Achieving, Detecting and Preventing NAT Traversal for Peer-to-Peer Networks

Andrew McKenzie

As technology rapidly develops, many new software solutions created to manage these technologies have been found lacking when required to operate effectively across a range of different applications. One such problem facing Allied Telesis is its current firewalls; while capable of managing single forms of data flow, are now being found inadequate when required to manage multiple data types such as voice and multimedia. Separate network infrastructures utilised for different services are now being combined through firewalls, presenting new problems for current software.

Allied Telesis produce Network Address Translation (NAT) devices that allow internal computer networks to communicate with external networks. The use of multiple data types however creates conflict for the server. This problem is typically faced by developers of client-to-client networking applications especially in Peer-to-Peer and Voice over Internet Protocol networks. While NAT traversal refers to a solution to this common problem, many techniques of NAT traversal exist and no technique works in every situation since NAT behavior is not standardized.

This project will investigate current NAT traversal techniques and methods of limiting and blocking Peer-to-Peer (P2P) traffic at the point of NAT. Several popular P2P applications will be analysed and the techniques they adopt for traversal will be combined within a test application. This application will then be used to develop and test a new method of successfully limiting NAT traversal. The utilisation of this new application when successfully finalised, will form the basis of new software that will be employed in the company’s software releases giving customers a more intelligent fully featured solution.