Opening Nuts and Bolts of Linux WiFi Subsystem

Dheryta Jaisinghani

Why do we need to understand this?

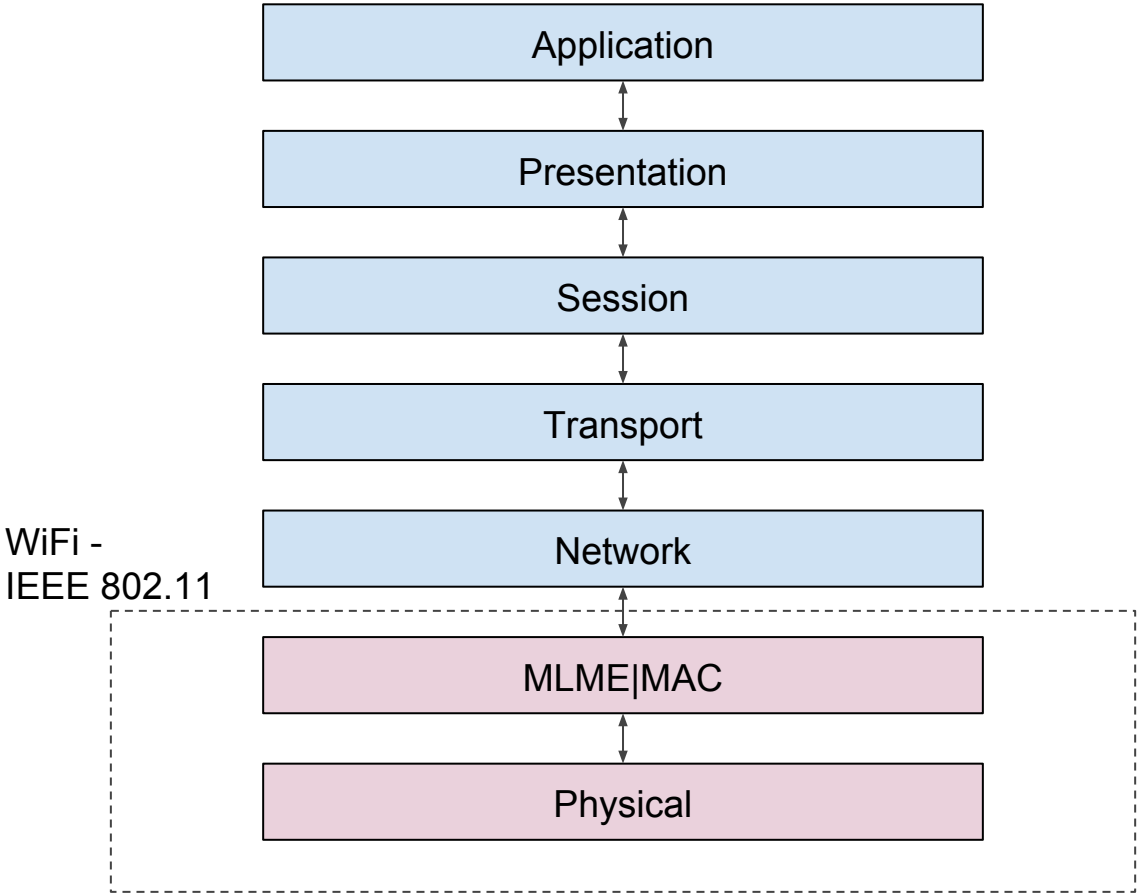
I wonder

- What happens in the background (in the Operating System) when I connect to WiFi?
- How does a packet travels all the way from my application to kernel to air and back?
- How can I modify the code to try my own algorithms?

Structure of this talk

- Linux WiFi Subsystem - Bird’s Eye View
- Types of WiFi drivers
- Working with code - Source, Compilation, Kernel Module Insertion
- Flow of code - where to make changes
- Important commands - events, connection establishment, information on card and modules, logging
- Important pointers - Tutorials

Networking Layers



What does MAC - Medium Access Control do?

- MLME - MAC SubLayer Management Entity
  - Authenticate
  - Deauthenticate
  - Associate
  - Disassociate
  - Reassociate
  - Beacon
  - Probe

Know about your WiFi card

sudo lshw -C network

```
*-network
     description: Wireless interface
     product: AR9462 Wireless Network Adapter
     vendor: Qualcomm Atheros
     physical id: 0
     bus info: pci@0000:0d:00.0
     logical name: wlan0
     version: 01
     serial: 44:6d:57:31:40:6f
     width: 64 bits
     clock: 33MHz
     capabilities: pm msi pciexpress bus_master cap_list rom ethernet physical wireless
     configuration: broadcast=yes driver=ath9k driverversion=3.19.0-25-generic firmware=N/A
wireless=IEEE 802.11abgn
```

iwconfig

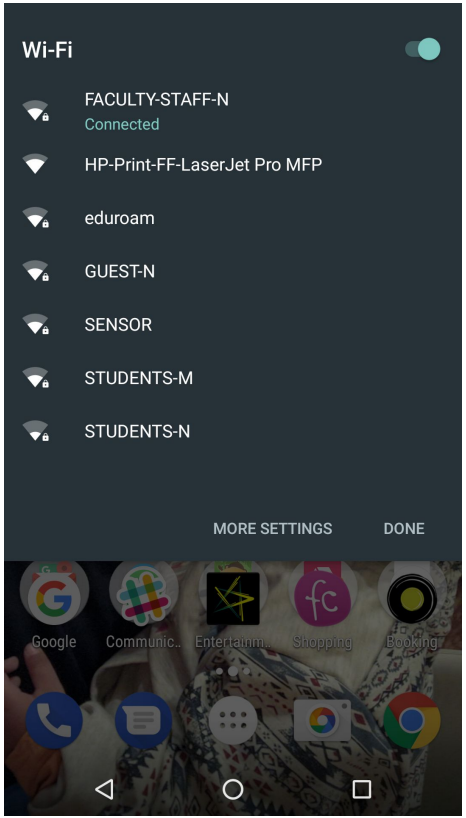
```
wlan0     IEEE 802.11abgn  ESSID:"FACULTY-STAFF-N"
          Mode:Managed  Frequency:2.437 GHz  Access Point: C4:0A:CB:5C:07:05
          Bit Rate=81 Mb/s   Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=41/70  Signal level=-69 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:91   Missed beacon:0
```

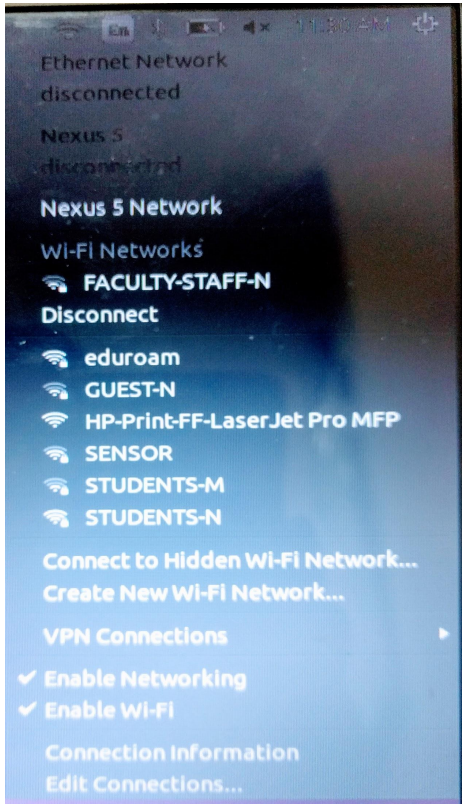
ifconfig

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.[redacted]  netmask 255.255.240.0  broadcast 192.168.[redacted]
        inet6 fe80::466d:57ff:fe31:406f  prefixlen 64  scopeid 0x20<link>
        ether 44:6d:57:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 126046  bytes 41264323 (39.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62148  bytes 24986154 (23.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

WiFi connection in Application Layer?

- WPA_Supplicant
- WICD
- Network Manager
- More ...





Types of WiFi Devices

Full MAC: MAC in hardware

Soft MAC: MAC in software

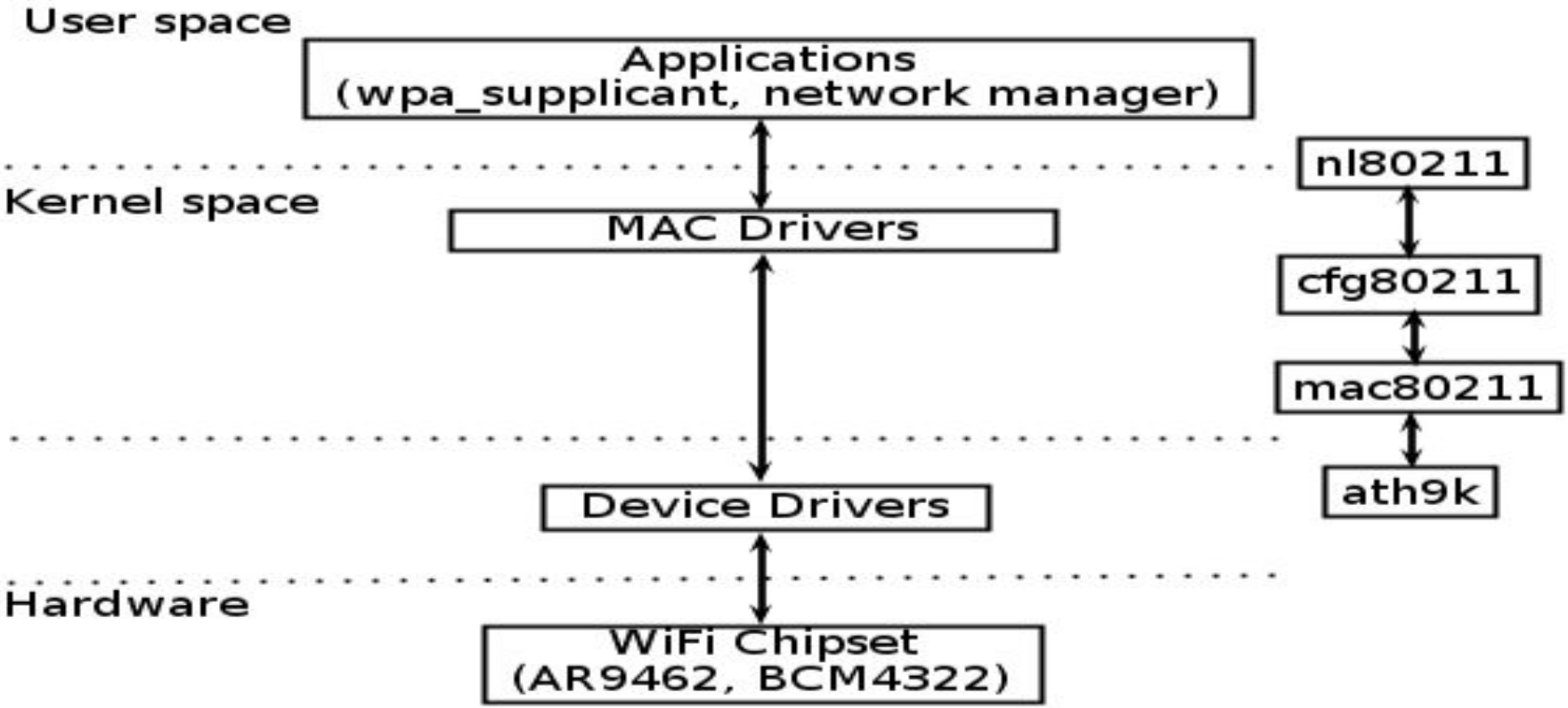
[1] https://wireless.wiki.kernel.org/en/developers/documentation/glossary

WiFi Interface Modes

```
Supported interface modes:
         * IBSS
         * managed
         * AP
         * AP/VLAN
         * WDS
         * monitor
         * mesh point
         * P2P-client
         * P2P-GO
software interface modes (can always be added):
         * AP/VLAN
         * monitor
```

[1] https://wireless.wiki.kernel.org/en/developers/documentation/glossary

Linux WiFi Subsystem - Bird's Eye View



[1] D. Jaisinghani, -, S. Kaul, and S. Roy. Sniffer-based Inference of the Causes of Active Scanning in WiFi Networks. NCC 2017

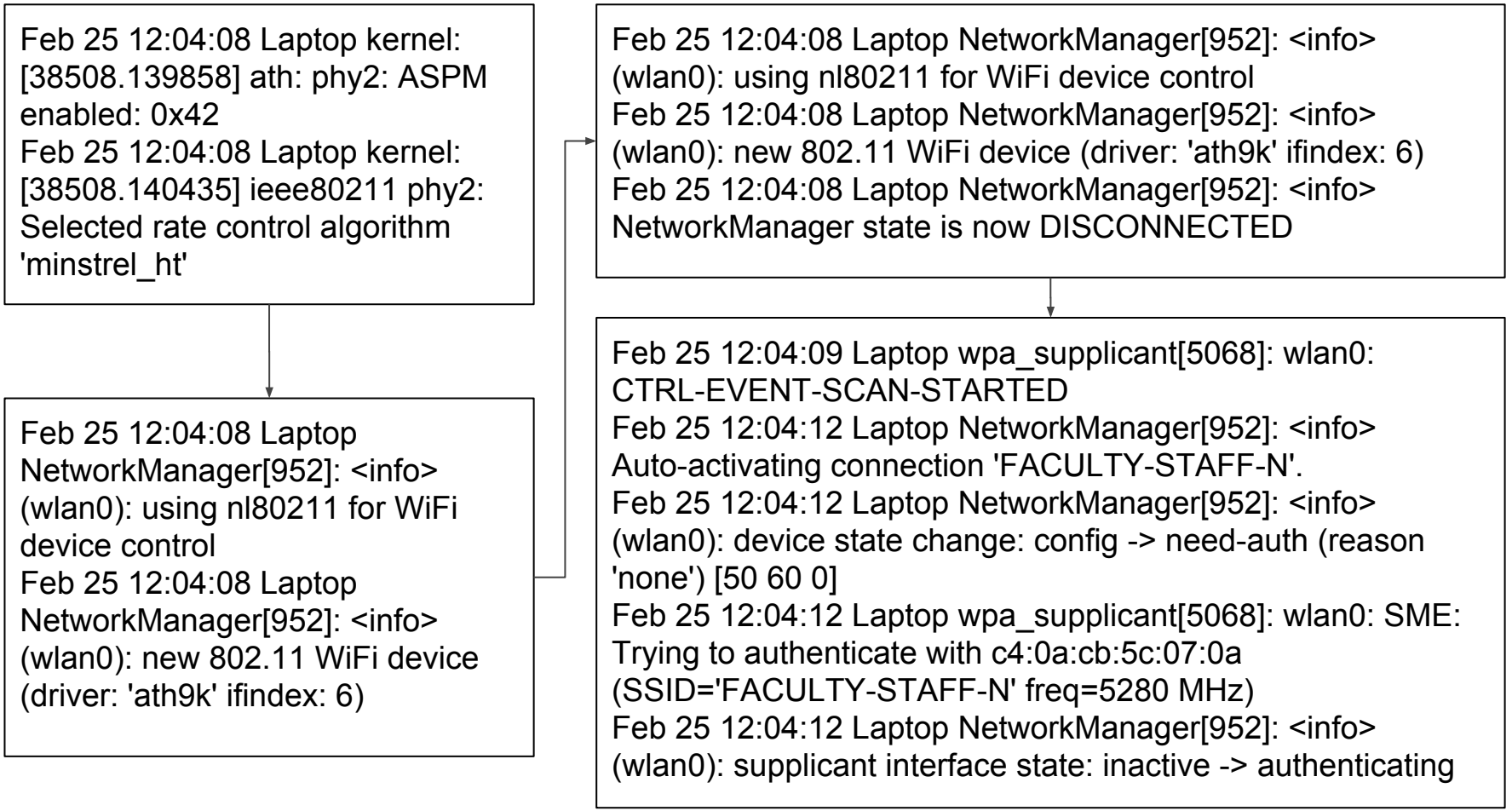
What happens when a WiFi card is plugged in?

- Device drivers load order -
  - cfg80211 -> mac80211 -> ath9k
- LibNL, Wireless Information
  - /usr/include/linux/nl80211.h
  - /proc/net/wireless
  - /proc/net/dev
- Events
  - WiFi connection establishment -
    - Associate
    - Authenticate
  - DHCP
    - Network - IP
- Terminal command - tail -f /var/log/syslog or dmesg (Look for keywords - wpa_supplicant, network manager, kernel, dhclient)

[1] http://moi.vonos.net/linux/wireless-stack/

Live Demonstration

1. Open 2 terminals - terminal 1 and terminal 2
2. In terminal 1 - sudo tail -f /var/log/syslog
3. In terminal 2 - sudo rmmod ath9k
4. Notice the messages in terminal 1
5. In terminal 2 - sudo modprobe ath9k
6. Notice the messages in terminal 2


Feb 25 12:04:08 Laptop kernel: [38508.139858] ath: phy2: ASPM enabled: 0x42
Feb 25 12:04:08 Laptop kernel: [38508.140435] ieee80211 phy2: Selected rate control algorithm 'minstrel_ht'
Feb 25 12:04:08 Laptop NetworkManager[952]: <info> (wlan0): using nl80211 for WiFi device control
Feb 25 12:04:08 Laptop NetworkManager[952]: <info> (wlan0): new 802.11 WiFi device (driver: 'ath9k' ifindex: 6)
Feb 25 12:04:08 Laptop NetworkManager[952]: <info> (wlan0): using nl80211 for WiFi device control
Feb 25 12:04:08 Laptop NetworkManager[952]: <info> (wlan0): new 802.11 WiFi device (driver: 'ath9k' ifindex: 6)
Feb 25 12:04:08 Laptop NetworkManager[952]: <info> NetworkManager state is now DISCONNECTED
Feb 25 12:04:09 Laptop wpa_supplicant[5068]: wlan0: CTRL-EVENT-SCAN-STARTED
Feb 25 12:04:12 Laptop NetworkManager[952]: <info> Auto-activating connection 'FACULTY-STAFF-N'.
Feb 25 12:04:12 Laptop NetworkManager[952]: <info> (wlan0): device state change: config -> need-auth (reason 'none') [50 60 0]
Feb 25 12:04:12 Laptop wpa_supplicant[5068]: wlan0: SME: Trying to authenticate with c4:0a:cb:5c:07:0a (SSID='FACULTY-STAFF-N' freq=5280 MHz)
Feb 25 12:04:12 Laptop NetworkManager[952]: <info> (wlan0): supplicant interface state: inactive -> authenticating

Feb 25 12:04:16 Laptop wpa_supplicant[5068]: wlan0: Trying to associate with c4:0a:cb:5c:07:0a (SSID='FACULTY-STAFF-N' freq=5280 MHz)
Feb 25 12:04:16 Laptop kernel: [38515.397527] wlan0: send auth to c4:0a:cb:5c:07:0a (try 2/3)
Feb 25 12:04:16 Laptop kernel: [38515.398891] wlan0: authenticated
Feb 25 12:04:16 Laptop kernel: [38515.401031] wlan0: associate with c4:0a:cb:5c:07:0a (try 1/3)
Feb 25 12:04:16 Laptop kernel: [38515.402612] wlan0: RX AssocResp from c4:0a:cb:5c:07:0a (capab=0x11 status=0 aid=2)
Feb 25 12:04:16 Laptop kernel: [38515.402686] wlan0: associated

Feb 25 12:04:16 Laptop NetworkManager[952]: <info> (wlan0): device state change: config -> ip-config (reason 'none') [50 70 0]
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> Activation (wlan0) Beginning DHCPv4 transaction (timeout in 45 seconds)
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> dhclient started with pid 6172

Feb 25 12:04:16 Laptop NetworkManager[952]: <info> address 192.168.X.X
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> prefix 20 (255.255.240.0)
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> gateway 192.168.X.X
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> nameserver '192.168.X.X'
Feb 25 12:04:16 Laptop NetworkManager[952]: <info> domain name 'iiitd.edu.in'

watch -n1 "cat /proc/net/wireless"

```
Every 1.0s: cat /proc/net/wireless

Inter-| sta-|   Quality        |   Discarded packets               | Missed | WE
 face | tus | link level noise |  nwid  crypt   frag  retry   misc | beacon | 22
 wlan0: 0000   41.  -69.  -256        0      0      0      0     45        0
```

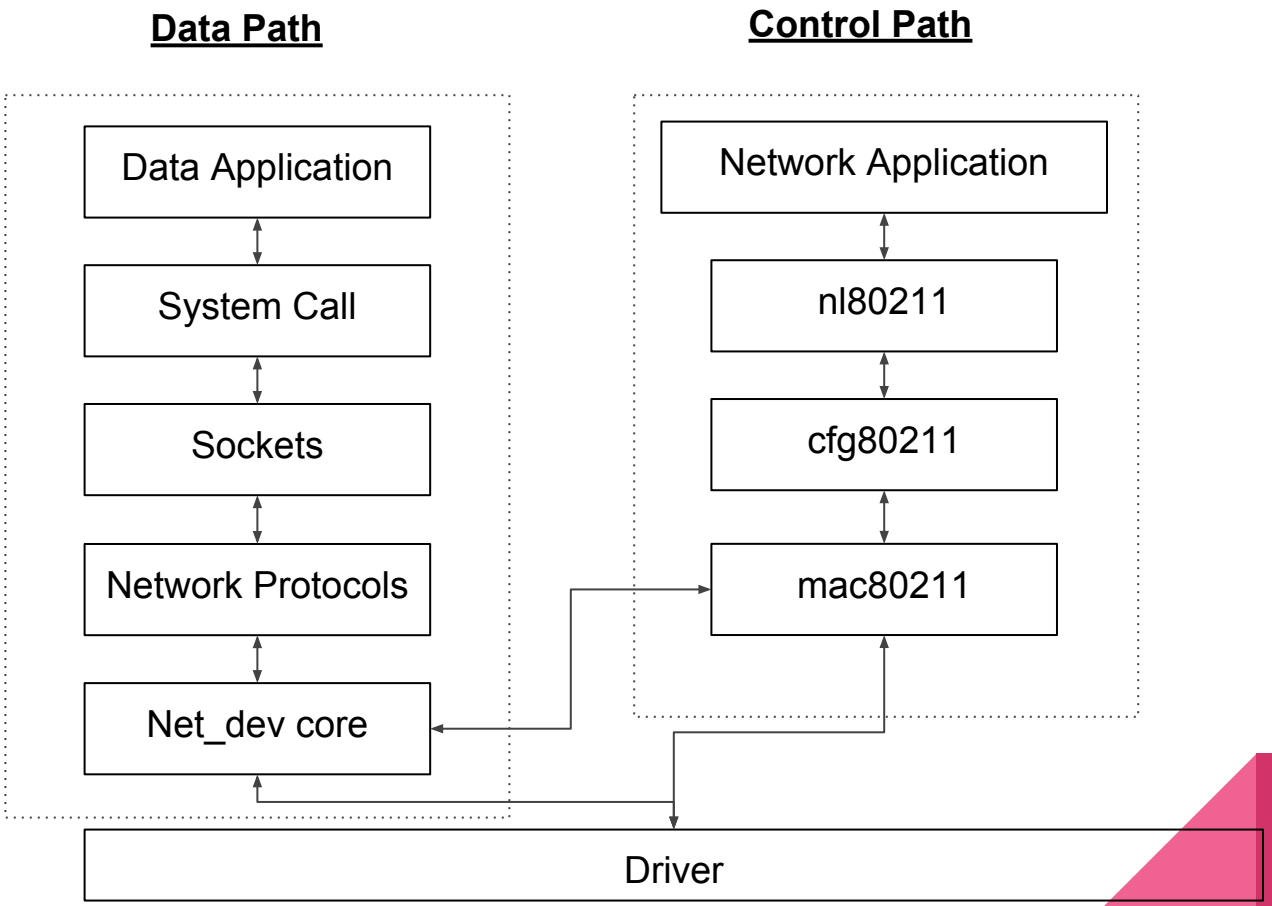
watch -n1 "cat /proc/net/dev"

```
Every 1.0s: cat /proc/net/dev                                        Sat Feb 25 14:30:54 2017

Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes    packets errs drop fifo colls carrier compressed
  eth0:       0       0    0    0    0     0          0         0        0       0    0    0    0     0       0          0
 wlan0: 3643071   11956    0    0    0     0          0         0  3009045    6568    0    0    0     0       0          0
    lo: 46094645  421635    0    0    0     0          0         0 46094645  421635    0    0    0     0       0          0
lxcbr0:       0       0    0    0    0     0          0         0    12551      92    0    0    0     0       0          0
```

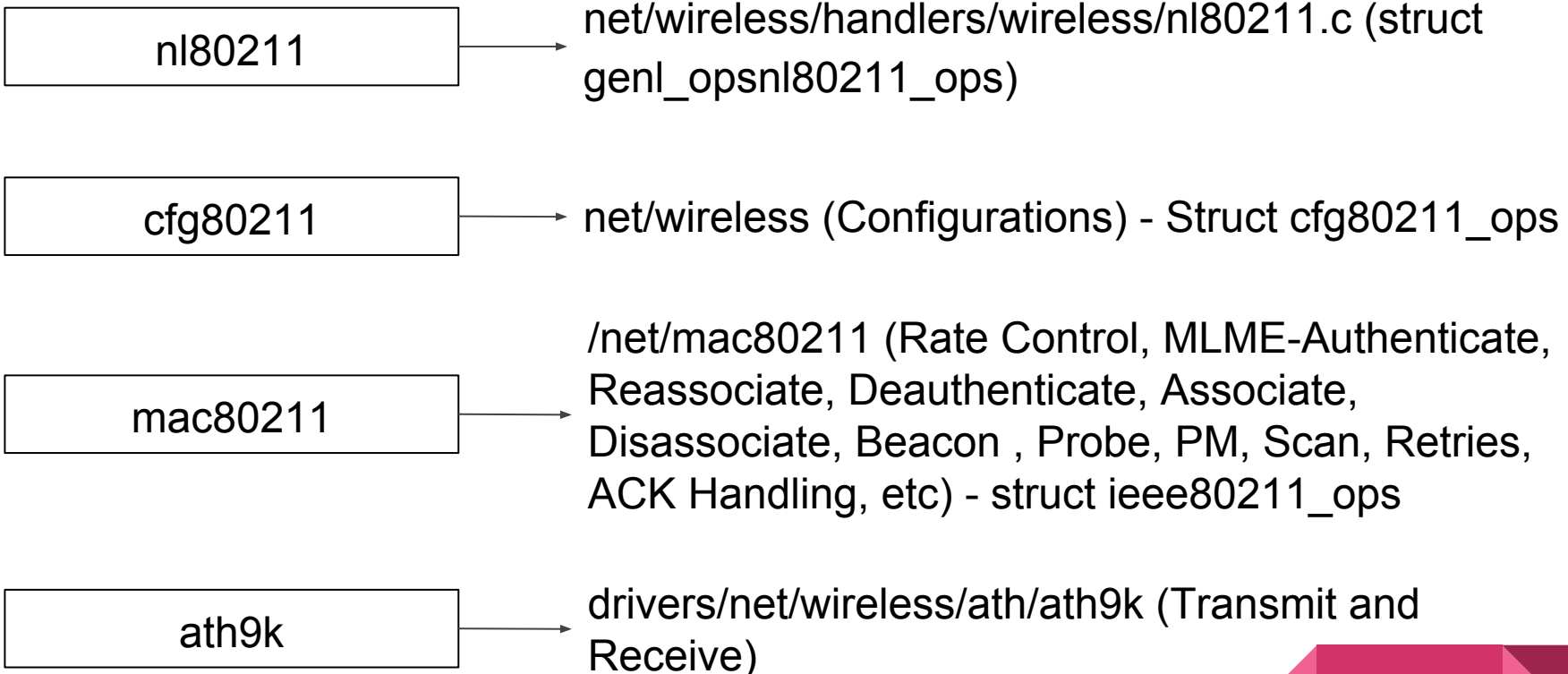
Flow of Packets in an Operating System

- Data vs Control Path
- Transmit vs Receive Path



[1] https://www.linux.com/blog/linux-wireless-networking-short-walk

Backports Code Structure


nl80211
net/wireless/handlers/wireless/nl80211.c (struct genl_opsnl80211_ops)
cfg80211
net/wireless (Configurations) - Struct cfg80211_ops
mac80211
/net/mac80211 (Rate Control, MLME-Authenticate, Reassociate, Deauthenticate, Associate, Disassociate, Beacon , Probe, PM, Scan, Retries, ACK Handling, etc) - struct ieee80211_ops
ath9k
drivers/net/wireless/ath/ath9k (Transmit and Receive)

How is a Packet Received?

Main.c: Interrupt from hardware to ath9k: irqreturn_t ath_isr

Recv.c : ath_rx_tasklet ()

rx.c : ieee80211_rx () ->

ieee80211_prepare_and_rx_handle() ->

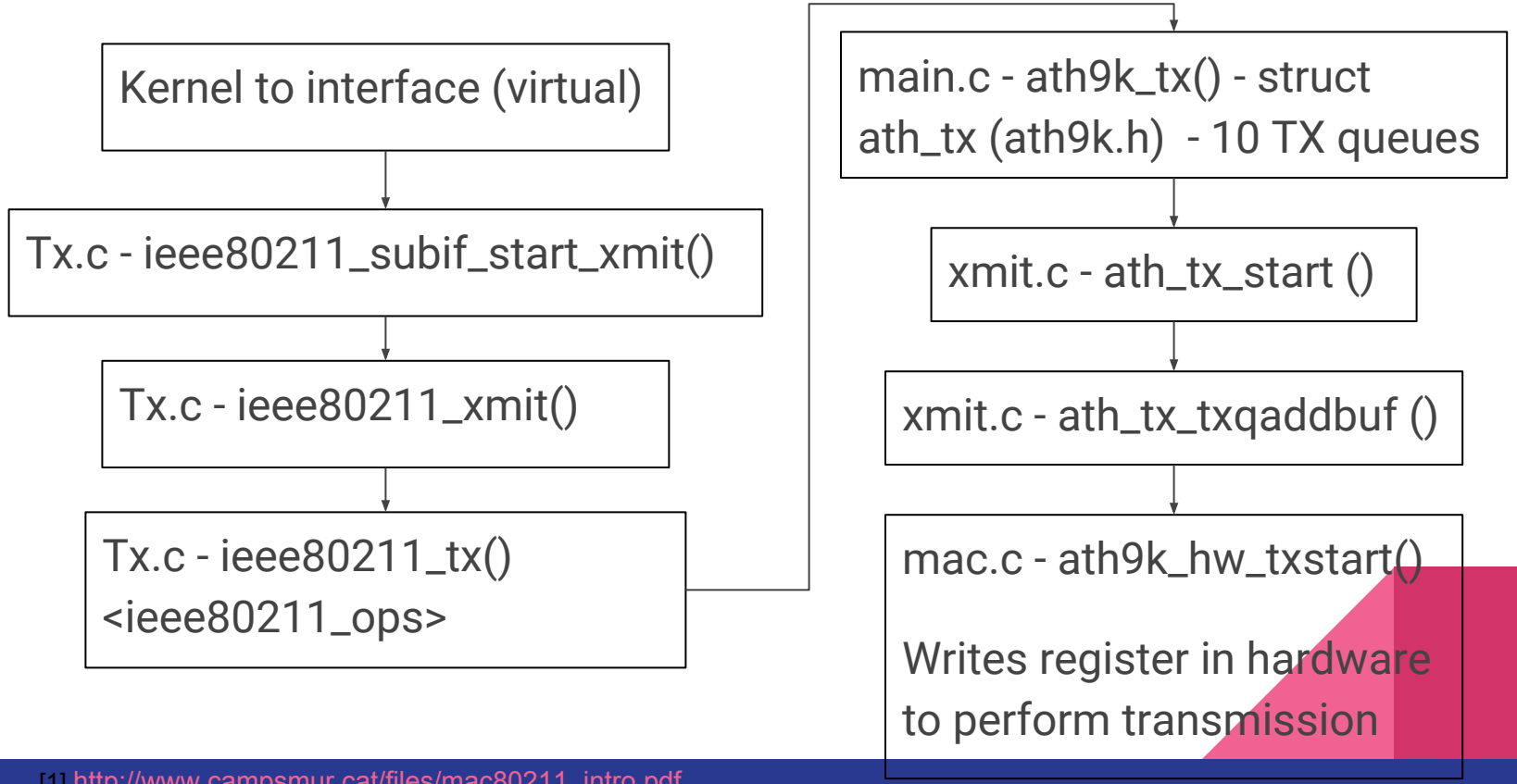
ieee80211_rx_handlers() ->

ieee80211_deliver_skb() - go up or down to air ->

- netif_receive_skb() (rx.c) - up
- dev_queue_xmit() - send to air

[1] http://www.campsmur.cat/files/mac80211_intro.pdf

How is a packet transmitted?



[1] http://www.campsmur.cat/files/mac80211_intro.pdf

Debugging Options

Debug Ath9k

1. sudo make menuconfig - Enable debug options as specified in the above mentioned link
2. sudo make
3. sudo make install with flags
4. modprobe ath9k debug=0x00000200 (or) modprobe ath9k_htc debug=0x00000200
5. ATH_DBG_ANY = 0xffffffff
6. tail -f /var/log/syslog

Debug mac80211/cfg80211

1. sudo modprobe mac80211 debug=0xffffffff
2. sudo trace-cmd record -e mac80211
3. trace-cmd report -i trace.dat | grep scan

Live Demonstration

sudo watch -n1 “cat /sys/kernel/debug/ieee80211/phy4/ath9k/recv”

```
Every 1.0s: cat recv

          PKTS-ALL :      25356
         BYTES-ALL :    6677243
           BEACONS :       6518
             FRAGS :          1
          SPECTRAL :          0
           CRC ERR :       1018
   DECRYPT CRC ERR :          0
           PHY ERR :          0
           MIC ERR :          0
 PRE-DELIM CRC ERR :          0
POST-DELIM CRC ERR :      10801
  DECRYPT BUSY ERR :          0
        LENGTH-ERR :          0
           OOM-ERR :          0
          RATE-ERR :          0
    TOO-MANY-FRAGS :          0
```

sudo watch -n1 “cat /sys/kernel/debug/ieee80211/phy4/ath9k/xmit”

```
Every 1.0s: cat xmit

                          BE         BK         VI         VO

MPDUs Queued:              0          0          0        565
MPDUs Completed:           4          0          0        617
MPDUs XRetried:            0          0          0          0
Aggregates:              117          0          0          0
AMPDUs Queued HW:          0          0          0          0
AMPDUs Queued SW:       6926          0          0         52
AMPDUs Completed:       6922          0          0          0
AMPDUs Retried:            5          0          0          0
AMPDUs XRetried:           0          0          0          0
TXERR Filtered:            0          0          0          0
FIFO Underrun:             0          0          0          0
TXOP Exceeded:             0          0          0          0
TXTIMER Expiry:            0          0          0          0
DESC CFG Error:            0          0          0          0
DATA Underrun:             0          0          0          0
DELIM Underrun:            0          0          0          0
TX-Pkts-All:            6926          0          0        617
TX-Bytes-All:        3175453          0          0      24249
HW-put-tx-buf:          6636          0          0        617
HW-tx-start:               0          0          0          0
HW-tx-proc-desc:        6636          0          0        616
TX-Failed:                 0          0          0          0
```

Important and Useful Commands

- Wireless Events (scan, authentication etc) - sudo iw event -t
- Connection Stats (inactive time, rx/tx bytes/packets, signal, bitrate etc) - sudo iw dev wlan0 station dump
- Regular Monitoring - watch -n1 “<command>”
- lshw -C network, lsusb, lspci
- Debug Messages - tail -f /var/log/syslog, dmesg

Important URLs

- All about Wireless Kernel: https://wireless.wiki.kernel.org/en/users
- Tracing the code paths: http://blog.cerowrt.org/post/wifi_software_paths/
- Networking Stack Programming: http://www.geeksofpune.in/files/GEEP-NetworkingStack-28may14.pdf
- Download backports:
  - https://backports.wiki.kernel.org/index.php/Main_Page
  - http://drvbp1.linux-foundation.org/~mcgrof/rel-html/backports/
- Debugging backports: https://wireless.wiki.kernel.org/en/users/drivers/ath9k/debug

Questions?

- Webpage: www.dheryta.co.in
- E-Mail: dherytaj@iiitd.ac.in

Abstract

Title: Opening Nuts and Bolts of Linux WiFi Subsystem

While we understand the complex interplay of OSI layers, in theory, in practice understanding their implementation is a non-trivial task. The implementation details that enables a network interface card to communicate with its peers are oblivious to the end-users. Naive developers such as undergraduate and graduate students often find it hard to find relevant tutorials that enable them to understand these implementation details.

The aim of this talk is to provide an overview of WiFi Subsystem implemented in the Linux operating system. Specifically, this talk will explain the sequence of events that occur from application layer till physical layer when a connection is established over WiFi.

After this talk, the audience will understand -- (1) the bird's eye view of Linux WiFi Subsystem, (2) what happens in an operating system when a WiFi card is plugged-in, (3) how is a packet received/transmitted from physical layer to operating system kernel and vice-versa, (4) brief overview of code structure of open-source drivers, and lastly (5) important pointers to kickstart driver code modifications.

Duration: 30-40 minutes Add-ons: Minimal Demonstration