**Spoofing MAC Address and Deny Internet Access to a Computer**

Arjun Sethi

Keith Nguyen

**Abstract**

Each computer connected to the internet must have both and IP address and a MAC address. The router maintains an Address Resolution Protocol (ARP) table that pairs IP and MAC together. At the moment, we know that MAC address cannot be the same for computers in a network and each computer also keeps its own ARP table. Therefore, we want to know what happens if two computers in a network have the same MAC. And what happens if two computers have the same IP. Finally, we want to see if the server is confused between two computers having the same MAC address or the same IP address, how do we listen or pretend to be one of the computers by changing our IP or MAC address.

Finally, if the MAC address is mutually exclusive, we look for a way to disconnect the real computer from the network long enough to get in its place, or to become the middleman between the router and the real computer. We explore possibilities such as DoS attack, physical blocking and other methods.

**Concepts**  
MAC address

ARP table

IP address

DoS attack

Physical blocking

**Spoofing MAC Address**

We use Ubuntu and CentOS as our preferred operating system as Linux gives us more control over a computer’s lower level data. They also have many penetration testing tools from Kali Linux so we have more options to explore our project. There are several ways to change the MAC address on Linux: use built in “Edit Connection”, use macchanger, use ifconfig.

**Spoofing IP Address**