**Title**: SEAMLESS HOST MIGRATION BASED ON NAT TYPE

**Abstract**: Systems and methods of the present invention for maintaining network data distribution are provided. Network data may be distributed in such a manner as to allow a network session to weather interrupted communications between host and clients without significant loss of data. Embodiments of the present invention provide for one or more clients to serve as backup host(s) for the network session, such determinations including the use of NAT profile information. When the other clients transmit data to the host, they may also transmit the data to one or more backup hosts if there are any indications of interrupted communication.
Field of the Invention

[0001] The present invention relates generally to networks. More specifically, the present invention relates to data distribution in networks and the use of Network Address Translation (NAT).

Description of Related Art

[0002] A network may include a group of computing devices connected together by a communications system. A computer in the network may communicate, exchange data, and share resources with the other computers in the network. Examples of networks include a personal area network (PAN), local area network (LAN), and wide area network (WAN).

[0003] Various network configurations are known in the art. The traditional client-server network illustrated in FIGURE IA includes a host 110 connected to clients 120A-D. The host 110 establishes the network session 130, controls which and how many clients may join the network session 130 and how the clients 120A-D interact with each other once they have joined network session 130. Because the host 110 generally has large amounts of bandwidth and processing power, the host 110 is may be capable of managing and distributing data to and from all the clients 120A-D in the network session 130. In such a configuration, data from a particular client (e.g., client 120D) may be distributed to other clients (e.g., clients 120A-C) through the host 110. For example, client 120D may transmit data to the host 110. When another client, such as client 120A, requests that data, the host 110 transmits that data to client 120A.

[0004] By virtue of being connected to the host, a client may request only the data that the client needs (via the host) so that the client does not have to manage otherwise unneeded data. Such an arrangement may be common amongst clients that do not have the ability to effectively manage all the data exchanged within a network session. These clients may require a host to manage and distribute the data.
A disadvantage of having the host manage and distribute data in a network session is that data can be lost when there are connectivity issues affecting communications between the host and any one of the session clients. In such an instance, the data from a particular client cannot be transmitted to the host. That data would also be unavailable to the other clients in the network. For example, client 120D may suddenly become disconnected from the host 110. Information that client 120D would have sent to the host 110 never reaches the host 110 and, as a consequence, the information cannot be transmitted to the rest of the network (i.e., clients 120A-C). The missing information may cause a disruption to the network session 130, possibly affecting the operations of the other clients. This may be especially true in the context of interactive network game play.

A further problem may arise with respect to network address translation (NAT) when trying to establish communication amongst clients through peer-to-peer communication (P2P). P2P communication generally refers to direct communication between client devices connected to a network. Examples of P2P applications include, but are not limited to, voice over Internet protocol (VoIP), bit torrent transmission, video transmission, file sharing, data sharing, and other types of direct data transfer between clients that does not exceed the bandwidth capabilities of an individual client.

Utilizing the NAT protocol, multiple nodes or computing devices may share a single Internet or local network Internet Protocol (IP) address. In one example, a local area network may use a public, global address for external network traffic and a (or set of) private IP address(es) for internal network traffic. Most clients in a network are connected to a central server, which is situated behind a NAT firewall (hereinafter referred to as a NAT). Four types of NAT are generally known in the art: full cone, restricted cone, port restricted, and symmetric.

A full cone NAT takes all requests from the same internal IP address and port and maps them to the same external IP address and port. Any external host can send a packet to the internal host by sending a packet to the mapped external address. In a restricted cone NAT, all requests from the same internal IP address and port are likewise mapped to the same external IP address and port. Unlike a full cone NAT,
however, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

[0009] A port restricted NAT is like a restricted cone NAT but the restriction includes port numbers. Specifically, an external host can send a packet with source IP address X and source port P to the internal host only if the internal host had previously sent a packet from IP address X and port P. In the final example—a symmetric NAT—all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a user data protocol (UDP) packet back to the internal host.

[0010] There is, therefore, a need in the art for improved systems and methods for network data distribution that addresses problems related to network session connectivity and maintaining an uninterrupted exchange of data in the session. In this context, it is desirable for a host in a P2P network to have a favorable NAT profile in order to create an optimal P2P network. There is, therefore, a further need in the art for determining a host with a favorable NAT profile amongst several clients connected to a central server.
Systems and methods of the present invention provide for maintaining network data distribution that would allow a network session to weather interrupted communication between a host and clients without any loss of data. Host functions migrate to a client seamlessly and without significant loss of data. Embodiments of the present invention provide for one or more clients to serve as a backup host for the network session. When the other clients transmit data to the host, they may also transmit the data to one or more backup hosts. For example, a client that sends data to the host may not receive acknowledgement of the data within a certain period of time. That client may re-transmit the data to the host, as well as transmit the data to the backup host. Determining a backup host may be based on (NAT) profile information shared between the host and clients upon establishment of the connections between the host and the plurality of clients.

Various embodiments of the present invention include methods for network data distribution. Such methods include connecting a host to clients, determining whether a client is capable of serving as a backup host, and if so, transmitting to that client certain information that would allow the client serve as the backup host. This determination may utilize NAT profile information. Serving as the backup hosts includes receiving information from other clients when those other clients cannot communicate with the host. In some embodiments of the present invention, the method further provides for indicating that communications between a host and a client are interrupted and for terminating the connection between the host and the particular client.

Various embodiments of the present invention include systems for network data distribution. Such systems may include a host, a first client capable of serving as a backup host, and a second client capable of transmitting data to the first client when communications between the host and the second client is interrupted. In some embodiments of the present invention, the second client may also serve as a backup host. Some embodiments of the present invention may include a plurality of
clients, each configured to serve as backup hosts. NAT profile information may be utilized in determinations as to backup host viability.

[0014] A host system for use in network distribution systems may also be provided by embodiments of the present invention. Such host systems may include an acknowledgement module to acknowledge client communications upon receipt, a negotiation module to negotiate whether a particular client is capable of serving as a backup host, and a backup application module to deliver to the client an application providing host information. Some embodiments of the present invention further include a host information database and a timer. NAT profile information may be collected, analyzed, and utilized in determining backup host viability.

[0015] Some embodiments of the present invention include computer storage media and instructions for network data distribution. Such instructions may provide for connecting a host to clients, negotiating with a client capable of serving as a backup host through the use of NAT profile information, and transmitting host information to the client so that it may begin serving as a backup host.
BRIEF DESCRIPTION OF THE FIGURES

[0016] FIGURE IA illustrates a client-server network configuration as it is known in the art.

[0017] FIGURE IB illustrates an exemplary system for network data distribution with one backup host.

[0018] FIGURE IC illustrates an exemplary system for network data distribution with several backup hosts.

[0019] FIGURE ID illustrates an exemplary system for network data distribution utilizing a NAT.

[0020] FIGURE 2 illustrates an exemplary configuration for a computing device offering seamless host migration in a network data distribution system.

[0021] FIGURE 3A illustrates an implementation of an exemplary system for network data distribution, which may include a network address translator.

[0022] FIGURE 3B illustrates an alternate implementation of an exemplary system for network data distribution, which may include a network address translator.

[0023] FIGURE 4 depicts an exemplary method for network data distribution, which may include the use of NAT profile information.
DETAILED DESCRIPTION

[0024] The present invention includes systems and methods for network data distribution. Embodiments of the present invention may allow host migration to occur seamlessly. A network session may continue without significant loss of data in the event of interrupted communication between a host and a client. A host of a network session may be connected to a number of clients. One (or more) of these clients may be capable of serving as a backup host. Backup viability is negotiated with a client and host information is transmitted to the client, which may then act as a backup host. The backup host may then connect to and receive data from the other clients in the network session. Thereafter, if communication between the host and a particular client is interrupted, that particular client may transmit its data to the backup host allowing the network session to continue without any loss of data.

[0025] The elements identified throughout are exemplary and may include various alternatives, equivalents, or derivations thereof. Various combinations of hardware, software, and computer-executable instructions may be utilized. Program modules and engines may include routines, programs, objects, components, and data structures that effectuate the performance of particular tasks when executed by a processor, which may be general purpose or application specific. Computer-executable instructions and associated data structures stored in a computer-readable medium represent examples of programming means for executing the steps of the methods and/or implementing particular system configurations disclosed herein.

[0026] In the client-server network configuration illustrated in FIGURE 1A and as discussed in detail above, each client does not have to process all the data in a network session. Instead, each client receives and processes only the data that is necessary for the client to participate in the network session. Some clients are not capable of managing all the data efficiently due to, for example, lack of bandwidth or lack of processing power. Some clients, however, do have the ability to manage all the data in a network session. These particular clients may act as backup hosts, storing some or all of the data from the network session.
In contrast to the system configuration of FIGURE IA, FIGURE 1B illustrates an exemplary system for network data distribution with one backup host, client 160A. A backup host may be any client capable of performing some or all of the functions of a host of a network session. When the host 140 of the network session 150 cannot or does not perform, some or all of the hosting responsibilities may migrate to a backup host. To qualify as a backup host requires the candidate host (client) to exhibit backup viability. Exhibiting backup viability may involve meeting one or more requirements concerning, for example, bandwidth, processing power, memory, hardware or software configurations, or quality of service. A client's backup viability may be determined through negotiation with the host.

After completing negotiations concerning and confirming backup viability, host information may be transmitted between host 140 and client 160A through network session 150. The host information may include the network name, the internet protocol (IP) addresses of the clients in the network, firewall information, and information concerning specific responsibilities should client 160A need to take over certain host responsibilities. Using the host information, client 160A may be able to act as a backup host in the event that one or more connections between the host 140 and the other clients 160B-D become interrupted. For example, if client 160B becomes disconnected from host 140, client 160B may transfer data to client 160A as will be illustrated in the context of FIGURE 3A and FIGURE 3B. By migrating host responsibilities from host 140 to client 160A, information from client 160B is not completely lost to the network session 150.

In some embodiments, more than one client may be capable of serving as backup hosts. FIGURE 1C illustrates an exemplary system for network data distribution with several backup hosts — clients 190A-D. Each client in the network session 180 of FIGURE 1C may be responsible for particular backup host responsibilities should original host 170 become unavailable. For example, client 190A may be responsible for scorekeeping while client 190B may be responsible for state changes in the game environment. Client 190C may be responsible for admissions criteria (e.g., who may participate in the game) whereas client 190D may be responsible for chat functionality.
Alternatively, client 190A may be responsible for all of the aforementioned tasks and clients 190B-D take over those tasks should client 190A subsequently fail.

FIGURE ID illustrates an exemplary system for network data distribution utilizing a NAT. Client devices 195A, 195B, 197, and 195D on the network are initially connected to server 191 in an external network 199. Server 191 may monitor data for game play between clients 195A, 195B, 197, and 195D connected to the external network 199.

Clients 195A, 195B, 197, and 195D may be situated behind corresponding network address translators (NAT) 192A, 192B, 192C, and 192D. Each NAT may be configured according to an Internet standard that enables a local area network (LAN) to use one set of private IP addresses for internal traffic and a second set of global IP addresses for external traffic. Most NATs perform dynamic translation on IP addresses such that external networks have no way of reaching the internal network prior to the internal network initiating communication. Because clients 195A, 195B, 197, and 195D establish server-client relationships, however, communication between the server 191 and clients 195A, 195B, 197, and 195D is not limited by the NATs 192A, 192B, 192C, and 192D.

In establishing a P2P network in which clients can communicate directly with each other, one client may be established as a host 197 by which other peers 195 (clients connected to the P2P network who are not the host) may establish direct connections with each other. Peers 195 may be connected in a configuration known as a fully connected grid (FCG). Such a configuration may prevent any one peer from being a bottleneck. Host 197 may be determined based on the NAT profile of each client. The NATs 192A, 192B, 192C, and 192D may be of one of four different NAT configurations referenced above (Full Cone, Restricted Cone NAT, Port Restricted Cone, and Symmetric).

Traversal of full cone, restricted cone and port restricted cone NATs is generally more complicated than traversing symmetric NATs. NAT traversal may be implemented if a client is behind a symmetric NAT as is described in U.S. patent application number 11/243,853, the disclosure of which has been previously incorporated. In particular, the client may perform a port prediction involving
construction of a list of predicted transport addresses on the NAT behind which the client is situated. The client may then send an INVITE message containing the list of predicted transport addresses from the first node to a second client. The client behind the symmetric NAT may then perform a connectivity check with the second node using the predicted transport addresses. Connectivity checks may be performed by sending Simple Traversal of UDP through NAT (STUN) requests to each predicted transport address in parallel. When the client behind the symmetric NAT receives the requests, the client sends a STUN response to the second client. If the second client receives the STUN response, it can then begin to send information to that address.

There may be NAT types other than the four described above. In some cases it may be possible to traverse NATs using standard techniques. In other instances, NAT behavior may be so unpredictable or unstable that communication with a client behind such a NAT is unreliable. Because the duty of the host 107 is to communicate information between other peers 195A, 195B, and 195D, it is important that the host 197 be behind a NAT of a type that does not interfere with its ability to communicate. In those instances where the peers 195A, 195B, 195D and the host 197 are in a fully connected grid (FCG), it may be particularly desirable to use a host behind a NAT that does not interfere with its ability to communicate. This allows for providing the highest level of service to the greatest number of peers.

By selecting a host 197 with the most favorable NAT profile, more reliable P2P communication may be obtained. Once the host 197 has been established, peers 195 can communicate with each other by initially transmitting information to the host 197, which then relays that information to the respective recipient peer 195. Clients may also transmit information directly after using host 197 to establish a direct communication path.

In certain embodiments, clients 195A, 195B, 195D, and 197 may obtain NAT profile information through a STUN server 193 that is associated with the external network 199. STUN server 193 utilizes a lightweight protocol that allows an IP enabled client to discover the presence and types of NAT behind which the client is situated. STUN server 193 works with most NAT types and does not depend on any special behavior of the NAT. STUN server 193, in one respect, acts like a mirror held up to a
client 195A so that the client 195A can see how its local transport address gets mapped to a public transport address. The client 195A can also determine the type of the NAT 192A behind which the client 195A is situated through communication with the STUN server 193.

[0037] Each client 195A, 195B, 197, 195D may use a STUN server 193 to obtain NAT profile information, which it may then relay to the central server 191 in order for the central server 191 to determine which client would make the most favorable host 197. Likewise, a client 195A, 195B, 197, 195D may use a STUN server 193 to obtain NAT profile information that may then be relayed to all other clients 195 attempting to communicate through the P2P network in order for the clients 195A, 195B, 197, 195D to best determine the host 197.

[0038] Each client connected to the server 191 may collect its own NAT profile information for use within the P2P network. This profile information may include information regarding the NAT type behind which the client is situated, information regarding whether the NAT supports universal plug and play (UPnP), information regarding whether the NAT exhibits port preservation, and information regarding whether the NAT supports port predictability.

[0039] Port preservation, as used in the context of the present applications, means that once an internal IP address is mapped to a particular external port that it will be consistently mapped to that particular port. Similarly, port predictability means that it is possible to predict the external port to which an internal IP address will be mapped even if it is not always the same port. For example, the external port number may be consistently incremented with each attempted mapping of the internal IP address.

[0040] The NAT profile information for each client may be used to create a priority list amongst all the clients connected to the server in order to best select the host for P2P communication. If there is a tie in priority between potential hosts, ordinal numbers may be assigned to determine which potential host is selected as the actual host. In some embodiments, such ordinal numbers may be assigned by a server in the order in which the clients connected to the server. Alternatively, a distributed arbitration algorithm may be used to select a host from amongst two or more equally suitable potential hosts. If the initial host decides to leave the P2P network or is
somehow disconnected from the network, this information may be used to select the next host for the P2P network in order to seamlessly maintain network connectivity.

Once profile information has been collected by a given client, the NAT profile for that client is shared with other clients that are connected to the server. Distribution may occur through peer-to-peer distribution or from the client to the server to the remaining clients. A server may distribute profile information through a dedicated network connection. Once all NAT profiles have been submitted by the clients, a determination is made as to whether a particular client should be a host, peer, or if they fail to meet the requirements for network interaction as a whole. This determination may be made based on the profile information obtained for each client described above.

For example, by assigning a priority based on a number of factors, a host can be selected from amongst the available clients based on the client having the most favorable profile. The rest of the clients may be assigned as peers or may fail to be recognized as a peer or host based on their profile information. For example, a client behind a non-traversable NAT may not meet the requirements necessary to connect to the network as a peer or host.

An exemplary prioritization scheme may break clients down into five separate distinctions: Active, Likely, Unknown, In Progress, and Inactive. An active tag indicates that a client is a very good candidate for host. A likely tag indicates that a client is a good candidate for host but priority is still given to a client with an active tag. An unknown tag indicates that the network is unable to decide whether that particular client is a good candidate for host. An in progress tag indicates that the network is still deciding whether the client is a good candidate for host. Lastly, an inactive tag indicates that a client is unable to assume the duties of a host.

Priority tags may be based on four exemplary criteria: NAT type, universal plug and play (UPnP) capability, port preservation, and port predictability. Several other factors may also be used in determining priority. These factors may fall under a client’s quality of service profile and may include QoS information including but not limited to ping time, bandwidth behavior, geography, latency, and IP provider.
[0045] FIGURE 2 illustrates an exemplary configuration 200 for a computing
device offering seamless host migration in a network data distribution system. The host
200, which may act as a central communications hub in a network, may be a computing
device such as a server. A computing device typically reserved for client operations
may also exhibit some or all of the configurations of host 200 due to the fact that a client
may, at some point, become a backup host. Host 200 may include a network interface
210, acknowledgement module 220, negotiation module 230, host information database
240, backup application module 250, polling module 260, timer 270, and NAT module
280.

[0046] A module (or application), as referenced in the present invention, is a
collection of routines that perform various system-level functions. A module may be
dynamically loaded and unloaded (e.g., executed) by hardware (such as processing
devices) and device drivers as required. The modular software components described
herein may also be incorporated as part of a larger software platform or integrated as
part of an application specific component.

[0047] Network interface 210 may be any of a variety of hardware and/or
software components configured to allow for communication between the host and
other computing devices in the network. Network interface 210 may include
components for communicating over wired, wireless, and/or Internet-based
communications networks.

[0048] Acknowledgement module 220 allows for verification that information
transmitted by a client was received by the host 200. When host 200 receives
information from a client through network interface 210, acknowledgement module 220
may transmit an acknowledgement of receipt (ACK) to the client sending the
information. For example, if a client sends information concerning a change in game
state data to host 200, acknowledgement module 220 may transmit an ACK reply to the
transmitting client indicating that information was received. The ACK reply sent by
acknowledgement module 220 may further include an indication of what information
was received and how much of that information was received and/or if any of that
information was corrupted or otherwise incomplete.
[0049] Non-receipt of an ACK with respect to a particular data transmission by the transmitting client may indicate that the data transmission was never received by the host 200. Non-receipt of the data transmission (or a portion thereof) by the host 200 may indicate a problem with the connection between the host 200 and the client that sent the data transmission or the host 200 in and of itself. If a particular number of data transmissions fail to receive an ACK reply from the host 200, the transmitting client may invoke a migration operation whereby some or all of the host functionalities are migrated to a backup host.

[0050] Negotiation module 230 negotiates the backup viability of a client based on a variety of parameters. For example, a viable backup host/client candidate may be required to have a certain amount of available bandwidth. The bandwidth of the client may need to be sufficient to allow the client to manage all the data in the network session. Backup viability may require that the client conform to various quality of service standards as they relate to, for example, ping rate, packet loss, available memory, processor speed, and the like.

[0051] Negotiation module 230 may further determine whether the client candidate is capable of connecting to each of the other clients in the network. A viable backup host may need to be able to connect to and receive information from each of the other clients in the network. The parameters for backup viability may be determined by the type of network session. For example, a particular gaming network session may require a certain amount of bandwidth and processor speed for backup viability due to the number of state changes that may occur in the game environment. Less complex transactions, such as simple file transfers, may require less bandwidth and/or processing power.

[0052] Negotiation module 230 may be configured to negotiate backup viability with multiple clients thereby resulting in a series of backup hosts. Alternatively, the negotiation module 230 may be configured to allocate backup responsibilities for particular tasks amongst a group of clients. By providing for a series of backup hosts, hosting duties may migrate seamlessly from a host to a first backup host to a second backup host and so on as network or host/client conditions warrant. An order of backup host responsibilities and/or the particular responsibilities may be assigned based on the
Host information database 240 may store information concerning the host, the clients, or the network session. The information stored in host information database 240 may allow for a computing device to perform certain hosting duties, such as connecting to the other clients in the network session. Such host information may include the network name, the Internet protocol (IP) addresses of the clients in the network, and firewall information. Host information database 240 may be updated when events such as a client disconnecting from the network or a new client joining the network occur. The IP addresses of the new clients would, for example, need to be added to the host information database 240.

Operating in conjunction with host information database 240, backup application module 250 generates an application that may be downloaded, installed, and executed on the client. This application provides a client with certain operational functionality that may be required of the client in order for it to serve as a backup host in addition to satisfying underlying viability requirements. The application may configure the client for connecting to and for exchanging data with other clients in the network session.

Optional polling module 260 may be configured to poll all the clients in a network session. Polling module 260 may be used to poll clients for connectivity. Polling for connectivity may include sending small packets of data to each client in the network session, receiving replies/acknowledgments from clients that have received the data packets, and determining which clients have problems communicating with the host 200.

Polling module 260 may automatically poll clients at periodic intervals. Polling module 260 may also be configured to poll clients when certain events occur, such as a new client joining the network session or an indication of interrupted communication (e.g., a client does not acknowledge data sent by host 200). The polling operation of polling module 260 may be akin to a periodic heartbeat like that described in U.S. patent publication number 2003-0204566 for a "Multi-User Application Program Interface," the disclosure of which has previously been incorporated by reference.
Host 200 may also include a timer 270. Timer 270 may be configured to measure how much time has elapsed after an event. Host 200 may use timer 270 to determine the time between a data transmission like that generated by polling module 260 and acknowledgement of that data transmission. Such information may be used to determine whether to terminate a connection to a particular client. If host 200 receives no acknowledgment or no poll response from a particular client for a period of time, as measured by timer 270, host 200 may terminate the connection with that client.

The application generated by the backup application module 250 may further include certain functionality similar to that of polling module 260 and timer 270. Unlike the host 200 that may be seeking to determine whether to eject a particular client from the network session, this 'heartbeat' functionality may be used by a client designated as a backup host to determine when the host 200 is no longer capable or has continuously failed to fulfill certain host duties. The inability or failure of a host 200 to fulfill certain duties may be indicated by a continued lack of receipt of an ACK or heartbeat as may be generated by acknowledgment module 220.

The host 200 may also include a NAT module 280. Execution of the NAT module 280 may allow for the collection, sharing and receipt of NAT profile information. Execution of the NAT module 280 may similarly allow for a determination as to a most viable host in a network utilizing NAT profile information. NAT profile information may be stored in memory, a dedicated database, or other database such as host information database 240.

Host 200 (and any number of clients) may reside behind a network address translator, which translates an internal IP address to a public IP address for a particular computing device. The public IP address is that address seen by other computing devices in a network. In some embodiments, host 200 or other computing device may incorporate the network address translator. In some networks, however, a NAT may not be used at all. NAT profile information may include information about the type of NAT (if any) in use, the ability of the NAT to engage in universal plug and play (UPnP), the NAT's ability to maintain port preservation, and the NAT's port predictability.
In some instances, host 200 (or other computing devices in the network) may apply a supplemental arbitration filter based on additional information such as quality of service information, to arbitrate a determination of the host device from among two or more equally likely candidate devices. Quality of service information may include factors such as the client's ping time, bandwidth behavior, geography, latency, IP provider, and so forth. Such additional information may also be stored in the memory or databases (dedicated or otherwise).

FIGURE 3A illustrates an implementation of an exemplary system 300 for network data distribution, which may include a network address translator (not shown). Host 200 is connected to a plurality of clients 310A-D. Client 310A has successfully negotiated backup viability with host 200 and received host information through connection 320. Using the host information, client 310A connects to the other clients in the network, namely, clients 310B-D. Connections 330 allow for clients 310B-D to communicate directly (i.e., not through host 200) with client 310A. Clients 310B-D may use the connections 330 to exchange data with client 310A if each respective client has difficulty transmitting that data to the host 200. Clients 310B-D may also transmit data to client 310A automatically, irrespective of any difficulties with data transmissions to the host 200.

FIGURE 3B illustrates an alternate implementation of an exemplary system for network data distribution, which may include a network address translator (not shown). In particular, FIGURE 3B illustrates an exemplary system for network data distribution where communications between a host 200 and a client 310D are interrupted. Specifically, the illustrated data transmission 340 between host 200 and client 310D is shown as being unsuccessful. While client 310D is attempting to send data transmission 340 to the host 200, a faulty connection prevents the transmission from ever being received by the host 200.

Because client 310A is a backup host for the network session, client 310D can send the same data intended for the host 200 in a backup data transmission 350 directly to client 310A (i.e., not through host 200). Client 310A may then send that data in a data transmission 360 to the host 200. Client 310A, in this particular embodiment, acts as a proxy between client 310D and host 200 due to the faulty connection separating
client 310D and host 200. Host 200 may then distribute the data from client 310D to clients 310B and 310C albeit received via client 310A. Alternatively, client 310A may send the data to clients 310B or 310C if, for example, host 200 was unable to maintain host duties versus the connection between client 310D and host 200 simply being defective.

[0065] Because communications between the host 200 and client 310D has been disrupted, client 310D may need to obtain session data through client 310A. Client 310A may act as an intermediary for both the receipt and transmission of data with respect to host 200 and client 310D in addition to making requests for data on the behalf of either computing device.

[0066] FIGURE 4 is a flowchart depicting an exemplary method 400 for network data distribution, which may include the use of NAT profile information. The steps identified in FIGURE 4 (and the order thereof) are exemplary and may include various alternatives, equivalents, or derivations thereof including but not limited to the order of execution of the same. The steps of the process of FIGURE 4 (and its various alternatives) may be embodied in hardware or software including a machine-readable or computer-readable storage medium (e.g., optical disc, memory card, or hard drive) including instructions executable by a processor.

[0067] In step 410, a host (e.g., host 200) establishes a network session. The host may set certain parameters for who may join the network session, as well as various aspects of how the network session will proceed. A host may establish a private network session that only certain clients or invited clients may join. Alternatively, the host may establish a network session that is open to the public and any client may join.

[0068] In step 420, multiple clients join the network session by connecting to the host. If the host has set certain parameters concerning who may join the network session, the clients may need to satisfy those parameters before being allowed to connect the host or to participate in the network session.

[0069] In step 430, backup viability is negotiated via the negotiation module 220 of FIGURE 2. One or more clients may be viable backup hosts with the capacity and resources to serve as a backup hosts. Backup viability may be negotiated as soon as a client joins the network session. Various aspects of backup viability, including
bandwidth and quality of service, may be evaluated to determine whether a particular client is capable of serving as a backup host. NAT profile information may likewise be considered. Depending on the requirements of negotiation module 220, there may be one, more than one, or no viable backup hosts among the clients in the network session. Backup responsibilities may also be distributed.

In step 440, backup responsibility is allocated. Where there are multiple clients that are viable backup hosts, backup responsibility may need to be allocated among those clients with respect to order and/or particular responsibilities. Clients in the network session may transmit their data to the first viable backup host as may have been identified by the host or the first deemed backup through a broadcast or other communication as exemplified in U.S. patent publication number 2003-0217135 for "Dynamic Player Management," the disclosure of which has previously been incorporated by reference. If the first viable backup host is or becomes incapable of serving as a backup host, the other clients may transmit their data to the second viable backup host to join the network session. The need to communicate with a secondary backup host may be indicated utilizing means as disclosed herein and/or the aforementioned "Dynamic Player Management" application.

In step 450, it is determined whether a particular client can connect to each of the other clients in the network session. A backup host needs to be able to connect to each and every other client in the session. If a first client cannot connect to a second client, that first client cannot serve as a backup host for the network session. For example, the first client may have firewall issues that would prevent the first client from making certain types of connections. If a potential backup host cannot connect to another client for any reason, the method may return to step 440 and re-allocate backup responsibility.

Once it has been determined that a client is a viable backup host and can connect to all of the other clients in the network session, the method proceeds to step 460. In step 460, backup information is downloaded to a viable backup host. By providing the backup information to a backup host, the host can drop out of the network, and the backup host is capable of providing any information required by the other clients in the network session. Backup information may be provided as a part of
the download and installation of an application facilitating seamless host transitions as discussed in the context of backup application module 250 of FIGURE 2.

[0073] In step 470, network data distribution may commence. As illustrated in FIGURE 3A, the data transmissions may occur between a host and a client. As FIGURE 3B further illustrates, data transmission may also occur between two clients, from a client with host connectivity issues to a client capable of acting as a backup host. Further, that backup host may forward that data on to the host or directly to the other clients upon request. Through whatever connection(s) the data must be relayed, the data is provided to those computing devices that require that data.

[0074] While the present invention has been described with reference to exemplary embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted for elements thereof without departing from the true spirit and scope of the present invention. In addition, modifications may be made without departing from the essential teachings of the present invention. Various alternative systems may be utilized to implement the various methodologies described herein and various methods may be used to achieve certain results from the aforementioned systems.
WHAT IS CLAIMED IS:

1. A method for maintaining network data distribution, comprising:
   establishing connections between a host and a plurality of clients, wherein data exchanged between the host and each of the plurality of clients is acknowledged upon receipt-
   determining backup viability of a first client from the plurality of clients based on at least Network Address Translation (NAT) profile information shared between the host and the plurality of clients upon establishment of the connections between the host and the plurality of clients; and
   transmitting host information to the first client, wherein the first client establishes connections to all other clients from the plurality of clients based on at least the host information, and the first client receives data from a second client from the plurality of clients if communication between the host and the second client is interrupted.

2. The method of claim 1, further comprising collecting NAT profile information via a STUN server prior to sharing the NAT profile information between the host and the plurality of clients.

3. The method of claim 1, wherein the NAT profile information is shared between the host and the plurality of clients utilizing a client-server configuration.

4. The method of claim 1, wherein the NAT profile information is shared between the host and the plurality of clients utilizing a peer-to-peer configuration.
5. The method of claim 1, further comprising assigning a priority value to each of the clients from the plurality of clients using the NAT profile information, and wherein determining backup viability of the first client from the plurality of clients based on at least NAT profile information includes use of the priority value.

6. The method of claim 5, further comprising resolving a priority dispute when the first client has a priority value equal to the priority value assigned to another client from the plurality of clients.

7. The method of claim 6, wherein resolving the priority dispute includes reference to a higher ordinal value of the first client versus an ordinal value assigned to the other client from the plurality of clients, the ordinal value having previously been assigned to each of the plurality of clients.

8. The method of claim 1, wherein the NAT profile information for each of the plurality of clients includes a NAT type, and wherein determining backup viability of the first client from the plurality of clients based on at least NAT profile information includes use of the NAT type.

9. The method of claim 1, wherein the NAT profile information for each of the plurality of clients includes information regarding whether the NAT supports universal plug and play (UPnP), and wherein determining backup viability of the first client from the plurality of clients based on at least NAT profile information includes use of the information regarding whether the NAT supports UPnP.

10. The method of claim 1, wherein the NAT profile information for each of the plurality of clients includes information regarding port predictability information for the NAT, and wherein determining backup viability of the first client from the plurality of clients based on at least NAT profile information includes use of the port predictability information.
11. The method of claim 1, wherein the NAT profile information for each of the plurality of clients includes information regarding port preservation information for the NAT, and wherein determining backup viability of the first client from the plurality of clients based on at least NAT profile information includes use of the port preservation information.

12. The method of claim 1, wherein the interrupted communication is identified by a lack of acknowledgement from the host to the second client within an amount of time after the second client transmits data to the host.

13. The method of claim 1, further comprising polling the plurality of clients to determine connectivity between the host and each of the plurality of clients.

14. The method of claim 13, wherein the interrupted communication is indicated by results of the polling.

15. The method of claim 1, further comprising sending an indication from the host to each of the plurality of clients concerning the interrupted communication.

16. The method of claim 1, further comprising terminating a connection between the host and the second client based on the interrupted communication.

17. The method of claim 1, wherein negotiating the backup viability of the first client comprises determining a bandwidth of the first client.

18. The method of claim 1, wherein negotiating the backup viability of the first client further comprises determining whether the first client is capable of connecting to each of the other clients from the plurality of clients.

19. The method of claim 1, wherein transmitting host information to the first client comprises transmitting an application providing the host information.
20. The method of claim 1, further comprising
determining backup viability of a third client from the plurality of clients based on at least NAT profile information shared between the host and the plurality of clients upon establishment of the connections between the host and the plurality of clients; and transmitting host information to the third client such that the third client connects to all other clients from the plurality of clients based on at least the host information and the NAT profile information, and the third client receives data from the second client if communication between the first client and the second client is interrupted.

21. The method of claim 20, wherein the second client is further configured to transmit the data to the first client before transmitting the data to the third client based on at least an order in which a connection was established with the host.

22. The method of claim 20, wherein the second client is further configured to transmit the data to the first client before transmitting the data to the third client based on at least bandwidth of the first client and bandwidth of the third client.
23. A system for maintaining network data distribution, comprising:
   a host configured to connect to a plurality of clients, wherein the host receives
   and acknowledges the receipt of data from each of the plurality of clients;
   a first client configured to receive host information, wherein the first client
   connects to all other clients from the plurality of clients based on at least Network
   Address Translation (NAT) profile information shared between the host and the
   plurality of clients upon establishment of connections between the host and the plurality
   of clients, and wherein the host is further configured to negotiate backup viability of the
   first client; and
   a second client configured to transmit data to the first client if communication
   between the host and the second client is interrupted.

24. The system of claim 23, wherein the interrupted communication is indicated by a
   lack of acknowledgement from the host within an amount of time after the second client
   transmits the data to the host.

25. The system of claim 23, wherein the second client is further configured to re-
   transmit the data to the host.

26. The system of claim 23, wherein the second client is further configured to notify each
   of the plurality of clients concerning the interrupted communication between the host
   and the second client.

27. The system of claim 23, wherein the second client is further configured to terminate
   a connection between the host and the second client.

28. The system of claim 23, wherein the host is further configured to poll the plurality of
   clients concerning connectivity.
29. The system of claim 23, wherein the host is further configured to notify each of the plurality of clients concerning the interrupted communication between the host and the second client.

30. The system of claim 29, wherein the host is further configured to terminate a connection between the host and the second client.

31. The system of claim 23, wherein the host further negotiates backup viability based on a bandwidth of the first client.

32. The system of claim 23, wherein the host further negotiates backup viability based on whether the first client is capable of connecting to each of the other clients from the plurality of clients.

33. The system of claim 23, wherein the host is further configured to transmit the host information to the first client.

34. The system of claim 33, wherein the host transmits the host information by transmitting an application configured to provide information concerning each of the other clients from the plurality of clients.

35. The system of claim 23, wherein a third client from the plurality of clients is configured to receive host information, such that the third client connects to all other clients from the plurality of clients based on at least the NAT profile information shared between the host and the plurality of clients upon establishment of connections between the host and the plurality of clients.

36. The system of claim 35, wherein the second client is further configured to transmit data to the third client if communication between the first client and the second client is interrupted.
37. A computing device for maintaining data distribution in networks, comprising:
   an acknowledgement module configured to transmit a reply acknowledging data received from a client;
   a negotiation module configured to negotiate backup viability of a first client based at least on shared Network Address Translation (NAT) profile information; and
   a backup application module configured to transmit an application providing host information to the first client, such that the first client connects to all other clients from the plurality of clients based on at least the NAT profile information and receives data from a second client.
38. A computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for group messaging comprising:

connecting a host to a plurality of clients, such that data exchanged between the host and each of the plurality of clients is acknowledged upon receipt—

determining backup viability of a first client from the plurality of clients based on at least Network Address Translation (NAT) profile information shared between the host and the plurality of clients upon establishment of the connections between the host and the plurality of clients; and

transmitting host information to the first client, such that the first client connects to all other clients from the plurality of clients based on at least the host information and the first client receives data from a second client from the plurality of clients.

39. The computer-readable storage medium of claim 38, wherein the program further comprises executable instructions for terminating a connection between the host and the second client.
FIGURE 1D
FIGURE 2

- Input/Output 210
- Backup Application Module 250
- Acknowledgement Module 220
- Polling Module 260
- Negotiation Module 230
- Timer 270
- Host Information Database 240
- NAT Module 280
400

Host Establishes Session 410

Clients Join Session 420

Negotiate Backup Viability 430

Allocate Backup Responsibility 440

Can Backup Connect? 450

Download Backup Information 460

Commence Data Distribution 470

FIGURE 4
## INTERNATIONAL SEARCH REPORT

### A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/16 (2008.04)
USPC - 709/217

According to International Patent Classification (IPC) or to both national classification and IPC

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 15/16 (2008.04); USPC - 709/217

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 709/204,205,217-219,227-229,370/392: 700/1.90 - see search terms below

Electronic database consulted during the international search (name of data base and, where practicable, search terms used)
Google; Google Scholar; Google Patents; PubWest(PGPB, USPT, USOC, EPAB, JPAB);
Search Terms Used: data distribution, networks, connecting, host, plurality of clients, backup viability, Network Address Translation (NAT) profile, transmitting host information, network data distribution, communication, interrupted

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>


### D. Further documents are listed in the continuation of Box C.

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "Q" document member of the same patent family

Date of the actual completion of the international search
19 November 2008 (19.11.2008)

Date of mailing of the international search report
05 DEC 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Ativ ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer: Lee W. Young
PCT Helpdesk 571-272-4300
PCT OSP 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)