File sharing y Retroshare

Jammily Ortigoza
jammy8806@gmail.com

Universidad Católica Nuestra Señora de la Asunción
Facultad de Ciencias y Tecnología
Ingeniería Informática

Resumen En este artículo se dará a conocer Retroshare, una herramienta sencilla y eficaz al momento de compartir archivos de forma segura a través de Internet. Se conocerá qué es Retroshare, cómo opera y porqué confiar al momento de utilizarla en las diferentes funcionalidades que nos provee.

1. Introducción

El acto de compartir archivos es el intercambio u ofrecimiento de acceso público o privado de datos informáticos (recursos informáticos, documentos, multimedia, imágenes, programas de computadoras, *e-books* y gráficos) o espacio en la red con varios niveles de privilegio de acceso. Aunque los archivos pueden ser fácilmente compartidos fuera de la red (por ejemplo a través de dispositivos de almacenamiento), el uso del término *File Sharing* casi siempre significa compartir archivos en una red, aunque sea en una pequeña red de área local. La compartición de archivos permite que un número de personas tenga acceso a él con el mismo o diferente nivel de privilegios.
Los métodos más comunes de almacenamiento, distribución y transmisión a parte de los dispositivos de almacenamiento extraíbles son: instalación de servidores de hosting de archivos centralizados en redes, documentos con hipervínculos orientados a la *World Wide Web* y redes *Peer-to-Peer*. Como en Internet nada es completamente seguro, los archivos a ser compartidos están expuestos a varios niveles de riesgos. Una manera de combatir la inseguridad es con la utilización del software **Retroshare** el cuál nos provee un método eficaz y seguro de compartir y obtener datos proveyendo identificación y autenticación fiable de amigos, comunicación cifrada, una plataforma de comunicación que puede soportar potencialmente servicios como correo electrónico seguro, uso compartido de archivos, *streaming*, vídeo o voz sobre IP, fotos, muro y mensajería y una red de intercambio social descentralizada diseñada “para el pueblo” sin dependencias en cualquier sistema corporativo o servidores centrales.

2. *File Sharing*

Es el acto de distribuir o proveer acceso a información almacenada digitalmente, tales como programas informáticos, multimedia (audio, imágenes y video), documentos o libros electrónicos. Puede ser implementado con distintos tipos de almacenamiento, transmisión y modelos de distribución. Algunos de los métodos más comunes son la distribución manual mediante el uso de medios extraíbles (CD,DVD, disquetes, cintas magnéticas, memorias flash), instalaciones centralizadas de servidores de archivos en redes informáticas, documentos enlazados de la *World Wide Web*, y el uso de redes *peer-to-peer* distribuidas. [2]

3. Redes *Peer-to-Peer*

Una red *peer-to-peer* (P2P) o red punto a punto 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.

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 (archivos) de cualquier tipo (audio, vídeo o software). Este tipo de red también suele usarse en telefonía VoIP (*Voice over IP*)[1] 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 (*firewall*[2], NAT (*Network Address Translation*)[3], ruteadores, etc.), velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco.

[6]

[1] Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

[2] Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

[3] Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

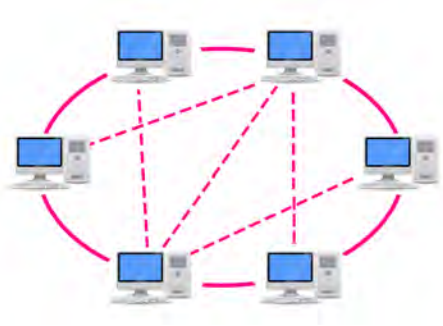


Figura 1. . Red *Peer-to-Peer*

3.1. Características

Las característias deseables de *peer-to-peer*:

- **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.
- **Robustez**. La naturaleza distribuida de las redes P2P 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.
- **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.
- **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 [4], gestión de derechos de autor, reputación, comunicaciones seguras, comentarios sobre los ficheros, etc.

3.2. Clasificación

- Redes P2P centralizadas: Este tipo de red P2P se basa en una arquitectura monolítica en la que todas las transacciones se hacen a través de un único servidor que sirve de punto de enlace entre dos nodos y que, a la vez, almacena y distribuye los nodos donde se almacenan los contenidos.
  Poseen una administración muy dinámica y una disposición más permanente de contenido. Sin embargo, está muy limitada en la privacidad de los usuarios y en la falta de escalabilidad de un sólo servidor, además de ofrecer problemas en puntos únicos de fallo, situaciones legales y enormes costos en el mantenimiento, así como el consumo de ancho de banda.
  Una red de este tipo reúne las siguientes características:
  - Se rige bajo un único servidor, que sirve como punto de enlace entre nodos y como servidor de acceso al contenido, el cual distribuye a petición de los nodos.
  - Todas las comunicaciones (como las peticiones y encaminamientos entre nodos) dependen exclusivamente de la existencia del servidor.

  Ejemplos de este tipo de redes son Napster[5] y Audiogalaxy[6].
- Redes P2P semicentralizadas o mixtas: En este tipo de red, se puede observar la interacción entre un servidor central que sirve como hub y administra los recursos de banda ancha, enrutamientos y comunicación entre nodos pero sin saber la identidad de cada nodo y sin almacenar información alguna, por lo que el servidor no comparte archivos de ningún tipo a ningún nodo. Tiene la peculiaridad de funcionar (en algunos casos como en Torrent) de ambas maneras, es decir, puede incorporar más de un servidor que gestione los recursos compartidos, pero también, en caso de que el servidor o los servidores que gestionan todo caigan, el grupo de nodos puede seguir en contacto a través de una conexión directa entre ellos mismos, con lo que es posible seguir compartiendo y descargando más información en ausencia de los servidores.
  Este tipo de P2P presenta las siguientes características:

[4] Es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros.

[5] Fue un servicio de distribución de archivos de música (en formato MP3), la primera gran red P2P de intercambio creado por Sean Parker y Shawn Fanning.

[6] En sus inicios se utilizó como motor de búsqueda para mp3 sobre servidores FTP, actualmente es una aplicación P2P destinada al intercambio de música entre usuarios a través de Internet.

- Tiene un servidor central que guarda información en espera y responde a peticiones para esa información.
- Los nodos son responsables de hospedar la información (pues el servidor central no almacena la información) que permite al servidor central reconocer los recursos que se desean compartir, y para poder descargar esos recursos compartidos a los usuarios que lo solicitan.
- Las terminales de enrutamiento son direcciones usadas por el servidor, que son administradas por un sistema de índices para obtener una dirección absoluta. Algunos ejemplos de una red P2P híbrida son BitTorrent[7], eDonkey y Direct Connect.

- Redes P2P puras, totalmente descentralizadas: Las redes P2P de este tipo son las más comunes, siendo las más versátiles al no requerir de un gestionamiento central de ningún tipo, lo que permite una reducción de la necesidad de usar un servidor central, por lo que se opta por los mismos usuarios como nodos de esas conexiones y también como almacenadores de esa información. En otras palabras, todas las comunicaciones son directamente de usuario a usuario con ayuda de un nodo (que es otro usuario) quien permite enlazar esas comunicaciones.

  Las redes de este tipo tienen las siguientes características:
  - Los nodos actúan como cliente y como servidor.
  - No existe un servidor central que maneje las conexiones de red.
  - No hay un enrutador central que sirva como nodo y administre direcciones.

  Algunos ejemplos de una red P2P "pura" son: Kademlia, Ares Galaxy, Gnutella, Freenet y Gnutella2.

[7] Es un protocolo diseñado para el intercambio de archivos peer-to-peer en Internet.

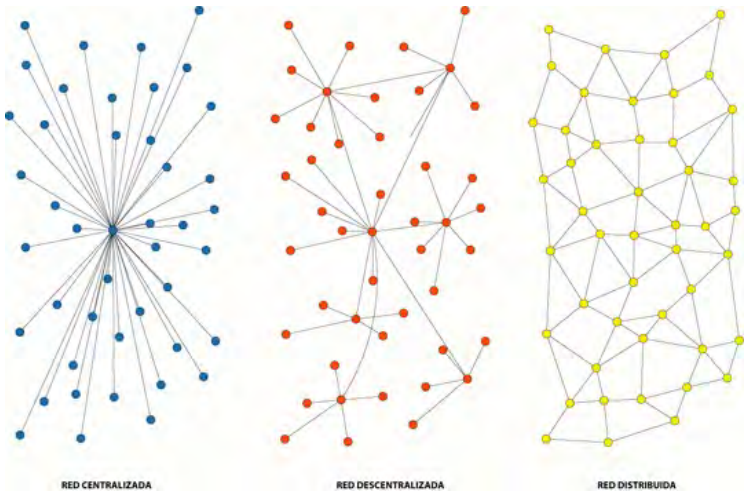


Figura 2. . Topologías de red

3.3. Otra clasificación

También se podría clasificar las redes P2P según su generación:

- **Primera generación de P2P**: son literalmente las primeras redes P2P, que eran centralizadas.
- **Segunda generación de P2P**: en esta generación se implementó por primera vez la característica de la descentralización, y esta característica es la más frecuente en los actuales P2P.
- **Tercera generación de P2P**: los más recientes, que implementan una comunicación no directa, cifrada y anónima.

Existe también la posibilidad de clasificar las redes P2P según sus características de anonimidad o exclusividad:

- Sin características de anonimidad
- Pseudónimo
- Red P2P Privada
- *Friend-to-Friend* (De amigo a amigo)

3.4. Peer to Peer anónimo

Peer-to-Peer anónimo es un tipo particular de red peer-to-peer en la que los usuarios y sus nodos son pseudoanónimos por defecto. Por tanto este tipo de tecnologías pertenecen a la llamada *Darknet*[8]. La principal diferencia entre

[8] Se puede decir que es una colección de redes y tecnologías usadas para compartir información y contenidos digitales que está "distribuida" entre distintos nodos y que trata de preservar el anonimato de las identidades de quienes intercambian dichas información.

las redes habituales y las anónimas está en el método de encaminamiento de las respectivas arquitecturas de redes. Estas redes permiten el flujo libre de información.
Esto es debido a su diseño, un nodo de la red debe tener un pseudónimo desde que tiene que tener una «dirección» para poder ser alcanzado por otro nodo igual para intercambiar datos. Sin embargo, normalmente esta dirección, especialmente en redes anónimas, no contiene ninguna información que pueda permitir la identificación.
Cuando se reciben datos en cualquier red, esta debe venir de algún sitio y los datos se deben haber pedido anteriormente por alguien. El anonimato viene de la idea en la que nadie sabe quién requiere la información ya que es difícil, pero no imposible, determinar si un usuario ha pedido los datos para él mismo o simplemente está pidiendo datos que le ha requerido otro usuario. El resultado final es que todo el mundo en una red anónima actúa como un emisor y un receptor universal para mantener el anonimato. Por tanto, un usuario es casi pero no completamente anónimo.
[7]

3.5. *Friend-to-Friend*

Una red de ordenadores *friend-to-friend* (F2F) o "amigo a amigo" es un tipo particular de P2P anónimo en donde la gente se conecta directamente con sus "amigos". Los programas F2F solamente permiten personas en las cuales uno confía, usando direcciones de IP o firmas digitales para hacer los intercambios de archivos. De esta manera los amigos de sus amigos (y así sucesivamente) podrán descargar indirectamente archivos de una persona de manera anónima. Una de las mayores ventajas de este tipo de redes es que pueden crecer en tamaño sin comprometer el anonimato del usuario. [3]

Red o Protocolo	Clasificación	Uso
Ares	P2P descentralizadas	Intercambio de ficheros
Audiogalaxy	P2P centralizadas	Intercambio de multimedia
BitTorrent	P2P semicentralizadas	Intercambio de ficheros / Distribución de Software / Distribución multimedia
Direct Connect	P2P semicentralizadas	Intercambio de ficheros / chat
eDonkey	P2P semicentralizadas	Intercambio de ficheros
Freenet	P2P descentralizadas	Almacenamiento distribuido
Gnutella	P2P descentralizadas	Intercambio de ficheros
Gnutella2	P2P descentralizadas	Intercambio de ficheros
Kademlia	P2P descentralizadas	Intercambio de ficheros
Napster	P2P centralizadas	Intercambio de ficheros
Retroshare	F2F	Intercambio de ficheros / Chat / Instant Messenger / Grupos de noticias

Cuadro 1. . Tabla de Redes y Protocolos

4. Riesgos de *File Sharing*

- **Instalación de código malicioso**: al utilizar aplicaciones P2P, es difícil, por no decir imposible, comprobar si el origen de los archivos es de confianza. Estas aplicaciones son de uso frecuente por los atacantes para transmitir código malicioso. Los atacantes pueden incorporar software espía, virus, troyanos o *worms* en los archivos.
- **Exposición de información sensible o personal**: mediante el uso de aplicaciones P2P, se puede dar a otros usuarios el acceso a la información personal ya sea porque ciertos directorios son accesibles o porque se piensa que la dicha información se proporciona a personas u organizaciones de confianza. Una vez que los datos personales han sido expuestos a personas no autorizadas, es difícil saber cuántas personas no autorizadas han tenido acceso a ellas. La disponibilidad de informaciones como datos médicos, financieros o documentos personales puede aumentar el riesgo de robo de identidad.
- **Suceptibilidad al ataque**: Algunas aplicaciones P2P pueden tener la necesidad de abrir puertos en el *firewall* para transmitir archivos. Sin embargo, la apertura de algunos puertos puede dar a los atacantes el acceso a la computadora o dar oportunidad de atacar al ordenador mediante el aprovechamiento de las vulnerabilidaddes.
- ***Denial of service***: la descarga de archivos hace que una gran cantidad de tráfico pase a través de la red. Esta actividad puede reducir la disponibilidad de ciertos programas en la computadora o puede limitar el acceso a Internet.
- ***Prosecution***: los archivos compartidos a través de aplicaciones P2P pueden incluir software pirata, el material con derechos de autor o la pornografía. Si se descargan estos archivos, aún sin saberlo, es posible enfrentar multas u otras acciones legales. Si el equipo está expuesto a una red corporativa y expone información del cliente, tanto el dueño de la empresa puede ser responsable. [13]

5. Conceptos

5.1. Criptografía asimétrica

La criptografía asimétrica, también llamada criptografía de clave pública, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.
[1]

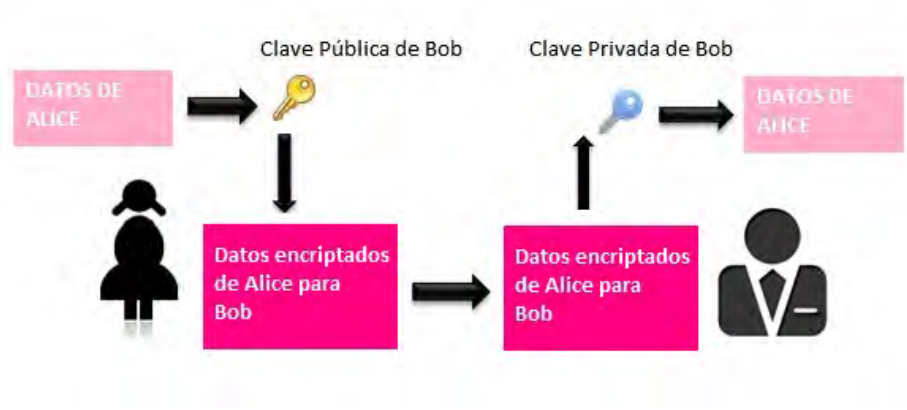


Figura 3. . Criptografía asimétrica

5.2. *GNU Privacy Guard* (GPG)

Es una herramienta de cifrado y firmas digitales, que viene a ser un reemplazo del PGP (*Pretty Good Privacy*) pero con la principal diferencia que es software libre licenciado bajo la GPL [9]. GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios de muchas maneras, un ejemplo de ello es depositándolas en los servidores de claves. Siempre deben ser compartidas cuidadosamente para prevenir falsas identidades por la corrupción de las claves públicas. También es posible añadir una firma digital criptográfica a un mensaje, de esta manera la totalidad del mensaje y el remitente pueden ser verificados en caso de que se desconfíe de una correspondencia en particular. [4]

5.3. *Distributed Hash Tables* (DHT)

Las *Distributed Hash Tables* (DHT) o Tablas de Hash Distribuidas, son una clase de sistemas distribuidos descentralizados que proveen un servicio de búsqueda similar al de las tablas de hash, donde pares (clave, valor) son almacenados en el DHT, y cualquier nodo participante puede recuperar de forma eficiente el valor asociado con una clave dada. La responsabilidad de mantener el mapeo de las claves a los valores está distribuida entre los nodos, de forma que un cambio en el conjunto de participantes causa una cantidad mínima de interrupción. Esto permite que las DHTs puedan escalar a cantidades de nodos extremadamente grandes, y que puedan manejar constantes errores, llegadas y caídas de nodos. [9]

[9] *GNU General Public License* es la licencia más ampliamente usada en el mundo del software y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar software.

5.4. *Secure SHell* (SSH)

Secure SHell (SSH) o Intérprete de Órdenes Segura, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH. [10]

5.5. *OpenSSL*

Consiste en un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como *OpenSSH* y navegadores web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el *Secure Sockets Layer* (SSL), así como otros protocolos relacionados con la seguridad, como el *Transport Layer Security* (TLS). Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina con un sistema operativo libre basado en GNU/Linux. *OpenSSL* también permite crear certificados digitales que pueden aplicarse a un servidor, por ejemplo Apache. [5]

6. Retroshare

Es un software para comunicaciones de red encriptadas, sin-servidores, email, Instant messaging, BBS[10] y compartición de archivos basada en una red *friend-to-friend*, haciendo uso de GPG. No es estrictamente una *darknet* dado que los pares pueden opcionalmente comunicar certificados y direcciones IP de/a sus amigos. [11], [8]

6.1. Características

- Red horizontal y sin servidores, completamente descentralizada.
- Múltiples y simultáneas descargas/subidas.
- Buscador de amigos.
- Chat.
- Foros.
- Canales.
- Voz sobre ip (VoIP).

[10] *Bulletin Board System* o Sistema de Tablón de Anuncios (BBS) es un software para redes de computadoras que permite a los usuarios conectarse al sistema y utilizando un programa terminal, realizar funciones tales como descargar software y datos, leer noticias, intercambiar mensajes con otros usuarios, disfrutar de juegos en línea, leer los boletines, etc.

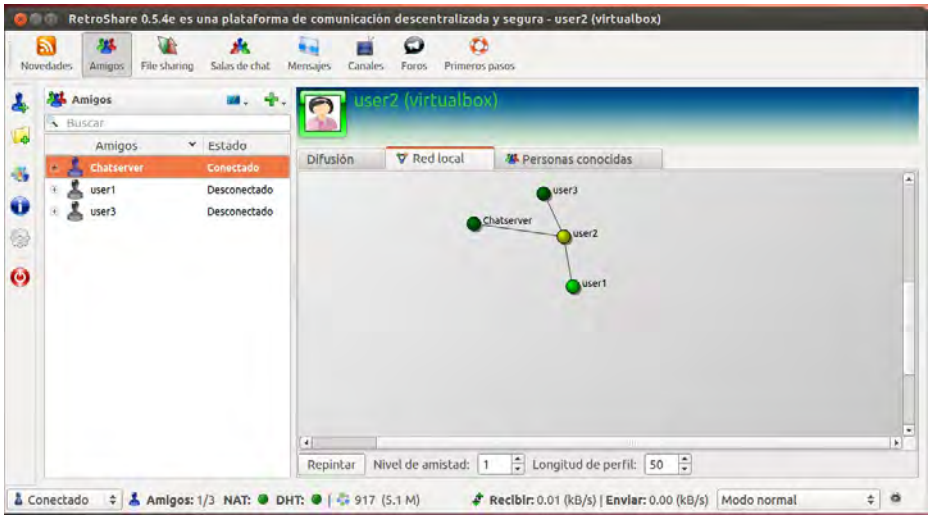
- Mensajería instantánea.
- Chat grupal.
- Autenticación mediante el sistema cifrado GnuPG.
- Encriptación mediante *OpenSSL*.
- Añadir descargas a través de enlaces a sitios web.
- Soporte de complementos (*pluggins*).
- Soporte para reenvío de puertos UPnP / NAT-PMP.
- Interfaz gráfica escrita en con el set de herramientas Qt4.
- Integración en la barra de tareas del sistema operativo.
- Disponible en 15 idiomas y aumentando.
- Soporte para reanudación de las descargas tras el cierre de la aplicación.
- Vista de estadísticas internas del router.
- Guía de instalación rápida (para sencilla configuración inicial de RetroShare).
- Multiplataforma (Windows XP/Vista/7/8, Mac OSX, Ubuntu, Debian, Fedora, OpenSUSE, Mandriva, entre otros).

6.2. La forma descentralizada

La naturaleza descentralizada de la red Retroshare requiere que la información fluya progresivamente a través de amigos mientras se conectan a los demás. Esto sucede, por ejemplo, con los foros y canales Retroshare, donde los suscriptores propagan temas interesantes a sus amigos. Esto anima a poner las cosas en movimiento y dejar que la red los maneje en silencio: enviar mensajes a los amigos, inicio de descargas, suscripción a canales - y dejar Retroshare se preocupe de eso en *background*. Actualizará a los amigos cuando estén en línea, y avisará cuando lleguen los nuevos contenidos. Se puede incluso leer los nuevos mensajes fuera de línea, ya que la mayoría del contenido estará en la caché local para que pueda ser accedida en cualquier momento.

6.3. Red localizada

Retroshare informa acerca de las personas nos rodean: amigos y, opcionalmente, amigos de amigos, pero muy poco acerca de lo que hay más allá. Se puede recibir información como mensajes en el foro y archivos desde el resto de la red, pero no se tiene conocimiento acerca de la fuente original de la información. El diseño de Retroshare asegura se tenga poca idea de lo que está ahí fuera - son sólo los amigos, de los amigos, de los amigos *ad infinitum*.



Cuadro 2. . Información sobre personas con las que "user2" esta conectado.

6.4. Autenticación y conectividad

Tras la instalación, RetroShare genera un par de claves GPG. Luego de la autenticación e intercambio de una clave asimétrica, se usa SSH para establecer la conexión. La encriptación extremo-a-extremo se realiza mediante *OpenSSL*. Amigos de amigos no pueden conectarse por defecto, pero pueden verse entre ellos si los usuarios así lo permiten.
Es posible compartir carpetas entre amigos. La transferencia de archivos se realiza sobre el uso de un sistema de enjambre de múltiples saltos. En esencia, los datos sólo se intercambian entre amigos, aunque la última fuente y el destino de una transferencia son amigos, posiblemente, sea transmitida a amigos múltiples. Una función de búsqueda de la realización de búsqueda anónima *multi-hop* es otra fuente de búsqueda de archivos en la red. Los archivos se representan por su *hash* SHA-1 y HTTP compatibles con los enlaces a archivos los cuales pueden ser exportados, copiados y pegados en la entrada/salida de RetroShare y publicar su ubicación virtual en la red RetroShare.

6.5. Anonimato

El *friend-to-friend* estructura de la red RetroShare hace que sea difícil de invadir y casi imposible de controlar, desde un punto de vista externo, el grado de anonimato todavía se puede mejorar mediante la desactivación de la tabla DHT e IP, además de los servicios de certificados de intercambio, por lo que la red RetroShare no es una verdadera *darknet*.
Amigos de los amigos no pueden conectarse directamente entre sí, sin embargo, existe la posibilidad de compartir archivos de forma anónima con amigos de

amigos, si está habilitado por el usuario. Buscar, acceder y tanto la carga como la descarga de estos archivos se realiza mediante "rutas" a través de una serie de amigos. Esto significa que la comunicación entre la fuente de datos (carga) y el destino de los datos (el programa de descarga) es hecho indirectamente a través de amigos mutuos. Aunque los amigos intermediarios no pueden determinar la fuente original o destino final, pueden ver sus enlaces próximos en la cadena de comunicación (sus amigos). Dado que el flujo de datos es encriptada, sólo la fuente original y destino final son capaces de ver lo que contienen los datos.

6.6. Interfaz de usuario

El núcleo del software RetroShare se basa en una biblioteca en línea, a la que se conectan dos ejecutables: un ejecutable de línea de comandos, que ofrece casi ningún control, y una interfaz gráfica de usuario escrita en Qt4, que es la que la mayoría de los usuarios usen. Además de las funciones muy comunes a otros programas de intercambio de archivos, tales como una ficha de búsqueda y visualización de las transferencias, RetroShare ofrece a los usuarios la posibilidad de gestionar su red mediante la recopilación de información opcional sobre amigos vecinos y visualizar como una matriz de confianza o como una red dinámica el gráfico.

7. Conclusión

Retroshare permitirá establecer una comunicación entre usuarios de forma segura a través de un canal de comunicación encriptado obteniendo como resultado una red de intercambio que puede operar con poco riesgo bajo regímenes o entornos opresivos, por ejemplo, para el intercambio de información sensible o para el intercambio de información considerados "hostiles" para un Gobierno (libros, videos, documentos, etc).
Este modelo descentralizado de RetroShare tiene ventajas importantes, como la inexistencia de una autoridad central que pueda filtrar, capturar o eliminar contenidos. Esto hace que la supervisión del gobierno a los usuarios se haga extremadamente difícil.
Además, ésta red de distribución de "amigos-a-amigos" solo permitirá el intercambio de información con personas de confianza a través de una variedad de servicios disponibles como correo electrónico, uso compartido de archivos, voz sobre IP, mensajería, etc.

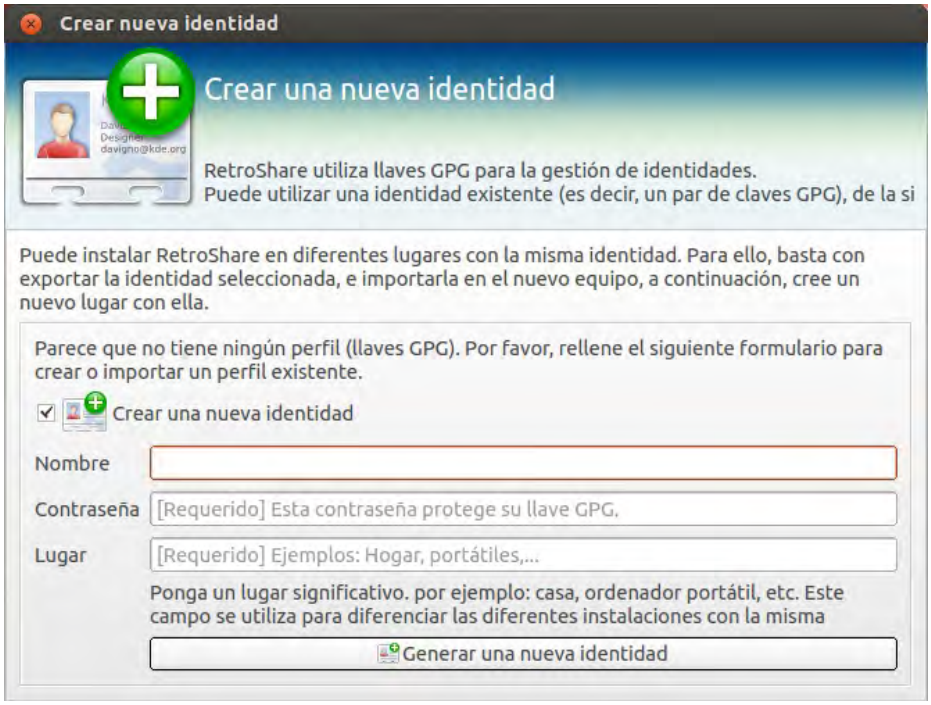
8. Anexo

8.1. Instalación

Como Retshare es un software multiplataforma, en la página oficial existen las diversas formas de la sencilla instalación en los diferentes sistemas operativos que soporta. [11]

8.2. Primeros pasos

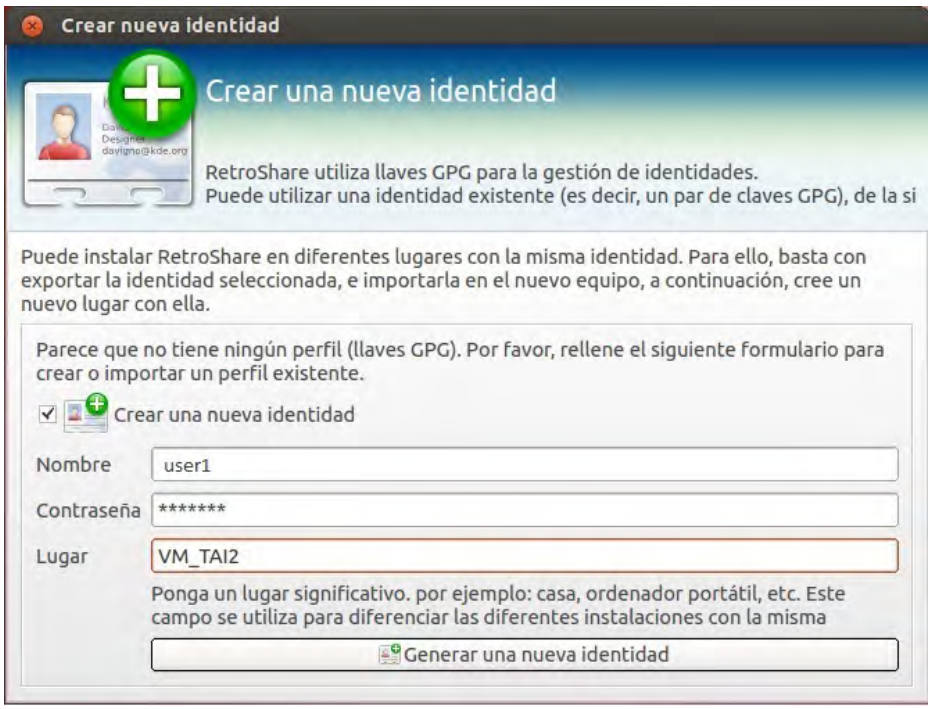
El enfoque verdaderamente importante se encuentra en la creación de nuestra **llave GPG**, la cual es imprescindible para el funcionamiento y cifrado del programa y para su posterior distribución a los "amigos".
Al finalizar la instalación, la primera ventana que aparece es la de crear una identidad para nuestra clave de cifrado. [12]



Cuadro 3. . Ventana para crear una nueva identidad.

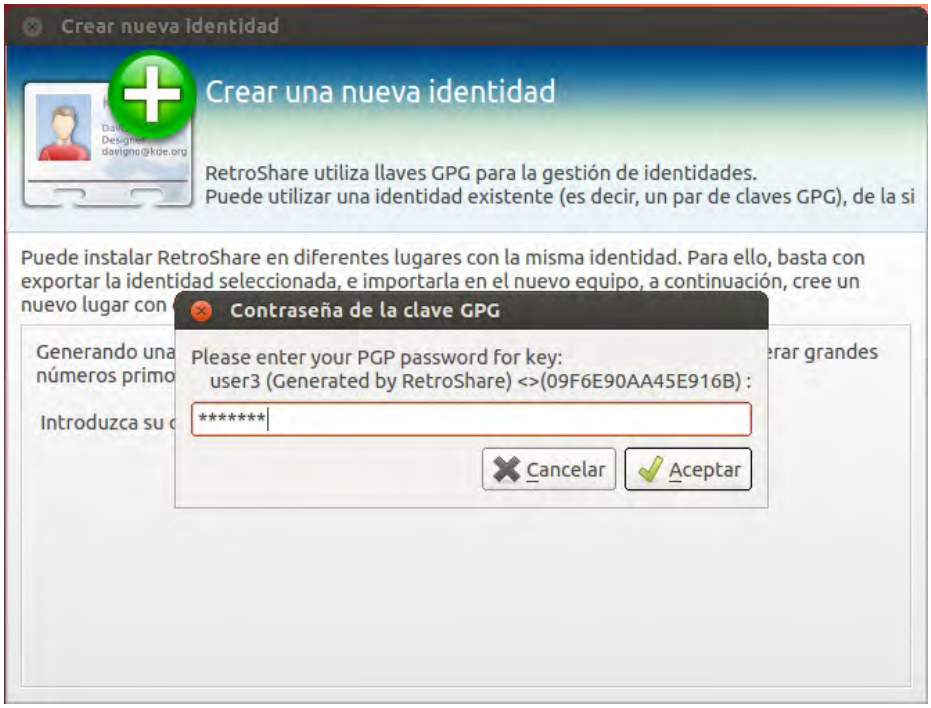
[11] http://retroshare.sourceforge.net/downloads.html

Se ingresa un nombre (en nuestro caso “user1”), una contraseña (es importante que esta sea segura) y definir el lugar de instalación (en la imagen vemos “VM_TAI2” ya que uno de los usuarios de prueba fue creado en una máquina virtual con sistema operativo Ubuntu).Esta demás decir que estos datos pueden ser inventados.
Una vez que se pulse “Generar una nueva identidad”, el programa creará nuestra llave GPG con todos los datos que se han ingresado, el cual se podrá utilizar en otras instalaciones (lugares) para luego enviarlo a los “amigos” por el medio que se prefiera.



Cuadro 4. . Ventana para crear una nueva identidad con datos cargados.

En la siguiente ventana se debe introducir la contraseña elegida para arrancar el programa, luego el programa se reiniciará, nos indicará que ha encontrado un nuevo plugin (de momento sólo el de VoIP), si se desea se pulsa “Si”, y en los siguientes inicios aparecerá la ventana de inicio normal, desde donde se podrá exportar la llave, para guardarla como medida de seguridad.

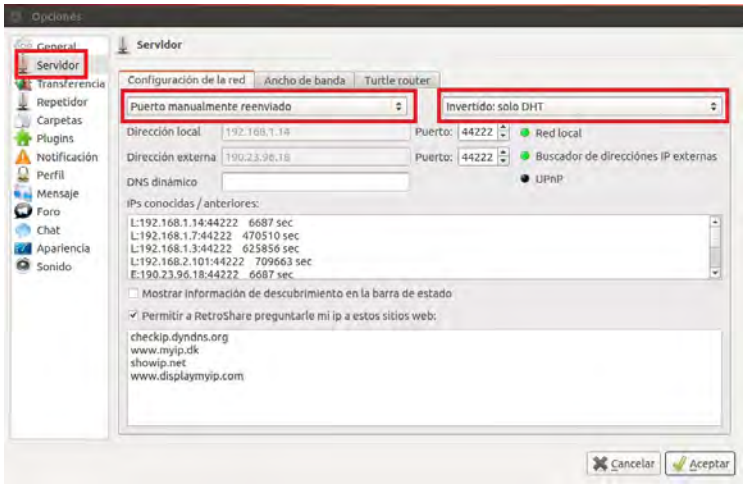


Cuadro 5. . Ventana donde se ingresa la contraseña de la clave GPG.

8.3. Configuración de la red

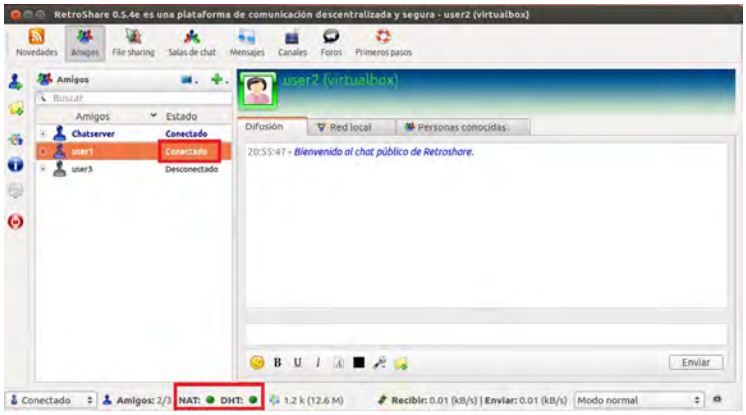
Lo primero se realiza al utilizar RetroShare es configurar el servidor para intentar mejorar la conexión con los amigos, y que los íconos de NAT y DHT estén en verde, esto dependerá de si se está detrás de un router, un *firewall*, etc. En la barra lateral se seleccion **Configuración** → **Servidor** y se selecciona:

- **Puerto manualmente reenviado**, la mejor opción, es se ha podido configurar el ordenador con una IP fija y el NAT del router para que reenvíe las peticiones desde Internet por un puerto especifico a una IP interna para TCP y UDP. Si se tiene un *firewall* por software también se tendrá que configurar dando los permisos necesarios a RetroShare.
- **Público: DHT & descubrimiento**, la mejor opción, la opción DHT, donde utiliza las tablas de hash al igual que la red BitTorrent, para encontrar a los otros nodos conectados a la red, y el "descubrimiento" es un servicio de RetroShare que intercambia los certificados y los lugares de los amigos con todos sus amigos. Esto es útil, cuando un amigo crea una nueva ubicación o tiene una dirección IP dinámica (que es normalmente el caso).
- **Invertido: solo DHT**, solo utiliza DHT. Esta última opción fue la marcada en la imagen debido a que se trataba únicamente de un usuario de prueba dentro de una red local.



Cuadro 6. . Ventana en donde se realiza la configuración de la red.

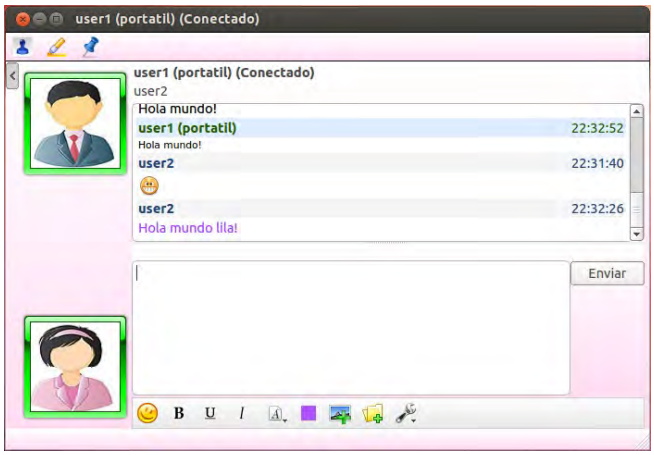
Al finalizar, se deben poner en verde los botones de los puestros NAT y DHT (esto puede tardar varios minutos).



Cuadro 7. . Ventana con el servidor configurado.

8.4. Inicio

Si nuestra configuración es correcta, los botones ya están en verde y se han añadido las llaves GPG de los amigos, podemos empezar a utilizar Retroshare con todas las funcionalidades que nos ofrece. Un dato a tener en cuenta es que únicamente al haber guardado la llave de un amigo y este haya guardado la propia, se lo podrá ver a través de Retroshare.



Cuadro 8. . Conversación en Retroshare con dos usuarios de prueba.

Retroshare nos ofrece una cantidad de funcionalidades, para un conocimiento más avanzado de la herramienta se puede utilizar la página oficial[12] o también en el tutorial de Retroshare[13]

[12] http://retroshare.sourceforge.net/index.html
[13] https://sites.google.com/site/lapaginadesenpai/articulos/retroshare

Referencias

[1] http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica. Criptografía asimétrica.

[2] http://es.wikipedia.org/wiki/Distribuci%C3%B3n_de_archivos. Distribución de archivos.

[3] http://es.wikipedia.org/wiki/Friend-to-friend. Friend-to-friend.

[4] http://es.wikipedia.org/wiki/GNU_Privacy_Guard. Gpg.

[5] http://es.wikipedia.org/wiki/OpenSSLs/ST05-007. Openssl.

[6] http://es.wikipedia.org/wiki/Peer-to-peer. Peer-to-peer.

[7] http://es.wikipedia.org/wiki/Peer-to-peer_an%C3%B3nimo. Peer-to-peer anónimo.

[8] http://es.wikipedia.org/wiki/RetroShare. Retroshare.

[9] http://es.wikipedia.org/wiki/Tabla_de_hash_distribuida. Dht.

[10] http://es.wikipedia.org/wiki/Tabla_de_hash_distribuida. Ssh.

[11] http://retroshare.sourceforge.net. Retroshare.

[12] https://sites.google.com/site/lapaginadesenpai/articulos/retroshare. Tutorial de retroshare.

[13] http://www.us-cert.gov/ncas/tips/ST05-007. Risk of file sharing technology.