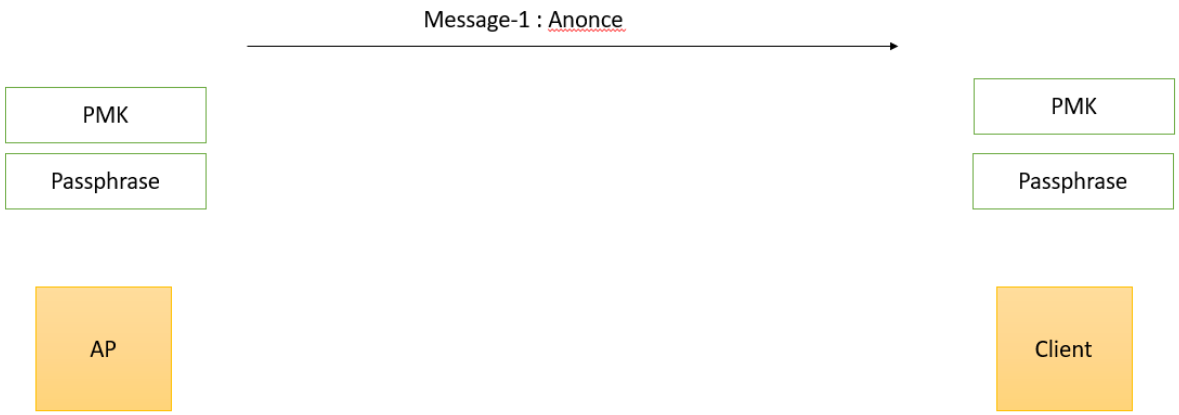
Answers for session 4b - Authentication and Encryption Mechanisms

1. **If the applicant does not send PTK on air to AP then how AP will understand it is the same PTK, which is it has calculated?**

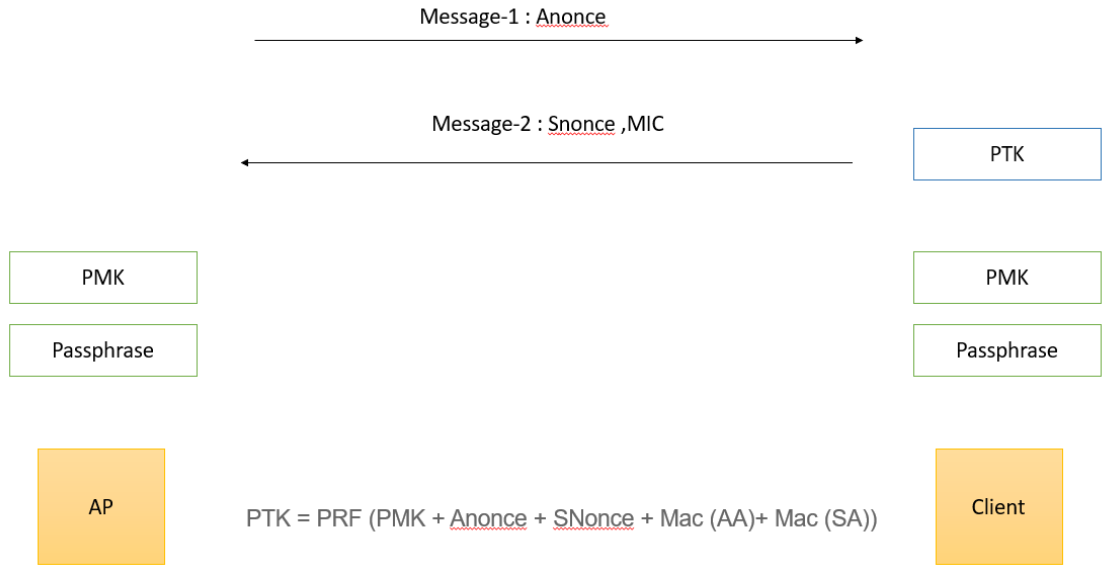
   The client and AP will have the same passwords saved so they will have the same PMK.



After the ‘message 1’ has been sent from AP to the client. The client will calculate the PTK using a pseudo random function.

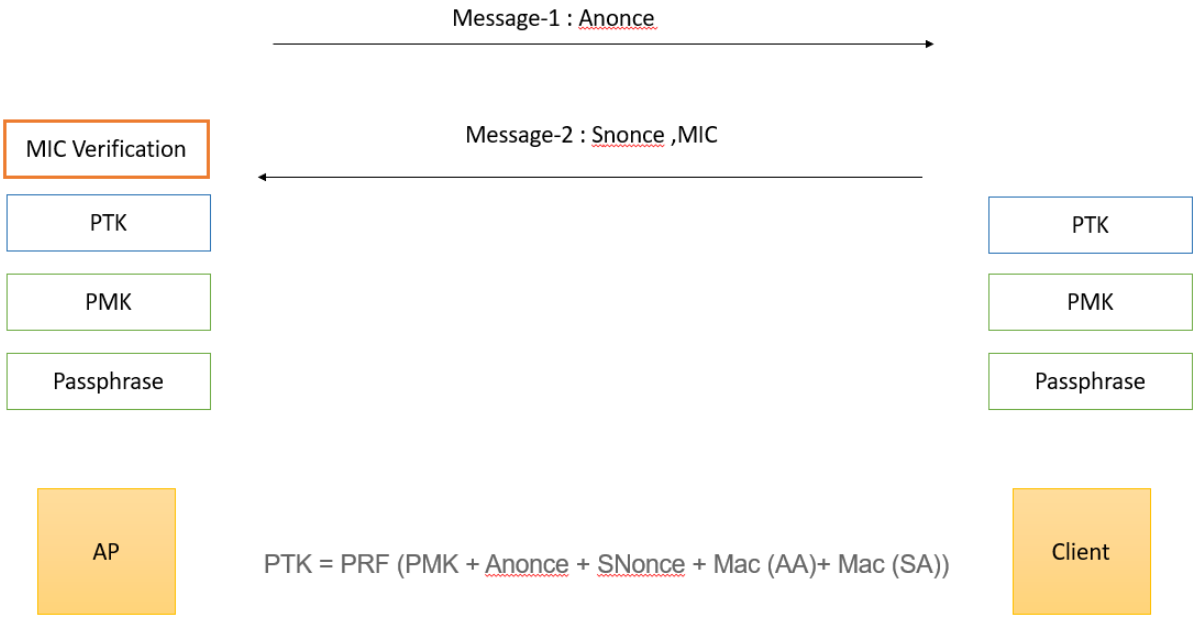
$$PTK = PRF\ (PMK + Anonce + SNonce + Mac\ (AA) + Mac\ (SA))$$

Instead of sending the PTK over the air, the MIC is calculated and will be sent over air.

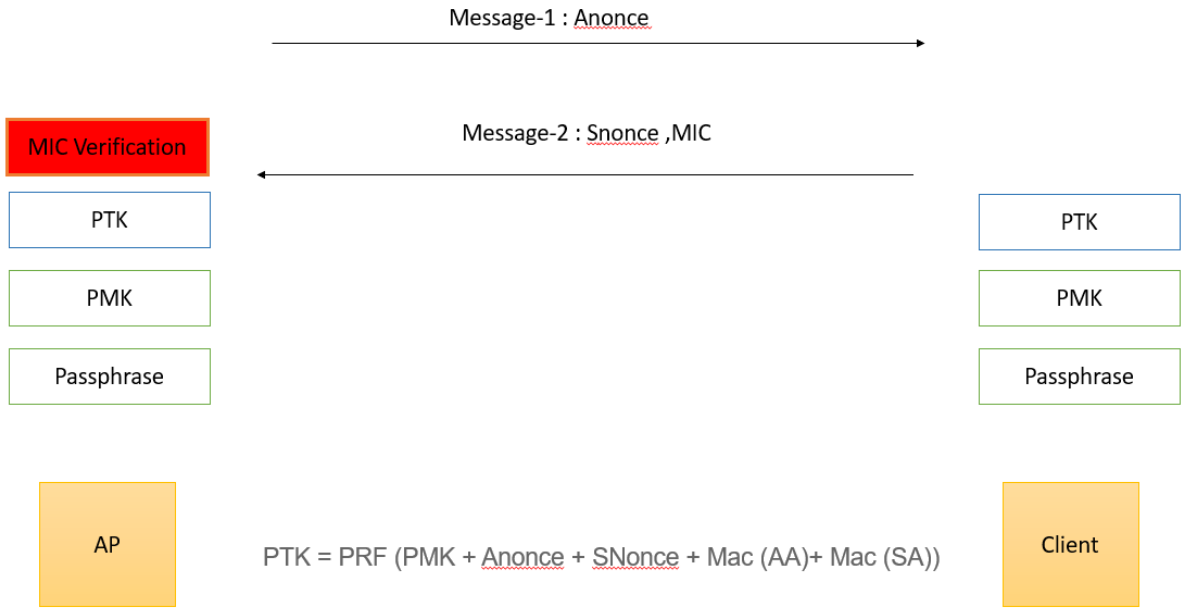


With Snonce, from Message 2 AP will also generate PTK and calculate the MIC internally and compare with the MIC being sent in the Message 2.

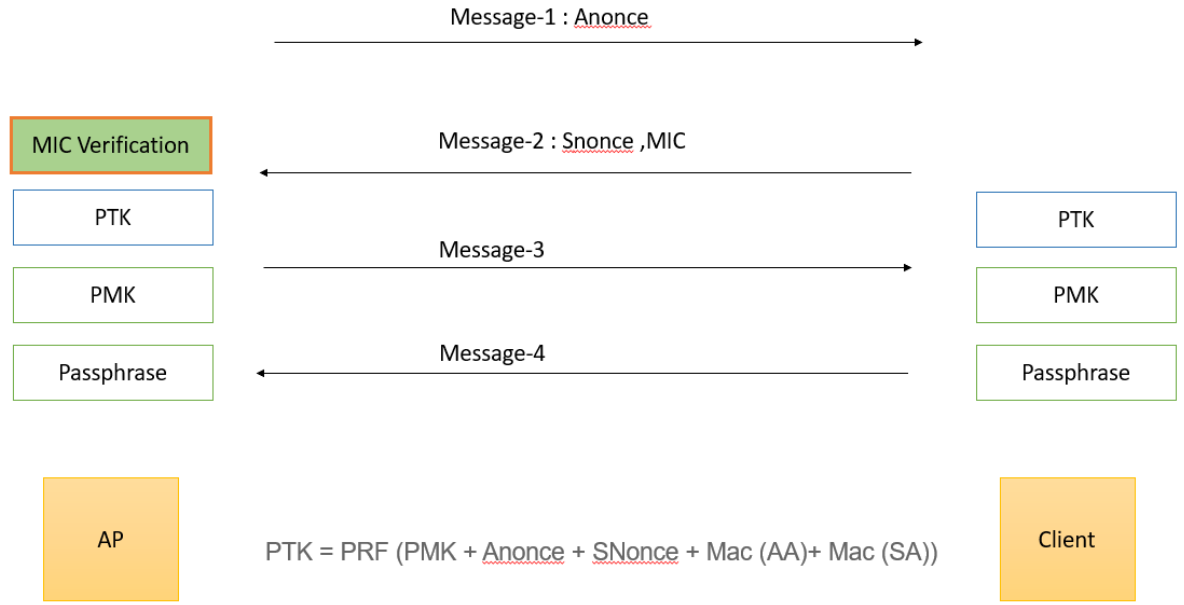
If the MIC matches, we can say the PTK on either end are same.



If the MIC doesn't match:



If MIC Matches, the 4 way handshake completes:



You can refer to: https://www.wifi-professionals.com/2019/01/4-way-handshake

2. When Unicast communication is happening between AP and Client. Why is GTK needed ? At what frame the frame exchange will stop in a four way handshake, when we give the wrong password while associating?

It will stop in the second message, Please refer to answer1. If the passphrase is wrong the MIC verification fails and the 4 way handshake stops after message 2.

3. In Enterprise security if we have 10 devices , do we need to have 10 different username and password ?
We can have the same username and password for all 10 different devices.

4. Is the PMK stored in the AP after the authentication process? Why? Is that used to decrypt the client traffic?

5. How will it generate A-nonce and S-nonce , What is the formula ?

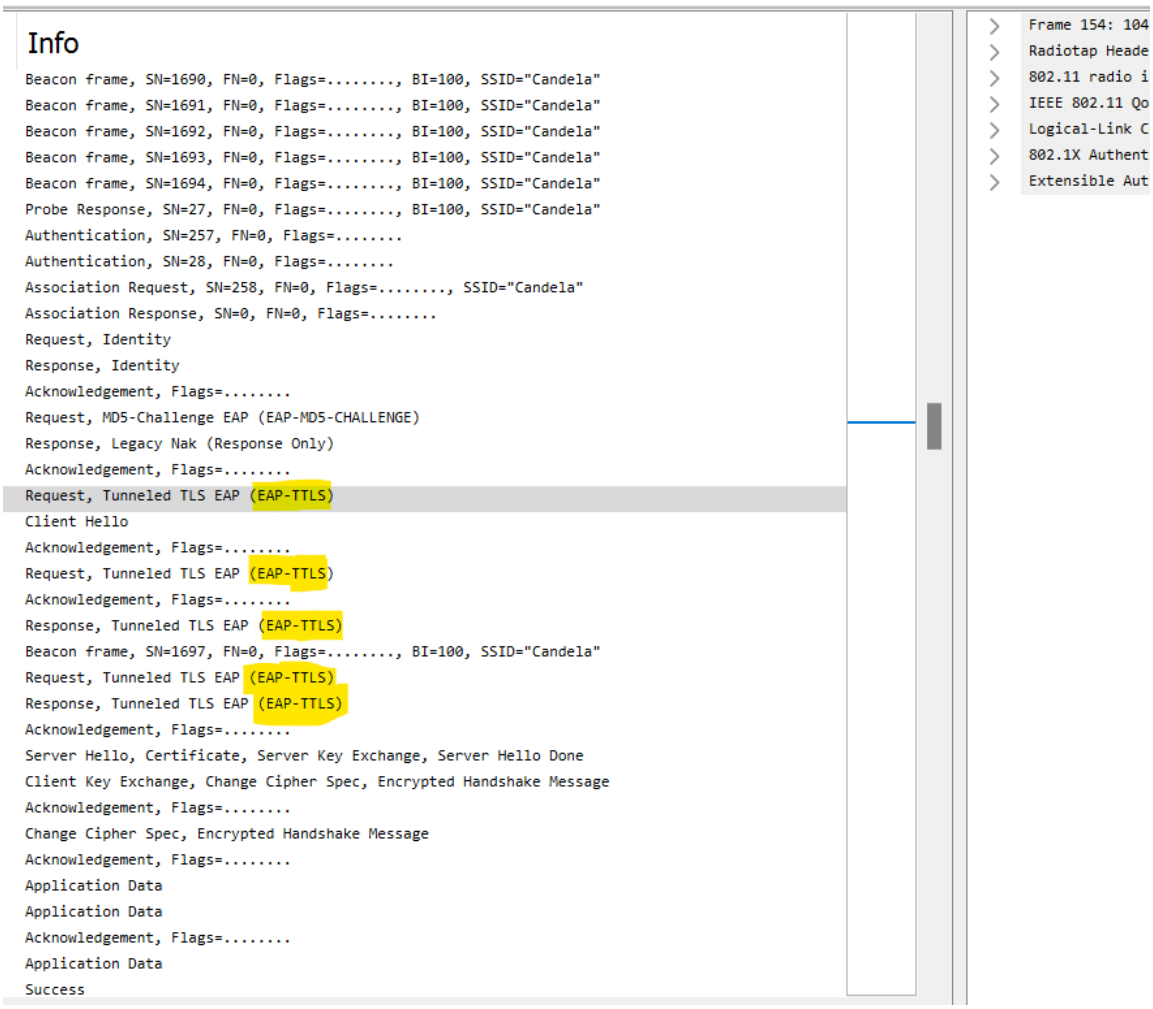
Anonce is a random number generated by an access point (authenticator), Snonce a random number generated by the client device (supplicant)

Generally the random numbers are generated with a pseudo random function.

6. If mic is being sent over air, using reverse process we can create ptk and hence key also ..

7. Is there any method to know the PEAP,TTLS(MSCHAPv1,MSCHAP2,CHAP,PAP ...etc) inner authentications Using Wireshark tool?

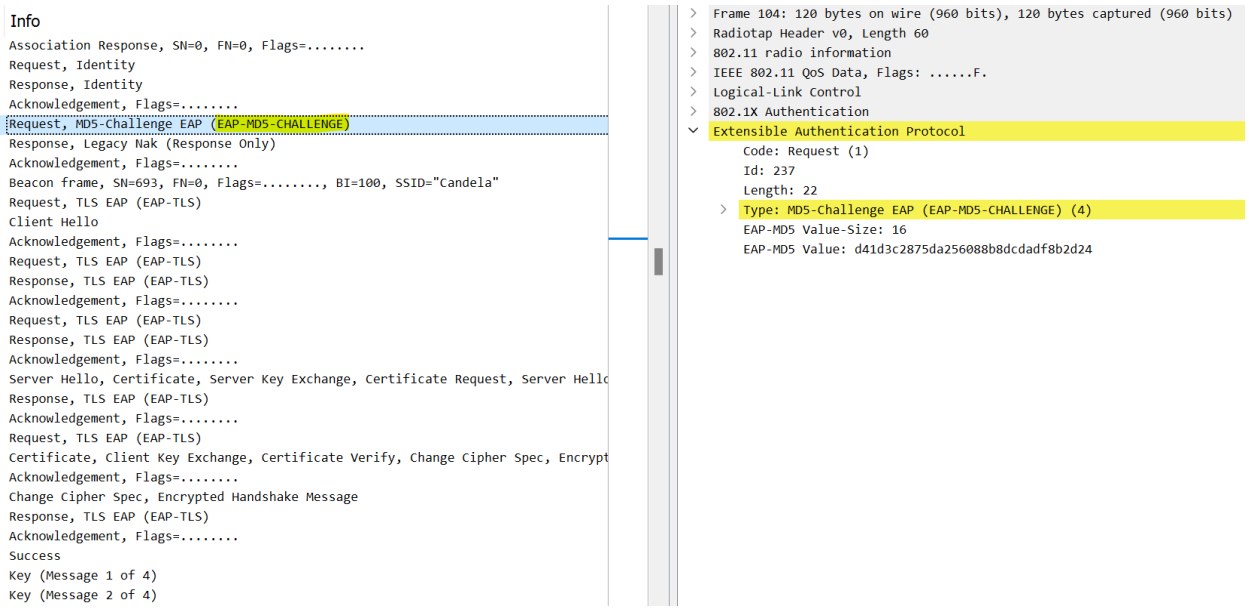
For TTLS:


Info
Beacon frame, SN=1690, FN=0, Flags=........, BI=100, SSID="Candela"
Beacon frame, SN=1691, FN=0, Flags=........, BI=100, SSID="Candela"
Beacon frame, SN=1692, FN=0, Flags=........, BI=100, SSID="Candela"
Beacon frame, SN=1693, FN=0, Flags=........, BI=100, SSID="Candela"
Beacon frame, SN=1694, FN=0, Flags=........, BI=100, SSID="Candela"
Probe Response, SN=27, FN=0, Flags=........, BI=100, SSID="Candela"
Authentication, SN=257, FN=0, Flags=........
Authentication, SN=28, FN=0, Flags=........
Association Request, SN=258, FN=0, Flags=........, SSID="Candela"
Association Response, SN=0, FN=0, Flags=........
Request, Identity
Response, Identity
Acknowledgement, Flags=........
Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
Response, Legacy Nak (Response Only)
Acknowledgement, Flags=........
Request, Tunneled TLS EAP (EAP-TTLS)
Client Hello
Acknowledgement, Flags=........
Request, Tunneled TLS EAP (EAP-TTLS)
Acknowledgement, Flags=........
Response, Tunneled TLS EAP (EAP-TTLS)
Beacon frame, SN=1697, FN=0, Flags=........, BI=100, SSID="Candela"
Request, Tunneled TLS EAP (EAP-TTLS)
Response, Tunneled TLS EAP (EAP-TTLS)
Acknowledgement, Flags=........
Server Hello, Certificate, Server Key Exchange, Server Hello Done
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Acknowledgement, Flags=........
Change Cipher Spec, Encrypted Handshake Message
Acknowledgement, Flags=........
Application Data
Application Data
Acknowledgement, Flags=........
Application Data
Success
Frame 154: 104
Radiotap Heade
802.11 radio i
IEEE 802.11 Qo
Logical-Link C
802.1X Authent
Extensible Aut

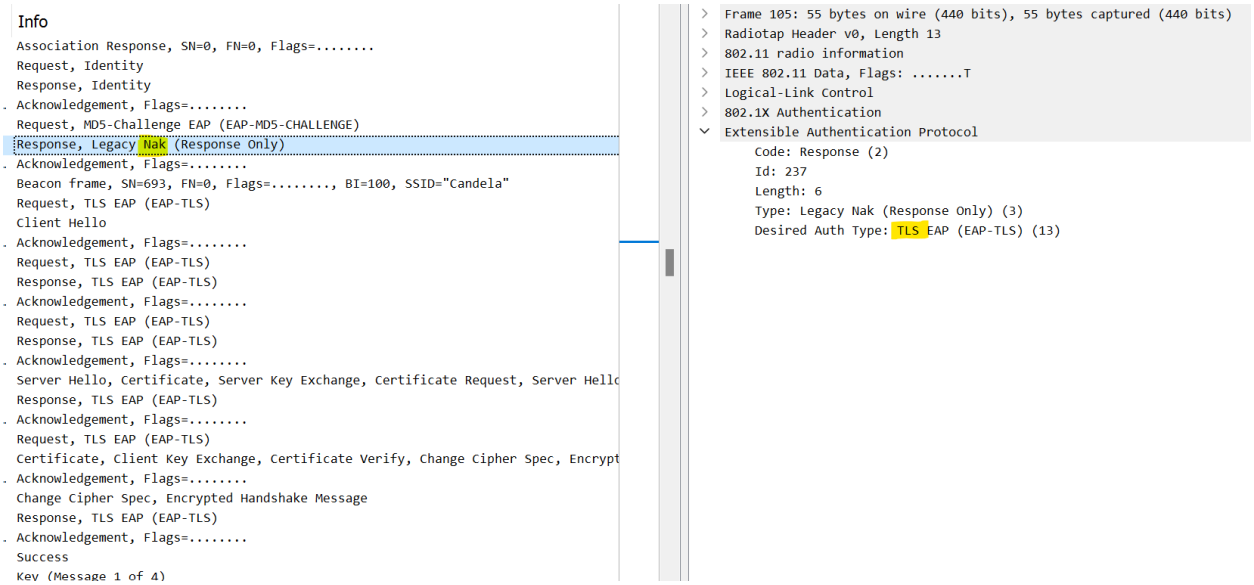
For TLS:

Authentication, SN=257, FN=0, Flags=........	802.11
Authentication, SN=33, FN=0, Flags=........	802.11
Association Request, SN=258, FN=0, Flags=........, SSID="Candela"	802.11
Association Response, SN=0, FN=0, Flags=........	802.11
Request, Identity	EAP
Response, Identity	EAP
Acknowledgement, Flags=........	802.11
Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)	EAP
Response, Legacy Nak (Response Only)	EAP
Acknowledgement, Flags=........	802.11
Beacon frame, SN=693, FN=0, Flags=........, BI=100, SSID="Candela"	802.11
Request, TLS EAP (EAP-TLS)	EAP
Client Hello	TLSv1.2
Acknowledgement, Flags=........	802.11
Request, TLS EAP (EAP-TLS)	EAP
Response, TLS EAP (EAP-TLS)	EAP
Acknowledgement, Flags=........	802.11
Request, TLS EAP (EAP-TLS)	EAP
Response, TLS EAP (EAP-TLS)	EAP
Acknowledgement, Flags=........	802.11
Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done	TLSv1.2
Response, TLS EAP (EAP-TLS)	EAP
Acknowledgement, Flags=........	802.11
Request, TLS EAP (EAP-TLS)	EAP
Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message	TLSv1.2
Acknowledgement, Flags=........	802.11
Change Cipher Spec, Encrypted Handshake Message	TLSv1.2
Response, TLS EAP (EAP-TLS)	EAP
Acknowledgement, Flags=........	802.11
Success	EAP
Key (Message 1 of 4)	EAPOL
Key (Message 2 of 4)	EAPOL
Acknowledgement, Flags=........	802.11
Key (Message 3 of 4)	EAPOL
Key (Message 4 of 4)	EAPOL
Acknowledgement, Flags=........	802.11
Data, SN=2055, FN=0, Flags=.p....F.	802.11
Acknowledgement, Flags=........	802.11
Action, SN=1, FN=0, Flags=.p.....	802.11
Data, SN=0, FN=0, Flags=.p.....T	802.11
802.11 Block Ack, Flags=........	802.11
Data, SN=2056, FN=0, Flags=.p....F.	802.11
Beacon frame, SN=694, FN=0, Flags=........, BI=100, SSID="Candela"	802.11

The Request will be sent from the RADIUS Server to AP, That is forwarded to the client.



The request will be by default encryption method. If the client is using other encryption it sends the NAK specifying the inception being used.



Now the request will be sent again with requested EAP method