./

SHADOW PROJECT REPORT



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PS Number** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be Approved** | **Remarks/Revision Details** |
| 99002503 | 17/12/2020 | Praveen Kumar Chaubey | - | CS Raghavendra |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Details**

Contents

[Contents 3](#_Toc59555335)

[Module/s 5](#_Toc59555336)

[Topic and Subtopics 5](#_Toc59555337)

[1. Testing: 5](#_Toc59555338)

[2. IEEE 803 Protocol Basics. 5](#_Toc59555339)

[3. Common Wi-Fi Standards 5](#_Toc59555340)

[3. Open System Interface (OSI) Basics 6](#_Toc59555341)

[4. Physical Layer Frame Structure and its types 9](#_Toc59555342)

[5. Data Link Layer 9](#_Toc59555343)

[6. Wi-Fi Standard Evolution 13](#_Toc59555344)

[7. OFDMA, DSSS, FHSS 13](#_Toc59555345)

[8. 802.11 MIMO 16](#_Toc59555346)

[9. Channel Bonding 17](#_Toc59555347)

[10. Active and Passive Scanning 18](#_Toc59555348)

[11. MAC Layer Specification (AMPDU & AMSDU) 20](#_Toc59555349)

[12. Wi-Fi Security (WEP, WPA, WPA2, WPA3) 20](#_Toc59555350)

[13. CSMA/CD & CSMA/CA 22](#_Toc59555351)

[14. Hidden Terminal and Exposed Terminal Problem with MACA Solution. 24](#_Toc59555352)

[15. Important Protocols 25](#_Toc59555353)

[Objectives 31](#_Toc59555354)

[Requirements: 32](#_Toc59555355)

[High Level Requirements: 32](#_Toc59555356)

[Low Level Requirements: 32](#_Toc59555357)

[Design 32](#_Toc59555358)

[Test Plan 33](#_Toc59555359)

[High Level Test Plan (Integration Test Plan) 33](#_Toc59555360)

[Low Level Test Plan (Unit Test Plan) 33](#_Toc59555361)

[Implementation Summary 38](#_Toc59555362)

[Summary 38](#_Toc59555363)

[Scanning Testing 39](#_Toc59555364)

[Authentication, Association and Encryption Testing 42](#_Toc59555365)

[Client Connectivity Testing 49](#_Toc59555366)

[Layer 3 Connectivity: IP addressing(DHCP) 49](#_Toc59555367)

[Signal Testing 55](#_Toc59555368)

[Security Testing 56](#_Toc59555369)

[1.1 WEP (Wired Equivalent Privacy) 57](#_Toc59555370)

[1.2 WPA (Wi-Fi Protected Access) 57](#_Toc59555371)

[1.3 WPA2 (Wi-Fi Protected Access 2) 57](#_Toc59555372)

[Video Summary 58](#_Toc59555373)

[Git Link 58](#_Toc59555374)

[Git Dashboard 58](#_Toc59555375)

[Git inspector summary 58](#_Toc59555376)

[Build 58](#_Toc59555377)

[Code quality and Issues or Bug Tracking 58](#_Toc59555378)

[Individual Contribution & Highlights 58](#_Toc59555379)

[Challenges faced and how were they overcome 58](#_Toc59555380)

[Future Scope 59](#_Toc59555381)

[References 59](#_Toc59555382)

**Table of Figures**

[Figure 1: Ethernet Frame Format 5](#_Toc59555414)

[Figure 2: Wi-Fi Standards 6](#_Toc59555415)

[Figure 3: OSI Model Stack 7](#_Toc59555416)

[Figure 5: LLC PDU Format 10](#_Toc59555417)

[Figure 5: Data Link Layer 11](#_Toc59555418)

[Figure 4: Physical Layer Frame Structure 12](#_Toc59555419)

[Figure 6: OFDMA 14](#_Toc59555420)

[Figure 7: DSSS 15](#_Toc59555421)

[Figure 8: FHSS 16](#_Toc59555422)

[Figure 9: 2.4 GHz Band Frequency Allocation 18](#_Toc59555423)

[Figure 10: 5 GHz band Frequency Allocation 18](#_Toc59555424)

[Figure 11: CSMA/CD 23](#_Toc59555425)

[Figure 12: CSMA/CA 23](#_Toc59555426)

[Figure 13: Hidden Terminal Problem 24](#_Toc59555427)

[Figure 14: Exposed Terminal Problem 25](#_Toc59555428)

[Figure 15: CTS & RTS Frame 25](#_Toc59555429)

[Figure 16: EAPOL Handshake 26](#_Toc59555430)

[Figure 17: ICMP Echo 27](#_Toc59555431)

[Figure 18: ICMP Protocol 27](#_Toc59555432)

[Figure 19: DHCP Protocol 28](#_Toc59555433)

[Figure 20: ARP Protocol 28](#_Toc59555434)

[Figure 21: TCP 29](#_Toc59555435)

[Figure 22: UDP 30](#_Toc59555436)

[Figure 23: DNS 30](#_Toc59555437)

[Figure 24: HTTP 31](#_Toc59555438)

[Figure 26: Active Scanning Probe Request 40](#_Toc59555439)

[Figure 27: Active Scanning Probe Response 40](#_Toc59555440)

[Figure 28: Passive Scanning 41](#_Toc59555441)

[Figure 29: Authentication Request 42](#_Toc59555442)

[Figure 30: Authentication Response 43](#_Toc59555443)

# Module/s

1. Wireshark is majorly used for packet sniffing and packet analysis.

2. Cisco Packet Tracer is used for simulation.

3. V-Model is followed.

# Topic and Subtopics

## 1. Testing:

a. User Registration and Login Testing

b. Signal Testing

c. Security Testing

d. Client Connectivity Test

e. Authentication Test

f. Scanning Testing

## 2. IEEE 803 Protocol Basics.

It is most widely used Wired LAN technology. It operates in Data Link layer and physical layer. It’s presence in family of networking technology defined in 802.2 and 802.3 protocol standards. It has Ethernet Frame Format. Here preamble and SFD are used in synchronization, CRC for check error detection. Data and padding contains info from upper network layer. Its max length = 1518 bytes and min Length = 64 bytes.

MAC address is used as Ethernet address and its6 bytes. In first byte if 0th bit is 0, then its unicast else multicast, if all the bits of all bytes are 1 then its broadcast.

Link: <https://www.youtube.com/watch?v=MzhiVE6OuQA&t=231s>

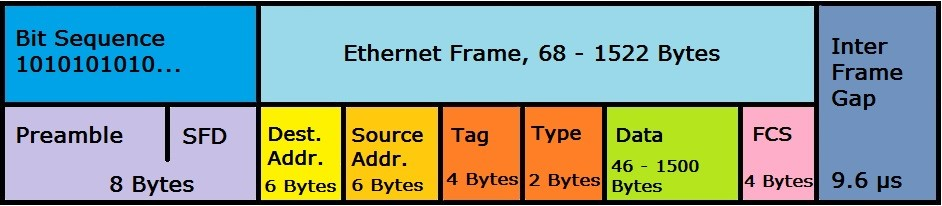


Figure 1: Ethernet Frame Format

## 3. Common Wi-Fi Standards

#### IEEE 802.11

This was the original and was created in 1997. Devices using this haven't been made for over a decade and won't work with today's equipment.

#### IEEE 802.11a

Created in 1999, this version of Wi-Fi works on the 5GHz band. This was done with the hope of encountering less interference since many devices (like most wireless phones) also use the 2.4GHz band. 802.11a is fairly quick too, with maximum data rates topping out at 54Mbps. However, the 5GHz frequency has more difficulty with objects that are in the signal's path, so the range is often poor.

#### IEEE 802.11b

Created in 1999, this standard uses the more typical 2.4GHz band and can achieve a maximum speed of 11Mbps. 802.11b was the standard that kick-started Wi-Fi's popularity.

#### IEEE 802.11g

Designed in 2003, the 802.11g standard upped the maximum data rate to 54Mbps while retaining usage of the reliable 2.4GHz band. This resulted in widespread adoption of the standard.

#### IEEE 802.11n

Introduced in 2009, this version had slow initial adoption. 802.11n operates on both 2.4GHz and 5GHz, as well as supporting multi-channel usage. Each channel offers a maximum data rate of 150Mbps, which means the maximum data rate of the standard is 600Mbps.

#### IEEE 802.11ac

Initially released in 2014, ac drastically increases the data throughput for Wi-Fi devices up to a maximum of 1,300 megabits per second. Furthermore, ac adds MU-MIMO support, additional Wi-Fi broadcast channels for the 5GHz band, and support for more antenna on a single router.

#### IEEE 802.11ax

When ax completes it can reach theoretical network throughput of 10Gbps. wireless ax will increase network capacity by adding broadcast subchannels, upgrading MU-MIMO, and allowing more simultaneous data streams.

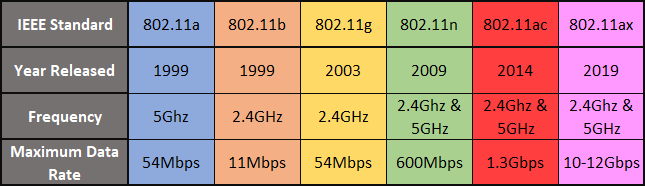


Figure 2: Wi-Fi Standards

## 3. Open System Interface (OSI) Basics

OSI is a [conceptual model](https://en.wikipedia.org/wiki/Conceptual_model) that characterizes and standardizes the communication functions of a [telecommunication](https://en.wikipedia.org/wiki/Telecommunication) or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard [communication protocols](https://en.wikipedia.org/wiki/Communication_protocols). The original objective of the OSI model was to provide a set of design standards for equipment manufacturers so they could communicate with each other. The OSI model defines a hierarchical architecture that logically partitions the functions required to support system-to-system communication.

The OSI model can be seen as a universal language for computer networking. It’s based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

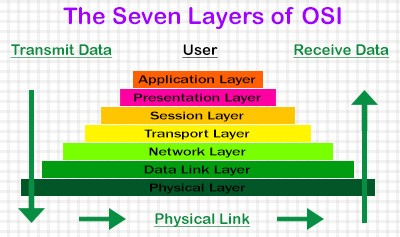


Figure 3: OSI Model Stack

#### Application Layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

#### Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/), and compression of data. Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data. Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

#### Session Layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

#### Transport Layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn’t overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn’t.

#### Network Layer

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender’s device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

#### Data Link Layer

The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

#### Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices

## 4. Physical Layer Frame Structure and its types

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Hub, Repeater, Modem, Cables are Physical Layer devices.

Functions of the physical layer are,

#### Bit synchronization

The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

#### Bit rate control

The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

#### Physical topologies

Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.

#### Transmission mode

Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

## 5. Data Link Layer

Is the protocol layer in a program that handles the moving of data into and out of a physical link in the network. Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same [LAN](https://searchnetworking.techtarget.com/definition/local-area-network-LAN) or [WAN](https://searchnetworking.techtarget.com/definition/WAN-wide-area-network). The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time. The data link layer has two sub layers.

#### Logical link control ([LLC](https://searchnetworking.techtarget.com/definition/Logical-Link-Control-layer)) sublayer

LLC, [multiplexes](https://en.wikipedia.org/wiki/Multiplexing" \o "Multiplexing) protocols running at the top of the data link layer, and optionally provides flow control, acknowledgment, and error notification. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

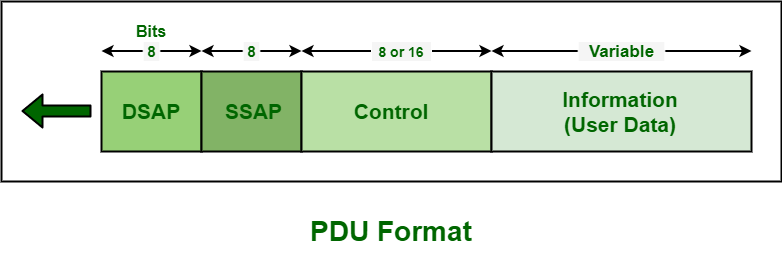


Figure 5: LLC PDU Format

#### Media access control ([MAC](https://searchsecurity.techtarget.com/definition/message-authentication-code-MAC)) sublayer.

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The essence of the MAC protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. MAC can be classified into two types –

##### Point Coordination Function (PCF)

PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

##### Distributed Coordination Function (DCF)

DCF uses CSMA/CA as access method as wireless LAN can’t implement CSMA/CD. It only offers asynchronous service.

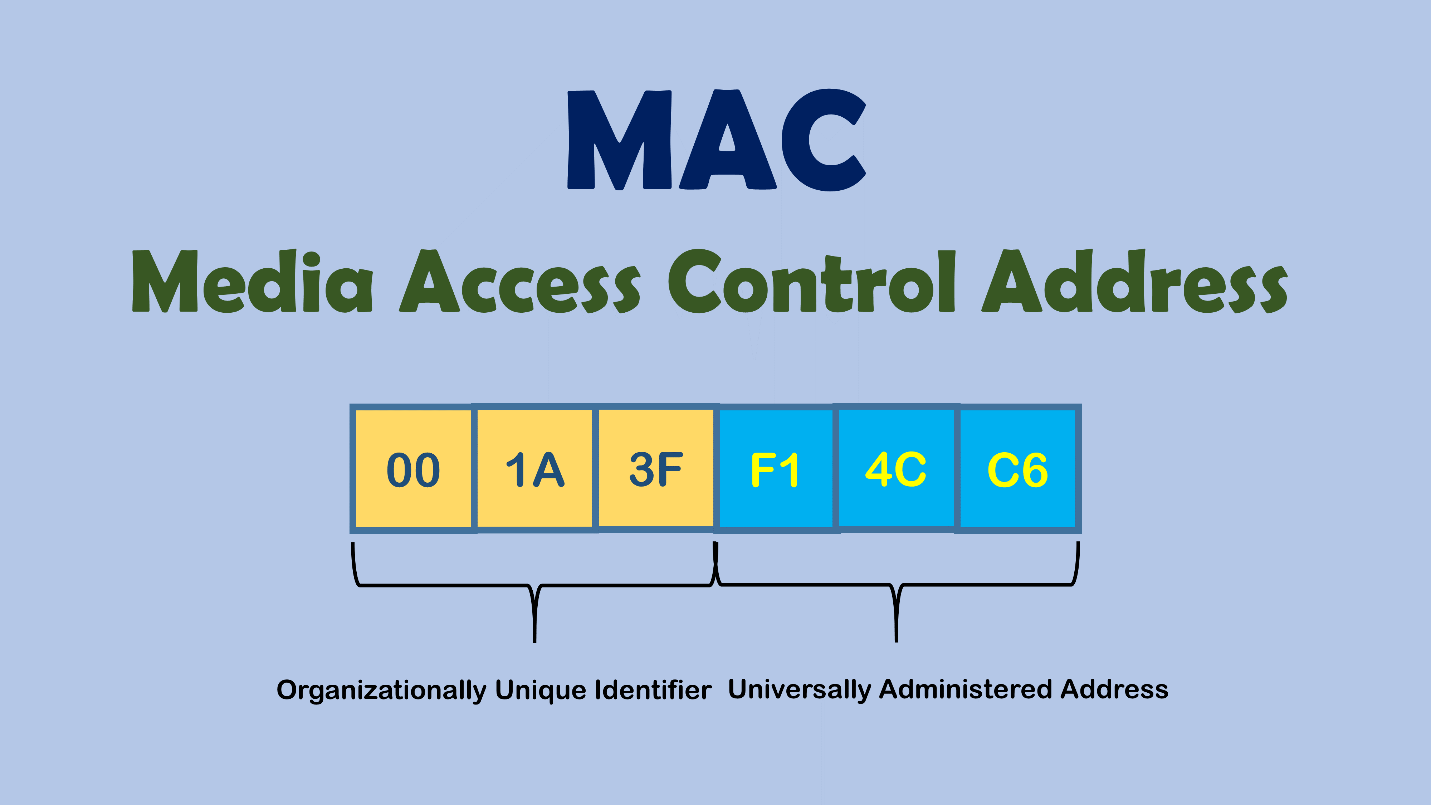


Figure 5: Data Link Layer

#### WLC MAC Frames

MAC Frame consist of Preamble, Header, and Payload Data. Preamble is used for time and frequency synchronization. Header for packet configuration, Payload is used for packet data. Each Frame consist of MAC header, payload and Frame Check Sequence. Each MAC header consist of Frame Control field, Duration ID field, Sequence Control field and Quality Service Control Field

Frame – 1. Management Frame 2. Control Frame 3. Data Frame.

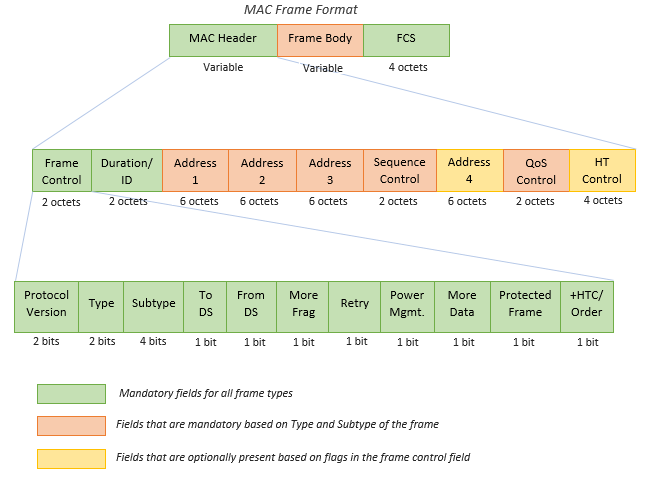


Figure 4: Physical Layer Frame Structure

##### Management Frame

Allow for the maintenance of Communication.

They are of 10 types,

1. Authentication Frame

2. Association Request Frame

3. Association Response Frame

4. Beacon Frame

5. De-authentication Frame

6. Di-Association Frame

7. Probe Request Frame

8. Probe Response Frame

9. Re-Association Request Frame

10. Re-Association Response Frame

Link: <https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf>

##### Control Frame

Facilitates in the exchange of Data.

Types are,

1. ACK Frame

2. Request to Send Frame (RTS): provide collision Reduction stream for AP with hidden stations.

3. Clear to Send (CTS): provide clearance for the requesting station to send a data frame.

##### Data Frame

They carry higher –level protocol data in the frame body.

Link: <https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html>

Link: <https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf>

## 6. Wi-Fi Standard Evolution

**1. 802.11a** was more costly and a little more difficult to implement as it operated at 5 GHz and it was difficult for the hardware implementation as a result initially not widely accepted because higher frequency was involved and led rise to 802.11b.

**2. in 802.11b,** speed and interference was the problem hence 802.11g was established.

**3. 802.11g** was fully backwards compatible with 802.11b hardware hence the presence of 802.11b device significantly reduced the speed of the overall 802.11g network, also suffered from same interference in the existing crowd of 2.4 GHz, hence to improve WLAN Range, Reliability and throughput amendments were done and 802.11n was established.

4. Need of new usage Models which would require higher throughput such as wireless display, In home distribution of IPCV, Rapid upload and download of large files and backhaul traffic, **802.11ac** was established

Link: <https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf>

Link: <https://www.netspotapp.com/explaining-wifi-standards.html>

## 7. OFDMA, DSSS, FHSS

#### OFDMA (Orthogonal Frequency Division Multiple Access)

Orthogonal Frequency Division Multiplex, OFDM is a form of signal format that uses a large number of close spaced carriers that are each modulated with low rate data stream. The close spaced signals would normally be expected to interfere with each other, but by making the signals orthogonal to each other there is no mutual interference. The data to be transmitted is shared across all the carriers and this provides resilience against selective fading from multi-path effects.

The use of OFDMA with 802.11ax increases the capacity of the system by segmenting the channels into smaller sub-channels that overlap in frequency. Previous generations of Wi-Fi would wait until there was an available slot for the whole channel, but 802.11ax enables different devices to use sections of the channel.

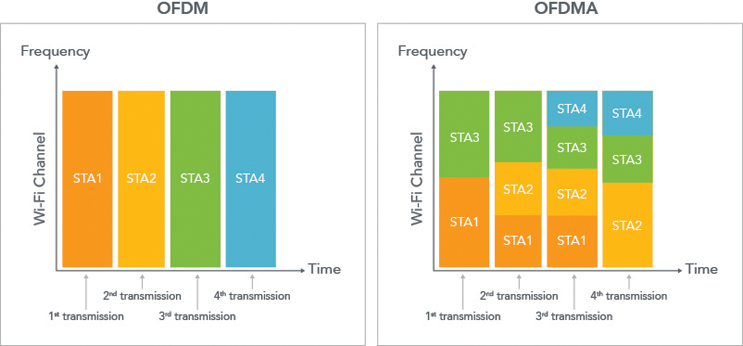


Figure 6: OFDMA

#### DSSS (Direct Sequence Spread Spectrum)

Spreading technique which extends bandwidth of input Signal. Here Input signal can be modulated by PSK/QPSK/QAM then it is speeded using signal generated by Chip generator or barker code using XNOR operation or any relevant operation. It is digital spread spectrum technique. It has better security and immunity against Jamming compared to FHSS. It is applied in CDMA.

Link: <https://www.youtube.com/watch?v=MqnzaHsQ90U>

Link: <https://www.electronics-notes.com/articles/radio/dsss/what-is-direct-sequence-spread-spectrum.php>

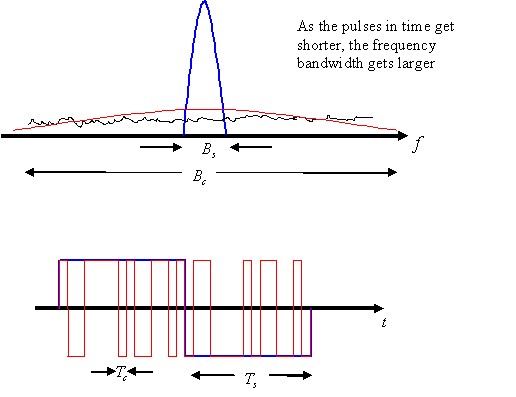


Figure 7: DSSS

#### FHSS (Frequency Hopping Spread Spectrum)

Here original signal is modulated with Frequency Shift Keying as other methods like QAM etc are costly. Then it is passed to a spreader, where it is modulated with carrier from frequency synthesizer using code generated from PN Generator. Here with respect to time frequency gets changed. Frequency hopping occurs for set of frequencies for particular cycle and it repeats for next cycle.

FDM -> Here channel will not change frequency with respect to time.

FHSS -> Here channel are changing frequency w.r.t to time, in other words, frequency is hopping w.r.t to time for particular channel.

Chip Period > Bit Period → Slow Hopping, Chip Period < Bit Period → Fast Hopping.

Applied in Bluetooth, Joint Tactical Radio System (JTRS) etc.

Link: <https://www.youtube.com/watch?v=PUQMKrtUYz8>

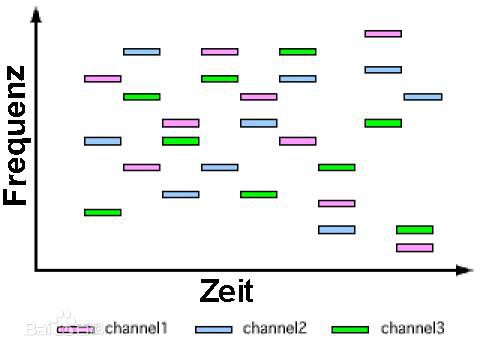


Figure 8: FHSS

## 8. 802.11 MIMO

#### MIMO

MIMO is a form of antenna technology that uses multiple antennas to enable signals travelling via different paths as a result of reflections, etc., to be separated and their capability used to improve the data throughput and / or the signal to noise ratio, thereby improving system performance.

The 802.11n standard allows for up to four spatial streams to give a significant improvement in the available data rate available as it allows a number of different data streams to be carried over the same channel.

The number of data streams and hence the overall data capacity is limited by the number of spatial streams that can be carried - one of the limits for this is the number of antennas that are available at either end.

#### Antenna Technology

The antenna associated technologies have been significantly improved by the introduction of beam forming and diversity. Beam forming focuses the radio signals directly along the path for the receiving antenna to improve the range and overall performance. A higher signal level and better signal to noise ratio will mean that the full use can be made of the channel.

Diversity uses the multiple antennas available and combines or selects the best subset from a larger number of antennas to obtain the optimum signal conditions. This can be achieved because there are often surplus antennas in a MIMO system. As 802.11n supports any number of antennas between one and four, it is possible that one device may have three antennas while another with which it is communicating will only have two. The supposedly surplus antenna can be used to provide diversity reception or transmission as appropriate.

## 9. Channel Bonding

In simple terms channel bonding is use of more than one frequency or channel in the same bandwidth to increase throughput (Like going from 2 Lane to 4 Lane Highway). Came with 802.11n for 40 MHz Channels. Achievable data rate between 2 radios is a function of the Signal-to-Noise ratio (SNR) at a receiver. A higher Noise floor results in lower effective maximum transmission speed.

There are two types of band

1. 2.4 Ghz

2. 5 Ghz

The following link explains in depth about channel bonding and its rules and regulations

Link1: <https://www.networkcomputing.com/wireless-infrastructure/channel-bonding-wifi-rules-and-regulations>

Link2: <https://www.sourceonetechnology.com/802-11ac-wireless-channel-bonding-mimo-spatial-streams-and-beamforming/>

#### 2.4 GHz

802.11 WLAN Standards specify a bandwidth of 20 MHz and channels are on 5 MHz incremental steps. There are 14 channels defined in 2.4 Ghz. The differences occur in RF Modulation schemes used, but the WLAN channels are identical across all the Applicable 802.11 standards. Longer Range than 5 Ghz. Non-Overlapping Channels for 2.4 Ghz band are 1,6 and 11. That is 2.41, 2.43 and 2.46 Ghz.

Graphical representation of 2.4 Ghz Band Channels Overlapping is shown

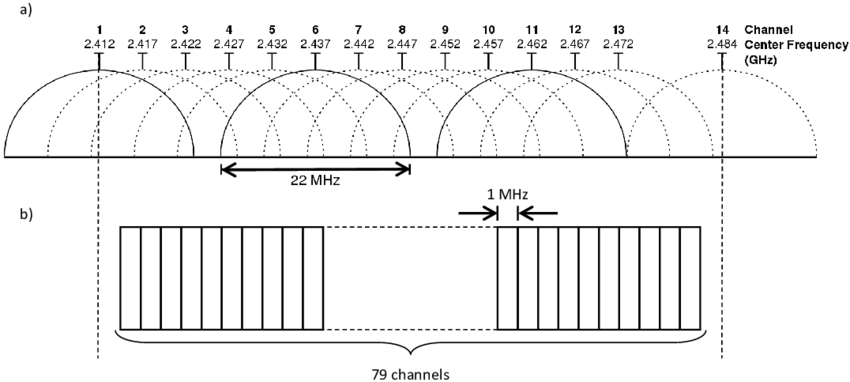


Figure 9: 2.4 GHz Band Frequency Allocation

#### 5 GHz

All 25 of the available 5 Ghz channels non-overlapping at 20 MHz incremental width. Band is divided into several different sections, they are as follows: Unlicensed National Information Infrastructure (U-N II) – 1, 2a, 2c, 3, Industrial Scientific & Medical (ISM).

1. UNII -1 = It is regulated by [Federal Communication Commission (FCC)](https://en.wikipedia.org/wiki/Federal_Communications_Commission). Allowed for Outdoor and Indoor Wi-Fi at the same power. 802.11ac and 802.11n client devices use this band.

2. UNII -2 = Reserved by FCC for weather radar system. Dynamic Frequency switching (DFS) is required by Access Point and Client services. Only higher end 802.11ac and older 802.11n.

3. UNII -2 Extended = Reserved by FCC for govt weather radar system.

UNII -3 = Designed for Indoor & Outdoor Usage by FCC. Supported by 802.11n and 802.11ac.

4. ISM = Supported by 802.11a, 802.11n, 802.11ac

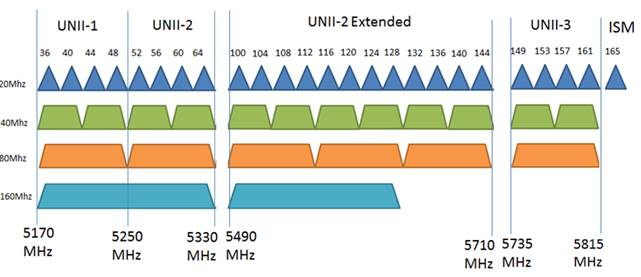


Figure 10: 5 GHz band Frequency Allocation

## 10. Active and Passive Scanning

#### Reason

Determine the suitable AP to which the client may need to connect/roam now or in the future.

#### Types of Scanning

1. Active Scanning

2. Passive Scanning

#### Active Scanning

Here Client Radio transmits probe request to AP. A P sends probe response to Client where it ask about password. After successful authentication of password, AP gives acknowledgement to client.

##### Scanning Duration

Scanning is sensitive to high priority (voice or video) traffic or heavy data traffic. If (voice or video traffic) at 64 Kbps or higher, in this case active- scanning scans for 30 ms every 60 seconds. Heavy Data traffic is present at 4 Mbps or high, In this case, active scanning scans for 30 ms every 5 seconds. In all other cases, it scans for 30 ms every seconds.

#### Passive Scanning

Client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for beacon.

Link:[https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning#:~:text=During%20an%20active%20scan%2C%20the,sent%20periodically%20by%20an%20AP](https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning)

#### Difference between Probe Response and Beacon

1. Beacon frame contains a TIM, Probe response does not.

2. The Beacon frame is broadcast packet whereas Probe Response is unicast packet.

3. Beacon frame contains all information element (IE), whereas the probe response contain the requested information element that may have been requested by the probing station

## 11. MAC Layer Specification (AMPDU & AMSDU)

#### [SDU](https://en.wikipedia.org/wiki/Service_data_unit)

It is unit of data passed down from OSI layer to Lower Layer without any kind of [encapsulation](https://en.wikipedia.org/wiki/Service_data_unit). Then it gets encapsulated into Lower layer Protocol Data Unit (PDU) and the process continues until reaching Physical layer. It is set of data sent of user of particular layer to lower layer. The SDU accepted by any given layer (n) from layer (n+1) is a PDU of the layer (n+1). In other words SDU is the payload of a given PDU. Layer may add up [headers](https://en.wikipedia.org/wiki/Header_(computing)) and [trailers](https://en.wikipedia.org/wiki/Trailer_(computing)) or both to SDU and may do other kinds of processing.

The primary goal of both 802.11n and 802.11ac was to provide high throughput and bigger data rates. frame aggregation is one key aspect of 802.11n/ac that did enhance airtime efficiency. Fixed MAC layer overhead and medium contention overhead are reduced, which results in less airtime consumption.

#### [MSDU](https://en.wikipedia.org/wiki/MAC_service_data_unit)

Media Access Control is the service data unit that is received from the [Logical Link Control](https://en.wikipedia.org/wiki/MAC_service_data_unit) sublayer which lies above MAC sub-layer in protocol stack. It is the layer 3–7 payload of an 802.11 data frame

#### MPDU

It is essentially a technical term for wireless frame. An MPDU consists of a frame header, body and trailer with the MSDU payload encapsulated in the frame body.

#### Methods of Frame Aggregation

1. A-MSDU -> *Aggregation MAC Service Data Unit (A-MSDU)* aggregates multiple MSDUs into a single frame transmission.

2. A-MPDU -> *Aggregate MAC Protocol Data Unit (A-MPDU)* aggregates multiple frames into a single transmission followed by a Block Acknowledgement.

802.11ac used only AMPDU for frame aggregation and 802.11n used both AMPDU and AMSDU. 80211ax introduces ***Multi-Traffic Identifier Aggregated MAC Protocol Data Unit (Multi-TID AMPDU)***, which allows the aggregation of frames from multiple traffic identifiers (TIDs), from the same or different QoS access categories.

Link:[https://www.extremenetworks.com/extreme-networks-blog/802-11ax-frame-aggregation-enhancements/?aliId=eyJpIjoiTFVRK3Vlamo2S3cyT0I1MCIsInQiOiI1S2M0dVVneFlPUFVHcW1JemhDeFJBPT0ifQ%253D%253D](https://www.extremenetworks.com/extreme-networks-blog/802-11ax-frame-aggregation-enhancements/?aliId=eyJpIjoiTFVRK3Vlamo2S3cyT0I1MCIsInQiOiI1S2M0dVVneFlPUFVHcW1JemhDeFJBPT0ifQ%3D%3D)

## 12. Wi-Fi Security (WEP, WPA, WPA2, WPA3)

#### WEP

Earliest Security Protocol. It provides privacy to wireless device equivalent to Wired Device. It uses the stream cipher RC4 for confidentiality and CRC-32 checksum for integrity. It aims at providing data encryption [confidentiality](https://en.wikipedia.org/wiki/Confidentiali) and [integrity](https://en.wikipedia.org/wiki/Data_integrity) protection for 802.11 standards. WEP clients share a secret key known as WEP key used for authentication and for encryption and decryption of messages.

1. WEB Frame = Header + [Initialization vector](https://en.wikipedia.org/wiki/Initialization_vector) + [Key](https://en.wikipedia.org/wiki/Key_(cryptography)) Number +Payload + Integrity Check Value (CRC 32).

2. Data Encryption Scheme -> (User) X-OR (Keystream (pseudorandom))

[Rivest Cipher 4](https://en.wikipedia.org/wiki/Stream_cipher) (key stream) = Initialization vector (24 Bit) + key (40 Bit)

Flaws :

1. WEB cannot prevent forgery of packets

2. Cannot prevent Replay of attack

3. Reuses IV

Link: <https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy>

Link: <https://www.youtube.com/watch?v=dB3kfXtaugQ>

#### WPA

It is known as Wi-Fi protected Access. It’s a protocol which implements much of the IEEE 802.11i standards. TKIP (Temporal Key Integrity Protocol) was adopted for WPA. t was a solution to replace WEP without replacing its hardware as it was already deployed. It’s a message integrity check algorithm to verify integrity of the packets. It was a solution to replace WEP without replacing its hardware as it was already deployed. It made following changes

1. It implies a key mixing function that combines key with IV before passing it to RC4 cipher unlike in WEP where they were merely concatenated.

2. It implements Sequence counter and Time stamps to prevent [Replay attacks](https://www.youtube.com/watch?v=ZeuWpL-7EwY). By this data packets received out of order or delayed would be rejected.

3. It Implements 64-Bit [Message Integrity Check (MIC)](https://en.wikipedia.org/wiki/Message_authentication_code) and e-initialize the sequence number each time when a new key(Temporal key) is used.

4. TKIP ensures that every data packet is sent with a unique encryption key (Temporal key + packet sequence counter)

Link: <https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol>

#### WPA2

It’s an up gradation of WPA and its aim was to provide even more security then TKIP Algorithm used in WPA. It uses AES(Advanced Encryption Standards). TKIP is not as strong as AES because it relied on older weakness of WEP. AES is a variant of Rijndael which was recently chosen as the standard symmetric key encryption algorithm. It is based on design principle known as a substitution - permutation network.

Total number of rounds depends on the length of the data block being encrypted and the length of the encryption key being used. The Square block cipher which Rijndael improved upon was vulnerable to a set of attacks known collectively as the Square attack. Resistance to this was worked in by substituting the Shift Row transformation for a transpose of the square matrix of bytes which allowed diffusion over an entire data block via alternating Mix Column and Mix Row transformations. A round key before rounds was added to improve overall security. Process of encryption requires Substituting bytes, Shifting rows, Mixing columns with user input matrix and output of that was multiplied with the set of keys. A 128 bit / 4 word key is expanded to 44 words for 10 rounds + 1 usage of 4 words key matrix.

Link: <https://blog.finjan.com/rijndael-encryption-algorithm/>

Link: <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

#### WPA3

WPA3 is more about personal level protection and to tackle few drawbacks of WPA2 such as [brute-force-attacks](https://en.wikipedia.org/wiki/Brute-force_attack) which is a critical vulnerability of WPA2. In WPA2, once the hackers captured the right data from airwaves, they can take it to offshore and perform password guessing. Complexity of the network’s WPA2-Personal passphrase had a correlation to the complexity of cracking the security and majority keep simple password. User with the passphrase could snoop on another user’s network traffic and perform attacks.

WPA adds the following notable features:

**1. Simultaneous Authentication of Equals (SAE) Protocol**

This is used to create a secure handshake, where a network device will connect with Wireless access point and both device communicate to verify authentication and connection

**2. Stronger Brutal force attacks**

Here WPA protects against offline password guess by allowing user only one guess, making the user to interact directly with the network which means he has to be physically present each time.

**3. Individual Data Encryption**.

For the safety of each and every data we need Individual Data encryption.

## 13. CSMA/CD & CSMA/CA

#### CSMA/CD

Known as Carrier Sense Multiple Access/Collision Detection. Each computer first senses if the wire is idle, if its idle then it sends the data. Since they all are sharing data on a cable, the cable must be regulated so that no computer send data at the same time. If collision happens between two signals then a jamming signal is sent by one computer which notifies all others and after that computer who had collision wait for an random time and transmission resumes whoever finds the path empty.

Link: <https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection>



Figure 11: CSMA/CD

#### CSMA/CA

Known as Carrier Sense Multiple Access Collision Avoidance. Used In wireless Networks. Here once the destination device receives the data, it will respond back with the ACK. If the sending computer does not receive an ACK from the destination, it will assume that it did not get the data and resend it again until it receives an ACK. Here Carrier sensing is used but nodes attempt to avoid collision by beginning transmission after the channel is sensed to be idle.

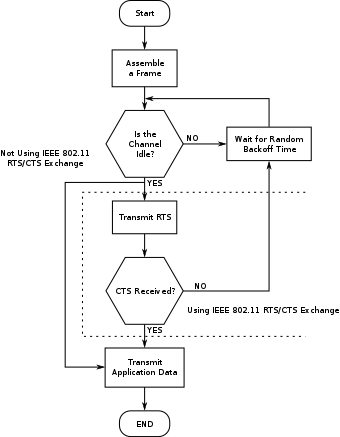


Figure 12: CSMA/CA

Link: <https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance>

## 14. Hidden Terminal and Exposed Terminal Problem with MACA Solution.

#### Hidden Terminal Problem

Suppose both A & C wants to communicate with B, so they send it a frame. A & C are unaware of each other. When both of them send signal at a time, collision happens. Unlike Ethernet A & C are unaware of each other and A & C are said to be hidden nodes with respect to each other.

**Solution**: MACA Algorithm

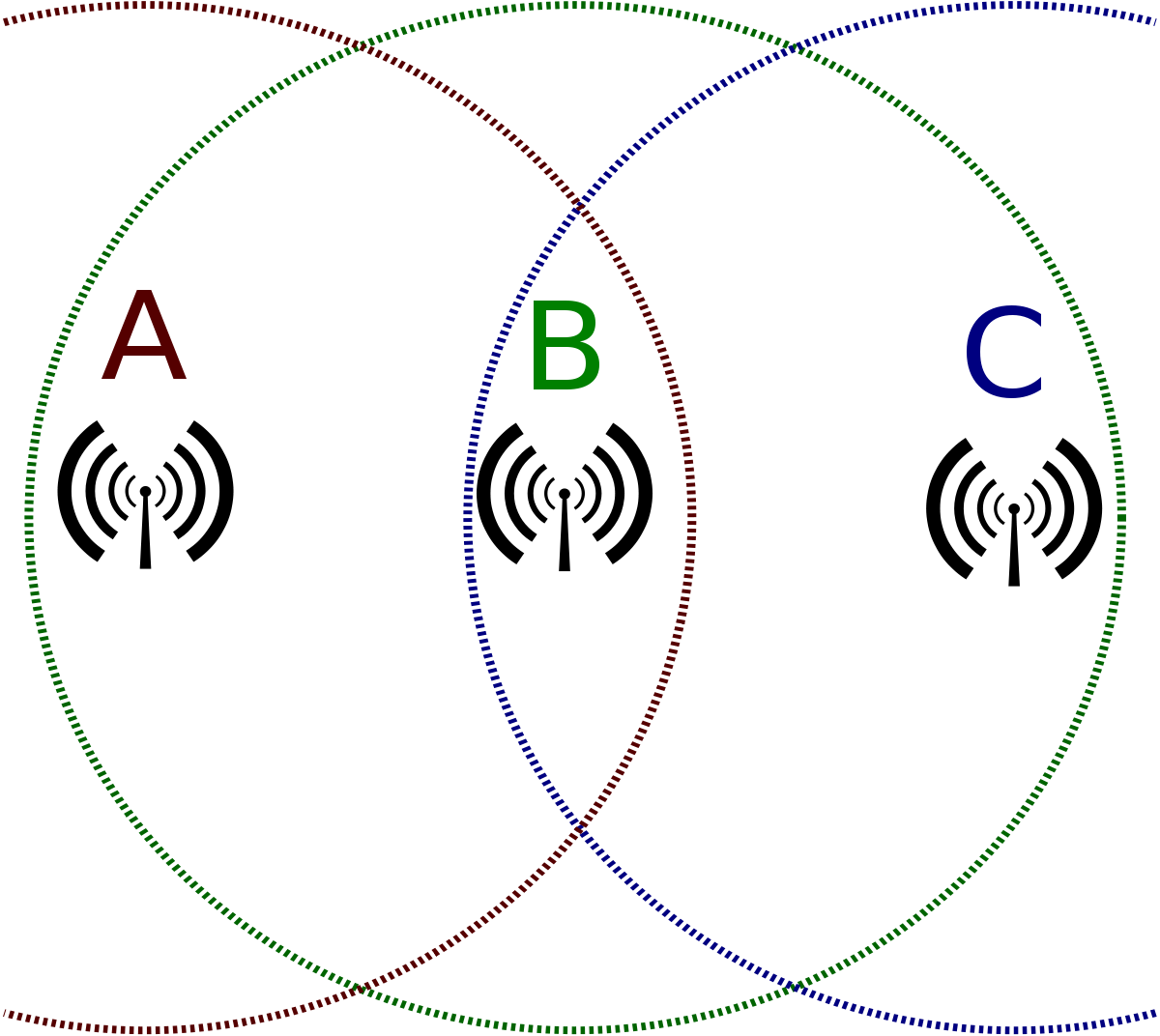
****

Figure 13: Hidden Terminal Problem

Link: <https://www.youtube.com/watch?v=_oz4WTWRfGs>

#### Exposed Terminal Problem

If B is communicating with A. Node C is aware of this communication because it hears B’s Transmission. It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B’s Transmission. C can transmit to D with any effect on A

**Solution**: MACA Algorithm

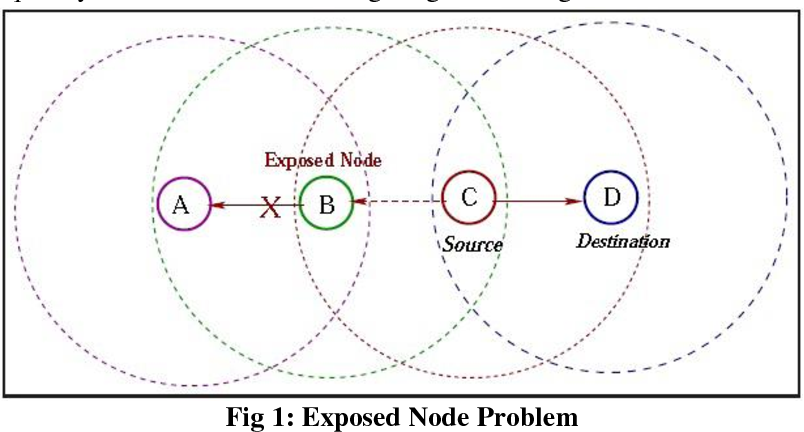
****

Figure 14: Exposed Terminal Problem

Link: <https://www.youtube.com/watch?v=mhuXdaRoLzA>

#### MACA Solution

Key Idea:

Sender and Receiver Exchange Control frames with each other before the sender actually transmit the data.

This exchange informs all nearby nodes that transmission is about to begin. Sender Transmits RTS frame to receiver and it replies with CTS frame. RTS frame and CTS frame are shown below. Any node that sees CTS frame knows that it is close to the receiver, therefore cannot transmit for the period of time it takes to send a frame of the specified length. Any node that sees the RTS frame but not the CTS frame knows that it is not close enough to the receiver and therefore it won’t interfere with it.

Usage of ACK in MACA:

Receiver sends an ACK to the sender after successfully receiving a frame. All nodes must wait for an ACK before trying to transmit. If 2 or more nodes detect an idle line and try to transmit, an RTS frame at the same time then collision happens. Unfortunately, 802.11 does not support collision. When they don’t get CTS, they realise that a Collision has happened. They resend this whole thing again after waiting for time defined by the same exponential back off algorithm used in the Ethernet.

Link: <https://www.youtube.com/watch?v=mhuXdaRoLzA>

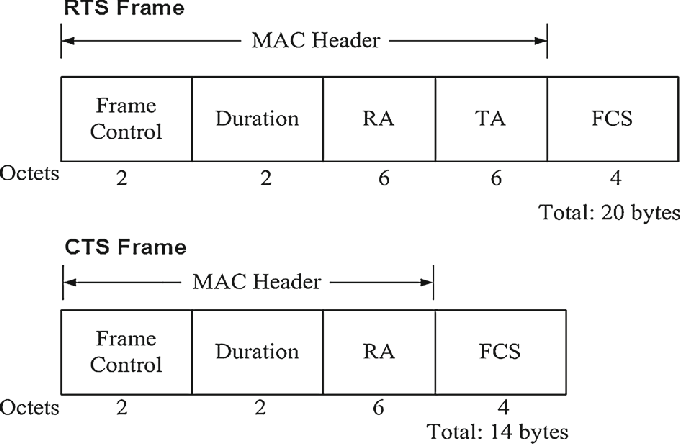


Figure 15: CTS & RTS Frame

## 15. Important Protocols

#### EAPOL Protocol

The 4-way handshake is the process of exchanging 4 messages between an access point (authenticator) and the client device (supplicant) to generate some encryption keys which can be used to encrypt actual data sent over Wireless Medium.

Link:<https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/#:~:text=Extensible%20Authentication%20Protocol%20(EAP)%20over,on%20to%20access%20network%20resources>.

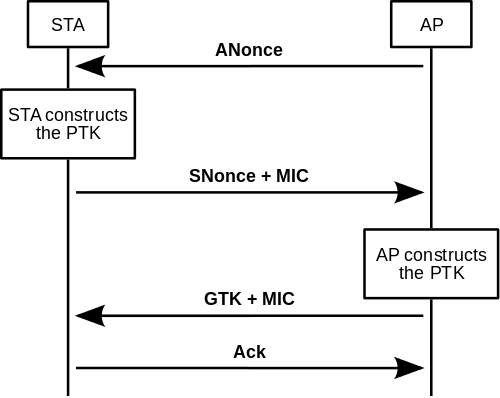


Figure 16: EAPOL Handshake

#### ICMP (Internet Control Message Protocol)

ICMP is a transport level protocol within TCP/IP which communicates information about network connectivity issues back to the source of the compromised transmission. It sends control messages such as destination network unreachable, source route failed, and source quench. It uses a data packet structure with an 8-byte header and variable-size data section.

ICMP is used by a device, like a router, to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong. It's a protocol that believes in direct communication in the workplace.

Ping is a utility which uses ICMP messages to report back information on network connectivity and the speed of data relay between a host and a destination computer. It's one of the few instances where a user can interact directly with ICMP, which typically only functions to allow networked computers to communicate with one another automatically.

Link: <https://geek-university.com/ccna/internet-control-message-protocol-icmp/>

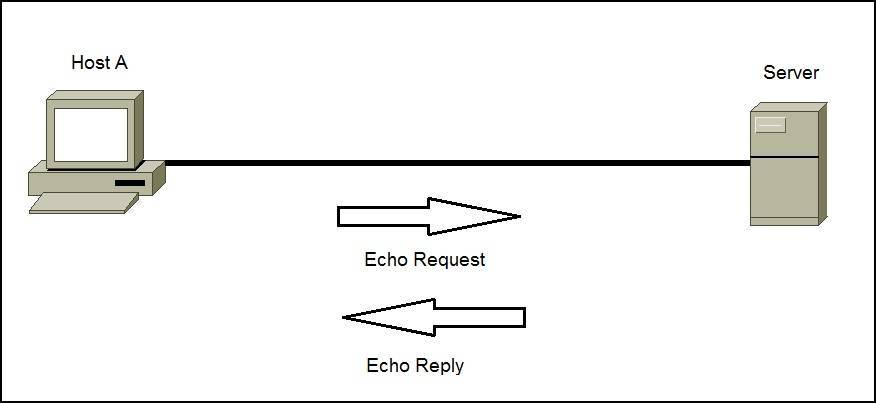


Figure 17: ICMP Echo

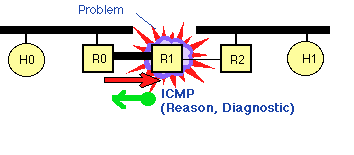


Figure 18: ICMP Protocol

#### DHCP (Dynamic Host Configuration Protocol)

It is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) [networks](https://en.wikipedia.org/wiki/Computer_network), whereby a DHCP [server](https://en.wikipedia.org/wiki/Server_(computing)) dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to each device on the network, so they can communicate with other IP networks.

A DHCP server enables computers to [request](https://en.wikipedia.org/wiki/Request%E2%80%93response) IP addresses and networking parameters automatically from the [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) (ISP), reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a [user](https://en.wikipedia.org/wiki/User_(computing)) to manually assign IP addresses to all network devices.

 In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

Link: <https://geek-university.com/ccna/dynamic-host-configuration-protocol-dhcp/>

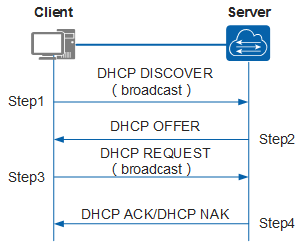


Figure 19: DHCP Protocol

#### ARP (Address Resolution Protocol)

It is a network protocol used to find the hardware (MAC) address of a host from an IP address. ARP is used on Ethernet LANs because hosts that want to communicate with each other need to know their respective MAC addresses. It is a request-reply protocol; ARP request messages are used to request the MAC address, while ARP reply messages are used to send the requested MAC address.

Link: <https://geek-university.com/ccna/address-resolution-protocol-arp/>

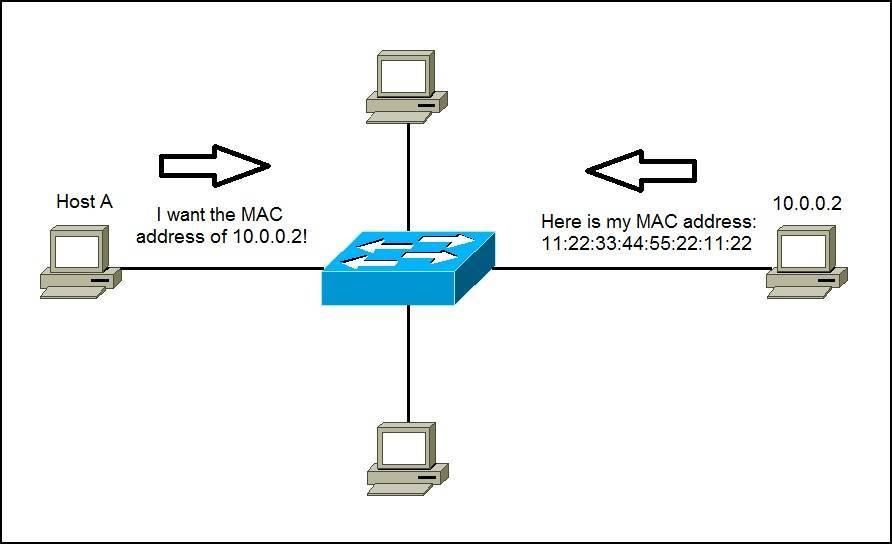


Figure 20: ARP Protocol

#### Transmission Control Protocol (TCP)

TCP is a standard that defines how to establish and maintain a network conversation through which application programs can be exchanged. TCP works with Internet Protocol which defines how computers send packets of data to each other.

TCP is a [connection-oriented](https://searchnetworking.techtarget.com/definition/connection-oriented) protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages [flow control](https://whatis.techtarget.com/definition/flow-control) and -- because it is meant to provide error-free data transmission -- handles retransmission of dropped or garbled packets and acknowledges all packets that arrive.

TCP is used for organizing data in a way that ensures the secure transmission between the server and client. It guarantees the integrity of data sent over the network, regardless of the amount.

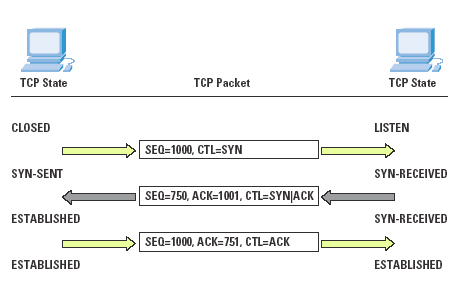


Figure 21: TCP

#### User Datagram Protocol (UDP)

Simplest Transport Layer Communication Protocol. It involves Minimum Amount of Communication mechanism. In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

UDP is deployed where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

UDP Header contains,

1. Source Port
2. Destination Port
3. Length
4. Checksum

Application of UDP,

1. Domain Name Services
2. Simple Network Management Protocol.
3. Trivial File Transfer Protocol.
4. Routing Information Protocol.

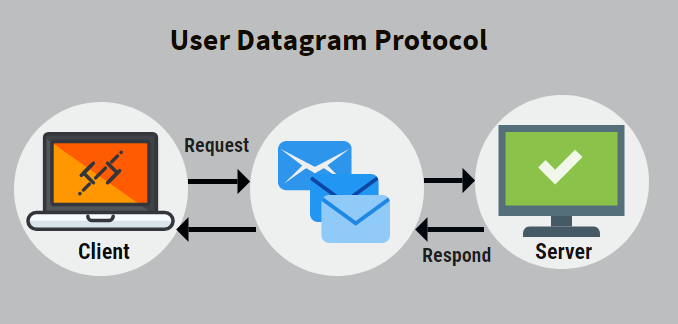


Figure 22: UDP

#### Domain Name Server

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement: Every host is identified by the IP address but remembering numbers is very difficult for the people and the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So, DNS is used to convert the domain name of the websites to their numerical IP address.

Kinds of Domain are,

1. Generic Domain: .com (commercial), .edu (educational), .mil (Military) etc.
2. Country Domain: .in (India), .us, .uk etc.
3. Inverse Domain if we want to know name of the website. IP to domain name mapping.

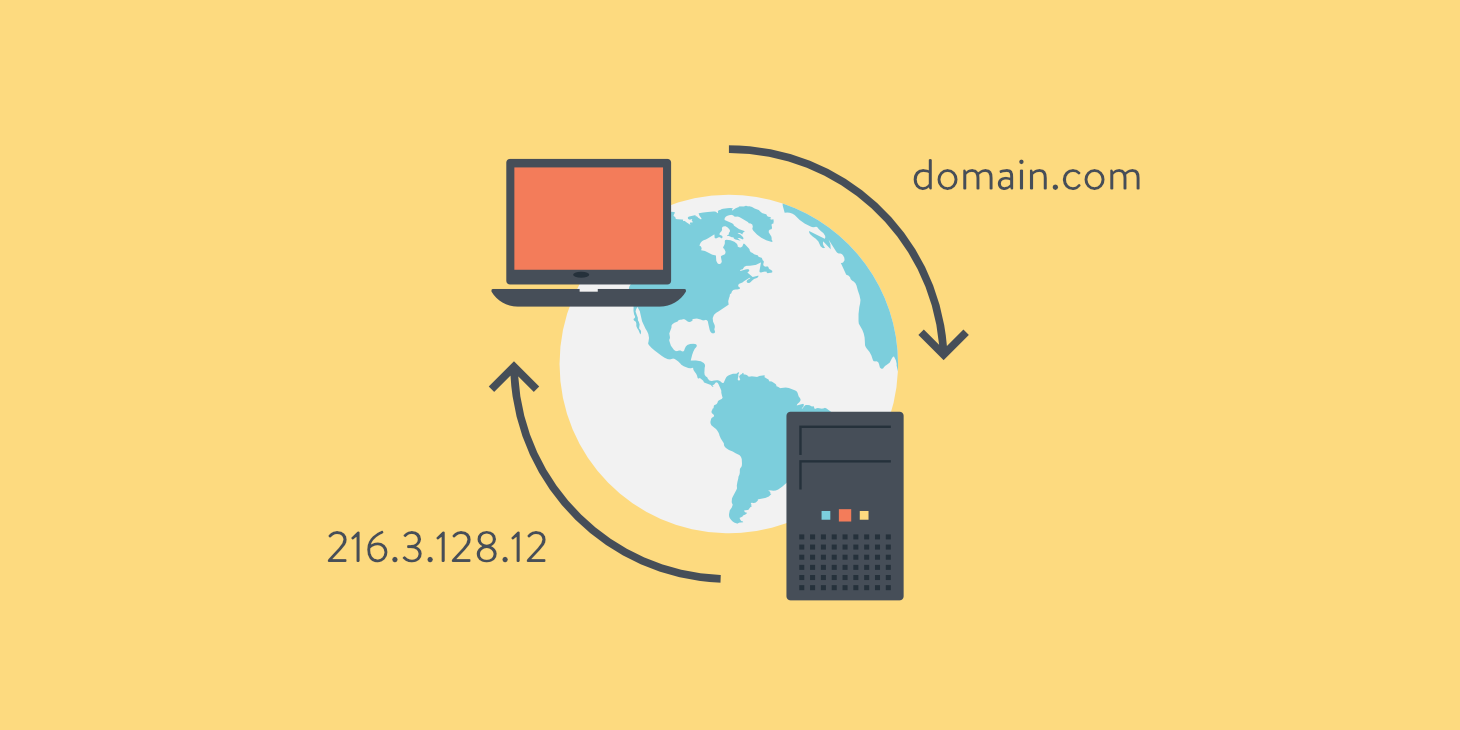


Figure 23: DNS

#### Hyper Text Transfer Protocol (HTTP)

It is an Application-level protocol. HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

Basic features of HTTP,

1. HTTP is connectionless: client and server knows about each other during current request and response only.
2. HTTP Is Media Independent: any type of data can be sent by HTTP if both the client and the server know how to handle the data content.
3. HTTP is Stateless: The server and client are aware of each other only during a current request. Afterwards, both forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.

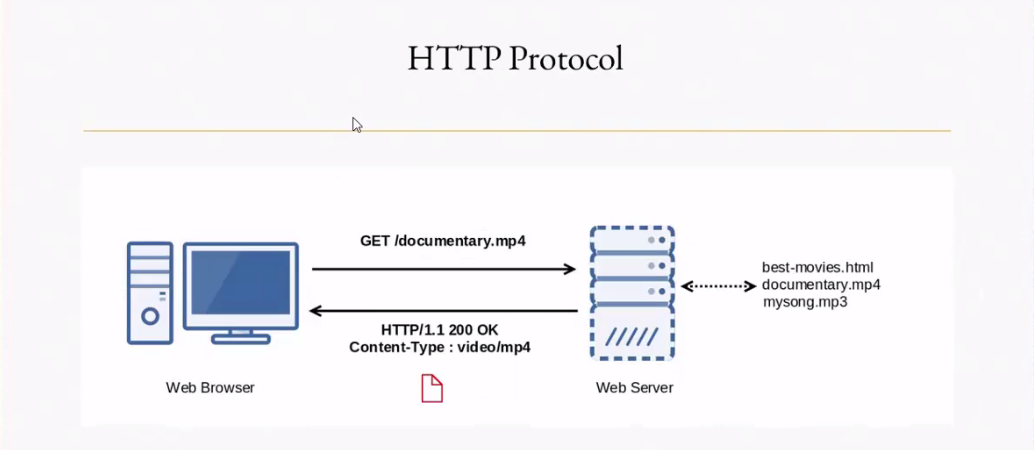


Figure 24: HTTP

# Objectives

1. Learning various Wi-Fi standards and architecture.

2. Testing activities documentation

3. Working or Wi-Fi / WLAN (wireless local area network) devices

4. End to End testing experience

5. Collaboration and teamwork

# Requirements:

## High Level Requirements:

|  |  |
| --- | --- |
| ID | Description |
| HL\_01 | Check for Successful User Registration and Login for registering any product |
| HL\_02 | Configuration of Router. |
| HL\_03 | Signal Testing. |
| HL\_04 | Security Testing and Analysis. |
| HL\_05 | Authentication Testing. |
| HL\_06 | Client Connectivity Testing. |

## Low Level Requirements:

|  |  |
| --- | --- |
| ID | Description |
| LL\_01 | Connection and Setting of router. |
| LL\_02 | Safety Measures for Router |
| LL\_03 | Antenna Signal strength, Data rate, Modulation format and scheme, spectrum band, channel, GSM, Vendor info for FHSS and Frequency information for signal Analysis. |
| LL\_04 | Check for Security protocol and Ciphers used for respective protocol. |
| LL\_05 | 4 Way Handshake between access point and Station for Authentication |
| LL\_06 | Exchange Station Identification for Authentication. |
| LL\_07 | IP Address Allocation for connectivity Testing. |
| LL\_08 | MAC Address Identification for connectivity Testing. |
| LL\_09 | 3 Way Handshake between Client and AP for connectivity Testing. |
| LL\_10 | Successful Conversation at Transport Level for connectivity Testing. |

# Design

Not Applicable

# Test Plan

## High Level Test Plan (Integration Test Plan)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test ID | Requirements Mapping | Description | Expected Input | Expected Output | Actual Output |
| IT\_01 | HL\_01 | Registration Testing & Login Testing for Router | 1. Email id  2. Name  3. Country  4. Password  5. Checkmarks  6. Click on  7. Submit Button | 1. Successful Registration Link  2. My Products Page | 1. Successful Registration Link  2. My Products Page |
| IT\_02 | HL\_02 | Configuration of Router | IP address | Successful Configuration | Successful Configuration |
| IT\_03 | HL\_03 | Testing of Antenna Signal Strength | - | Signal Strength in dBm | Successfully got signal Strength in dBm |
| IT\_04 | HL\_04 | Security Protocol Identification | - | Identification of Security Protection Protocol | Successful identified Security Protection Protocol |
| IT\_05 | HL\_05 | Check for Authentication protocol | Pre-Shared Key | Successful Authentication | Successful Authentication |
| IT\_06 | HL\_05 | Check for Exchange Station Identification Protocol | - | XID Protocol | XID Protocol |
| IT\_07 | HL\_06 | Check for Client Connectivity Protocol | - | Successful client Connectivity | Successful  Client Connectivity |
|  |  |  |  |  |  |

## Low Level Test Plan (Unit Test Plan)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test ID | Requirements Mapping | Description | Expected Input | Expected Output | Actual Output |
| UT\_01 | LL\_01 | Connecting to Router | 1. IP address  2. Enter default Username and Password  3. Reset Username and Password | Successful Connection to Router | Successful Connection to Router |
| UT\_02 | LL\_01 | Setting up Wireless Network | 1. Enter SSID  2. Choose Encryption type  3. Enter PSK | Successful Setting Up Wireless Network | Successful Setting Up Wireless Network |
| UT\_03 | LL\_01 | Forwarding Ports for local IP addresses. | 1. Enter Local IP address in advanced Setting of router configuration | Successful forwarding of ports | Successful forwarding of ports |
| UT\_04 | LL\_02 | Configuring web page filtering and firewall protection | 1. Enter Time access rule, Session Duration, Inactivity time  2. Enable Trusted User  3. Enter sites to be blocked | Successful Configuration for protection. | Successful Configuration for protection. |
| UT\_05 | LL\_03 | Signal Analysis | - | 1. Antenna Signal Strength  2. Data Rate  3. Modulation format  4. Modulation Scheme  5. Spectrum band  6. channel No  7. Frequency  8. GSM  9. Vendor information | 1. Antenna Signal: -45dBm  2. data Rate: 1.0Mb/ps  3. Modulation format: DSSS  4. Modulation scheme: CCK  5. Spectrum band: 2.4 Ghz  6. Channel no: 6  7. Frequency: 243 7MHz  8. GSM: N/A  9. Vendor: N/A |
| UT\_06 | LL\_04 | Security protocol to prevent unauthorized damage and theft of data packets and Replay attacks | Pre-Shared Key | 1. Secure bit = True  2. Encrypted Key data bit = True  3. Pairwise Key bit = True | 1. Secure bit = True  2. Encrypted Key data bit = True  3. Pairwise Key bit = True |
| UT\_07 | LL\_04 | Cipher used in Security protocol | - | Check Key Descriptor Version in Key information of authentication packet: AES/TKIP/RC4 stream cipher | AES Cipher (WPA2/PSK) |
| UT\_08 | LL\_05 | Message1 of 4 Way Handshake | Pre-Shared Key | 1. Station Receives Anounce.  2. Successful Acknowledgement. | Station Receives Anounce.  2. Successful Acknowledgement. |
| UT\_09 | LL\_05 | Message2 of 4 Way Handshake. | - | 1. Access Point receives Snounce  2. Successful Message Integrity Check.  3. Robust Security Network (RSN) Capabilities. | 1. Access Point receives Snounce  2. Successful Message Integrity Check.  3. Robust Security Network (RSN) Capabilities. |
| UT\_10 | LL\_05 | Message3 of 4-way Handshake. | - | 1. Successful Message Integrity Check  2. Station Receives A nounce, RSN-IE.  3. Confirmation of TPK (Install Set Key=1) | 1. Successful Message Integrity Check  2. Station Receives A nounce, RSN-IE.  3. Confirmation of TPK (Install Set Key=1) |
| UT\_11 | LL\_05 | Message 4 of 4 Way Handshake. | - | 1. Successful Message Integrity Check  2. Confirmation of Successful Installation of Temporal Key (Secure Set Bit =1) | 1. Successful Message Integrity Check  2. Confirmation of Successful Installation of Temporal Key (Secure Set Bit =1) |
| UT\_12 | LL\_06 | Convey of Identification from Secondary Station. | - | Response to exchange information in the control field. | Response to exchange information in the control field. |
| UT\_13 | LL\_07 | DHCP Discovery | - | 1. Message Type: Boot Request.  2. Show Client MAC Address. | 1. Message Type: Boot Request.  2. Show Client MAC Address. |
| UT\_14 | LL\_07 | DHCP Offer | - | 1. Message Type: Boot Reply  2. Identify Server IP Address.  3. Show renewal Time.  4. Router Address  5. Broadcast Address | 1. Message Type: Boot Reply  2. Identify Server IP Address.  3. Show renewal Time.  4. Router Address  5. Broadcast Address |
| UT\_15 | LL\_07 | DHCP Request | - | 1. Message Type: Request  2. Show Requested IP Address | 1. Message Type: Request  2. Show Requested IP Address |
| UT\_16 | LL\_07 | DHCP ACK | - | 1. Message Type: ACK.  2. Show IP Address Lease time.  3. ACK of IP Address in Transport layer. | 1. Message Type: ACK.  2. Show IP Address Lease time.  3. ACK of IP Address in Transport layer. |
| UT\_17 | LL\_08 | Address Resolution Protocol for mapping a dynamic IP Address to permanent physical machine (MAC)address |  | 1. Sender MAC and IP Address.  2. Target IP address.  3. ARP type: Request | 1. Sender MAC and IP Address.  2. Target IP address.  3. ARP type: Request |
| UT\_18 | LL\_08 | Address Resolution Protocol for mapping a dynamic IP Address to permanent physical machine (MAC)address | - | 1. ARP type: Reply  2. Sender MAC Address along with IP Address | 1. ARP type: Reply  2. Sender MAC Address along with IP Address |
| UT\_19 | LL\_08 | Duplicate Address Detection. Send IP probe and if no one responds then claim IP Address. IP address probe request. | - | 1. Opcode: Request (1)  2. Sender MAC address=True  3. Target IP Address: True | 1. Opcode: Request (1)  2. Sender MAC address=True  3. Target IP Address: True |
| UT\_20 | LL\_08 | ARP Announcement to claim IP address | - | 1. Opcode: Request (1)  2. Sender MAC address=True  3. Sender IP address: True  4. Target IP Address: True | 1. Opcode: Request (1)  2. Sender MAC address=True  3. Sender IP address: True  4. Target IP Address: True |
| UT\_21 | LL\_09 | 3 Way handshake to establish a reliable Connection.  Step 1: Client SYN | - | 1. SYN Bit = True  2. Client Seq number | 1. SYN Bit = True  2. Client Seq number |
| UT\_22 | LL\_09 | Step 2: Server SYN/ACK | - | 1. SYN & ACK Bit = True  2. Incremented SYN number by server as ACK number | 1. SYN & ACK Bit = True  2. Incremented SYN number by server as ACK number |
| UT\_23 | LL\_09 | Step 3: Client ACK | - | 1. ACK Bit = True  2. ACK number of Client and Server should match. | 1. ACK Bit = True  2. ACK number of Client and Server should match. |
| UT\_24 | LL\_10 | HTTP Get Request | Open a browser | 1. ACK and Push (End of Request) in TCP = True  2. Sequence Number 1  3. Show ACK number | 1. ACK and Push in TCP = True  2. Sequence Number = 1  3. Show ACK number = 1 |
| UT\_25 | LL\_10 | Data Response from Server | - | 1. ACK Bit = True  2. Show Source & Destination Port  3. Sequence Number  4. ACK number: LL\_10 Next Seq number | 1. ACK Bit = True  2. Show Source & Destination Port  3. Sequence Number = 1  4. ACK number: LL\_10 Next Seq number (162) |
| UT\_26 | LL\_10 | ACK from Server of Completion of Data Transmission. | - | 1. ACK Number same as Response from server  2. ACK Bit = True  3. Completion Status from Server | 1. ACK Number same as Response from server = 162  2. ACK Bit = True  3. Completion Status: 200 |
| UT\_27 | LL\_10 | ACK from the Client for receiving each and every transmission. | - | 1. Sequence Number  2. ACK for receive of data from client to Server  ACK = Sequence Number of Transmitted Data | 1. Sequence Number = 162  2. ACK for receive of data from client to Server,  a. ACK1 = Sequence number of 1st data = 1409  b. ACK2 = Sequence number of 2nd data = 2817  c. ACK3 = Sequence number of 3rd data = 3478 |
| UT\_28 | LL\_10 | End of Transmission | - | 1. ACK Number = UT\_10 sequence number  2. FIN & ACK flag = True | 1. ACK Number = 162  2. FIN & ACK flag = True |

# Implementation Summary

### Summary

### Scanning Testing

Wi-Fi scanning is one of the basic functions in a wireless network. It is the mechanism by which a client device (e.g. computer) or an application discovers the wireless networks that are in range of the Wi-Fi adapter. As part of this process, a scanning device or application gathers information about the signal strength, channel, security configuration and capabilities of nearby networks. Client devices use this information to determine which networks they can join or roam to.

There are two methods to perform Wi-Fi scanning: active and passive.

#### Active Scanning

Active scans are enabled by default but can be disabled in a Radio profile. During active scans, the radio sends probe-any requests (probe requests with a null SSID name) to solicit probe responses from other devices. In other words, access points actively look for other devices, in addition to listening for them.

1. Probe Request are broadcasted by the client advertising its capabilities like supported data rates, security and encryption etc along with its source address and waits for the probe response from the AP.

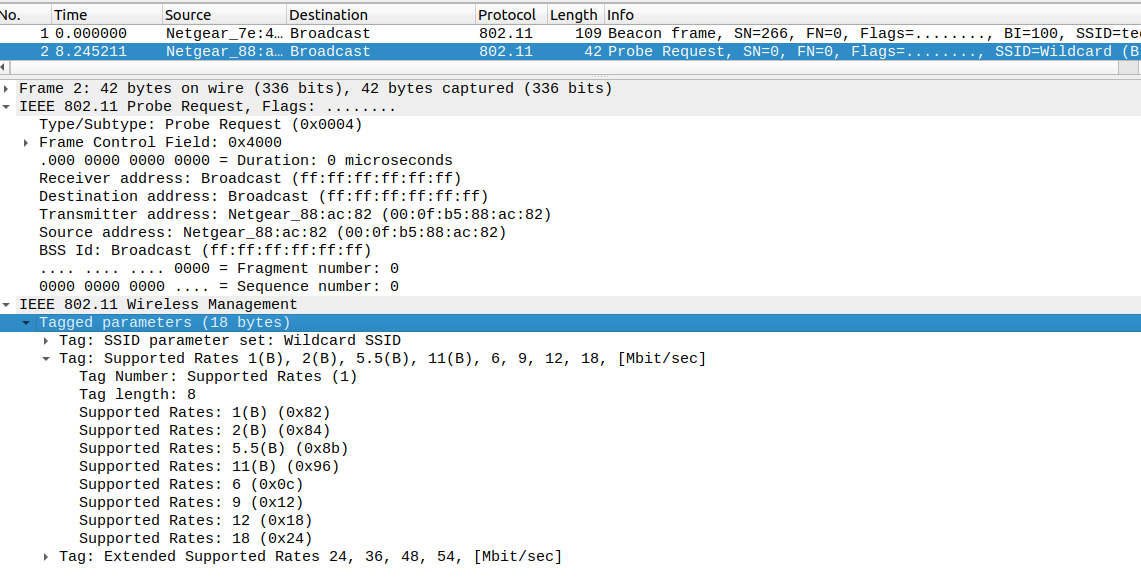


Figure 26: Active Scanning Probe Request

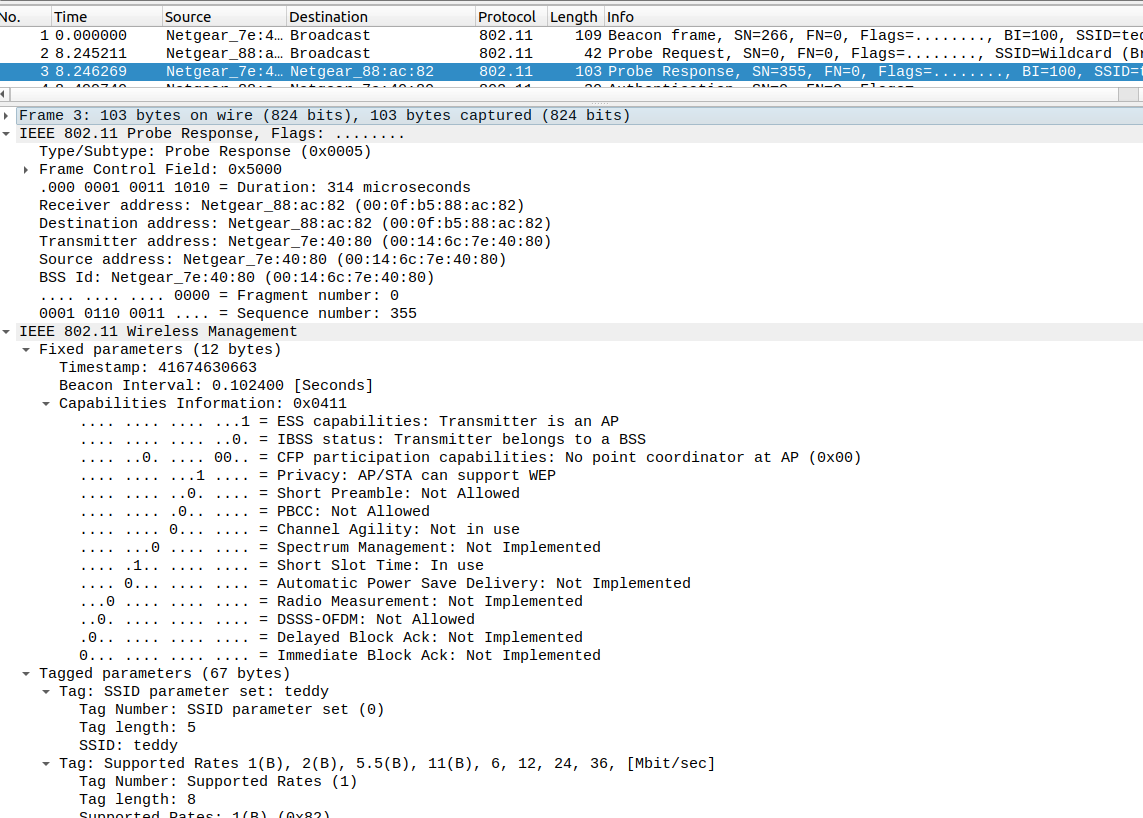
2. AP, on receiving Probe request, checks, capabilities of the Client and if it is capable enough, unicast probe response and then authentication and association starts.

Figure 27: Active Scanning Probe Response

#### Passive Scanning

During passive scans, the radio listens for beacons and probe responses. If you use only passive mode, the radio scans once per second, and audits packets on the wireless network. Passive scans are always enabled and cannot be disabled because this capability is also used to connect clients to access points.

1. Access Points broadcast continuous beacon frames advertising about their Capabilities, sequence number, SSID name and source address etc.

2. Client who listens for beacons on each channel, on receiving broadcasted frame, checks for the capabilities and if its capable enough then it sends a probe response requesting for authenticate and associate.

Beacons are sent periodically at a time called Target Beacon Transmission Time(TBTT)

Beacon Interval=100 TU (100x 1024 microseconds or 102.4 milliseconds)

Since, 1 TU=1024 microseconds

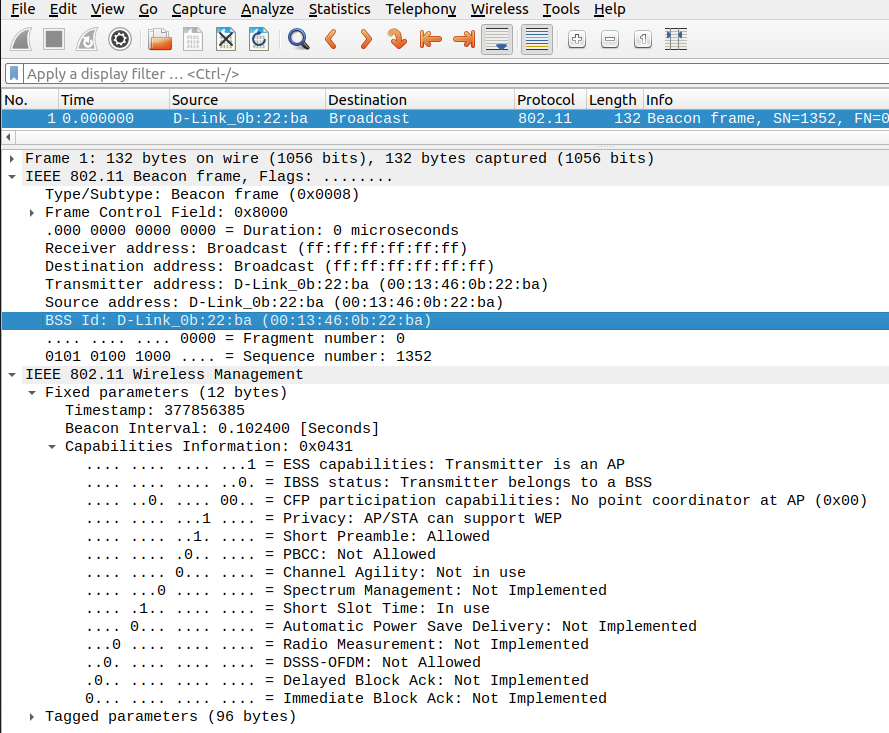


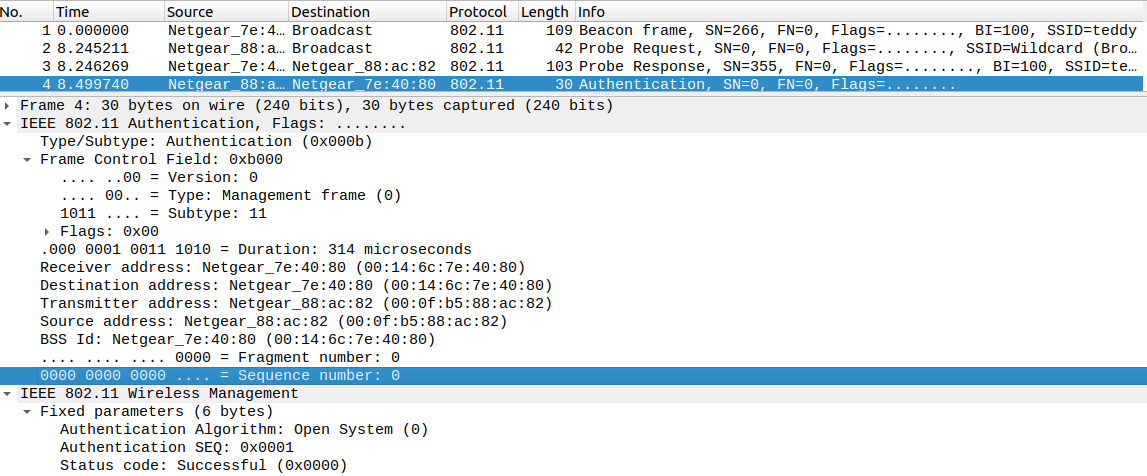
Figure 28: Passive Scanning

### Authentication, Association and Encryption Testing

#### Authentication Testing

It’s a process in which the credentials provided by the client are compared to those on file in a database on a local router or on an authentication server. If the credentials match then process is completed and user is granted authorization for access. It has 2 messages,

##### Authentication Request

 Figure 29: Authentication Request

##### Authentication Response

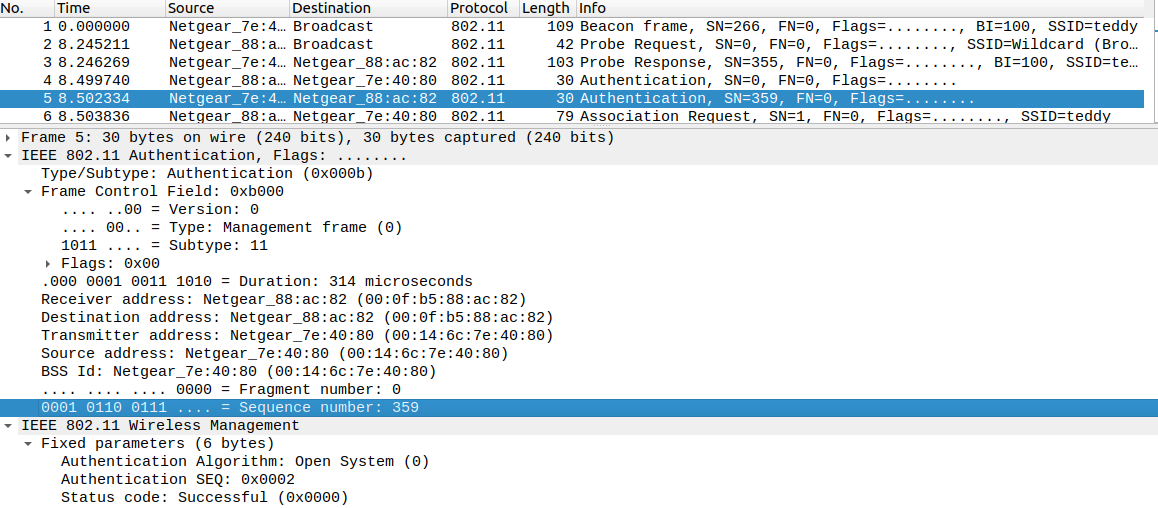
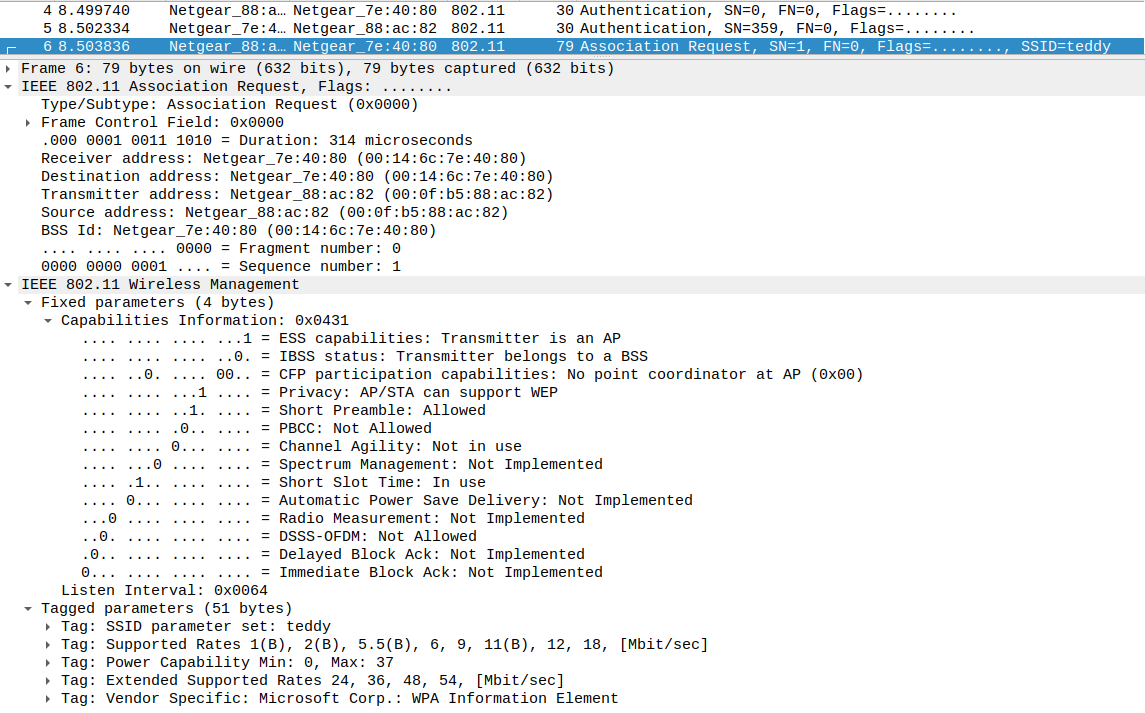


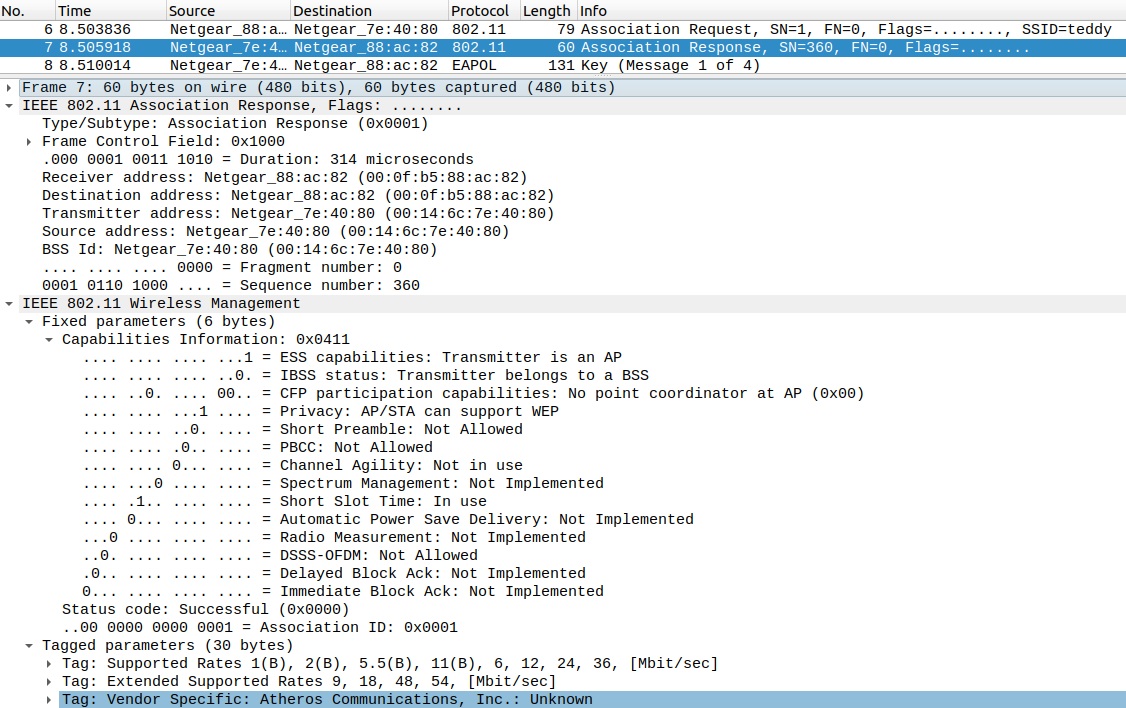
Figure 30: Authentication Response

#### Association Testing

After Successful Authentication frame exchanges, Client unicasts an Association Request Frame Containing its capabilities like Power Capability, Supported rates, Privacy etc. As shown in below figure.



Upon receiving Association request frame, Access Point checks Clients Capabilities and if its satisfactory, then AP responds with an Acknowledgement Frame and transmits an Association Response frame with the result of successful or unsuccessful.

 Fig: Association Response Frame

#### Encryption Testing

Here 4-way handshake is used and it’s the process of exchanging 4 messages between an access point and the client device to generate some encryption keys which can be used to encrypt actual data sent over Wireless medium.

Pairwise Transit Key (PTK) = PRF (PMK+ Anounce + Snounce + Mac (AP) + Mac (client))

PRF= PRF is a pseudo-random function which is applied to all the input.

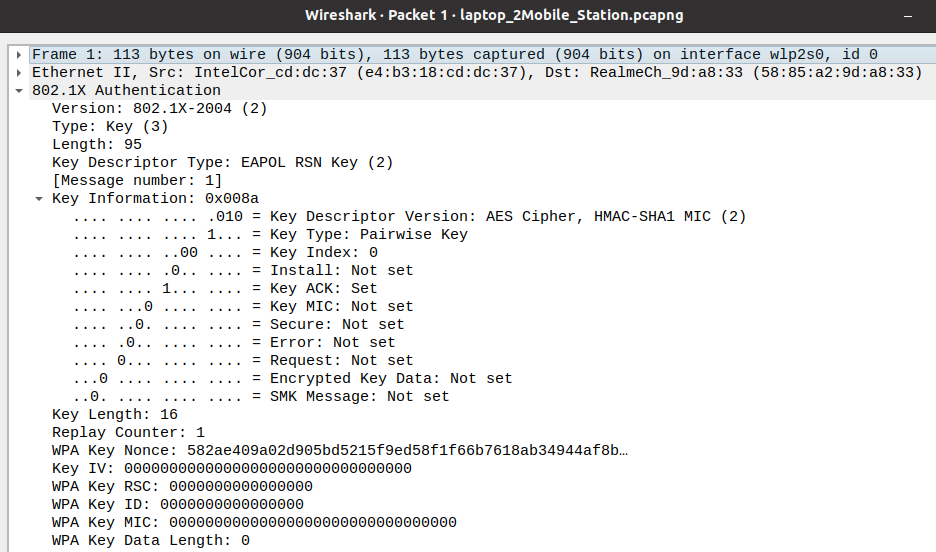
PMK=Pairwise Master Key, is generated from PSK

Announce = Random Number from AP

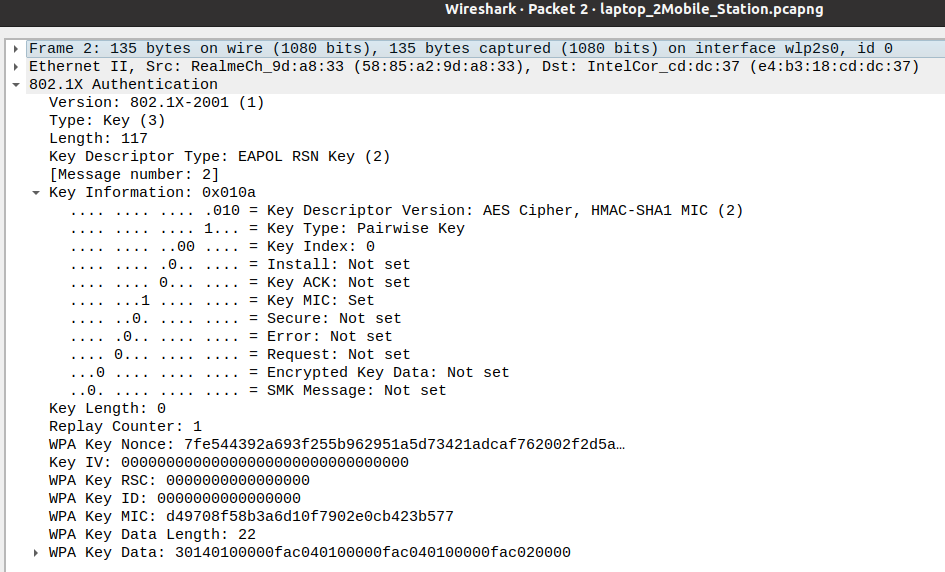
Snounce = Random Number from Client

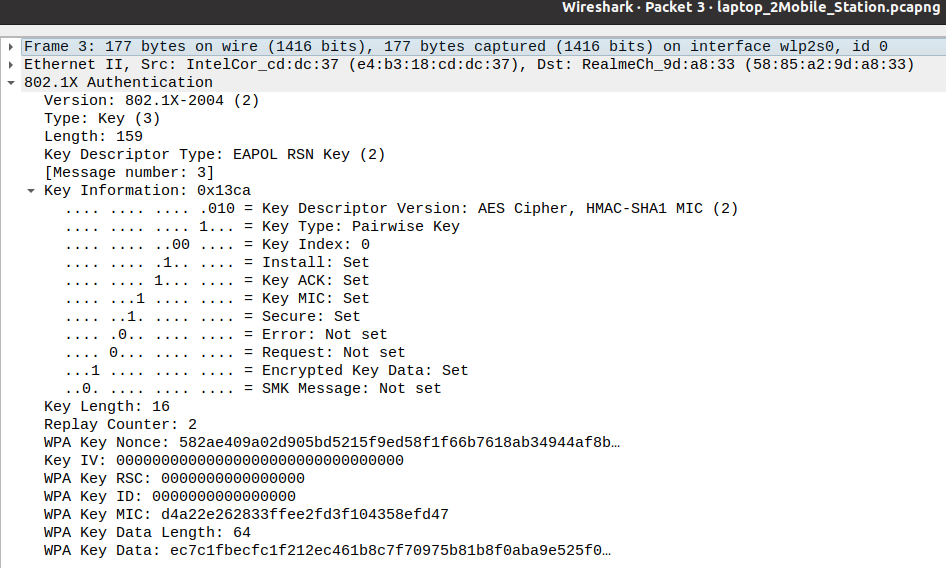
1. Message 1, AP shares it’s Anounce to Client so that Client produces its PTK.
2. Message 2, Client shares its Snounce to AP so that client produces its PTK.
3. Message 3, AP compares with client PTK.
4. Message 4, if PTK is same then client sends an ACK and authentication completes.

Below screenshots shows encryption key generation step by step,

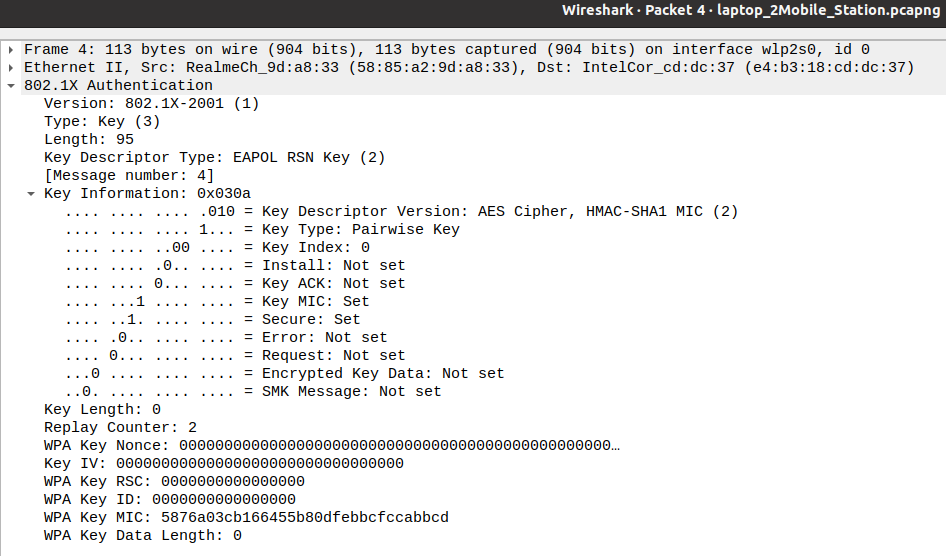
Message 1,

Message 2,



Message 3,

Message 4,



### Client Connectivity Testing

Connectivity Testing involves four major steps. They are as follows:

#### Layer 3 Connectivity: IP addressing(DHCP)

DHCP involves 4 steps,

##### DHCP Discover

Here Client device broadcasts a DHCP Discover message over the Ethernet network to locate all available DHCP servers on the same subnet network.

##### DHCP Offer

After receiving discover message from the client, it broadcasts a DHCP offer message over the ethernet network informing the client that it is available. Message contains info about IP address, subnet mask, default gateway IP address, DNS IP address, IP lease time and DHCP server IP address.

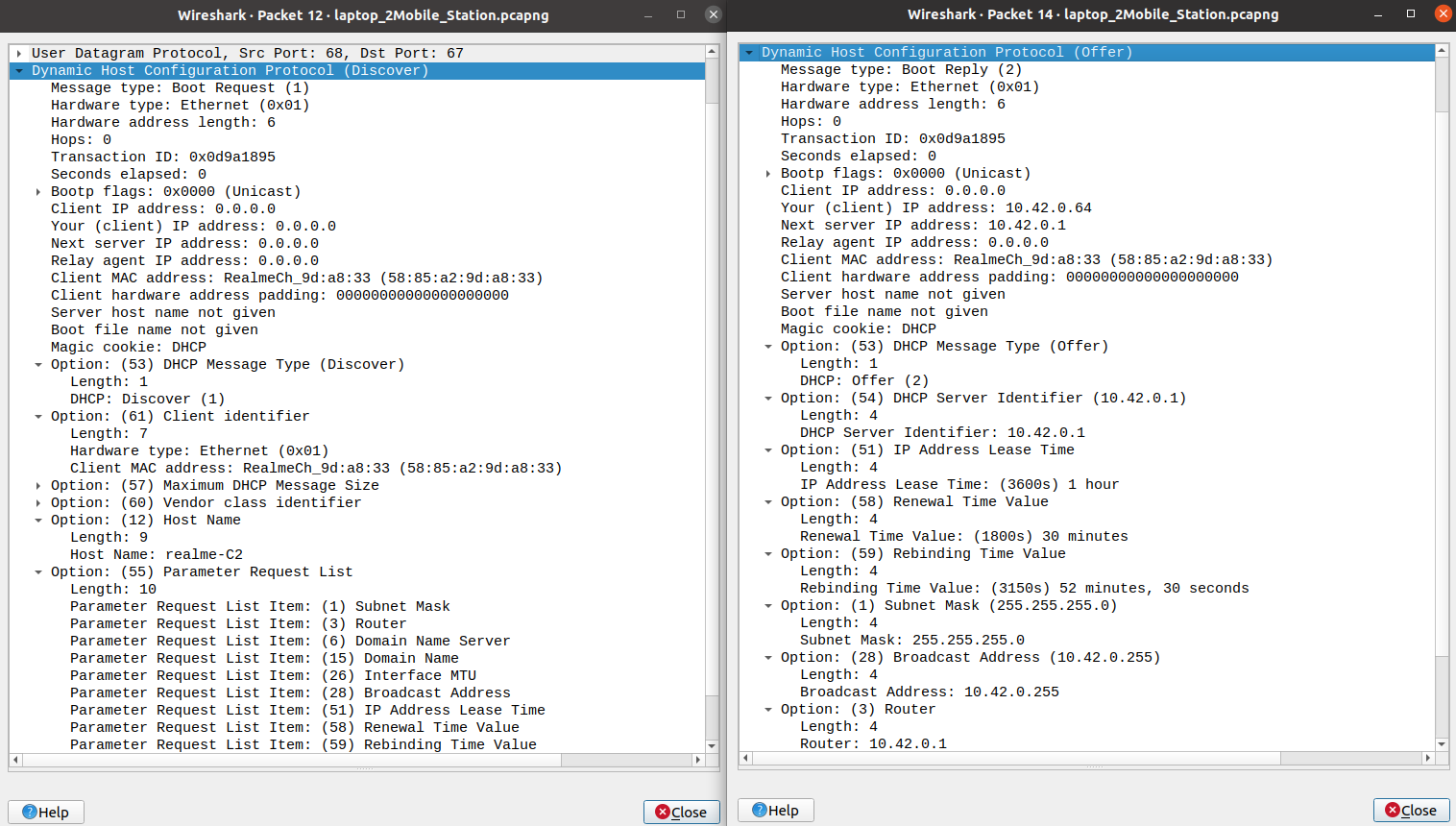


Fig: DHCP Discover and Offer

##### DHCP Request

Here client broadcasts DHCP request message to DHCP server. It requests for the IP address allocation and through the message it notifies other Server about its selection of the DHCP server.

##### DHCP ACK

Here DHCP server broadcasts a DHCP ACK messages ensuring that client can receive the message after checking if the IP address shown in the DHCP Server Identifier field matches its own. Now, the DHCP server transfers all the network configuration data to the client

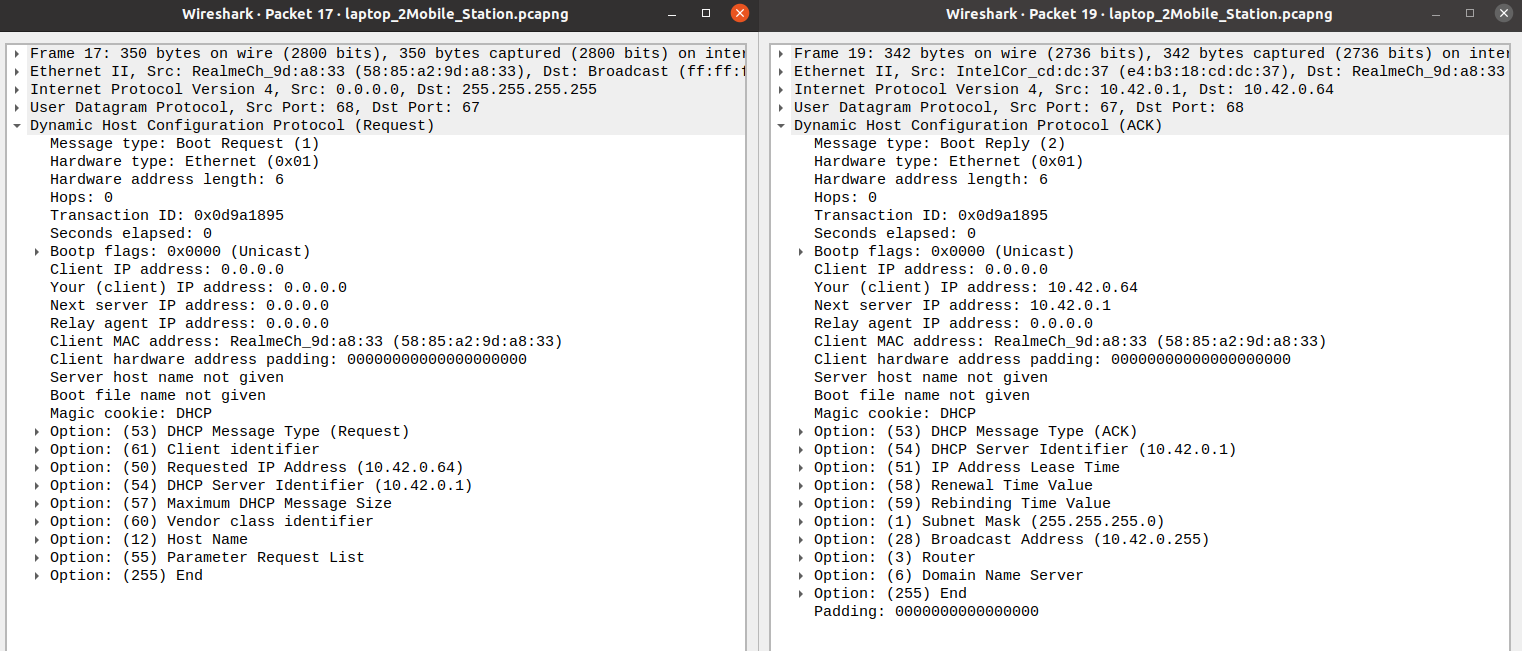


Fig: DHCP Request and ACK

#### Layer 2 Connectivity: MAC address identification (ARP).

This protocol is used for the identification of MAC address. Here using IP address, source broadcasts a message which includes IP address of source and destination and MAC address of the source. This process is called ARP Probe and its broadcasts.

In ARP Response, Destination on identification using IP address, unicasts a message with payload as its own MAC address and destination of source MAC address.

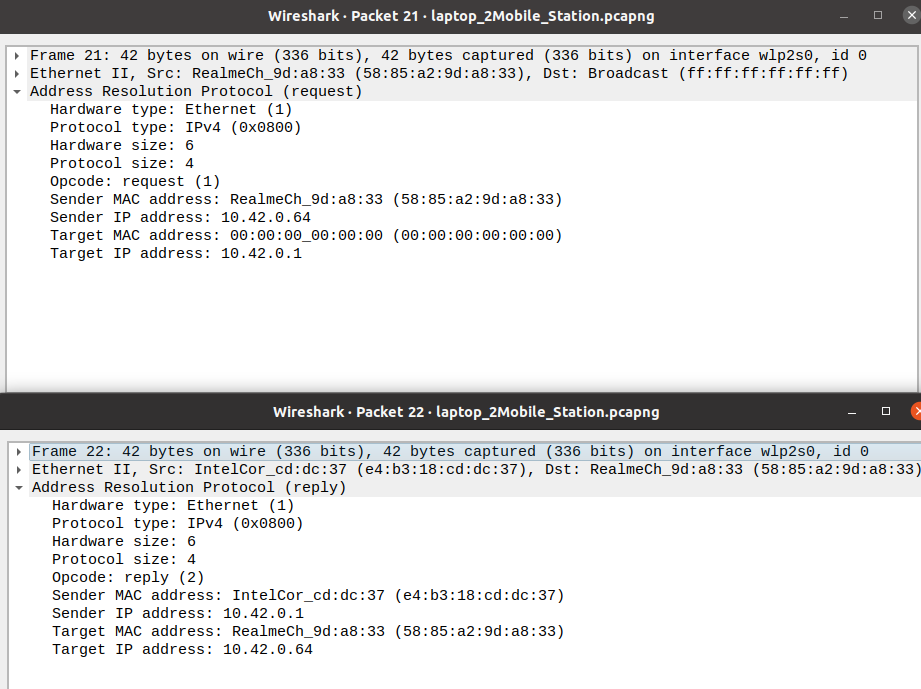
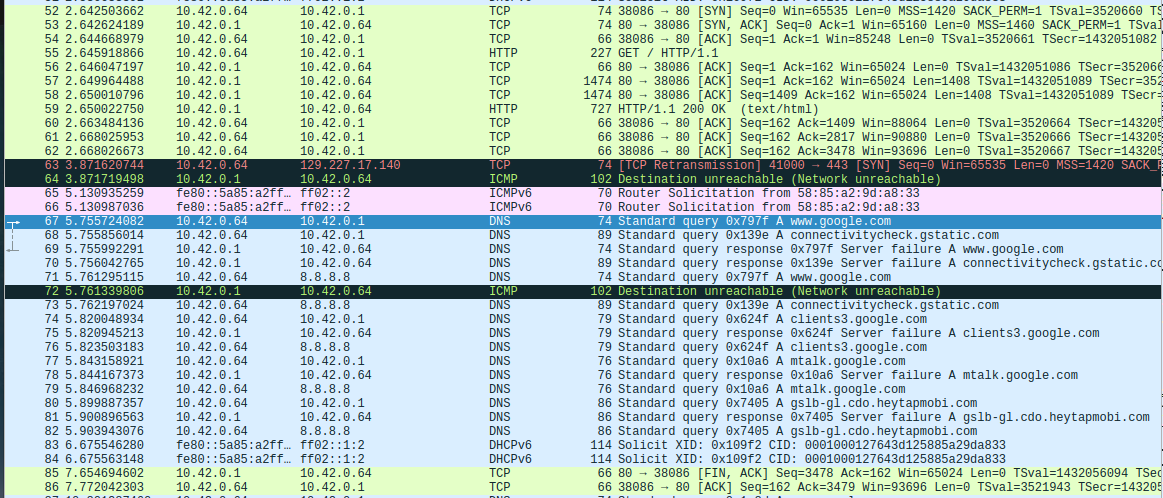


Fig: ARP Testing

#### Layer 4 Connectivity : Three Way Handshake ([SYN] , [SYN, ACK], [ACK])

This 3-way handshake between client and Server is required for the synchronization of their segment sequence numbers used during their transmission. There are 3 steps,

* 1. SYN – Here Client informs the server that it wants to start a communication and what should be its sequence number.
  2. Here server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
  3. ACK – Client acknowledges server’s response.

 Fig: 3 Way handshake

#### Layer 5 Connectivity: GET / HTTP / 1.1

* Here to establish a conversation channel between TCP layer and Application layer, HTTP GET request is sent to retrieve and request for TCP Data.
* On request TCP sends data as per sequence number established during 3-way handshake and final sequence number is initial sequence number + length of data sent.
* After TCP data is sent successfully, HTTP OK is sent to the client. After that acknowledgement of the sent TCP data happens between client and server.
* After successful data transfer, finish flag along with ACK is sent from server to client.

### Signal Testing

Involves Testing of various signal parameters like Antenna Signal strength, Data rate, Modulation format and scheme, spectrum band, channel, GSM, Vendor info for FHSS, Frequency information etc. for signal Analysis.

We have used Monitor Mode to capture Radio information packet and Radio Tap Header Packet.

In our log analysis, values obtained are as shown below,

* Antenna Signal & Signal Strength: -45dBm
* data Rate: 1.0Mb/ps
* Modulation format: DSSS
* Modulation scheme: CCK
* Spectrum band: 2.4 Ghz
* Channel no: 6
* Frequency: 2437MHz
* GSM: N/A
* Vendor: N/A

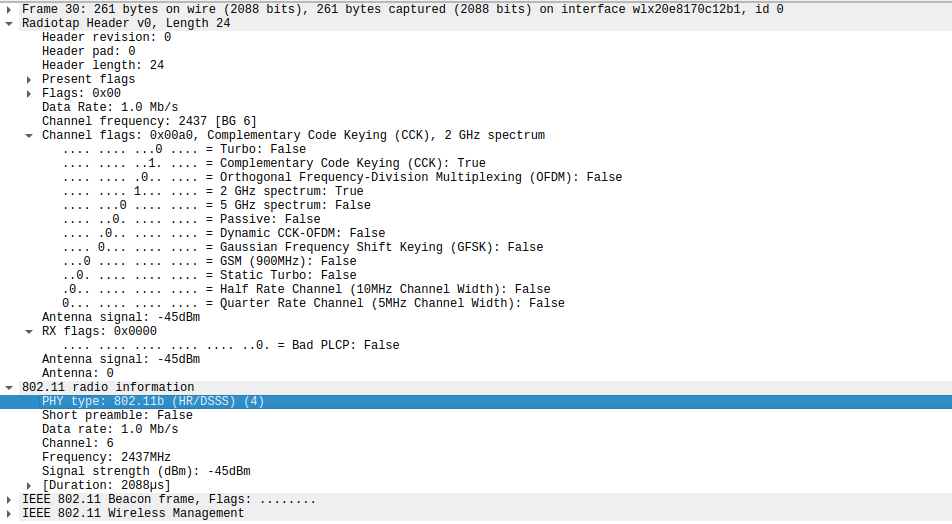


Fig: Signal Testing

### Security Testing

Involves Testing of Security Protocol and ciphers used for respective protocol. In our log analysis WPA2 Security Protocol is used as concluded from AES cipher as shown in the below picture. Currently used Security Protocols are,

## WEP (Wired Equivalent Privacy)

* Earliest Security Protocol.
* It uses stream cipher for RC4 for Confidentiality and CRC – 32 checksums for Integrity.
* Vulnerable to hackers as 40-bit encryption key was not enough.

## WPA (Wi-Fi Protected Access)

* Uses Stronger encryption method called Temporal Key Integrity protocol (TKIP).
* Here Key is dynamically changed.

## WPA2 (Wi-Fi Protected Access 2)

* Provides better security then WPA
* Uses Advanced Encryption Standard (AES) cipher

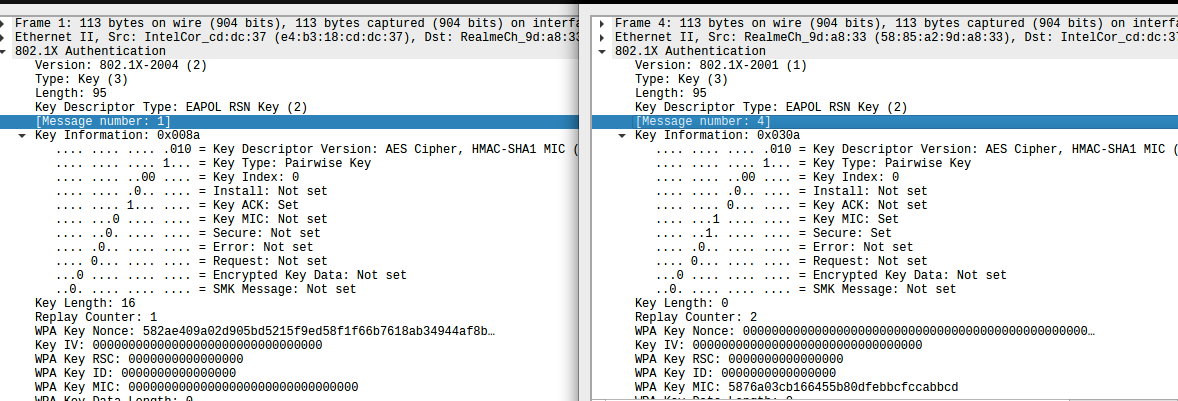


Fig: Security Testing

## Video Summary

Not Applicable

## Git Link

<https://github.com/99002503/Shadow-Project->

## Git Dashboard

Not Applicable

# Git inspector summary

Not Applicable

# Build

Not Applicable

# Code quality and Issues or Bug Tracking

Not Applicable

# Individual Contribution & Highlights

1. Test Plan Preparation.
2. Presentation Preparation for Demo
3. Generation of logs.
4. Authentication Testing.
5. Connectivity Testing.
6. 3 – Way handshake Testing.
7. Testing of communication channel setup between Transport and Application layer.
8. Report Preparation.

# Challenges faced and how were they overcome

1. Spectrum Limitations

Projected is limited to 2.4 GHz of Spectrum.

1. User Mobility

Improper network connection due to non-availability of reliable AP. We had to adjust with Laptop and Mobile hotspot as AP.

1. Wi-Fi Dead Spots

Had tough time in finding Wi-Fi dead spots. Experiments with Site survey helped.

1. Network Security

Had tough time in finding network security logs. We got Network security info in Monitor mode in Wireshark.

1. Lack of Infrastructure

We did not have Enterprise AP. Had tough time to get Wi-Fi adapter and AP.

1. Lack of Training

Lack of proper head-on training delayed our understanding towards problem statement and its requirement.

# Future Scope

1. Wi-Fi 6 (802.11x)
2. Li-Fi (Light fidelity)
3. Use of Multi User MIMO
4. IOT which requires network connectivity will increase demand of Wi-Fi.

# References

1. <https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp>
2. <https://www.wi-fi.org/>
3. <https://www.lifewire.com/>
4. <https://linuxhint.com/>
5. <https://www.vocal.com/>
6. <https://geek-university.com/ccna/>