PUNTO DE ENCUENTRO VIRTUAL P2P CON ACCESO MÓVIL

ANEXO I - "LA COMUNICACIÓN P2P"

RICARDO ALBERTO CAMACHO GÓMEZ

LUIS ERNESTO GARCÍA MARTÍNEZ

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE TELEMÁTICA

LÍNEA DE ÉNFASIS EN INGENIERÍA DE SISTEMAS TELEMÁTICOS

POPAYÁN

TABLA DE CONTENIDO

LISTA DE FIGURAS 3

LA COMUNICACIÓN P2P 4

1. ARQUITECTURA DE RED EN JXTA 4

1.1. ORGANIZACIÓN DE LA RED 4
1.2. ÍNDICE DISTRIBUIDO DE RECURSOS COMPARTIDOS (SRDI) 6
1.2.1. Consultas 6
1.3. FIREWALLS Y NATS 8

2. ACCESO A SERVICIOS ENTRE DISPOSITIVOS 9

2.1. LOCALIZACIÓN DE ADVERTISEMENTS 9
2.1.1. Localización de advertisements sin descubrimiento 10
2.1.2. Localización de advertisements mediante Descubrimiento directo 12
2.1.3. Localización de advertisements mediante descubrimiento indirecto. 13
2.2. DESCUBRIMIENTO DE PEERS RENDEZVOUS Y ENRUTAMIENTO DE MENSAJES 16
2.3. DESAFÍOS EN LA COMUNICACIÓN DIRECTA. 17
2.3.1. Los firewalls 17
2.3.2. Los NAT (Network Address Translation) 19
2.4. PASANDO EL LÍMITE DEL FIREWALL/NAT 22
2.5. ENRUTAMIENTO DE MENSAJES ENTRE PEERS 23

LISTA DE FIGURAS

Figura 1.1 Propagación de peticiones a través de Peers rendezvous

Figura 1.2 Distribución y consulta de entradas SRDI

Figura 1.3 Escenario de enrutamiento de mensajes a través de un firewall

Figura 2.1 Descubrimiento de peers usando advertisements almacenados en caché

Figura 2.2 Descubrimiento directo de peers

Figura 2.3 Descubrimiento indirecto a través de un peer rendezvous

Figura 2.4 Caos en la propagación del descubrimiento

Figura 2.5 Ilustración del TTL en la propagación del descubrimiento

Figura 2.6 Topología de Red usando un Firewall

Figura 2.7 Topología de Red usando un NAT

Figura 2.8 Traspasando el Firewall/NAT

Figura 2.9 Saliendo a través de un solo Firewall/NAT

Figura 2.10 Atravesando dos Firewall

ANEXO I - LA COMUNICACIÓN P2P

1. ARQUITECTURA DE RED EN JXTA

1.1. Organización de la Red

La red JXTA es una red ad hoc multisalto, compuesta por peers interconectados. Las conexiones en la red pueden ser temporales, y el enrutamiento de mensajes entre peers es no determinístico. Los peers pueden ingresar a la red o dejarla en cualquier momento, y las rutas de comunicación entre terminales pueden cambiar frecuentemente.

El papel que juega cada peer en la red JXTA no lo determina la red en sí, ya que cada peer puede funcionar de varias formas, aún simultáneamente, sin embargo en la práctica generalmente se usan cuatro clases de peer:

- **Peers con Funcionalidad Mínima (Minimal Edge Peer):** los peers pueden enviar y recibir mensajes, pero no almacenan en caché los advertisements o enrutan mensajes para otros peers. Los peers con recursos limitados (PDAs, celulares,…) constituirían esta clase de peers.
- **Peers con todas las características (Full-featured edge peers):** un peer de este tipo puede enviar y recibir mensajes, y generalmente almacena en caché los advertisements. Un peer simple responde a peticiones de descubrimiento con la información que tiene en caché, pero no reenvía ninguna petición de descubrimiento. La mayoría de los peers son de este tipo.
- **Peer de punto de encuentro (Peer rendezvous)**: un peer rendezvous es como cualquier otro peer, también mantiene una caché de advertisements, con la diferencia de que los peers rendezvous reenvían peticiones de descubrimiento para ayudar a otros peers a descubrir recursos.

  Cuando un peer se une a un peer group, este automáticamente busca un peer rendezvous. Si no encuentra ningún peer rendezvous, este dinámicamente se convierte en un peer rendezvous para ese peer group.

Cada peer rendezvous mantiene una lista de otros peers rendezvous conocidos y también de los peers que lo están usando como peer rendezvous. Cada peer groupmantiene su propio conjunto de peers rendezvous, y puede tener tantos peers rendezvous como se necesiten. Solo los peers rendezvous que sean miembros de un peer group recibirán las peticiones específicas de dicho peer group.

- **Los peers Edge (peers que constituyen un nodo cualquiera en la red):** envían peticiones de búsqueda y descubrimiento a los peers rendezvous, los cuales reenvían dichas peticiones a las cuales no saben responder a otros peers rendezvous conocidos. El proceso de descubrimiento continúa hasta que un peer tiene la respuesta o la petición expira. Los mensajes tienen un temporizador por defecto *(TTL – Time To Live) de siete saltos*. Los bucles se evitan manteniendo una lista de los peers por los que el mensaje ha pasado.
- **Peer Repetidor (Peer Relay):** un peer relay mantiene información acerca de las rutas hacia otros peers y funciona como un enrutador de mensajes entre los peers. Un peer primero mira en su caché local información acerca de las rutas que conoce. Si no encuentra la ruta hacia el destino deseado, el peer consulta al relay por información sobre dicha ruta. Los peer relay también reenvían mensajes a nombre de los peers que no pueden acceder a otros peers directamente (por ejemplo, en entornos con NATs), sirviendo así como puente entre diferentes redes físicas y/o lógicas.

Cualquier peer puede implementar los servicios de un peer relay o un peer rendezvous. Los servicios de relay y rendezvous pueden ser implementados simultáneamente en el mismo peer.

1.2. Índice Distribuido de Recursos Compartidos (SRDI)[1]

La plataforma JXTA soporta un servicio de indexado distribuido de recursos compartidos para proveer un mecanismo más eficiente de difusión de las consultas dentro de la red JXTA. Los peers rendezvous mantienen un índice de de los advertisements publicados por los peers edge asociados. Cuando un peer edge publica un nuevo advertisement, usa el servicio SRDI para poner dicho advertisement en el índice en su peer rendezvous. Con esta jerarquía, las consultas se difunden entre los peers rendezvous solamente lo cual implica una reducción significativa en la cantidad de peers involucrados en la búsqueda de un advertisement.

Cada peer rendezvous mantiene su propia lista de rendezvous conocidos en el peer group, un rendezvous puede obtener la información de punto de encuentro a partir de un conjunto predefinido de rendezvous base, en su inicio. Los rendezvous periódicamente seleccionan un número aleatorio de peers rendezvous y les envían una lista aleatoria de sus rendezvous conocidos. Los rendezvous también eliminan rendezvous que no responden. De esta manera, mantienen una red consistente de peers rendezvous. Cuando un peer publica un nuevo advertisement, el advertisement es indexado por el servicio SRDI usando claves como el nombre del advertisement o el ID. Solo los índices de los advertisements son puestos en el rendezvous por el SRDI, minimizando la cantidad de información que necesite ser almacenada en el rendezvous. El rendezvous también pone el índice en otros rendezvous (seleccionados mediante el cálculo de una función hash del índice del advertisement)

1.2.1. Consultas

Véase la configuración de ejemplo mostrada en la Figura 1.1. El peer A es un peer edge, y está configurado para usar el Peer R1 como rendezvous. Cuando el peer A hace una petición de búsqueda o descubrimiento, esta se envía inicialmente a su peer rendezvous – R1, y mediante multicast a otros peers en la misma subred.

[1] JXTA Project;"JXTA Programmer Guidev2.3"; http://www.jxta.org/docs/JxtaProgGuidev2.3.pdf

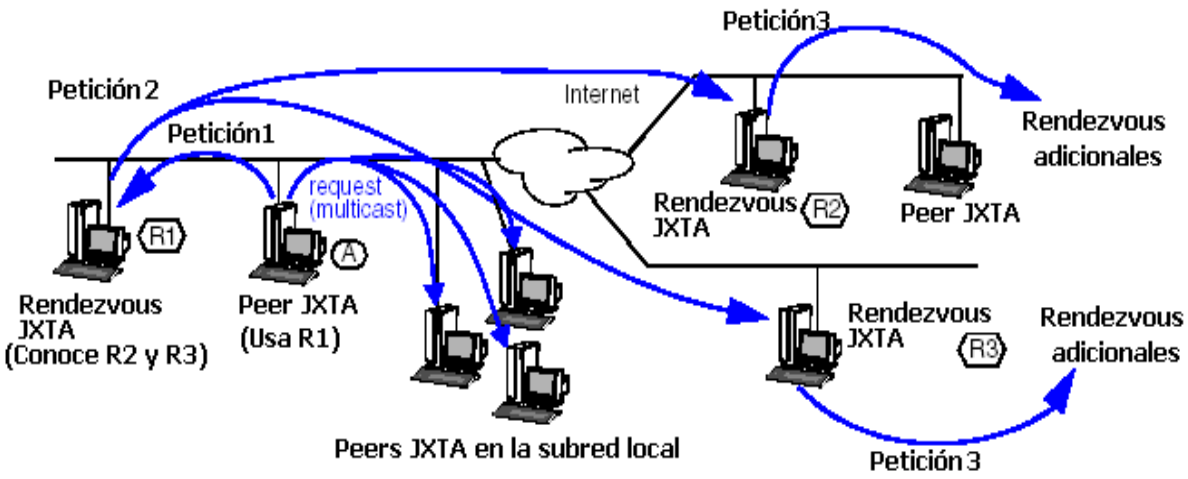

Figura 1.1 Propagación de peticiones a través de Peers rendezvous

Las consultas de los vecinos locales, dentro de la subred, se propagan hacia sus peers cercanos usando bien sea multicast o broadcast. Los peers que reciben la consulta responden directamente al peer solicitante, si contienen la información en su caché local.

Las consultas hechas más allá del entorno local son enviadas al peer rendezvous, el rendezvous intenta responder a la consulta con la información almacenada en su caché local, si contiene la información pedida, este responde directamente al peer solicitante y no sigue difundiendo la petición. Si contiene el índice para el recurso en su SRDI, se notificará al peer que publicó el recurso y ese peer responderá directamente al peer que hizo la solicitud. No hay que olvidar que el rendezvous almacena solamente el índice del advertisement, y no el advertisement en sí.

Si el peer rendezvous no contiene la información solicitada, se usa un algoritmo de búsqueda que consulta en un rango limitado de los rendezvous vecinos el índice del advertisement consultado. Un contador de saltos se usa para especificar el número máximo de veces que la solicitud puede ser reenviada. Una vez que la consulta alcanza el peer, este responde directamente a quien hizo la consulta. La Figura 1.2. muestra un bosquejo de cómo trabaja el SRDI. El peer 2 publica un nuevo advertisement, y se envía un mensaje SRDI a su rendezvous, R3. Los índices serán almacenados en R3, y pueden ser copiados en otro rendezvous en el peer group. Ahora, el Peer 1 envía una petición de consulta

para este recurso a su rendezvous, R1. El rendezvous R1 chequeará su cache local de entradas SRDI, y difundirá la consulta si no la encuentra. Cuando el recurso es localizado en el Peer2, el Peer 2 responderá directamente al Peer 1 con el advertisement solicitado.

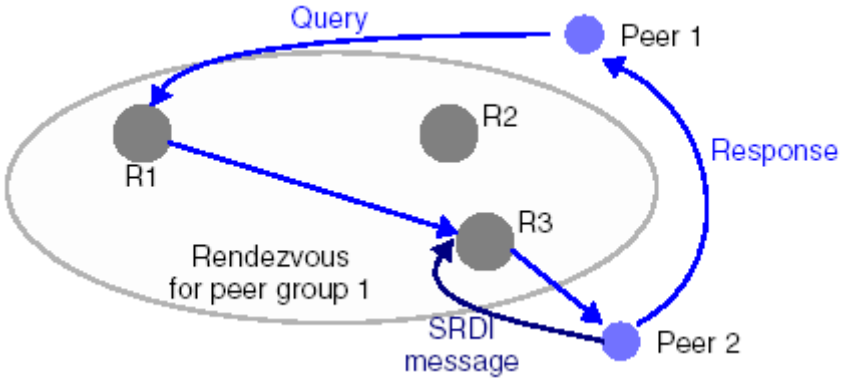

Figura 1.2 Distribución y consulta de entradas SRDI

1.3. Firewalls y NATs

Un peer detrás de un firewall puede enviar un mensaje a otro peer fuera del firewall. Pero un peer fuera del firewall no puede establecer una conexión directamente con un peer que está detrás de un firewall. Con el propósito de que los peers JXTA se comuniquen entre sí a través de un firewall, deben cumplirse las siguientes condiciones:

- Al menos un peer en el peer group dentro del firewall debe conocer la ubicación de un peer fuera del firewall.
- El peer dentro de la red protegida por el firewall y el peer fuera del firewall deben tener conocimiento mutuo y deben soportar HTTP.
- El firewall debe permitir transferencia de datos por el protocolo HTTP.

Estas transferencias HTTP a través del firewall necesitan estar habilitadas en el puerto 80, aunque ese sea el puerto utilizado por defecto por la mayor parte de los navegadores web y por la plataforma actual del proyecto JXTA.

La Figura 1.3 da un bosquejo de cómo se enruta un mensaje a través de un firewall. En este escenario, los peers JXTA A y B quieren pasar un mensaje, pero el firewall no permite que se comuniquen directamente. El peer JXTA "A" primero

hace una conexión al peer C usando un protocolo como HTTP y que pueda penetrar el firewall. El peer C entonces hace una conexión al peer B usando un protocolo tal como TCP/IP. Una conexión virtual se ha establecido entre los peers A y B.

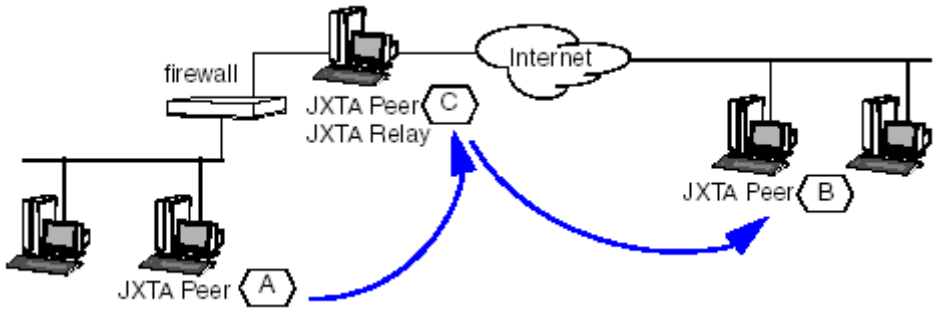

Figura 1.3 Escenario de enrutamiento de mensajes a través de un firewall

2. ACCESO A SERVICIOS ENTRE DISPOSITIVOS

El problema fundamental en las redes P2P es habilitar el intercambio de servicios entre los dispositivos, y poder lograr esto implica encontrar peers y servicios sobre la red P2P sin el conocimiento de la existencia de un peer o un servicio en la red, no hay ninguna posibilidad de que un dispositivo emplee ese servicio. También es importante hacer que los dispositivos que están en redes privadas participen en la red P2P porque muchos dispositivos estarán generalmente separados de la red por equipos de networking diseñados para prevenir o restringir conexiones directas entre dispositivos que estén al interior de diferentes redes privadas.

2.1. Localización de Advertisements

Cualquiera de los bloques básicos de construcción de una red P2P puede representarse como advertisements, lo cual simplifica considerablemente el problema de encontrar peers, peer groups, servicios, pipes, y endpoints. En lugar de preocuparse por el caso específico, de encontrar a un peer, sólo es

necesario resolver el problema general de encontrar los advertisements en la red.

Un peer puede descubrir un advertisement de tres maneras:

- Sin descubrimiento.
- Descubrimiento directo.
- Descubrimiento Indirecto.

La primera técnica implica la no conectividad en red y puede ser considerada una técnica de descubrimiento pasivo. Las otras dos técnicas involucran conectividad en red para realizar el descubrimiento y son consideradas técnicas de descubrimiento activo.

2.1.1. Localización de advertisements sin descubrimiento

La forma más fácil para que un peer descubra los advertisements es eliminando el proceso de descubrimiento por completo. En lugar de buscar los advertisements de forma activa en la red, un peer puede depender de una caché donde almacene los advertisements previamente descubiertos y así proporcionar información sobre los recursos de otros peers en la red, como se muestra en la Figura 2.1.

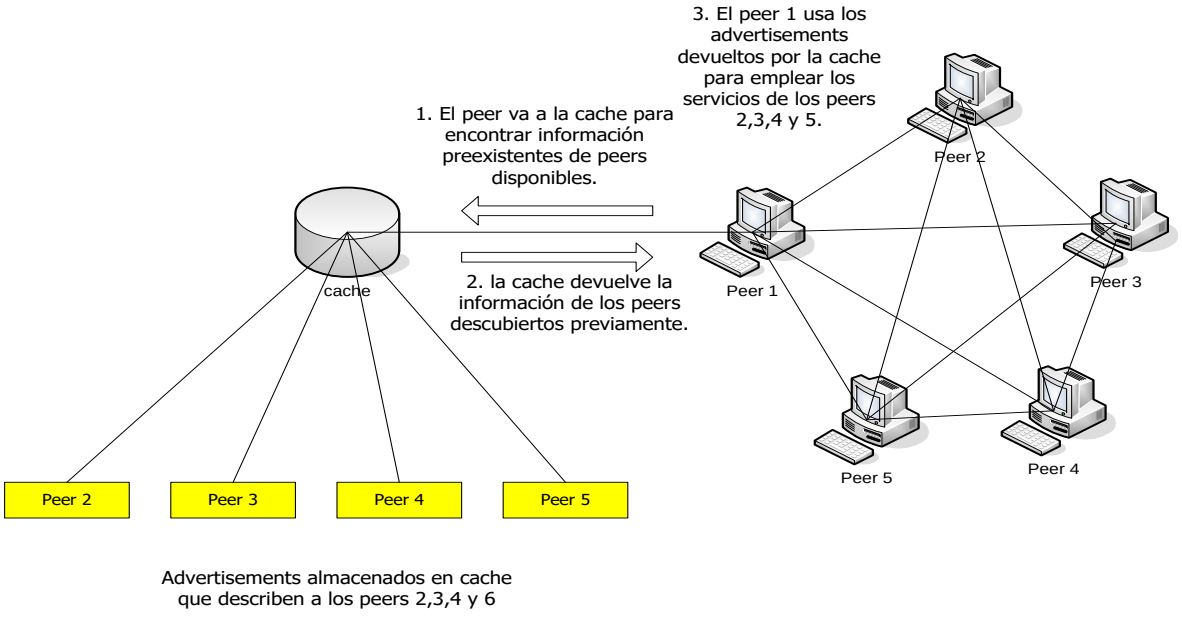

Figura 2.1 Descubrimiento de peers usando advertisements almacenados en caché

Aunque este método podría parecer trivial, puede reducir eficazmente la cantidad de tráfico generado por el peer y permitir a los peers obtener resultados casi de forma instantánea, a diferencia de los métodos de descubrimiento activo.

La caché local en este caso podría consistir en un archivo de texto que lista las direcciones IP y los puertos de los peers rendezvous descubiertos previamente, y de esta forma se proporciona un punto de arranque para activar el descubrimiento de peers. En el otro extremo, la caché podría ser una especie de base de datos que almacena cada advertisement descubierto por el peer.

Un inconveniente de usar la caché para almacenar los advertisements conocidos es el hecho de que podrían existir advertisements viejos o defectuosos describiendo recursos que ya no están disponibles en la red. Esto representa un problema en caso de que un peer intente conectarse a los recursos descritos por un advertisement de estos, ya que fallaría la conexión al servicio. Aunque la caché tiene el potencial de reducir el tráfico en la red, en este caso, los advertisements averiados en la caché incrementan el tráfico en la red. Cuando un peer intenta conectarse a un recurso en red y descubre que el recurso ya no existe o no esta disponible, el peer tendrá probablemente que acudir a un método de descubrimiento activo.

Para reducir la posibilidad de que un advertisement esté desactualizado o defectuoso, la caché puede hacer expirar los advertisements, y de este modo quitarlos de la zona de almacenamiento donde aún hay advertisements válidos.

Una técnica para hacer expirar los advertisements que usan la caché es implementar una cola tipo FIFO (First In First Out el primero en entrar a la pila, es el primero en salir de la pila), donde la pila de advertisements tiene un tamaño máximo fijo. Cuando la caché está llena, y se agrega un nuevo advertisement a la pila, éste expulsa el advertisement más viejo que fue el primero en entrar a la pila. Usar una caché para descubrir los advertisements es fácil de implementar, especialmente cuando se hace en conjunto con métodos de descubrimiento activo.

2.1.2. Localización de advertisements mediante descubrimiento directo

Los peers que están en una misma LAN podrían ser capaces de descubrir directamente a otros sin contar con la intermediación de un peer rendezvous que les ayude en el proceso de descubrimiento. El descubrimiento directo requiere que los peers tengan capacidades de broadcast o multicast, en su red de transporte, como se muestra en la Figura 2.2.

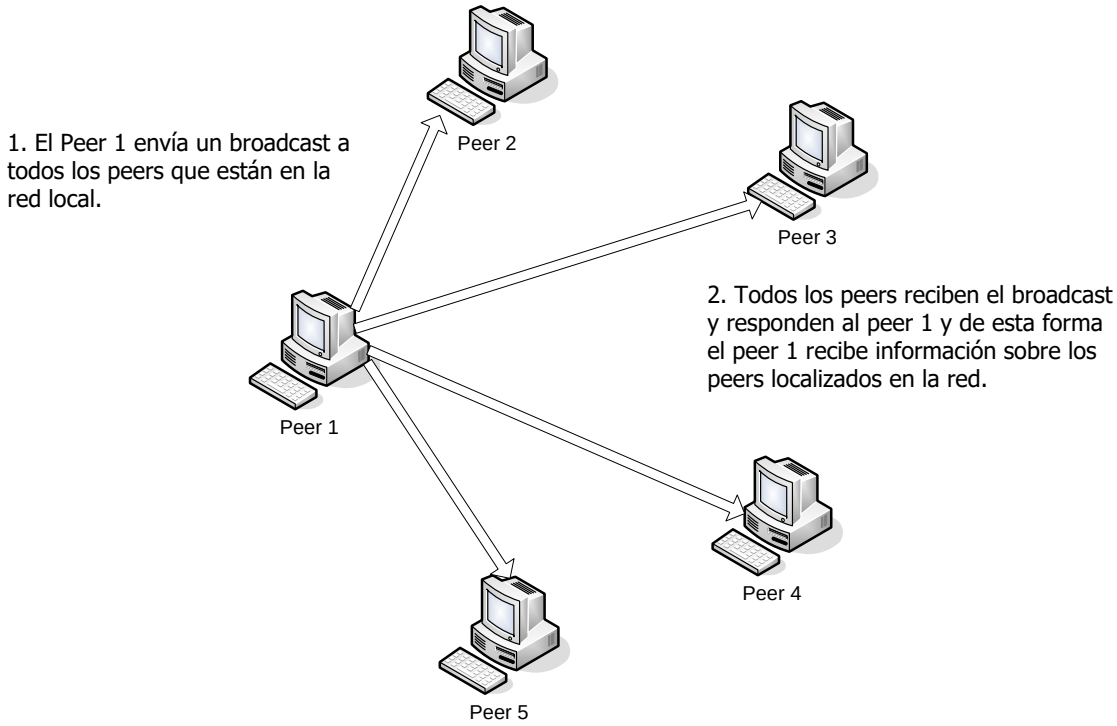

Figura 2.2 Descubrimiento directo de peers

Cuando los peers han sido descubiertos usando este mecanismo, un peer puede descubrir advertisements comunicándose directamente con los peers, sin necesidad de usar broadcast o multicast.

Desafortunadamente, esta técnica de descubrimiento esta limitada a peers localizados sobre el mismo segmento de LAN y normalmente no puede usarse para descubrir peers que estén fuera de la red local. Los peers descubiertos y los advertisements que estén fuera de la red privada requieren un descubrimiento indirecto a través de un peer rendezvous y/o un peer relay.

2.1.3. Localización de advertisements mediante descubrimiento indirecto.

El descubrimiento indirecto requiere usar un peer rendezvous que actúe como la fuente de los peers y de los advertisements conocidos, para así poder realizar el descubrimiento sobre la representación de estos peers.

Esta técnica puede ser usada por peers en una LAN local para encontrar a los peers sin usar broadcast o multicast, o por los peers que están en el interior de una red privada para encontrar peers que estén fuera de ella.

Los rendezvous peers ofrecen dos formas de localizar peers y sus advertisements:

Propagación: Un peer rendezvous pasa la petición de descubrimiento a los peers en la red que él conoce, incluyendo otros peers rendezvous que también propagarán la petición a otros peers.

Advertisements almacenados en caché: De la misma manera que un peer simple puede usar los advertisements almacenados en la caché para reducir el tráfico de la red, un peer rendezvous, puede usar los advertisements guardados en la caché para responder a las peticiones de descubrimiento de un peer.

Cuando se usan ambas formas, propagación y almacenamiento en caché, como se muestra en la Figura 2.3, se proporciona una efectiva solución para que los peers rendezvous guarden un gran número de advertisements que les sirvan a los peers simples. Como cada peer simple o peer rendezvous responde a una petición de descubrimiento, los peers rendezvous pueden guardar las peticiones para futuros usos, reduciendo el tráfico y aumentando el rendimiento de la red.

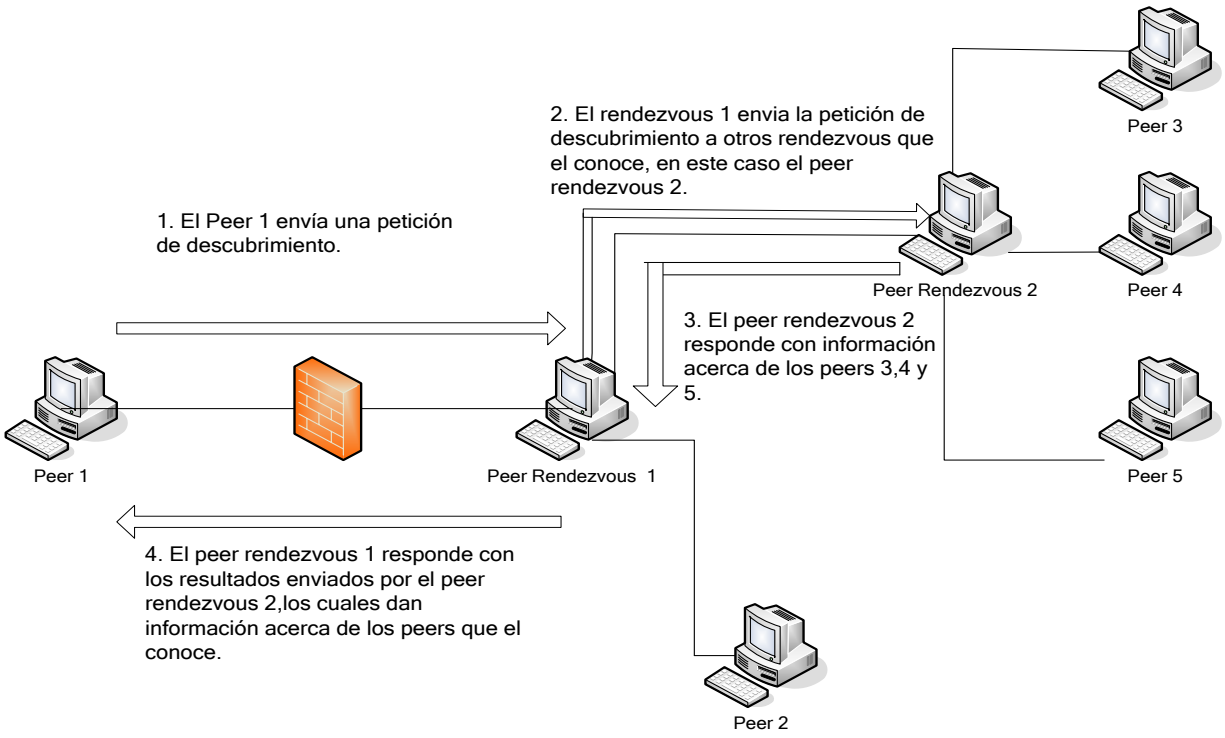

Figura 2.3 Descubrimiento indirecto a través de un peer rendezvous

Aunque el almacenamiento en caché reduce el tráfico de la red producido al descubrir recursos, o al propagar peticiones de descubrimiento de los peers rendezvous; hacer esto sin restricción puede llevar a severas congestiones de la red P2P, como se muestra en la Figura 2.4. Cuando un peer rendezvous recibe una petición de descubrimiento, remite la petición a todos los rendezvous peers que él conoce; es decir una consulta entra, y muchas consultas salen.

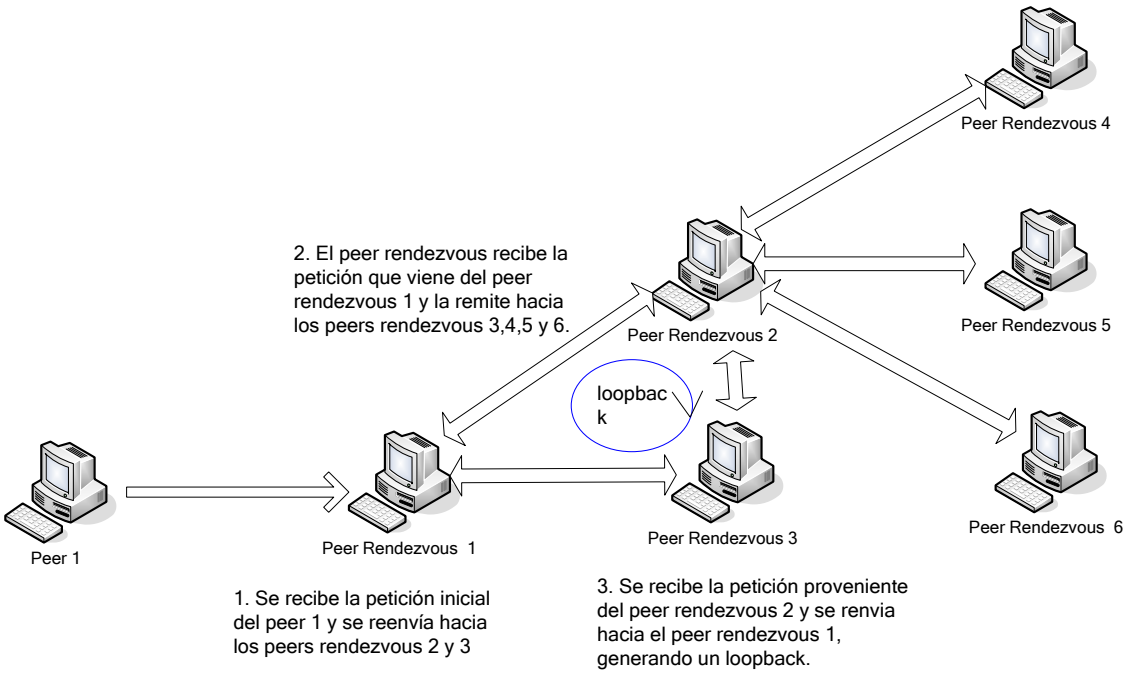

Figura 2.4 Caos en la propagación del descubrimiento

Esta retransmisión amplifica la petición de descubrimiento. Cuando la petición se propaga a otros peers rendezvous, es amplificada de nuevo, aumentando dramáticamente la carga en la red. Adicionalmente al problema de propagación desenfrenado, una ruta a una petición de descubrimiento podría aumentarlo, creando un bucle de retroalimentación o loopback en la red.

Para prevenir las propagaciones excesivas de las peticiones, los mensajes incorporan normalmente un atributo llamado Tiempo de Vida (TTL Time To Live). El TTL se expresa como el tiempo máximo en que una petición debe propagarse entre los peers de la red. Como se muestra en la Figura 2.5, cuando un peer rendezvous recibe un mensaje que contiene una petición de descubrimiento, se decrementa el TTL del mensaje en 1 y se descarta la petición si el valor del TTL resultante es 0.

Como resultado, cada mensaje tiene un radio máximo en la red por el que puede viajar. Claro que para trabajar esta técnica, todos los rendezvous peers deben decrementar adecuadamente el campo de TTL.

Para solucionar el problema del loopback, los mensajes propagados pueden incluir la información de la ruta junto con la petición. Los peers rendezvous a lo

largo del camino podrían usar la información de la ruta para evitar propagar un mensaje a un peer rendezvous que ya ha recibido el mensaje. Aunque esta técnica elimina el loopback, aún no se ha implementado y por lo tanto no evita que un peer rendezvous obtenga el mismo mensaje muchas veces.

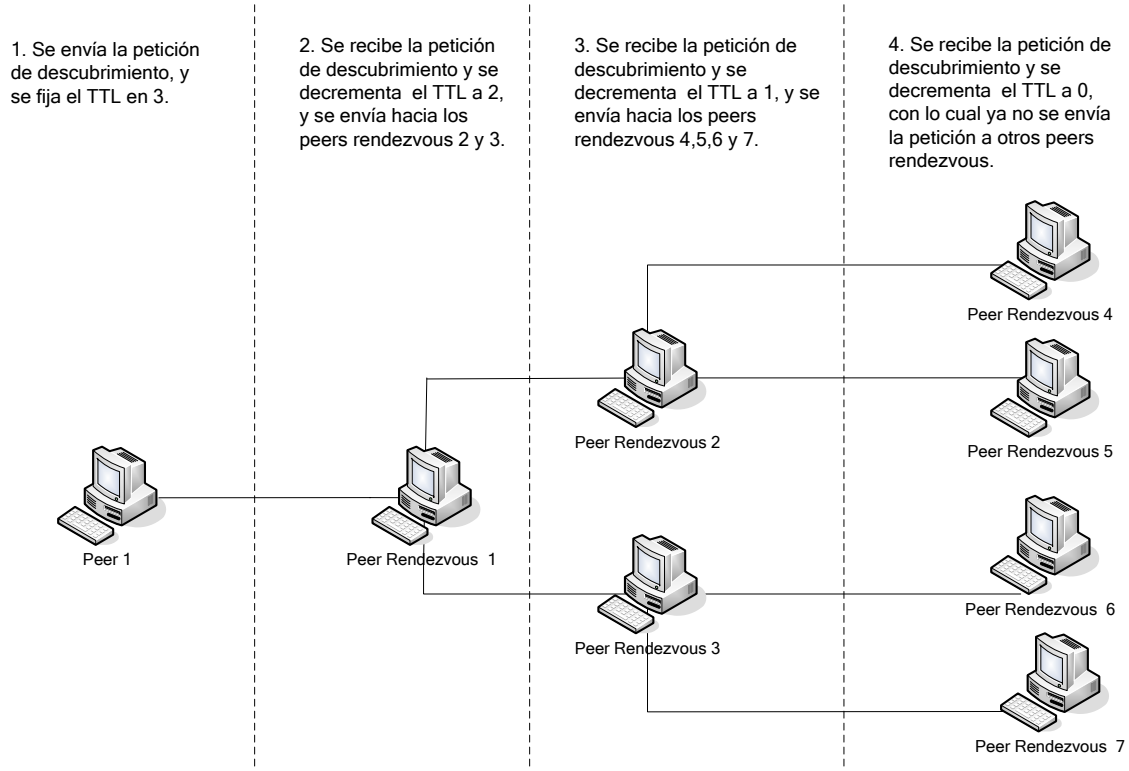

Figura 2.5 Ilustración del TTL en la propagación del descubrimiento

2.2. Descubrimiento de Peers rendezvous y Enrutamiento de Mensajes

Para la mayoría de los peers que existen al interior de una red privada, encontrar peers rendezvous y peers router es crítico a la hora de participar en la red P2P. Debido a las restricciones del firewall en la red privada, un peer al interior de una red no tiene capacidades de usar el descubrimiento directo para realizar un descubrimiento fuera del interior de la red. Sin embargo, un peer puede ser capaz de ejecutar un descubrimiento indirecto usando un rendezvous y un peer router en la red interna.

Los peers rendezvous y los peers router tienen una dirección IP estática y son usados por los peers como punto de entrada a la red P2P. Un peer localizado

detrás de un firewall puede usar los rendezvous estáticos como punto de partida para descubrir a otros peers y sus servicios, y puede conectarse a otros peers usando los peers router estáticos para atravesar el firewall.

2.3. Desafíos en la Comunicación Directa.

El uso de firewalls y NATs en las redes privadas presentan un serio obstáculo para el networking P2P. Los NAT y los firewalls normalmente se usan en conjunto para asegurar una red corporativa ante ataques tanto desde la red interna como desde Internet por parte de crackers u otras amenazas para una red de datos, manteniendo un entorno privado y seguro, véase a continuación lo que implicaría cada uno de estos elementos en el networking P2P.

2.3.1. Los firewalls

Los firewalls son usados para proteger las redes corporativas de conexiones de red no autorizadas ya sea desde el exterior de la red o desde el interior de la misma. Como se muestra en la Figura 2.6, los firewalls usan filtros IP para regular cuáles son los protocolos que se pueden usar para conectarse desde el exterior del firewall al interior de la red y viceversa. Un firewall también puede regular los puertos usados por los clientes externos para iniciar las conexiones que salen desde la red privada.

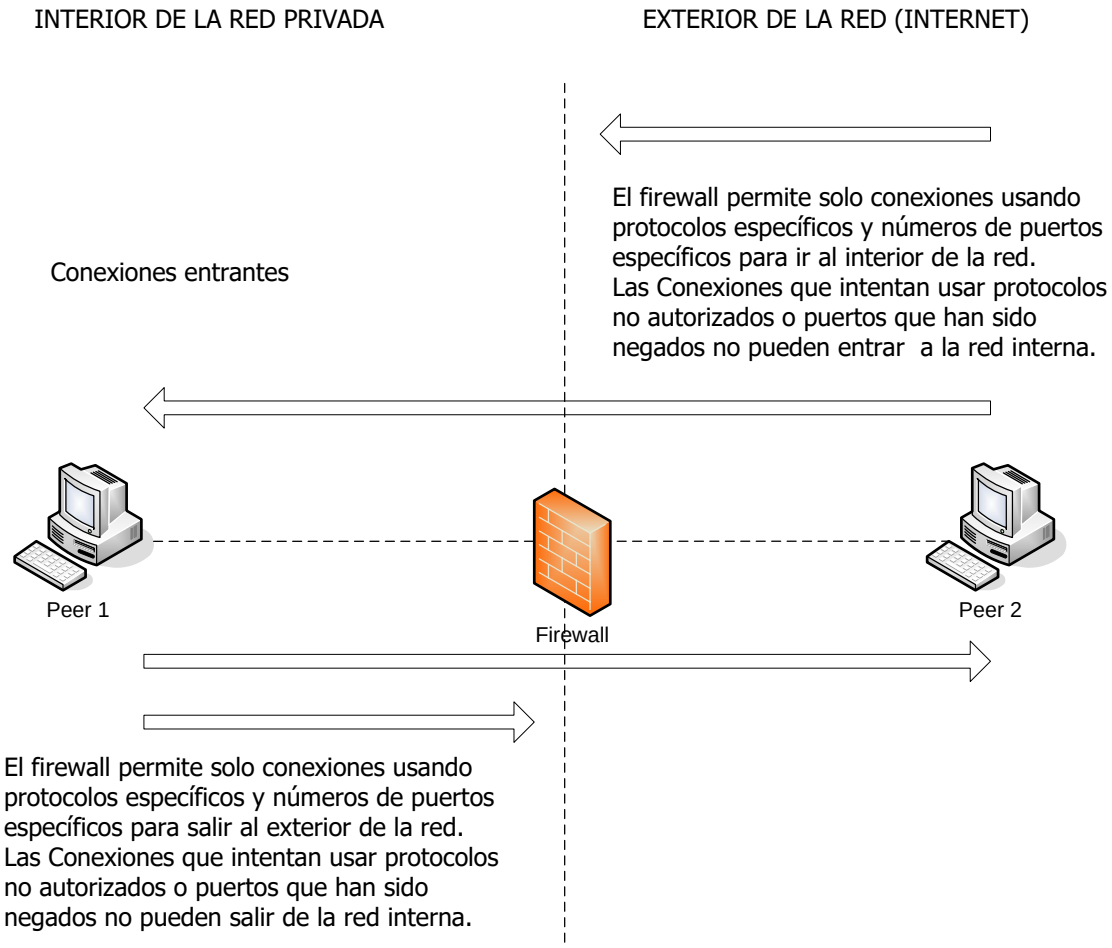

Figura 2.6 Topología de Red usando un Firewall

Debido a que un firewall puede bloquear las conexiones entrantes, un peer que este fuera del firewall, muy probablemente no estaría en capacidad de conectarse directamente a un peer detrás del firewall. Un peer al interior de la red podría también restringirse a usar sólo ciertos protocolos (como HTTP) para conectarse a sitios fuera del firewall, limitando aun más la comunicación P2P.

2.3.2. Los NAT (Network Address Translation)

NAT es una técnica usada para asignar direcciones IP al interior de una red usando un conjunto de direcciones IP oficiales y de esta forma conectarse a la red pública. NAT opera dos formas:

- **NAT estático:** En el NAT estático, la relación de adaptación entre direcciones IP internas y externas es uno-a-uno. Cada dirección IP al interior es adaptada a una y sólo una dirección IP externa.
- **NAT Dinámico**: En el NAT dinámico se adapta el conjunto de direcciones IP internas a un muy pequeño conjunto de direcciones IP externas.

Una red privada que emplee NAT asigna direcciones IP internas entre los rangos definidos para las direcciones IP en redes privadas:

- Clase A: **10.0.0.0** a **10.255.255.255**
- Clase B: **172.16.0.0** a **172.31.255.255**
- Clase C: **192.168.0.0** a **192.168.255.255**

Una máquina que use una dirección IP dentro de este rango es probable que esté detrás de un equipo NAT.

NAT se usa por muchas razones, la razón más popular es que elimina la necesidad de una dirección IP única global para cada estación de trabajo dentro de una corporación, y reduce de esta forma el costo de una red corporativa. NAT también permite a los administradores del sistema proteger la red proporcionando sólo un punto de entrada a la red interna. NAT logra esto permitiendo sólo conexiones entrantes con máquinas internas que originen la conexión a la red externa. En lugar de intentar proteger cada máquina usando un firewall para filtrar las conexiones entrantes, un administrador del sistema, pueda usar NAT para asegurar que las únicas conexiones permitidas detrás de la red sean solo aquellas que se originaron al interior de ella.

NAT normalmente es implementado por un router o por un firewall que actúa como gateway en Internet para la red interna privada. Para dirigir un paquete

desde una dirección IP interna a una dirección IP externa, el router hace lo siguiente:

1. Almacena la dirección IP de origen y el número del puerto del paquete en la tabla de translación del router.
2. Reemplaza la dirección IP de origen del paquete con una de las direcciones IP públicas que el router maneja, guardando la asignación de direcciones en el proceso de la tabla de translación.
3. Reemplaza el número del puerto de origen con un nuevo número de puerto y guarda esta asignación en la tabla de translación.

Después de que cada paso se ha realizado, el paquete se pasa a la red externa. Los paquetes de datos que llegan a una de las direcciones IP públicas externas del router pasan por un proceso de asignación inverso que usa la tabla de translación del router para asignar el número del puerto y la dirección IP externa a una dirección interna y a un número de puerto. Si la entrada no corresponde a una dirección IP pública dada y el número del puerto se encuentra en la tabla de translaciones, el router bloquea los datos desde la entrada a la red privada. El flujo de datos a través del router NAT se ilustra en la Figura 2.7.

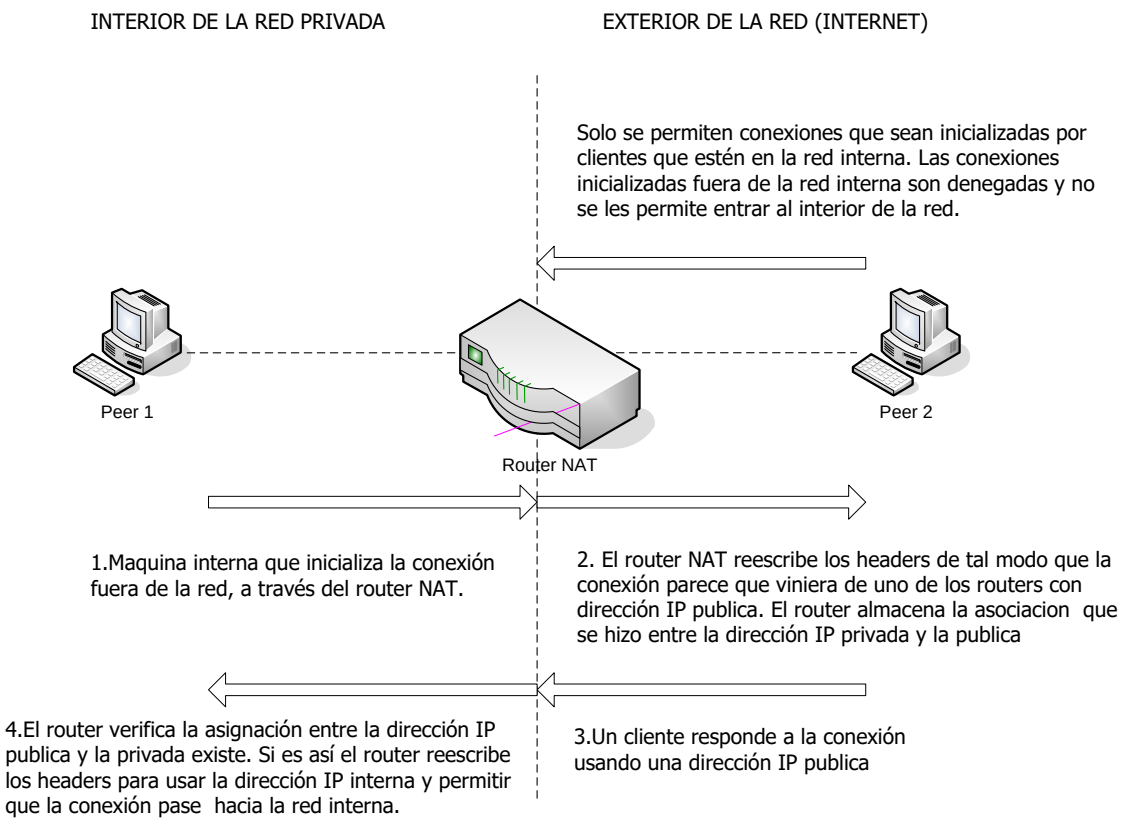

Figura 2.7 Topología de Red usando un NAT

El NAT protege las redes permitiendo sólo conexiones a la red interna que son originadas dentro de la misma. Una máquina fuera de la red no puede conectarse a una máquina en la red interna a menos que la máquina del interior haya comenzado la conexión con la máquina externa. Como resultado, un peer externo en una red P2P no tiene ningún mecanismo para conectarse espontáneamente a un peer localizado detrás de una gateway NAT. Desde el punto de vista de un peer externo, el peer no existe porque no hay ninguna asignación entre las direcciones IP exteriores e interiores y los números de puertos existentes en la tabla de translación del router.

2.4. Pasando el límite del Firewall/NAT

El uso combinado de NAT y firewall da como resultado un conjunto de circunstancias especiales en la comunicación entre peers: Los peers no pueden conectarse a las máquinas que estén detrás de un NAT a menos que la comunicación sea iniciada por un peer que esté en el interior, y las conexiones pueden bloquearse en el firewall dependiendo del protocolo de conexión o de la dirección IP y número de puerto de destino.

La única herramienta que un peer tiene para solucionar este problema es su capacidad de crear conexiones de red salientes a los hosts que estén fuera de la gateway Firewall/NAT. Los peers pueden usar los protocolos permitidos por el firewall para crear una conexión de túnel a través del firewall hacia la red externa. Inicializando la conexión dentro de la red interna, se fija la asignación necesaria en la tabla de translación del router NAT, permitiendo que una máquina externa pueda enviar datos a la red interior. Sin embargo, si un firewall se configura para negar todas las conexiones salientes, la comunicación entre peers es imposible.

En la mayoría de las redes corporativas, HTTP es probablemente el protocolo más habilitado por un firewall para conexiones salientes. Desafortunadamente, HTTP es un protocolo de petición-respuesta: Cada conexión HTTP envía una petición y después espera una respuesta. La conexión permanece abierta después de la petición inicial para recibir la respuesta. Aunque HTTP proporciona a un peer un mecanismo para enviar peticiones desde la red interna, no proporciona la capacidad para que los peers externos de forma natural crucen el limite del firewall para conectarse a los peers que están al interior de una red.

Para solucionar este problema, un peer dentro de un firewall usa un peer router que esté localizado fuera del firewall o que sea visible desde el exterior de este para poder cruzarlo, como se muestra en la Figura 2.8, los Peers que intentan conectarse con un peer que esté detrás de un firewall se conectan primero a un peer router, y el peer que esta al interior del firewall debe conectarse periódicamente a este peer router para que cualquier mensaje entrante se envíe a este en una respuesta HTTP.

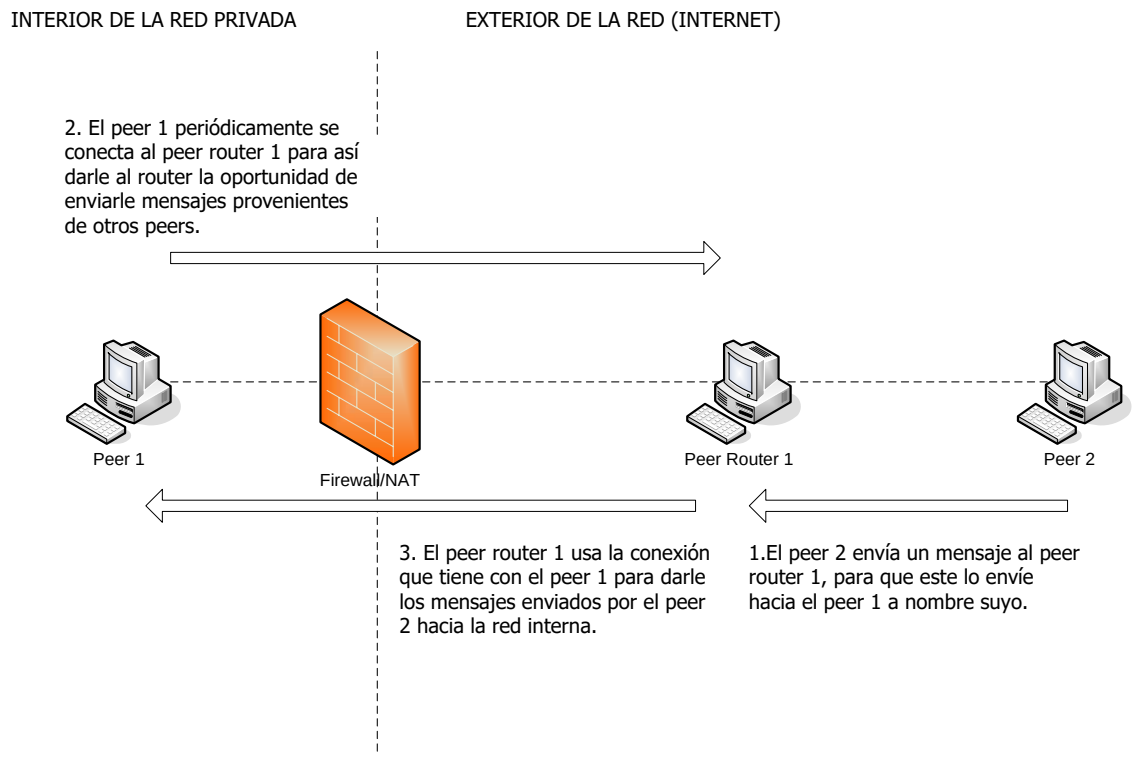

Figura 2.8 Traspasando el Firewall/NAT

Esta técnica puede usarse con cualquier protocolo permitido por el firewall y entendido por el peer router. El peer router efectivamente traduce entre la red de transporte usada para la comunicación P2P y el transporte usado para hacer el túnel a través del firewall.

2.5. Enrutamiento de Mensajes entre Peers

En los casos en los que el firewall o el NAT se localicen entre dos peers, un peer router debe ser usado para una conexión Proxy entre la red pública y el peer localizado dentro del firewall. En un caso sencillo, como por ejemplo cuando hay solo un firewall que separa los peers de origen y destino, tan solo es requerido un único peer router. En casos más complejos, un firewall o NAT pueden proteger cada uno de los peers y requerir el uso de múltiples peers router para cruzar el límite de cada firewall/NAT.

Saliendo a través de un solo firewall/NAT

La Figura 2.9 ilustra el proceso de envío de mensajes fuera de un firewall/NAT.

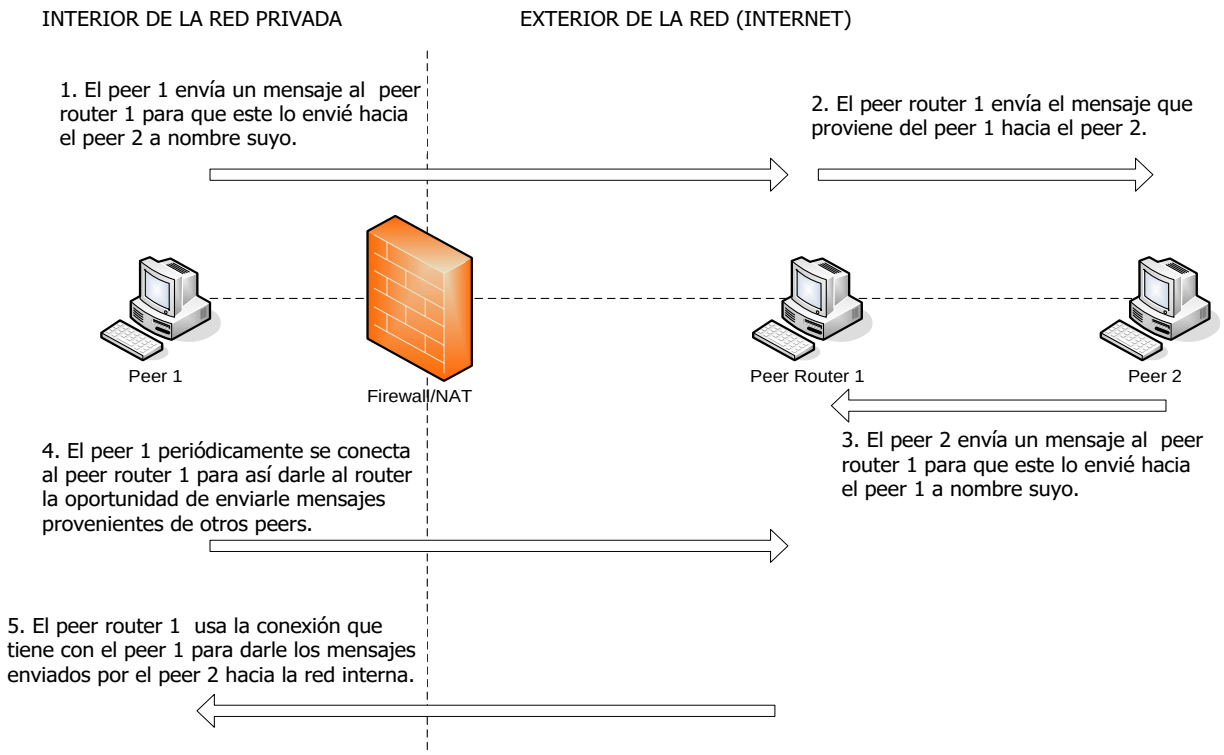

Figura 2.9 Saliendo a través de un solo Firewall/NAT

Para permitir que un peer localizado al interior de un Firewall/NAT envíe un mensaje a un peer localizado en la red pública, se deben seguir estos tres pasos:

1. El peer al interior del firewall/NAT se conecta al peer router usando un protocolo capaz de pasar el firewall, como HTTP, y le pide al peer router enviar un mensaje al peer de destino.
2. El router acepta la conexión del peer que esta al interior del firewall e inicia una conexión con destino solicitado en representación del peer de origen. Esta conexión usa cualquier red de transporte que tengan en común el peer router y el peer de destino.
3. El mensaje se envía desde el origen al peer de destino a través del peer router, el cual actúa como un Proxy para el peer de origen.

Después de que el mensaje del peer de origen se ha enviado al peer de destino, la conexión se cierra. Otros mensajes pueden ser enviados repitiendo el procedimiento, pero el mensaje podría usar un peer router diferente y por consiguiente podría seguir una ruta diferente hacia el peer de destino.

Para permitir a un peer público enviar un mensaje a un peer localizado al interior de un firewall/NAT, el peer de origen debe tener conocimiento de la información de ruta descrita por el peer router el cual está en capacidad de enrutar el mensaje al peer de destino. La información de ruta podría ser obtenida previamente durante el descubrimiento o puede obtenerse mediante una petición de descubrimiento adicional a la red P2P. Cuando el peer de origen obtiene la información de la ruta debe enviar el mensaje, lo cual involucra tres pasos:

1. El peer de origen abre una conexión al peer router, preguntándole si envía el mensaje al peer de destino.
2. El peer router espera hasta que el peer de destino se conecte a él usando un protocolo que sea capaz de cruzar el firewall, como HTTP.
3. El peer de destino se conecta periódicamente al peer router, en cuyo instante el mensaje se envía al peer de destino.

De nuevo, cuando el mensaje llega al peer de destino, la conexión entre el peer router y los otros dos peers es cerrada. Para enviar otro mensaje desde el peer de origen se debe repetir el procedimiento y posiblemente se usará un peer router diferente para dar conectividad con el peer destino.

Atravesando un Firewall/NAT doble

La mayoría de los peers simples están localizados al margen de Internet y son probablemente protegidos por un firewall/NAT, es por esto que cualquier mensaje enviado desde un peer de origen a un peer de destino probablemente necesite pasar por dos firewall/NAT. El procedimiento para cruzar dos firewalls es similar al de cruzar uno solo y básicamente combina ambos casos, el entrante y el saliente de cada escenario de cruzar el firewall. La Figura 2.10 ilustra cómo pasar un firewall/NAT doble.

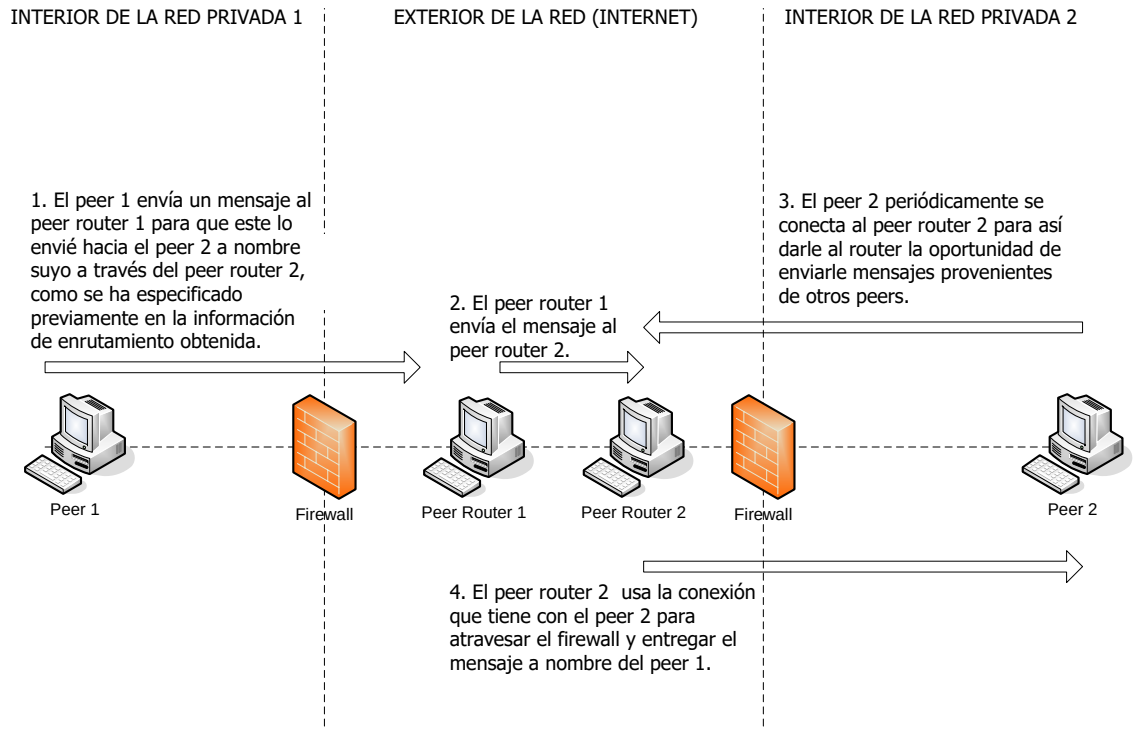

Figura 2.10 Atravesando dos Firewall

Antes de que un peer de origen pueda enviar el mensaje, necesita localizar la información de enrutamiento, la cual describen los peers router que llevarán el mensaje hasta el destinatario. En este caso, más de un peer router será involucrado; un peer router es necesario para permitirle al peer de origen atravesar su firewall, y otro para cruzar el firewall que proporciona acceso al destinatario. Cuando el peer origen tiene esta información de enrutamiento, el envío de un mensaje involucra cuatro pasos:

1. El peer de origen abre una conexión con el peer router de origen, invitándolo a enviar el mensaje al peer de destino por medio de una ruta proporcionada por el peer router destino.
2. El peer router de origen abre una conexión con el peer router de destino. Esta conexión usa una red de transporte que sea común para ambos peers.

3. El peer router destino espera hasta que el peer destino se conecte a él usando un protocolo que sea capaz de traspasar el firewall, como HTTP.
4. El peer destino se conecta periódicamente al peer router, y el mensaje es enviado finalmente al peer destino.

Traspasar dos firewalls involucra a un sólo peer router si ambos, el origen y el destino, tienen un peer router en común; sin embargo, pasar los límites del firewall no es la única razón para usar un peer router. Múltiples peers router pueden ser usados por un peer para navegar alrededor de los cuellos de botella de la red y lograr un mejor desempeño, o para lograr traducción de protocolos entre dos redes incompatibles. Cuando el peer se conecta al peer router de origen, este le proporciona una lista ordenada de otros peers router que pueden usarse para enviar mensajes a nombre del mismo.