Стек ZigBee для Linux

https://sourceforge.net/projects/zigbee-stack-t/

Задачи

- [+] установить связь с отладочной платой; мануал на процессор; – готово, работает;
  - [+] выяснить, можно ли это сделать по USB? – результат отрицательный;
  - [+] если по USB – нет, выяснить, каким должен быть кабель RS-232; – кабель обычный, прямой;
- разобраться с драйвером ZigBee и предоставляемым им интерфейсом;
  - [+] какие типы сокетов можно создать в PF_ZIGBEE? – SOCK_DGRAM и SOCK_RAW, сейчас идентичные по функциональности;
  - [?] как посылать через сокеты команды разным уровням стека протоколов zigbee?
  - [?] как получать через сокеты принимаемые и отправляемые через стек пакеты?
    - [+] с помощью PF_PACKET/SOCK_RAW; получаемые сейчас пакеты содержат кусок PDU уровня MAC, спереди отрезано 9 байт того же уровня, сзади отрезано 5 байт, 3 из которых – какого-то мустора;
- разобраться с Wireshark – как написать свой анализатор протокола;
  - [+] научиться получать файл с link encap=wpan, чтобы скормить его существующему диссектору; – вручную, pcap_open_dead(195,...);
  - [-] создать сетевой интерфейс, из которого можно получать пакеты wpan; – интерфейс создается при активизации ldisc; wpan не распознается dumpcap;

Результаты

User Mode Linux

Входит в ядра серии 2.6. Должен собираться и работать по make ARCH=um defconfig ; make ARCH=um. Однако, статистика такова: 2.6.17-2.6.23 не собирается ни одно. 2.6.24-2.6.25 собираются все.

Вместо http://uml.nagafix.co.uk/FedoraCore5/FedoraCore5-x86-root_fs.bz2 стоит использовать http://uml.nagafix.co.uk/Fedora8/Fedora8-x86-root_fs.bz2. И вообще, занятный сайт – http://uml.nagafix.co.uk/

Драйвер ZigBee

Собирается и устанавливается. В readme написано modprobe zb_tty dev_name="my_dev1" mac_addr=1, однако последний модуль называется zb-ldisc и параметр mac_addr он не поддерживает.

roadmap по граблям

1. на этапе сборки ядра, после make defconfig ARCH=um выполнить make menuconfig ARCH=um и поставить M в Library routines/CRC* functions;
2. после загрузки в uml отредактировать /etc/inittab, убрав последнюю строку (что-то заканчивающееся на ttyS0, через который мы работаем с устройством);
3. для запуска sock-coord и sock-router требуется поддержка PF_ZIGBEE. Для этого следует modprobe af_zigbee. А предварительно поменять include/linux/net.h и include/linux/socket.h:

```
diff -bur linux-2.6.25-org/include/linux/net.h
linux-2.6.25/include/linux/net.h
--- linux-2.6.25-org/include/linux/net.h        2008-04-17
06:49:44.000000000 +0400
+++ linux-2.6.25/include/linux/net.h    2008-08-10 00:58:00.000000000 +0400
@@ -26,7 +26,7 @@
 struct inode;
 struct net;

-#define NPROTO          34              /* should be enough for now..   */
+#define NPROTO          35              /* should be enough for now..   */

 #define SYS_SOCKET     1               /* sys_socket(2)                */
 #define SYS_BIND       2               /* sys_bind(2)                  */
diff -bur linux-2.6.25-org/include/linux/socket.h
linux-2.6.25/include/linux/socket.h
--- linux-2.6.25-org/include/linux/socket.h     2008-04-17
06:49:44.000000000 +0400
+++ linux-2.6.25/include/linux/socket.h 2008-08-10 00:57:47.000000000 +0400
@@ -189,7 +189,7 @@
 #define AF_BLUETOOTH   31      /* Bluetooth sockets            */
 #define AF_IUCV                32      /* IUCV sockets                 */
 #define AF_RXRPC       33      /* RxRPC sockets                */
-#define AF_MAX         34      /* For now.. */
+#define AF_MAX         35      /* For now.. */

 /* Protocol families, same as address families. */
 #define PF_UNSPEC      AF_UNSPEC
```

Отладочная плата

Пытался установить взаимодействие с отладочной платой по USB и по RS-232. Ожидал, что при получении команды (например, “zb\x1”) загорится первый светодиод.

Вопросы:

- на отладочной плате есть интерфейс USB, в readme тоже указан /dev/ttyUSB, должно ли оно так работать (было бы проще чем через COM, однако, у меня не получилось – нет реакции, вообще никакой);
- при подключении через RS-232, каким должен быть кабель? (подозреваю, что прямым); по скольки линиям идет взаимодействие? (судя по тому, что тестовые программы

включают аппаратный flow-control, 3-проводного кабеля мало);
- тестовые программы через RS-232 запускаются однократно. при следующем запуске они повисают на открытии /dev/ttyS. почему? как (и можно ли) протестировать отладочную плату без драйвера, просто посылая команды в /dev/ttyS?

Wireshark

Начало где-то здесь: http://www.wireshark.org/docs/wsdg_html_chunked/PartDevelopment.html

Уже существует анализатор IEEE802.15.4: wireshark/epan/dissectors/packet-ieee802154.*

Страничка на wiki wireshark: http://wiki.wireshark.org/IEEE_802.15.4

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

Permanent link:
http://wiki.osll.ru/doku.php/etc:common_activities:zigbee?rev=1218406768

Last update: **2008/08/11 02:19**