ABSTRACT

Rapidly growing of internet user caused IPv4 address allocation become rare. Every single computer must have IP address in order to communicate in the internet. Decreased of IPv4 address quantity had solve with NAT technology but NAT blocked point to point connection for realtime application. IPv6 address with huge addressing must be the solution of limited IPv4 address today but impossible between IPv4 and IPv6 can take communication each other because they have different in format addressing, header and operating system command. This can be solved by transition technology.

The transition technology must match properly with network characteristic today that almost using NAT. Teredo mechanism serves migration solution from IPv4 into IPv6 addressing and support NAT. Security implication that appear in teredo mechanism is that host behind NAT become discovereable and can be remote from outside. This final project will be implemented transition network of IPv4 and IPv6 using teredo mechanism in laboratorium coverage and then it will be analize and test system security in the end to end data communication through http, https, ftp and ssh between IPv4 user and IPv6 user.

As the result, we can see that teredo mechanism protect secret transfer data in end user (client teredo). Http and ftp application without teredo mechanism caused password authentication can be known by intruder using man in the middle attack. Teredo data will be encapsulated by UDP header after implemented. Arp poisoning attack at the client side didn’t affect teredo mechanism process. The ability of teredo to bypass NAT and allow only ICMP paket from the outside. Http, https, ftp and ssh in teredo mechanism didn’t walk two way.