DATE

MODULE V

SECURITY IN CURRENT DOMAINS

Wireless LAN Security

There are two principles types of WLANs (Wireless local Area N/w)

1) Adhoc N/w - Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc nlw don't require a centralized access point (AP). Instead, devices on the wireless nlw connect directly to each other. If you set up the two laptops in ad-hoc wireless mode, they'd connect directly to each other without the need of a centeralized access point

2) Infrastructure WLAN - Most Wifi nlw function in infrastructure mode. Devices on the nlw all communicate though a single AP, which is generally the wireless router. Eg:- if there are two laptops next to each other, they don't communicate directly. Instead they communicate indirectly through the Wireless AP. They send pkts to the AP - probably a wireless router - and it sends the pkts back to the other laptop. Infrastructure mode requires a central AP that all devices connect to.

Access Point (AP)

A wireless AP is a network device that transmits and receives data over a wireless local area nlw (WLAN). The wireless AP serves as the interconnection point blw the WLAN and a fixed wire nlw. Coceptually, an AP is like an Ethernet hub, but instead of relaying LAN frames only to other 802.3 stations, an AP relays 802.11 frames to all other 802.11 or 802.3 stations in the same subnet. When a wireless device moves beyond the range of one AP, it is handed over to the next AP.

DATE

Page No 2

In many organizations, the wired n/w is an Ethernet LAN with an existing security infrastructure that includes an Authentication Server (AS). AAA (Authentication / Authorization / Accounting) functionality is often provided by a RADIUS (Remote Authentication Dial-in User Service) server. Develop protocols that seamlessly integrate the WLAN with the security infrastructure of the wired n/w.

A n/w of wireless station (WS) associated with an AP is referred to as a basic service set. The APs in the different basic service sets are often connected over a wired n/w

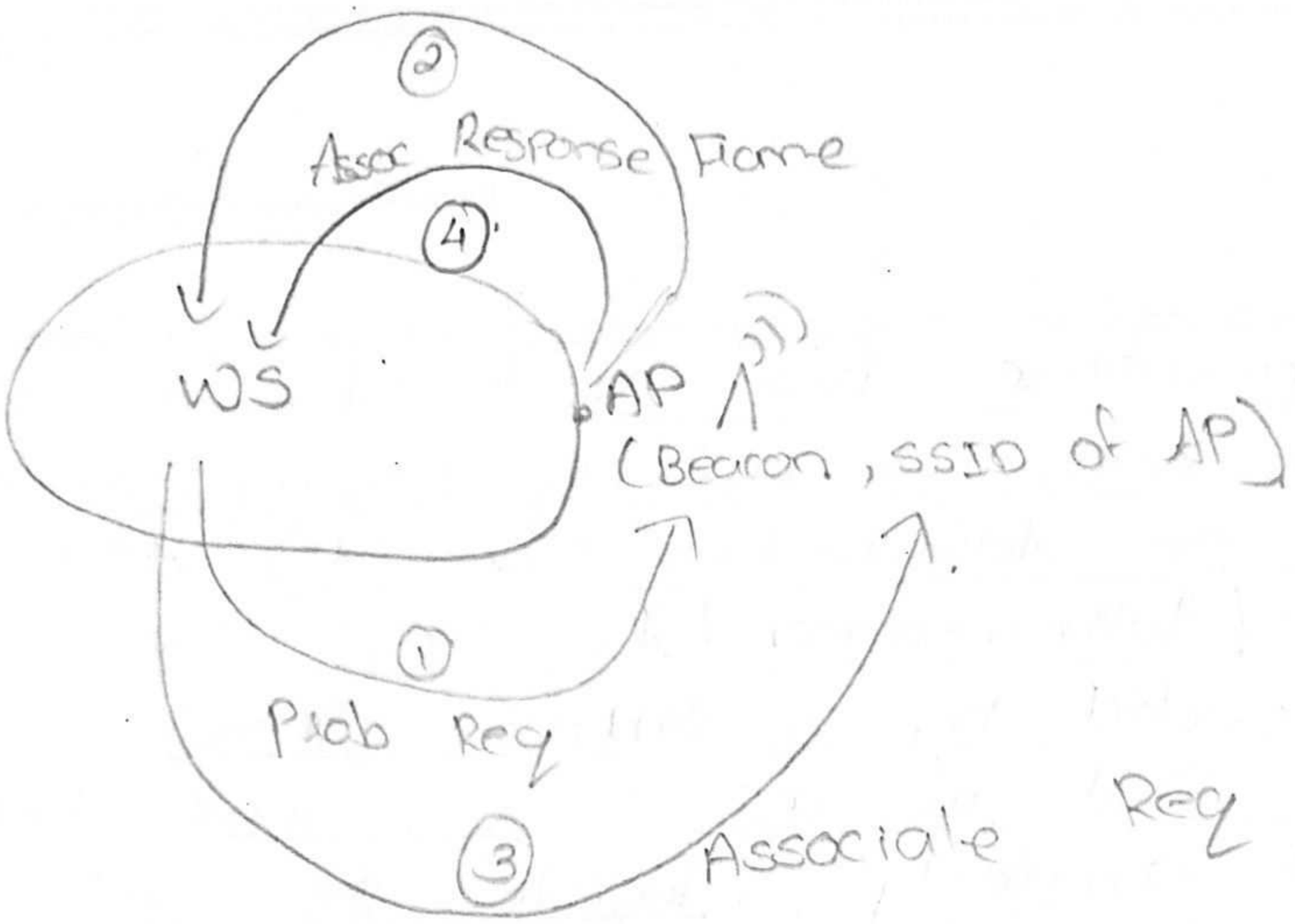
Open Sys Authentication

- Each AP is identified by an SSID (Service Set ID), character string, 32 characters.

- A wireless station (WS) first tries to identify an AP., This is done by monitoring the wireless medium for a special kind of frame called a Beacon.

- Beacon is broadcasted by the AP periodically and it contains the SSID of the broadcasting AP.

RAMSONS



A station may send a Probe Request Frame which probes for APs within the range. An AP on hearing the request, responds with a Probe Response Frame. The Prob Response Frame contains the SSID of the AP and also information about its capabilities, supported data rates etc. TO become part of the WLAN. a station will have to associate with an AP.

A station can associate with only one AP.

A station that wishes to associate with an AP. sends a Associate Request Frame. The AP replies with an Associate Response Frame. Before associating 802.11 requires the station to authenticate itself to the AP.

DATE

Page No 3

Authentication

1) Pre - WEP Authentication

Mere knowledge of the SSID is sufficed for a station to be authenticated to the AP. An attacker could easily sniff the value of SSID from frames such as the beacon or probe response and then use it for authentication.

Another method is to restrict admission to the WLAN by MAC address. Only the stations with permitted MAC can join the WLAN. But the valid MAC address could be obtained by sniffing the wireless medium.

2) Authentication in WEP.

In WEP, the station authenticates itself to the AP using a challenge (nonce) – response protocol.

AP generates a challenge (nonce) and sends it to the station. The station encrypts the challenge and send it to AP. The stream cipher RC4 is used for encryption.

RESPONSE = CHALLENGE ⊕ KEYSTREAMS (S, IV)

RAMSONS

where,

S → shared secret (40-bit)

IV → Initialization Vector (24-bit)

S is common to all stations authorized to use the WLAN.

Drawback

Its possible for an attacker to obtain S, itself by eavesdropping on several challenge - response pairs b/w AP and various stations., an attacker could lauch a dictionary attack and eventually obtain-S.

3) Authentication & Key Agreement in 802-11i

Three entities involved-are.

i) Supplicant / wireless client (wireless station) - Is the one asking for authentication.

ii) Authenticator / controller (AP in this case) - it doesn't doesn't play any role in auth its called the authenticator because its the point where we ask for authentication

iii) Authentication Server - The device that auth the client.

DATE

There are two protocals 802.1x / EAP . 802.1x . - It is role allows the AP to close the RADIUS and not to allows any access to nlw to the supplicant as long as the AS has not agreed to the authentication

- In auth process supplicant asking for authication and then ask for association, at this point the authentication will ask the AS to verify the supplicant / station, only after verifying the supplicant / station will be given access to the n/w.

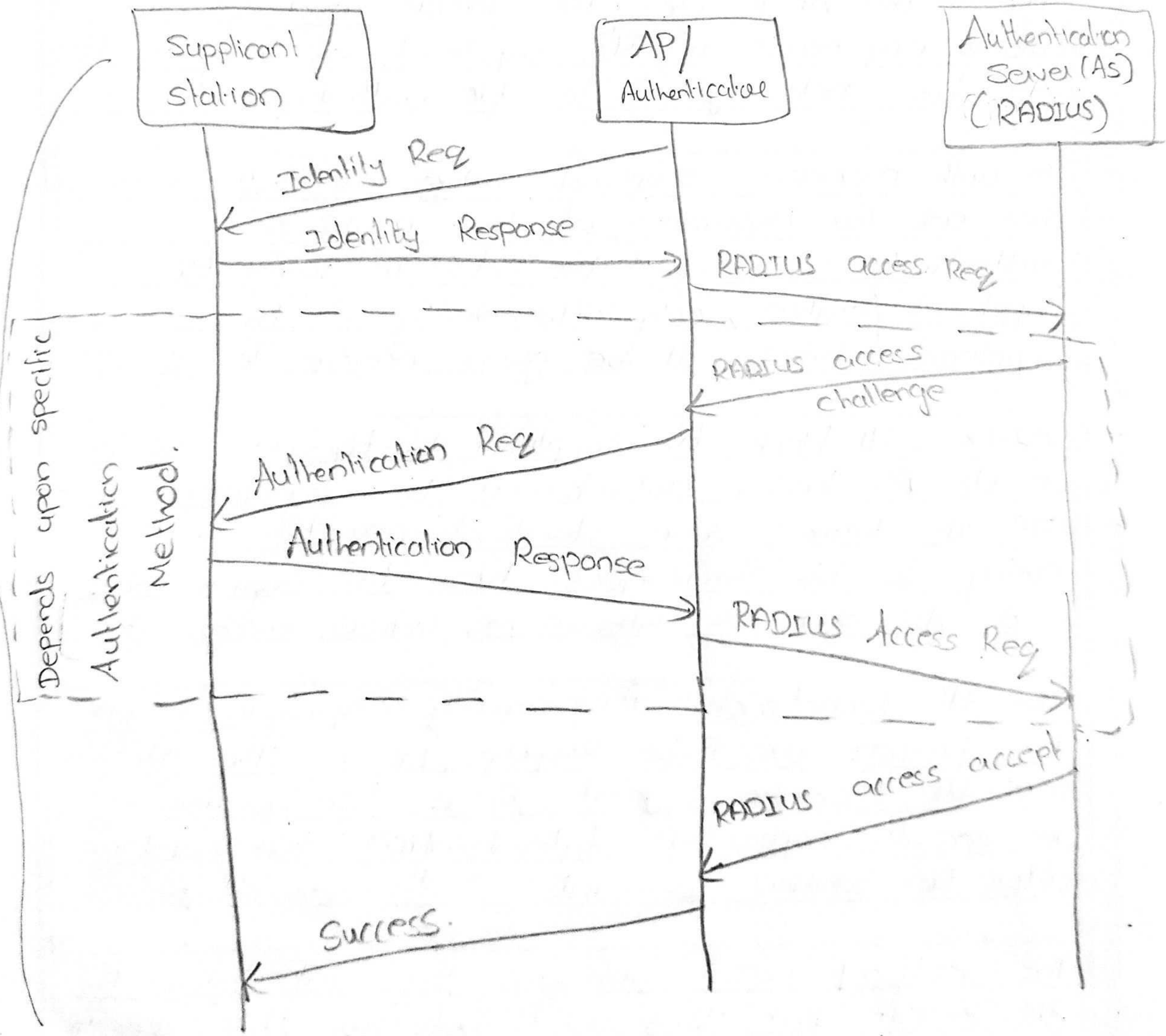
- 802.1x will block the supplicant to the nlw as long as the AS hasn't authenticated the supplicant.
- EAP it defines some standard msg that are going to be exchanged blw the supplicant and As such as Authicate me, failure, success etc.

- The AP broadcasts its security capabilities in the Beacon or Probe Response Frame. The station uses the Associate Request Frame to communicate its security capabilities. Authentication takes place after the station associates with an AP.

The protocol used between the station and the AP is EAP but that used between the AP and the authentication server (AS) depends on the specifics of the latter.

AS is often a RADIUS Server which uses its own msg type and formats.

(RADIUS - Remote Authentication Dial in User Service)



EAP - Extensible Auth Protocol

EAPOL - EAP over LANS

DATE

Page No 5

The main authentication methods supported by EAP are.

EAP - MDS
EAP - TLS
EAP - TTLS
EAP - PEAP.

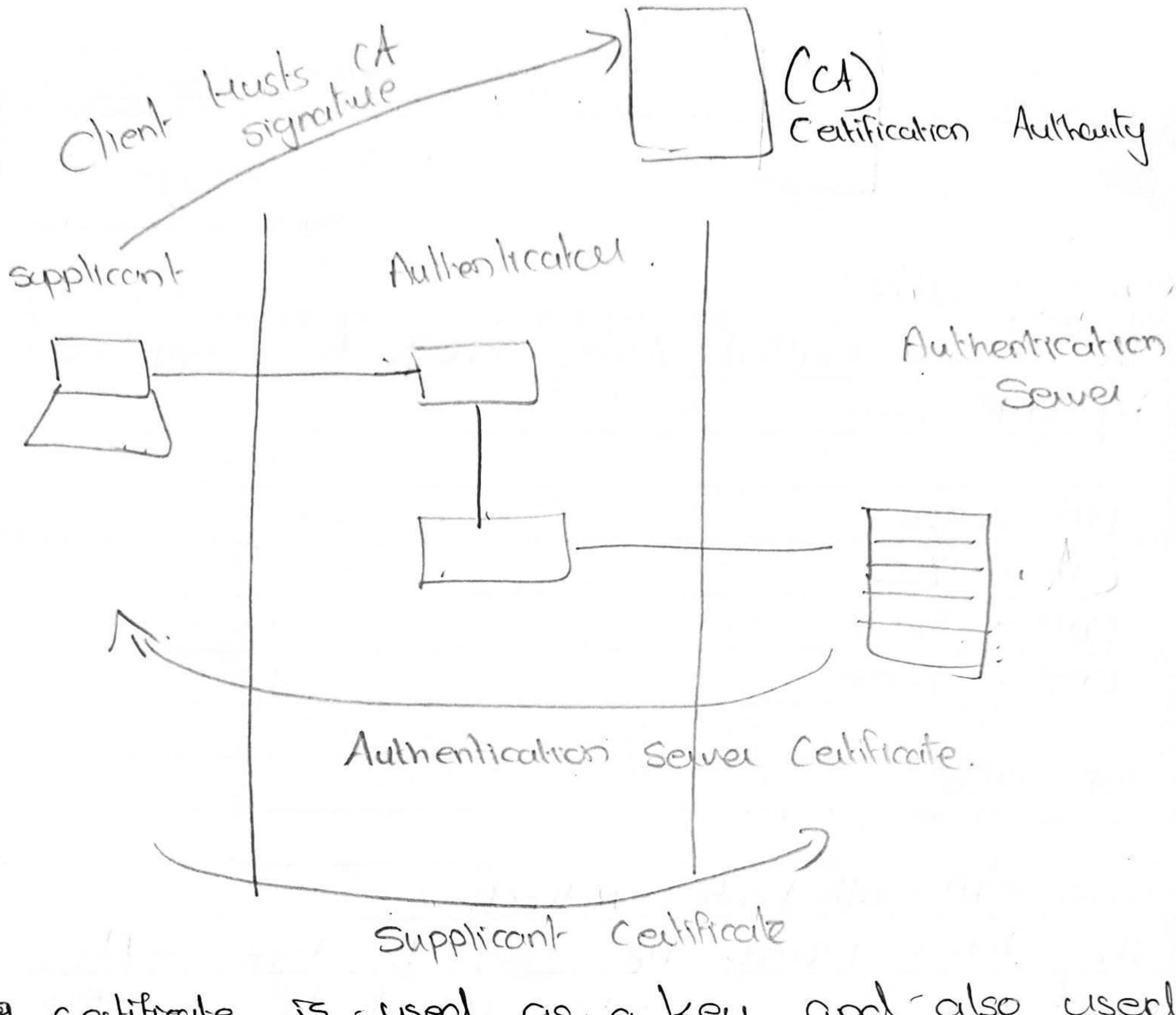
EAP - MDS

- Basic EAP authentication Method.
- The station prompts the user to type his/her pwd. It then computes the hash of the pwd and sends it to the AS.
- Drawback - The attacker could eavesdrop on such msg exchange and then replay the hashed pwd thus impersonating the owner of the pwd.

EAP - TLS

- AP and supplicant uses certificates.
- AP sends its certificate and this certificate is used as a key to encrypt what ever the client needs to send to the server

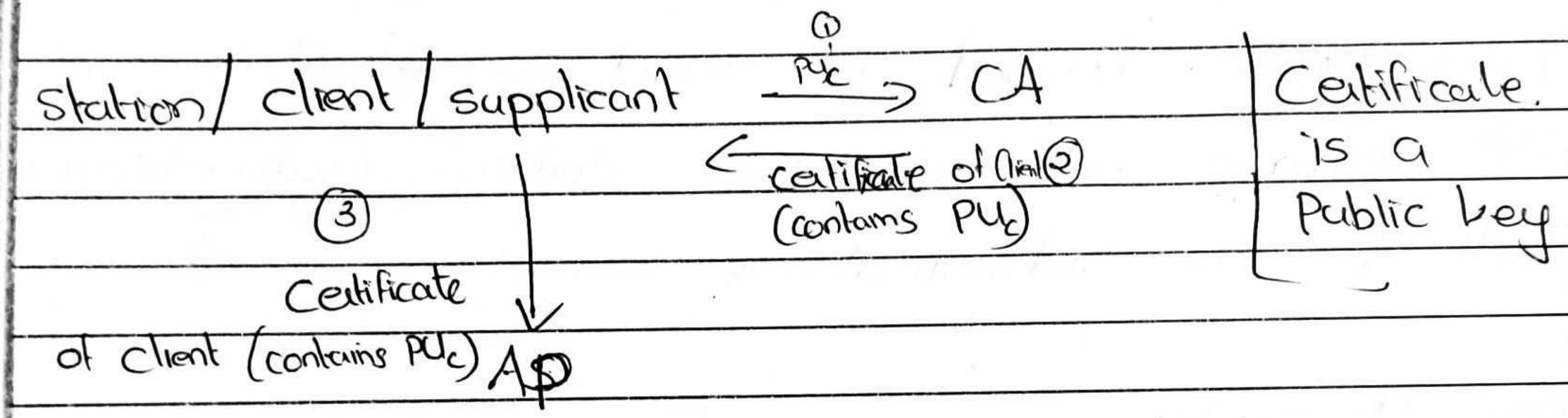
RAINSONS



- The certificate is used as a key and also used to verify (auth)
- Certificate is a public key. When the AP sends the certificate the client has to make sure that it is the certificate from the AP and not from any hacker.
- To ensure the that the certificate is genuine there is an external sever that both the client/ supplicant and the AS trust

⇒ AS it sends it certificate to the certification Authority (CA). The CA is going to verify that certificate

with the signature of the CA. Now AS sends the certificate to the client / supplicant. Now the client can verify if the certificate was verified by the CA. The same process will be done on the client side



Drawback

When there are many no. of clients ~~ver~~ new certificates has to be created and deleted which is very difficult to manage.

EAP-TTLS (tunnelled TLS)

- It requires the certificate only at the AP
- The AP authenticates itself to the station and both sides construct a secure tunnel blw themselves.
- Over this secure tunnel the station authenticates itself to the AP.

- The station transmits attribute - value pairs. such as.

username = ABC

pwd = D#4C

Protected EAP (PEAP)

- Its similar to EAP_TTLS
- The secure tunnel is used to start a second EAP exchange wherein the station authenticates itself to the authentication server.

Key Hierarchy

There are 2 types of keys used in WLANs

① Pairwise keys – to protect traffic b/w station and AP.

② Group key – to protect broadcast or multicast traffic b/w an AP and multiple stations.

- The root of the key hierarchy is the Pairwise Master Key (PMK). This is obtained in any of the ways. either MSK or PSK.

DATE

Page No 7

- The station and the AS may agree on Master session key (MSK) as part of the authentication Procedure. The AS communicates this key to the AP. The AP and station then derive the PMK from the MSK.

- Alternate way for generating PMK
To compute a fresh PMK for each session the Pre-shared key (PSK), which is used as the PMK. One possibility is for each station to be configured with the PSK. While the PSK approach is easier to administer it is much less secure than generating fresh Master keys. for each session.

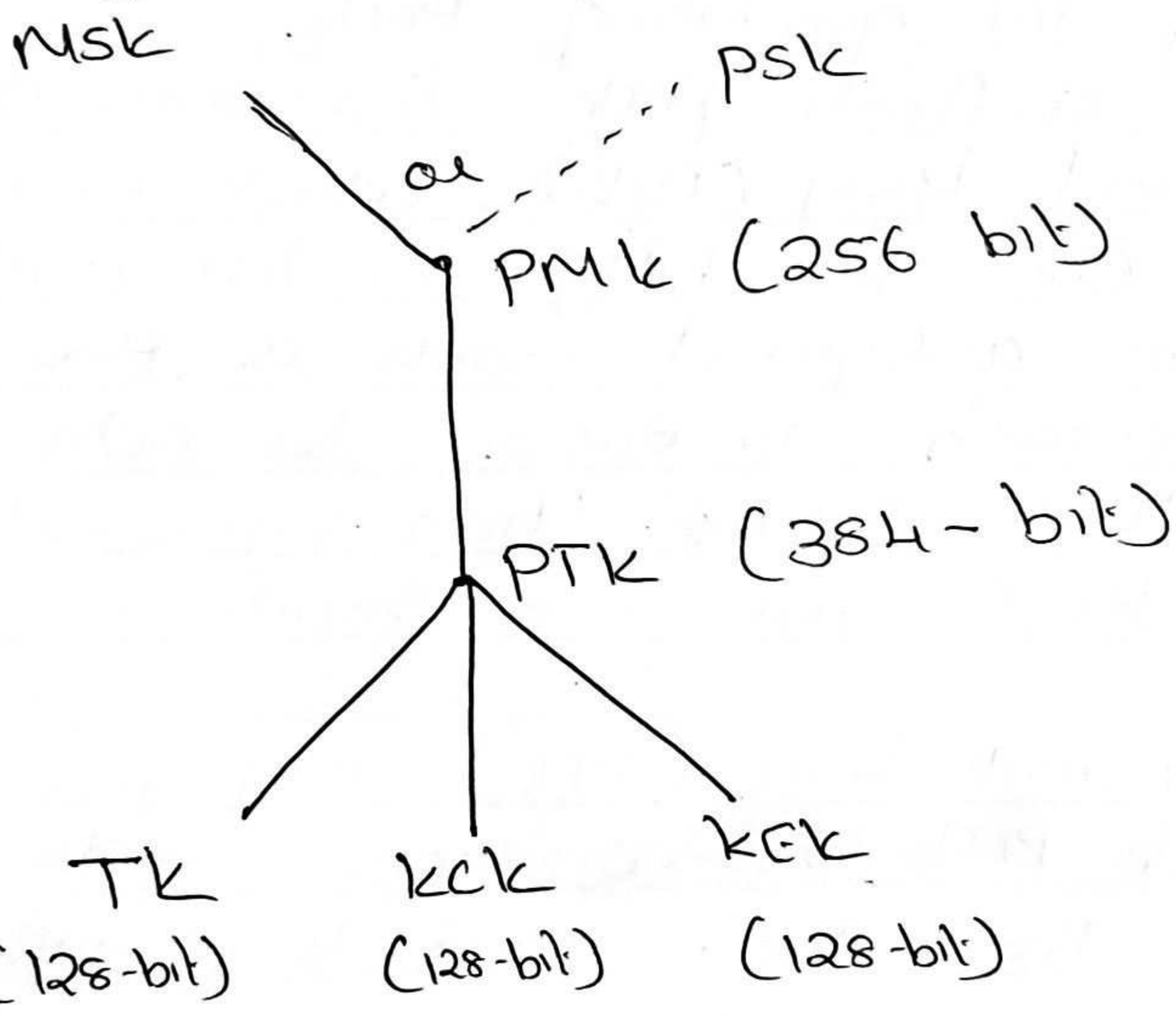
- Pairwise Transient key (PTK) is a pseudorandom function of the PMK, two nonces chosen by the AP and the station and their MAC addr.

- 3 chunks extracted from PTK.

(1) Temporal key (TK) - used for encry & integrity protection of data b/w the AP and station.

② Key Confirmation key (KCK) - used to ~~integ~~ integrity - protect some msg in 4-way handshake
Integrity - protect is supported by MAC compiled fn.

③ Key Encry key (KEK) - used to encrypt the msg containing the group key.



Four-Way Handshake

- Its a process where some source key material is turned into data encryption material (keys) that can be used to encrypt the data frames.
- Data encry material is the group encryption keys.

DATE

Page No 8

i/p to the encryption keys.

1. PMK (both end pts have it)
2. Nonce (N_A, N_S)
3. MAC of client / station
4. MAC of AP.

Msg1

AP sends the first frame that contains Authenticated Nonce(N_A) which is a randomly generated number used as i/p to the encry keys.

- The station has already calculated its Nonce
- Since i/p 3 and 4 are already available on the wireless medium ∴ the station has all the i/p to create the encryption keys

  $PTK = prf(PMK, N_A, N_S, MAC_A, MAC_S)$

- ∴ The station is going to derive PTK which is a set of encryption keys used for encrypt and data protection

Msg2

Station responds to AP by sending its Nonce(N_S) since its derived PTK it can protect it with a Message Integrity check(MIC)

- AP receives the Nonce(N_S) and so it can calculate the PTK and then validate the MIC send by the station to make sure there was no tampering of the MIC during transaction

Msg3

GTK (Group Transient key) is send to station with MIC. Now station can also calculate the GTK

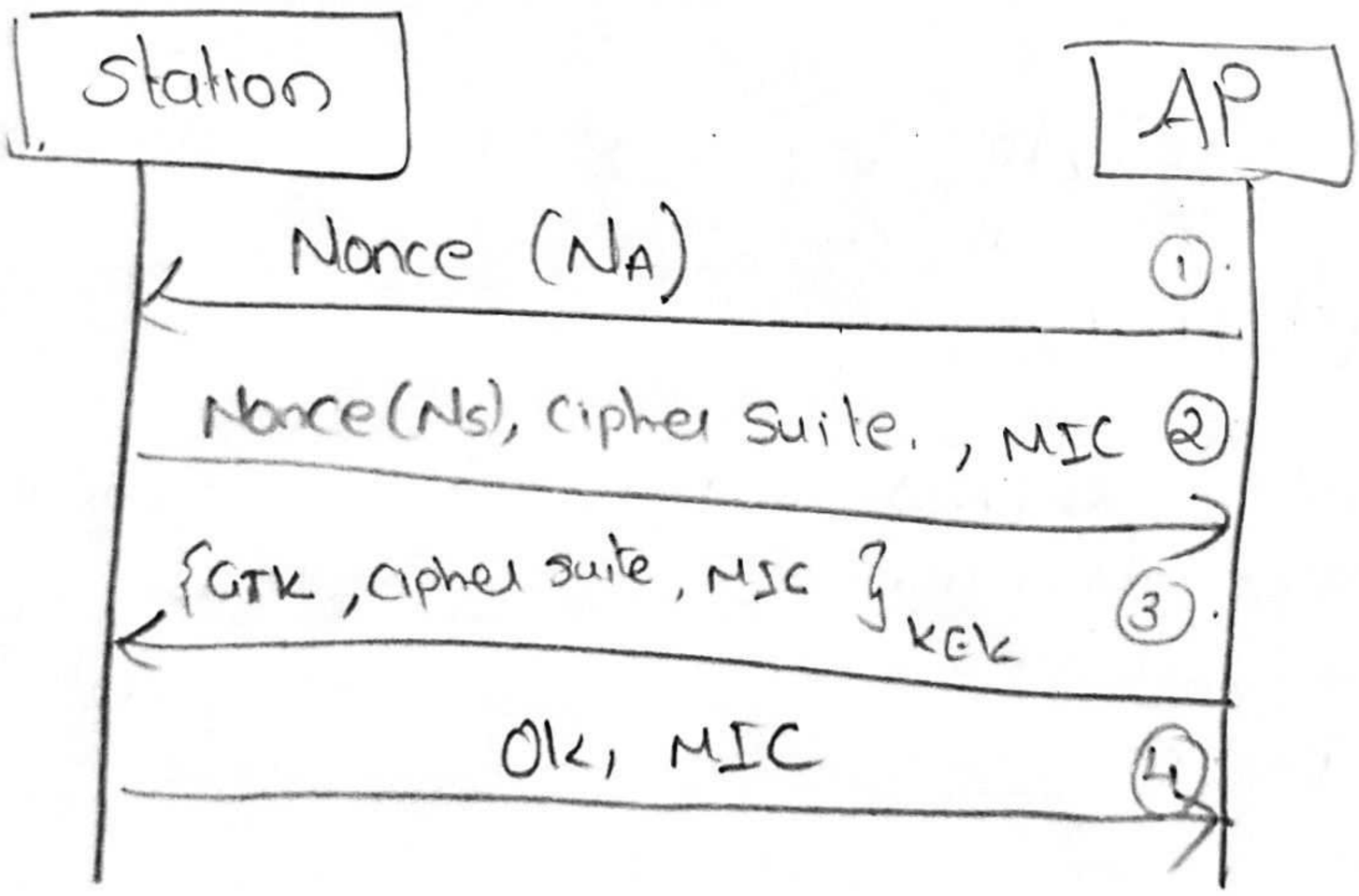
GTK is the key used by the AP and all

RAMSONS

stations to integrity protect all multicast or broadcast msg.

Msg 3 also contains cipher suite chosen by the AP. The msg is encrypted using KEK and is integrity protected using KCK

Msg4 is an ack from the station that it has received the prev msg without error. It is a signal to the AP that all msgs will be integrity-protected and encrypted with the TK.



4-way handshake.