Ryan Stearns  
Jack Holland  
CNA 432  
Class Activity 4

**Class Activity 4 - MIPv6**

The problem is packets are being blocked by the firewall, and this is because most firewalls are configured to drop packets coming from a foreign network by default.  Firewalls would have to be configured to let RRT messages pass through the firewall and thus reach the CN.  A vulnerability within this would be a DoS Attack which would block valid RRT messages through Rate Limiting.  This attack happens after an attacking node sends a large number of MIPv6 signaling.  Another solution to this problem would be to configure the firewall to create packet filters for sent traffic to the COA.  Vulnerabilities to this solution include rogue address updates that enable an attacker to have all their traffic enter the network.  A solution to fixing this vulnerability would be to configure the firewall to create/update an entry in its table of the Binding Acknowledgement Message upon receiving it.  When a Binding Update Message is received, the inner node will send a Binding Acknowledgement Message.  The maximum time this entry if valid will be derived from the lifetime of the Binding Update Message.  Incoming and Outgoing Packets will also need to be filtered against at least these IP Addresses.  When a deregistration message is received, or expiration of the lifetime, the state will be deleted.