Contents

[1. Overview 2](#_Toc121865811)

[2. Network Services: - 4](#_Toc121865812)

[3. Fragmentation and reassembly: - 4](#_Toc121865813)

[4. Address fields: - 5](#_Toc121865814)

[5. Generic 802.11 MAC Frame: - 5](#_Toc121865815)

[6. Management frame: - 5](#_Toc121865816)

[6.1 Beacon frame: - 6](#_Toc121865817)

# Overview

There are three types of wireless driver configurations in Linux:

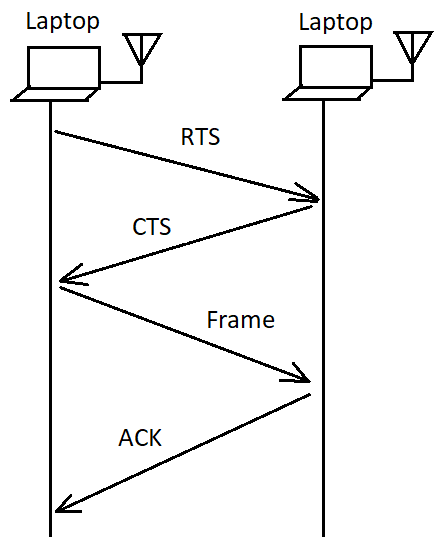
* Cfg80211 — The configuration API for 802.11 devices in Linux. It works together with FullMAC drivers, which also should implement the MAC Sublayer Management Entity (MLME).
* Mac80211 — A subsystem of the Linux kernel that works with soft-MAC/half-MAC wireless devices. MLME is mostly implemented by the kernel, at least for station mode (STA).
* WEXT — Stands for Wireless-Extensions, which is a driver API that was replaced by cfg80211. New drivers should no longer implement WEXT

Note: -

1. In [IEEE](https://en.wikipedia.org/wiki/IEEE) [802.11](https://en.wikipedia.org/wiki/IEEE_802.11) (Wi-Fi) terminology, a station (abbreviated as STA) is a device that has the capability to use the 802.11 protocol.
2. At the heart of 802.11 is a white lie about the meaning of media access control (MAC). Wireless network interface cards are assigned 48-bit MAC addresses, and, for all practical purposes, they look like Ethernet network interface cards. In fact, the MAC address assignment is done from the same address pool so that 802.11 cards have unique addresses even when deployed into a network with wired Ethernet stations.
3. To outside network devices, these MAC addresses appear to be fixed, just as in other IEEE 802 networks; 802.11 MAC addresses go into ARP tables alongside Ethernet addresses, use the same set of vendor prefixes, and are otherwise indistinguishable from Ethernet addresses. The devices that comprise an 802.11 network (access points and other 802.11 devices) know better.
4. IEEE 802 family is a series of specifications for local area network (LAN) technologies.
5. IEEE 802 specifications are focused on the two lowest layers of the OSI model because they incorporate both physical and data link components. All 802 networks have both a MAC and a Physical (PHY) component.
6. 802.11 splits the PHY into two generic components: the Physical Layer Convergence Procedure (PLCP), to map the MAC frames onto the medium, and a Physical Medium Dependent (PMD) system to transmit those frames.
7. BSS: -

The basic building block of an 802.11 network is the basic service set (BSS), which is simply a group of stations that communicate with each other.

1. Stations are identified by 48bit IEEE 802 MAC addresses.
2. IEEE 802.11 uses CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance).
3. To prevent collisions, 802.11 allows stations to use Request to Send (RTS) and Clear to Send (CTS) signals to clear out an area.



# Network Services: -

802.11 provides nine services. Only three of the services are used for moving data; the remaining six are management operations that allow the network to keep track of the mobile nodes and deliver frames accordingly.

Table

Description automatically generated



# Fragmentation and reassembly: -

Higher-level packets and some large management frames may need to be broken into smaller pieces to fit through the wireless channel.

Fragments all have the same frame sequence number but have ascending fragment numbers to aid in reassembly.

Frame control information also indicates whether more fragments are coming. All the fragments that comprise a frame are normally sent in a fragmentation burst, as shown in figure below.

The figure also shows how the NAV and SIFS are used in combination to control access to the medium.

Diagram

Description automatically generated

# Address fields: -

An 802.11 frame may contain up to four address fields. The address fields are numbered because different fields are used for different purposes depending on the frame type. The general rule of thumb is that Address 1 is used for the receiver, address 2 for the transmitter, with the Address 3 field used for filtering by the receiver.

Addresses are 48 bits long. If the first bit sent to the physical medium is a 0, the address represents a single station (unicast). When the first bit is a 1, the address represents a group of physical stations and is called a multicast address. If all bits are 1s, then the frame is a broadcast and is delivered to all stations connected to the wireless medium.

# Generic 802.11 MAC Frame: -

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Frame Control | Duration/  ID | Address 1 | Address 2 | Address  3 | Seq  Ctrl | Address  4 | Frame Body | FCS |

2 2 6 6 6 2 6 0-2312 4

# Management frame: -

Broadcast and multicast frames have the simplest frame exchanges because there is no acknowledgment. Framing and addressing are somewhat more complex in 802.11, so the types of frames that match this rule are the following:

* Broadcast data frames with a broadcast address in the Address1 field
* Multicast data frames with a multicast address in the Address1 field
* Broadcast management frames with a broadcast address in the Address1 field (Beacon, Probe Request, and IBSS ATIM frames)

Frames destined for group addresses cannot be fragmented and are not acknowledged.

## 6.1 Beacon frame: -

Beacon frame is one of the management frames in [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) based WLANs. It contains all the information about the network. Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronise the members of the service set.

Beacon frames are transmitted by the [access point](https://en.wikipedia.org/wiki/Wireless_access_point) (AP) in an infrastructure [basic service set](https://en.wikipedia.org/wiki/Service_set_(802.11_network)) (BSS). In IBSS network beacon generation is distributed among the stations. For the 2.4 GHz spectrum, when having more than 15 [SSIDs](https://en.wikipedia.org/wiki/SSID) on non-overlapping channels (or more than 45 in total), beacon frames start to consume significant amount of air time and degrade performance even when most of the networks are idle.

# WiFi Chip: -

Reference - <https://www.youtube.com/watch?v=dDMNNDTzjQ0>

Till – 22:46

## Full Mac vs Soft Mac

Primary difference is where upper-level logic resides.

**Full MAC –**

In chips’s firmware. MLME code is in hardware.

**Soft MAC –**

In Linux’s mac80211. MLME code is in software. Soft MAC uses mac80211.

Most chips must load firmware, even soft-MAC chips have firmware. If driver uses below things, then it means our driver is a soft MAC –

ieee80211\_ops

ieee80211\_alloc\_hw

ieee80211\_register\_hw

**cfg80211: -**

All drivers whether full/soft mac uses – cfg80211. It has main configuration APIs. It stands between user space and driver. Scanning, setting a regulatory domain, setting a connection are done by this.

**nl80211: -**

Userspace interface to cfg80211. No more ioctls.

**User space management: -**

* Basic tools like “ip” , “iw”.
* wpa\_supplicant
* Higher level tools like NetworkMangare, Conman etc.

# Linux WIFI stack: -

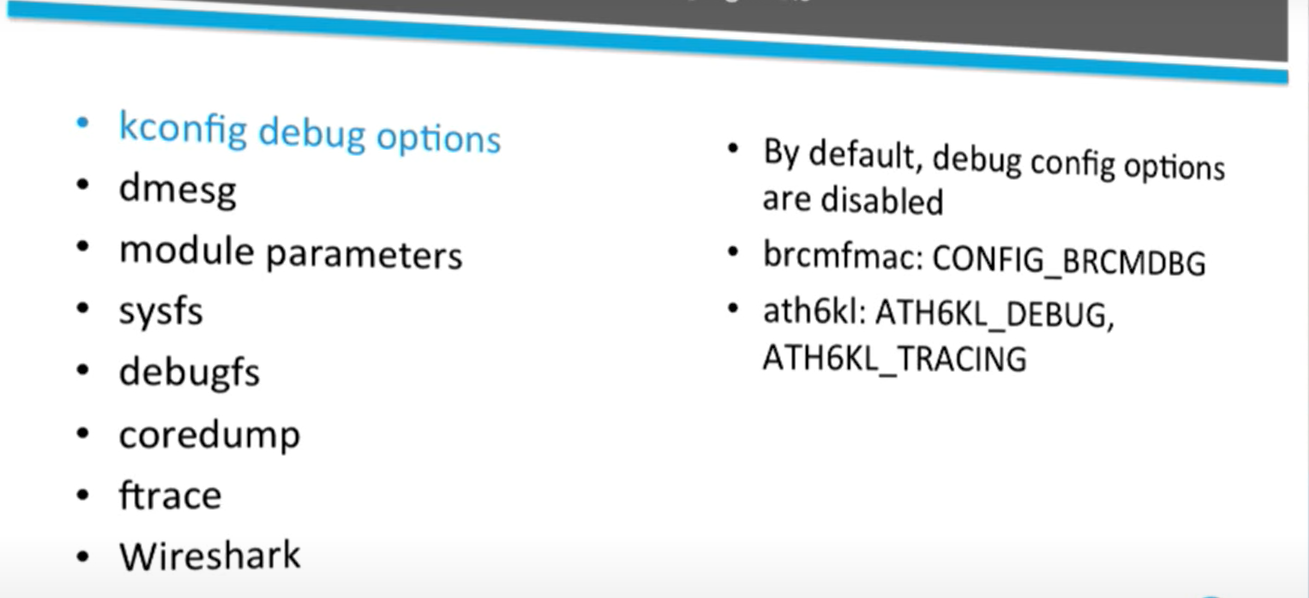
Graphical user interface

Description automatically generated

# WiFi Data: -

In Wifi, there is no difference in data communication side as compared to normal Ethernet. Open UDP or TCP sockets.

# Debugging Tools: -



Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated with low confidence

Graphical user interface, text, application

Description automatically generated

