COMP9332 Network Routing and Switching
Self-assessed Tutorial for Virtual Private Network

Q1. List the steps involved in a minimum IKE communication that uses XAUTH on a client to VPN gateway connection. For each step specify the activities that take place between an initiator and a responder.

Answer:

Step	Initiator	Responder
1	g^a mod p, crypto proposal, N_i	$Cookie_R$
2	g^a mod p, crypto proposal, N_i	g^b mod p, crypto accepted, N_R
3	EncK(IDI, AUTHI, [cert], child- SA)	EncK(IDR, AUTHR, [cert], child- SA)
4	Both generate key K = f(N_i, NR, crypto, g^{ab}mod p)	
5	EncK(SA proposal, NI, [g^a mod p], Traffic selector])	EncK(SA, NR, [g^b mod p], Traffic selector])
6		Request XAUTH
7	XAUTH Credentials	PASS/FAIL

Q2. Describe the relationship between IKE and ESP.

Answer:
IKE provides the fresh keys for ESP using a IKE Child SA that is established during IKE phase 1 or phase 2. The SAs contain cryptographic algorithms, keys, IVs, lifetimes, sequence numbers and the mode, i.e. transport or tunnel. Thus ESP can perform the protection dictated by the corresponding SA.

Q3. Using a table compare the differences and similarities that exist between L2TP /IPsec and IKE/IPsec. Compare such items as port number, mode , packet structure etc.

Answer:

	L2TP /IPSec	IKE/ IPsec
Port Number	UDP 1701 initially	UDP 500
Mode	Transport Mode	Transport & tunnel
Authentication	Authentication provided by existing IKE/IPsec SA plus PPP Authentication when the L2TP tunnel is first opened.	Two factors: Machine: certificate and shared keys. Optional User: XAUTH password prompt.
Packet structure	IP Header(Original)||Authenticated(ESP Header||Encrypted[UDP header||L2TP header||PPP header||PPP payload(IP datagram)])||ESP auth	AH and ESP have different formats for transport & tunnel mode.
Protection	Tunnel Authentication Privacy protection Integrity protection Replay protection	
NAT compatible	Yes, use of the original IP header permits NAT routing	If NAT-T is supported
phases	Call IKE to establish SA Establish Control Connection Establish a session triggered by an incoming call or outgoing call	IKE SA established using DH. IPsec SA derived from IKE SA. Use different SA's for different conversations.
Layer	Layer 5/2	Layer 3

Q4. Describe the mechanism employed by the sliding window to defeat replay attacks.

Answer:
1) The sender initializes 32-bit counter to 0, increments by 1 for each packet.
2) The recipient maintains a 64-bit sliding window, (minimum size is 32).

3) The sequence number should be the first check on a packet when looking up an SA, and duplicate packets will be rejected.

4) The receiver proceeds to ICV verification when the sequence number is in the sliding window.

5) The Sliding Window should not be advanced until the packet has been authenticated.

Q5. Does tunnel mode cause any problems with NAT?

Answer:
ESP in tunnel mode can be compatible with NAT. However, protocols with embedded addresses (e.g., FTP, IRC, SIP) can present additional complications and application gateways are usually deployed to mitigate the complications.