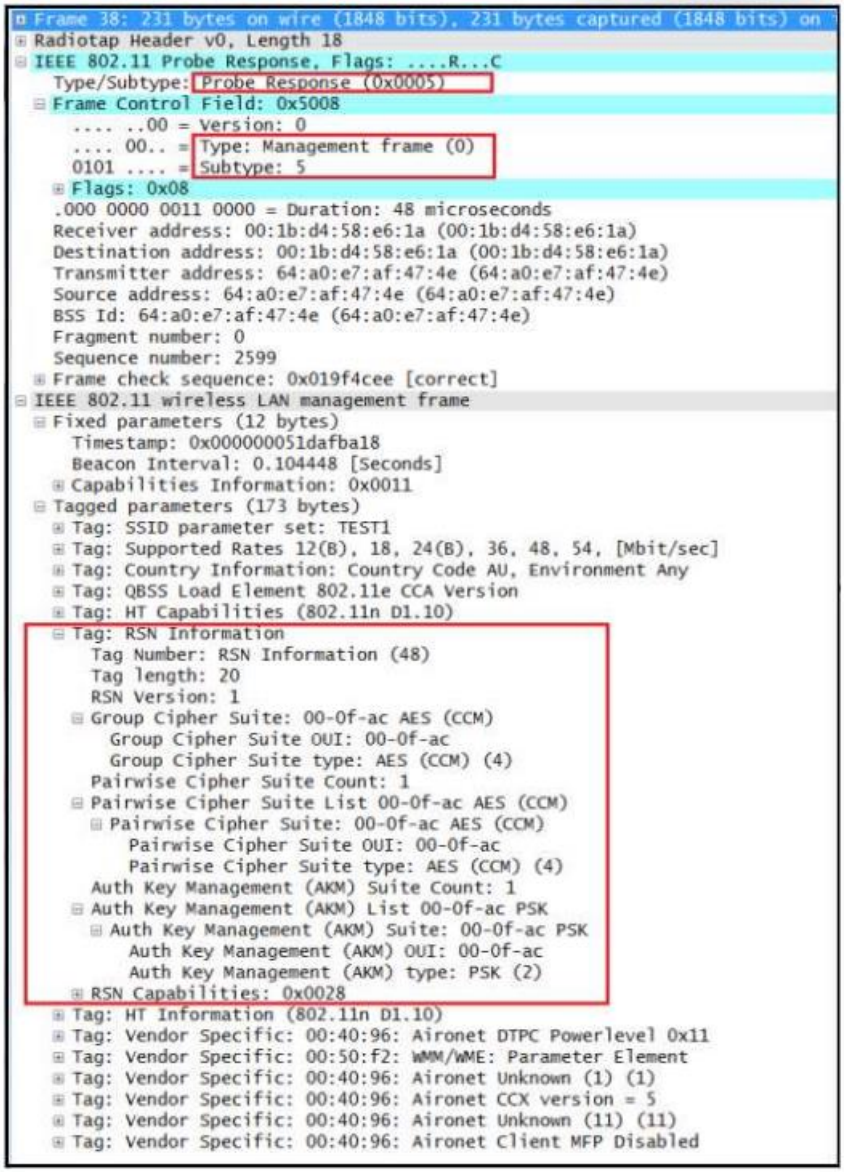

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE
Module 4: Security in Wi-Fi
Session 4b:
AUTHENTICATION AND ENCRYPTION MECHANISMS

RSN Information Element:

For connecting to an Access Point, the client needs to know the capabilities that the access point can support. RSN Information Element is used to advertise the access point capabilities and the security methods it supports. This IE is used by the client to check which security the access point is using.

RSN (Robust Security Network) Information Element in the beacon and probe response an has the following information:

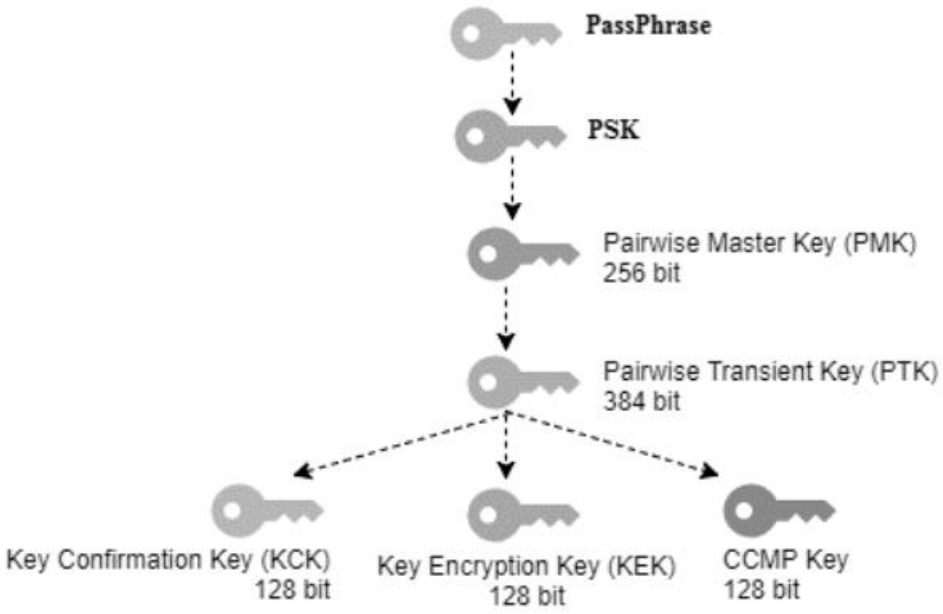
1. Whether the access point is using pre-shared key or authentication server (key management)
2. What group security mechanism is operating
3. A list of one or more pairwise key security mechanisms that are supported



From Passphrase to Key Generation:

In a personal security, where there is only authenticator and a client device. In the AP we can select a security and give a passphrase that can be 8 to 63 characters long. All the clients that would connect to the AP needs to know the passphrase.

1. Passphrase is known to both AP and supplicant.
2. PSK (pre-shared) gets generated from the Passphrase from the following function. We need passphrase and SSID to generate the PSK.
   PSK = pbkdf2.pbkdf2(str.encode(passphrase), str.encode(SSID), 4096, 32)
3. From PSK, PMK (Pairwise Master Key) gets generated from the below function which uses HMAC-SHA1 to encode the data. If an 802.1X EAP exchange was carried out, the PMK is derived from the EAP parameters provided by the authentication server.
   PMK = PBKDF2(HMAC−SHA1, PSK, SSID, 4096, 256)
4. PTK (Pairwise Transient Key) that can be used for only one session can be generated during a 4-way handshake process with a function (customPRF512) and this function expects few values to be passed as a arguments to regenerate the PTK which is the length of 384-bit, and additional 128-bit only for TKIP Configurations.
   PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))
5. PTK Consists of multiple keys they are
   a. KEK (Key Encryption Key) – Used to encrypt the keys such as GTKs
   b. KCK (Key Confirmation Key)– Used during the creation of the MIC, Hash will be generated using KCK.
   c. TK (Temporal Key) – Encryption and decryption of unicast packets.
   d. MIC Tx – Only used with TKIP configurations for unicast packets sent by access points.
   e. MIC Rx – Only used with TKIP configurations for unicast packets sent by clients.



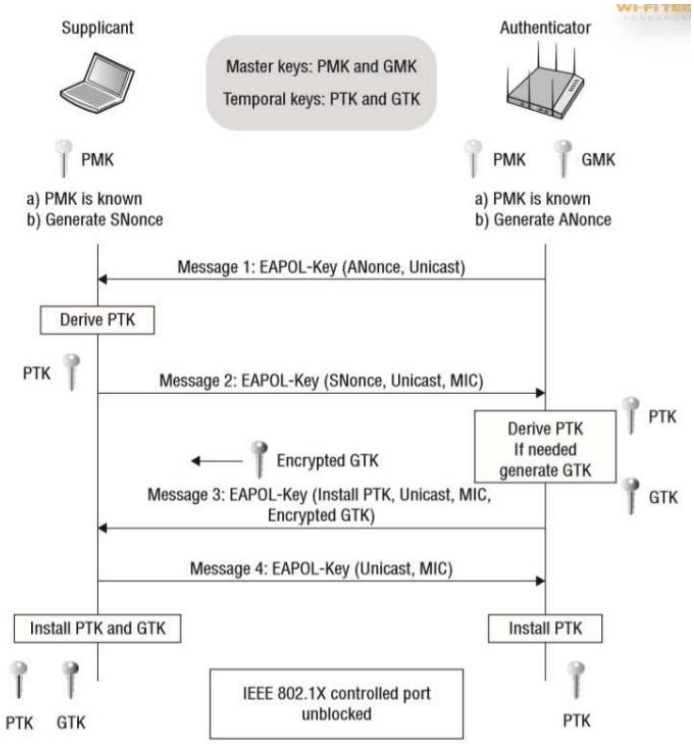
The 4-way Handshake Process:

The PMK (Pairwise Master Key is present with both the supplicant and the Authenticator generated based on the passphrase. The client generates SNonce and the AP generates it ANonce which are a random sequence of bits.

Then the 4-way handshake process happens as follows:

1. Message 1: The authenticator sends its Anonce to the supplicant. The supplicant now has all the information needed to generate the PTK using the pseudo-random function.
   PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))
   The PTK protects the unicast data traffic and is not transmitted.
2. Message 2: The supplicant will send its SNonce to the authenticator. The authenticator now has all the information needed to generate a matching PTK using the pseudo-random function.
3. Message 3: The authenticator generates the GTK from the GMK and transfers the GTK to the supplicant. The GTK is encrypted using the KEK i.e., present in PTK and a secure exchange takes place. The GTK protects the broadcast and multicast traffic.
4. Message 4: An acknowledgement that the client has successfully installed the PTK and GTK.

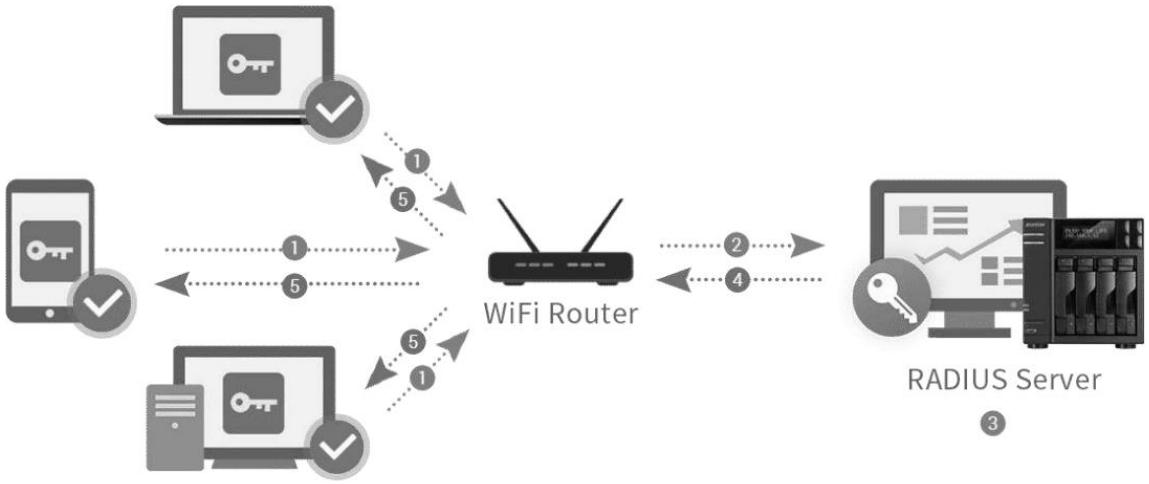
Now the information can be shared by encrypting using the generated keys and can be decrypted at the authenticator using the keys generated at Access point.



Server Based Authentication:

In an enterprise security, it is difficult to install the keys in the clients of all the access points present.

1. A possible solution for the security problem is maintaining centralized key servers like a RADIUS server for centralized key generation and distribution.
2. This would reduce the overhead of maintaining the key information of all the clients at the AP as instead they will be handled by the centralized server (Radius server).
3. With RADIUS, authentication is user-based rather than device-based that is the client enters a username and password instead of passphrase – for example, a stolen laptop does not necessarily imply a serious security breach
4. RADIUS eliminates the need to store and manage authentication data on every AP on the WLAN, making security considerably easier to manage and scale



Radius Server:

RADIUS (Remote Authentication Dial-In User Service) is one of the most used Authentication served and is a networking protocol used to manage Authentication, Authorization, and Accounting (AAA) for remote users who access a network service. It provides a centralized means of managing network access control and can be used to authenticate users connecting to a network through a variety of devices, including routers, firewalls, and VPNs.

The RADIUS protocol uses a RADIUS Server and RADIUS Clients and provides 3 major services like:

1. Authentication - This refers to the confirmation of the user which can be accomplished via presenting identity and credentials (for example: username and password or OTP or digital certificates.)
2. Authorization - This refers to the granting of specific types of services or resources based on the authentication process of the user. This helps in giving restricted permissions to the users. These restrictions may be based on the physical location, IP address, or time of access.
3. Accounting - This refers to the tracking of consumption of resources by the users. This feature can be used independently of RADIUS authentication or authorization. This may be used for management, planning, billing, etc.

Digital Certificate:

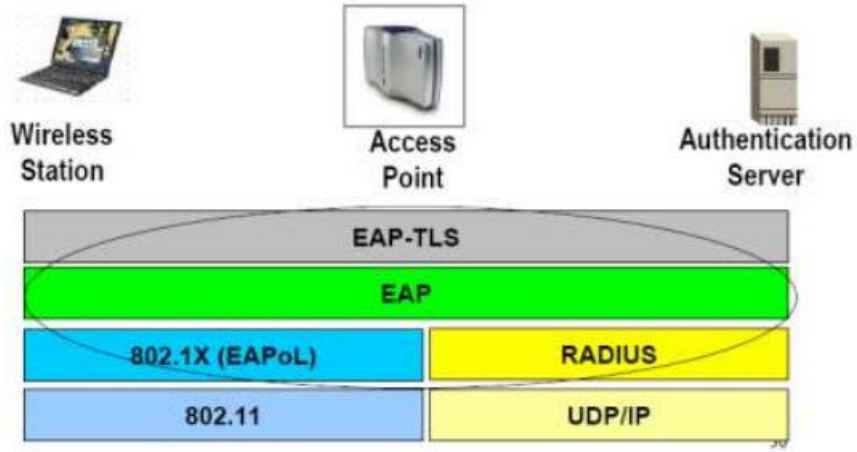
A Digital certificate is used to authenticate between the client and the authentication server. A Digital Certificate is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate.

Digital certificate contains:

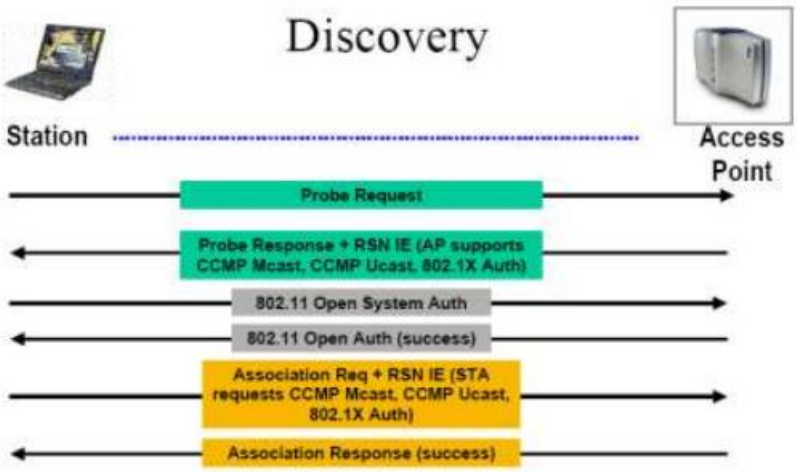
1. Your organization's name and information — The subject field shows that your organization is legitimate and owns the certificate.
2. Your public key — This is the half of your public-private key pair that's publicly known.
3. The certificate issuer's name — This is the name of the certificate authority that issues the certificate.
4. The CA's digital signature — This shows that the certificate was, in fact, issued by a reputable CA.
5. A serial number — This is a code that's unique to your individual SSL/TLS certificate.
6. Your certificate's issuance and expiration dates — These certificates are only valid for a set amount of time — up to 398 days starting Sept. 1, 2020).

Server-Based Security: 802.1x / 802.11i\

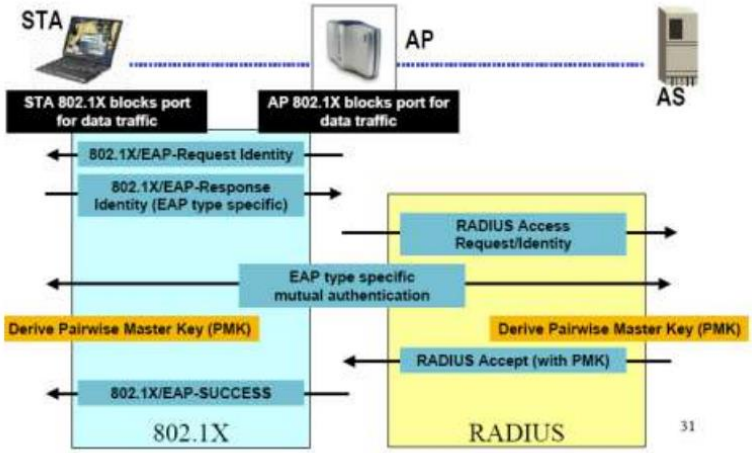
The communication between the access point and the client occurs through the EAPoL (EAP over LAN) on top of 802.11 whereas the data exchange between the access point and the authentication server uses the Radius protocol on top of UDP / IP protocol. This entire end to end communication is referred to as EAP (Extensible Authentication Protocol).



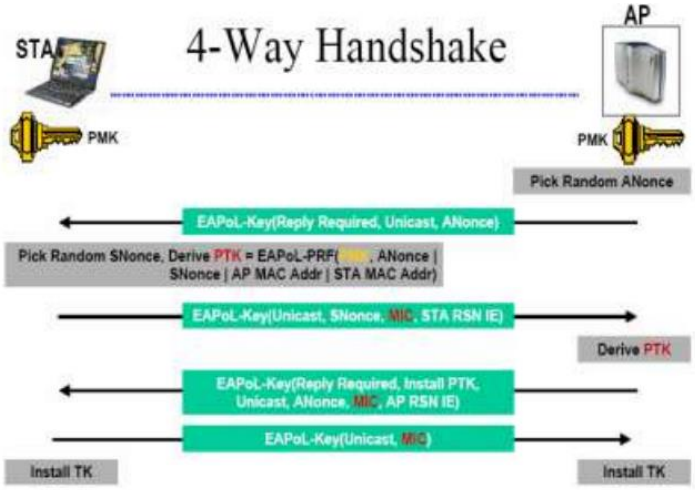
Initially, during the connection first the station sends a probe request to the Access point then the AP sends the probe response having the RSN IE stating the capabilities of the access point like the security it supports etc. Then the client gets authenticated and associated to the AP.



Now the client needs to get authenticated with the authentication server, where the client shares its certificates etc to the server where the 802.1x and the Radius protocols are used and the PMK is automatically generated.



Once the PMK is generated the 4-way handshake occurs then the PTK is generated which is used for encrypting the further data.



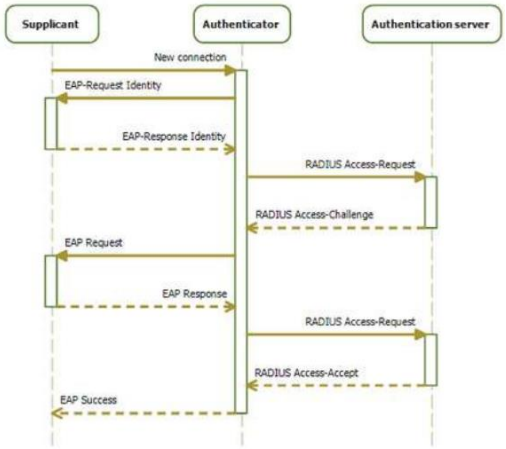
802.1x Authentication:

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over wired IEEE 802 networks and over 802.11 wireless networks, which is known as "EAP over LAN" or EAPOL.

The authentication method begins when the client device requests to connect to the network. The authenticator receives the request and creates a virtual port with the supplicant. The authenticator acts as a proxy for the end user, passing authentication information to and from the authentication server on its behalf.

The authenticator limits traffic to authentication data to the server. A negotiation takes place, which includes:

1. The client may send an EAP-start message.
2. The access point sends an EAP-request identity message.
3. The client’s EAP-response packet with the client’s identity is “proxied” to the authentication server by the authenticator.
4. The authentication server challenges the client to prove itself and may send its credentials to prove itself to the client (if using mutual authentication).
5. The client checks the server’s credentials (if using mutual authentication) and then sends its credentials to the server to prove itself.
6. The authentication server accepts or rejects the client’s request for connection.
7. If the end user is accepted, the authenticator changes the virtual port with the end user to an authorized state allowing full network access to that end user.
8. The client’s virtual port is changed back to the unauthorized state at log-off.



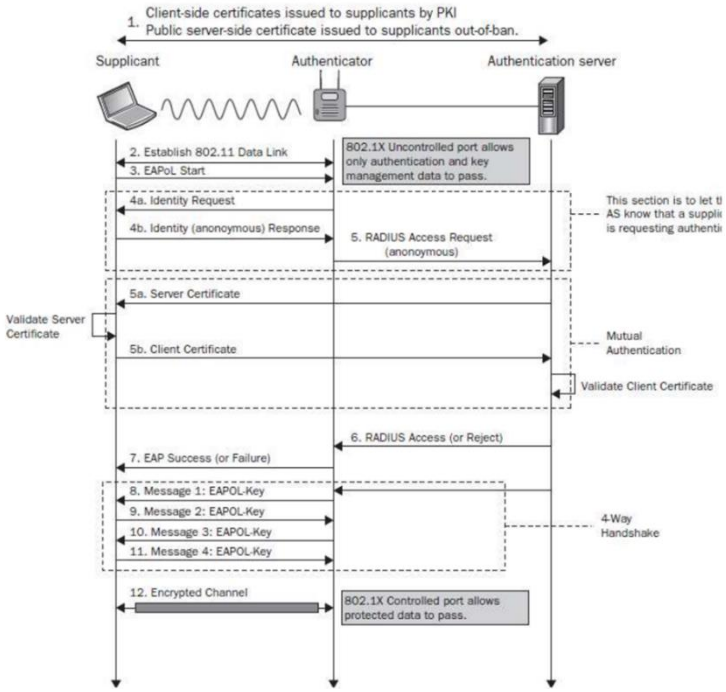
EAP-TLS Method:

One of the most used EAP methods is the EAP-TLS method and it follows the below procedure for authenticating a client.

1. Client-side certificates issued to supplicants by PKI, Public server-side certificate issued to supplicants out-of-band.
   The supplicant and the authentication server begin by saying “hello” and prepare their certificates for authentication to establish a trusted connection.
2. Establish 802.11 Data Link
   The supplicant establishes a connection to the authenticator. This will allow for a secure exchange of information between the two parties.
3. EAPoL Start: EAPoL (Extensible Authentication Protocol over LAN) indicates that information can be exchanged between all three parties over a secured LAN channel. Additionally, this is where the authentication method is determined – in this case, EAP-TLS.
4. Identity Section
   Identity Request : The supplicant requests the identity of the authenticator to ensure it is sending the client certificate to the correct place.
   Identity (anonymous) Response: The authenticator requests that the supplicant identify itself.
5. RADIUS Access Request (anonymous)
   The information that identifies the supplicant and authenticator is sent to the RADIUS to confirm their identity and allow for authenticating information to be sent.
   1. Server Certificate: The RADIUS sends its server certificate to confirm its identity through server certificate validation
   2. Client Certificate: The supplicant validates the identity of the authentication server certificate. After validation, the supplicant sends its client certificate.
6. RADIUS Access (or Reject): The RADIUS authentication server receives the client certificate and authenticates its identity as an approved network user.

Depending on the user's certificate, the RADIUS sends an Access or Reject message to the authenticator.

7. EAP Success (or Failure): Based on the RADIUS Access or Reject message, the authenticator sends a Success or Failure message to the supplicant to indicate whether they have been approved or denied network access. If the message is Success, the switch port is opened for direct network communication between the supplicant and authentication server.
8. Message 1/2/3: EAPOL-Key
9. Message 4: EAPOL-Key
   The next step is a series of messages known as the EAPOL-Key exchange. It is a 4-step handshake between the authenticator and supplicant that generates encryption keys. These keys are used to encrypt information that will be sent over the wireless connection and ensures that all ongoing network communications are encrypted and cannot be read by outside parties.
   Linked here is a detailed list of keys that are generated during this handshake.
10. Encrypted Channel:
    The end result of EAP-TLS authentication is an encrypted channel of communication. The user is ready to access the secure network and utilize all resources available to them.

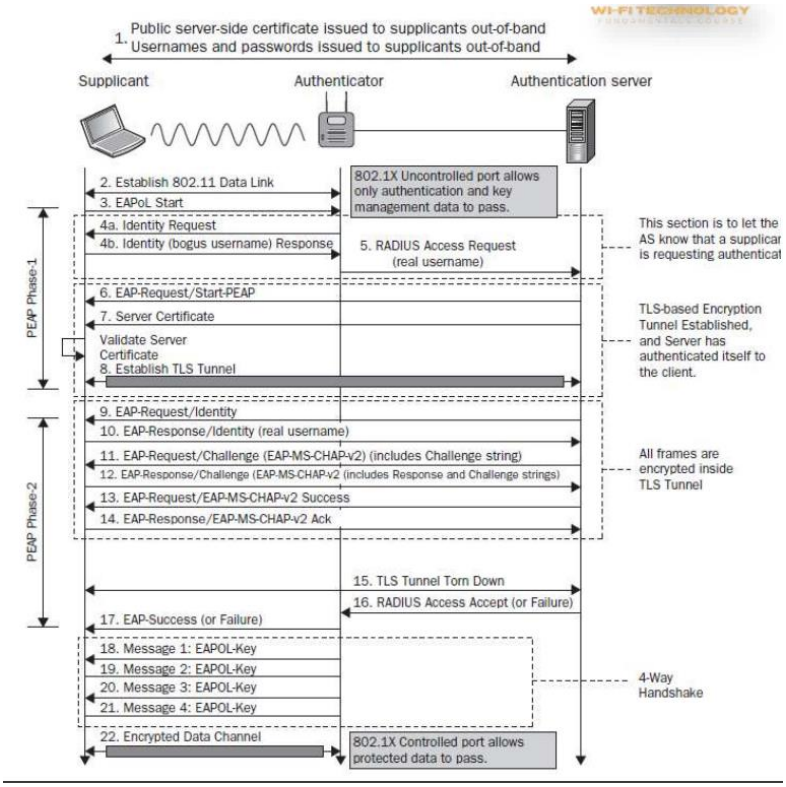


EAP-PEAP Method:

There are other EAP methods, among which few are challenge based, few are certificate based, few are username password based but having the base process of Authentication as same.

1. Developed by Microsoft, Cisco & RSA Security.
2. Referred as EAP within EAP.

3. 3 major versions of PEAP:
    a. EAP-PEAPv0(EAP-MSCHAPv2) => most widely used
    b. EAP-PEAPv0(EAP-TLS)
    c. EAP-PEAPv1(EAP-GTC)
4. PEAPv0 & PEAPv1 refer to the outer authentication method and are the mechanism that create the secure TLS tunnel to protect subsequent authentication transaction.
5. EAP protocol inside parenthesis (i.e. MSCHAPv2, TLS & GTC) is the Inner Authentication/EAP Protocol.
6. Identity (client's username) should not be sent in cleartext, only an "anonymous" identity should be sent to server before TLS tunnel establishment.



Comparison of Various EAP methods:

Module4: Security in Wi-Fi

Session4b: Basics of Authentication and Encryption

Feature	EAP-MD5	LEAP	EAP-TLS	EAP-FAST	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)
Server Certificate	No	No	Yes	Optional (can use PAC instead)	Yes	Yes	Yes	Yes
Client Certificate	No	No	Yes (also supports smartcard)	No	Optional	No	Yes	Optional
Supported Client Authentication	MD5 hash challenge response	MSCHAPv2 challenge/response	Via Certificate/Smart card	MSCHAPv2, GTC	PAP, CHAP, MSCHAPv2, GTC, Certif.	MSCHAPv2	Certificate	GTC
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Identity Protection	No	No	Yes (anonymous)	Yes (bogus username)	Yes (TLS encryption)	Yes (TLS encryption)	Yes (TLS encryption)	Yes (TLS encryption)
Client Auth in cleartext	Yes (sniffing possible)	Yes (sniffing possible)	No	No	No	No	No	No
Client Auth Handhshake offline cracking	Tool eapmd5pass	Tool Asleap	No	Tool Asleap (for MSCHAPv2)	Tool Asleap (for MSCHAPv2)	Tool Asleap	No	Cleartext (inside TLS tunnel)
Evil Twin Attack Possible ?	Yes	Yes	No	Yes if no server's PAC validation	Yes if no server's certif validation	Yes if no server's certif validation	No	Yes if no server's certificate validation