BALI/EVIA series

WiFi 802.11ac + BT5.0 LGA Wireless Modules

Enterprise Security (EAP) App notes

Version 0.5

Table of Contents

Table of Figures

1. Scope of the Document

This document describes about Enterprise security and why it is used and how it works with detailed procedure.

2. Introduction

Wi-Fi Protected Access-Enterprise (WPA-Enterprise) is a wireless security mechanism designed for small to large enterprise wireless networks. It is an enhancement to the WPA security protocol with advanced authentication and encryption.

WPA2 Personal is what most home and small business users should use. It uses a single password. Most WiFi networks use this method.

WPA2 Enterprise is also called 802.1x and is the enterprise method. This method it requires a RADIUS authentication server and needs a username and password. It supports multiple accounts for each user.

A RADIUS Server is Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

The WEP is more secure than WPA2 because the Enterprise variants of WPA and WPA2, also known as 802.1x uses a RADIUS server for authentication purposes. Authentication is achieved using variants of the EAP protocol. This is more complex but more secure setup.

3. Connection setup

- EAP requires three components
  - STA_UT (Supplicant)
  - AP (Authenticator)
  - Free Radius Server (Authentication Server)

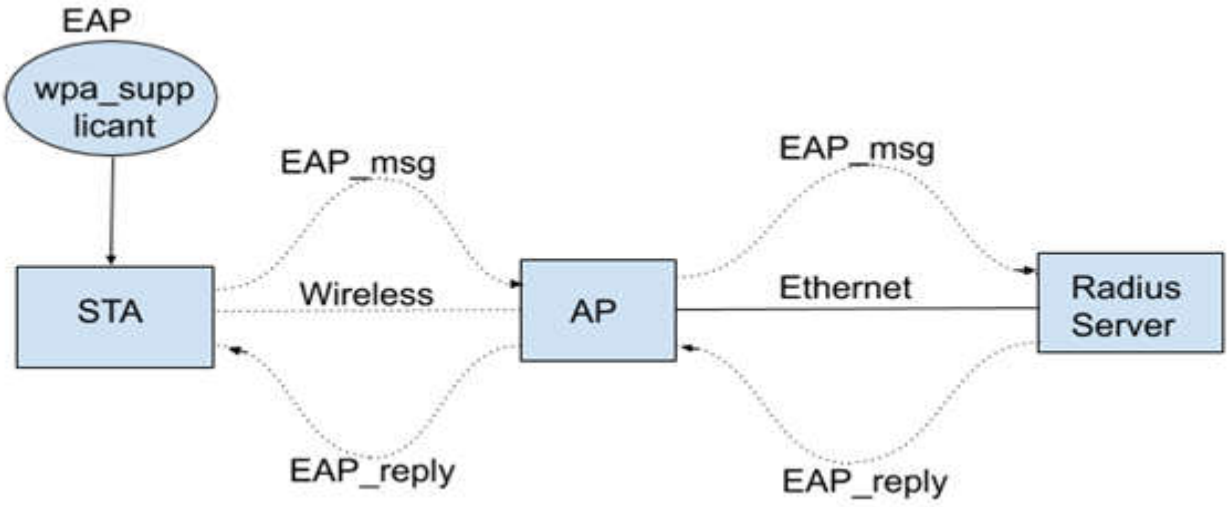

Figure 1: Connection setup for WEP

Here two PC's are used, one PC is used as a free radius server and another one is used as a supplicant (STA_UT). One PC (Radius server) is connected to AP by using Ethernet cable, in that PC need to install freer radius server. The free radius is control the all EAP messages and send the EAP reply messages here AP is just mediator. Another side STA_UT is connected to AP by using commands (wireless).

Here for EAP security purpose free radius is used at AP Side and wpa_supplicant is used at station side.

4. Procedure

4.1 Using TTLS

4.1.1 Radius Server Installation and Configuration

- Set up Access Point in enterprise mode and disable WPS.

  Note: In AP while enabling the Enterprise security, it is asking about Radius server IP address, here that IP address is nothing but the Linux PC/Laptop eth0 interface IP address

- Access Point should be connected to Internet
- Connect Linux PC or Laptop to AP by using Ethernet cable(which is named as Radius server PC)
- Download the free radius server in Radius server PC by using below command

  $ sudo apt-get install freeradius

- Verify certificates are generated or not. Certificates are available in below path

  $ cd /etc/freeradius/certs/

- Now edit ***clients.conf*** which is located in */etc/freeradius/* , and add AP information

client <AP ipaddr>/24{	#Here it is AP IP address not eth0 interface IP address
secret=<secret code of the AP>	#which is set by you in AP for EAP mode
}	

- Now edit ***/etc/freeradius/users*** with STA information like below

  <username> Cleartext-Password :=”<password>”

  Note: Here “username” and “password” are user preferable. Need to use the same username and password in wpa_supplicant.conf file (station side) later. Make sure username and password should be same in Station and Radius Server.

- Now select one of the EAP methods in ***/etc/freeradius/eap.conf*** file, in our case it is TTLS method.

  default_eap_type = ttls

- Now run the below command from PC(Radius server PC)

  $ sudo killall freeradius *(*run this command until output as “*no process found”)*

  $ sudo freeradius –X

- Now coming to Station side, insert the EVK, load the driver files if needed and *up* the interface.

- Now copy the *ca.pem* file from Radius server PC to WLAN station system path */etc/cert/* , (from command line) remember that path, because the path is needed to specify in *wpa_supplicant.conf* file.
- Edit */etc/wpa_supplicant.conf* file and configure SSID, Identity and Password.

```
#EAP-TTLS
network={
ssid="<AP-name>"
scan_ssid=1
key_mgmt=WPA-EAP
eap=TTLS
identity="<username>"        #Here the username is username in the users file in free radius PC
ca_cert="/etc/cert/ca.pem"    #this is the path of the "ca.pem" file, which is copied from Radius server PC
password="<password>"       #Here the password is password in the users file in free radius PC
}
```

Note: Make sure username and password should be same in Station and Radius Server, i.e., Need to use the same username and password in **users** file (Radius server side) and **wpa_supplicant.conf** file (station side).

- Initiate connection from STA to AP by using below command.

  $ sudo wpa_supplicant -D nl80211 -i wlanX -c /etc/wpa_supplicant.conf -B

- Get the IP address by using below command

  $ udhcpc –i <wlan_interface>

  (Or)

  $ dhclient <wlan_interface> -v

- Now it is connected successfully, for verification purposes ping the devices

  $ ping <ip_addr>