IPSEC uses

As you see these are the scenarios that can happen in ipsec . lets say this guy want to send something important to this guy and as you see the network are , having this router and this router device with ipsec, generally this is going to be file ,as you see these guys are preparing the network with ip address and ip pay load and that way this guys are making this ip payload secure and Ip address secure and its going to put a dummy ip header and that will be the address of the router and its going to come here and this router will remover this ip header and remove the secure ip payload and send it to the actual address, if you are a hacker right here you done know who is receiving this mail , but you know that whoever is receiving this mail is in this network but you don't know actually the address of this guy, if you change the source address of the network then you cant work , but you can change the source address of this one so what were are going to do is we are going to make it secure by using the mac, we are going to come out with two different concepts one is mutable and the other is immutable fields of ip protocol mutable fields are fields that are changed during transmission and immutable fields are the fields that are not changed during transmission when you come to one router it is changing some fields before coming to the router and what are those fields they are mutable and what are the change that router cannot make and we are going to look at both , mutable and immutable fields of ip header , this is just the brief explanation ,if you don't understand it don't worry about it because we are going to go step by step as this guy is going to send message to this guy ,you see this guy doesn't have any protection against firewalls or something ,if this is the case then we are going to send again the ip sec header and ip payload with the Ip header and this ip header will be the destination header of this guy and this guy will be able to recover the payload ,like this way I can send the information to the public network but in the public network no one can see what kind of information im exchanging, in other words im exchanging ,im having a private network and sending my data on the private network so that outside network cannot see the network basically that's why ipsec is very important network for vpn , this is very important application in military I worked with those guys in there and they love it , they are using ipsec all the time and these ipsec is also going to avoid replay attacks and we will see how they provide protection from those attacks , in a firewall router provides strong security to all traffic crossing the protocol in other words we have to use the firewalls and it is resistant to bypass and it is below transport and it is transparent to all end users and it is transparent to transport layer and it is going to handled by OS, so you don't have to do anything and can provide security for individual users if desired , personal VPNS on your desktop we have vpn ,we have vpn access in our campus I can use my laptop from home and access college computer , that's how vpn , it is little different than other things ,as I said ssl vpns are much more faster and effective , much more easier to implement and ipsec is difficult and like x500 it ihas huge amount of definition and like simplicity complexity is too much is going to cause problem and so that's what the reason why this guy is not gaining momentum,

IPsec architecture

Specification are quite complex, defined in numerous RFC's , these are the RFC and many other s grouped by category and mandatory in ipv6 and it is compulsory there and it is optional in IPV4 ,but todays is ipv6, this is the architecture we are going to have two protocols one is AH and the other is ESP, this ESP will deal with actual encryption and definition of all those encryption algorithm that are

compatible and ESP can also come with authentication as option if that's the case what authentication option can be used down the parameters and also another parameter and it ideal with only authentication if that's the case this is the authentication algorithms for the definitions and parameter required for these documents and all the parameters are going to deal with DOI, one part extra that's the key management, that the protocol that will solve the problem or which will address the requirements of encryption and authentication algorithm over here we are going to sue two more protocols Oakley and ISKMP this is going to to be the actual structure of ip it seems a more info for one security ,

IP services

It is going to provide access control and connectionless integrity ,it is not connection oriented ,data origin authentication, rejection of replay packets how we are going to do it im going to show it , we are going to use sequence numbers ,confidentiality will be provided and limited traffic flow confidentiality will be provided , why is it limited ?.. why it is not full?..think about the scenarios..you can see which network it goes but you cannot see which recipient receives the ,message ,you know the network but you don't the actually destination user, so that's why its going to provide limited traffic flow confidentiality.