The Fire Walls Example:

We can work on this example through out the class. You are not expected to finish it all in one go. The purpose of the exercise is to learn how to write good SPARK Ada programs. As the term progresses I may have to change the exercise to better illustrate different design options. While writing the Ada Program write down a summary of the design decisions you made and, where appropriate what has been *proven or verified*.

A firewall has an home port, an outside port and a state consisting of a table of rules. Messages from the outside are only passed from the outside to the inside only as a reply to a message passing the other way from some one on the inside messages some one on the outside.

Messages consist of a sequence of packets, each packet has header and some data. The header has both a from and a too address. At any point in time a packet exists on a port attached to some device such as the firewall.

Design a firewall object with a *"process message"* method that appropriately processes massages that arrive at either of the firewalls ports. Decide upon what should be private and what public and justify. Prove what you can about the firewall and document.

Initial firewall object should use equality match on from or too address. Refine the initial firewall by adding the ability to record and update a white list. That is outside addresses that are always allowed to message anyone at home. The updating of the white list must be in response to a message from a designated control port.

Make a second refinement to introduce partial matching between the addresses of a rule with the address of a packet.