AN EXTENDABLE AND MODULAR APPLICATION FRAMEWORK FOR WLAN FEATURE VALIDATION

Major Project Report

Submitted in fulfillment of the requirements
for the degree of

Master of Technology
In
Electronics & Communication Engineering
(Embedded Systems)

By

Ashwini Bhat
(14MECE02)

Department of Electronics & Communication Engineering
Institute of Technology
Nirma University
Ahmedabad-382 481
May 2016

AN EXTENDABLE AND MODULAR APPLICATION FRAMEWORK FOR WLAN FEATURE VALIDATION

Major Project Report

Submitted in fulfillment of the requirements
for the degree of

Master of Technology
In
Electronics & Communication Engineering
(Embedded Systems)

By

Ashwini Bhat
(14MECE02)

Under the guidance of

External Project Guide:

Ms. Yashasvi MV
Broadcom Pvt. Ltd.
Mr. Saurav Singh
Broadcom Pvt. Ltd.

Internal Project Guide:

Dr. Nagendra Gajjar
Professor, EC Department,
EE Branch, Institute of Technology,
Nirma University, Ahmedabad.

Department of Electronics & Communication Engineering
Institute of Technology
Nirma University
Ahmedabad-382 481
May 2016

Declaration

This is to certify that

a. The thesis comprises my original work towards the degree of Master of Technology in Embedded Systems at Nirma University and has not been submitted elsewhere for a degree.

b. Due acknowledgment has been made in the text to all other material used.

- Ashwini Bhat
14MECE02

Disclaimer

"The content of this thesis does not represent the technology, opinions, beliefs or positions of Broadcom Pvt. Ltd., its employees, vendors, customers, or associates."

BROADCOM PVT LTD

Bengaluru, Karnataka

Certificate

This is to certify that the Major Project (Phase- I) entitled **"An Extendable And Modular Application Framework For WLAN Feature Validation"** submitted by **Ashwini Bhat (14MECE02)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Embedded Systems, Nirma University, Ahmedabad is the record of work carried out by her under our supervision and guidance. In our opinion, the submitted work has reached a level required for being accepted for examination.

Mr. Saurav Singh

Senior Engineer

Broadcom Pvt.LTD

Bangalore

Certificate

This is to certify that the Major Project entitled **"An Extendable And Modular Application Framework For WLAN Feature Validation"** submitted by **Ashwini Bhat (14MECE02)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Embedded Systems, Nirma University, Ahmedabad is the record of work carried out by her under our supervision and guidance. In our opinion, the submitted work has reached a level required for being accepted for examination.The results embodied in this major project, to the best of our knowledge,haven't been submitted to any other university or institution for award of any degree or diploma.

Date: Place: Ahmedabad

Guide

Dr. N. P. Gajjar
(Professor, EC)

Program Coordinator

Dr. D.K.Kothari
(Professor, EC)

HOD

Dr. P.N.Tekwani
(Director, IT, NU)

Director

Dr. P.N.Tekwani
(Director, IT, NU)

Acknowledgements

I would like to express my gratitude and sincere thanks to **Dr. P.N.Tekwani**, Head of Electrical Engineering Department, and **Dr. N.P.Gajjar**, PG Coordinator of M.Tech Embedded Systems program for allowing me to undertake this thesis work and for his guidelines during the review process.

I take this opportunity to express my profound gratitude and deep regards to **Dr. Nagendra Gajjar**, guide of my major project for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I would take this opportunity to express a deep sense of gratitude to my Project Managers **Mr. Jimut Sahoo**, **Ms. Yashasvi MV** and **Mr. Saurav Singh** for their cordial support and for providing valuable information regarding the project and guidance, which helped me in completing this task through various stages.I would also thank **Mr. Anand Swami**, **Mr. Ananth Mudumba**, **Mr. Avish Shah**, **Mr. Sandeep Kumar**, **Mr. Anil Kumar Hanagi**, and **Mr. Nithin N** for always giving good suggestions and solving my doubts to complete my project in better way.

Lastly, I thank almighty, my parents and friends for their constant encouragement without which this assignment would not be possible.

- Ashwini Shekhar Bhat

14MECE02

Abstract

IEEE 802.11 is a set of (MAC Layer) Media Access Control (MAC) and (PHY Later) Physical Layer (PHY) Specifications for implementation of (WLAN) wireless local area network communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. IEEE 802.11 Standard is similar to Ethernet on a superficial level. Many additional features were added to clear out the differences between wireless media used by 802.11 and wired networks. The implementation of these features for testing and development is redundant and long process requiring much effort. The reason behind developing an extensible and modular framework for the validation of these features was to reduce the human intervention and reduce the time required to bring up the WLAN drivers in specific modes. In this report, IEEE 802.11 standard and its components are described in brief. The flow of the working of the tool is described in this report.

Entire tool is implemented and developed in Python. This tool is mainly used for the validation of different WLAN features enabled. The tool allows easy extension to the module to be used for various different test cases which can be easily modified by the developer. It is used to bringup various kinds of test scenarios to be validated. Throughput tests are included by using the Iperf tool and logs of the throughput results are also taken. Configuration and bringing up of all components used at the test bed can be done by using this tool. Logging is included which extracts the required terminal and dmesg logs along with the Iperf throughput logs. By studying these logs the errors can be found out about where the firmware crashed. Error checks are include such as detecting whether device is active, each command executed on the terminal returns success, interface creation of each mode of the DUT are included. The tool exits when a crash occurs. Proper logs and dumps are taken and are pushed to proper location for further use.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

Most of the devices today are mobile. In order to support the mobility, it is required for the devices to be able to communicate using wireless interfaces. IEEE 802 is a family of standards that specify the protocols for networking for both wired devices as well as wireless devices. IEEE 802.11 is a standard that specifies the interface between the wireless stations and wireless clients to communicate over the air.

All the 802.11 specifications use the Ethernet protocols. Carrier Sense medium Access including Collision Avoidance (CSMA/CA) is used for sharing of the path or the medium for communication. For wireless communication there can be many modes in which the WLAN chip can be brought up for working for different applications. For example there can be a mode in which there is wireless communication between two clients through an Access point. Other mode can be two devices communicating with each other over a Direct Link. so here access point is not used. The configuration in the various modes requires a lot of redundant steps and also a lot of effort is required to load the correct binaries into the firmware. Using the application the bringing up of the chip can be done easily with minimum human intervention. Making it modular makes it easy to add different test cases and configurations used for different modes.

1.2 Problem Statement

Main objective of this project is to minimize the effort required for the developers to bring up the WiFi chip for different test scenarios. The language used to make automate the process of configuring the chip is Python. Using different modules of Python, it is possible to run shell commands, creating new threads for achieving parallel processing. It is also possible to give command line arguments, connect using secure as well as telnet sessions. also Squlite is integrated with python making it easier to create databases ad maintain the relevant data.

1.3 Overview

All 802.11 Wireless standards are ideal for widespread use in general system. There is no requirement for licensing to be able to operate within the frequency bands which are included within Industrial, Scientific and Medical (ISM) frequency band.

Commonly there many standards exist which are used. Some of these namely are 802.11-a, 802.11-b, and 802.11-g. The latest standard is 802.11-n which provides data rates of about 600 Mbps. [3].

Each of the distinctive norms has diverse elements and they were propelled at distinctive times. The initially acknowledged 802.11 WLAN standard was 802.11b. This utilized frequencies as a part of the 2.4 GHz Industrial Scientific and Medial (ISM) recurrence band, this offered crude, over the air information rates of 11 Mbps utilizing an adjustment plan known as Complementary Code Keying (CCK) and in addition supporting Direct-Sequence Spread Spectrum, or DSSS, from the first 802.11 particular. Very nearly in parallel with this a second standard was characterized. This was 802.11a which utilized an alternate regulation system, Orthogonal Frequency Division Multiplexing (OFDM) and utilized the 5 GHz ISM band [3]. Of the two gauges it was the 802.11b variation that got on. This was essentially in light of the fact that the chips for the lower 2.4 GHz band were less demanding and less expensive to make.

The 802.11b standard turned into the primary Wi-Fi standard. Hoping to build the rates, another standard, 802.11g was presented and endorsed in June 2003. Utilizing the more prevalent 2.4 GHz band and OFDM, it offered crude information rates of 54 Mbps, the same as 802.11b. Notwithstanding this, it offered in reverse similarity to 802.11b. Indeed, even before the standard was endorsed, numerous sellers were putting forth chipsets for the new standard, and today by far most of PC systems administration that is dispatched utilizes 802.11g[3].

1.4 Thesis Organization

The rest of the thesis organized as follows.

Chapter 2 gives details about the IEEE 802.11 standard and it Architecture is explained in detail. Also it includes the description of the various components of the standard.

Chapter 3 includes the description of the various services provided by the standard. Details of the services provided by the station as well as the distribution system is explained. An overview about the mobility types of the station is also included.

Chapter 4 deals with the detailed description of the MAC architecture of the 802.11 standard. Various coordination functions and the Inter Frame Spacing are also included therein.

Chapter 5 explains about the access procedure used by the DCF fr accessing the medium for wireless communication. Also the Backoff procedure for DCF is included.

Chapter 6 describes the modular framework in detail that is used to develop the tool. It includes the description of the modules of Python scripting language that are used in the tool. And overview of the flow of code is also included.

Chapter 2

Architecture of IEEE 802.11

2.1 Architecture Overview

The 802.11 standard defines the list of wireless procedures that are essential for successful transmission of the frames. The first member of the 802.11 family was developed in 1997. This was followed by the standard variations namely b,a g,n, and then latest one is ac.

Some particular changes to the features are implemented to different standards as per the requirement of the applications. 802.11a uses 5Ghz band while standards 802.11b and 802.11 g utilize 2.4Ghz bands. As a result of this problems arise for 802.11b and g standards as there was interference due to the waves emitted by microwaves, Bluetooth gadgets and cordless phones. These two standards then utilized OFDM and DSS multiplexing techniques to get over the limitations.[1]. For different countries there are variations in the radio frequencies used. For example, There is no licensing required for the 802.11 a and g standard in country US. the different standards and their specifications are listed in the Figure 2.1:

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

Figure 2.1: IEEE 802.11 Standards

2.2 Components

Few components are defined within the 802.11 standard to provide the proper support for the stations in order to for a wireless network. The basic block of the standard is known as BSS which stands for Basic Service Set. The Figure 2.2 shows arrangement of the different blocks of the 802.11 standard. BSSs are represented by oval structures and the range which they cover. The area which the basis service sets cover is known as BSA which stands for Basic Service Area. Once a STA moves out of the boundary of a particular BSS that is when it moves out of a particular BSA, if cannot communicate with the other STAs within that particular BSA.[6] Different components included in the 802.11 standard are enlisted below:

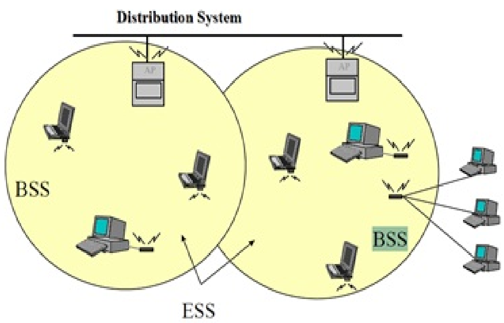


Figure 2.2: Basic Architecture IEEE 802.11

2.2.1 The independent BSS (IBSS)

IBSS is the Independent BSS. As the name indicates it consists of independent set of STAs. This means that AP has no role for communication between the two STAs. As shown in the Figure 2.3 , the network is comprised of two STAs only.IBSS is the basic and most fundamental component of the 802.11 Standard. This form of networking is also known as ad-hoc networking. This mode of networking can be used to form a network over the wireless medium. An example of utility of this form of network is sharing a large file from one to other laptop y using the ad hoc mode. This eliminates the requirement of installation of AP for wireless access and have cables for wired access.[9]

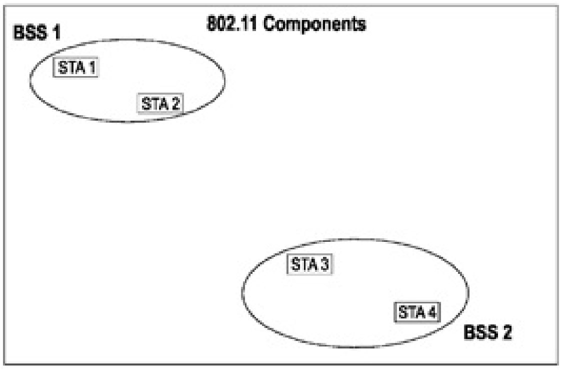


Figure 2.3: BSSs

2.2.2 Distribution system (DS)

Some distance between the STAs within a particular range is supported by the standard. So for greater distance than that particular range of distance between the two STAs, an increased coverage range is required. Multiple BSSs can coexist within the same physically spread area. Distribution System is the 802.11 component that is used to connect different BSS within a particular wireless range.

The DS supports the integration between multiple BSSs. It thus provides the logical services to enable the device support to handle the destination address mapping. AP is defined as an logical unit with which the STA associates . AP also provides access for the associated stations to the DS through a wireless medium. So the transition of the data is carried out between a BSS and Ds through an AP only. The Figure 2.4 shows the relationship between the AP and DS. It can be seen that two physically disjoint BSSs are interconnected by DS through an AP.

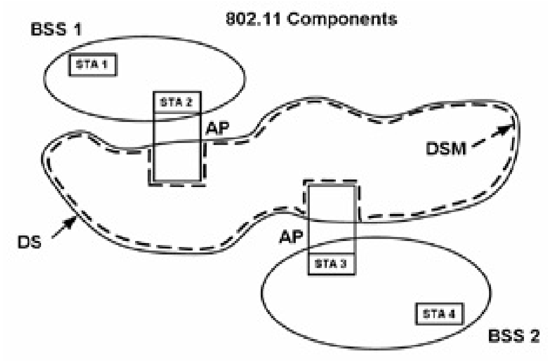


Figure 2.4: Dss and Aps

2.2.3 Extended service set (ESS)

A wireless network can be created of a particular complexity and size with the use of DS and BSS for 802.11. The collective network created by DS and BSS is referred to as ESS which stands for Extended Service Set network. In other words the combination of the BSSs that are connected by a single DS is known as ESS. But the distribution system is not included in ESS. Within an ESS, a STA may communicate to other STA within the same ESS. Also mobility of STA is supported within the ESS. The following cases are possible:

a. Partially overlapping of BSS : To provides continous coverage for the STAs

b. Physically disjoint BSS : There can be any distance between the BSSs

c. Physically collocated BSS : Used to provide redundancy

d. Single or multiple IBSS or ESS networks might be present physically in the same ESS or different ESS networks.

2.2.4 Integration with wired LANs

The direct integration of the 802.11 wireless standard with that of the wired LAN network is not present directly. So an additional architectural component is defined which is known as a portal. So a portal is the defined logical point of entrance at which wired 802.11 LANs enter the wireless DS. The portal is as shown in the Figure

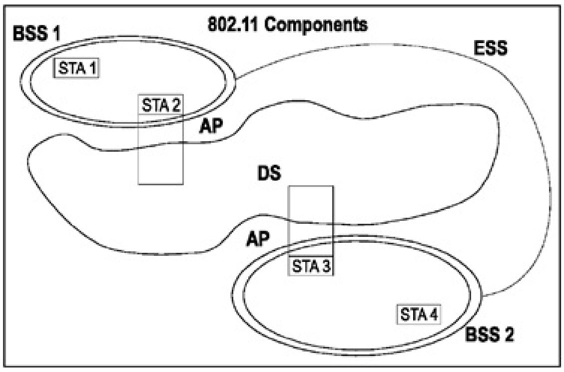


Figure 2.5: ESS

2.6. So for transmission of data to and from the wired network to the wireless ones, the data has to pass through the portal. When the frames pass between the LAN and the DS some frame formats or some addressing changes are required which are taken care of by the portal. This integration service is provided by the portal. Also a single device can function as a portal and the same device can have AP functionality.

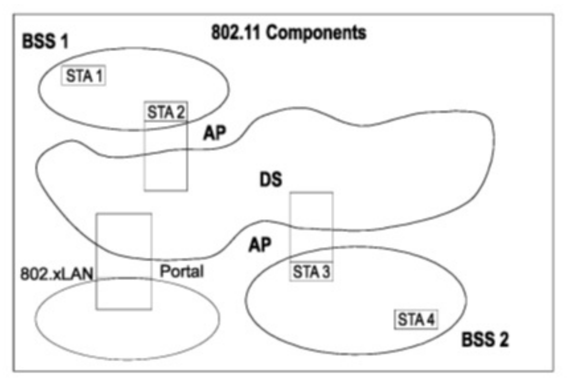


Figure 2.6: Connecting to other IEEE 802 LANs

2.3 Sevices

Different technologies can be used for the creation of a Distribution system. This may also include the wired LANS under the 802.11 standard. The distribution system thus created may or may not be distributes or centralized in nature. there is no constraint over the DS to network layered based or data link based. The implementation of DS is not specified by the standard in depth. Instead the standard specifies the list of services provided by the DS and the Stations. Both of the categories of services are utilized by MAC layer of the Standard

2.3.1 Station Service (SS)

There are number of services that are provided by the Station. Collectively they are know as SS which stands for Station Service. The services provided by the Stations are listed below:

a. Authentication : Used as a prerequisite for association when only authorized users are to be allowed to access the network.

b. De-authentication : Service used to terminate the existing authentication

c. Data confidentiality : Service used to protect the content of the messages being shared in the network.

d. DFS : Dynamic frequency Selection : Service used to uniform utilization of channels

e. TPC : Transmit Power Control : Used to adapt the transmission power to reduce the interference with the satellites

2.3.2 Distribution System Service (DSS)

There are number of services that are provided by the Distribution System. Collectively they are know as DSS which stands for Distribution System Service. The Access Point mentioned in the basic architecture is an entity that can be shared among one or more entities (STAs). These services have the capability to cross the network media and they can address to the locations within the logical boundaries. [1].

The services provided by the DSS are listed below:

a. Association : This service is used for association of the physical entity with the AP

b. Disassociation : This service is used for terminating the existing association

c. Distribution : This service is used when the frame is received by AP then it is used to deliver the frame to the assigned destination.

d. Integration : This service is used for communication with the Non IEEE 802.11 networks.

e. Re-association : When the device moves from one BSS to another, this service is initiated. Mainly used to initiate a more reliable association.

2.4 Mobility types

The types of STA mobility from one service set to another through out the network are defined below:[1]:

a. No-transition: within this type of transition two subtypes are defines which are explained below:

  - Static : This type indicated that STA was not in any kind of motion.
  - Local movement : This mobility type specifies that the movement of the STA in the same basic service area.

b. BSS-transition : This mobility type specifies that the STA has been in motion from one BSS to other but in same ESS.

c. ESS-transition : This mobility type specifies that the STA has been in motion from one BSS to other but in different ESS.

Chapter 3

Media Access Control

The modelling of the MAC architecture is as shown below. It contains various functions as DCF, PCF and HCF, each having different functionality. Some functions cannot be enabled for STAs under certain conditions. For example STA having quality of services enabled cannot include HCF function. But the PCF function will be available to all the STAs.

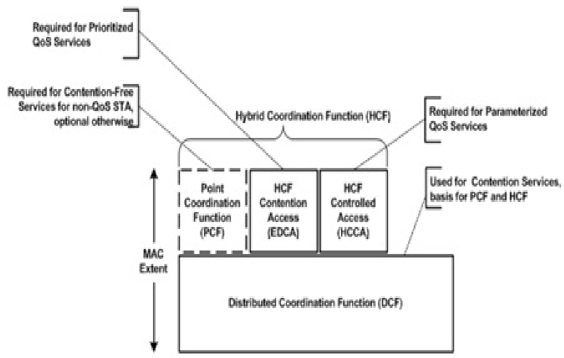


Figure 3.1: MAC Architecture

3.1 Coordination Functions

3.1.1 Distributed Coordination Function (DCF)

DCF is a protocol which enables mechanism for carries sensing. This is implemented through a four way handshake of the signals to yield maximum throughput. This also results in to lower number of collisions.When more than one packets are received at a particular node, it is defined as a collision. Due to this out of all the packets received, not even a single packet is received correctly. In most of the real time operations this becomes a very crucial issue. So DCF coordination function is used which implements sensing mechanism of the medium along with avoidance of such collisions.

The procedure of the operation of this function is as described further. Suppose there is a particular node having some packets to be transmitted. Initially the node waits for a random time period known as a backoff time period. Within this time period of the contention window, the node does not transmit any packet. Now if the node senses that the channel is being used by another node, it will pause the transmission of the packet till the other node finishes its transmission. In case if the timer indicating the backoff value for the node counts to null and still the medium is sensed to be busy then it waits till the channel is free. Now if the channel is sensed to be free it waits for a short amount of time and the transmits its frames. After transmission if the channel is sensed to be free it will request the destination for transmission of frames further. If the node receives a positive response from the destination for sending more frames then it will transmit more frames in the same way as described. DCF function includes multiple frames after transmission and reception of which the transmission of packets occur at a node. These frames include RTS(Request to send) frames, CTS (clear to send) frames along with a NAV frame which is network allocation factor. Details about NAV and the backoff timer are explained in Chapter 4.[7]

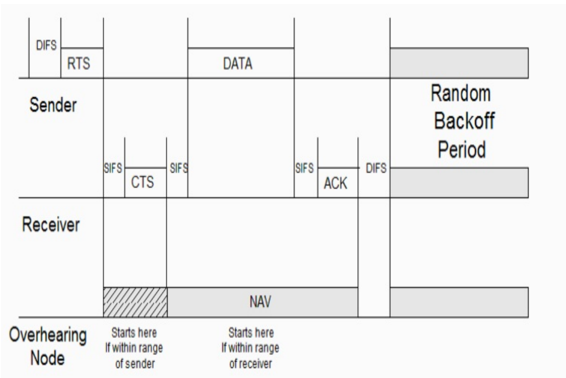


Figure 3.2: DCF

3.1.2 Point Coordination Function (PCF)

PCF or Point Coordination function is an 802.11 procedure. This function implements polling mechanism for the detection of the channel available for transmission. The polling mechanisms included may be either priority based mechanism or simple round robin mechanism. The working of the PCF function for sensing the channel is as shown in Figure 3.3.

The access point first senses whether the medium is idle or not for a time period equivalent to PIFS. It then sends a beacon frame at the beginning of the period to all the associated stations. PIFS time period is more than that of SIFS but it is smaller than DIFS time period. The beacon frame that is sent by The AP contains the information regarding the interval for the beacon, identifier details for the appropriate BSS and the duration of the frame.

Now the each station is polled by the AP by sending the frames for polling which are namely CF-poll frame or the DATA+CF-poll frame. If the frames sent by the AP for data and CF are received by the destination station then it replies to the AP by sending a set of frames which can be either CF-ACK frame or DATA+CF-ACK for acknowledgement. If the station only receives the frames for CF then it responds by sending a null frame to the AP.

An priority mechanism is implemented by PF for sensing the channel virtually. PCF function is available by default for all the STAs. In order to gain priority over other frames for accessing the channel, the inter-frame spaces for the Station is reduced while using PCF. Thus the STA using DCF for the channel access have less priority than the STAs utilizing PCF.[8]

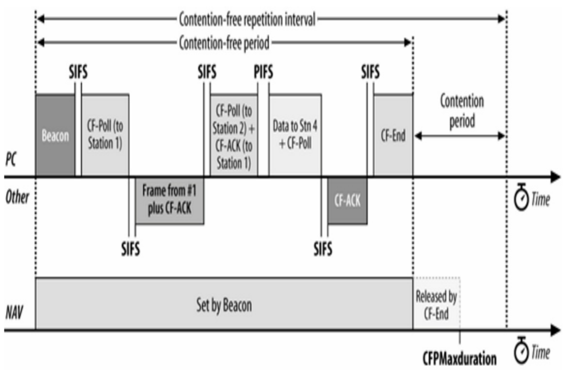


Figure 3.3: PCF

3.1.3 Hybrid coordination function (HCF)

There is one more additional function which is known as HCF which stands for Hybrid Coordination Function. This function can only be use in case of configurations involving Qos. This function is a combination of both of the above mentioned functions namely PCF and DCF. Some enhancements are also made to these coordination functions with specific procedures and frames related to Qos to enable smooth transmission of frames containing QoS data. HCF uses two kinds of channel access methods namely HCF controlled channel access which is used for contention free transmission and second one is enhanced distributed channel access (EDCA) which is a contention based mechanism. Both the procedures are as described below.[6]

3.1.4 HCF contention-based channel access (EDCA)

This function is used to prioritize the frames. The traffic can be sent according to its respective priority. Higher priority traffic will be sent at higher probability as compared to the lower priority traffic. This is implemented by the STA by waiting for less time period for the greater priority traffic as compared to the less priority traffic. The protocol used here is a variation of CSMA/CA protocol that is normally used. This protocol is know as TCMA. This protocol uses shorter inter-frame space namely related to arbitration for the packets having higher priority. A period named as TXOP which stands for Transmit Opportunity, is the time period for which contention-free access is provided to the channel by this protocol. During this interval, the station is free to send any number of frames possible before the time period gets ended. In case of frames that are very large and cannot be transmitted over a single duration of TXOP, these frames are further divided into shorted segments and then they are transmitted. In case the TXOP is equal to zero, it means that the time period is limited to a particular MMPDU which is the protocol data unit for MAC. EDCA provides a range of levels for prioritizing the stations. These are know as Access Categories.A list of such access categories are listed below in Figure 3.4.[6]

-	802.1D			802.11e	
Priority	Priority Code Point (PCP)	Acronym	Traffic Type	Access Category (AC)	Designation
Lowest	1	BK	Background	AC_BK	Background
	2	--	Spare	AC_BK	Background
	0	BE	Best Effort	AC_BE	Best Effort
	3	EE	Excellent Effort	AC_BE	Best Effort
	4	CL	Controlled Load	AC_VI	Video
	5	VI	Video	AC_VI	Video
	6	VO	Voice	AC_VO	Voice
Highest	7	NC	Network Control	AC_VO	Voice

Figure 3.4: Access Categories

3.1.5 HCF controlled channel access (HCCA)

This coordination function has many similarities as the point coordination function (PCF). But there are some differences between the two functions. This function does not have the division of time period into CP and CPF which lies between any two beacons. Instead it allows at any point of time during the CP, CPF to be initialized. The CPF that is initiated between the CP is known as CAP which stands for Controlled Access Phase. This phase is used in contention free period when a frame is to be sent or received to or from a station. In CAP, the access point has the control to the medium. Also in this function traffic class and streams are defined. So the channel can provide a service according to each session instead of providing queues for each station. The information about the queue length of each station is provided to the traffic class. In this function each of the stations are allotted the transmission window which is the Transmit Opportunity individually. This enables the stations to send multiple packets for a particular allotted time period by the function. HCCA can also be used for high accuracy configuration of the quality of service. This function is the most complex among all the available functions. This is used in applications involving voice over Internet protocol for a smooth working over WiFi.[6]

3.2 Inter Frame Spacing

IFS is the specific time period which exists between two frames. During this time period STA shall check whether the medium is busy or idle by using the appropriate Carrier sensing mechanisms that are defined therein. Figure 3.5 shows the different kinds of inter-frame spaces and their interrelationships.[6] The different kinds of IFS are listed below

a. AIFS Arbitration Interframe Space : Used for prioritizing Access Categories

b. DIFS DCF Interframe Space : This is minimum time period used for services that are contention based.

c. EIFS Extended Interframe Space : This is not a fixed kind of IFS. It comes into picture only when frame transmission is error-ed.

d. SIFS Short Interframe Space : This kind of IFS is used for transmissions of frames having highest priority.

e. PIFS PCF Interframe Space : This is minimum time period used for services that are contention free.

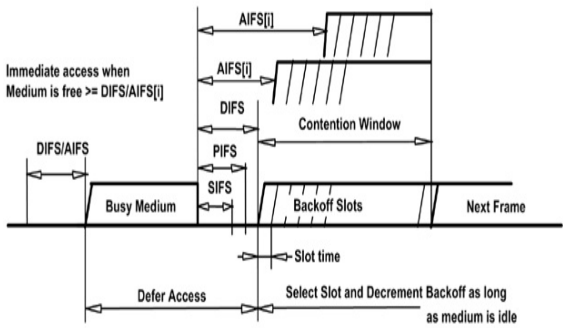


Figure 3.5: Inter Frame Spacing

Chapter 4

DCF Access Procedure

The main access procedure for sensing the channel for DCF is CSMA/CA. The method to sense the channel varies with the coordination function used.

4.1 Basic Access

The basic access procedure defines the method by which a station can associate and whether or not it can transmit the frames.
A pending frame containing the payload may be transmitted by a STA when DCF function is used for accessing the medium. This may e the case in which the Point Coordination function may or may not be included. If the medium is detected as idle by the STA for a time period greater than of equal to the DIFS or EIFS periods, an event is caused which indicated the medium is busy. This is done by detecting a particular frame with the appropriate address and frame check sequence value at the STA that is not received. So some of the procedures initiating the backoff for the transmission of the frames is initiated. The procedures are described in the following sections.
It is mandatory that when a ST transmits a frame, it should receive its appropriate acknowledgment frame. This depicts that the entire frame is successfully transmitted along with the payload contained in it. Also there are certain counters which enable the retrying the transmission for a fixed amount of times. The Figure 4.1 shows the time frames for the basic access procedure.

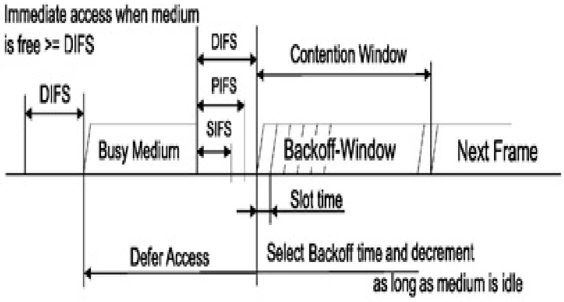
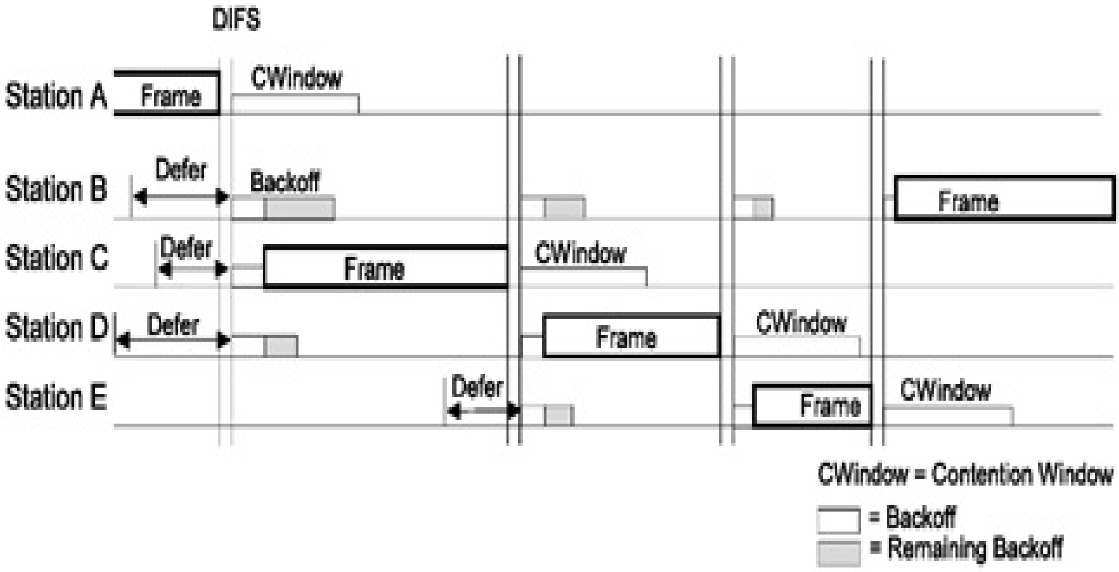


Figure 4.1: Basic Access Method

4.2 Backoff procedure for DCF

This section describes the procedure that is used for backoff when the distributive coordination function is used. this process is operational for a station if the medium is found to be busy by either of the medium sensing mechanisms. this procedure is usually invoked for a sta when it it trying to transfer a frame but the medium is busy. First of all, the station (also known as STA) will pic a random value according to the equation used and set it as its timer value for Backoff period. During the period equivalent to DIFS period or the time period equivalent to EIFS which is follows next, the medium is assumed to be idle and ready for carrying out transmissions. Now any of the carrier sensing mechanisms are used to determine the availability of the medium by the STA. If it is found that no active transmissions are taking place over the medium then the timer indicating the backoff period is reduced by a certain minimum amount.

Now in case the medium is detected to be having transmission active (i.e. if it is busy), then the procedure for backoff is now delayed. This means that the times will not be decremented for that particular transmission period. Now before the backoff procedure is resumed, the medium is assumed to be idle for DIFS or EIFS time period whichever is applicable. Once the backoff timer is zero, the transmission will be continued. At the end of each of the transmission frames, the procedure for backoff is followed. This is done eve if there are additional transmissions that are queued. This procedure is also performed when an acknowledgment frame is received. In case of acknowledgment frames not received the backoff will be done at the end of the timeout for acknowledgment. This happens when a STA is unable to receive ACK frame within the specified time period. Backoff procedures are included so that all the frames transmitted by STA are differentiated. This increases the rate of successful transmission and avoids probability of collisions.



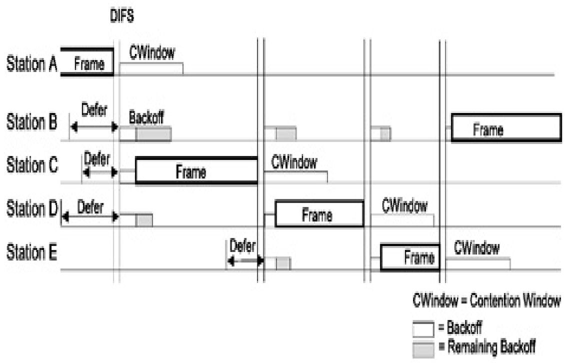


Figure 4.2: BackOff Procedure

4.3 Setting and resetting the NAV

A frame that is valid will be received by STA. Then the STA will update NAV information corresponding to it in Duration fields where the current value of NAV is less than the new value of NAV. When a PS-Poll frame is receiver NAV setting will be updated by the STA. The duration will be equal to (microseconds unit) time required Short Interframe gap and one acknowledge frame. For this to occur it is mandatory that current value of NAV is less than the new one. In case of fractions of microseconds, the rounding up of the value will be done to the next integer higher than the current one. Some other conditions may also cause variation in the value of NAV. Figure 4.3 shows how the STA will receive the frames consisting information about NAV. Due to lower value for NAV, for some STAs , only CTS frames may be received.

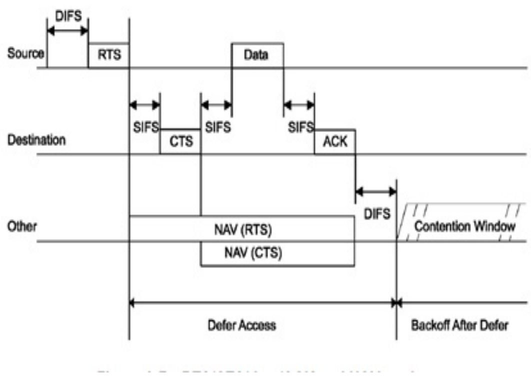


Figure 4.3: NAV Setting

Chapter 5

Feature Validation Tool

5.1 Overview

The feature validation tool is used to bring up the WLAN chips in different modes as and when required by the developer for testing. There can be different test scenarios which have to be reproduced by the developer in order to verify the issues. Doing this manually can be tiresome and may be error-ed. This consumes a lot of time which is not desired. By using the tool, the developer has to edit the configuration file or just give proper command line arguments in order to get his job done. There are many error checks included to catch the error and exit the execution of the code after taking the proper logs. This enabled the developer to narrow down the area where the problem can be there. Also logs are moved to a text file which can be viewed later or sent easily without any hassle.

The entire tool is written in python, which is easy to read and understand. The tool has no dependency over the user or the particular location of his work. This tool is also provides the flexibility of providing inputs in three different manners. Either the user can use command line arguments, or configuration file can be edited or the data can be passed as parameters directly to the APIs created. The APIs are simple to use. The user can just import the tool and used them to create the user defined script performing only the processes that are needed by the user. The logs are arranged in particular folders depending on what kind of test is run, date and time on which it was run. This makes the management of the logs very easy. Database is also created about the status of the issues, which can be queried according to the date and range of dates on which the particular records are to be viewed.

5.2 Python Modules

Python language is a very popular and can be learnt very easily. It makes modular programming very simple and easy to understand. Many powerful and modular applications used for advance purposes are written in this language. Moreover it is freely available across different platforms. For Windows python package include IDLE which provides a GUI for implementing python programs. Basically it is an interpreter which can be used fo different applications. Python has modules which support various features such as SQlite for enabling database features, Multithreading for parallel programming and many more. More over it has support for C and C++languages which makes it easy for integration with other scripts.

In the script modules used are listed below [2]:

a. OS : The Operating System module is used to run shell commands by using python. Also it can perform shell operations like changing directory or writing the logs to a file.

b. Threading : This module helps to create threads that can operate in parallel for getting simultaneous execution.

c. Paramiko : This python module is used to make connections to the client device and also run the commands on the device. It can be used to implement SSH protocol using python

d. Queue : This module is used to store the values in a queue either in LIFO or FIFO fashion. this module can also be used to pass the values between different modules. This helps in sharing some data while retaining the accessibility limitations between the modules.

e. Telnetlib : This module is used to implement telnet protocol using Python scripting

f. Time : This module is used to do all the timing related operations. This includes returning current time and in a particular format.

g. ArgParse : This python module is used to parse the command line arguments provided by the user. It includes long and short options along with the help message and default values to be defined.

h. Pexpect : This module is used for automating the logging in process. The expected output after executing a command is mentioned and the relative inputs to be given can be specified.

i. Subprocess : This is an extension of the OS module. But it contains some additional features like spawning a new process which is not included in OS module.

j. Multiprocessing : This module is used to create parallel processes to be executed simultaneously. It is a super set of the threading module but it supports killing of the process which is not included in threading module.

k. Virtualenv : This module is used to create a virtual environment for locally making changes in the python support files and installing additional packages locally without making changes at the Python package installed at the server.

l. Squlite3 : Python has direct support for squlite. This helps to create databases using python scripts. Also a query script can be made by the use of this package.

5.3 Code Flow

The following figures (Figure 5.1 and 5.2) shows how exactly the code works.

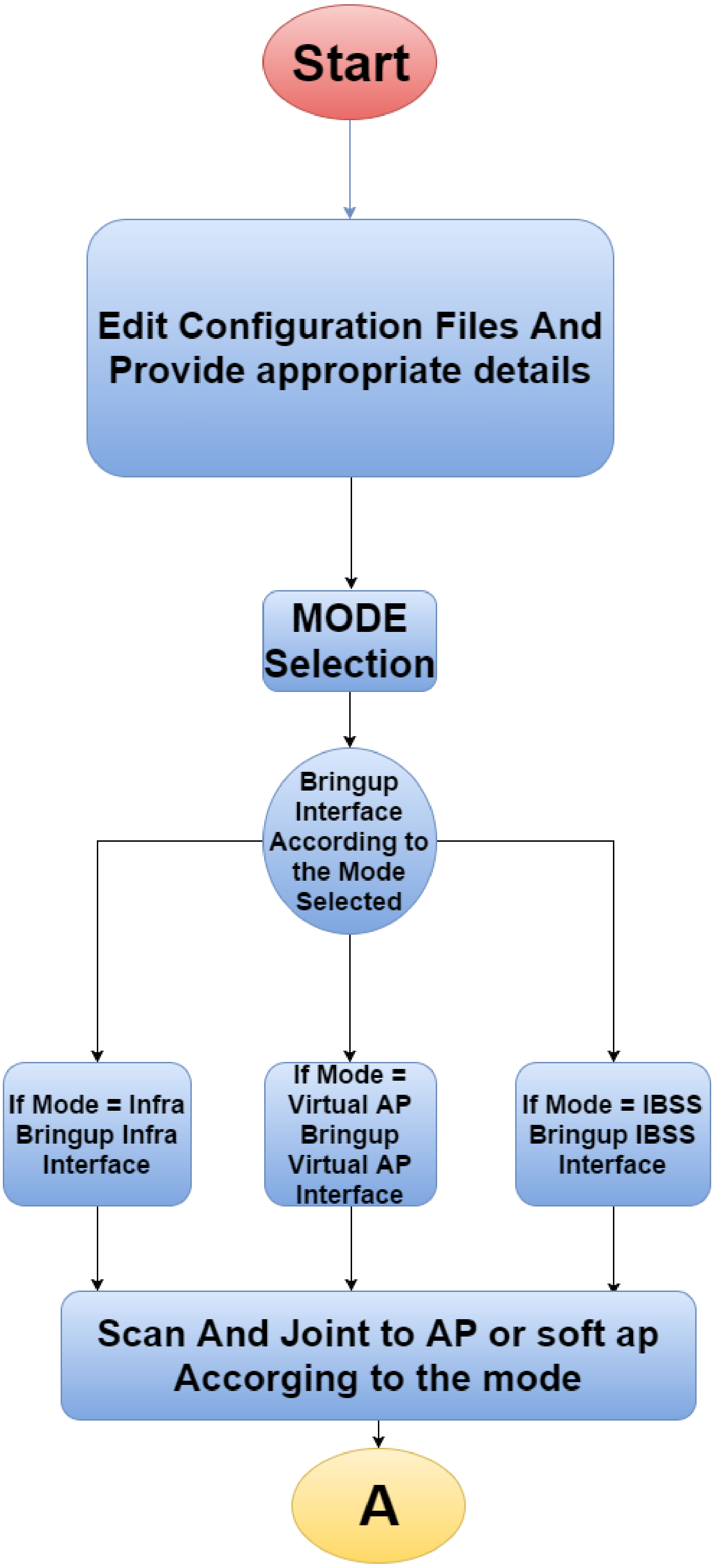


Figure 5.1: Code Flow

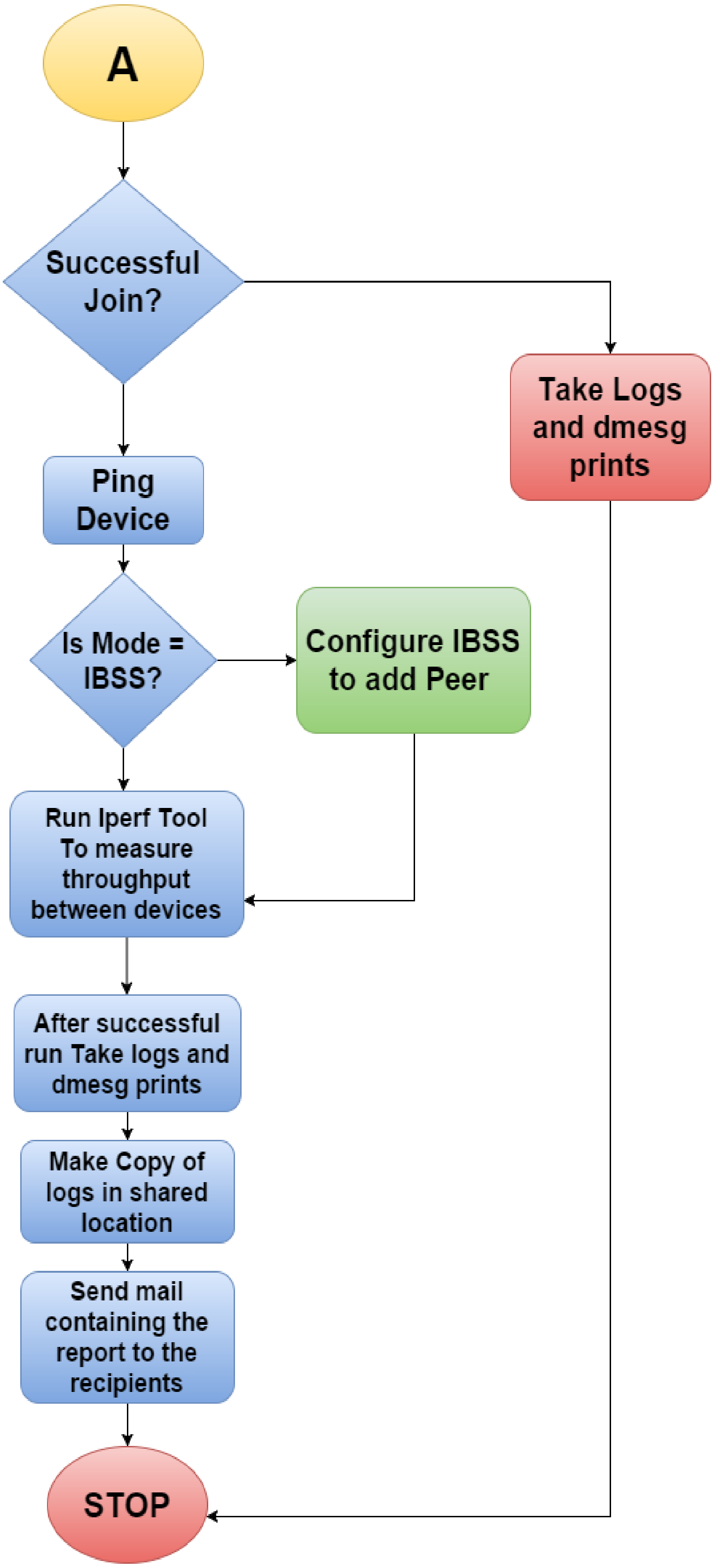


Figure 5.2: Code Flow

5.4 Summary

The functioning of entire tool can be summarized as follows:

First the developer will enter the details of the test scenario like

a. the kind of chip that is to be tested
b. the files to be loaded
c. details of the device machine
d. IP addresses to be configured on each interfaces
e. IP Addresses of APs
f. MAC (Hardware) address to each interface
g. username and password for logging in
h. web switch IPs
i. Security mode in which testing is to be done
j. IP Address on which IPERF tool is to be run fr carrying out throughput testing

The next step is to develop the script. The developer can either use the existing script or can make his own script by using the APIs that are already created in the tool.

Now when the script is initiated, first all the interfaces of the DUT (Device Under Test) will be brought up. these interfaces include Infra interface, Virtual AP interface, or the IBSS interface. Initially all the interfaces would be inactive. Depending on the mode of the test to be carried out, the interfaces would be brought up. The user has to specify about the interface to be brought up. this means is the mode is INFRA, the corresponding interface would be enabled. Similarly for IBSS and Virtual AP modes the respective interfaces would be brought up.

Now, once the interfaces are up, the IPERF tool is used to run the throughput testing between the two devices. he output of this command is directed to a separate log file having Iperf logs in the respective folder that is sorted according to the date and time at which the test was fired. Also the dmesg logs will be directed to a text file to have a back up of the logs and commands getting executed. Due to modular APIs, the addition and modification of the test cases can be done very easily without any effort.

Also if in the middle of execution the test fails, the script exits taking the dmesg logs so that the developer can debug the error and find out the reason for crash.

References

[1] Matthew S Gast,
802.11 Wireless Networks, The Definitive Guide
OReilly Publications, Third edition

[2] Python Documentation,
https://www.python.org/

[3] IEEE 802.11 Wi-Fi Standards,
http://www.radio-electronics.com/info/wireless/wi-fi
/ieee-802-11-standards-tutorial.php
Last Updated: November 2015

[4] Chapter 17 Wireless Lans,
https://www.rivier.edu/ Last Updated: July 2015

[5] Iperf Tutorial,
http://openmaniak.com/iperf.php Last Updated: August 2015

[6] IEEE 802.11 Basics,
http://www.ie.itcr.ac.cr/asistenteweb/pmwiki/pmwiki.php
/AcercaDe/AcercaDe Last Updated November 2015

[7] 802.11 DCF,
http://www.vocal.com/networking/802-11-distributed-coordi
nation-function-dcf/ Last Updated December 2015

[8] 802.11 PCF,
https://software.intel.com/en-us/articles/mac-80211-point-
coordinator-function Last Updated December 2015

[9] 802.11 IBSS,
http://www.wi-fiplanet.com/tutorials/article.php/1451421/Un
derstanding-Ad-Hoc-Mode.htm Last Updated December 2015