Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies

A SYSTEM FOR ROBUST PEER-TO-PEER COMMUNICATION WITH DYNAMIC PROTOCOL SELECTION

Mark Wallis, Frans Henskens, Michael Hannaford
School of Electrical Engineering and Computer Science
University of Newcastle, Newcastle, N.S.W, Australia
mark.wallis@studentmail.newcastle.edu.au

Abstract

Continued growth in peer-to-peer (P2P) networking is introducing new challenges for network designers and administrators. P2P communication is no longer the sole domain of the home-based, technically savvy user. Instead, corporations are now starting to investigate the use of P2P communication as a valid technology for distributing data to a large user base. Existing network protocols that support P2P communication, such as UPnP, do not scale well to larger corporate and institutional networks. This paper introduces a new, dynamic system that is capable of supporting P2P communication in a large array of networks designs ranging from smaller home networks to larger corporate networks that contain multiple layers of firewalls and proxies.

1. Introduction

Peer-to-peer (P2P) communication is a common networking paradigm that involves many-to-many communication between multiple client processes [4]. Continued growth in P2P networking [1] is introducing new challenges for network designers and administrators. Historically, P2P networks have been limited to purposes such as community file sharing [2], but it is becoming increasingly common to see large corporations deploying the use of P2P technology [3] for distribution of their own applications and data.

P2P communication requires certain network properties to function correctly. Generally, the requirement is defined as the capability of the network edge router to forward relevant incoming datagrams to the P2P client software behind a network or port address translation. Protocols such as UPnP IGD [5] have been designed and implemented to ease the fulfilment of this requirement, but they do not scale well to larger, corporate networks that might involve multiple firewalls and network proxies. With the increase in corporate use of P2P technology this scalability limitation is becoming an issue that needs addressing.

This paper abstract introduces a new concept of a service that is responsible for enabling a client for P2P communication. The service is capable of operating in different modes depending on the support available from the network surrounding the P2P client.

2. Problem Description

At a network layer, P2P communication is fundamentally different to classical client/server communication. This is due to the fact that the required network sockets are no longer only uni-directional in nature. P2P communication requires that sockets can be opened in both ingress and egress fashion from a client [4]. This requirement is in conflict with the standard firewall approach that can be found in most commercial and home networks.

Ingress communication requires that the edge router of the home network is capable of forwarding the relevant P2P packets through to the client host. While various methods such as dynamic networking protocols already exist for this to occur, they are decentralised and require that the P2P client software supports each method explicitly. Commercial networks are typically stricter and block all forms of ingress and egress communication without explicit permission.

Figure 1 depicts a standard P2P communication system where each peer is behind a home networking network address translation and firewall.

The NAT/Firewall device must perform two functions. Firstly, it provides a network and port address translation function such that one or more machines on the internal network can access the Internet through a common Internet-routable address space. Secondly, the device must forward incoming P2P traffic connections to the P2P client inside the network. In the standard home networking environment, there are two possible ways to achieve the configuration of

0-7695-3049-4/07 $25.00 © 2007 IEEE
DOI 10.1109/.70

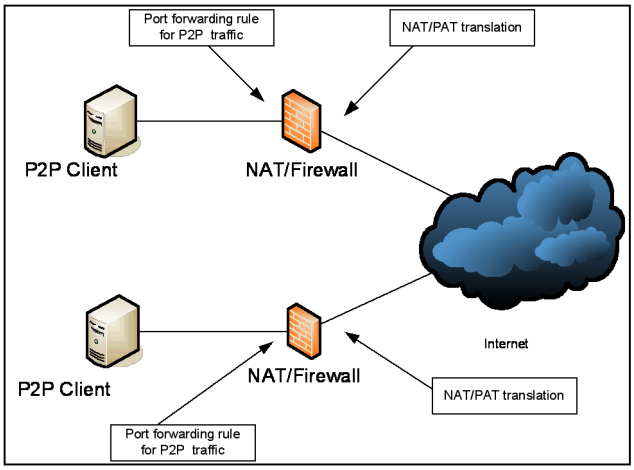

Figure 1. P2P System

this second requirement.

1. Manually configure a port forward command in the configuration of the NAT/firewall device. This requires that the user have access to the configuration of the NAT/firewall device and the technical capability of correctly configuring the port forward in a secure manner. In some situations this is the only option available for the user if their hardware does not support dynamic network protocol

2. A dynamic networking protocol such as UPnP can be implemented in both the P2P client software and the NAT/Firewall device. The UPnP protocol allows the P2P client software to request that a port forward be established automatically without the user needing be involved in the technical setup.

The primary existing dynamic networking support protocol is the Internet Gateway Device (IGD) [5] subset of the UPnP protocol. The IGD UPnP protocol defines a method in which an application can request the network edge router to establish a port forward configuration on the users behalf without their direct intervention. There are various design and implementation flaws within the IGD UPnP protocol that cause it alone not to be a viable solution to the P2P communication problem in the longer term. Specifically, the IGD UPnP protocol does not cater for corporate environments where the user is not directly attached to the network edge router.

3. Proposed Solution

To solve the P2P communication problem in a scalable and secure manner the following system titled P2PBroker has been designed by the Distributed Computing Research Group at the University of Newcastle, Australia. This design allows us to address the issues described above and provide a framework that can solve the P2P communication problem in a large range of network designs.

The benefits of the P2P Broker system are as follows:

1. It provides a centralised method of establishing P2P communications for all P2P enabled software on a specific client. This allows P2P client software to communicate in various network designs without being required to implement multiple technologies directly.

2. Abstracting P2P communications into a separate service allows new P2P communications protocols to be developed and retrofitted to existing systems without having to upgrade the each piece of P2P client software.

The P2P Broker service could be implemented as a local service running on each host, or as a shared network resource capable of brokering P2P connections for all machines connected to a LAN. After the initial brokering is completed the service is no longer involved in the P2P communication.

4. Conclusion

The proposed design provides a tool that allows greater flexibility to address the P2P communications problem. It provides a scalable and abstracted implementation that removes the P2P communication problem from the P2P client software and into a centralised service that can be tailored both statically and dynamically to provide the best possible solution for each P2P client. This added flexibility allows the development of new Modes of Operation that are able to address the specific issues listed above with the current industry standard solution UPnP. While UPnP is a suitable protocol for addressing the issue in smaller home/SOHO networks, it fails to address it in larger corporate networks. From here, additional MODs can be designed and implemented that solve the P2P communications problem in each specific network design.

References

[1] J. Carleton. Fast growth forecast for enterprise p2p. *ZDNet Tech Update*, 2002.
[2] B. Dessent. *BitTorrent FAQ and Guide*, 2005.
[3] B. Helm. Bittorrent goes hollywood. *BusinessWeek Technology Review*, 2006.
[4] R. Subramanian and B. D. Goodman. *Peer-to-Peer Computing: The Evolution of a Disruptive Technology*. IGI Publishing, 2005.
[5] UPnPForum. *InternetGatewayDevice:1 Device Template Version 1.01, Internet Gateway Device (IGD) Standardized Device Control Protocol*, 2001.