecutar el SERVIDOR DE DTP.
- El USUARIO PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del SERVIDOR PI y de controlar al USUARIO DE DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor.
Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la transferencia de información entre dos procesos del servidor conectados en el puerto correcto.



En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

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

El FTP anónimo es un servicio que nos permite acceder a ficheros que están situados en un ordenador sin tener cuenta o estar registrados en él. Se accede utilizando el usuario especial anonymous y la contraseña es nuestra dirección de correo electrónico (por cortesía, como mínimo). Está específicamente orientado para trabajar con ficheros, cuyo contenido puede ser de lo más variado (texto, fotos, software, ejecutables...) y la transferencia se puede realizar entre ordenadores con distintos sistemas operativos y entre distintas redes, siempre que se tenga una aplicación que maneje este servicio.

Los servidores de FTP anónimo son los que permiten que cualquiera que esté conectado a Internet se conecte a ellos y descargue archivos. Es por ello que se utilizan para poner a disposición del gran público todo tipo de archivos.

Es la mejor alternativa al envío de mensajes de correo electrónico con ficheros grandes, ya que evita que los mensajes atraviesen varios servidores, saturándolos. Dichos ficheros se colocan en el servidor FTP anónimo y pueden ser recogidos por quien los necesite de una manera rápida y eficaz.

Para recoger un fichero, se necesita saber obligatoriamente el ordenador en el que está y se recomienda conocer la localización del fichero a transferir y el tipo de fichero, para saber si después de transferido, se disponen de las herramientas adecuadas para manejarlo como se desea.

Es muy recomendable guardar los archivos que descarguemos en un directorio temporal, ya que siempre vendrán comprimidos y su directorio final será probablemente otro distinto al de descarga. De esta forma siempre conservaremos el archivo comprimido inicial en un lugar localizado.

El FTP Autenticado se utiliza para conectarse a un servidor y enviar/recibir archivos a o desde un directorio para luego hacerlos públicos o privados. Por ejemplo, si deseásemos colocar estas páginas en Internet, habría que enviarlas al servidor. Pero, por otro lado, no nos gustaría que cualquiera pudiese acceder a ellas para cambiarlas o eliminarlas. Por tanto, se necesita un protocolo con contraseña.

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

PERMISOS

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.

CUOTAS

Si queremos que los usuarios de nuestro sistema no consuman más recursos de los disponibles resulta indispensable habilitar un límite de ocupación de espacio en el disco duro.
Esto es lo que se conoce como cuotas de disco.

Los pasos son los siguientes:

* Instalar la característica de control de cuotas

apt-get install quota

* Indicar las particiones en las que aplicaremos las quotas editando /etc/fstab y añadiendo las opciones usrquota, grpquota

<file system> <mount point> <type> <options> <dump> <pass>

/dev/hda5 /home ext3 defaults, usrquota, grpquota 0 2

* Crearemos los archivos de control de quota y reiniciamos las particiones

touch /home/quota.user /home/quota.group
chmod 600 /home/quota.*
mount -o remount /home

* Editar la quota de los usuarios

Antes de nada deberíais saber que existen dos tipos de cuota:
- Cuotas rígidas: no será posible superar el límite y será negado el acceso.
- Cuotas flexibles: se pueden superar y el usuario sólo recibirá un aviso de

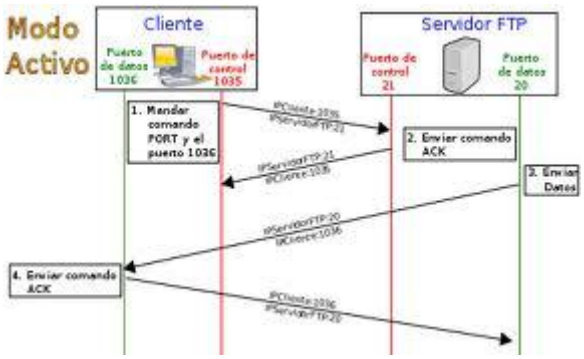
Se nos mostrará una serie de registros con los siguientes campos:

Filesystem (el sistema de archivos en el que se aplica la cuota)
blocks (el número de bloques máximo a ocupar. 0 = ilimitado)
soft (el número de KB máximo a ocupar para cuota flexible. 0 = ilimitado)
hard (el número de KB máximo a ocupar para quota rígida. 0 = ilimitado)
inodes (el número de archivos máximo. 0 = ilimitado)

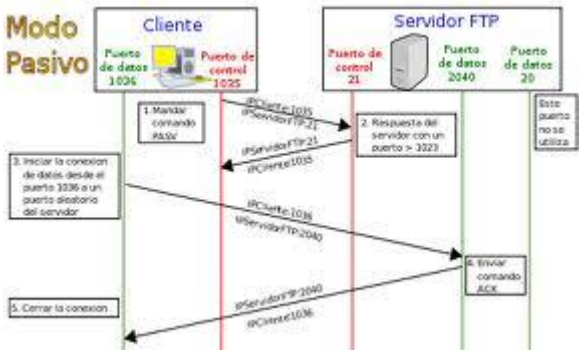
Conexiones y modos: Conexión de control y conexión de datos. Modos activo y pasivo.

Formas de conectarse a un servidor FTP:

- De modo Activo
  El cliente se conecta al puerto 21 del servidor desde un puerto superior al 1024 para enviarse comandos.
  El cliente le indica al servidor el puerto por el cual recibirá los datos.
  El servidor abre su puerto 20 para realizar la transferencia de datos sobre el cliente en el puerto especificado.
  Importante: El servidor siempre emplea el puerto 20 para transmisión de datos.
  Problema: El cliente debe aceptar conexiones en puertos superiores a 1024 (se evita con un Firewall).



- De modo Pasivo
  El cliente emplea un puerto superior al 1024 para conectar con el puerto 21 del servidor FTP y enviarle comandos.
  El servidor enviará por ese puerto, el puerto aleatorio que va a emplear para la comunicación de datos (puerto mayor a 1023).
  El cliente y el servidor abren el puerto especificado por el servidor y comienzan a transmitir datos.
  Aspectos a destacar: El cliente siempre inicia las comunicaciones y nunca se emplea el puerto 20 para transmitir datos.



Tipos de transferencia de archivos: ASCII y Binario.

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 (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

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

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.

Monitorización y registro del servicio de transferencia de archivos.

Se requiere cada vez más control sobre los archivos, bien por análisis posteriores, perdida de datos o robo de archivos. Una creciente regulación de los gobiernos (Sarbanes-Oxley, Gramm-Leach-Bliley Act, HIPAA) requiere cada vez más y más el cumplimiento de regulaciones standards y disponer de trazas de auditoría.

SFM proporciona alertas inmediatas, y en tiempo real cuando los trabajos FTP fallan, y un unas completas trazas de auditoría extremo a extremo. SFM deja un detallado log y trazas de auditoría para todas las transferencias FTP y SSH Tectia y de las sesiones de transferencia de ficheros indicándonos Quien transfiere Qué, Cuando y Donde (Who, What, When, Where). ¿Era una transferencia autorizada? ¿Terminó bien? SFM responde a estas preguntas y muchas más.

SFM dispone de informes standard, como los usuarios más activos, trabajos más utilizados, tamaño de archivos, tiempo de transferencia, y sesiones con problemas, transferencias fallidas, transferencias sospechosas, y por supuesto intentos fallidos de acceso al servidor.

Los auditores FTP pueden revisar cada aspecto del histórico de transferencias, obteniendo fácilmente los detalles de un sistema dado, sesión FTP, ficheros transferidos, o ID de usuario.

Seguridad en FTP.

Por naturaleza, el FTP no es seguro: El nombre de usuario, la contraseña y el resto de credenciales se transmiten por la red en texto sin cifrar. Del mismo modo, los archivos que se cargan o descargan lo hacen también en texto sin cifrar, por lo que su contenido puede ser visto y utilizado de forma malintencionada. Además, cualquier atacante podría suplantar al servidor FTP, en cuyo caso no se podría saber si un determinado servidor FTP es, en efecto, el equipo con el que el usuario intenta comunicarse. Por lo tanto, resulta muy arriesgado utilizar el adaptador de FTP para transmitir datos confidenciales a través de una red no segura, a menos que se pueda garantizar la seguridad en las capas de archivo o mensaje mediante cifrado y firmas digitales.

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

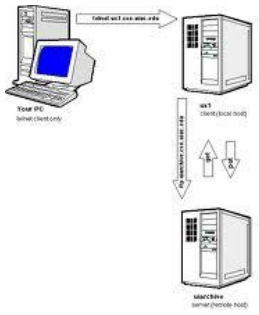
FTPS (comúnmente referido como FTP/SSL) es un nombre usado para abarcar un número de formas en las cuales el software FTP puede realizar transferencias de ficheros seguras. Cada forma conlleva el uso de una capa SSL/TLS debajo del protocolo estándar FTP para cifrar los canales de control y/o datos. No debería confundirse con el protocolo de transferencia de ficheros SFTP, el cual suele ser usado con SSH.

El uso más común de FTP y SSL es:

- AUTH TLS o FTPS Explicito, nombrado por el comando emitido para indicar que la seguridad TLS es obligatoria. Este es el método preferido de acuerdo al RFC que define FTP sobre TLS. El cliente se conecta al puerto 21 del servidor y comienza una sesión FTP sin cifrar de manera tradicional, pero pide que la seguridad TLS sea usada y realiza la negociación apropiada antes de enviar cualquier dato sensible.

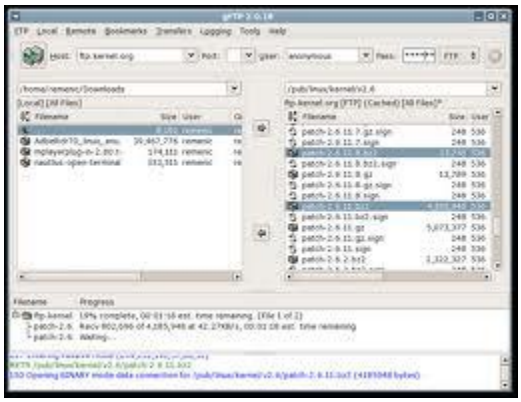
- AUTH como está definido en RFC 2228.

- FTPS Implícito es un estilo antiguo, pero todavía ampliamente implementado en el cual el cliente se conecta a un puerto distinto (como por ejemplo 990), y se realiza una negociación SSL antes de que se envíe cualquier comando FTP.



Protocolo FXP (File eXchange Protocol).

File Exchange Protocol (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 más 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.



•Servicio TFTP (Trivial File Transfer Protocol).

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Windows o cualquier otro cliente ligero arranca desde un servidor de red.

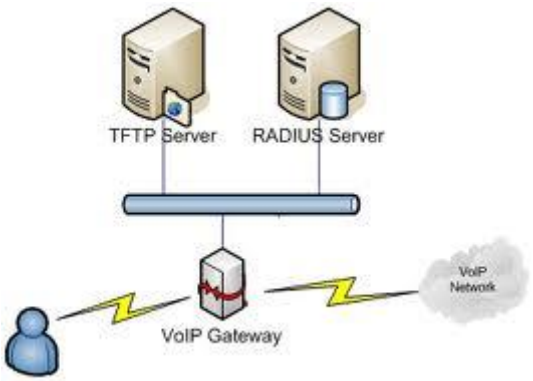
Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ASCII" e "imagen" (binario) del protocolo FTP.

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta.

Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.
- B responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.
- La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.
- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.



•Servicios SFTP/SCP.

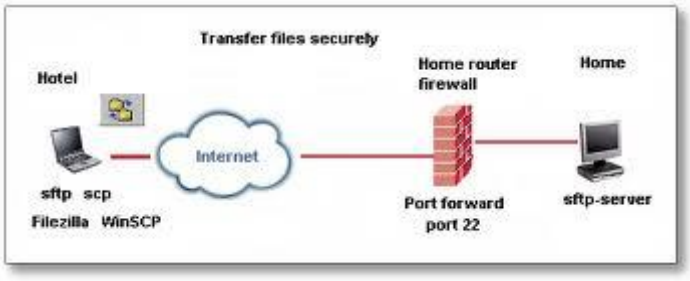
SFTP

SSH File Transfer Protocol (también conocido como SFTP o Secure File Transfer Protocol) es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar la seguridad a los datos, aunque permite ser usado con otros protocolos de seguridad. Por lo tanto, la seguridad no la provee directamente el protocolo SFTP, sino SSH o el protocolo que sea utilizado en su caso para este cometido.

En comparación de capacidades con el anterior protocolo SCP, que únicamente permite la transferencia de archivos (copia), el protocolo SFTP permite una serie de operaciones sobre archivos remotos. SFTP intenta ser más independiente de la plataforma que SCP, por ejemplo, con el SCP encontramos la expansión de comodines especificados por el cliente hasta el servidor, mientras que el diseño SFTP evita este problema. Aunque SCP se aplica con más frecuencia en plataformas Unix, existen servidores SFTP en la mayoría de las plataformas.

El Secure Internet Live Conferencing (SILC) define el protocolo SFTP como su protocolo de transferencia de archivos por omisión. En el SILC, los datos del protocolo SFTP no están protegidos con SSH pero el protocolo de paquetes seguros de SILC se utiliza para encapsular los datos SFTP dentro de los paquetes de SILC para que se la llevara de igual a igual (peer to peer, P2P). Esto es posible ya que SFTP está diseñado para ser un protocolo independiente.

SFTP utiliza el puerto 22 de TCP.



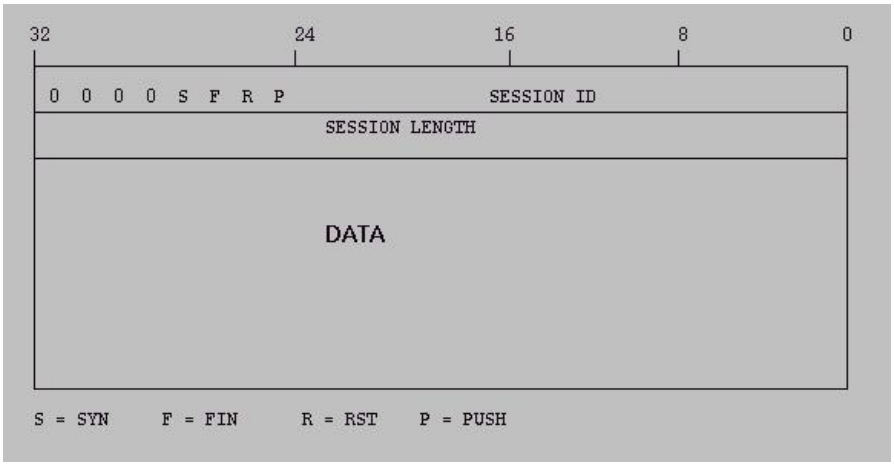
SCP

El protocolo SCP es básicamente idéntico al protocolo rcp de BSD. A diferencia de rcp, los datos son cifrados durante su transferencia, para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos. Sin embargo, el protocolo mismo no provee autenticación y seguridad; sino que espera que el protocolo subyacente, SSH, lo asegure.

El modo SCP o simple communication protocol, es un protocolo simple que deja al servidor y al cliente tener múltiples conversaciones sobre una TCP normal. Este protocolo está diseñado para ser simple de implementar.

El servicio principal de este protocolo es el control del dialogo entre el servidor y el cliente, administrando sus conversaciones y agilizadas en un alto porcentaje, este protocolo le permite a cualquiera de los dos establecer una sesión virtual sobre la normal.

La descripción de un formato de comunicación en las cabeceras enviadas por la red es la siguiente:



SCP puede solicitar de manera iterativa cualquier contraseña para establecer una conexión con un host remoto.

El protocolo SCP implemente la transferencia de archivos únicamente. Para ello se conecta al host usando SSH y allí ejecuta un servidor SCP. Generalmente el programa SCP del servidor es el mismo que el del cliente.

Para realizar la subida, el cliente le proporciona al servidor los archivos que desea subir y opcionalmente puede incluir otros atributos (permisos, fechas, etc.) Esto es una ventaja sobre el protocolo FTP.

Para descargar, el cliente envía una solicitud por los archivos que desea descargar. El proceso de descarga está dirigido por el servidor y es el que se encarga de la seguridad del mismo. Frecuentemente, para los usos aquí detallados se utiliza el protocolo SFTP, también basado en SSH.

El programa SCP es un cliente que implementa el protocolo SCP, es decir, es un programa que realiza copia segura.

El cliente SCP más ampliamente usado es el programa scp del Intérprete de comandos, que es incorporado en la mayoría de las implementaciones de SSH. El programa scp es el análogo seguro del comando rcp. El programa scp debe formar parte de todos los servidores SSH que quieran proveer el servicio SCP, así como scp funciona como servidor SCP también.

Algunas implementaciones de SSH proveen del programa scp2, el cual usa el protocolo SFTP en lugar de SCP, pero provee los mismas interfaz del Intérprete de comandos el scp. Este scp es normalmente un enlace simbólico a scp2.

•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.

CARACTERISTICAS

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

PROTOCOLOS y SOFTWARE

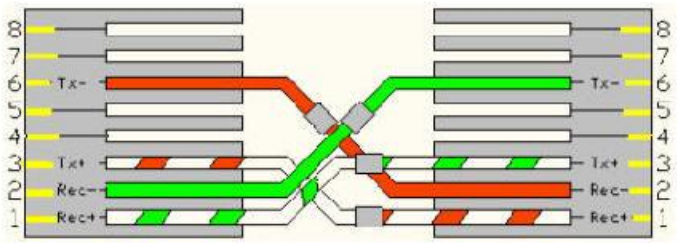
- Ares: Ares Galaxy, FileCroc, KCeasy, Warez P2P
- BitTorrent: AllPeers, ABC [Yet Another BitTorrent Client], Azureus, BitComet, BitSpirit, BitTornado, BitLord, BitTorrent, BitTorrent.Net, Burst!, G3 Torrent, Lphant, mlMac, MLDonkey, QTorrent, Shareaza, Transmission, Tribler, µTorrent
- CSpace: sistema de comunicaciones basado en peer-to-peer
- Direct Connect network: DC++, NeoModus Direct Connect, BCDC++, StrongDC++
- Domain Name System
- eDonkey2000: aMule, eDonkey2000, eMule, LMule, Lphant, MLDonkey, mlMac, Shareaza, xMule, iMesh
- FastTrack: giFT, Grokster, iMesh (y sus variantes sin adware incluyendo aiMesh Light), Kazaa (y todas sus variantes libres de adware como Kazaa Lite), KCeasy (plugin requerido), Mammoth, MLDonkey, mlMac, Poisoned
- Freenet: Entropy (bajo su propia red), Freenet
- GNUnet: GNUnet, (GNUnet-gtk)
- Gnutella: Acquisition, BearShare, Cabos, Gnucleus, Grokster, iMesh, gtk-gnutella, KCeasy, Kiwi Alpha, LimeWire, FrostWire, MLDonkey, mlMac, Morpheus, Phex, Poisoned, Swapper, Shareaza, XoloX
- Gnutella2: Adagio, Caribou, Gnucleus, iMesh, Kiwi Alpha, MLDonkey, mlMac, Morpheus, Shareaza, TrustyFiles
- Kad (usando el protocolo Kademlia): aMule, eMule, Lphant (a partir de la versión 3.50), MLDonkey,
- Lime Wire
- MANOLITO/MP2P: Blubster, Piolet
- MFPnet: Amicima
- Napster: Napigator, OpenNap, WinMX
- NEO Network: Morpheus
- P2PTV tipo de redes: TVUPlayer, CoolStreaming, Cybersky-TV, TVants
- Peercasting tipo de redes: PeerCast, IceShare, FreeCast
- Usenet
- WPNP: WinMX

- Otras redes: ANts P2P, Applejuice, Audiogalaxy, Avalanche, CAKE, Chord, The Circle, Connecta 2000, Coral, Dijjer, EarthStation 5, FileTopia, Groove, Hamachi, iFolder, konspire2b, Madster/Aimster, MUTE, OpenFT, P-Grid, IRC, JXTA, KoffeePhoto, Peersites, MojoNation, Mnet, Octoshape, Omemo, Overnet, Scour, Skype, Solipsis, soribada, Soulseek, SPIN, Swarmcast, WASTE, Winny

CONFIGURACIÓN

REQUISITOS PARA LA CONFIGURACIÓN:

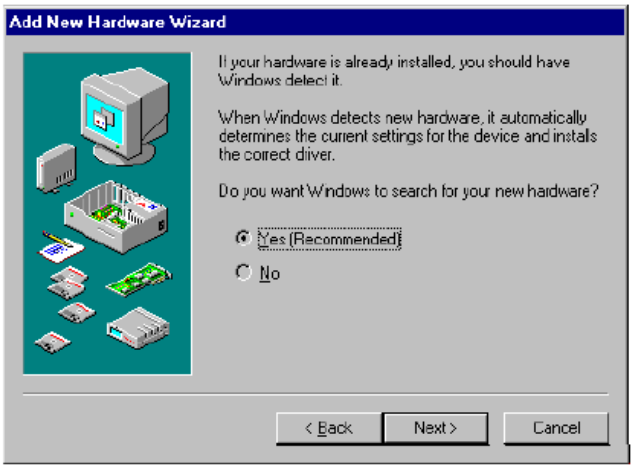
1. Dos computadoras
2. Adaptadores de red, uno para cada computadora.
3. Si tienes adaptadores tipo T, y sólo tienes dos computadoras, puedes conectar una computadora directamente a la otra. Pero necesitarás modificar el cable de conexión , conectando los pines: 1--3, 2--6, 3--1, 6--2, y los 4,5,7 y 8 no se usarán.



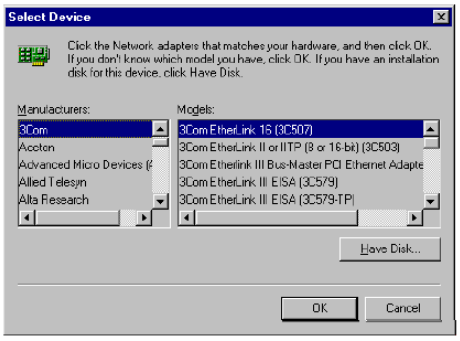
4. Si tiene más de dos computadoras, necesitará un hub.
5. Cables apropiados dependiendo del tipo de adaptadores que use.

AGREGANDO EL ADAPTADOR DE RED

1. Abra el Panel de Control
2. Haga clic en Agregar Nuevo Hardware
3. Haga clic en el botón siguiente.
4. Seleccione Si, para la búsqueda automática, o seleccione No, para la búsqueda manual.



5. Haga clic en el botón Siguiente.
6. Si selecciona NO, necesitará seleccionar un adaptador de una lista.



7. Reinicie la máquina si se lo pide

AGREGANDO LOS PROTOCOLOS

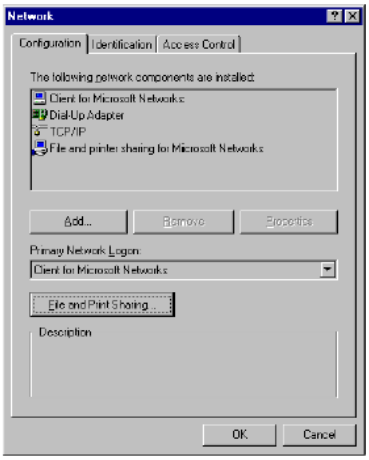
1. Necesitará decidir qué protocolo usará para su red.
2. Si nunca va a utilizar el dial-up para Internet, podría usar el NetBEUI o IPX.
3. Si va a conectarse a Internet, puede seleccionar el TCP/IP y simplemente asignar una dirección IP arbitraria para su Lan. También puede tener el NetBEUI o IPX, junto con el TCP/IP.
4. Abra el Panel de control.
5. Haga clic en el botón del icono de Red
6. De su detección del adaptador de red, debe tener Client for Microsoft network, Clients for Netware, your adapter, IPX y NetBEUI instalados.
7. Si quiere el NetBEUI, remueva el IPX o viceversa.
8. Si quiere agregar TCP/IP, Haga clic en el botón Add.
9. Haga clic en el botón de Protocolo.
10. Haga clic en el botón de Microsoft.
11. Haga clic en el botón de TCP/IP.

CONFIGURANDO LA RED

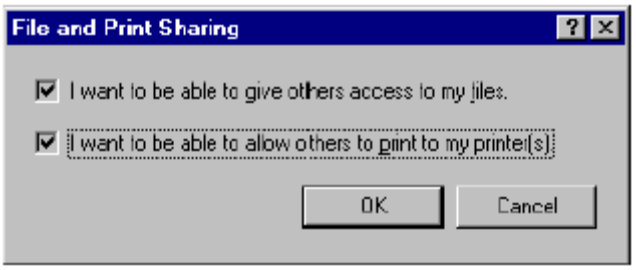
1. Bajo el Panel de Control / Red / Identificación, fíjese que cada computadora tenga un único nombre.
2. Asegúrese que el nombre de Workgroup es el mismo para todas las computadoras.
3. No ponga ningún espacio en el nombre del Workgroup.
4. Si tienes el TCP/IP instalado, seleccione IP diferentes con la misma máscara. No tiene que llenar el campo WINS, Gateway ni DNS.
5. Haga clic en el botón de Compartir Archivos e Impresoras y verifique, que es lo que quiere compartir.

COMPARTIENDO RECURSOS LOCALES

1. Abra el Icono de Red en el Panel de Control.
2. Debe ver Compartir Archivo e Impresora debajo de los protocolos.

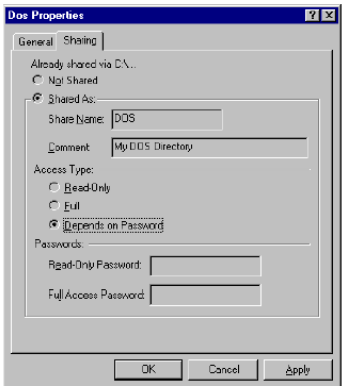


3. Si no los ve Haga clic en el botón de Compartir Archivo e Impresora .
4. Haga clic en las opciones, haga clic en OK para activarlas.



RECURSOS LOCALES

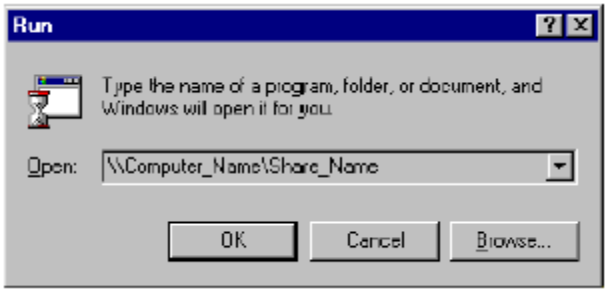
1. Abra el Explorador.
2. Haga clic en el directorio que quiere compartir y seleccione Compartir.



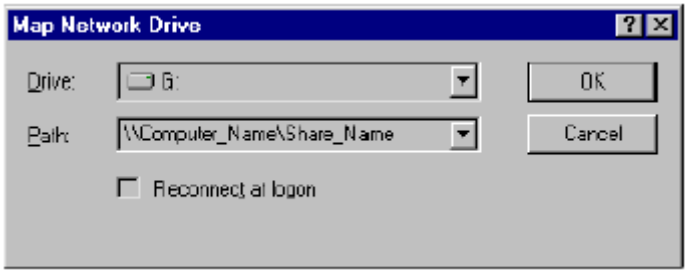
3. Escriba el nombre
4. Seleccione los atributos de Lectura, Escritura o con Clave.
5. Escriba la clave si es necesario.
6. Pasos similares para compartir una impresora.

PARA CONECTARSE A LOS RECURSOS COMPARTIDOS DE OTRA COMPUTADORA

1. Vaya a Inicio / Ejecutar
2. Escriba \ \nombre_de_computadora\nombre_compartido.



3. O abra el Explorador.
4. Haga clic en el primer icono para conectar a una unidad de red (o herramientas/Mapa de unidades de red)
5. Seleccione una unidad.
6. Escriba \ \nombre_de_computadora\nombre_compartido.



7. Ahora podrá enviar y recibir archivos.