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, man 7 packet – стандартный интерфейс для этой задачи;
- специализированной библиотекой, типа libpcap – 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).

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 (wpan_phy), выделяющий поля SHR и PHR, передающий PSDU дальше, диссектору wpan.

From:
http://wiki.osll.ru/ - **Open Source & Linux Lab**

Permanent link:
http://wiki.osll.ru/doku.php/etc:common_activities:zigbee:wireshark?rev=1221385688

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