如何在Linux下写无线网卡的驱动

版本：v0.3

How to write wireless network card driver under Linux

Crifan Li

摘要

本文主要介绍了Linux下的无线网络相关的基础知识，从网络到无线网络再到802.11的无线网络，然后再介绍Linux无线网络的框架，最后介绍如何在Linux的框架下编写无线驱动

本文提供多种格式供：

在线阅读	HTML[1]	HTMLs[2]	PDF[3]	CHM[4]	TXT[5]	RTF[6]	WEBHELP[7]
下载（7zip压缩包）	HTML[8]	HTMLs[9]	PDF[10]	CHM[11]	TXT[12]	RTF[13]	WEBHELP[14]

HTML版本的在线地址为：

http://www.crifan.com/files/doc/docbook/linux_wireless/release/html/linux_wireless.html

有任何意见，建议，提交bug等，都欢迎去讨论组发帖讨论：

http://www.crifan.com/bbs/categories/linux_wireless/

修订历史		
修订 0.2	2011-07-02	crl
1. 基本写好了一些名词的解释		
修订 0.3	2012-08-09	crl
1. 通过Docbook发布		

[1] http://www.crifan.com/files/doc/docbook/linux_wireless/release/html/linux_wireless.html
[2] http://www.crifan.com/files/doc/docbook/linux_wireless/release/htmls/index.html
[3] http://www.crifan.com/files/doc/docbook/linux_wireless/release/pdf/linux_wireless.pdf
[4] http://www.crifan.com/files/doc/docbook/linux_wireless/release/chm/linux_wireless.chm
[5] http://www.crifan.com/files/doc/docbook/linux_wireless/release/txt/linux_wireless.txt
[6] http://www.crifan.com/files/doc/docbook/linux_wireless/release/rtf/linux_wireless.rtf
[7] http://www.crifan.com/files/doc/docbook/linux_wireless/release/webhelp/index.html
[8] http://www.crifan.com/files/doc/docbook/linux_wireless/release/html/linux_wireless.html.7z
[9] http://www.crifan.com/files/doc/docbook/linux_wireless/release/htmls/index.html.7z
[10] http://www.crifan.com/files/doc/docbook/linux_wireless/release/pdf/linux_wireless.pdf.7z
[11] http://www.crifan.com/files/doc/docbook/linux_wireless/release/chm/linux_wireless.chm.7z
[12] http://www.crifan.com/files/doc/docbook/linux_wireless/release/txt/linux_wireless.txt.7z
[13] http://www.crifan.com/files/doc/docbook/linux_wireless/release/rtf/linux_wireless.rtf.7z
[14] http://www.crifan.com/files/doc/docbook/linux_wireless/release/webhelp/linux_wireless.webhelp.7z

如何在Linux下写无线网卡的驱动: How to write wireless network card driver under Linux

Crifan Li

版本：v0.3

出版日期 2012-08-09

[15] http://www.crifan.com/files/doc/docbook/soft_dev_basic/release/html/soft_dev_basic.html#cc_by_nc

目录

插图清单

缩略词

常用缩略词如下：

A

AP (AP)	Access Point

B

BPSK (BPSK)	Binary Phase Shift Keying
BSS (BSS)	Basic Service Set

C

CCK (CCK)	Complementary Code Keying
CRC (CRC)	Cyclic Redundancy Check
CRDA (CRDA)	Central Regulatory Domain Agent
CSMA/CA (CSMA/CA)	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD (CSMA/CD)	Carrier Sense Multiple Access with Collision Detection
CTS (CTS)	Clear To Send

D

DCF (DCF)	Distribution Coordination Function
DHCP (DHCP)	Dynamic Host Configuration Protocol
()	
DS (DS)	Distribution System
DSSS (DSSS)	Direct Sequence Spread Spectrum

E

ESS (ESS)	Extended Service Set
ETSI (ETSI)	European Telecommunications Standards Institute

F

FCC (FCC)	Federal Communications Commission (USA)
FDDI (FDDI)	Fiber Distributed Data Interface
FHSS (FHSS)	Frequency Hopping Spread Spectrum

I

IBSS (IBSS)	Independent Basic Service Set 参见BSS.
IEEE (IEEE)	Institute of Electrical and Electronics Engineers
()	
IETF (IETF)	Internet Engineering Task Force
IP (IP)	Internet Protocol
IPSec (IPSec)	Internet Protocol security
ISA (ISA)	Integrated Services Architecture
ISM (ISM)	Industry, Scientific, and Medical
ISO (ISO)	International Organization for Standardization
ITU-T (ITU-T)	International Telecommunication Union-Telecommunication

L

LLC (LLC)	Logical Link Control

M

MAC (MAC)	Media Access Control
MIB (MIB)	Management Information Base
MKK (MKK)	Radio Equipment Inspection and Certification Institute (Japan)

N

NIC (NIC)	Network Interface Card
NOS (NOS)	Network Operating System

O

OSI (OSI)	Open System Interconnection

P

PCF (PCF)	Point Coordination Function
PCI (PCI)	Peripheral Component Interconnect
PRNG (PRNG)	Pseudo Random Number Generator

Q

QPSK (QPSK)	Quadrature Phase Shift Keying

R

RC4 (RC4)	Rivest Cipher 4
RTS (RTS)	Request to Send

S

SNMP (SNMP)	Simple Network Management Protocol

T

TCP/IP (TCP/IP)	Transmission Control Protocol/Internet Protocol

W

WECA (WECA)	Wireless Ethernet Compatibility Alliance
WEP (WEP)	Wired Equivalent Privacy
Wext (Wext)	Wireless Extension
WLAN (WLAN)	Wireless Local Area Network
WLANA (WLANA)	Wireless LAN Alliance

正文之前

1. 目的

1. 搞懂如何写Linux无线网卡的驱动
2. 记录所学知识。把自己搞懂的东西，能写到让别人也能理解的程度，因为这样才是真正理解了。另外现在理解了，以后还是会忘，而好记性不如烂笔头，万一哪天再需要用到这些知识，也方便查看和温习。
3. 无线网络相关基础知识介绍：此贴不仅仅是要搞懂如何写Linux无线网卡驱动，因为在写驱动之前，肯定也要了解对应的无线网络基础知识，所以此贴也可以用作学习无线网络基础知识之用。

当然，写无线网卡驱动之前，肯定是不仅有了对应的硬件，也还要有无线网卡的datasheet（数据手册）。

再当然，写代码之前，肯定也要搞清楚Linux无线网络驱动的整体架构，

2. 前提

1. 有一定的网络基础知识。
2. 对Linux系统的驱动的基本架构有一定了解
3. 最好有写过其他Linux驱动的经验，这样对于文中所述内容，会有更好的了解

3. 声明

1. 鉴于书写和理解的方便，文中对于常见的缩写，就不一定全部都写中文了。而且表述内容的时候，有可能会出现中英文混杂，而且暂定一些内容，尽量用英文的术语，个人觉得这样有时候更容易把问题说的更透彻。
2. 由于笔者知识有限，错误在所难免，欢迎指正错误和切磋。
3. 任何人可以任意拷贝转载此文，但请注明出处。即版权所有，但欢迎传播。

4. 本文内容组织的逻辑

对于本文的组织内容的逻辑，简单解释一下。

此处，首先要搞懂我们的目的/目标是，好像听到旁边有人喊“没有蛀牙！”恭喜这位同学，你都抢答了！只可惜答案不对，囧。此文目的前面已经说了，就是想要搞懂如何去实现Linux下对应的无线网卡驱动。

而实现驱动之前，肯定至少要知道两件事情：

- 一是硬件上，有哪些东西，他们是如何放置的。
- 二是软件上，通信协议上，是如何实现通信的。

而对于硬件，无线网卡，就要知道其相关的基本名词，基本工作原理等等，对应的还有无线网络的知识。

而无线网络，是在有线网络之后才出现的，很多技术规范和设计等，也是参照和兼容有线网络而设计的，两者关系很紧密，所以也要知道有线网卡的一些知识。

最后，当然有线网络和无线网络，都属于网络，所以对于所涉及到的网络的基础知识，也要清楚。

正因此，才按照：

硬件：网络 + 有线网络 ⇒ 无线网络 ⇒ 80211无线网络

这样的顺序来介绍的。

而对于软件方面，无线网络驱动，是80211架构下的，而80211无线网络架构，也还是基于Linux的网络架构上的，所以要按照：

软件：Linux网络架构 ⇒ Linux下的80211 无线网络架构

来介绍的。

这样，将相关的硬件和软件的知识都介绍完了，也才能搞懂后面要介绍的，有哪些硬件，对应软件是如何工作的。

其中软件部分，知道Linux无线网络架构本身已经实现了哪些功能，剩下的部分，就是你要实现的驱动的细节部分，这样硬件和软件全部协同工作，才能让无线网卡正常工作。

第 1 章 Network

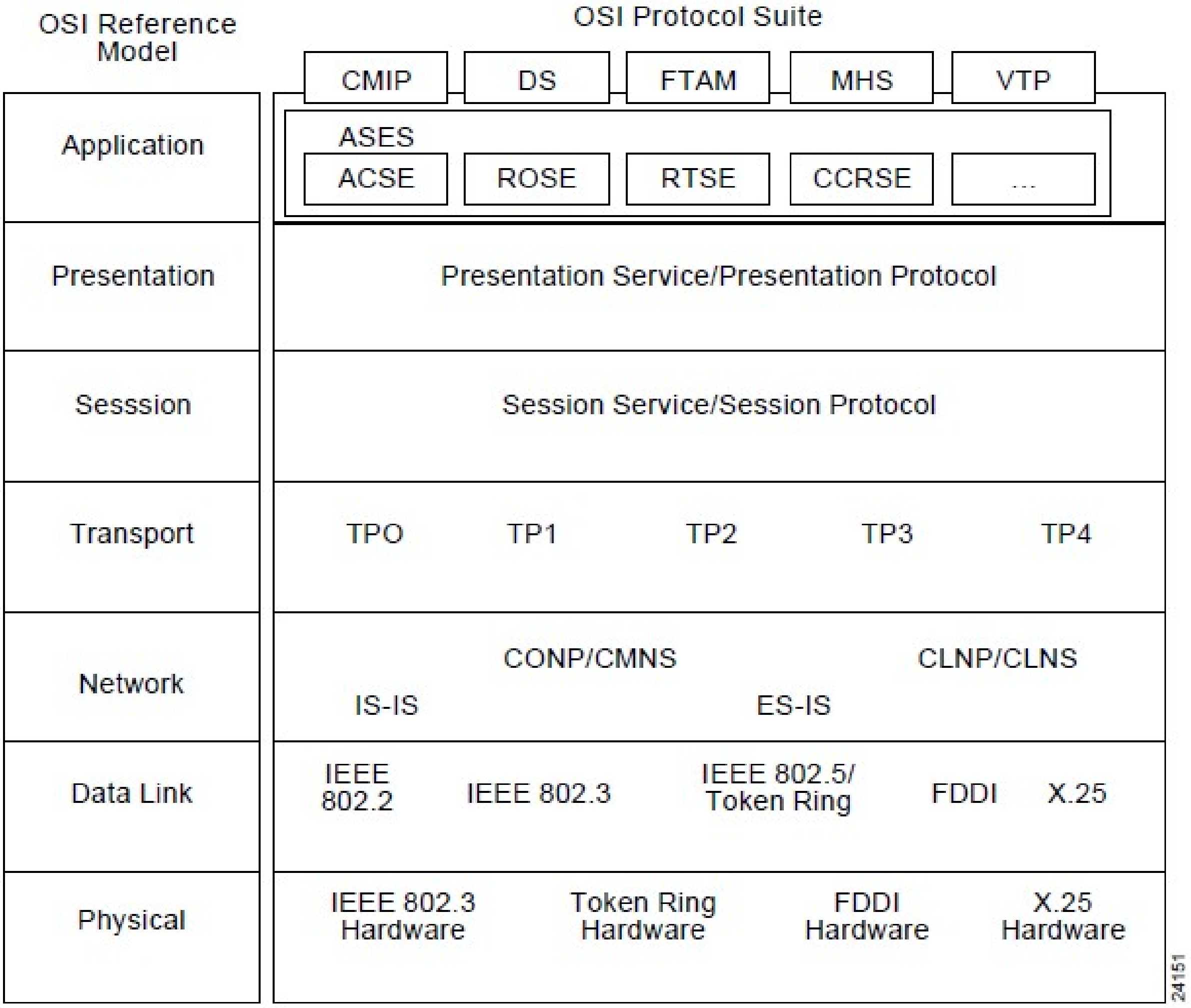
1.1. OSI

OSI是一套规范的总称，包含了很多具体的协议标准，用于方便不同的系统之间互操作。OSI是ISO和ITU-U这两个组织定义的。

其中最有名的就是OSI参考模型，将网络分成不同Layer层次，并且为不同的Layer制定了相应的N多协议规范。

图示如下：

图 1.1. OSI参考模型以及不同层所对应的协议



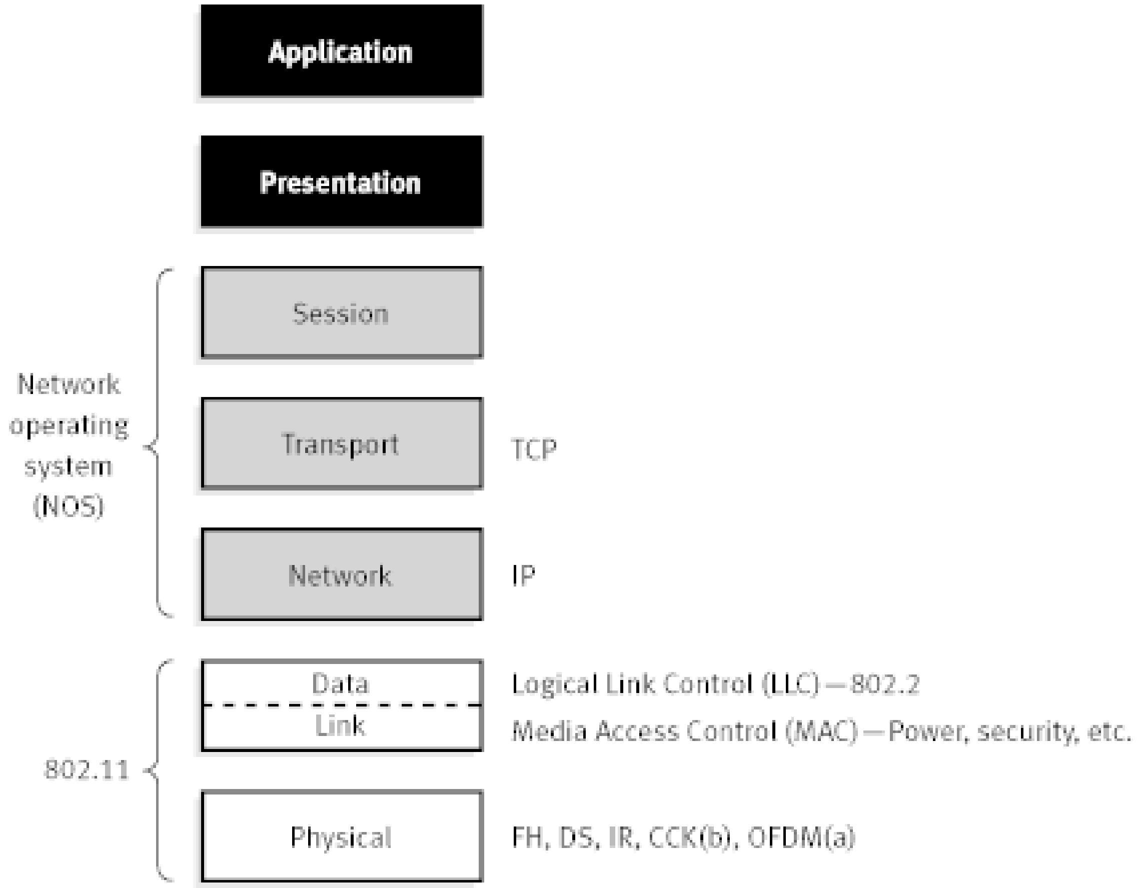
对应的物理层和数据链路层，OSI所支持的介质访问协议包括：

- IEEE 802.2 LLC
- IEEE 802.3
- Token Ring/IEEE 802.5
- FDDI
- X.25

而80211协议，只涉及最底层的，物理层和数据链路层。

下图是802.11和OSI模型的对应关系：

图 1.2. 802.11和OSI模型


Application
Presentation
Session
Transport
Network
Data
Link
Physical
Network operating system (NOS)
802.11
TCP
IP
Logical Link Control (LLC)—802.2
Media Access Control (MAC)—Power, security, etc.
FH, DS, IR, CCK(b), OFDM(a)

对应的物理层方面，可能用到.FH/DS/IR/CCK/OFDM等技术，这部分后面会有详细解释。

1.2. Ethernet

NIC

1.3. 802 Related Specifications

第 2 章 Wireless LAN

无线信号传输方式有两种，窄带通信与扩频通信：

- 窄带无线电通信(Narrow-Band Radio)
  这种技术类似于无线电台的广播，必须把发送器和接收器都调拨到同一频带。

  无线电信号可以穿越墙物，在一个很广的域内传播，所以不必把它调聚成束。

  然而，窄带射频发送有无线电波反射的问题，并受联邦通信委员会管制，它们必须准确地进行调谐，以防其它频率的干扰。

- 扩展频谱通信（Spread Spectrum Communication）
  简称扩频通信，是一种信息传输方式，其信号所占有的频带宽度远大于所传信息必需的最小带宽。

  频带的扩展是通过一个独立的码序列（一般是伪随机码）来完成，用编码及调制的方法来实现的，与所传信息数据无关

  在接收端则用同样的码进行相关同步接收、解扩及恢复所传信息数据。

  这种技术是在一个很宽的频率范围内广播信号，避免在窄带无线电通信中遇到的问题。

  用一种编码来传播信号，接收站用同一编码来恢复信号。用这种方法，扩频无　线电信号能工作在其它信号所占据的频率范围内。

  扩频无线电信号不会干涉常规的无线电广播，这是因为它的能量十分微弱。

2.1. 802.11

2.2. Bluetooth

2.3. IR

第 3 章 80211 Wireless LAN

3.1. BSS

1. BSS
   BSS stands for Basic Service Set. The coverage of an access point is called a BSS.

2. STA
   STA indicates a wireless device acting in in BSS as a regular STAtion.

3.2. ESS

3.3. IBSS

1. IBSS
   IBSS stands for Independent Basic Service Set. Its basically Ad-Hoc mode.

   详情参考：

3.4. DSS

3.5. SSID

1. SSID
   SSID stands for Service Set IDentifier. The SSID is a code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a string of 1-32 octets (usually represented as case sensitive alphanumeric characters).

   http://en.wikipedia.org/wiki/SSID

3.6. Frame Type

Frame Types

http://www.wi-fiplanet.com/tutorials/article.php/1447501

Management Frames：

- Authentication
  Authentication frame, Deauthentication frame

- Association
  Association request frame, Association response frame, Disassociation frame

- Reassociation
  Reassociation request frame, Reassociation response frame

- Beacon Frame
  Authentication frame, Deauthentication frame

- Probe

Probe request frame, Probe response frame

Control Frames

- Request to Send (RTS) frame
- Clear to Send (CTS) frame
- Acknowledgement (ACK) frame

Data Frames

PLME

On the other hand PLME stands for Physical Layer Management Entity.

3.7. 802.11 Beacons Related

http://www.wi-fiplanet.com/tutorials/article.php/1492071/80211-Beacons-Revealed.htm

3.8. Use RTS/CTS to avoid hidden station problem

http://www.pulsewan.com/data101/802_11_b_basics.htm

Another MAC-layer problem specific to wireless is the ?hidden node? issue, in which two stations on opposite sides of an access point can both ?hear? activity from an access point, but not from each other, usually due to distance or an obstruction. To solve this problem, 802.11 specifies an optional Request to Send/Clear to Send (RTS/CTS) protocol at the MAC layer. When this feature is in use, a sending station transmits an RTS and waits for the access point to reply with a CTS. Since all stations in the network can hear the access point, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision. Since RTS/CTS adds additional overhead to the network by temporarily reserving the medium, it is typically used only on the largest-sized packets, for which retransmission would be expensive from a bandwidth standpoint.

3.9. CSMA/CA working flow

http://www.pulsewan.com/data101/802_11_b_basics.htm

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) works as follows.

A station wishing to transmit senses the air, and, if no activity is detected, the station waits an additional, randomly selected period of time and then transmits if the medium is still free. If the packet is received intact, the receiving station issues an ACK frame that, once successfully received by the sender, completes the process. If the ACK frame is not detected by the sending station, either because the original data packet was not received intact or the ACK was not received intact, a collision is assumed to have occurred and the data packet is transmitted again after waiting another random amount of time.

第 4 章 Linux Network

已经实现了哪些层，（简单描述）有线网络是如何工作的

第 5 章 Linux Wireless LAN & 80211

Linux: Generic 2.6 Wireless Driver

http://kerneltrap.org/node/3245

这个解释了，当时为何选Host AP作为wireless stack 的来龙去脉。

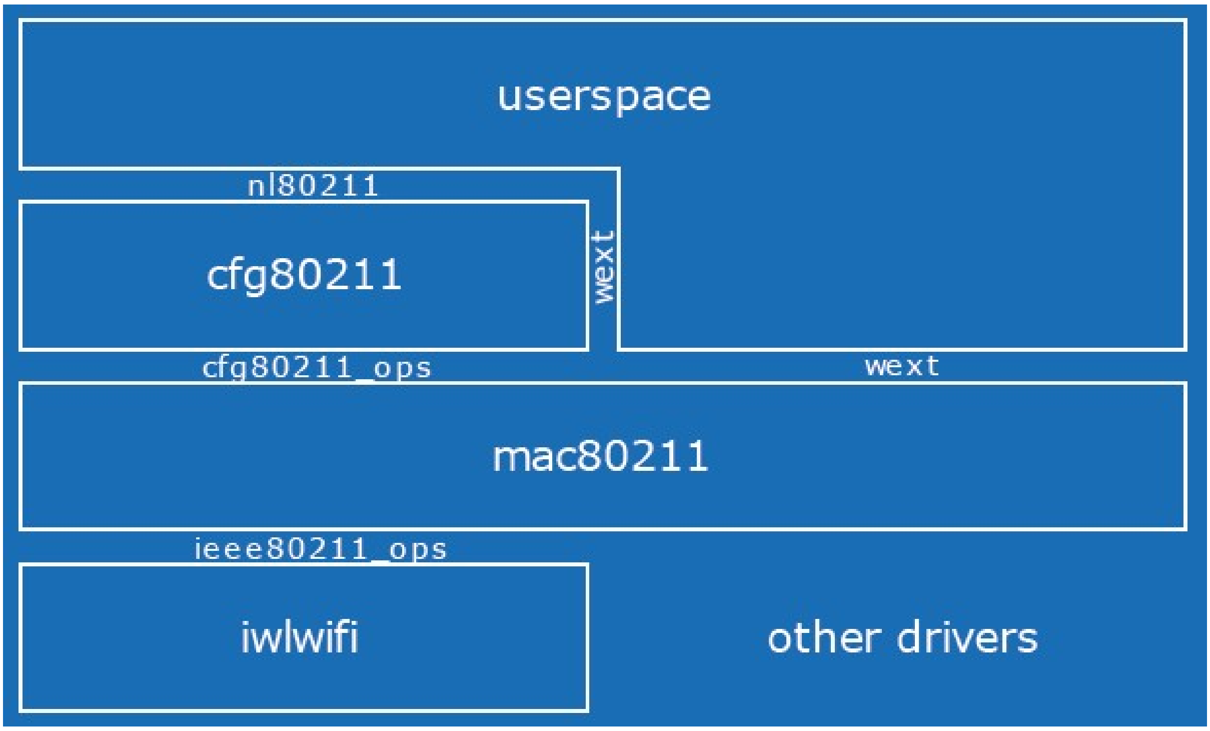
5.1. 无线网络的架构

5.1.1. Framework

From: Page 6/47 Johannes Berg's presentation[1]

Old:

图 5.1. 旧的Linux的网络架构



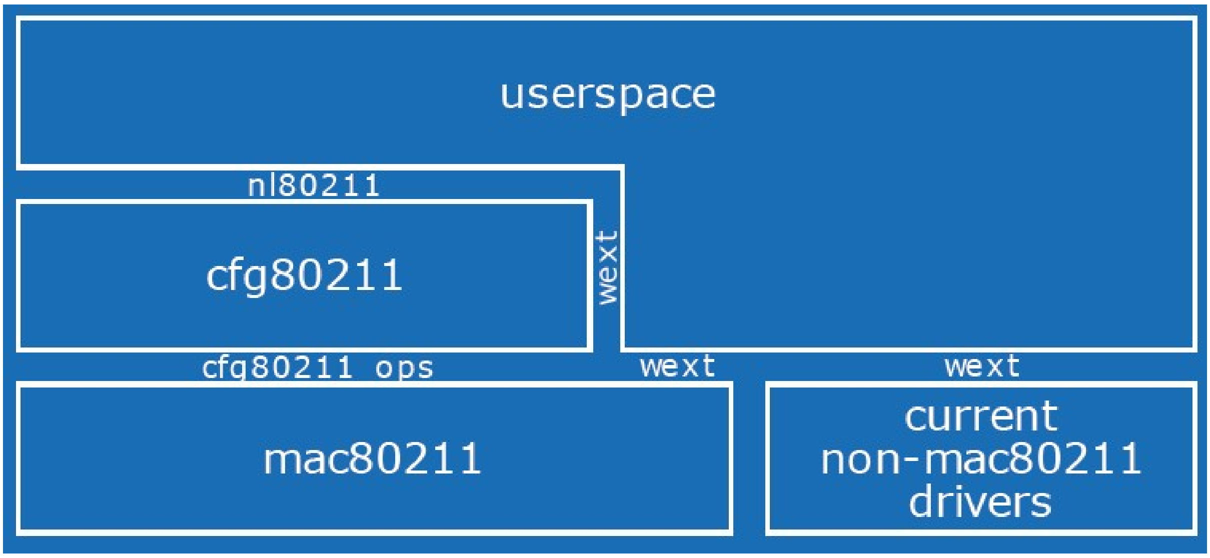
From: page 4/47 Johannes Berg's presentation[2]

New:

[1] http://wireless.kernel.org/en/developers/Documentation/mac80211?action=AttachFile&do=view&target=mac80211.pdf

[2] http://wireless.kernel.org/en/developers/Documentation/cfg80211?action=AttachFile&do=view&target=control.pdf

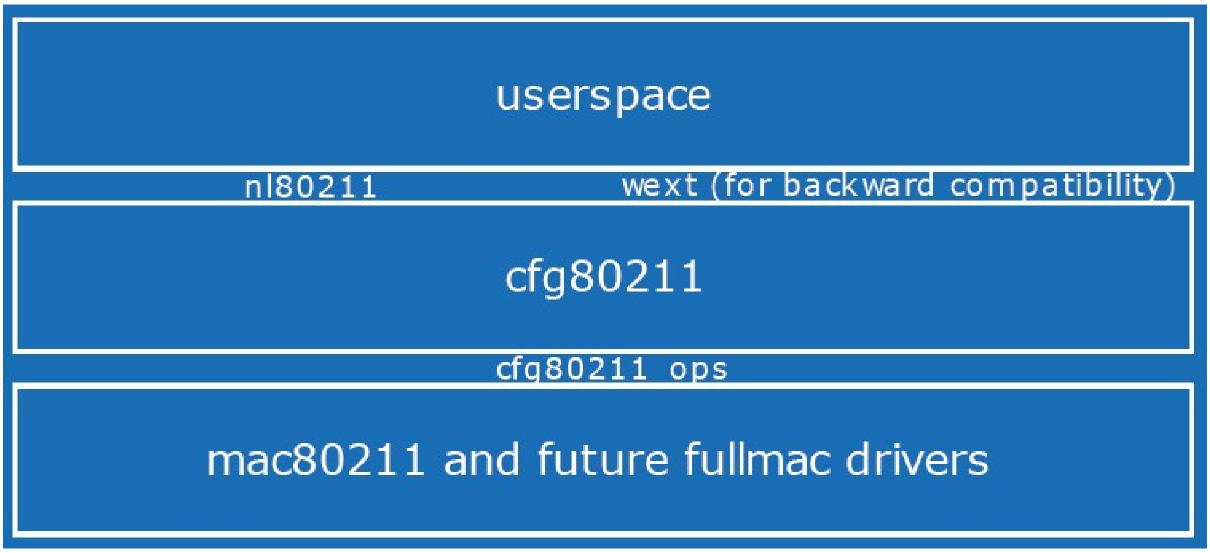
图 5.2. 新的Linux的网络架构



From: page 5/47 Johannes Berg's presentation[3]

Planned:

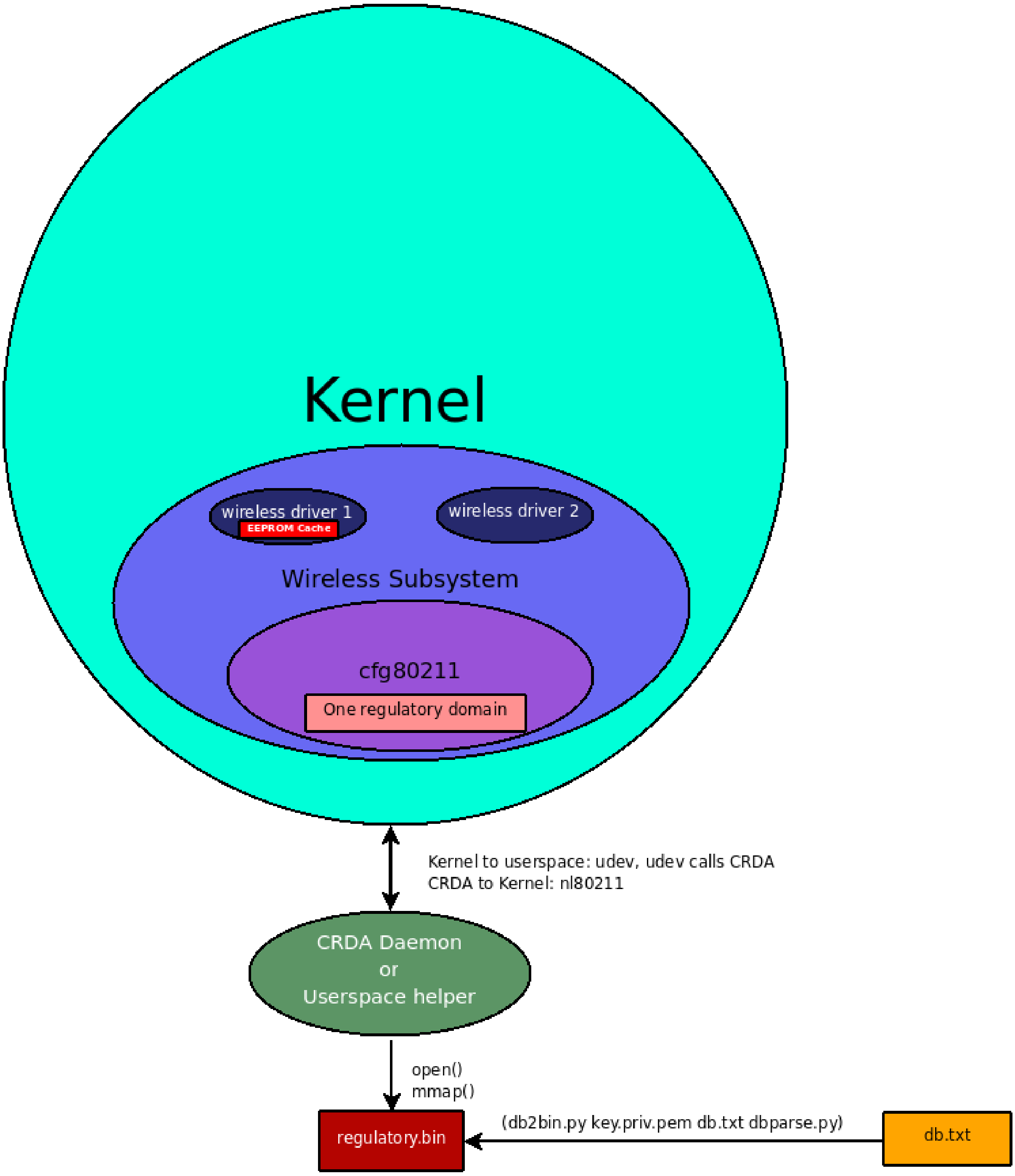
图 5.3. 计划的Linux的网络架构


userspace
nl80211
wext (for backward compatibility)
cfg80211
cfg80211 ops
mac80211 and future fullmac drivers

[3] http://wireless.kernel.org/en/developers/Documentation/cfg80211?action=AttachFile&do=view&target=control.pdf

5.1.2. CRDA

图 5.4. CRDA的架构



5.1.3. Wext/WE

Wireless Extensions的缩写，是旧的Linux无线网络的架构，其基于mac80211[4]。现在已逐渐转移到新的架构上面了，新的架构使用cfg80211[5]和nl80211[6]。

[4] http://linuxwireless.org/en/developers/Documentation/mac80211
[5] http://linuxwireless.org/en/developers/Documentation/cfg80211
[6] http://linuxwireless.org/en/developers/Documentation/nl80211

WE

WE stands for Wireless-Extensions[7] - the old driver API and user <–> kernel communication transport.

5.1.4. cfg80211

新的Linux无线网络架构中，为驱动提供配置接口/API。

5.1.5. nl80211

新的Linux无线网络架构中，为内核空间和用户空间之间，提供通讯转换接口。

5.1.6. Radiotap[8]

用于802.11的 帧接收(frame reception)和帧注入(frame injection)

5.1.7. Frame Reception/ Injection

所谓的帧接收，就是硬件（网卡）用中断通知CPU，一个数据帧到了，要CPU去接收。一般是在将无线网卡设置为 ？？？模式的时候，底层接受到数据帧之后，不处理，而是直接传送给上层处理，一般用于分析无线网络数据传输的时候，分析网络问题到底出现在哪。

5.1.8. MLME

MLME Stands for Media Access Control (MAC) Sublayer Management Entity. MLME is the management entity where the Physical layer (PHY) MAC state machines reside. Examples of states an MLME may assist in reaching:

- Authenticate
- Deauthenticate
- Associate
- Disassociate
- Reassociate
- Beacon
- Probe
- Timing Synchronization Function (TSF) [9]

5.1.9. FullMAC

FullMAC is a term used to describe a type of wireless card where the MLME is managed in hardware. You would not use mac80211 to write a FullMAC wireless driver.

5.1.10. SoftMAC

SoftMAC is a term used to describe a type of wireless card where the MLME is expected to be managed in software. mac80211 is a driver API for SoftMAC wireless cards, for example.

[7] http://linuxwireless.org/en/developers/Documentation/Wireless-Extensions
[8] http://linuxwireless.org/en/developers/Documentation/radiotap
[9] http://en.wikipedia.org/wiki/Timing_Synchronization_Function_(TSF)

第 6 章 以iwmc3200wifi为例，分析具体如何实现

6.1. 系统已经实现了哪些

6.2. 自己需要实现哪些

参考书目

[1] Network related training meterials[1]

[2] Linux Wireless - Developer Documentation[2]

[3] MLME[3]

[4] Glossary - Linux Wireless[4]

[5] Understanding Linux Network Internals: Frame Reception[5]

[6] Service set (802.11 network)[6]

[7] Wireless Tools for Linux[7]

[8] About Wireless-Extensions[8]

[9] A bit more about the technologies involved[9]

[10] Replacing iwconfig with iw[10]

[11] 802.11学习笔记[11]

[12] OSI Basic[12]

[13] 无线网络的通信技术（窄带通信、扩频通信、packet网络，蜂窝网络）[13]

[14] 扩展频谱通信[14]

[1] http://www.pulsewan.com/data_101.htm
[2] http://linuxwireless.org/en/developers/Documentation
[3] http://en.wikipedia.org/wiki/MLME
[4] http://linuxwireless.org/en/developers/Documentation/Glossary#SoftMAC
[5] http://whitepapers.zdnet.com/abstract.aspx?docid=324603
[6] http://en.wikipedia.org/wiki/Independent_Basic_Service_Set
[7] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
[8] http://linuxwireless.org/en/developers/Documentation/Wireless-Extensions
[9] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Overview.html
[10] http://linuxwireless.org/en/users/Documentation/iw/replace-iwconfig
[11] http://d.download.csdn.net/down/2916327/kennyli530
[12] http://www.pulsewan.com/data101/pdfs/osi_basics.pdf
[13] http://hi.baidu.com/karashun/blog/item/d24a207292e3ef148701b08c.html
[14] http://baike.baidu.com/view/3089584.htm