AN2

How to customize the QCA7000 via open-plc-utils

I2SE GmbH: Stefan Wahren, Christian Aurich

August 19, 2013

Revisions

Revision	Release Date	Changes
1	August 19, 2013	initial release

Contents

1 Introduction

The following document explains the customization of the Qualcomm QCA7000 settings via the open-plc-utils. You will be able to change parameters like the MAC address of the powerline chip and some other settings after reading this document. It is mainly intended for use by device manufacturers to customize their products.
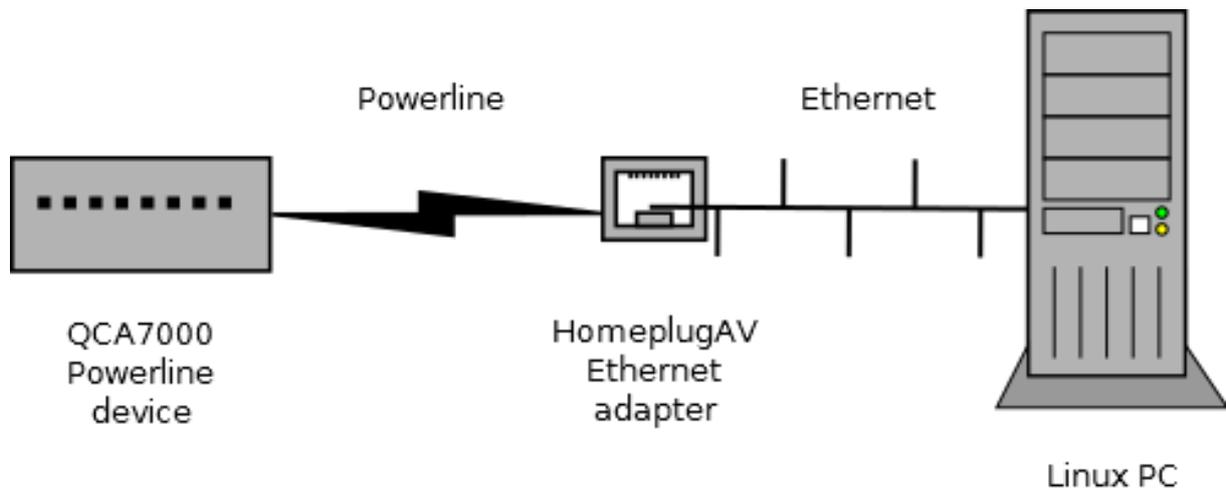
2 Requirements

Figure 1: Connection between your QCA7000 device and your PC

These are the requirements for this application note:

- QCA7000 Powerline device with disbled security features

- HomeplugAV Ethernet adapter

- open-plc-utils

Note: AN1 describes the installation of the open-plc-utils on a Linux PC.

3 Overview

The configuration of a Qualcomm powerline device like the QCA7000 is stored in the Parameter Information Block (PIB). This block can be stored in a binary file called PIB file. The structure in those files often changes, so PIB files are not very portable.

The following table shows the parameters that are changeable with modpib (part of open-plc-utils):

Abbr	Parameter	Type	Default
CCo	Central Coordinator Selection mode	0 = Auto, 1 = Never, 2 = Always, 3 = UserAssigned	0
DAK	Device Access Key	16 hex string	HomePlugAV
SL	Security Level	0 = push button enabled, 1 = push button disabled	0
MAC	MAC address	6 hex string	00:B0:52:00:00:01
NMK	Network member-ship key	16 hex string	HomePlugAV
MFG	Manufacturing string	63 character zero-terminated ASCII string	Qualcomm Atheros Home-Plug AV Device
NET	Network name string	63 character zero-terminated ASCII string	Qualcomm Atheros Enabled Network
USR	Username string	63 character zero-terminated ASCII string	Qualcomm Atheros Enabled Product

Please keep in mind that the parameters in the table above are only a small subset of all parameters in the PIB.

Note: The modification of the prescaler settings that are also saved in the PIB is not discussed in this application note.

The general process includes the following steps:

1. connect the PC and the HomeplugAV adapter via Ethernet

2. connect and pair the QCA7000 device and the HomeplugAV adapter over Powerline

3. use plctool to upload the PIB file from them QCA7000 on the PC

4. use modpib to modify the PIB file on the PC

5. use plctool to download the PIB file from the PC on the QCA7000

6. reset the QCA7000 device to make changes take effect

4 Central Coordinator Selection mode

Homeplug AV implements a centrally-managed architecture. The central manager of a AV Logical Network (AVLN) is called Central Coordinator (CCo). This role isn't fixed to a specific station, but the CCo is selected at runtime. The Central Coordinator Selection mode takes influence on the selection process.

Value	Description
0	Auto, the station may act either as a CCo or STA of an AVLN
1	Never, the station will never become the CCo of an AVLN
2	Always, the station will not join other AVLNs as a STA
3	User, the user assign how the station act either as CCo or STA of an AVLN

Note: all other values have an undefined behavior.

The following call sets the Central Coordinator Selection mode of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -C <MODE> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<MODE>	Central Coordinator Selection Mode as integer	0

5 Device Access Key

The Device Access Key should be unique for every HPAV device and is intended to encrypt data only for the device with this particular DAK. This secret key must never be transmitted over powerline (encrypted or unencrypted) and cannot be changed after production. Therefore it is not possible to change it in the same way as the other parameters. Hence the below steps only modify the PIB file without writing it back to the device. This command should be executed to modify a PIB file to get a unique DAK for each device.

The following call sets the Device Access Key in a PIB file:

```
$modpib -D <DAK> -v <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<DAK>	Device Access key as colon separated hex string	FF:EE:DD:CC:BB:AA:99:88:77:66:55:44:33:22:11:00
<PIBFILE>	Filename for temporary PIB file	settings.pib

6 Security Level

The Security Level defines how the Network Membership Key (NMK) can be distributed in the AVLN. So the Security Level is part of the Network ID (NID), all devices for a AVLN must have the same Security Level.

Value	Description
0	Simple connect, push button on station enabled
1	High Security Level, push button on station disabled

Note: all other values have an undefined behavior.

The following call would set the Security Level of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -L <SL> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<SL>	Security Level as integer	0

7 MAC Address

Every HPAV station is uniquely identified by it's MAC address. The format of this MAC address is exactly like in Ethernet and share the same address space.

The following call would set a new MAC address to a remote HPAV device:

```
$ plctool -i <NETIF> -p <PIBFILE> <OLDMAC> && \
modpib -M <NEWMAC> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <OLDMAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<OLDMAC>	Old MAC address of station as colon separated hex string	00:B0:52:00:00:01
<NEWMAC>	New MAC address of station as colon separated hex string	00:B0:52:00:00:02

8 Network membership key

The Network membership key (NMK) defines which devices are coupled. All HomePlug devices with identical Network membership keys belong to the same logical network (AVLan)
The following call would set the NMK of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -N <NMK> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<NMK>	Network membership key as colon separated hex string	50:D3:E4:93:3F:85:5B:70:40:78:4D:F8:15:AA:8D:B7

9 Manufacturing string

The Manufacturing string (MFG) provides a human friendly identifier (HFID) of the station set by the manufacturer.
The following call would set the MFG of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -S <MFG> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<MFG>	Manufacturing string as ASCII string	Qualcomm Atheros Home-Plug AV Device

Note: please keep in mind to escape special characters in the Manufacturing string from the executing shell.

10 Network name string

The Network name string (NET) provides a human friendly identifier (HFID) of the AVLN.

The following call would set the NET of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -T <NET> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<NET>	Network name string as ASCII string	Qualcomm Atheros Enabled Network

Note: please keep in mind to escape special characters in the Network name string from the executing shell.

11 Username string

The Username string (USR) provides a human friendly identifier (HFID) of the station set by the user.

The following call would set the USR of a remote HPAV device with a specific MAC address:

```
$ plctool -i <NETIF> -p <PIBFILE> <MAC> && \
modpib -U <USR> -v <PIBFILE> && \
plctool -i <NETIF> -P <PIBFILE> <MAC>
$ rm <PIBFILE>
```

This table explains the parameter from the call above:

Parameter	Description	Example
<NETIF>	Network interface connected to station	eth1
<PIBFILE>	Filename for temporary PIB file	settings.pib
<MAC>	MAC address of station as colon separated hex string	00:B0:52:00:00:01
<USR>	Username string as ASCII string	Qualcomm Atheros Enabled Network

Note: please keep in mind to escape special characters in the Username string from the executing shell.

12 Further Information

If you need to set the security features of the QCA7000 to prevent users from changing settings and / or firmware of the powerline devices I2SE can provide you assistance for the best possible configuration. Please feel free to contact us describing your specific application.

For the provisioning of firmware to a QCA7000 you need to use the SPI interface of the chip since powerline communication is not available without firmware. Generally you are free how to send data to the SPI but there are some tools that make this step easier. The above mentioned tools always use ethernet communication. Therefore the easiest solution is to use an adapter that converts ethernet to the QCA7000 spi. Qualcomm provides a development platform for QCA7000 named PL16 that includes this adapter but is relatively pricey. A smaller and cheaper alternative that provides an easy access is the I2SE development tool "Duckbill SPI". You can plug this in to your USB port, where it is recognized as USB Ethernet interface. The other side of this adapter then needs to be connected to the SPI of your QCA7000 device.

13 References

Title	Availability
HTML manual for the Qualcomm Atheros Open Powerline Toolkit	HTML
HomePlug AV White Paper	PDF

14 Contact

Home Page: http://www.i2se.com

Web Support: http://www.i2se.com/wiki

I2SE GmbH

Friedrich-Ebert-Str. 61

04109 Leipzig

Germany