

# Диссектор zigbee для Wireshark

Задача состоит из двух частей: получение пакетов наиболее низкого уровня стека протоколов zigbee и их разбор в wireshark.

## Получение пакетов

Варианты получения пакетов:

- через пакетный сокет (tap 7 packet) – стандартный интерфейс для этой задачи;
- специализированной библиотекой, типа libpcap (tap pcap) – обертка вокруг первого варианта, добавляет стандартный способ сохранения пакетов в файле;
- через частный интерфейс предоставляемый драйвером – это уж как фантазия развернется.

## Разбор в Wireshark

В wireshark есть код по разбору пакетов протокола ieee802.15.4 уровня MAC и выше (epan/dissectors/packet-ieee802154.c). Код регистрации оттуда:

```
dissector_add("wtap_encap", WTAP_ENCAP_IEEE802_15_4, ieee802154_handle);
```

Ключ wtap\_encap обозначает получение пакетов с уровня wiretap (из дампа), с кодом link\_encap WTAP\_ENCAP\_IEEE802\_15\_4

([http://www.wireshark.org/docs/wsdg\\_html\\_chunked/ChapterCapture.html](http://www.wireshark.org/docs/wsdg_html_chunked/ChapterCapture.html)).

Для разбора пакетов уровня PHY в wireshark добавлено следующее:

- новый тип link\_encap – WTAP\_ENCAP\_IEEE802\_15\_4\_PHY, содержащий, помимо PSDU, SHR и PHR (см. 802.15.4-2003.pdf, п.6.3);
- диссектор ieee802.15.4 уровня PHY (wrap\_phy), выделяющий поля SHR и PHR, передающий PSDU дальше, диссектору wrap.

From:

<http://wiki.osll.ru/> - Open Source & Linux Lab

Permanent link:

[http://wiki.osll.ru/doku.php/etc:common\\_activities:zigbee:wireshark](http://wiki.osll.ru/doku.php/etc:common_activities:zigbee:wireshark)

Last update: **2008/09/14 13:48**

