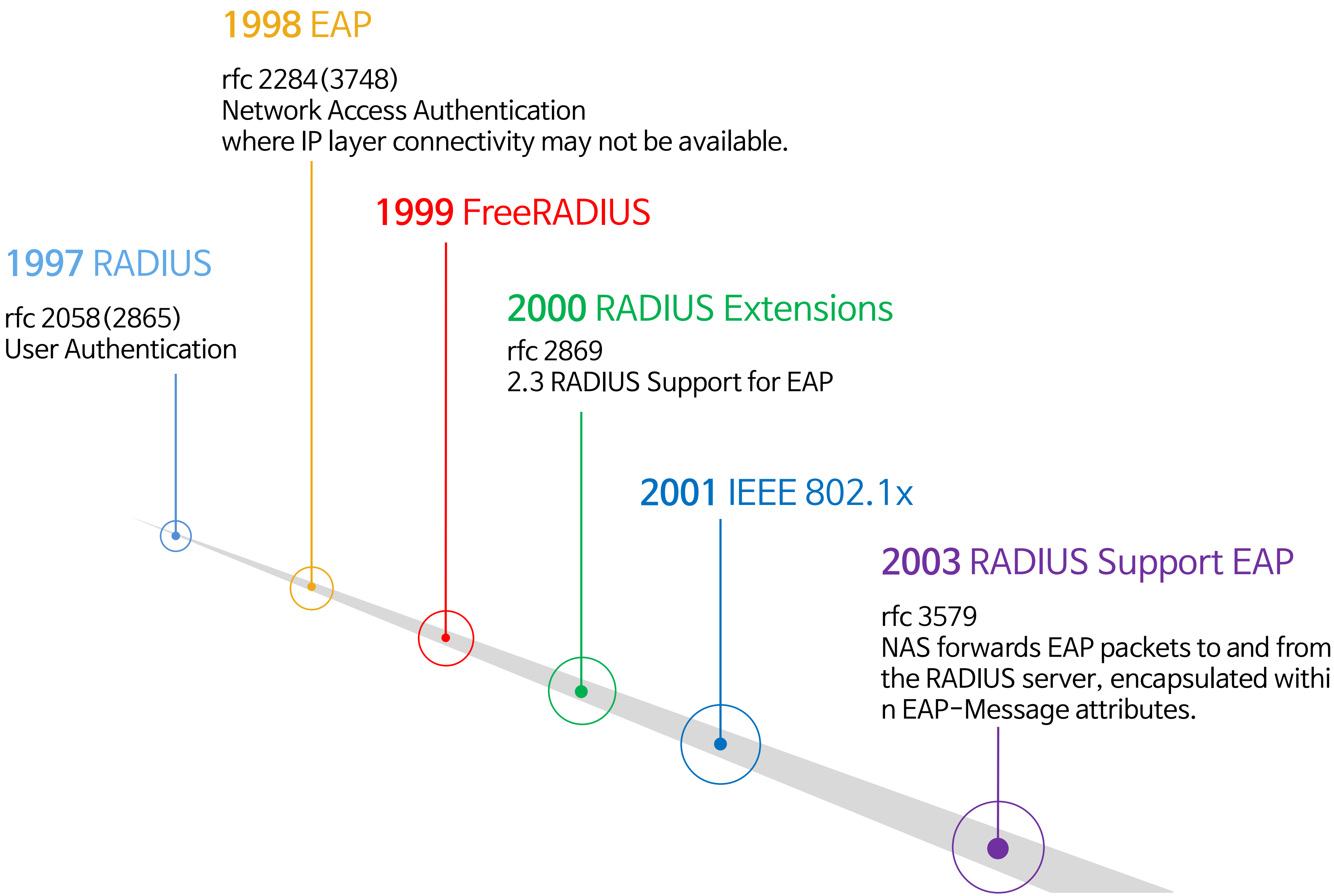
EAP & RADUIS

Extensible Authentication Protocol
Remote Authentication Dial In User Service

shin@basein.net

경기도 성남시 분당구 성남대로 69, 808호(구미동 로드랜드EZ타워)
대표전화: 031)713-7324 팩스: 031)713-7325

Timeline



1997 RADIUS

rfc 2058(2865)
User Authentication

1998 EAP

rfc 2284(3748)
Network Access Authentication
where IP layer connectivity may not be available.

1999 FreeRADIUS

2000 RADIUS Extensions

rfc 2869
2.3 RADIUS Support for EAP

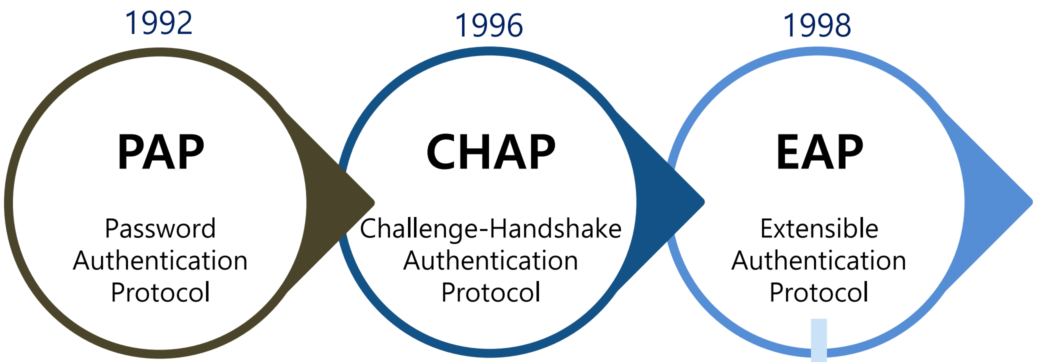
2001 IEEE 802.1x

2003 RADIUS Support EAP

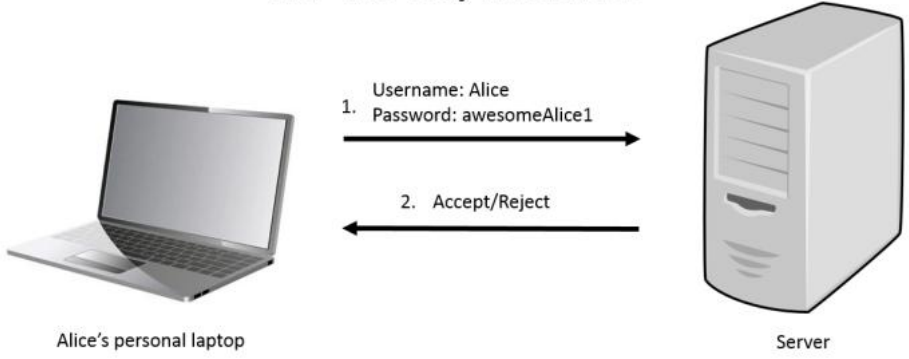
rfc 3579
NAS forwards EAP packets to and from
the RADIUS server, encapsulated withi
n EAP-Message attributes.

Authentication Protocols for PPP [12] [13]

- Protocols are used mainly by Point-to-Point Protocol (PPP) servers
  - to validate the identity of remote clients
  - before granting them access to server data.
- Most of them use a password as the cornerstone of the authentication.


1992
PAP
Password Authentication Protocol
1996
CHAP
Challenge-Handshake Authentication Protocol
1998
EAP
Extensible Authentication Protocol

PAP two-way handshake



EAP Methods

EAP-MD5
EAP-TLS
EAP-TTLS
EAP-FAST
EAP-PEAP
EAP-GTC
PEAP-GTC
.....

AAA architecture Protocols [13]

TACACS, XTACACS and TACACS+

The oldest AAA protocol using IP based authentication without any encryption.

RADIUS

Full AAA protocol commonly used by ISP.
Credentials are mostly username-password combination based.
Use NAS and UDP protocol for transport.

Diameter

From the earlier RADIUS protocol.
Use TCP or SCTP(Stream Control Transmission Protocol) unlike RADIUS which uses UDP

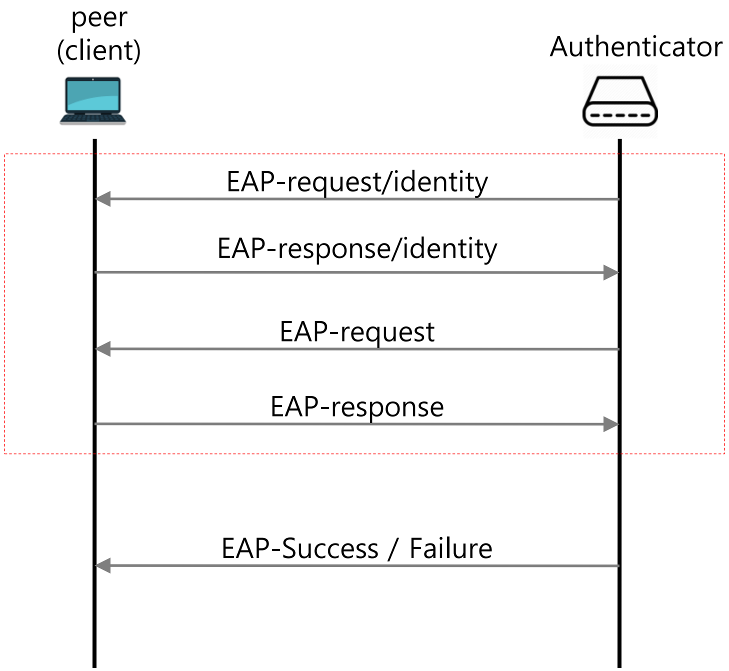
Kerberos

Centralized network authentication system developed at MIT.
The default authentication method in Windows 2000 and later

EAP Extensible Authentication Protocol

Abstract [4] [7]

- designed for use in network access authentication, where IP layer connectivity may not be available.
- Not a specific authentication mechanism but framework which supports multiple authentication methods.
- EAP methods
  - EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, EAP-TTLS …
- PEAP
  - Protected EAP
  - encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.



The conversation continues until the authenticator cannot authenticate or determines that successful authentication has occurred.

Packet format [4]

- Code identifies the Type of EAP packet.
  - Request (1), Response (2), Success (3), or Failure (4).
- Identifier aids in matching Responses with Requests.
- Length is the sum of the Code, Identifier, Length, and Data fields.
- The format of the Data field is determined by the Code field.
- The Type field is one octet. This field indicates the Type of Request or Response.
  - EAP-TLS, EAP-TTLS…

[EAP Packet Format]

code	identifier	length
Data….		

[EAP Success or Failure]

code	identifier	length

[EAP Request or Reply]

code	identifier	length
type	type-data ….	

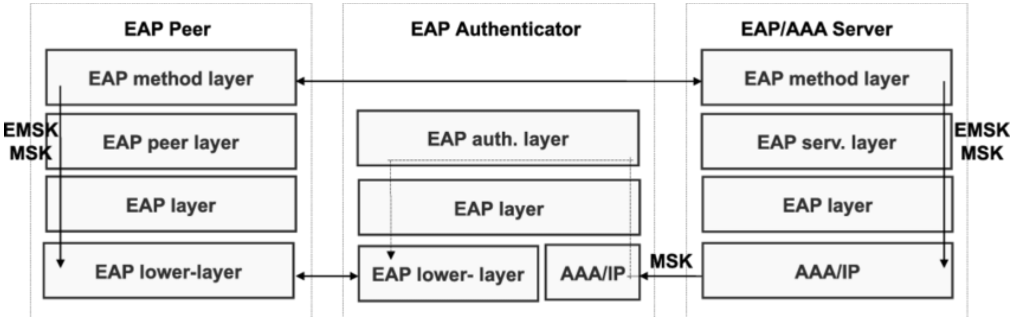
Method Types [9]

- https://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml

1	**Identity**
2	Notification
3	Legacy Nak
4	MD5-Challenge
5	One-Time Password (OTP)
6	**Generic Token Card (GTC)**
7	Allocated
8	Allocated
9	RSA Public Key Authentication
10	DSS Unilateral
11	KEA
12	KEA-VALIDATE
13	**EAP-TLS**
14	Defender Token (AXENT)
15	RSA Security SecurID EAP
16	Arcot Systems EAP
17	EAP-Cisco Wireless
18	GSM Subscriber Identity Modules (EAP-SIM)
19	SRP-SHA1
20	Unassigned
21	**EAP-TTLS**
22	Remote Access Service
23	EAP-AKA Authentication
24	EAP-3Com Wireless
25	**PEAP**
26	MS-EAP-Authentication
27	Mutual Authentication w/Key Exchange (MAKE)
28	CRYPTOCard
29	**EAP-MSCHAP-V2**
30	DynamID
31	Rob EAP
32	Protected One-Time Password
33	MS-Authentication-TLV
34	SentriNET
35	EAP-Actiontec Wireless
36	Cogent Systems Biometrics Authentication EAP
37	AirFortress EAP
38	EAP-HTTP Digest
39	SecureSuite EAP
40	DeviceConnect EAP
41	EAP-SPEKE
42	EAP-MOBAC
43	EAP-FAST
44	ZoneLabs EAP (ZLXEAP)
45	EAP-Link
46	EAP-PAX
47	EAP-PSK
48	EAP-SAKE
49	EAP-IKEv2
50	EAP-AKA'
51	EAP-GPSK
52	EAP-pwd
53	EAP-EKE Version 1
54	EAP Method Type for PT-EAP
55	TEAP

pass-through authenticator [4]

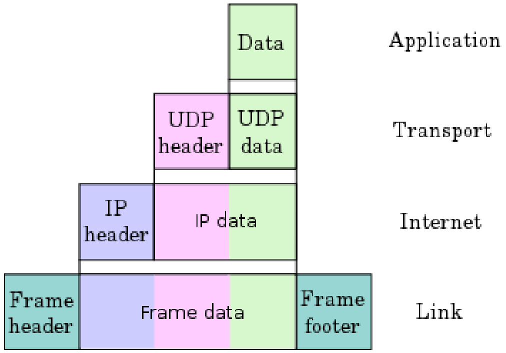
- Authenticator forwards
  - EAP packets received from the peer to the backend authentication server.
  - EAP packets received from the backend authentication to the peer.
- Peer/auth Layer: Code field
- Method Layer: Type field



EAP Method and Encapsulation [7]

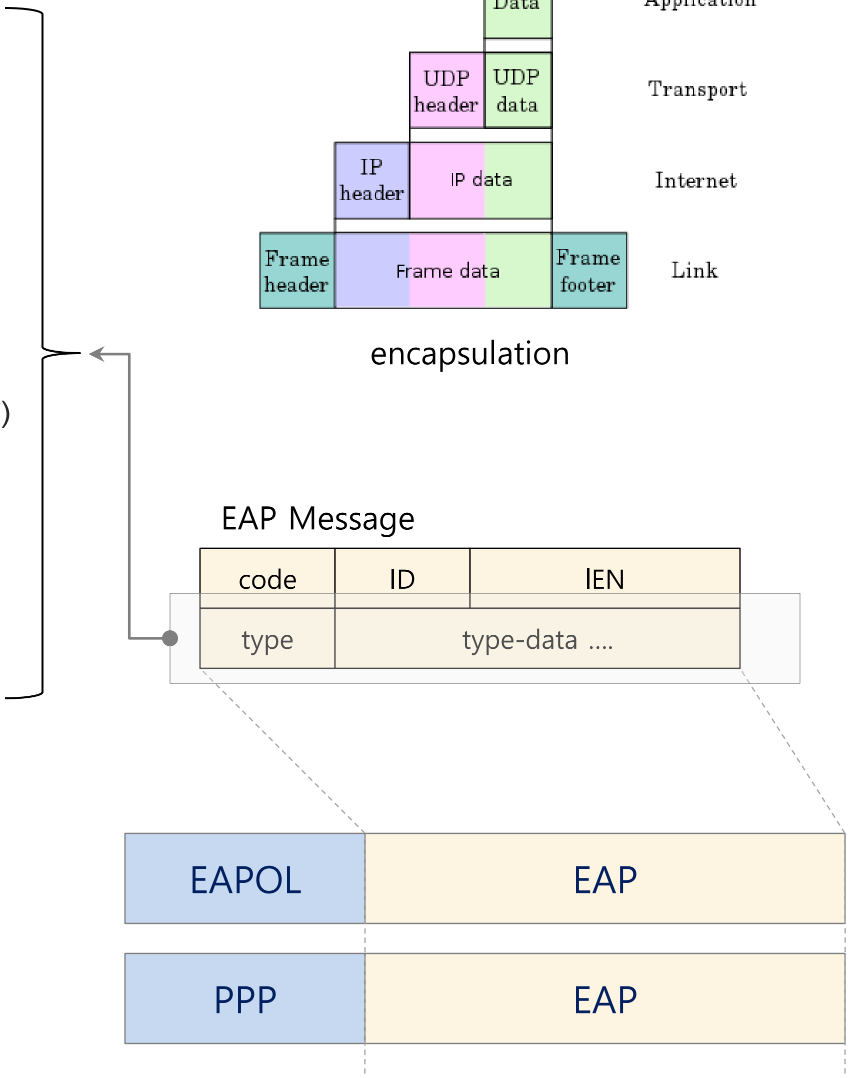
- Methods
  - Nimble out-of-band authentication for EAP (EAP-NOOB)
  - Lightweight Extensible Authentication Protocol (LEAP)
  - EAP Transport Layer Security (EAP-TLS)
  - EAP-MD5
  - EAP Protected One-Time Password (EAP-POTP)
  - EAP Pre-Shared Key (EAP-PSK)
  - EAP Password (EAP-PWD)
  - EAP Tunneled Transport Layer Security (EAP-TTLS)
  - EAP Internet Key Exchange v. 2 (EAP-IKEv2)
  - EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
  - Tunnel Extensible Authentication Protocol (TEAP)
  - EAP Subscriber Identity Module (EAP-SIM)
  - EAP Authentication and Key Agreement (EAP-AKA)
  - EAP Authentication and Key Agreement prime (EAP-AKA')
  - EAP Generic Token Card (EAP-GTC)
  - EAP Encrypted Key Exchange (EAP-EKE)

- Encapsulation
  - IEEE 802.1X: EAP over LAN (EAPOL)
  - PEAP: TLS tunnel
  - RADIUS and Diameter: EAP message to EAP attribute
  - PANA
  - PPP

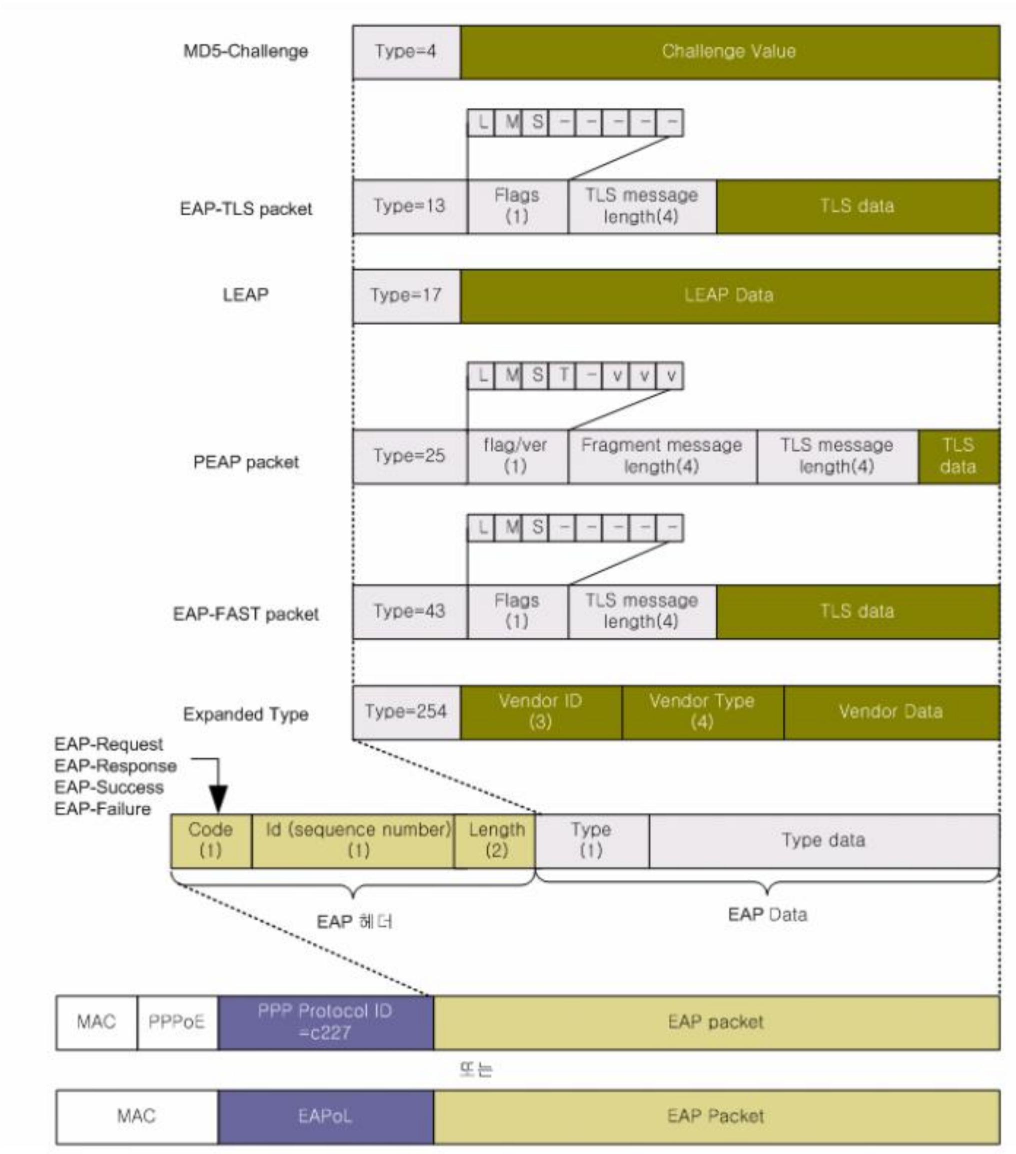


encapsulation

EAP Message



EAP Packet Format [12]



Phase 2 authentication [18] [19] [20]

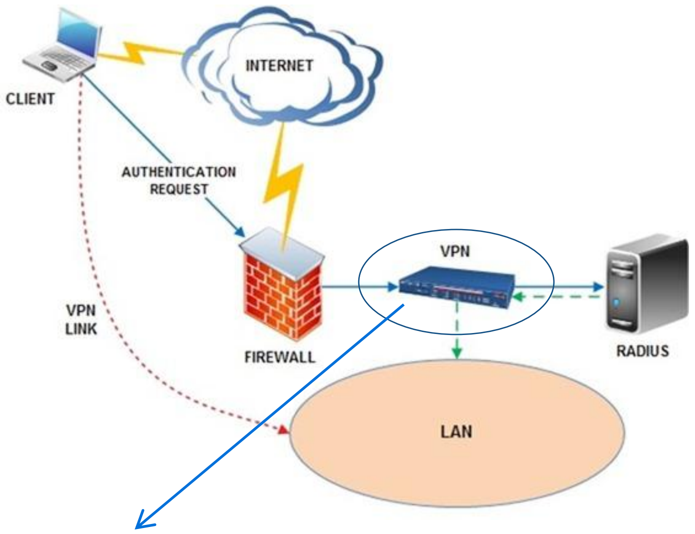
- PEAP
  - TLS session part
  - EAP conversation part
    - PEAPv0/EAP-MSCHAPv2
    - PEAPv1/EAP-GTC
- EAP-TTLS
  - TLS handshake phase
  - TLS tunnel phase.
    - PAP
    - MS-CHAP-V2
    - MS-CHAP-V2
    - EAP-GTC

The difference is that instead of encapsulating EAP messages within TLS, the TLS payload of EAP-TTLS messages consists of a sequence of attributes.

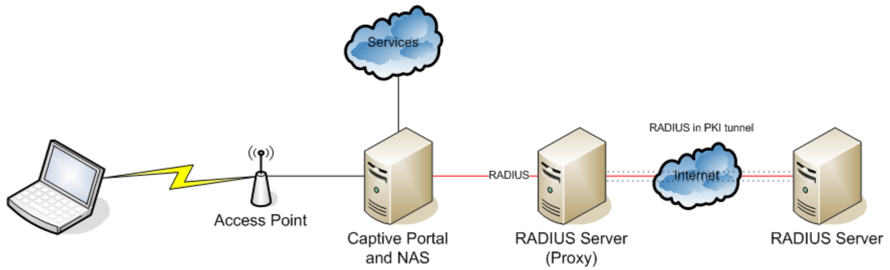
RADIUS Remote Authentication Dial In User Service

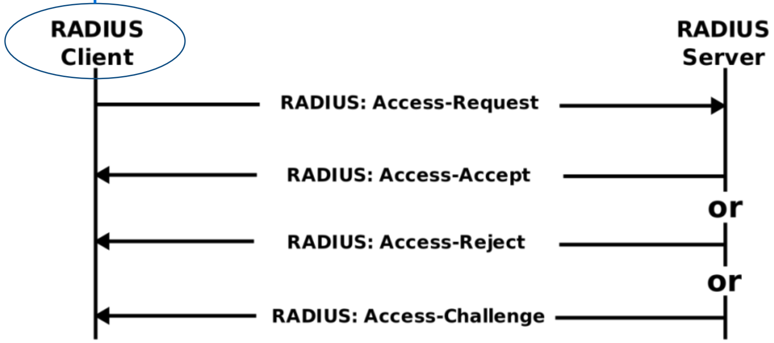
Abstract [2] [5]

- client/server protocol and can use either TCP or UDP.
- Authentication
  - used as a 'simple' authentication method to control
    - who can login to a router (or other device)
    - who can connect using a VPN client
    - the back-end of choice for 802.1X authentication
- Authorization
  - determine the privilege-level when you log in
- Accounting
  - for billing and statistical purposes



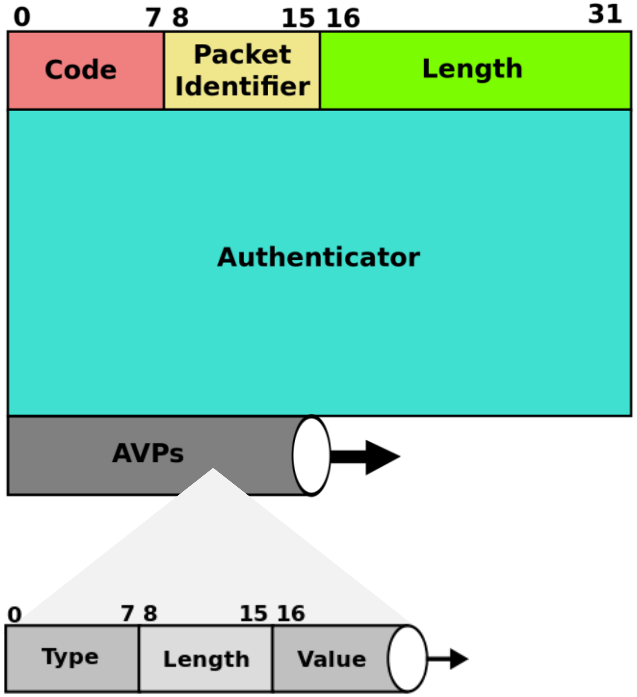
NAS(Network Access Server)





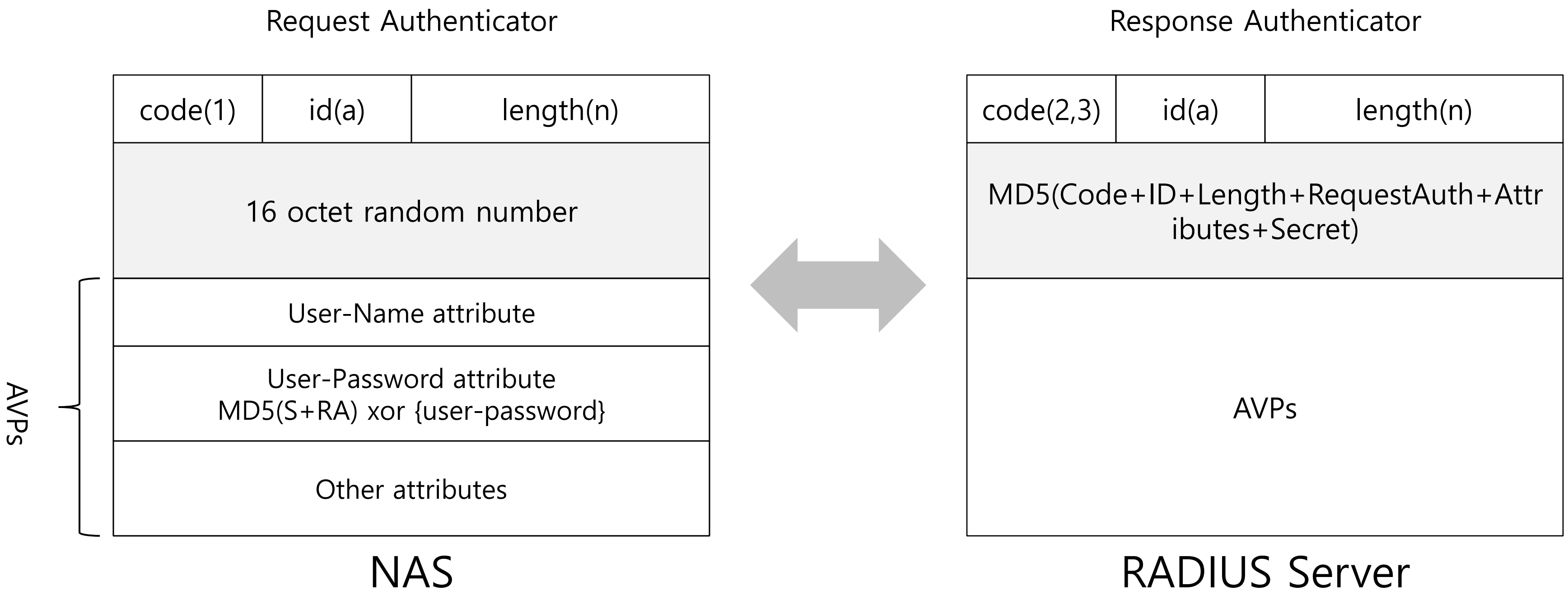
Packet format [5]

- Code
  - Access-Request(1), Access-Accept(2), Access-Reject(3) …
- Authenticator
  - Request Authenticator
  - Response Authenticator
- AVP(Attribute value pairs) or TLV
  - Attribute
    - authentication, authorization, information and configuration details for the request and reply.



Authenticator [2]

- pseudo-random value.
- used in the password hiding algorithm.
- used to authenticate the reply from the RADIUS server.



Attributes – User-Name [2]

Description	• It indicates the name of the user to be authenticated. • It MUST be sent in Access-Request packets. • It MAY be sent in an Access-Accept packet.
Type	1
Length	〉= 3
Value	**text**: Consisting only of UTF-8 encoded 10646 [7] characters. **network access identifier**: A Network Access Identifier as described in RFC 2486 **distinguished name**: A name in ASN.1 form used in Public Key authentication systems.

Attributes – User-Password [2]

Description	• Indicates the password of the user to be authenticated, or the user's input following an Access-Challenge. • It is only used in Access-Request packets. • On transmission, the password is hidden. • break the password into 16-octet chunks and create hash using the **shared secr et** and the **Request Authenticator**.
Type	2
Length	18 ~ 130
Value	String between 16 and 128 octets long

```
b1 = MD5(S + RA)              c(1) = p1 xor b1
b2 = MD5(S + c(1))            c(2) = p2 xor b2
          .                        .
          .                        .
          .                        .
bi = MD5(S + c(i-1))          c(i) = pi xor bi

String = c(1)+c(2)+...+c(i)
```

```
S: shared secret
RA: request authenticator,
```

```
01234567890123456789
```

```
b1 = MD5(s + ra)              c(1) = b1 xor “0123456789012345”
b2 = MD5(s + c(1))            c(2) = b2 xor “56789”
```

Attributes - NAS-IP-Address [2]

Description	• It indicates the identifying IP Address of the NAS. • It is only used in Access-Request packets. • Either NAS-IP-Address or NAS-Identifier MUST be present in an Access-Request packet.
Type	4
Length	6
Value	IPv4 address.

Attributes - NAS-Port [2]

Description	• It indicates the physical port number of the NAS which is authenticating the user. • port is physical connection port. • It is only used in Access-Request packets.
Type	5
Length	6
Value	4 octets

Table of Attributes - rfc 2865

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	1	User-Name
0-1	**0**	**0**	**0**	**2**	**User-Password [Note 1]**
0-1	**0**	**0**	**0**	**3**	**CHAP-Password [Note 1]**
0-1	**0**	**0**	**0**	**4**	**NAS-IP-Address [Note 2]**
0-1	0	0	0	5	NAS-Port
0-1	0-1	0	0	6	Service-Type
0-1	0-1	0	0	7	Framed-Protocol
0-1	0-1	0	0	8	Framed-IP-Address
0-1	0-1	0	0	9	Framed-IP-Netmask
0	0-1	0	0	10	Framed-Routing
0	0+	0	0	11	Filter-Id
0-1	0-1	0	0	12	Framed-MTU
0+	0+	0	0	13	Framed-Compression
0+	0+	0	0	14	Login-IP-Host
0	0-1	0	0	15	Login-Service
0	0-1	0	0	16	Login-TCP-Port
0	0+	0+	0+	18	Reply-Message
0-1	0-1	0	0	19	Callback-Number
0	0-1	0	0	20	Callback-Id
0	0+	0	0	22	Framed-Route
0	0-1	0	0	23	Framed-IPX-Network

[Note 1]
An Access-Request MUST contain either a User-Password or a CHAP-Password or State.
An Access-Request MUST NOT contain both a User-Password and a CHAP-Password.

[Note 2] An Access-Request MUST contain either a NAS-IP-Address or a NAS-Identifier (or both).

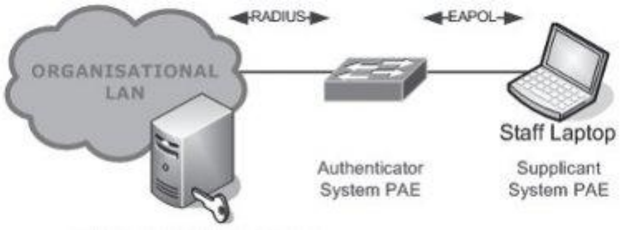
Table of Attributes - rfc 2865

Request	Accept	Reject	Challenge	#	Attribute
0-1	**0-1**	**0**	**0-1**	**24**	**State [Note 1]**
0	0+	0	0	25	Class
0+	0+	0	0+	26	Vendor-Specific
0	0-1	0	0-1	27	Session-Timeout
0	0-1	0	0-1	28	Idle-Timeout
0	0-1	0	0	29	Termination-Action
0-1	0	0	0	30	Called-Station-Id
0-1	0	0	0	31	Calling-Station-Id
0-1	**0**	**0**	**0**	**32**	**NAS-Identifier [Note 2]**
0+	0+	0+	0+	33	Proxy-State
0-1	0-1	0	0	34	Login-LAT-Service
0-1	0-1	0	0	35	Login-LAT-Node
0-1	0-1	0	0	36	Login-LAT-Group
0	0-1	0	0	37	Framed-AppleTalk-Link
0	0+	0	0	38	Framed-AppleTalk-Network
0	0-1	0	0	39	Framed-AppleTalk-Zone
0-1	0	0	0	60	CHAP-Challenge
0-1	0	0	0	61	NAS-Port-Type
0-1	0-1	0	0	62	Port-Limit
0-1	0-1	0	0	63	Login-LAT-Port

IEEE 802.1x / RADIUS support EAP

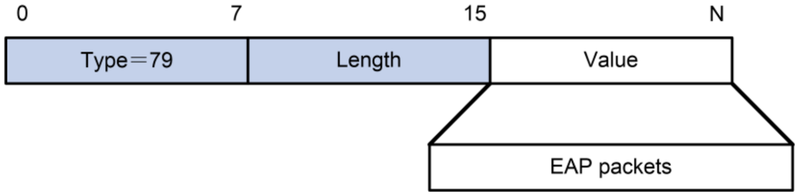
802.1X [6]

- It was developed as a mechanism for preventing unauthorised access to a LAN at the switch port level(NAC, Network Access Control).
  - by extending the EAP protocol over the network.
- EAP is the cornerstone of the 802.1X standard.
- RADIUS provides AAA functions within an organization’s network

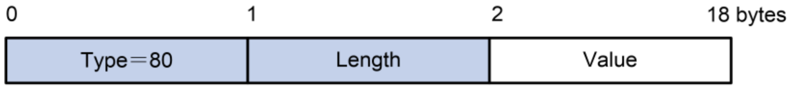


EAP over RADIUS [3] [8]

- RADIUS adds two attributes
  - EAP-Message and Message-Authenticator, for supporting EAP authentication.
  - rfc 3579, September 2003
    - old: rfc 2869, June 2000



EAP-Message attribute format



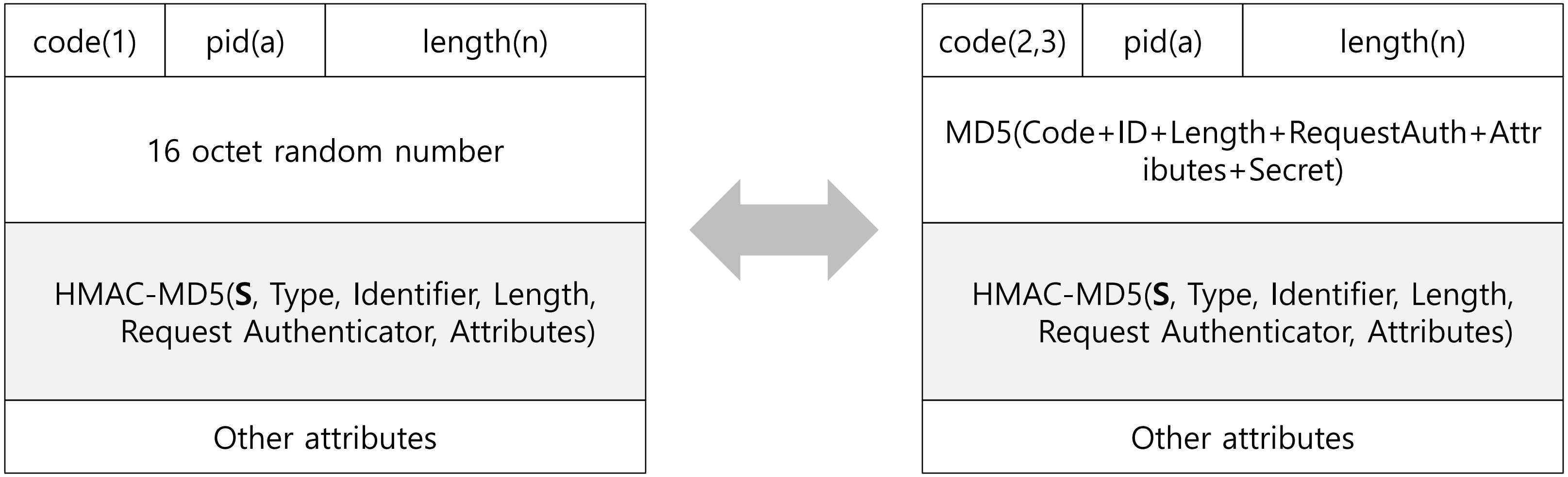
Message-Authenticator attribute format

Attributes - EAP-Message [3]

Description	• The NAS places EAP messages received from the authenticating peer into one or more EAP-Message attributes and forwards them to the RADIUS server within an Access-Request message.
Type	79
Length	〉= 3
Value	EAP packet

Attributes - Message-Authenticator [3]

Description	• It MUST be used in any Access-Request, Access-Accept, Access-Reject or Access-Challenge that includes an EAP-Message attribute. • RADIUS Server and Client MUST **calculate** the correct value of the Message-Authenticator and silently discard the packet if it does not match.
Type	80
Length	18
Value	HMAC-MD5 (**S**, Type, Identifier, Length, Request Authenticator, Attributes)



code(1)	pid(a)	length(n)
16 octet random number		
HMAC-MD5(**S**, Type, Identifier, Length, Request Authenticator, Attributes)		
Other attributes		

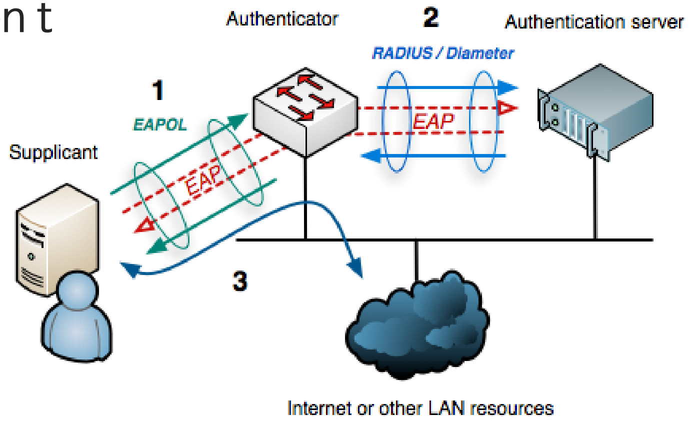
NAS

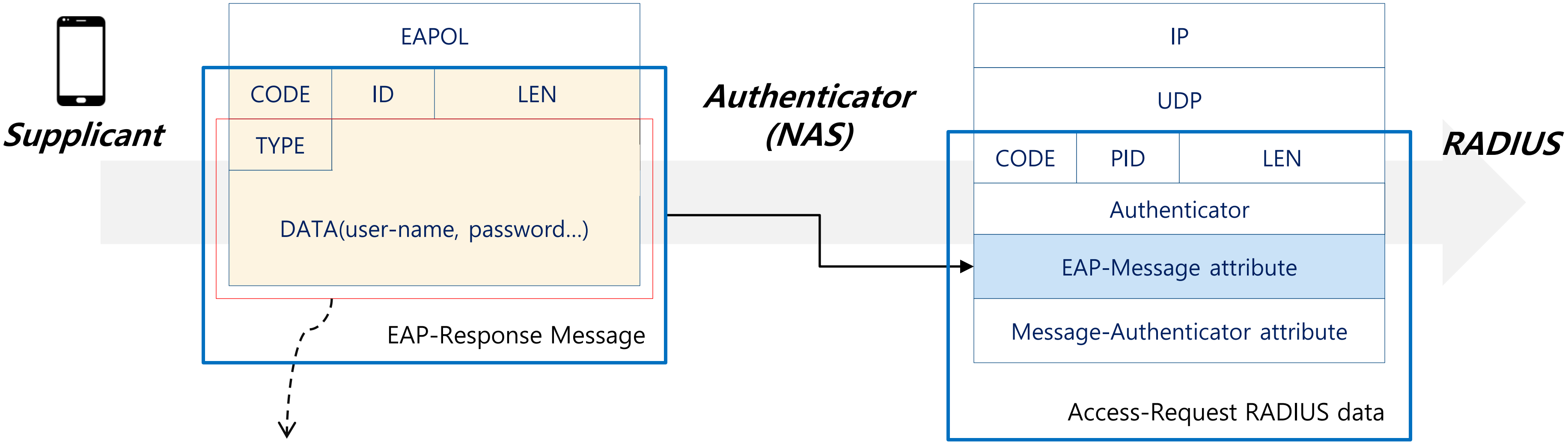
code(2,3)	pid(a)	length(n)
MD5(Code+ID+Length+RequestAuth+Attributes+Secret)		
HMAC-MD5(**S**, Type, Identifier, Length, Request Authenticator, Attributes)		
Other attributes		

RADIUS Server

Authenticator behavior [3]

- Act as a pass-through for an EAP conversation between the peer(supplicant) and authentication server.





Supplicant

EAPOL

CODE | ID | LEN

TYPE

DATA(user-name, password…)

EAP-Response Message

Authenticator (NAS)

IP

UDP

CODE | PID | LEN

Authenticator

EAP-Message attribute

Message-Authenticator attribute

Access-Request RADIUS data

RADIUS

One of
EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST,
EAP-PEAP, EAP-GTC, PEAP-GTC, ….

Table of Attributes - rfc 3579

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	1	User-Name
0	**0**	**0**	**0**	**2**	**User-Password [Note 1]**
0	**0**	**0**	**0**	**3**	**CHAP-Password [Note 1]**
0	0	0	0	18	Reply-Message
0	0	0	0	60	CHAP-Challenge
0	**0**	**0**	**0**	**70**	**ARAP(Apple Remote Access Protocol)-Password [Note 1]**
0	0	0	0	75	Password-Retry
1+	**1+**	**1+**	**1+**	**79**	**EAP-Message [Note 1]**
1	**1**	**1**	**1**	**80**	**Message-Authenticator [Note 1]**
0-1	0	0	0	94	Originating-Line-Info
0	0	0-1	0-1	101	Error-Cause

[Note 1]
An Access-Request that contains either a User-Password or CHAP-Password or ARAP-Password or one or more EAP-Message attributes **MUST NOT contain more than one type of those four attributes**.

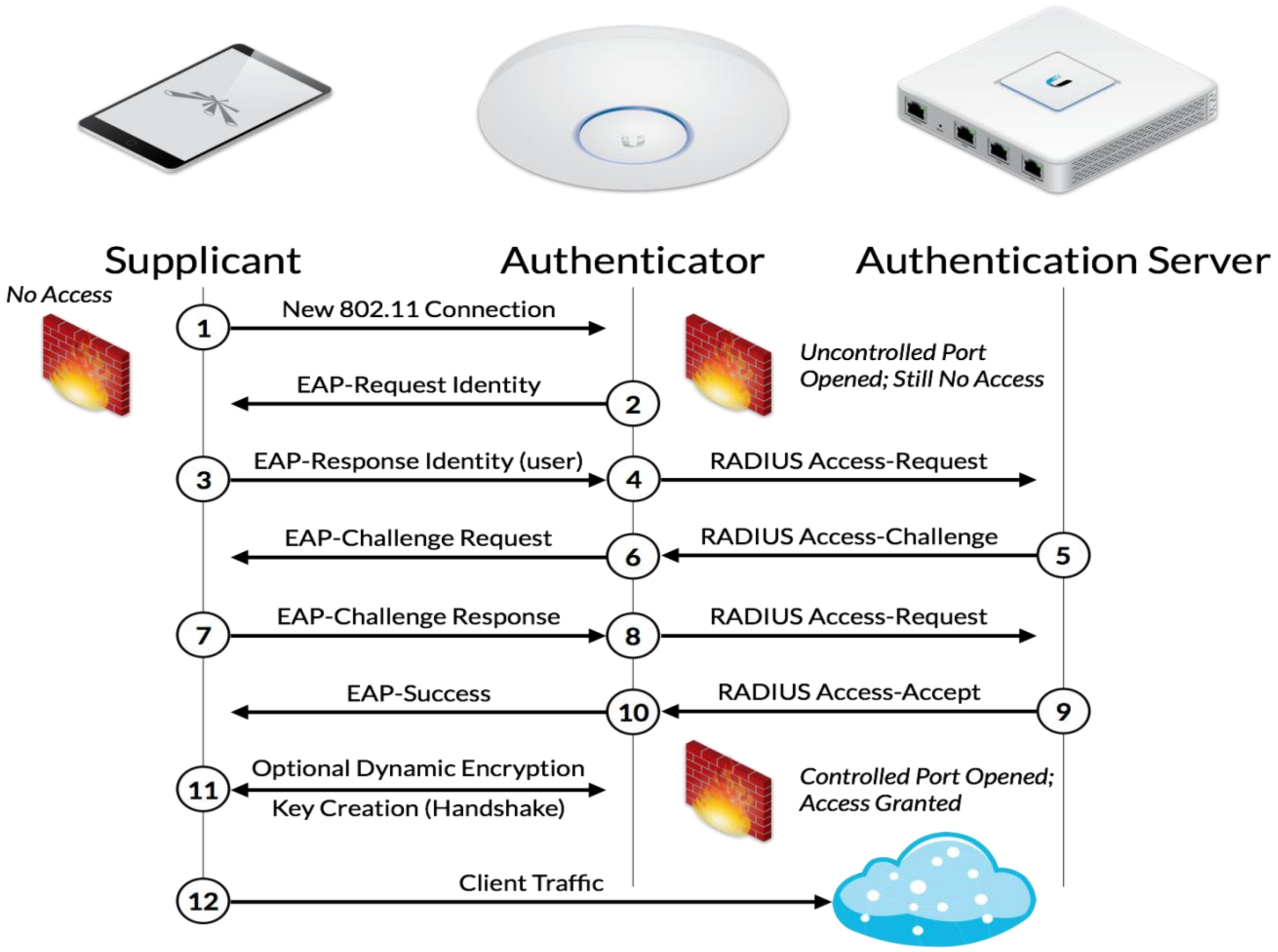
If it does not contain any of those four attributes, it SHOULD contain a Message-Authenticator.

If any packet type contains an EAP-Message attribute it MUST also contain a Message-Authenticator.

A RADIUS server receiving an Access-Request not containing any of those four attributes and also not containing a Message-Authenticator attribute SHOULD silently discard it.

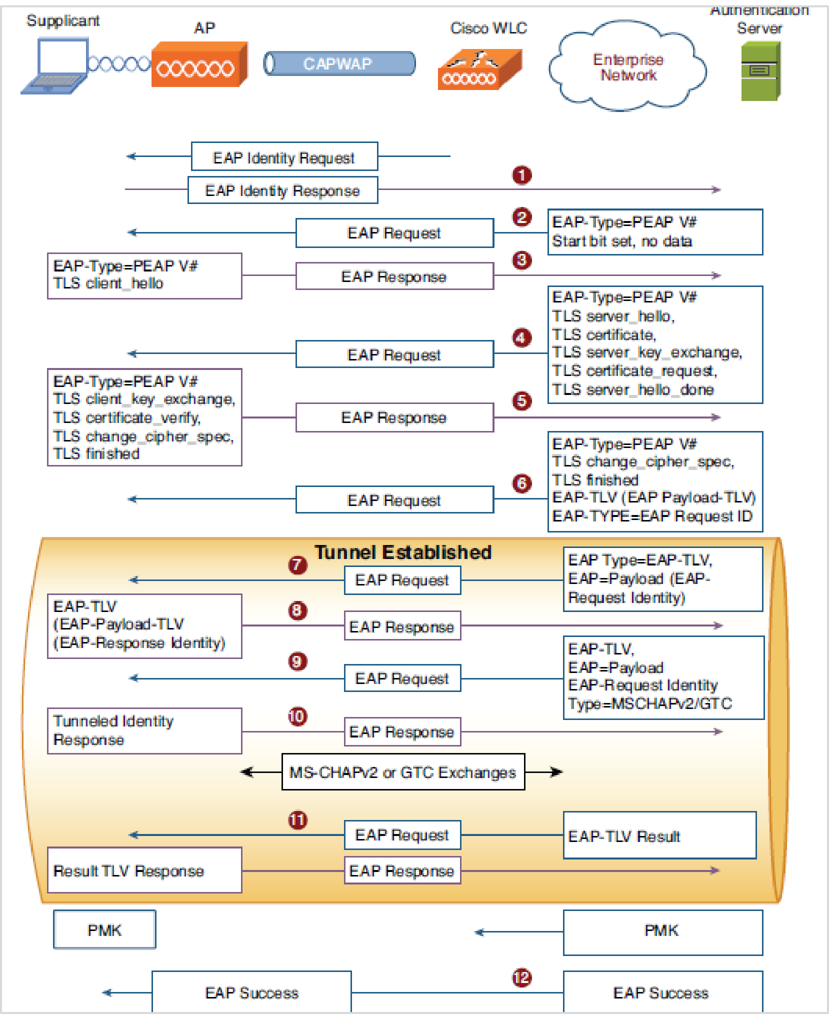
802.1X, EAP and RADIUS [15] [21]

- wireless standards



PEAP / EAP–TLS [17]

PEAP



Supplicant
AP
CAPWAP
Cisco WLC
Enterprise Network
Authentication Server

1
EAP Identity Request
EAP Identity Response

2
EAP Request
EAP-Type=PEAP V#
Start bit set, no data

3
EAP-Type=PEAP V#
TLS client_hello
EAP Response

4
EAP Request
EAP-Type=PEAP V#
TLS server_hello,
TLS certificate,
TLS server_key_exchange,
TLS certificate_request,
TLS server_hello_done

5
EAP-Type=PEAP V#
TLS client_key_exchange,
TLS certificate_verify,
TLS change_cipher_spec,
TLS finished
EAP Response

6
EAP Request
EAP-Type=PEAP V#
TLS change_cipher_spec,
TLS finished
EAP-TLV (EAP Payload-TLV)
EAP-TYPE=EAP Request ID

Tunnel Established

7
EAP Request
EAP Type=EAP-TLV,
EAP=Payload (EAP-Request Identity)

8
EAP-TLV
(EAP-Payload-TLV
(EAP-Response Identity)
EAP Response

9
EAP Request
EAP-TLV,
EAP=Payload
EAP-Request Identity
Type=MSCHAPv2/GTC

10
Tunneled Identity Response
EAP Response

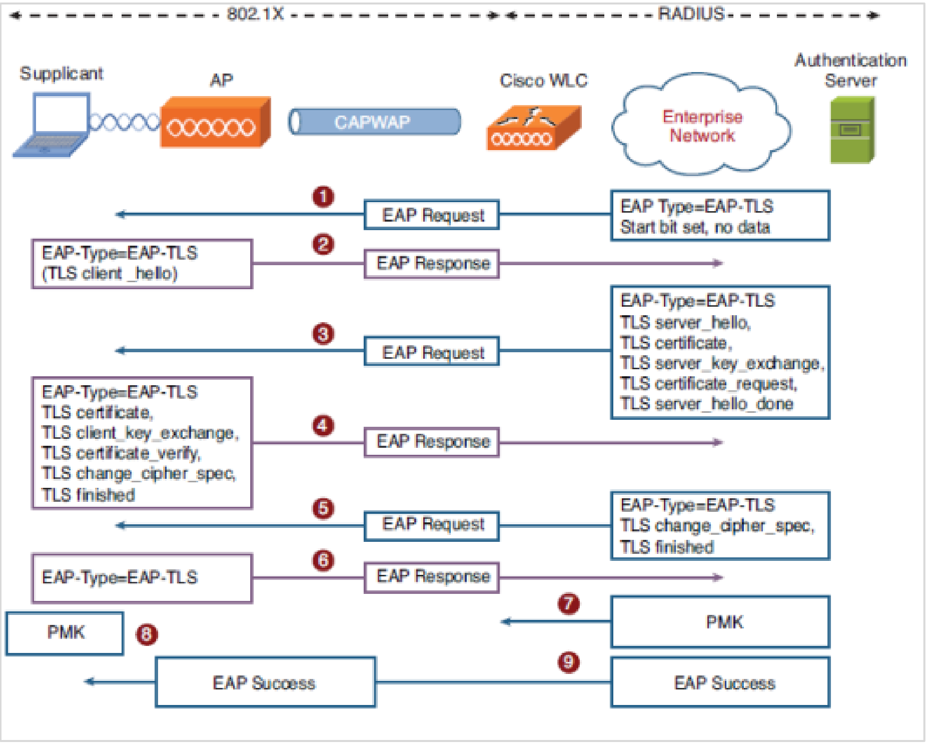
MS-CHAPv2 or GTC Exchanges

11
EAP Request
EAP-TLV Result
Result TLV Response
EAP Response

PMK
PMK

12
EAP Success
EAP Success

EAP-TLS



802.1X
RADIUS
Supplicant
AP
CAPWAP
Cisco WLC
Enterprise Network
Authentication Server

1
EAP Request
EAP Type=EAP-TLS
Start bit set, no data

2
EAP-Type=EAP-TLS
(TLS client _hello)
EAP Response

3
EAP Request
EAP-Type=EAP-TLS
TLS server_hello,
TLS certificate,
TLS server_key_exchange,
TLS certificate_request,
TLS server_hello_done

4
EAP-Type=EAP-TLS
TLS certificate,
TLS client_key_exchange,
TLS certificate_verify,
TLS change_cipher_spec,
TLS finished
EAP Response

5
EAP Request
EAP-Type=EAP-TLS
TLS change_cipher_spec,
TLS finished

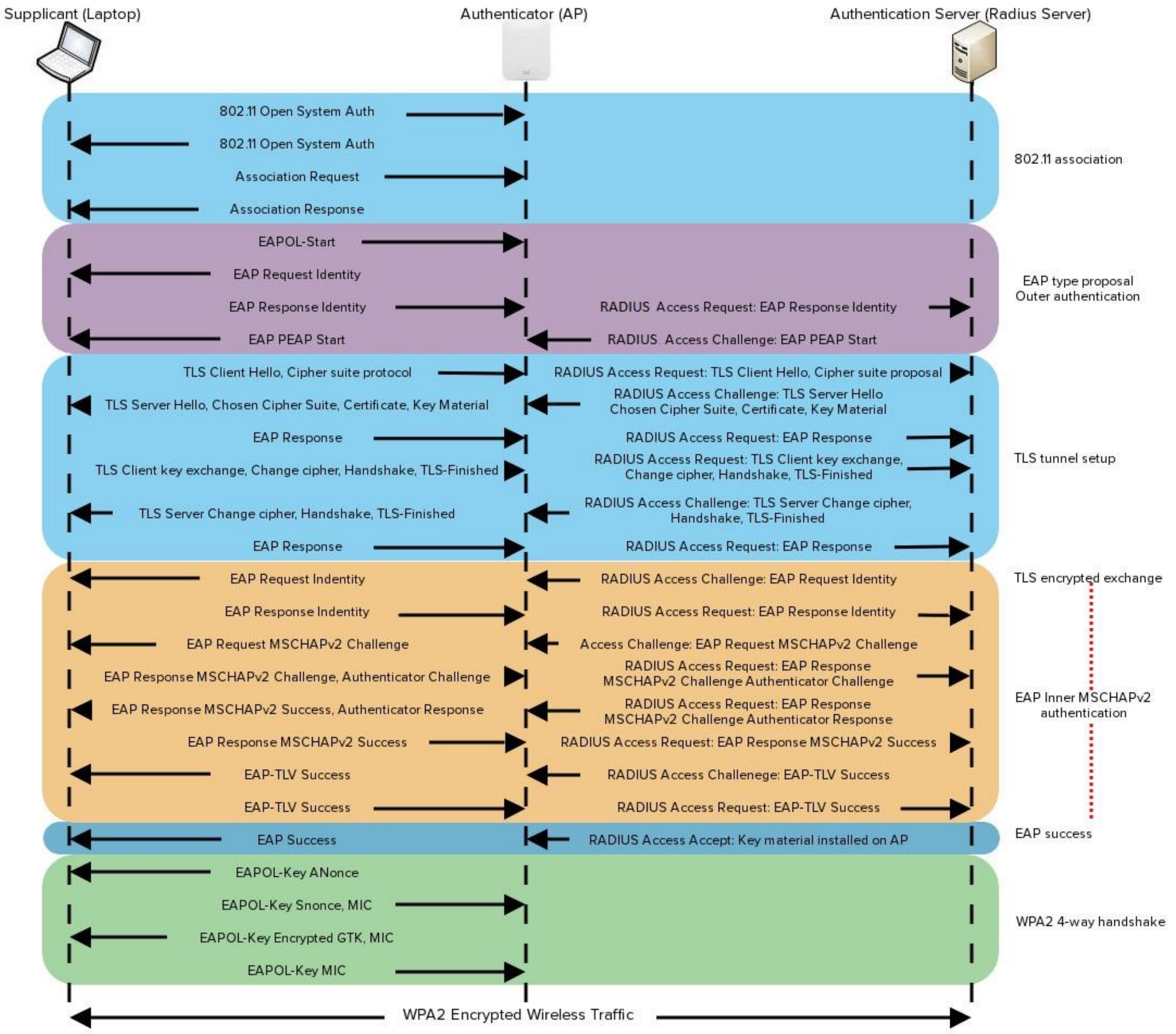
6
EAP-Type=EAP-TLS
EAP Response

7
PMK

8
PMK

9
EAP Success
EAP Success

WPA2 PEAP-MSCHAPv2 [22]



Supplicant (Laptop)

Authenticator (AP)

Authentication Server (Radius Server)

802.11 Open System Auth

802.11 Open System Auth

Association Request

Association Response

802.11 association

EAPOL-Start

EAP Request Identity

EAP Response Identity

RADIUS Access Request: EAP Response Identity

EAP PEAP Start

RADIUS Access Challenge: EAP PEAP Start

EAP type proposal
Outer authentication

TLS Client Hello, Cipher suite protocol

RADIUS Access Request: TLS Client Hello, Cipher suite proposal

TLS Server Hello, Chosen Cipher Suite, Certificate, Key Material

RADIUS Access Challenge: TLS Server Hello
Chosen Cipher Suite, Certificate, Key Material

EAP Response

RADIUS Access Request: EAP Response

TLS Client key exchange, Change cipher, Handshake, TLS-Finished

RADIUS Access Request: TLS Client key exchange,
Change cipher, Handshake, TLS-Finished

TLS Server Change cipher, Handshake, TLS-Finished

RADIUS Access Challenge: TLS Server Change cipher,
Handshake, TLS-Finished

EAP Response

RADIUS Access Request: EAP Response

TLS tunnel setup

EAP Request Indentity

RADIUS Access Challenge: EAP Request Identity

TLS encrypted exchange

EAP Response Indentity

RADIUS Access Request: EAP Response Identity

EAP Request MSCHAPv2 Challenge

Access Challenge: EAP Request MSCHAPv2 Challenge

EAP Response MSCHAPv2 Challenge, Authenticator Challenge

RADIUS Access Request: EAP Response
MSCHAPv2 Challenge Authenticator Challenge

EAP Response MSCHAPv2 Success, Authenticator Response

RADIUS Access Request: EAP Response
MSCHAPv2 Challenge Authenticator Response

EAP Inner MSCHAPv2
authentication

EAP Response MSCHAPv2 Success

RADIUS Access Request: EAP Response MSCHAPv2 Success

EAP-TLV Success

RADIUS Access Challenege: EAP-TLV Success

EAP-TLV Success

RADIUS Access Request: EAP-TLV Success

EAP Success

RADIUS Access Accept: Key material installed on AP

EAP success

EAPOL-Key ANonce

EAPOL-Key Snonce, MIC

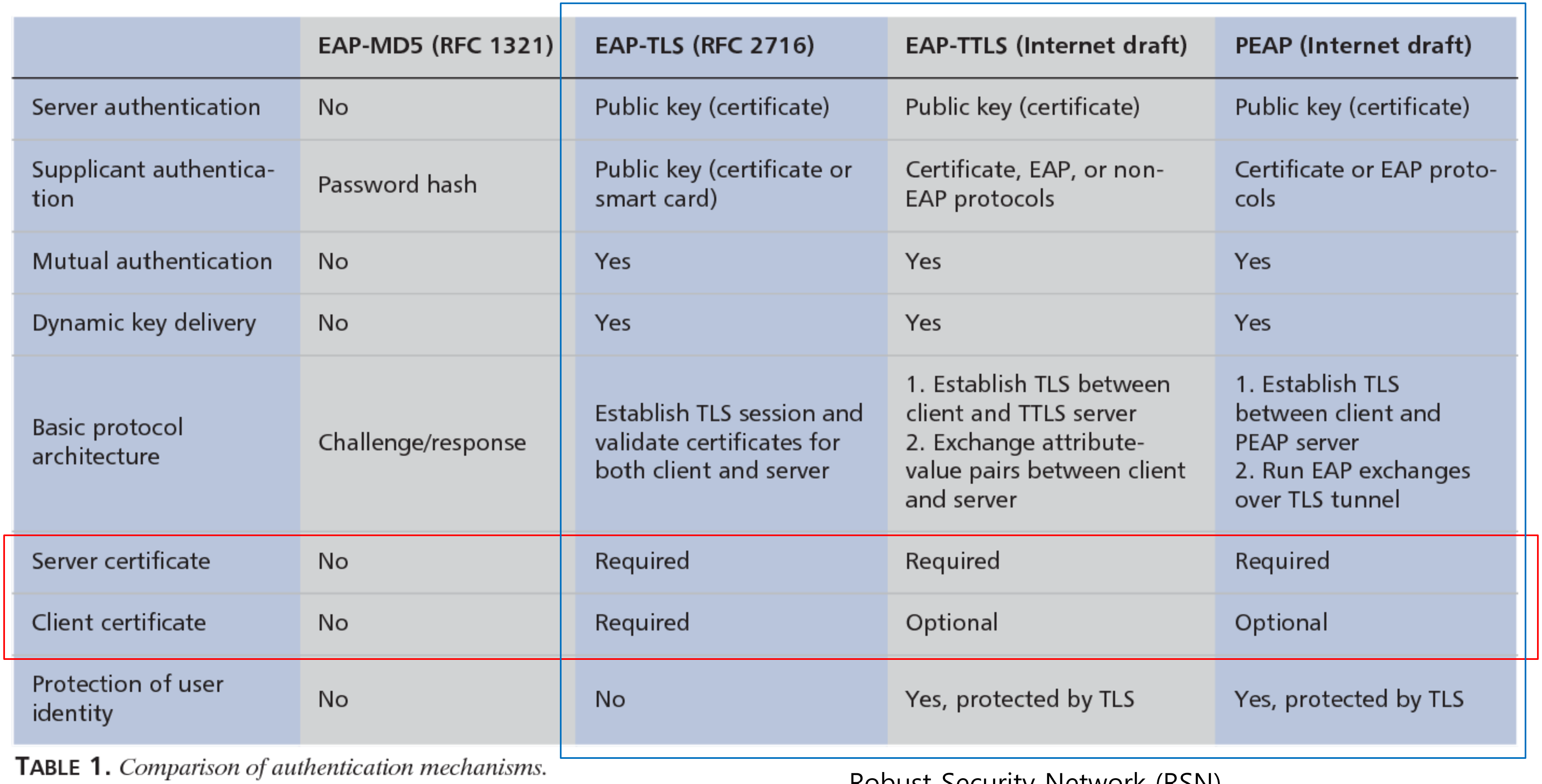
EAPOL-Key Encrypted GTK, MIC

EAPOL-Key MIC

WPA2 4-way handshake

WPA2 Encrypted Wireless Traffic

Comparison of 802.1x authentication mehtods [14]

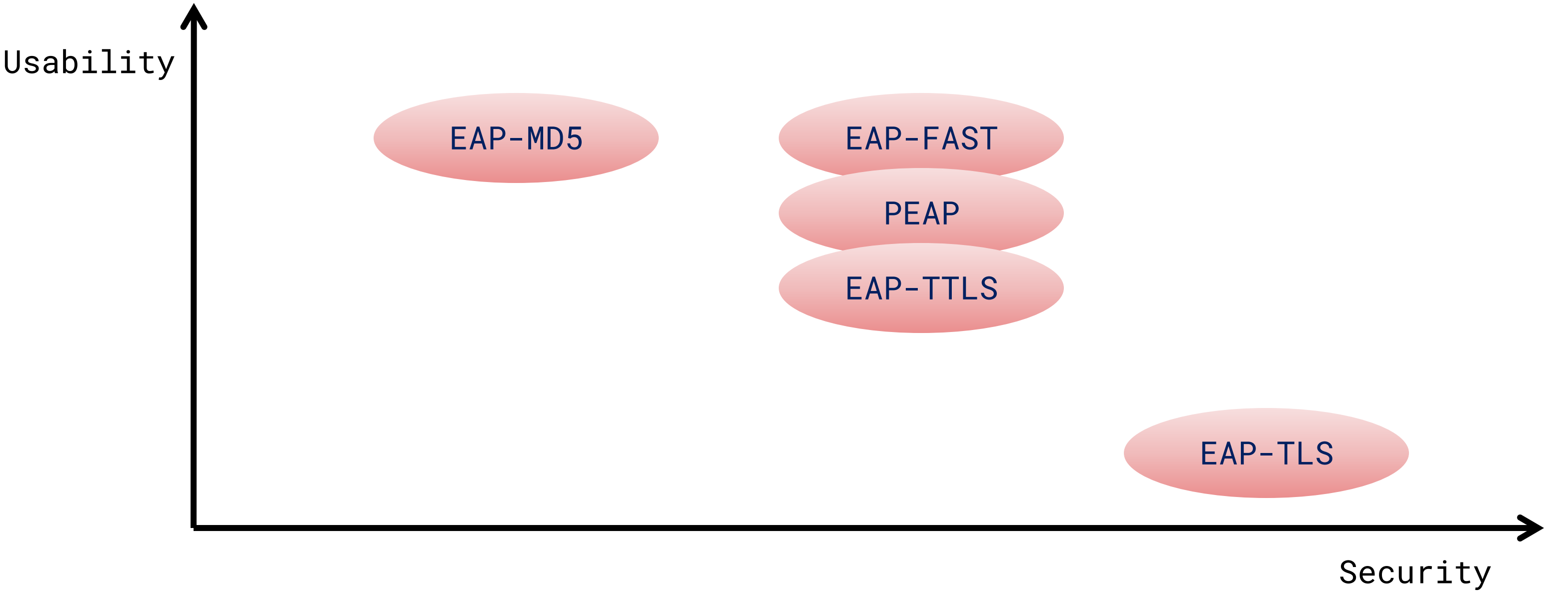


	EAP-MD5 (RFC 1321)	EAP-TLS (RFC 2716)	EAP-TTLS (Internet draft)	PEAP (Internet draft)
Server authentication	No	Public key (certificate)	Public key (certificate)	Public key (certificate)
Supplicant authentication	Password hash	Public key (certificate or smart card)	Certificate, EAP, or non-EAP protocols	Certificate or EAP protocols
Mutual authentication	No	Yes	Yes	Yes
Dynamic key delivery	No	Yes	Yes	Yes
Basic protocol architecture	Challenge/response	Establish TLS session and validate certificates for both client and server	1. Establish TLS between client and TTLS server 2. Exchange attribute-value pairs between client and server	1. Establish TLS between client and PEAP server 2. Run EAP exchanges over TLS tunnel
Server certificate	No	Required	Required	Required
Client certificate	No	Required	Optional	Optional
Protection of user identity	No	No	Yes, protected by TLS	Yes, protected by TLS

TABLE 1. *Comparison of authentication mechanisms.*

Robust Security Network (RSN)

Security and Usability comparison of 802.1x [12]



EAP under WPA/WPA2 Enterprise [12]

- Wi-Fi Protected Access

- WPA-Personal
  - WPA-PSK (pre-shared key)
  - doesn't require an authentication server.
  - wireless network device encrypts the network traffic by a shared key.
- WPA-Enterprise
  - WPA-802.1X mode or WPA
  - designed for enterprise networks and requires a RADIUS authentication server.
  - As of 2010 the certification program includes the following EAP types:
    - EAP-TLS (previously tested)
    - EAP-TTLS/MSCHAPv2 (April 2005)
    - PEAPv0/EAP-MSCHAPv2 (April 2005)
    - PEAPv1/EAP-GTC (April 2005)
    - PEAP-TLS
    - EAP-SIM (April 2005)
    - EAP-AKA (April 2009)
    - EAP-FAST (April 2009)

references

1. What's the difference between RADIUS and 802.1X Port-Based Authentication?
2. rfc 2865, Remote Authentication Dial In User Service (RADIUS)
3. rfc 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
4. rfc 3748, Extensible Authentication Protocol (EAP)
5. https://en.wikipedia.org/wiki/RADIUS
6. IEEE 802.1X implementation at Janet-connected organisations
7. https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
8. https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048061.htm
9. https://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml
10. https://security.stackexchange.com/questions/147344/eap-tls-vs-eap-ttls-vs-eap-peap/149643
11. https://www.wiresandwi.fi/blog/peap-eap-tls-vs-eap-tls
12. http://old.hsn.or.kr/workshop/hsn2006/document/2.22.Wed/Special%20Session/S-4.pdf
13. https://en.wikipedia.org/wiki/Authentication_protocol#DIAMETER
14. Comparison of authentication mechanisms.
15. https://stackoverflow.com/questions/19097125/how-and-where-radius-and-eap-combine/19100330
16. https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
17. EAP Overview
18. rfc 5281, Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
19. https://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-06.txt
20. https://www.ciscopress.com/articles/article.asp?p=369223&seqNum=2
21. https://help.ui.com/hc/en-us/articles/115007253447-Intro-to-Networking-AAA-802-1X-EAP-RADIUS
22. Configuring RADIUS Authentication with WPA2-Enterprise