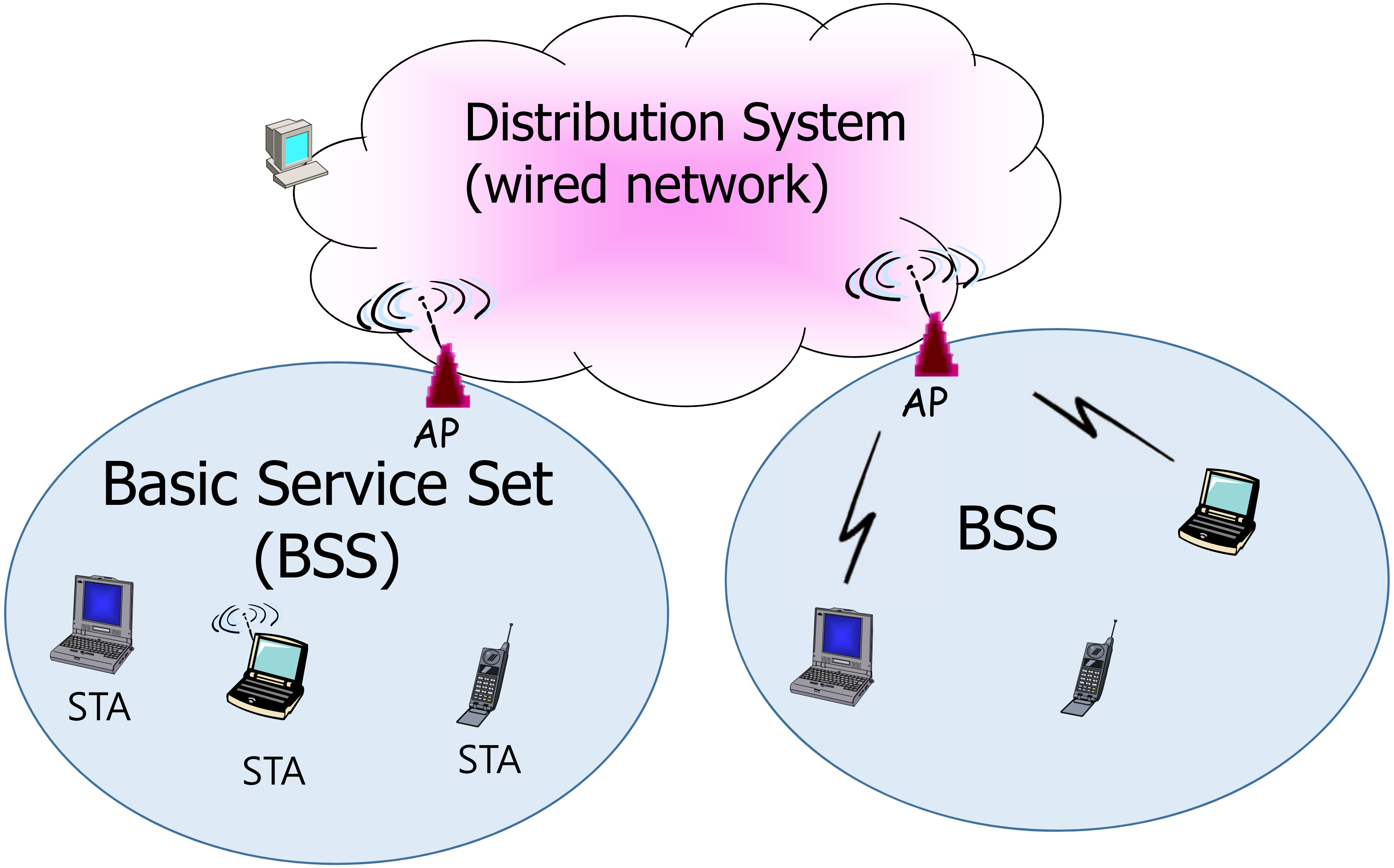
Wireless LAN Security
IEEE 802.11i

2019. 5. 13

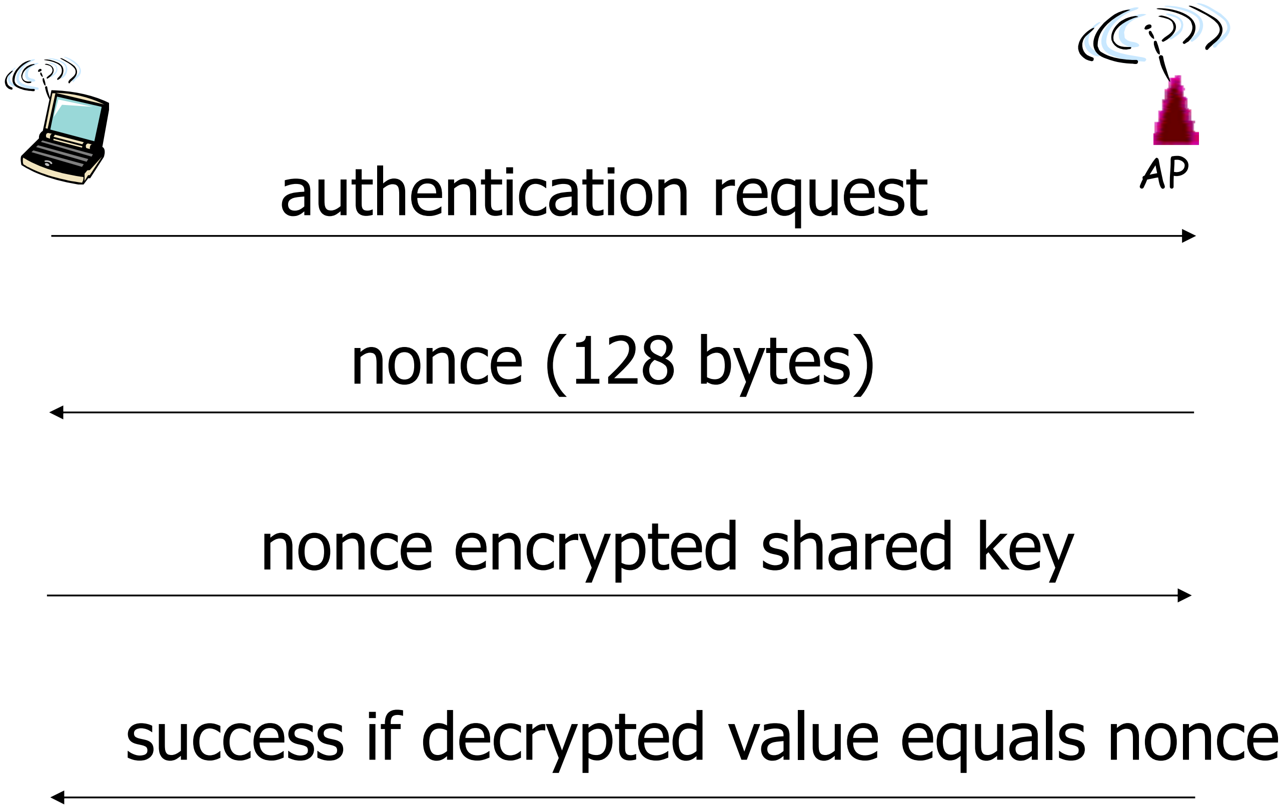
IEEE 801.11 Extended Service Set (ESS)



History

- WEP(Wired Equivalent Privacy)
  - IEEE 802.11 wireless LAN standard was published in 1999
  - Use RC4 algorithm with 64 bits (40bits symmetric key + 24 bits arbitrarily chosen from IV)
  - Only station authentication using symmetric key(no AP authentication)
- Wi-Fi Alliance published Wi-Fi Protected Access (WPA) as a Wi-Fi standard
- 802.11i RSN(Robust Security Network) standard
  - Published in 2004, replacing WEP
- WPA2 is a WiFi Alliance branded version of the final 802.11i standard.

Web authentication (one way)



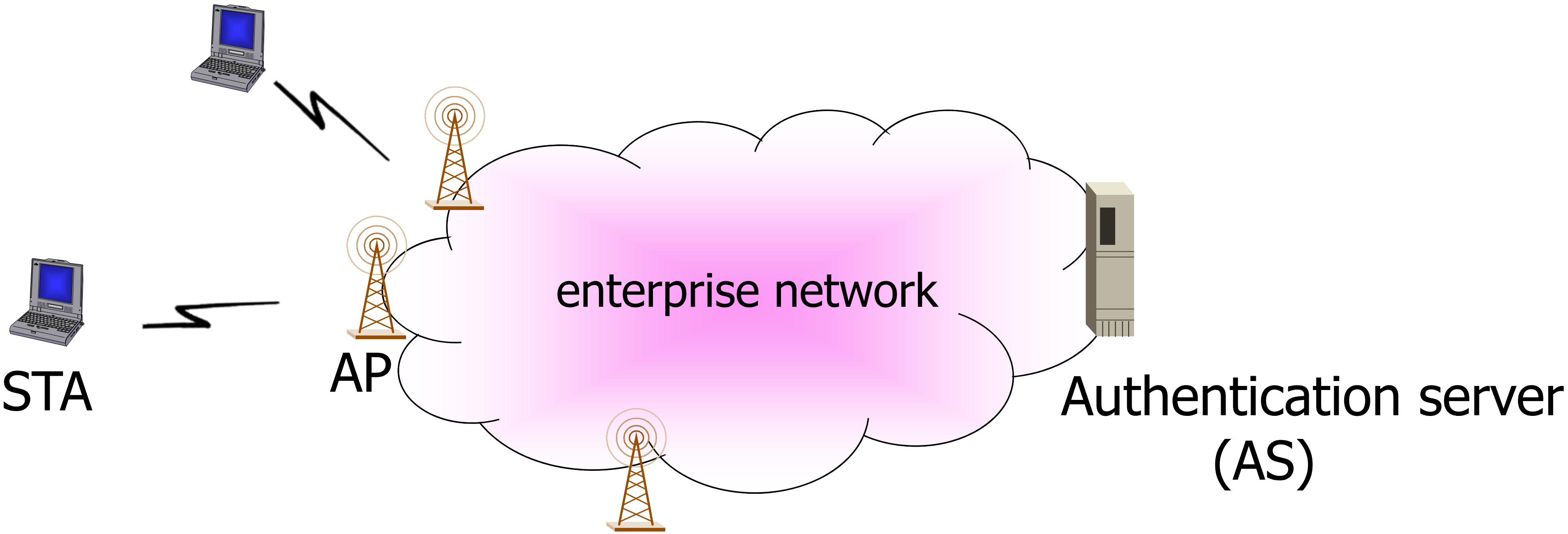
authentication request

nonce (128 bytes)

nonce encrypted shared key

success if decrypted value equals nonce

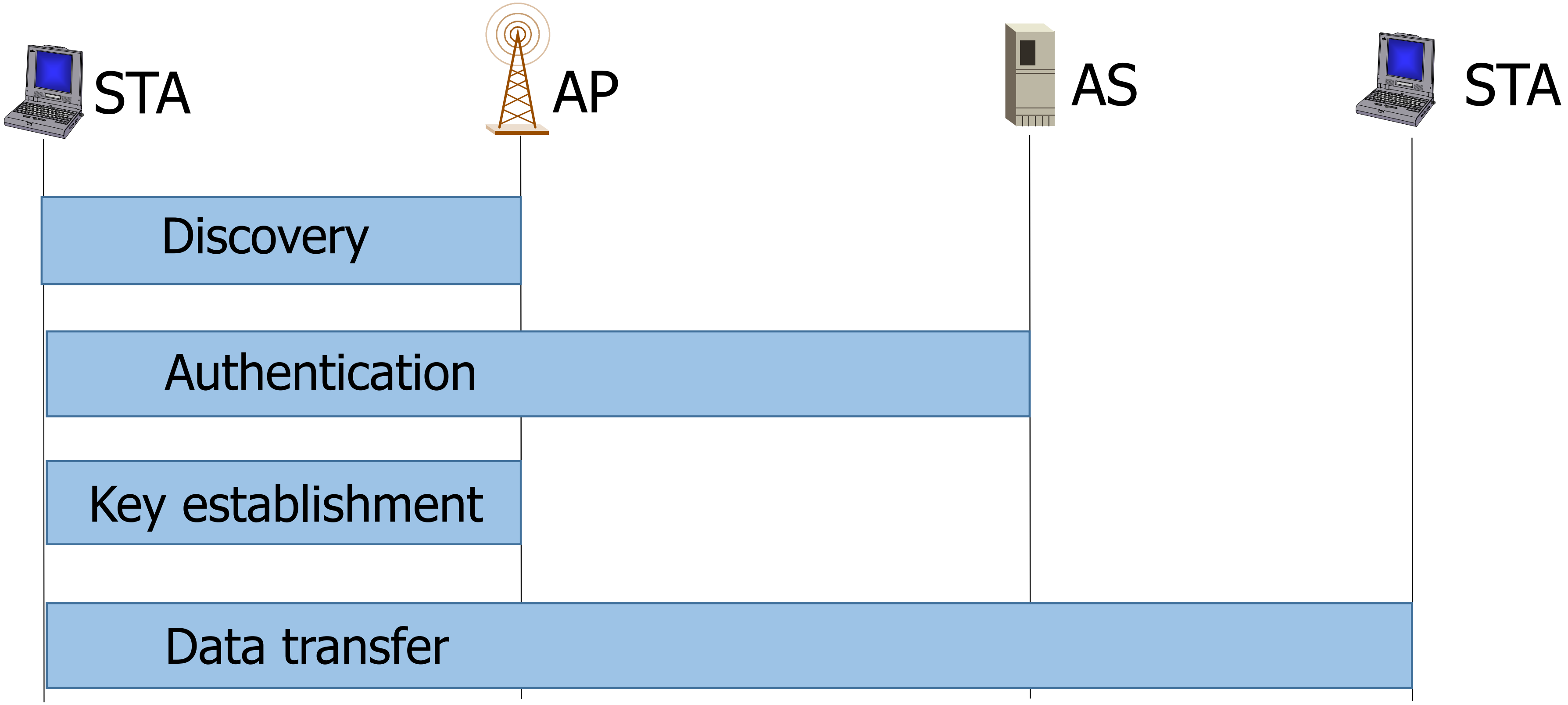
IEEE 802.11i security general architecture



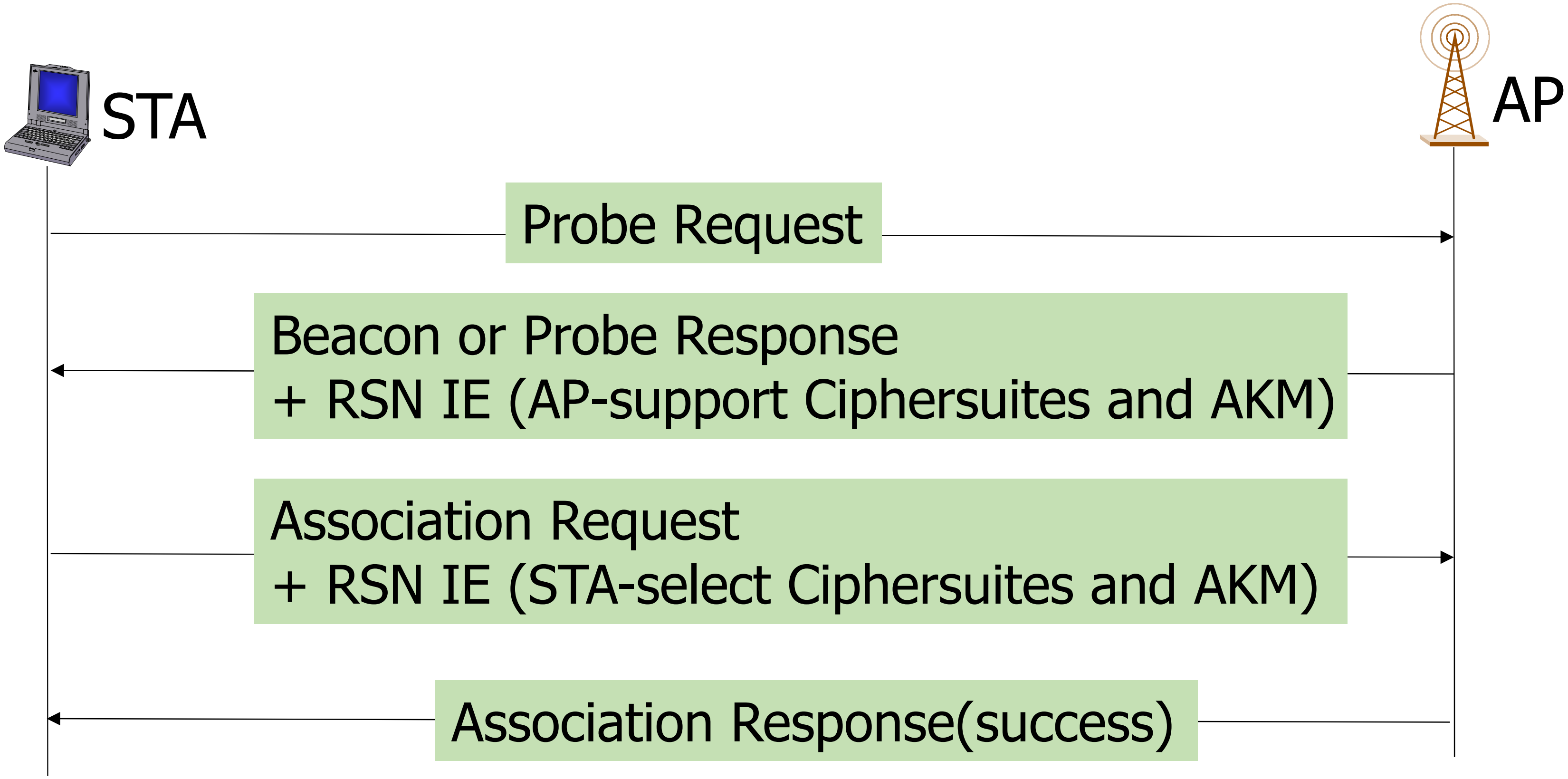
IEEE 802.11i operation phases

- Discovery
- Authentication
- Key establishment
- Protected data transfer

IEEE 802.11i operation phases



Discovery and Negotiation



STA

AP

Probe Request

Beacon or Probe Response
+ RSN IE (AP-support Ciphersuites and AKM)

Association Request
+ RSN IE (STA-select Ciphersuites and AKM)

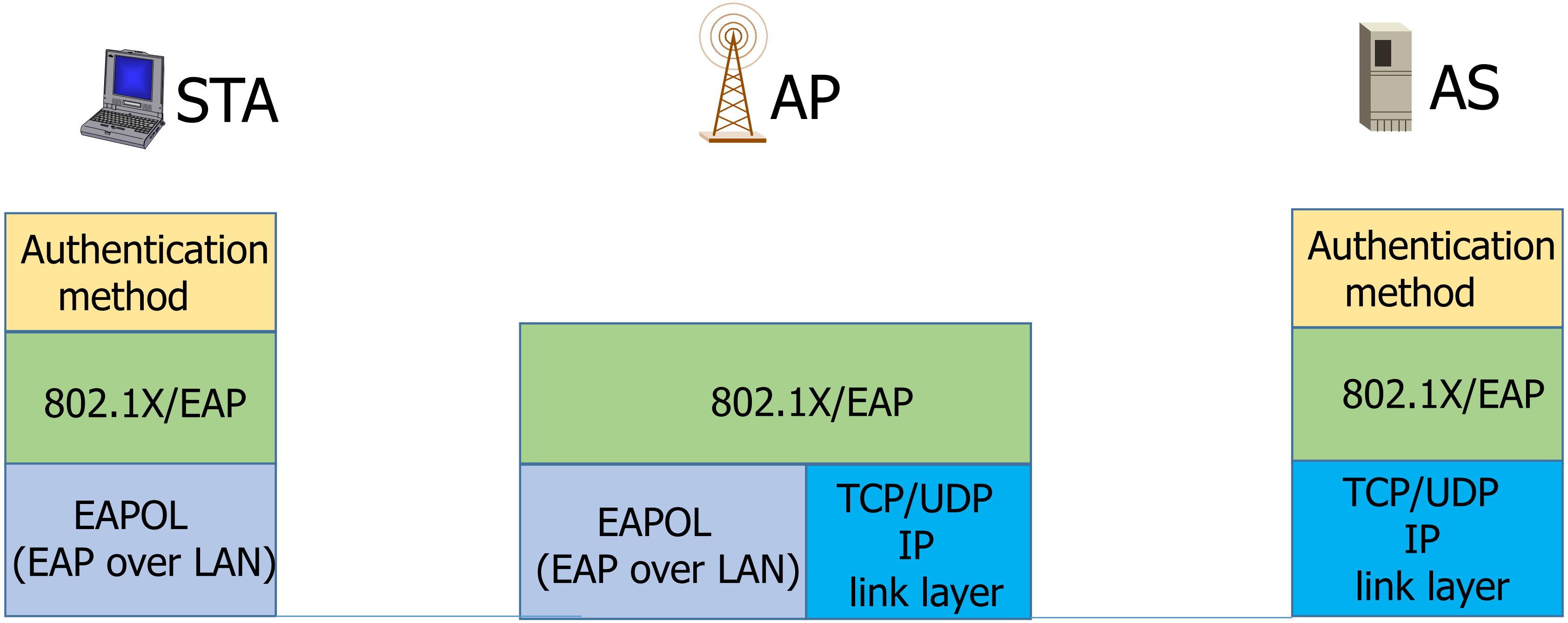
Association Response(success)

Cipher suites and Authentication and Key management(AKM)

- Defined Cipher suites
  - 1: WEP-40
  - 2: TKIP
  - 4: AES-CCMP
  - 5: WEP-104
  - Vendor OUI: any vendor specific
  - Other Reserved

- Defined AKMs
  - 1: 802.1X Authentication + 4-way Handshake
  - 2: PSK + 4-way Handshake
  - Vendor OUI: any vendor specific
  - Other Reserved

Authentication



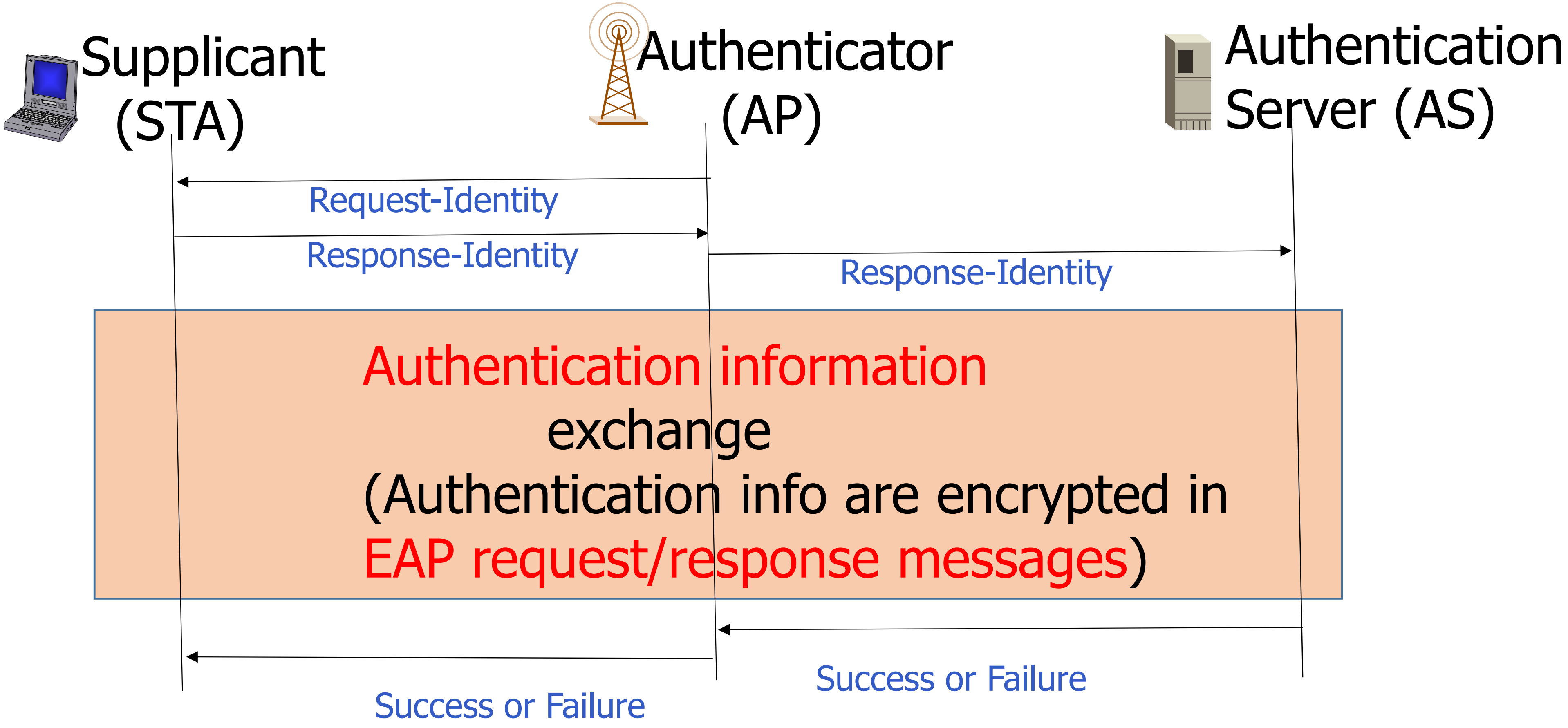
EAP

- EAP is not an authentication method or protocol itself.
- EAP is a framework to support multiple authentication mechanisms over multiple link layer networks.
  - It defines EAP packets which convey data related to a certain authentication method.
  - It defines the procedure to exchange EAP packets for the authentication process.
  - Authenticator do not have to understand each auth method and may act as a pass-through agent for AS.
  - It is independent of any specific link layer technology.

Lower layer under EAP

- EAP assumes that the lower layer is unreliable.
  - EAP defines its own retransmission scheme. The authenticator retransmits Request that have not yet received Responses.
- EAP assumes that the lower layer do error detection.
  - EAP itself does not provide error detection scheme.
- EAP MTU size is 1020 bytes or greater.
- EAP is reliant on lower layer ordering guarantee.

Authentication Process



Supplicant (STA)

Authenticator (AP)

Authentication Server (AS)

Request-Identity

Response-Identity

Response-Identity

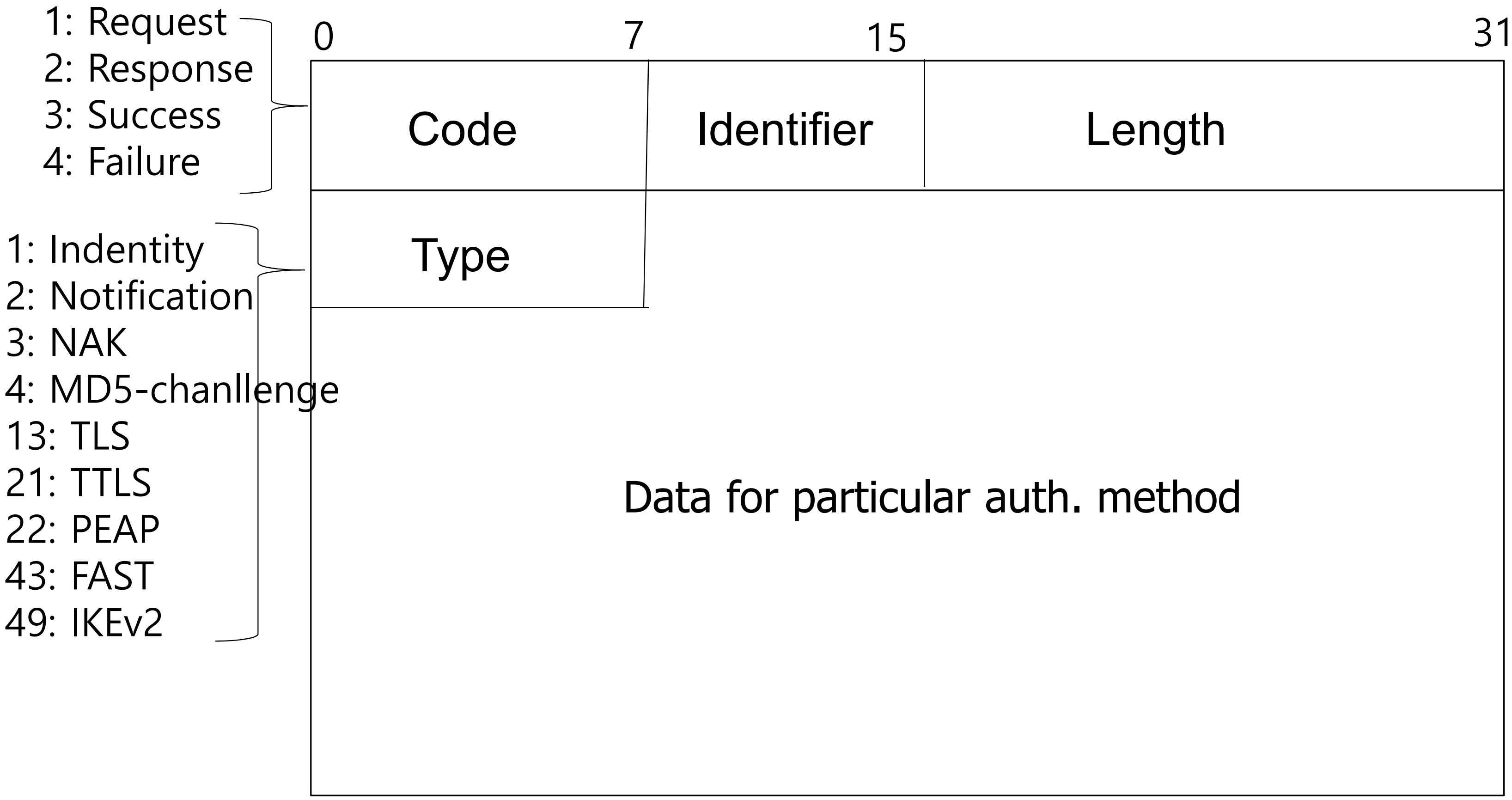
Authentication information exchange

(Authentication info are encrypted in EAP request/response messages)

Success or Failure

Success or Failure

EAP packet format



1: Request
2: Response
3: Success
4: Failure

1: Indentity
2: Notification
3: NAK
4: MD5-chanllenge
13: TLS
21: TTLS
22: PEAP
43: FAST
49: IKEv2

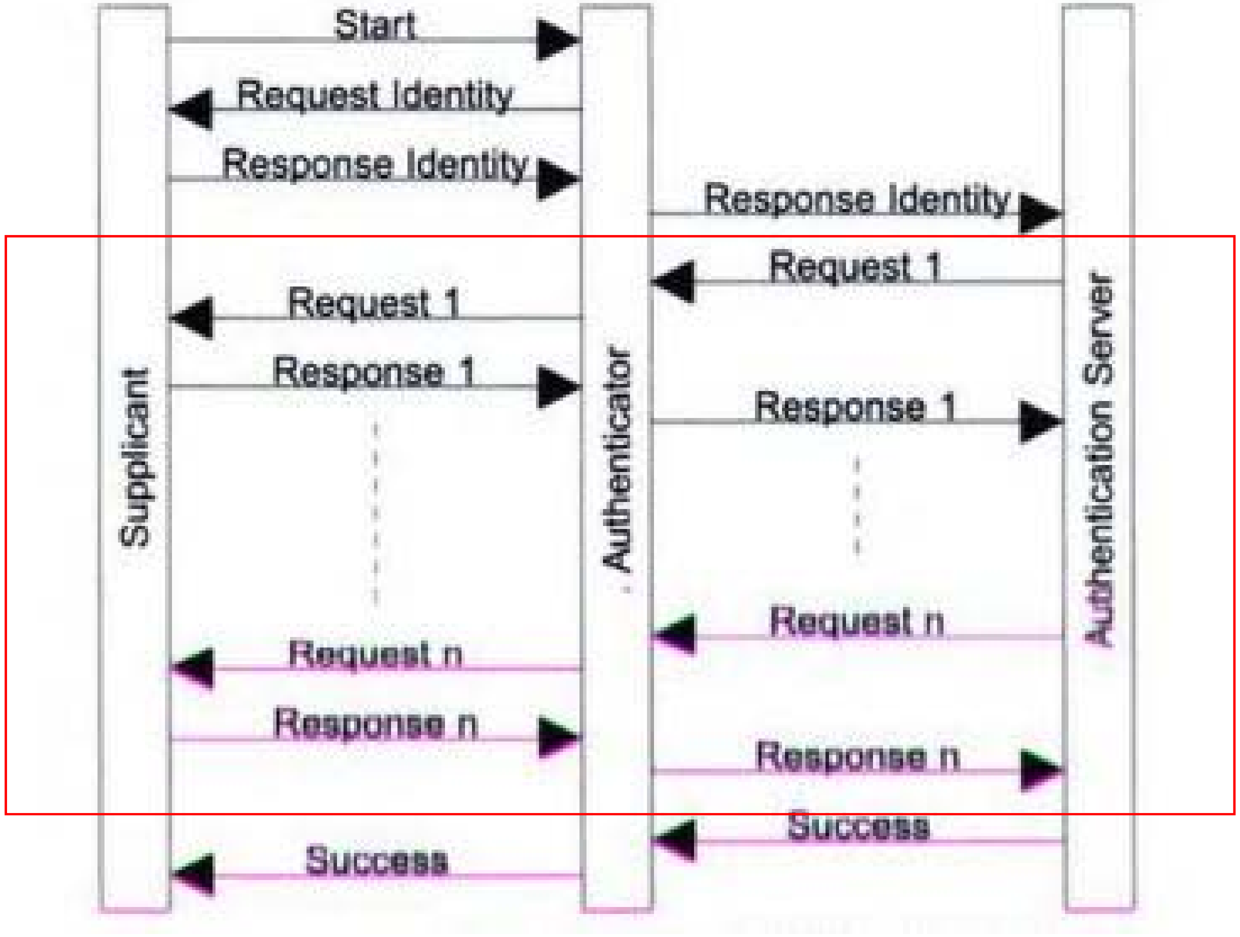
EAP message exchange

supplicant

Authenticator

Authentication Server

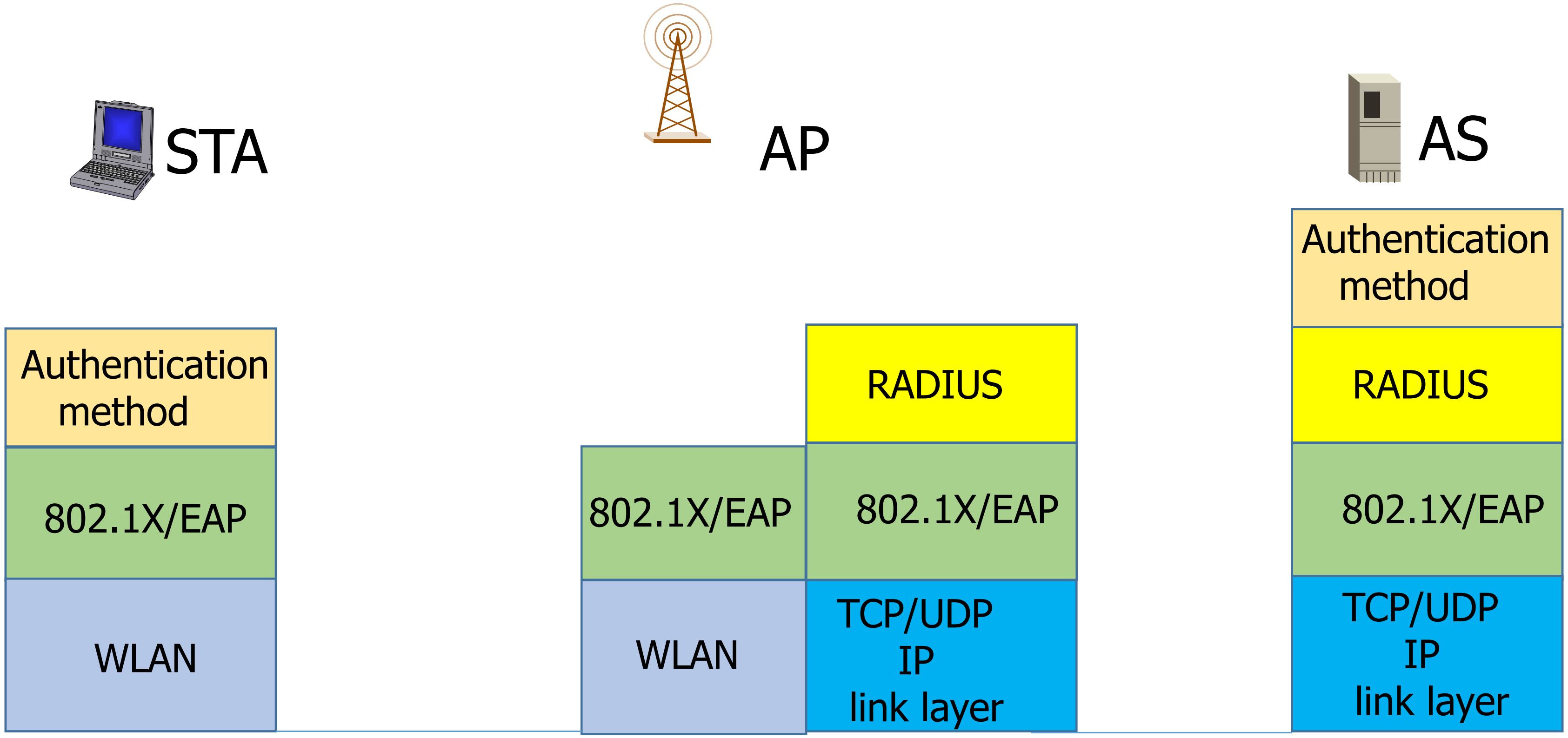
Authentication process



Remarks

- 802.11i does not prescribe any authentication method.
- The standard just specify the IEEE 802.1X Port-Based Network Access Control which is also used together with EAP (Extensible Authentication Protocol).
- Sometimes the enterprise network is based on a RADIUS server for authentication, authorization, and accounting. Then the protocol stack is like the next slide.
- Why RADIUS/Diameter?
  - Enterprises worldwide have invested billions of dollars in RADIUS authentication databases for remote access and network log-in

RADISU over EAP

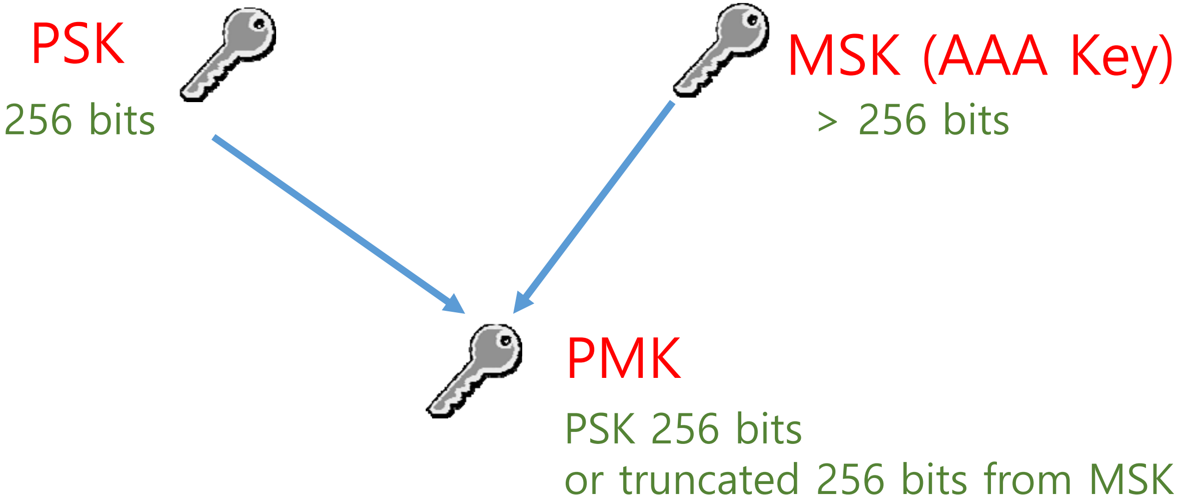


Key establishment

- Result of Authentication Phase
  - Once AS successfully authenticates STA, it generates a master session key (MSK), also known as the Authentication, Authorization, and Accounting (AAA) key.
- Then, AS sends the MSK to AP and STA.
- (Unfortunately,) IEEE 802.11i does not specify a method for secure delivery of the MSK, but relies on EAP.
- The result of the authentication process is that both STA and AP have the MSK, which is the starting point to derive all the keys.

PMK(Pairwise Master Key)

- Derived from a static Pre-Shared Key(PSK) which has to be manually installed on each device a priori
- Or, derived from the result of any method applied in the mutual authenticating phase (MSK), e.g., EAP-TLS



PSK

256 bits

MSK (AAA Key)

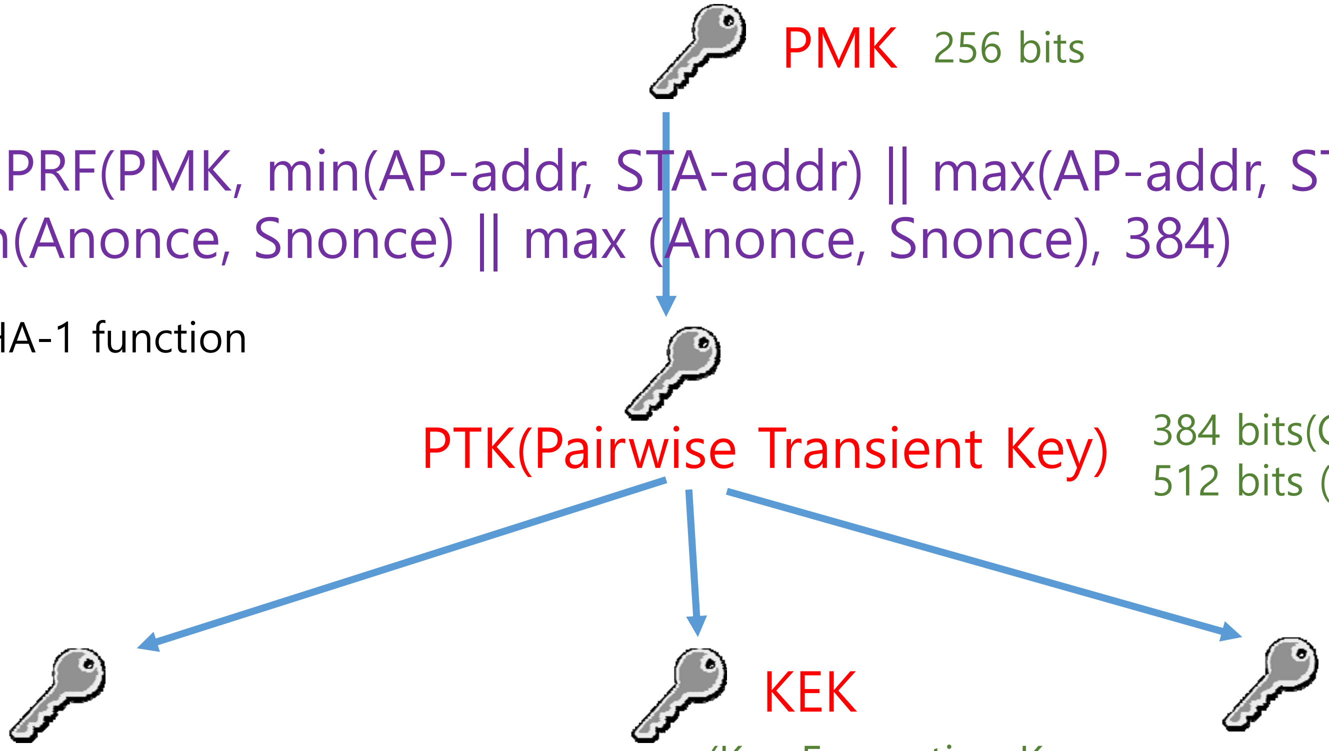
> 256 bits

PMK

PSK 256 bits

or truncated 256 bits from MSK

802.11i Pairwise Key Hierarchy



PMK 256 bits

PTK=PRF(PMK, min(AP-addr, STA-addr) || max(AP-addr, STA-addr) || min(Anonce, Snonce) || max (Anonce, Snonce), 384)

PRF: HMAC-SHA-1 function

PTK(Pairwise Transient Key) 384 bits(CCMP)
512 bits (TKIP)

KCK
(128 bits Key Confirmation Key used for EAPOL message authentication and integrity)

KEK
(Key Encryption Key
128 bits)

TK(Temporal Key)
Data encryption key
128 bits(CCMP)
256 bits (TKIP)

802.11i Group Key Hierarchy

GMK 256 bits

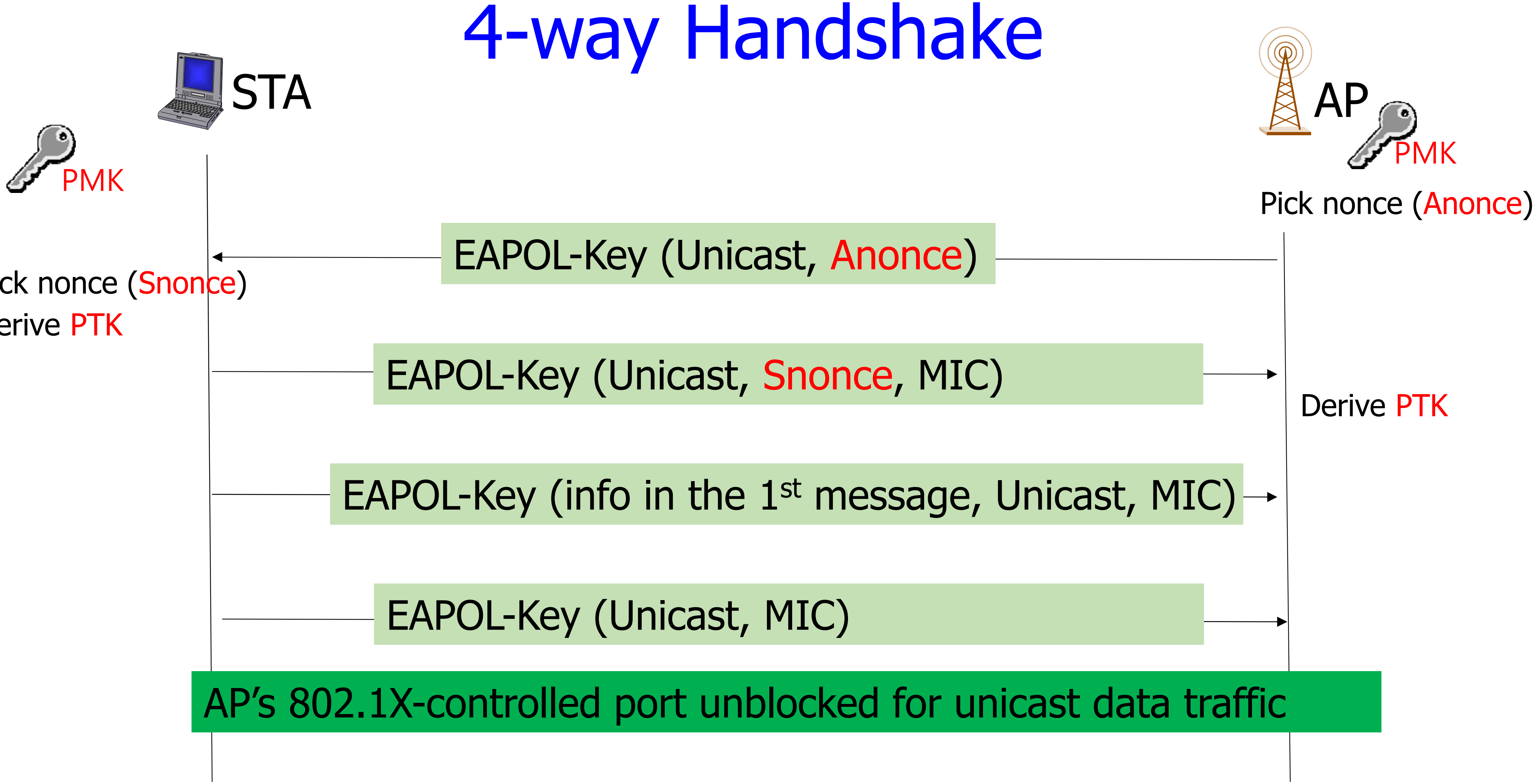
(But, the standard doesn’t specify how to generate GMK.)

GTK=PRF(GMK, “Group key expansion”, MAC || Gnonce, 256)

GTK(Group Temporal Key)

128 bits(CCMP)
256 bits (TKIP)

4-way Handshake



STA

AP

PMK

PMK

Pick nonce (Anonce)

EAPOL-Key (Unicast, Anonce)

Pick nonce (Snonce)

Derive PTK

EAPOL-Key (Unicast, Snonce, MIC)

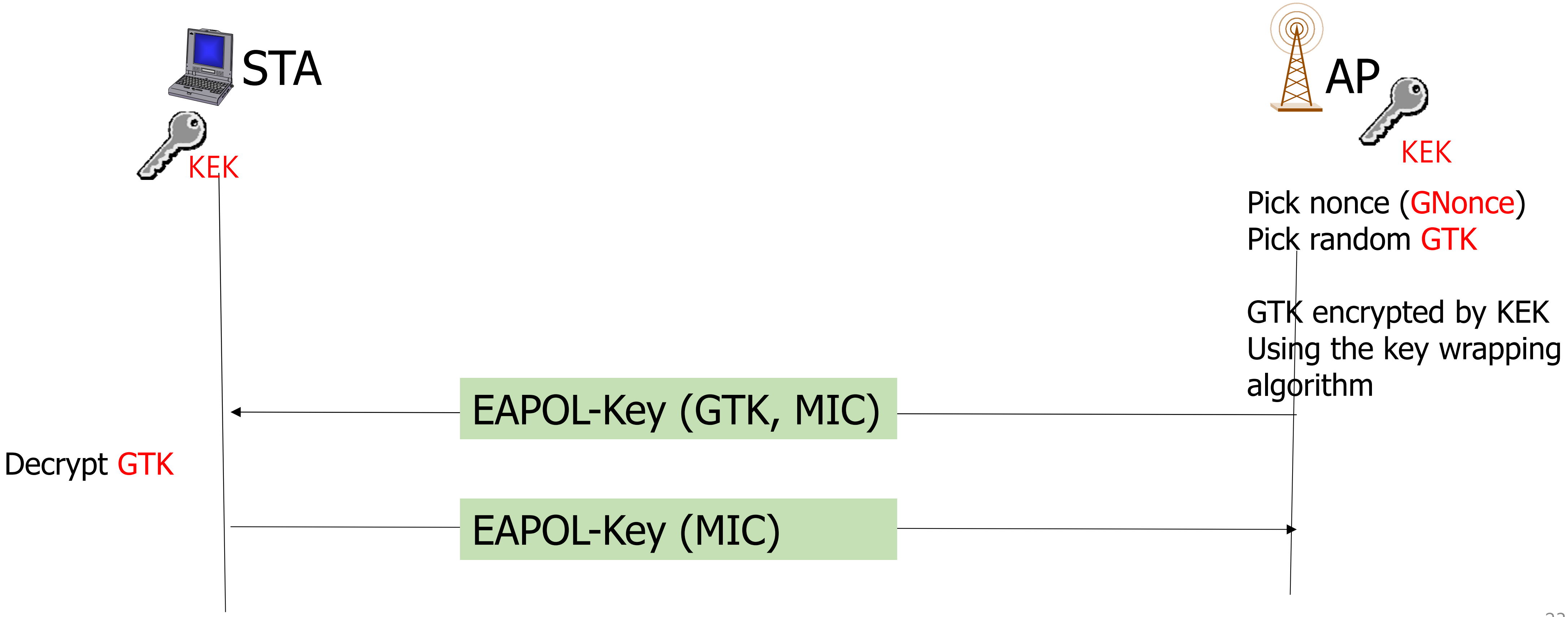
Derive PTK

EAPOL-Key (info in the 1st message, Unicast, MIC)

EAPOL-Key (Unicast, MIC)

AP's 802.1X-controlled port unblocked for unicast data traffic

Group Key establishment



STA

KEK

AP

KEK

Pick nonce (GNonce)
Pick random GTK

GTK encrypted by KEK
Using the key wrapping
algorithm

EAPOL-Key (GTK, MIC)

Decrypt GTK

EAPOL-Key (MIC)

TKIP

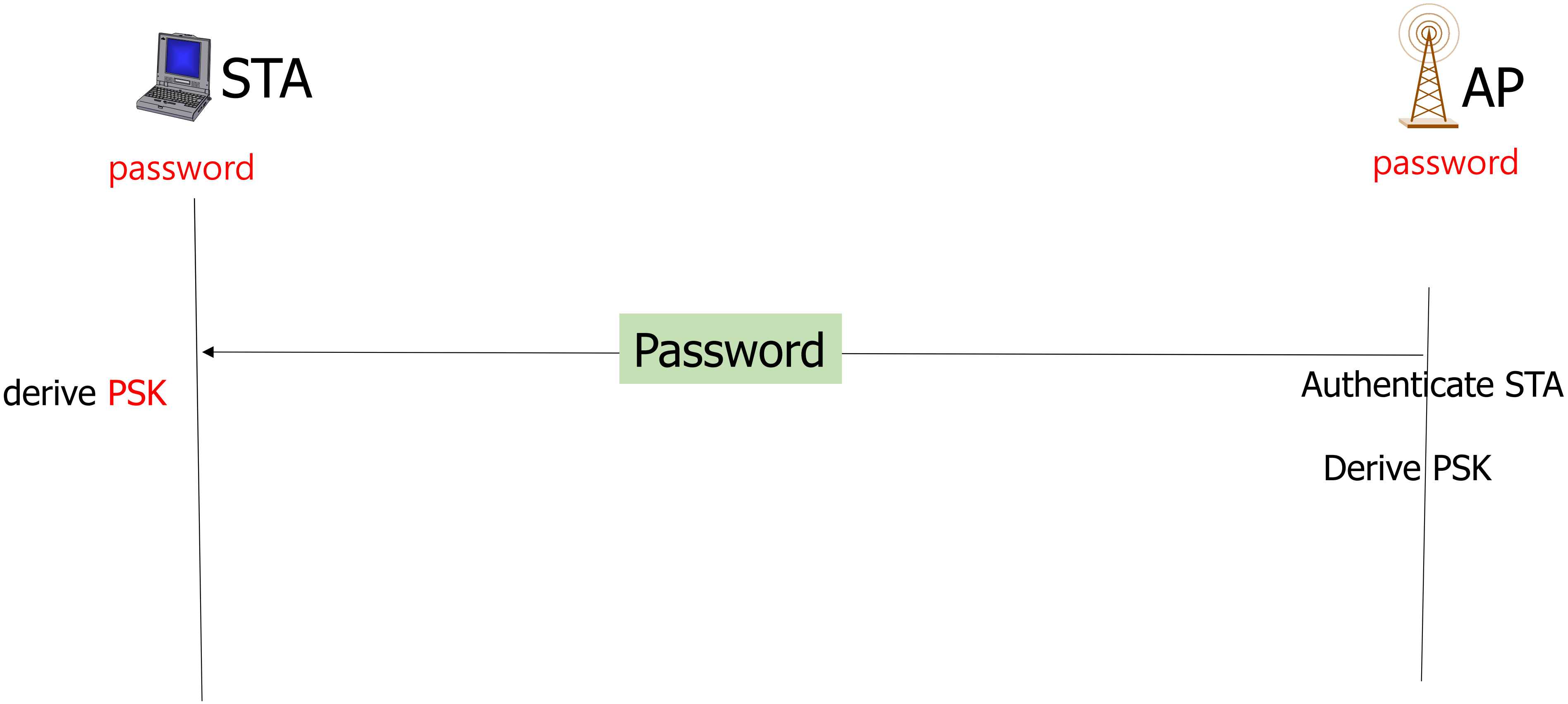
- Designed to require only software changes of old WEP.
- For encryption, use RC4 with 128 bits key
- For message integrity, TKIP computes a message integrity code(MIC) of 64 bits generated by an algorithm called Michael.
- So, two-64 bits keys are used by Michael to generate MIC for message authentication and integrity (64 bits for STA-to-AP, 64 bits for AP-to-STA), and 128buts are truncated to generate RC4 key used to encrypt data.

CCMP

- For data encryption, use 128 bits AES and CTR block cipher.
- For message authentication and integrity, the counter with CBC-MAC (CCM) is used.

Use Case1

- When we access the Wi-Fi network at home or in campus or hotels or most places except the enterprise networks, AP authenticate STA without any involvement of AS.
- In this case, we just enter a password which is shared with AP. Then, AP uses the password for user authentication, and derive PSK from the passworkd.
- This configuration is call WPA-PSK(Pre-Shared Key).



STA

password

AP

password

Password

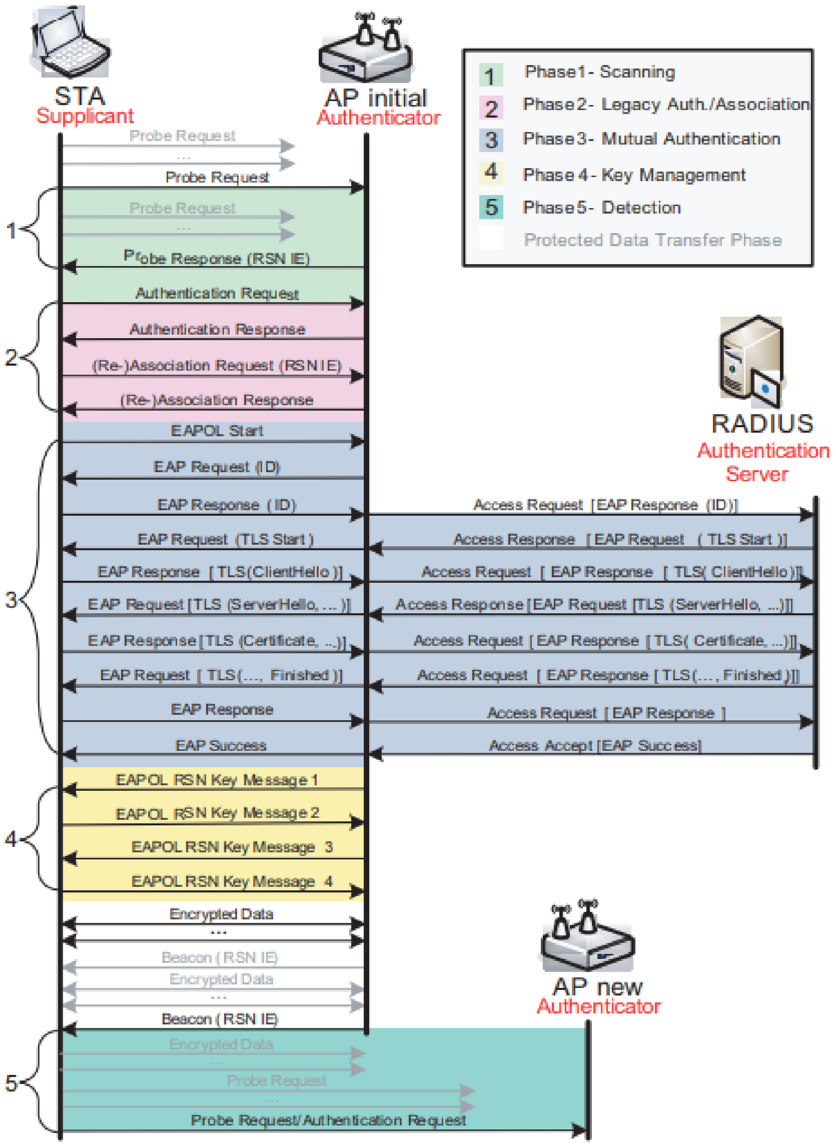
derive PSK

Authenticate STA

Derive PSK

Use Case2

- A company uses TLS as an authentication method.
- Then, the whole process is as in the following slide.



STA
Supplicant

AP initial
Authenticator

1 Phase1- Scanning
2 Phase2- Legacy Auth./Association
3 Phase3- Mutual Authentication
4 Phase 4- Key Management
5 Phase5- Detection
Protected Data Transfer Phase

Probe Request
...
Probe Request
Probe Request
...
Probe Response (RSN IE)
Authentication Request
Authentication Response
(Re-)Association Request (RSN IE)
(Re-)Association Response
EAPOL Start
EAP Request (ID)
EAP Response (ID)
EAP Request (TLS Start)
EAP Response [TLS(ClientHello)]
EAP Request [TLS (ServerHello, ...)]
EAP Response [TLS (Certificate, ...)]
EAP Request [TLS(..., Finished)]
EAP Response
EAP Success

RADIUS
Authentication
Server

Access Request [EAP Response (ID)]
Access Response [EAP Request (TLS Start)]
Access Request [EAP Response [TLS(ClientHello)]]
Access Response [EAP Request [TLS (ServerHello, ...)]]
Access Request [EAP Response [TLS(Certificate, ...)]]
Access Request [EAP Response [TLS(..., Finished)]]
Access Request [EAP Response]
Access Accept [EAP Success]

EAPOL RSN Key Message 1
EAPOL RSN Key Message 2
EAPOL RSN Key Message 3
EAPOL RSN Key Message 4
Encrypted Data
...
Beacon (RSN IE)
Encrypted Data
...
Beacon (RSN IE)

AP new
Authenticator

Encrypted Data
...
Probe Request
...
Probe Request/Authentication Request