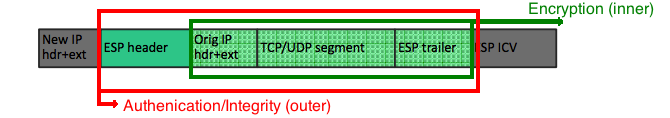
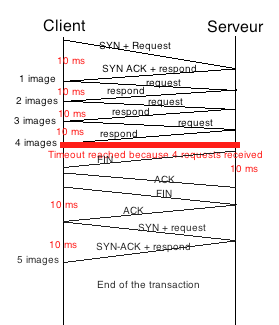
Homework 4. Internetworking. EP2120 . Pierre FLEITZ  
  
**I) DNS:**

1. Command used : dig +short –x 192.16.125.102  
   Result : mail.ssvl.kth.se.  
   Therefore, the domain name is mail.ssvl.kth.se.
2. TODO
3. TODO

**II) IPsec :**

1. IPsec provides differents security services :  
    - *Defining Algorithms and Keys :* The 2 entities that want to create a secure channel between themselves can agree on some avaible algorithms and keys to be used for security pruposes.  
    - *Packet Encryption :* The packet exchanged between 2 parties can be encrypted for privacy using one of the encryption algorithms and a shared key agreed upon ih the first step.   
   Note : This makes the packet sniffing attack useless !  
    - *Data Integrity :* Data integrity guarantees that the packet is not modified during the transmission. If the received packet does not pass the data integrity test, it is discarded.   
   Note : This prevents the packet modification attack.  
    - *Origin Authentication :* IPsec can authenticate the origin of the packet to be sure that the packet is not created by an imposter.  
   Note : This can prevent IP spoofing attack.
2. What to do when you receive an ESP encapsulated IP Packet :  
    1) Look up the Security Association based on the destination address and SPI ( Security Parameter Index ) -> If the packet is unsecured (there is no IPsec) then search through SPD (Security Policy Database) for match. -> If no matching entry or if policy is PROTECTED or DISCARD then the packet is discarded.  
    2) Find algorithm, algorithm key, sequence number etc in the SA based ( reminder : SA determines how packets are processed : cryptography, algorithms, key, ESP (or AH) etc..). -> That’s how the destination figures out what cryptographic to use to decrypt the packet.  
    3) Finally when finished decrypting the message, deliver packet to the next higher layer.
3. ****We can notice the presence of the « Orig IP hdr + ext » therefore this is tunnel mode.  
     
   **Original packet :**  
   Macintosh SSD:Users:pierre:Desktop:Capture d’écran 2015-10-04 à 19.47.25.png  
   **Redrawed packet to show how the differents parts of the packet can be protected :**

**III) IKE :**

1. Cookies are used against denial-of-services attacks and Nonces are used against replay attack.  
   Redraw of the figure to show where to add cookies and nonces :
2. HTTP version 1.1. The browser is requesting a persistent connection (Connection : keep-alive).
3. The server accepts a persistent connection (connection : Keep-alive).
4. We gonna have to make 5 requests but we can see that we have a keep-alive maximum at 4 requests (keep-alive : timeout=10, max=4), it means that after 4 requests the connection ends and we need to open a new one.  
   If we consider that opening a TCP connection requires 1 RTT, that closing a TCP connection requieres 2 RTT, we gonna have 7 \* RTT so 70 ms. (without counting the connection termination at the end if we do we gonna have 90ms).   
   Timetable :   
   
5. We can see that there is a cookie value, it means that the client’s browser found it in the cookie directory. Therefore we can conclude that the client received a cookie from that same server before thus that the client has visited this web site before.
6. We can see that cache-control is set to ”No-cache” therefore there is no response stored in the cache, the proxy server is going to send the request to the corresponding server.

**IV) DHCP :**

1. Because he didn’t received the DHCP ACK. Before receiving the DHCP ACK the client isn’t allowed to use the network configuration received from the DHCP server earlier. Client must include server ID (not shown here) to inform about selected offered address.
2. After receiving the DHCP ACK he will be able to use the IP address offered by the server.
3. Knowing that a client can receive DHCP offers from multiple servers and that it will accept only one DHCP offer, we can understand that the client will send the DHCP request as a broadcast message so servers can be informed whose offer the client has accepted and they can withdraw any offers that they might have made to the client and return the offered address to the pool of avaible addresses
4. It is to prevent a problem when the reply, from the server to the client, is broadcast. It prevent the use of the same two destination port numbers. And it is considered “bad manner“ to broadcast to a random port number