AN1501: SiWx917 NCP Enterprise Client Application Note

In wireless networks, most of the data transmissions are broadcast over radio waves through the open air. Hence, they are more susceptible to security attacks than wired networks. Network Security is vital in protecting client data and information, keeping shared data secure, ensuring reliable access, network performance, and protection from cyber threats.

This document provides information about how to configure the SiWx917 NCP (Network Co-Processor) device as Enterprise Client, and to connect with Enterprise Secured Access-Point (AP) using any of the EAP-TLS, EAP-TTLS, EAP-FAST, and PEAP methods. For reference, refer to latest enterprise client example in wiseconnect SDK.

Note: For NCP, SiWx917 would be called SiWN917 in the following document sections.

KEY POINTS

- Enterprise security and Enterprise network
- Supported EAP methods and configuration details
- Wireshark captures
- Recommendations

Table of Contents

1. Enterprise Security

Enterprise Security provides the capability to the Wi-Fi devices to connect to enterprise Wi-Fi networks with WPA and WPA2 security that leverage the IEEE 802.1x authentication mechanism using Extensible Authentication Protocol (EAP). EAP is used with an authentication server, which provides strong mutual authentication between the client and the wireless network via the access point.

Enterprise security mode is best suited for businesses and organizations with multiple Wi-Fi clients. Enterprise security mode provides better safety and security compared to the Personal or Pre-Shared Key (PSK) security mode. Securing the Network has three chief aims to,

1. prevent unauthorized access to network resources.
2. detect and stop cyberattacks and security breaches in progress,
3. ensure that authorized users have secure access to the network resources when they need them.

2. Enterprise Network

In Wireless Communication, an enterprise network refers to a wireless network infrastructure within an organization to facilitate seamless communication, data transfer, uninterrupted execution of business applications, and resource sharing among employees, and devices. Enterprise wireless networks are designed to provide reliable and secure wireless connectivity throughout the organization.

Here, a wireless station (supplicant) connects to an enterprise enabled access point. Firstly, Open System Authentication takes place with Authentication Request, Authentication Response, Association Request & Association Response. Once the Open System Authentication phase is completed, the EAP method starts.

The EAP authentication starts with the authenticator sending an EAP Request/Identity frame to the supplicant. The supplicant, on receiving the EAP Request/Identity, responds with EAP Response/Identity, response frame containing its identity information such as Username or User ID. The authenticator then forwards the EAP Response/Identity message to the authentication server (e.g., RADIUS server) for further processing. Depending on the EAP method being used and the security requirements, authentication server sends EAP request/access challenge to authenticator. The authentication server and the supplicant must agree on one EAP method to proceed with the authentication process. Based on the EAP method, EAP requests and EAP responses are sent between supplicant and authentication server until the authentication server responds with EAP-Success or EAP failure packet.

After verifying the supplicant's credentials, the authentication server sends an EAP Success message to the access point if authentication is successful. If authentication fails, the authentication server sends an EAP Failure message.

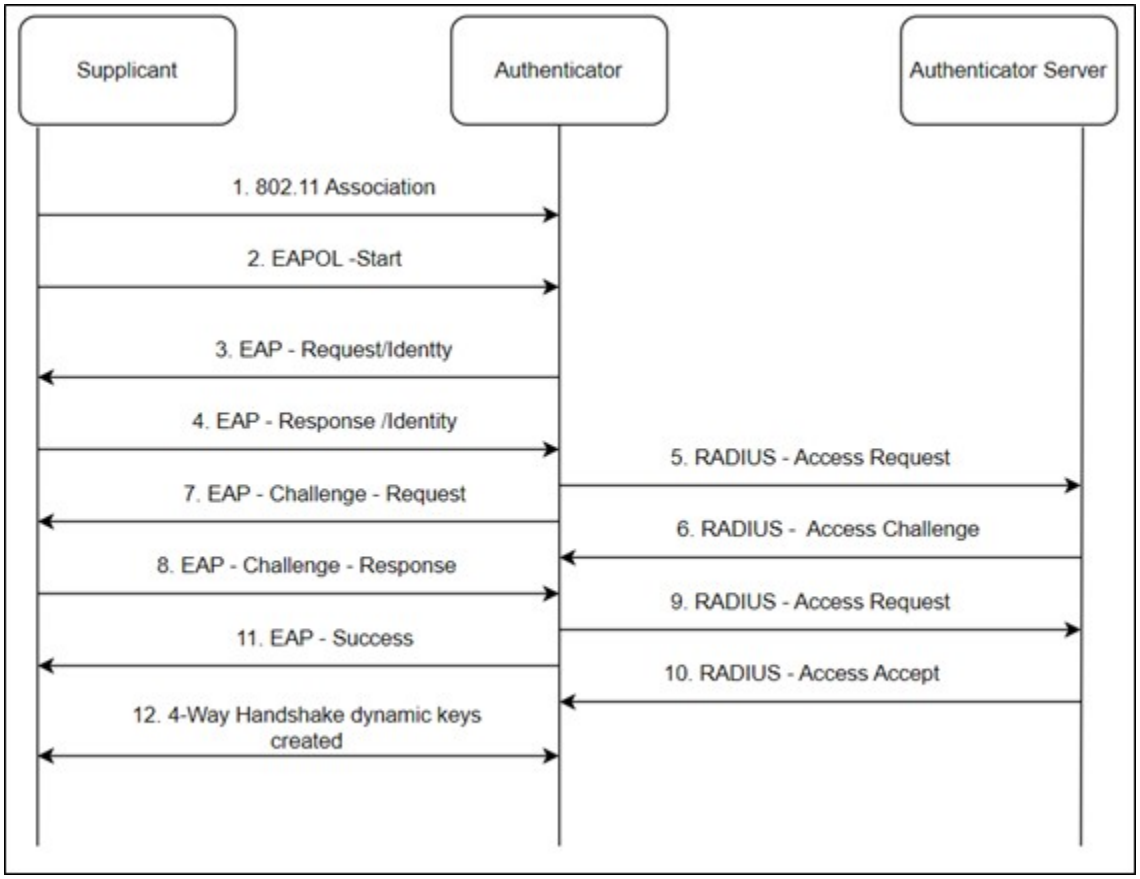


Figure 2.1. Enterprise Network Authentication Flow Diagram

3. EAP Methods

EAP methods are specific authentication mechanisms used within the EAP framework to facilitate the authentication process between a supplicant and an authentication server. These methods define how authentication credentials are exchanged and verified during the EAP authentication process. Here are the EAP methods supported by SiWN917.

3.1 EAP TLS - EAP Transport Layer Protocol

EAP-TLS utilizes mutual authentication and digital certificates to establish a secure TLS-encrypted tunnel between the supplicant and the authentication server. It is considered highly secure and is widely used in enterprise environments that require strong authentication.

- The supplicant sends an EAPOL-Start message to the access point (AP) to initiate the EAP authentication process.
- The EAP server must respond with EAP Request/Identity message to the supplicant with EAP-Type set to EAP-TLS, the Start(S) bit is set (True) and without any data and asks the supplicants to provide its identity.
- The supplicant then sends an EAP-Response packet with EAP-Type to EAP-TLS, containing a TLS client_hello along with the cipher suites supported, in the handshake message.
- The EAP server, then responds with a handshake message – server_hello (with the cipher suite picked and supported), TLS certificate, server_key_exchange, certificate_request, server_hello_done.
- The Client must respond to the EAP-Request with an EAP-Response packet of EAP-Type set to EAP-TLS. And the authentication server starts verifying the data sent by supplicant like TLS certificate verify, TLS client_key_exchange, change_cipher_spec.
- If a ChangeCipherSpec message is sent by the client and the server responds with its own ChangeCipherSpec message to confirm the change to new Cipher Spec.
- If the EAP server authenticates successfully, the peer must send an EAP-Response packet of EAP-Type to EAP-TLS
- The EAP server then responds with an EAP-Success message.

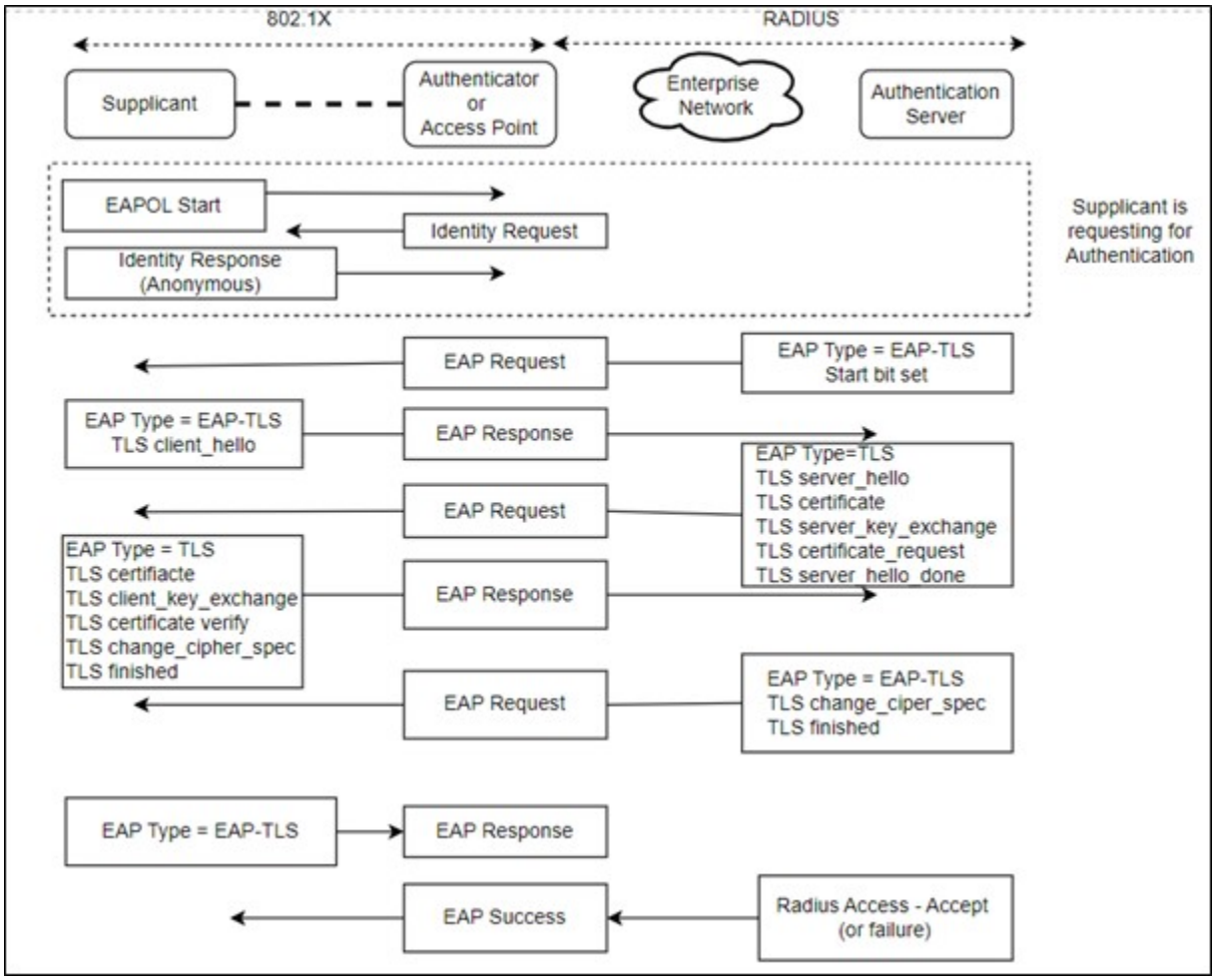


Figure 3.1. EAP - TLS Method

3.1.1 Configuring SiWN917 in EAP-TLS

To configure SiWN917 in EAP-TLS, follow the steps below:

- Change the security type to SL_WIFI_WPA2_ENTERPRISE. Supported Enterprise client securities are:
  - WPA-EAP: SL_WIFI_WPA_ENTERPRISE
  - WPA2-EAP: SL_WIFI_WPA2_ENTERPRISE
- Change the encryption type to SL_WIFI_EAP_TLS_ENCRYPTION.
- Mostly, EAP-TLS method uses root CA certificate and public-private key pairs for authentication.

Note: To know more about loading certificates, and other configurations, refer to the readme.

3.2 EAP TTLS - EAP Tunneled Transport Layer Security

EAP-TTLS was developed as an extension of the EAP-TLS (Transport Layer Security) protocol. It provides a way to secure the authentication process while still using existing username and password-based authentication mechanisms. In EAP-TTLS, the authentication process is divided into two phases, the tunnel establishment phase and the authentication phase.

Tunnel Establishment: This phase sets up a secure tunnel between the client and the authentication server using Transport Layer Security (TLS) to provide encryption and integrity protection. And this phase protects the subsequent authentication process within the tunnel, including the exchange of credentials.

Authentication: Once the secure tunnel is established, the client sends its credentials (typically a username and password) to the authentication server. The server authorizes client access based on the authentication and authorization results. If successful, the authentication process ends and provides a successful connection.

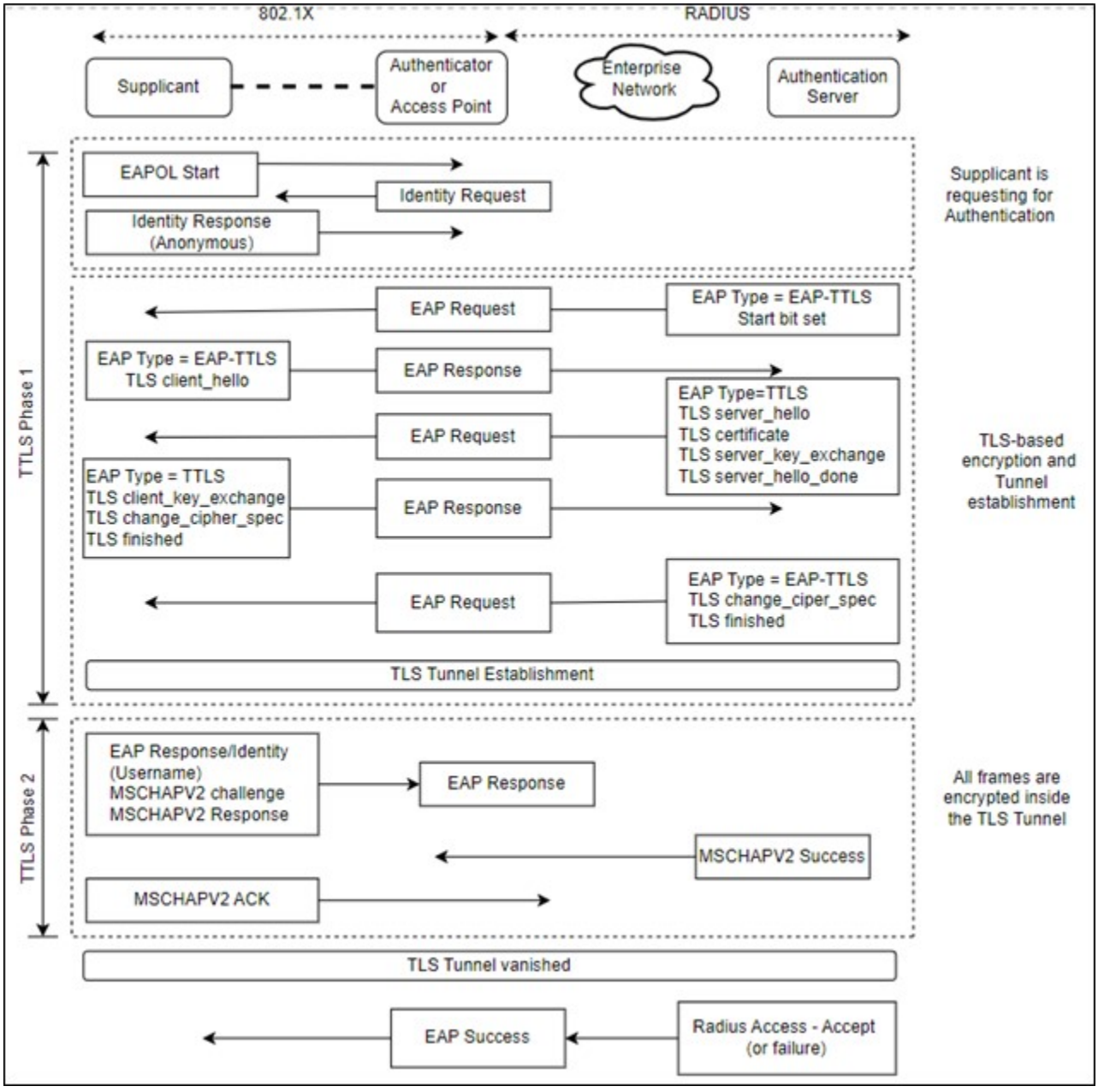


Figure 3.2. EAP - TTLS Method

3.2.1 Configuring SiWN917 in EAP-TTLS

To configure SiWN917 in EAP-TLS, follow the steps below

- •Change the security type to SL_WIFI_WPA2_ENTERPRISE. Supported Enterprise client securities are:
  - WPA-EAP: SL_WIFI_WPA_ENTERPRISE
  - WPA2-EAP: SL_WIFI_WPA2_ENTERPRISE
- Change the encryption type to SL_WIFI_EAP_TTLS_ENCRYPTION.

Note: To know more about loading certificates, and other configurations, refer to the readme.

3.3 EAP PEAP - EAP Protected Extensible Authentication Protocol

The Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

PEAP is similar to EAP-TTLS in design, requiring only a server-side certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. The tunnel method is also referred to as the "inner method" and provides user authentication.

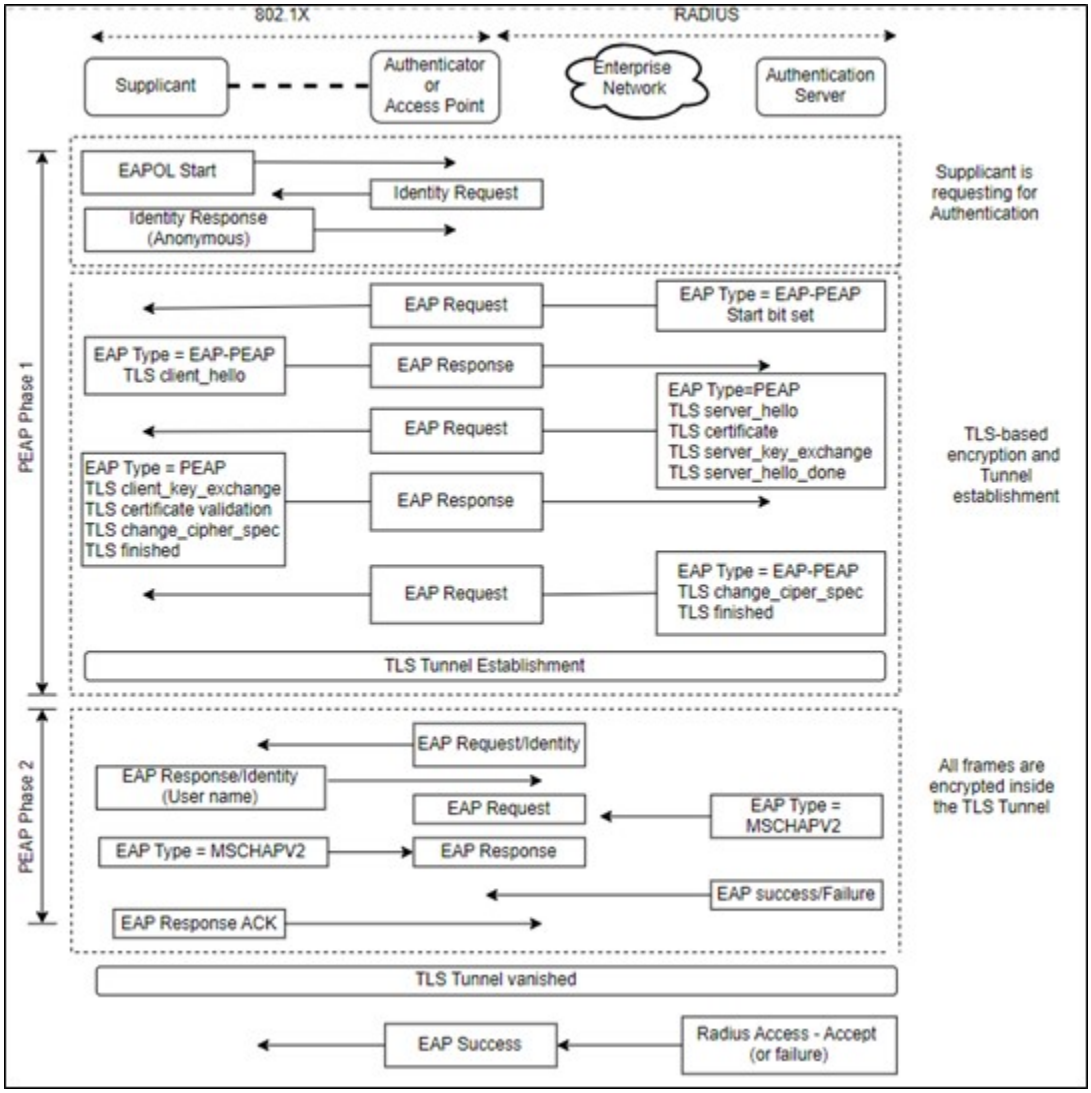


Figure 3.3. EAP - PEAP Method

3.3.1 Configuring SiWN917 in EAP-PEAP

To configure SiWN917 in EAP-TLS, follow the steps below:

- Change the security type to SL_WIFI_WPA2_ENTERPRISE. Supported Enterprise client securities are:
  - WPA-EAP: SL_WIFI_WPA_ENTERPRISE
  - WPA2-EAP: SL_WIFI_WPA2_ENTERPRISE
- Change the encryption type to SL_WIFI_PEAP_MSCHAPV2_ENCRYPTIONS.
- Supported inner method in SiWN917 is MSCHAPV2.

Note: To know more about loading certificates, and other configurations, refer to the readme.

3.4 EAP FAST - EAP Flexible Authentication via Secure Tunneling

In EAP FAST, Use of server certificates is optional and uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified and ensure a secure connection. These PAC files can be provisioned either AUTO or MANUAL.

1. Auto Provisioning (PAC file is not required)
2. Manual Provisioning (PAC file is required)

1. Auto Provisioning:

The connection between the AP and the client is done without loading the PAC file into the Client. And this can be done in 2 ways,

Internal Radius server: Some Access Points have this feature, configure the Access Point in the Enterprise mode by selecting an option for the Internal radius server and add a WLAN user with the username, password, and Shared secret. Configure the client in EAP-FAST and enter the username and Password as mentioned in the Access Point.

External Radius server: There is no specific Access Point required here, Any Access Point supporting EAP can be used. Configure the radius server for EAP-FAST and add the IP address of the PC running the radius server in Access Point settings. Configure the client in EAP-FAST and enter the username and Password as mentioned in the radius server.

2. Manual Provisioning:

The connection between the AP and the client is done only when the PAC file is loaded into the Client.

This can be done by using both internal and external radius servers. Any Access Point supporting EAP can be used. Configure the radius server for EAP-FAST and add the IP address of the PC running the radius server in AP settings. Configure the client in EAP-FAST, load the PAC file and enter the username and Password as mentioned in the radius server.

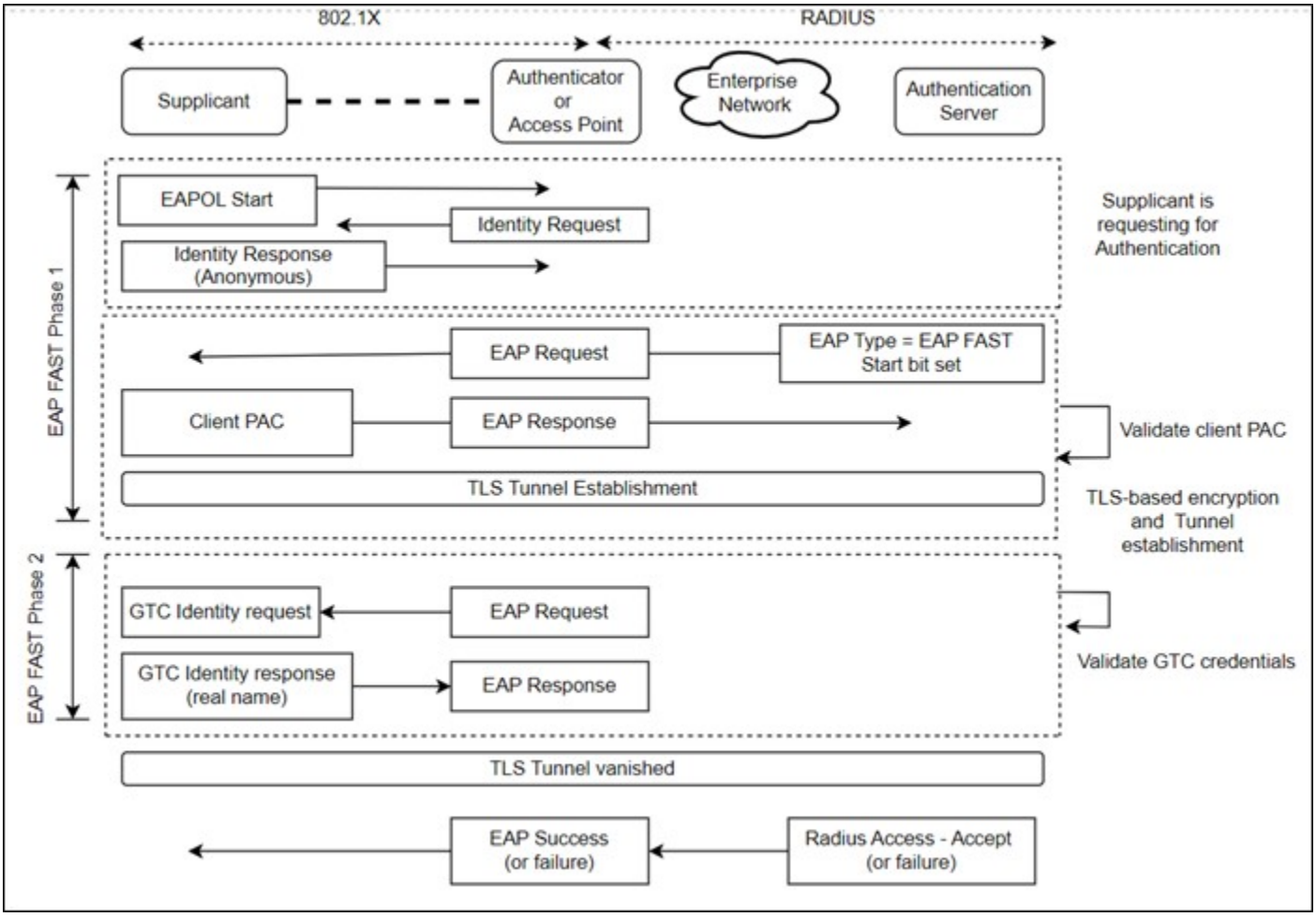


Figure 3.4. EAP - FAST Method

3.4.1 Configuring SiWN917 in EAP-FAST

To configure SiWN917 in EAP-FAST, follow the ste[s below:

- Change the security type to SL_WIFI_WPA2_ENTERPRISE. Supported Enterprise client securities are,
  - WPA-EAP: SL_WIFI_WPA_ENTERPRISE
  - WPA2-EAP: SL_WIFI_WPA2_ENTERPRISE
- Change the encryption type to SL_WIFI_EAP_FAST_ENCRYPTION.

Note: To know more about loading certificates, and other configurations, refer to the readme.

4. Cipher Suites Supported

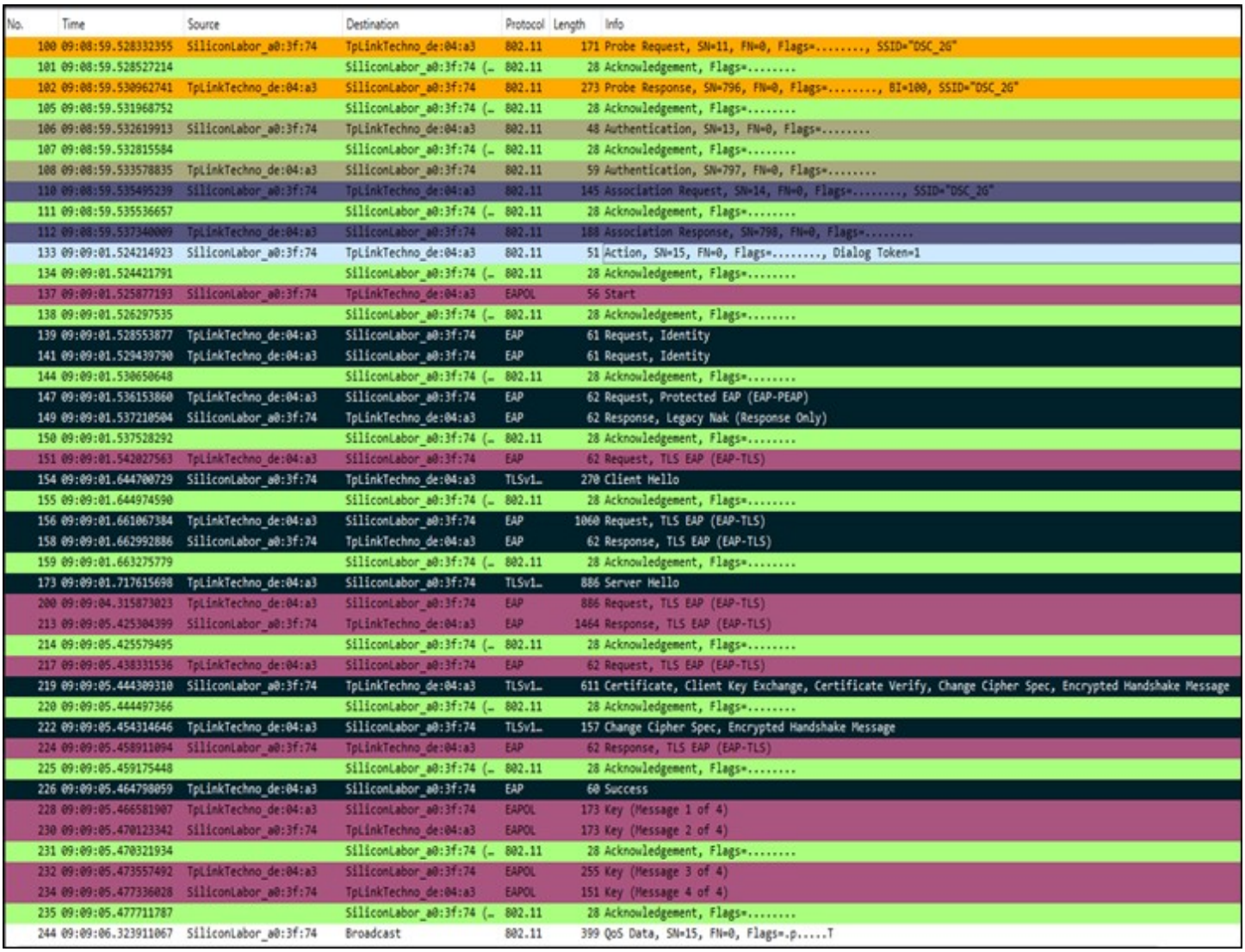
Below is the list of 11 cipher suites supported by the SiWN917

- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA
- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- RC4-SHA
- DES-CBC3-SHA
- RC4-MD5

5. Wireshark Captures

In this section, we can see the on-air sniffer captures (Wireshark captures) of different EAP methods.

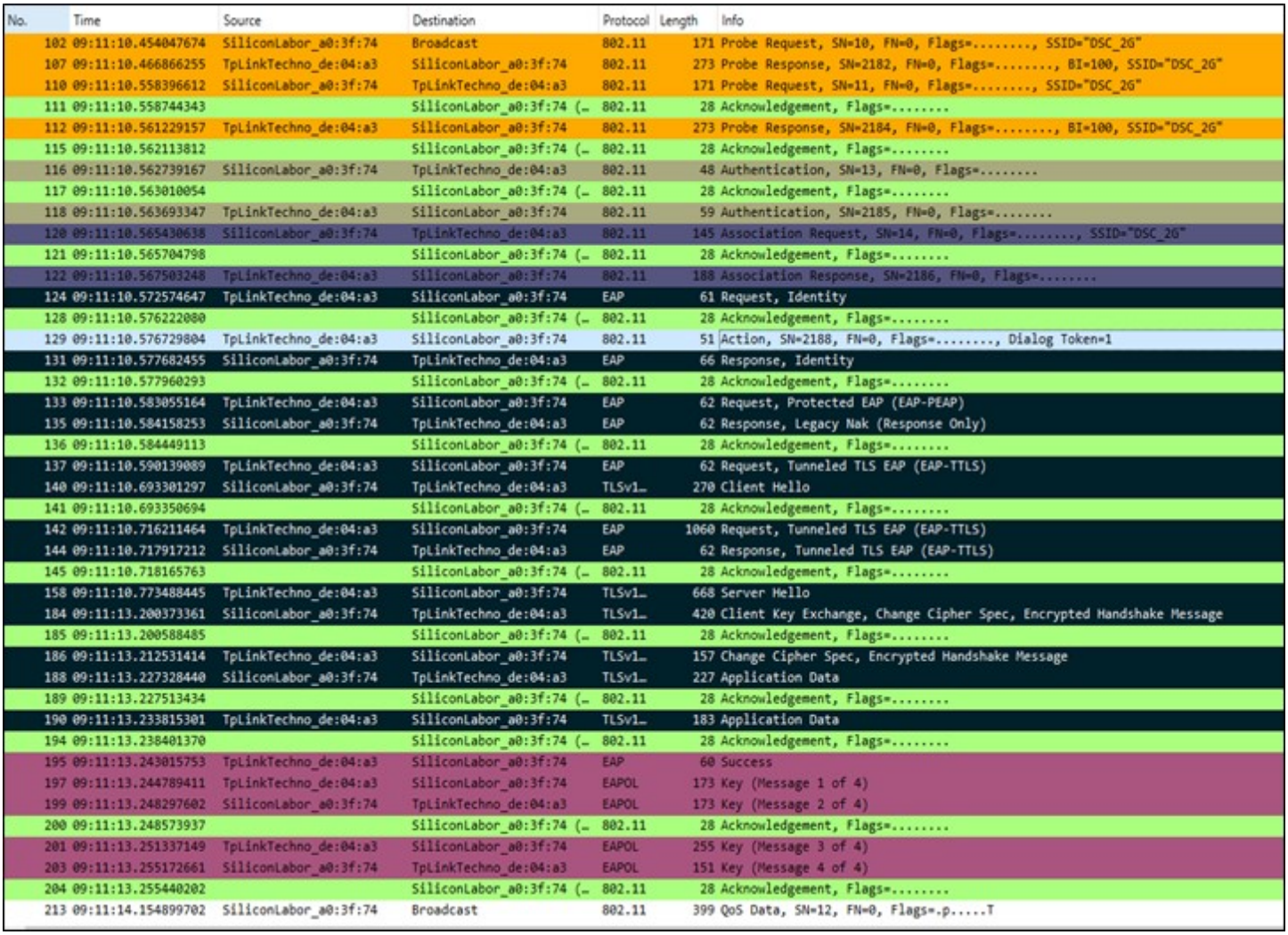
5.1 EAP-TLS



No.	Time	Source	Destination	Protocol	Length	Info
100	09:08:59.528332355	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	171	Probe Request, SN=11, FN=0, Flags=........, SSID="DSC_2G"
101	09:08:59.528527214		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
102	09:08:59.530962741	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	273	Probe Response, SN=796, FN=0, Flags=........, BI=100, SSID="DSC_2G"
105	09:08:59.531968752		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
106	09:08:59.532619913	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	48	Authentication, SN=13, FN=0, Flags=........
107	09:08:59.532815584		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
108	09:08:59.533578835	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	59	Authentication, SN=797, FN=0, Flags=........
110	09:08:59.535495239	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	145	Association Request, SN=14, FN=0, Flags=........, SSID="DSC_2G"
111	09:08:59.535536657		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
112	09:08:59.537340009	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	188	Association Response, SN=798, FN=0, Flags=........
133	09:09:01.524214923	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	51	Action, SN=15, FN=0, Flags=........, Dialog Token=1
134	09:09:01.524421791		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
137	09:09:01.525877193	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	56	Start
138	09:09:01.526297535		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
139	09:09:01.528553877	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	61	Request, Identity
141	09:09:01.529439790	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	61	Request, Identity
144	09:09:01.530650648		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
147	09:09:01.536153860	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, Protected EAP (EAP-PEAP)
149	09:09:01.537210504	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Legacy Nak (Response Only)
150	09:09:01.537528292		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
151	09:09:01.542027563	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, TLS EAP (EAP-TLS)
154	09:09:01.644700729	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	270	Client Hello
155	09:09:01.644974590		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
156	09:09:01.661067384	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	1060	Request, TLS EAP (EAP-TLS)
158	09:09:01.662992886	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, TLS EAP (EAP-TLS)
159	09:09:01.663275779		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
173	09:09:01.717615698	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	886	Server Hello
200	09:09:04.315873023	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	886	Request, TLS EAP (EAP-TLS)
213	09:09:05.425304399	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	1464	Response, TLS EAP (EAP-TLS)
214	09:09:05.425579495		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
217	09:09:05.438331536	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, TLS EAP (EAP-TLS)
219	09:09:05.444309310	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	611	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
220	09:09:05.444497366		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
222	09:09:05.454314646	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	157	Change Cipher Spec, Encrypted Handshake Message
224	09:09:05.458911094	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, TLS EAP (EAP-TLS)
225	09:09:05.459175448		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
226	09:09:05.464798059	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	60	Success
228	09:09:05.466581907	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	173	Key (Message 1 of 4)
230	09:09:05.470123342	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	173	Key (Message 2 of 4)
231	09:09:05.470321934		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
232	09:09:05.473557492	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	255	Key (Message 3 of 4)
234	09:09:05.477336028	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	151	Key (Message 4 of 4)
235	09:09:05.477711787		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
244	09:09:06.323911067	SiliconLabor_a0:3f:74	Broadcast	802.11	399	QoS Data, SN=15, FN=0, Flags=.p.....T

Figure 5.1. EAP-TLS Wireshark Capture

5.2 EAP-TTLS



No.	Time	Source	Destination	Protocol	Length	Info
102	09:11:10.454047674	SiliconLabor_a0:3f:74	Broadcast	802.11	171	Probe Request, SN=10, FN=0, Flags=........, SSID="DSC_2G"
107	09:11:10.466866255	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	273	Probe Response, SN=2182, FN=0, Flags=........, BI=100, SSID="DSC_2G"
110	09:11:10.558396612	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	171	Probe Request, SN=11, FN=0, Flags=........, SSID="DSC_2G"
111	09:11:10.558744343		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
112	09:11:10.561229157	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	273	Probe Response, SN=2184, FN=0, Flags=........, BI=100, SSID="DSC_2G"
115	09:11:10.562113812		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
116	09:11:10.562739167	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	48	Authentication, SN=13, FN=0, Flags=........
117	09:11:10.563010054		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
118	09:11:10.563693347	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	59	Authentication, SN=2185, FN=0, Flags=........
120	09:11:10.565430638	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	145	Association Request, SN=14, FN=0, Flags=........, SSID="DSC_2G"
121	09:11:10.565704798		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
122	09:11:10.567503248	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	188	Association Response, SN=2186, FN=0, Flags=........
124	09:11:10.572574647	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	61	Request, Identity
128	09:11:10.576222080		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
129	09:11:10.576729804	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	51	Action, SN=2188, FN=0, Flags=........, Dialog Token=1
131	09:11:10.577682455	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	66	Response, Identity
132	09:11:10.577960293		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
133	09:11:10.583055164	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, Protected EAP (EAP-PEAP)
135	09:11:10.584158253	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Legacy Nak (Response Only)
136	09:11:10.584449113		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
137	09:11:10.590139089	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, Tunneled TLS EAP (EAP-TTLS)
140	09:11:10.693301297	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	270	Client Hello
141	09:11:10.693350694		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
142	09:11:10.716211464	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	1060	Request, Tunneled TLS EAP (EAP-TTLS)
144	09:11:10.717917212	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Tunneled TLS EAP (EAP-TTLS)
145	09:11:10.718165763		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
158	09:11:10.773488445	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	668	Server Hello
184	09:11:13.200373361	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	420	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
185	09:11:13.200588485		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
186	09:11:13.212531414	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	157	Change Cipher Spec, Encrypted Handshake Message
188	09:11:13.227328440	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	227	Application Data
189	09:11:13.227513434		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
190	09:11:13.233815301	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	183	Application Data
194	09:11:13.238401370		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
195	09:11:13.243015753	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	60	Success
197	09:11:13.244789411	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	173	Key (Message 1 of 4)
199	09:11:13.248297602	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	173	Key (Message 2 of 4)
200	09:11:13.248573937		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
201	09:11:13.251337149	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	255	Key (Message 3 of 4)
203	09:11:13.255172661	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	151	Key (Message 4 of 4)
204	09:11:13.255440202		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
213	09:11:14.154899702	SiliconLabor_a0:3f:74	Broadcast	802.11	399	QoS Data, SN=12, FN=0, Flags=.p.....T

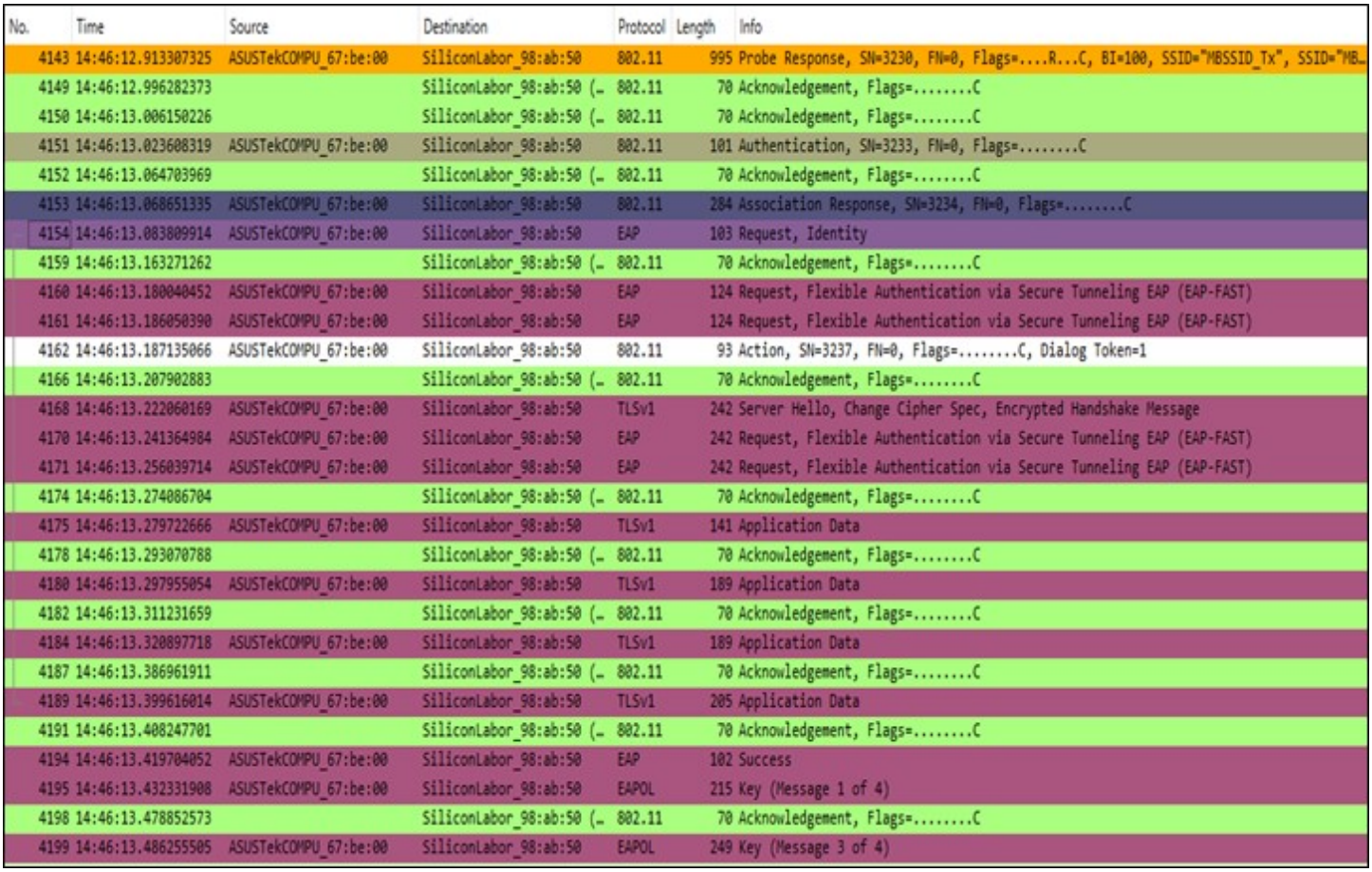
Figure 5.2. EAP-TTLS Wireshark Capture

5.3 EAP-PEAP

No.	Time	Source	Destination	Protocol	Length	Info
80	09:16:49.782092167	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	171	Probe Request, SN=11, FN=0, Flags=........, SSID="DSC_2G"
81	09:16:49.782331933		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
82	09:16:49.784693436	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	273	Probe Response, SN=1717, FN=0, Flags=........, BI=100, SSID="DSC_2G"
85	09:16:49.785770539		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
86	09:16:49.786342181	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	48	Authentication, SN=13, FN=0, Flags=........
87	09:16:49.786657307		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
88	09:16:49.787366253	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	59	Authentication, SN=1718, FN=0, Flags=........
90	09:16:49.789252054	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	802.11	145	Association Request, SN=14, FN=0, Flags=........, SSID="DSC_2G"
91	09:16:49.789377649		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
92	09:16:49.791088591	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	188	Association Response, SN=1719, FN=0, Flags=........
115	09:16:51.778624388		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
116	09:16:51.779167114	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	802.11	51	Action, SN=1740, FN=0, Flags=........, Dialog Token=1
118	09:16:51.780108695	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	56	Start
119	09:16:51.780336143		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
122	09:16:51.783836958	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	61	Request, Identity
124	09:16:51.784799804	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	66	Response, Identity
125	09:16:51.784963003		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
126	09:16:51.785574947	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	66	Response, Identity
127	09:16:51.785991446		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
128	09:16:51.790769383	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	62	Request, Protected EAP (EAP-PEAP)
131	09:16:51.894445860	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	274	Client Hello
132	09:16:51.894622534		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
133	09:16:51.916424812	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	1060	Request, Protected EAP (EAP-PEAP)
135	09:16:51.918276989	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Protected EAP (EAP-PEAP)
140	09:16:51.933060341		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
146	09:16:51.962291009	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	1056	Request, Protected EAP (EAP-PEAP)
148	09:16:51.963936478	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Protected EAP (EAP-PEAP)
149	09:16:51.964115017		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
150	09:16:51.973900896	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	664	Server Hello
176	09:16:54.416798148	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	TLSv1…	424	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
177	09:16:54.417047254		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
178	09:16:54.428734856	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	153	Change Cipher Spec, Encrypted Handshake Message
180	09:16:54.433615503	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAP	62	Response, Protected EAP (EAP-PEAP)
181	09:16:54.433850711		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
182	09:16:54.439684481	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	TLSv1…	131	Application Data
185	09:16:54.443663879		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
198	09:16:54.487220747	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAP	60	Success
200	09:16:54.489098697	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	173	Key (Message 1 of 4)
202	09:16:54.492582827	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	173	Key (Message 2 of 4)
203	09:16:54.492919155		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
204	09:16:54.496321258	TpLinkTechno_de:04:a3	SiliconLabor_a0:3f:74	EAPOL	255	Key (Message 3 of 4)
206	09:16:54.500115761	SiliconLabor_a0:3f:74	TpLinkTechno_de:04:a3	EAPOL	151	Key (Message 4 of 4)
207	09:16:54.500384902		SiliconLabor_a0:3f:74 (…	802.11	28	Acknowledgement, Flags=........
217	09:16:55.378171039	SiliconLabor_a0:3f:74	Broadcast	802.11	399	QoS Data, SN=16, FN=0, Flags=.p.....T

Figure 5.3. EAP-PEAP Wireshark Capture

5.4 EAP-FAST



No.	Time	Source	Destination	Protocol	Length	Info
4143	14:46:12.913307325	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	802.11	995	Probe Response, SN=3230, FN=0, Flags=....R...C, BI=100, SSID="MBSSID_Tx", SSID="MB…
4149	14:46:12.996282373		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4150	14:46:13.006150226		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4151	14:46:13.023608319	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	802.11	101	Authentication, SN=3233, FN=0, Flags=........C
4152	14:46:13.064703969		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4153	14:46:13.068651335	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	802.11	284	Association Response, SN=3234, FN=0, Flags=........C
4154	14:46:13.083809914	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	103	Request, Identity
4159	14:46:13.163271262		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4160	14:46:13.180040452	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	124	Request, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
4161	14:46:13.186050390	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	124	Request, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
4162	14:46:13.187135066	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	802.11	93	Action, SN=3237, FN=0, Flags=........C, Dialog Token=1
4166	14:46:13.207902883		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4168	14:46:13.222060169	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	TLSv1	242	Server Hello, Change Cipher Spec, Encrypted Handshake Message
4170	14:46:13.241364984	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	242	Request, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
4171	14:46:13.256039714	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	242	Request, Flexible Authentication via Secure Tunneling EAP (EAP-FAST)
4174	14:46:13.274086704		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4175	14:46:13.279722666	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	TLSv1	141	Application Data
4178	14:46:13.293070788		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4180	14:46:13.297955054	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	TLSv1	189	Application Data
4182	14:46:13.311231659		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4184	14:46:13.320897718	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	TLSv1	189	Application Data
4187	14:46:13.386961911		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4189	14:46:13.399616014	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	TLSv1	205	Application Data
4191	14:46:13.408247701		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4194	14:46:13.419704052	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAP	102	Success
4195	14:46:13.432331908	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAPOL	215	Key (Message 1 of 4)
4198	14:46:13.478852573		SiliconLabor_98:ab:50 (…	802.11	70	Acknowledgement, Flags=........C
4199	14:46:13.486255505	ASUSTekCOMPU_67:be:00	SiliconLabor_98:ab:50	EAPOL	249	Key (Message 3 of 4)

Figure 5.4. EAP-FAST Wireshark Capture

6. Recommendations

1. SiWN917 supports only .pem format certificates. Users need to convert their certificates of other formats (like .der) to .pem format and then load them into the module. One can use OpenSSL tool to convert .der format certificate into .pem using the following command:

```
openssl x509 -in <name of der format certificate> -out <name for pem format certificate>
Ex: openssl x509 -in cert.der -out cert.pem
```

2. Load the EAP certificates in order of private key, public key, and CA certificates individually with certificate type as 17,33 and 49 respectively. Maximum certificate length for each individual certificate is 4088 bytes or aggregate the certificates in to one file in a fixed order of private key, public key, intermediate CA/dummy certificate, and CA certificate and load the certificate with certificate type 1.
3. The maximum size for CA certificate is 12280 bytes. The maximum size for other certificate types like Client certificate and Private key etc., is 4088 bytes for each of them.
4. The total maximum size for a single certificate set of one CA certificate, one client certificate and one private key is 12280 bytes + 4088 bytes + 4088 bytes = 20456 bytes.
5. Supported TLS versions with WPA2 Enterprise Security are TLS v1.0 and TLS v1.2. And the corresponding settings for selecting TLS v1.0/v1.2 should be done at server end.
6. Whenever there is an EAP failure, user can check for the validity of the certificates loaded by decoding the certificates at cert logik.
7. During the handshake mechanism whenever the user observes the close notify alert, check whether the certificate loaded into the module has ended with proper " \n" which indicates the end of the certificate.
8. Make sure the certificate loaded has no space.
9. If the user wants to use a certificate size more than 2048 bytes, then the user needs to enable the following:

   `BIT(1) - SL_SI91X_EXT_FEAT_RSA_KEY_WITH_4096_SUPPORT`
   and
   `BIT(3) -SL_SI91X_EXT_FEAT_SSL_CERT_WITH_4096_KEY_SUPPORT` in extended custom feature bitmap.
   And, to enable parameters in extended custom feature bitmap, you need to first enable
   `BIT(31) - SL_SI91X_CUSTOM_FEAT_EXTENTION_VALID` in custom feature bitmap.

7. Revision History

Revision 1.0

April 2025

- Initial Release

Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

IoT Portfolio
www.silabs.com/IoT

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support & Community
www.silabs.com/community

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

www.silabs.com