# Secure Interface between an Access Point and Wireless LAN Controller

**SILLA VAMSI[1], S. RAMYA[2]**

*[1]Student, Department of Electronics and Communication Engineering, R.V. College of Engineering, Bangalore, Karnataka, India*
*[2]Assistant Professor, Department of ECE, R.V College of Engineering, Bangalore, Karnataka, India*

---

**Abstract –** *In the present world scenario, due to advancement in the computational power of handheld devices and an exponential growth in devices which make more people work remotely and many services are accessed from homes which demands for higher bandwidth. To attain a greater number of wireless devices that can connect with an Access Point with minimum sustainable internet connectivity. As mentioned, the growth in devices indeed increase the requirement of an Access point which further connects to a wired network. An Access point is a device which has the capability of supporting wireless technology i.e. wi-fi. All the wireless devices which are in the vicinity of an Access Point can connect to it and can form a wireless local area network. Since there are a greater number of Access Points being deployed over entire world. There must be a provision to manage these Access Points which encourages for an intellectual device. This device is known as Wireless LAN Controller whose main purpose is to manage a vast number of Access Points. The interaction between these two devices i.e. of an Access Point and a Wireless LAN Controller with the help of a protocol is discussed throughout this paper.*

***Key Words***: **Access Point (A.P), Wireless LAN Controller (W.L.C), Control and Provisioning of Wireless Access Points (CAPWAP), UDP, Wi-Fi**

## 1. INTRODUCTION

A Wi-Fi Access Point is a hardware device which has the capability of connecting different wi-fi supported gadgets and electronic machines. Any device which has its wi-fi enabled will display different SSID by the nearby active Access Points. Through a secure authentication the user can connect to that respective SSID. Once the authentication is approved by the Access Point then that user can access to internet. So, from the networking point of view every different SSID can be analogous to a vlan with a prescribed vlan id. An Access Point can support more than one SSID. At the back end, an Access Point is connected to a wired network. Another networking device is introduced which is Wireless LAN Controller whose sole importance is to manage Access Points. Both devices can be in same subnet or in an entirely different network. Mainly there are two types of packets which are data and control packets. Data packets are those which are generated from a user device routed to the destination. Control packets are for maintenance of the network. The communication between these two devices are done with the help of a protocol known as CAPWAP protocol. This protocol is developed by IEEE for control and provisioning of Access Points (CAPWAP) as the name suggests. The latter section describes about the CAPWAP protocol.

## 2. Architecture

Imagine a network scenario where there is an Access point and a Wireless LAN Controller which are deployed in two different networks. Assume there are two different SSID which is been supported by the Access Point. Let us discuss two different types of architecture which are

- Distributed Architecture
- Centralized Architecture

### 2.1 Distributed Architecture

In this type of architecture, an Access Point is connected to an access switch at the back end which is a wired network. An Access Point has the hardware capability of converting a wireless SSID to a unique wired vlan on that port which is connected to an access switch. This port in the Access Point which is connected to an access switch is configured as a trunk port. So, these two SSID's of an Access Point get two different vlan id's which are carried on the same link which is known as trunk link to an access switch. This further connects to the distribution switch. Think if the network scales up which consists of large number of Access Points at the background connected to an access switch that further connects to a distribution switch. To cover a large region many Access Points keeps the same SSID. Because it helps a user if he roams over that region without again connecting to a fresh SSID. So, due to which many Access Points have the same vlan id across different access switches. This concept of vlan extends from an end to end i.e. from Access Point to the distribution switch. And indeed, increase the delay and computation of the packets at every access switch to route to the destination. And, similarly an Access Point should support one more vlan id for management of the device through a centralized management device. At the end, this type of network infrastructure with increase number of vlan's will be cumbersome as it must be configured on every access switch connected. This led to less efficient and a poor design consideration. The next type of architecture makes use of a protocol to avoid these drawbacks.

## 2.2 Centralized Architecture

In this type of centralized architecture, the functions are completely divided into two sets. One set which is at the end of Access Point such as RF Management, Encryption techniques etc. And other set comprises of Security Management, Client Authentication, Upgradation etc. These devices are lightweight Access Points and Wireless LAN Controller, respectively. CAPWAP protocol supports two different frames such as data and control frames. As discussed above an access point is still connected to an access switch and that is further connected to distribution switch. But in this architecture Wireless LAN Controller plays a vital role. This CAPWAP protocol supports the tunnelling feature where all the vlan id's of the access point is been encapsulated by this new ip packet and then routed over the campus network. This avoid dependence on layer 2 since there is no visibility of this between an Access Point and a Wireless LAN Controller. As it is encapsulated between a CAPWAP packet. The data packets are flown through CAPWAP data – UDP 5247 and similarly the control packets are sent through CAPWAP control – UDP 5246. If the network scales to many Access Points, then different tunnels are created by the connected Wireless LAN Controller to the respective Access Points. So, there will be same vlan existing on different tunnels. The traffic must flow from the Access Point to the Wireless LAN Controller even if the destination is in same packet, it traverses to the W.L.C. and again reverts to the same subnet to a different client. As the bandwidth is plentiful it will not be an issue. The scalability of a Wireless LAN Controller can manage up to 2000 Access Points. As shown in fig 1, the dotted lines represent CAPWAP tunnel which carry the data and control packets. The Wireless LAN Controller is a server and Access Point is a client where this type of interface is server-client socket paradigm.

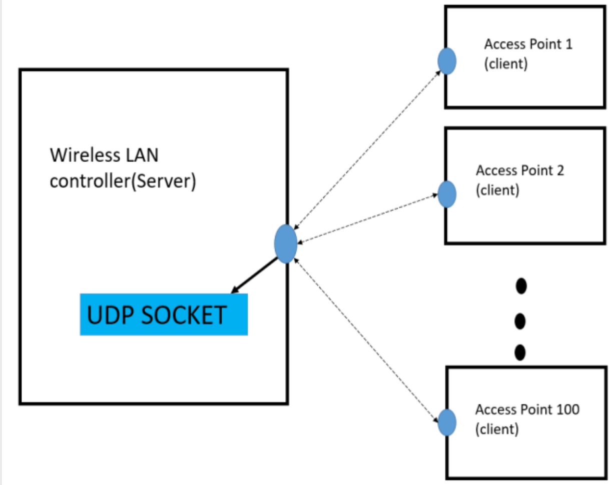

**Fig -1**: Tunneling Interface

## 3. CAPWAP Protocol

The emergence of wireless local area networks (LAN's) architecture has enhanced the usage of wireless termination points which are Access Points and wireless LAN controller. Here in this scenario simple wireless termination points are managed by wireless LAN controller with the help of CAPWAP protocol. Let us assume a network topology where multiple wireless termination points communicate to wireless LAN controller through internet (i.e. Internet protocol). Multiple radio interfaces on wireless termination points (access points) are controlled by access controller. [1]

## 4. Methodology

The initiation of CAPWAP protocol begins with discovery phase. An Initiation happens from the client side which are usually access points, when the radio interface comes up a discovery request occurs and send to active wireless LAN controller. In response to discovery request a discovery response is sent back to that access point. After configuration messages are exchanged where both devices agree on release information. Once the initial discovery packets are being exchanged client will start sending echo packets to the server which are then processed at the server end and then the server start sending back the packets which are response messages to the client. The 3 different programs which are evolved in the Wireless LAN Controller for different uses are:

- GUI program which deals with the interaction from the user and sending information to the background process otherwise known as daemons.
- The main code handles with the new requests from the clients in this case these are Access Points and also get the information from the GUI end, make changes in the database tables about different Access Points based on their state whether active or inactive.
- The third and the most critical part of the device software is a mariadb server where all the table based queries are been sent from the main code (server code) and executes those queries in this server and return the data if asked to the main code.

So as discussed above the GUI displays lots of web pages to the network administrator which helps him for configuring changes in the respective Access Points. So, when the administrator click on the view AP option in the GUI page, then the page retrieves the information from the database table showing all the Access Points which are in active state at the time of data fetch. Through which he/she can be able to see the interfaces which are up/down in the respective Access Points that he/she wants to see. So, the main web pages which are shown in the GUI are Radio, Media, SSID, Security etc. By clicking at the respective page, the needed parameters are shown in that page. Through which the administrator can change the settings and can send it on that respective Access Points. Let us site this topic with an example where the network administrator wants to change the SSID name, so by clicking at that SSID web page, he/she can change the SSID parameters. And then he can apply the changes made which can be send in a structure format that flows from the Controller to the Access Point through a socket. Once the command reaches at the client end based on the command it executes that particular set command and then changes are reflected back at the GUI end by sending an acknowledgement to the server code regarding the execution of command is successful or not. Based on this information the web page gives a notification to the administrator of successfully made the changes of the configuration made or not. The main functionality of a Wireless LAN Controller is:

- To maintain a database of how many Access Points are connected, what is the state whether up/down, etc., and other information such as Access Point ID, IP address of the Access Point connected.
- It also displays about the maintenance such as number of users connected to an Access Point, scan for the rogue Access Point and scan for environment.
- To keep up the backup and upgrade option such that if an Access Point boots up it pops up with an upgrade option.
- It helps in flexible client roaming where clients can roam between Access Points with fast switching of connecting with a new Access Point.

## 5. Conclusion

The interface between these 2 devices using UDP socket programming is thoroughly explained. The development built on both the ends in the model shows the complete architecture with configuration of messages (like set SSID, etc.) for setting various information on the access point. The proposed server-client based methodology can easily provide the communication interface and the if the device support Broadcom chips hardware can serve the purpose of executing wlctl commands. The interface is robust, cost effective and easy to use. The following conclusions are arrived at based on the experimental results:

This is a generic protocol where data and control frames are being exchanged. CAPWAP data messages encapsulate forwarded wireless frames. CAPWAP control messages are management messages which are used for administration purposes. Both these messages are being transferred in different UDP ports. At the coding end socket programming has been implemented for this interface to happen. Almost all the protocols which are in execution in the networking domain are software defined networks (SDN) which are easier to execute using sockets of Linux operating systems.

Although there are so many other ways of implementing this protocol which can be done using TCP protocol. But with the help of UDP protocol the complexity in the code reduces which is better to run for long time. Here for the communication to happen the access point and wireless LAN controller no need to be in same subnet. They can be in different networks which can then be tunneled through known public IP address with the help of CAPWAP protocol. Because of this mechanism in wireless technology, various factors like speed, roaming between access points, flexibility etc. are being achieved.

## REFERENCES

1. Kelly, S. and C. Clancy, "Control and Provisioning for Wireless Access Points (CAPWAP) Threat Analysis for IEEE 802.11 Deployments", IEEE journal of RFC 5418, 2009.