1. **Issues:**
   - Bill is out of town attending multiple conferences.
   - Zahid was meeting with Prof. Roy Campbell.
   - Progresses made in the last two weeks:
     1. Built a general model for PKC services and e-mail application in OPNET.
     2. Fixed some bugs in the OPNET model: the model is running now.
     3. Contacted OPNET technical support and found out how to combine PKC services and the e-mail application (see next for details).
     4. In the middle of renewing OPNET licenses.

2. **Coordinating actions of custom application (PKC request-response) and pre-defined application (email) in OPNET:**
   - We contacted OPNET technical support and successfully solved the problem.
   - Just for record and for future use, the solution is as follows:

     There are a couple of ways to model this behavior. We need to define two profiles, one containing our custom application PKC followed by an email, and a second one that contains only the email. For the first custom application, we can set the Operation Mode to be “Serial (ordered)” so that the email is sent after the key exchange. Also, both the applications in the first profile must be run once (repetition is “Once at start time”). The two profiles (email with and without key exchange) do not have any relation to each other. It is our responsibility to set the start times and repetition patterns of the two profiles so that they are interleaved.

     Another approach is to use the ACE whiteboard to build a complex application with logic. For more information on using the ACE whiteboard, please refer to the following resources:

3. **Modeling the PKC transactions (Suvda and Jun).**
   - Suvda and I finally made the simple model work after fixing some bugs and consulting OPNET technical support.
   - During the meeting, Suvda raised a question about how to measure the traffic for the combined service (PKC plus e-mail) at a node, because OPNET will keep track of the PKC and e-mail traffic separately. For example, in Figure 1, the node “Email/PKC Client” will not be able to keep track of the PKC and e-mail traffic together. I suggested that we could measure the IP layer or even the physical layer traffic instead of the application layer traffic, which will include all traffic.
We will continue to work on the PKI model to make it more realistic.
We will probably have to separate the PKI model and the application because according to a literature ("Understanding PKI," 2nd edition, by Carlisle Adams and Steve Lloyd), a real PKI system (including the client software) should be
independent of specific applications. But, our current investigation is definitely a must step. The separation should be easy to implement later.

4. Renewal of OPNET licenses (Jun)
   - Jun is renewing OPNET licenses. The current licenses will expire on December 22, 2005. After discussion, we decided not to renew the licenses for the ACE module and the Flow Analysis module at this time. These two modules might be very useful in the future when modeling more complex applications. But for now, we just need to keep the basic license for the Modeler and the license for the Wireless module, which will cost about $750 in total.

5. Future directions
   - Since we have made a good progress in modeling PKI services in OPNET, we have two possible future directions. The first option is to continue working on the PKI modeling for other applications, such as HTTP, database, etc. The second option is to start investigating how to model N2K in OPNET, starting with the e-mail application. More complex applications will be modeled together later for both PKI and N2K. I slightly prefer the second option because we have gained some knowledge of modeling PKI in OPNET and other applications should be easy to handle later---how to model N2K is more interesting and urgent at current stage.
   - Next week is finals week – don’t expect too much work being done.