SA parameters

These are the parameters for the security associations when we try to communicate with the other we are going to check this parameters other is the SA selectors we are going to have more than 1, SA imagine you are going to communicate with more than 100 people and those100 guys may be communicating with 100 other guys in IPSEC there are to f SA, SPI can identify the SA but I need something extra to make the SA clear for us and those things are called SA selectors , what we need is Destination IP address, what we are going to do is we are going to check the IP address is going to be important and im going to give the OS user id that is important , OS user id if the IPSEC is using the make OS then they are using the same user id , if it is different then this user id is going to be there ,then data sensitivity this could be DES kind of top secret kind of level ,so depending on that one you are going to select the security level, , and the transport layer protocol you are using ,which are the protocol?.. TCP and UDP these are the two major ones, TCP is connection oriented one and the UDP is connection less oriented ones ,which one you are using TCP or UDP?. And which ip sec protocol header you a re using AHS or ESP or AH with ESP, then which ports you are using? , this AH is not the actual AH ESP will come with option that it also provides ESP with AH as we cal, by default it is you are going to select this one SA here it is bit limited than AH we are going to have here , the ah will be authentication of ESP but it will include upper layer protocol as well, protocol address, source and destination port address ,what are the different kind of port address?.. I will explain again as this is mixed with undergrad class , I will explain again , we need couple of address in CN and the first address is physical connection address, as like im connecting to this connection address. And it is connected to this router and that address is called mac address and it comes from network card that you are using, to change the mac address you must change the network card and it is unique for every machine al around the world, I identified the machine address and lets say its number 3 lets say this network is internet how am i going to find this machine in the network so I need ip address so this helps in setting up the work station on the network, fine, you are sending email to this machine and email is displayed on the machine , how can I know that incoming packet is email, port address are going to help us to find the address on the ip, 3 major addresses I will be able to fine physical connection and the machine itself and the application on the machine, the network works like that so this guy wants to know which application you are using are you guys sending email or telneting you are using out network something like that , you don't know the destination by checking the mac address , it is as I said those address are meaning for local meaning and you know that ip address for that you should know the ip address , and then I will use ipv6classes what are they , ?.. are you familiar?.. Im going to try to explain that on , why we need ipv6?..what was the size of ipv4?32 bit for ipv4 but we have lot of machines connected to ip address ,everyone require ip address and they ran out of ip address and to increase the size of ip address they started ipv6 , size is 128 bit source and destination in ipv6 , it comes something like this ,these are 32 bit words and there is version number and there is DS and it is differential service, and there is ECN ,what is ECN, explicit congestion modification, flow label and payload length ,and next header and hop limit, and then source address 1,2,3 and destination address this is the overall structure of ipv6, and the version is going to ipv6 and what is DS?. Differential services remember in ipv4 we had different services , and then you had t o forward the packet to destination , don't drop this packet or drop this packet or give priority to this packet all this kind of information will go there , this ECN is going to solve congestion problem ,so

you are going to priority to those again saying that if it congested give this priority , don't loose this stuff and those kind of things, so its going to define ht type of services , flow label and this flow label and ECN and DS will define flow related problems and the payload length right here is going to define the length o f the payload and the next header is the upper layer header Is the upper layer header that we are going to see, and hop limit is the number of visits that you are making to the router until you reach the destination ,time to live in ipv4 is same thing and source and destination address is 128 bits and this is the overall structure of ipv6 ,but ipv6 comes with header and those header are hop by hop header , routing header, fragment header, and authentication header ,ESP header and destination option header, you may ask this question , remember ipv4, , we are fragmenting the data when you do that how do we assemble that ,remember we said some methods in ipv4 , offset to fragment field and we are using those kind of stuff to resemble the data, , the function over here , what is the problem ,are we not forwarding the data using ip , yes we are , there are fragment header and other header it will be part of ipv6 and next header you can define next header that you can use, hop by hop it is going to have special option for hop by hop ,remember strict routing mean routing in ipv6 this is going to be the header that says route this packet for special condition or specially handle this packet for this condition , its going to be with the flow label which will define the routing , AH and ESP is a part of ipv6 and w call it IPSEC{question from a student}, this is destination address, in routing address you can say I n hop by hop you can do this actually , so its called hop y hop processing generally we are not doing that ,if we are dealing with the multimedia traffic and al those kind of stuffs and these guys will tell, handle this packet when you receive like this , consider the congestion , come from flow , coming from this kind of services, DS, ECN, AH ,ESP ,all this kind of services , will come from this , only one type service, right now real time traffic, real time betrayed traffic these are big time things and you cannot handle this variable traffic in ipv4 in ipv4 we just gave only one connection to bandwidth and we were using that bandwidth , bandwidth requirement changed while im using so dynamically you have to assign me bandwidth , but dynamical not statically that's why atm plays a important role in transferring message , with ipv6 , you can watch tv on your comp and you can very nice voice transfer and you will have live tv and live transmission on your comp ,these are possible due to this guys so there are lot of things about these guys , what is the order this guys are appear in ipv6the first one is ipv6 header, followed by hop by hop, and destination options , routing header ,and fragment header ,AH and ESP and this is the order, 8 destination option header, these are version appear on the ipv6 packet when you receive the the ipv6 , depending on what type of transmission you are doing you can transmit the header, based in IPSEC, so this ipv6 and IPSEC is part of ipv6 because we are we are going to use 2 headers to make ipv4 secure, you can skip, these header number of headers that are there depends on the way you are transmitting the data, into other words the requirement of data ,each one of them are of different length may be payload length or total length ,header info and next header info these guys they are going to define all those things basically, , but asi said you may no have all the header, if you need some thing for routing , you will not do it , what you to do is use destination address for routing , all of them needs destination address, for fragments if you are not using the fragment data and you are using special something ,there will be no fragment header in ipv6 , todays world is based on ipv6 , with ipv6 how many devices you can address, ?.. 3 to power 128 different devices, it can be connected to the network, they said htat ,this is going to be enough for 1000 years or 2000 years of world all the needs can be accommodated using this 128 keys size, when we access this addressees what will happen most probably we will have ipv8 and

most probably we will use 256 bits , info or may be we are going to change the whole addresses and may be we are going to have new structure of CN, because quantum computing are coming, quantum network are coming , it could be different over there, in our lifetime we will be struck with ipv6 and that is part of the IPSEC part of this protocol in ipv6 we will have flow label and ipv4 will have type of services, flow label kind of service, the most important thing is real time bit rate traffic, if you take the broadband course you will see the details for routing and flow in different networks, atm and can and gigabit internet, we are going to use this SA selectors along with SPI to use the actual my communication we spent almost one hour to describe SA , this is big deal, imagine you are in army or military if you have 100 of users you have to installed everything in each device and establish security association for each users its going to be big deal , so after finishing security establishment based on the parameter we are going to start using the IPSEC, these are all user transparent you don't have to deal with anything, system takes all that information put those things based on those parameters you can change the spi , {question from student}, then you are not able to send unclassified or classified messages you can select whether you want confidentiality for the data you are transmitting or only authentication data but authentication header only you don't have to have confidentiality ,this security association related to that choice, when you transmitting unclassified data you don't have to transfer classified data there will be no classification the SA that you are using is AH if you need the classified data with confidentiality and that with ESP there you can transmit this way each one of them with AH and ESP , there are other things you can nest the stuff and how you can do that I wilt el later , so you can do this by using authentication technique and you got the packet now and you are going to do ESP on authentication data by using another security association this is nested ,but we don't have that kind of stuff, here in one authentication you do authentication and ESP no it is out of question.