Funzionamento schedina

#Scopo

Lo scopo della board esp32 è quello di sniffare i vari pacchetti PROBE REQUEST generati dai dispositivi vicini ed inoltrarli al server il quale si occuperà di gestirli.

#Utilizzo

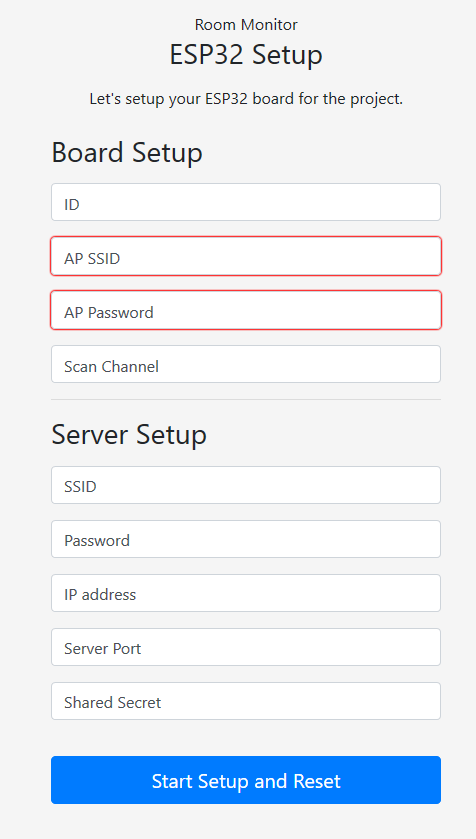
##Configurazione

In fase di montaggio del sistema, occorre un addetto per inizializzare i corretti valori necessari per il funzionamento.

Per garantire una facile configurazione è stato implementato un captive portal dove poter introdurre i valori necessari senza dover modificare il firmware.

Per collegarsi a tale portale occorre connettersi alla rete Wi-Fi della board che si vuole configurare (default SSID: 'esp32-ap', Password: 'progettopds'), dopo di che, tramite un browser (nota Chrome può avere problemi), collegarsi all'indirizzo https://192.168.1.1. (Nota, attenzione a non usare http ma https).

A questo punto verrà mostrata la pagina di configurazione della scheda dove poter inizializzare tutti i parametri necessari.



Come si vede è possibile cambiare le impostazioni della rete WiFi della scheda, assegnarle un ID (importante per configurazione server), e il canale su cui si vuole effettuare la scansione. Nella parte sottostante è possibile impostare tutti i parametri per la comunicazione con il server.

L’invio di questi parametri è reso sicuro tramite il protocollo https, garantendo confidenzialità, integrità ed autenticazione, invece per l’inoltro dei pacchetti sniffati verso il server sono garantite le proprietà di autenticazione e integrità tramite un hash sha256 sul singolo pacchetto inoltrato.

##Funzionamento

Una volta configurata, la board si collegherà alla rete wifi del server. È importante che tale rete abbia una connessione ad internet in quanto la scheda userà tale connessione per ricevere l’orario corretto tramite un server sntp.

Solo dopo aver acquisito l’orario, verrà avviata la procedura di sniffing e di inoltro.

Durante la fase di sniffing, verranno catturati tutti i vari PROBE REQUEST trasmessi sul canale indicato in fase di configurazione. Da tali pacchetti verranno estratte le informazioni necessarie e solo quando la fase di sniffing sarà terminata, tutti i dati acquisiti saranno inviati al server per poi riprendere con la prima fase.

Grazie all’utilizzo di un timer ogni minuto si provvede ad alternare la fase di sniffing e di inoltro. Per garantire il corretto sincronismo tra le varie schede e il server, lo stesso timer indica anche quando aggiornare l’orario eseguendo un’ulteriore richiesta al server sntp.

#Spiegazione tecnica

##Captive Portal

Per realizzare il meccanismo del captive portal è stato implementato un web server basato su https. Tale server risulta raggiungibile tramite l’indirizzo ip 192.168.1.1 sulla porta 80. Sono stati definiti un file html, uno css e uno javascript che permettono l’inserimento dei vari parametri di configurazione.

È stato necessario anche l’uso di un certificato e di un file contenente la chiave privata per https.

L’utilizzo di apposite partizione di memorie ha permesso di memorizzare i valori impostati e i vari file utilizzati per implementare il server, in particolare si è deciso di usare una partizione NVM, tipo chiave-valore, per memorizzare i vari valori di inizializzazione. Tale partizione è basata su memoria non volate permettendo il salvataggio dei parametri anche in assenza di tensione.

Per gestire le varie partizioni è stato usato un apposito file system chiamato SPIFFS (Serial Peripheral Interface Flash File System)**.**

##Sniffing

In tale fase la board intercetta i vari pacchetti dei vari dispositivi. Per far ciò si utilizza la modalità promiscua, attraverso la quale, è possibile ricevere ed elaborare pacchetti non destinati al proprio dispositivo.

##Inoltro