KNX IoT Hub

Installation Manual

Table of contents

List of Figures

List of Tables

1. About the KNX IoT Hub

1.1. Overview

Cascoda's KNX IoT Hub™ provides everything you need to configure your KNX IoT system and connect to an IPv4/IPv6 backbone network. It is a compact low-power design, featuring Cascoda's SMARTRange™ technology to provide long-range Thread connectivity for whole-house coverage. In addition, Cascoda provides a web-interface for comprehensive configuration and network management.

1.2. Features

- Acts as a Thread Border Router, forwarding KNX IoT datagrams between Thread and the IP Backbone
- Compatible with existing IPv4/IPv6 backbone networks
- Integrated Thread, Ethernet, and Wi-Fi connectivity
- OpenThread Thread stack for long-term maintenance
- Based on the popular and well-supported OpenWrt Operating System
- Comprehensive configuration, network management & visualization tools
- Can operate as either a router or a bridge

1.3. Optional extras

- KNX IoT Router, to communicate between KNX IoT and other KNX transports (KNX Classic and/or KNX RF)
- KNX IoT MQTT proxy, to communicate between KNX IoT and an MQTT server

1.4. Specification

- Qualcomm QCA9531 chipset, up to 650 MHz
- Flash 16 MB, SDRAM 128 MB
- Low power (12V, 1A DC), or Passive PoE (12-24V DC) input
- 2× Fast Ethernet, one with passive PoE (12-24V)
- IEEE 802.11b/g/n Wi-Fi connectivity
- IEEE 802.15.4 Thread connectivity
- USB interface to connect USB peripherals manufactured and supported by Alfa Networks Inc. Not used for other communications.
- Dimensions 98 x 74 x 28mm

2. General information

2.1. Document version information

This manual is amended periodically and will be brought into line with new software releases. The change status (date) can be found in the contents header. If you have a device with a later software version, please check www.cascoda.com to find out whether a more up-to date version of the manual is available.

2.2. Used terms

Sign	Description
DANGER!	Indicates an immediately hazardous situation which will lead to death or severe injuries if it is not avoided.
CAUTION!	Indicates a potentially hazardous situation which may lead to trivial or minor injuries if it is not avoided.
WARNING!	Indicates a situation which may lead to damage to property if it is not avoided.
NOTE!	Indicates a situation which may lead to possible (known) side effects.

Table 1: *Used Terms*

2.3. Safety instructions

Not applicable.

2.3.1. Cyber security

WARNING!

When the device is deployed the installer has to configure:

- userid/password for logging into the Hub.
- Wi-Fi password.
- SSH access.

If not configured, then the Hub is vulnerable for unauthorized access.

2.4. Issues

Questions about the product?

You can reach the technical service of Cascoda under Tel. +44 (0)2380 638 111 or support@cascoda.com.

We need the following information to process your service request:

- Type of appliance (model name or item number)
- Description of the problem
- Serial number or software version
- Source of supply (dealer/installer who bought the device from Cascoda)

For questions about KNX functions:

- Version of the device application
- ETS version used for the project

2.5. Contact information

info@cascoda.com
Threefield House,
Threefield Lane,
Southampton,
SO14 3LP, UK

3. Technical Information

4. Storage Conditions

Parameter	Min	Typ	Max	Unit
Storage Temperature	-25		70	°C
Storage Humidity	10		90	%RH

Table 2: *Storage Conditions*

4.1. Operating Conditions

Parameter	Min	Typ	Max	Unit
Operating Temperature	-20		60	°C
Supply Voltage (Power Adapter)	11.4	12	12.6	V
Supply Voltage (Passive POE)	12		24	V
Supply Current	1			A

Table 3: *Operating Conditions*

Note: Power Supply not provided with Product. 12V, 1A (min.) Power Supply with centre-positive barrel connector required.

4.2. Radio Specification

4.2.1. Wifi

Standard: IEEE 802.11n/b/g (2x2) Data Rates: 802.11n: up to 399 Mbps 802.11g: up to 54 Mpbs 802.11b: up to 11 Mbps

Antenna: 2x Internal Printed Circuit Antennas, 1 dBi Configuration: 2.4 GHz, 2 Streams, Channels 1-13

Parameter	Min	Typ	Max	Unit
Frequency Range	2412		2472	MHz
Transmit Power	0		20	dBm

Table 4: *Wifi Radio Information*

4.2.2. Thread

Protocol: KNX-IoT over Thread MAC Protocol: IEEE 802.15.4

Antenna: 5 dBi Dipole Omnidirectional Antenna Indoor, 2.4 GHz RP-SMA Male Configuration: 2.4 GHz, O-QPSK, 250 kbps, Channels 11-26

Parameter	Min	Typ	Max	Unit
Frequency Range	2405		2480	MHz
Transmit Power	0		9	dBm

Table 5: *Thread Radio Information*

5. Setup and Configuration

5.1. Requirements

- The Cascoda KNX IoT Hub
- 12V 1A Power Supply, with centre-positive barrel connector
- A Windows PC
- Two Ethernet cables

5.2. Initial setup and startup

1. Attach the antenna to the hub by screwing it in, then angle it upwards for maximum coverage.
2. Connect one end of the Ethernet cable to the socket on the hub marked **"PoE LAN1"**, and connect the other end to your desktop computer.

Fig 1: Lan connection.

3. Connect the hub to your internet router or switch via Ethernet, by connecting one end of the cable into the **"WAN/LAN2"** port of the hub, and the other end of the cable into your internet router/switch.
4. Connect the Power Supply to the hub.
5. Now power up the hub using the power adapter.
6. After about 30s, the Web GUI should become accessible. Navigate to http://openwrt.local.
7. Access the Web GUI by logging in as "root", with an empty password field. You now have full control over your KNX IoT Hub.

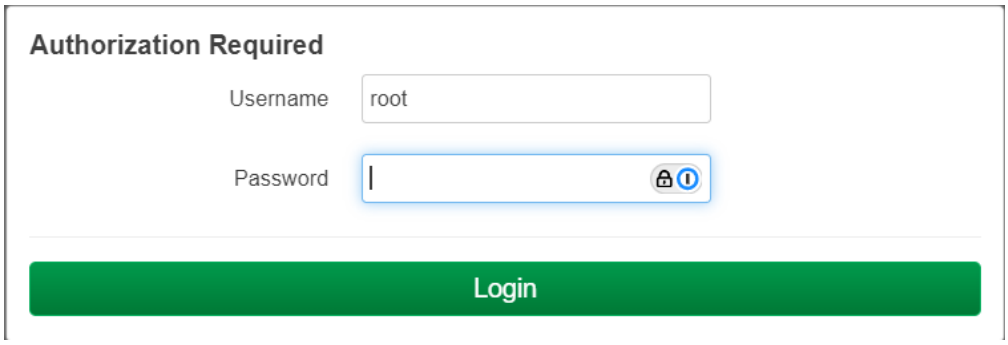


Fig 2: Login screen.

8. Double check that you have internet access via the hub by opening up any web browser and searching something.

After following the steps above, you will have a network topology that looks like the picture below. The Hub is also accessible via Wi-Fi, though by default the Wi-Fi Access Point is disabled. For instructions on how to enable it, please see this section.

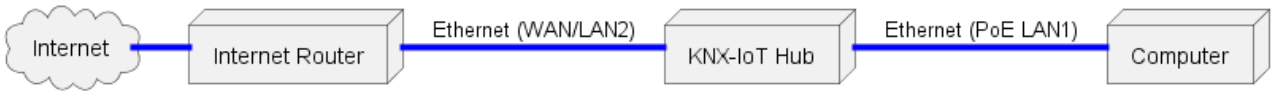


Fig 3: Typical Network topology.

We recommend that you change the hostname of your device:

1. Hover over "System" in the menu bar, and click on "System" from the dropdown menu. The default hostname is "OpenWRT", which makes the device accessible via http://openwrt.local.

2. Type in your desired hostname in the "Hostname" field, then press "Save & Apply". This will change the URL that you use to access the Web GUI, and make it convenient to use multiple KNX IoT Hubs. This change will take effect once the KNX IoT Hub is restarted.

3. It is also **recommended** that you set a login password, by navigating to "System - Administration" from the menu bar.

5.3. Enabling Wi-Fi

The KNX IoT Hub is capable of using Wi-Fi for either of its links: to the Computer or the the wider Internet.

5.3.1. Wireless link to the computer

You can create a Wi-Fi Access Point on the KNX IoT Hub, allowing you to connect other devices wirelessly to the Hub, instead of using Ethernet. This allows you to connect mobile phones, tablets, or laptops that do not have an Ethernet interface available. To do this, press the grey Wi-Fi button at the top of the device and wait for it to start blinking. Doing so creates an open Wi-Fi hotspot called "OpenWrt". Connecting to this hotspot gives you access to the Hub's OpenWrt Web GUI just like the LAN1 connection would.

Navigate to "http://openwrt.local" (or "http://openwrt.lan"), and check that your connection is successfully established. The resulting topology is shown below.

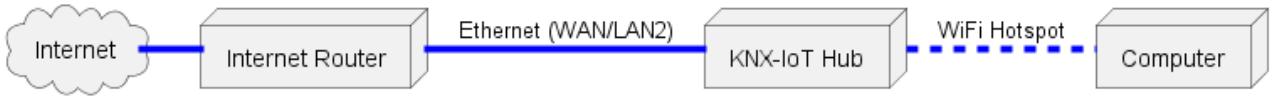


Fig 4: Network topology with Wi-Fi enabled.

> **NOTE!** You can connect to the LAN1 interface with Ethernet, and connect other devices using the Wi-Fi access point at the same time. **NOTE!** The name of the hotspot created, and the hostname of the Hub are independent from each other, even though they are both "OpenWrt" by default.

5.3.1.1. Wi-Fi Access Point Security

By default, the hotspot that is created doesn't have any security, allowing anyone to connect to it without requiring a password. It is therefore recommended to enable security for your Wi-Fi access point, as well as renaming the default name "OpenWrt". The steps below demonstrate how to do this:

1. Hover over "Network" on the menu bar, and click on "Wireless". You will be taken to the page that allows you to view all your wireless interfaces. You should see the one that you are currently connected to, and that is called "OpenWrt".

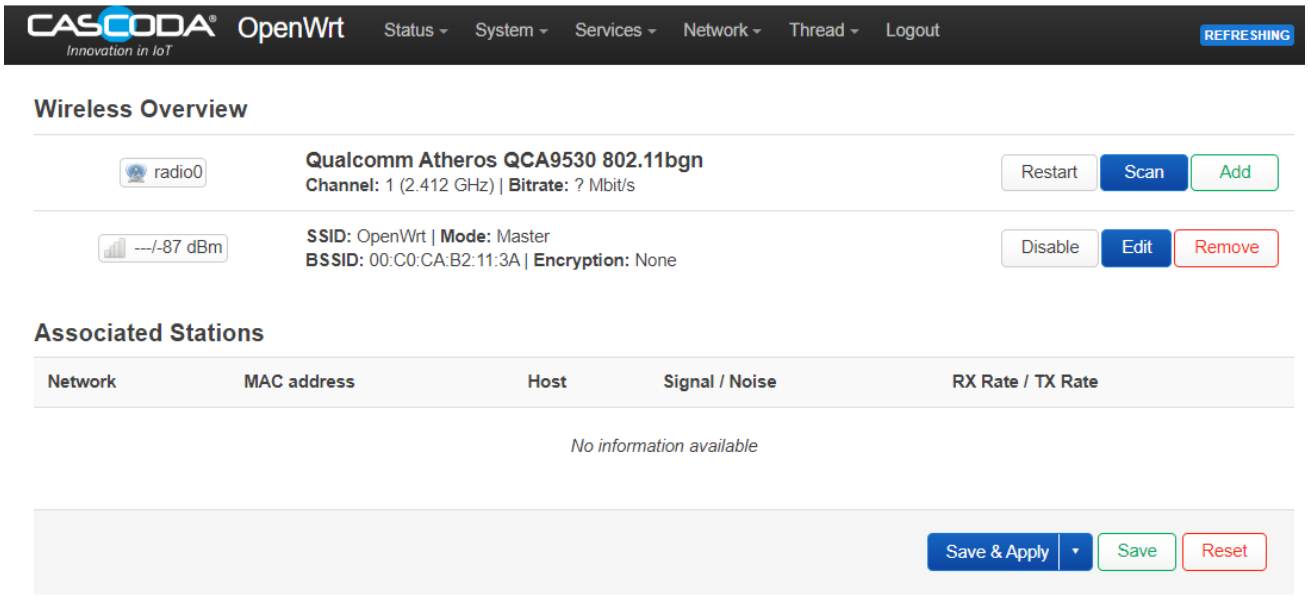


Fig 5: Wi-Fi Overview.

2. Click on "Edit". This will open a popup window with configuration options. We are interested at the bottom half of this window, which has the title "Interface Configuration".

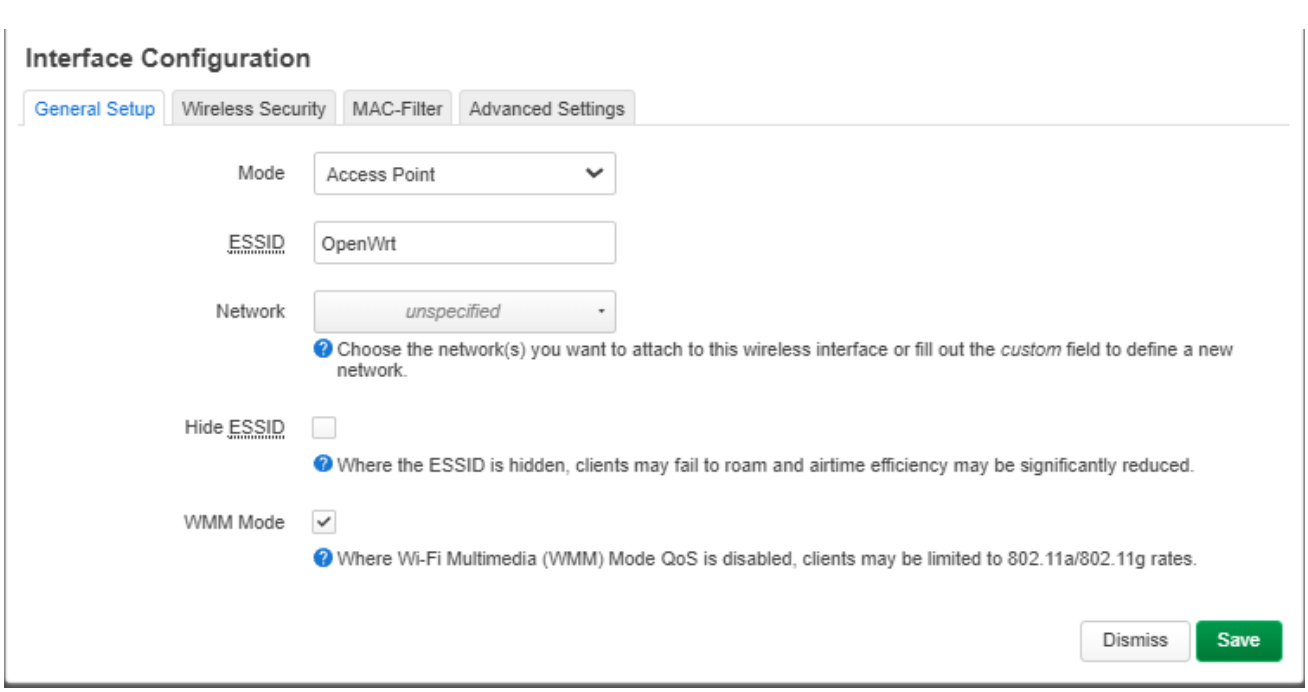


Fig 6: Wi-Fi Configuration Screen.

3. The "ESSID" field currently has the default text of "OpenWrt". Edit that text to the desired name. This is the name that will show up when you are searching for Wi-Fi networks to connect to on your device. In this example, we are renaming it to "KNX IoT Hub 1".

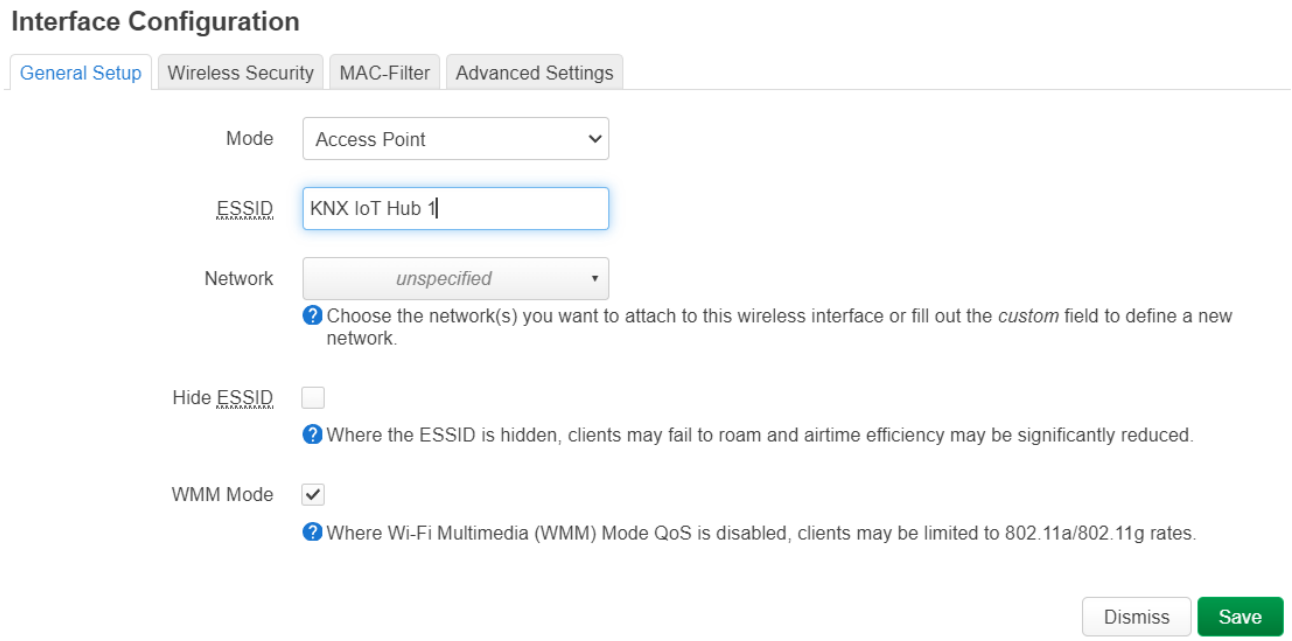


Fig 7: Naming the WiFi ESSID.

4. Next, click on the "Wireless Security" tab. You will find that at the moment no encryption is set.

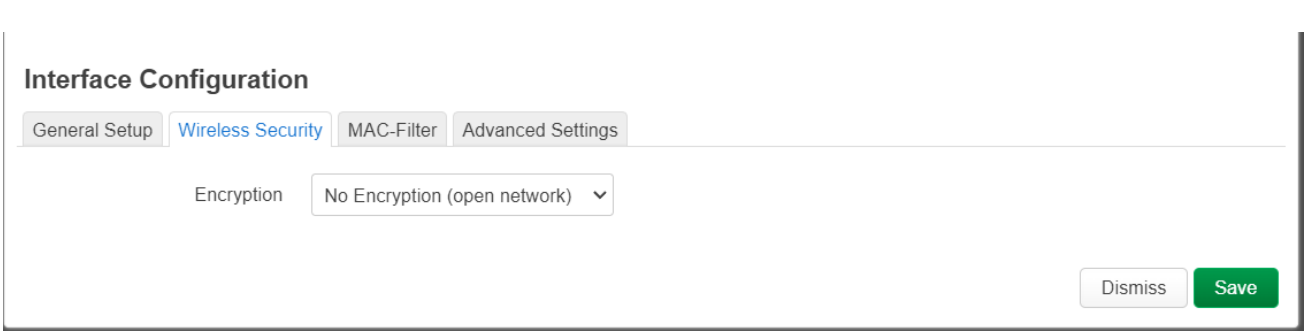


Fig 8: Wi-Fi Security.

5. Click on the dropdown, and select your encryption of choice. It is recommended to choose "WPA3-SAE", because it is the most secure. This will result in more input fields appearing below.

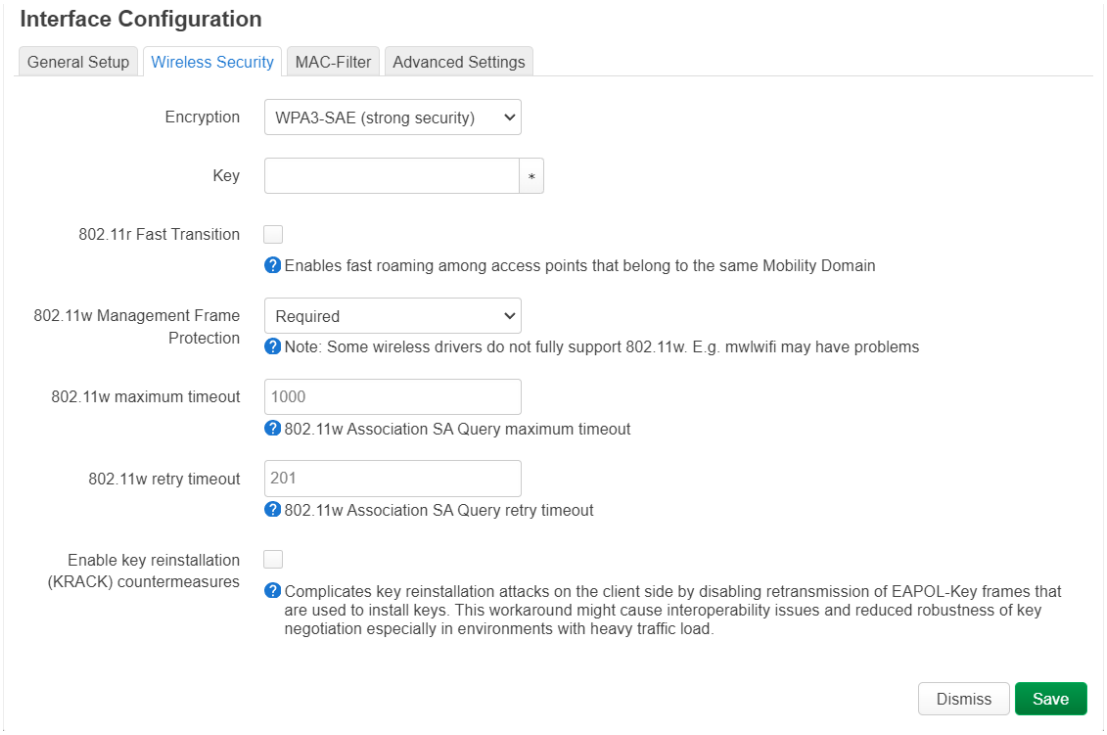


Fig 9: Enabling Wi-Fi Security.

Note that WPA3 might not be available when trying to connect to older computers or devices (built before 2020). In this case WPA2-PSK should be used.

6. You should now set a "Key". This is the Wi-Fi password that a new device would have to enter in order to join the Wi-Fi network.

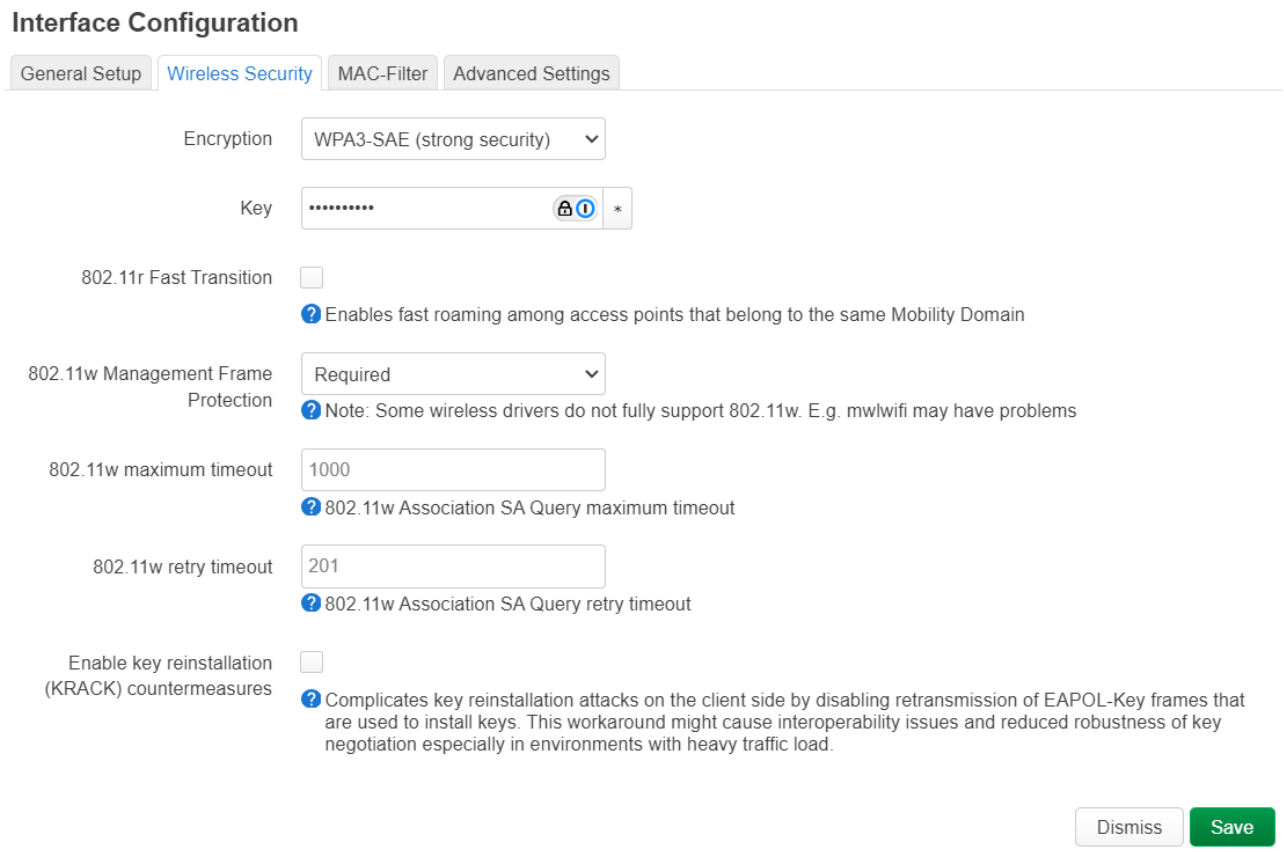


Fig 10: Supplying Wi-Fi Key.

7. Click "Save" to save all the changes you have made. This will close the popup window.

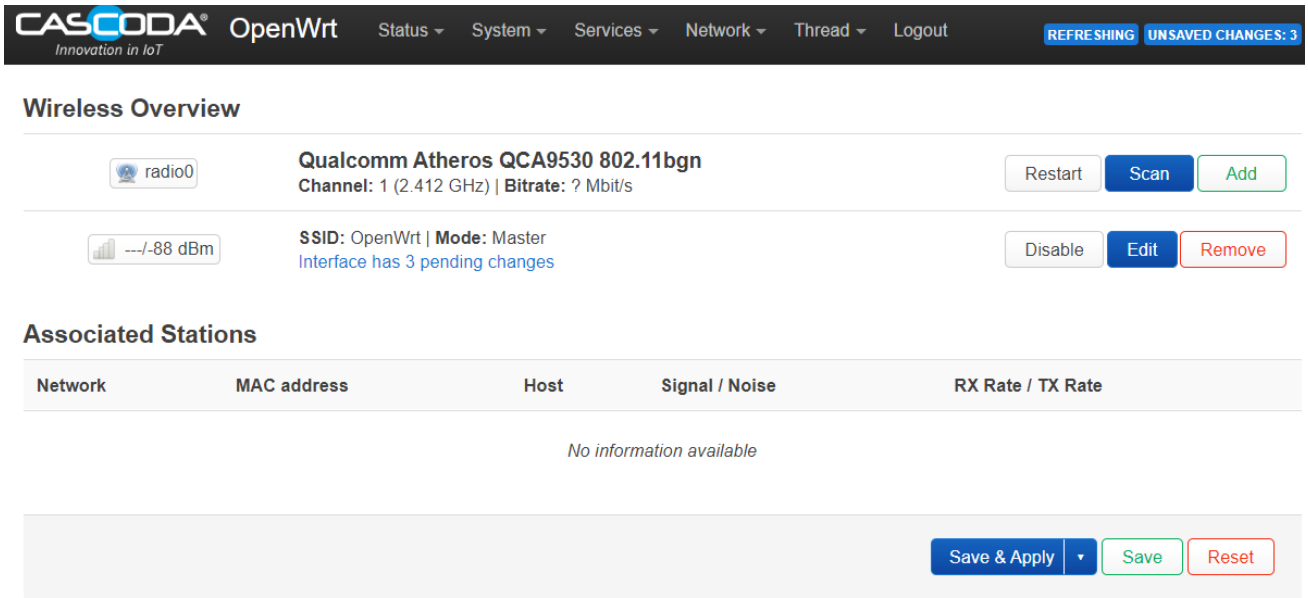


Fig 11: Save Wi-Fi Settings.

8. On the top right corner of the screen, you will notice there is a box with text that says "UNSAVED CHANGES: 3". This means your changes haven't yet been applied. Click on that box, and another window will pop up.

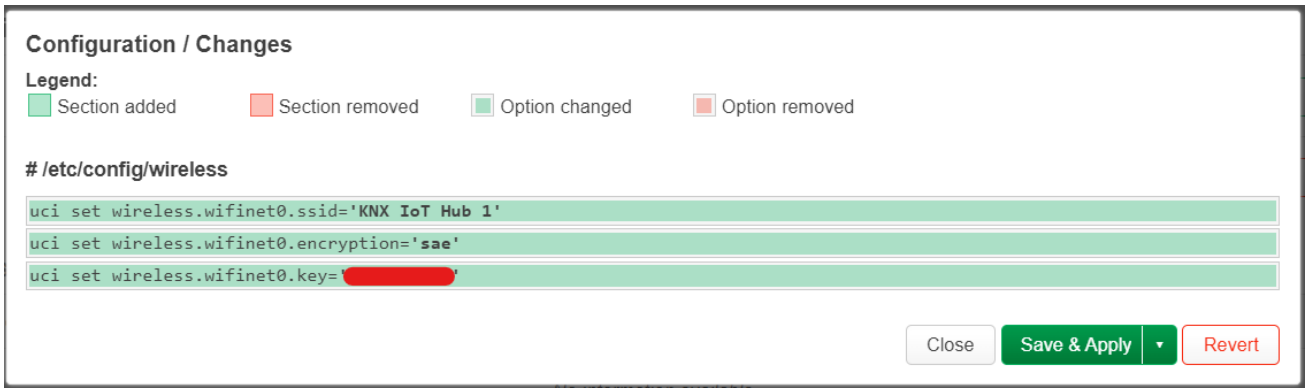


Fig 12: Save and Apply Wi-Fi Settings.

9. Review the changes, and click on "Save & Apply".

10. If you made those changes using a device that was connected to the hub via the once-open "OpenWrt" Wi-Fi access point, it is normal that you have now been disconnected. You need to reconnect to the Wi-Fi network using the new details (new name, and password), and then you can login to the Hub again in the usual way.

5.3.2. Wireless link to the Internet

Instead of using wired Internet access, you may set up the KNX IoT Hub™ to join a pre-existing Wi-Fi hotspot. Connect your computer to the Hub's "PoE LAN1" Ethernet port, and [follow OpenWRT's guide on connecting to a Client Wi-Fi network](#).

Fig 13: Hub connected via Wi-Fi.

5.4. Bridging the Ethernet ports

In the factory configuration, the KNX IoT Hub™ operates akin to a residential IP Router. The LAN1 port must connect to your local network, and the LAN2/WAN must connect to the Internet. In this configuration, messages are routed between these separate networks. There is a firewall blocking certain access, and unsolicited inbound requests are blocked on the WAN interface.

If this is not desired, you may bridge the two Ethernet ports together by converting the device to a switch. This is referred to as **Switch Mode** for the Hub. This configuration bridges the two networks together, as if they were one single larger network. An external router is required for routing, if desired. With no external router, communications will only be possible using link-local addresses.

The drawback of **Switch Mode** is that the Hub will no longer have a static IP address. To access the Web GUI, you will need to use either the hostname, or you must obtain the Hub's IP Address from your router's administration GUI.

As an example, the following diagram shows a network configuration with the KNX IoT Hub™ operating in **Switch Mode**. The advantage of **Switch Mode** is that both Computer 1 and Computer 2 can access the Web GUI on the Hub. Additionally, as there is no more firewall, Computer 1 and Computer 2 can talk directly to each other as if they are both connected to the Internet Router.

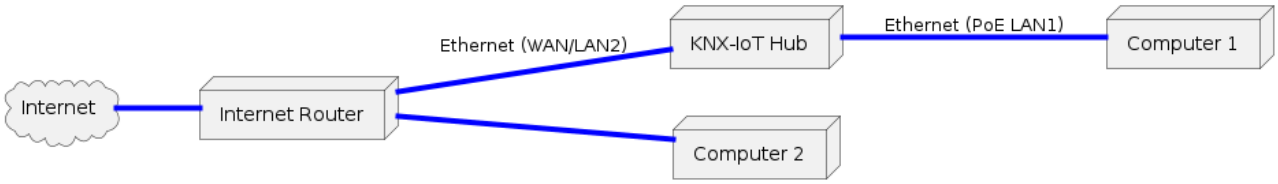


Fig 14: Hub connected in Switch Mode.

The **Switch Mode** configuration additionally allows you to daisy-chain several KNX IoT Hubs™ together, simplifying the installation of larger networks.

Here is how you can convert a device to **Router Mode** or **Switch Mode**:

1. Hover over "Network" in the menu bar and then click on "Device Type".
2. Press the "Convert to **Router Mode**" or "Convert to **Switch Mode**" button according to the desired configuration.
3. The device will either reboot and apply the configuration, or show that the desired configuration is already in effect.

   NOTE! Border Routers in **Switch Mode** allocate ULAs to devices on the local network, so that those devices can send routeable Thread frames. Hence **AVOID** using Border routers in **Switching Mode** and **Routing Mode** in 1 network.

5.5. Updating the firmware

Download the latest KNX IoT Hub™ image and update the firmware on the hub by navigating to "System - Backup/Flash Firmware" and uploading the firmware image using the "Flash image..." button near the bottom of the page.

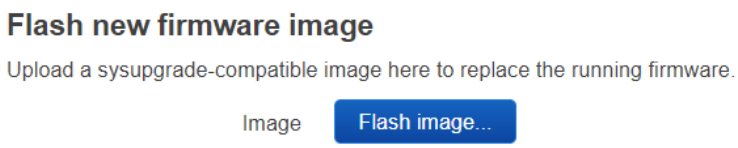


Fig 15: Firmware update.

5.6. Device protection

5.6.1. Password Protection

The website of the Hub can be protected for unauthorized access by a password. The system password can be set by navigating to "System - Administration" using the "Router Password" Tab. This tab allows to set the administrator (root) password.

5.6.2. SSH Access

The SSH can be set by navigating to "System - Administration" using the "SSH Access" Tab.

The SSH login can be configured or even be removed. when the userid/password is set for logging into the Hub website, the root password is then also set for logging into the system by SSH.

6. KNX IoT Hub as a Thread Border Router

The KNX IoT Hub is equipped with an IEEE 802.15.4 interface, and runs the Thread stack. It is set up as a Thread Border Router, and is therefore capable of routing IPv6 traffic between the Thread network and the adjacent Ethernet network and hosted Wi-Fi access point. Below is a diagram showing a typical network topology:

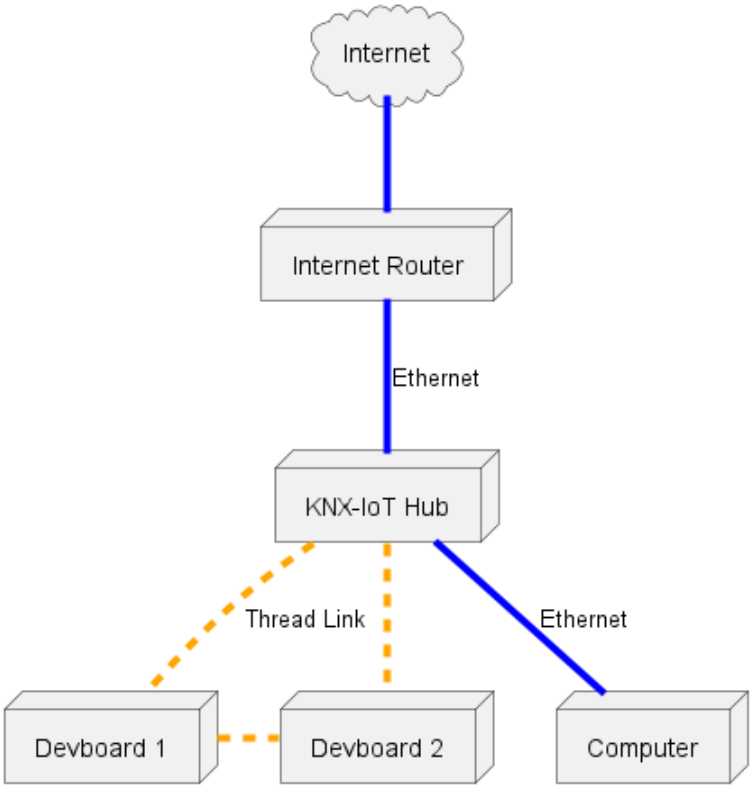


Fig 16: Typical Network Diagram with a Thread network.

The Thread network can be controlled and managed using the Web UI, making it possible to

create Thread networks, scan channels, commission devices onto the Thread network, and visualise the network topology.

6.1. Creating a Thread network

6.1.1. Thread network formation

The very first device on a Thread Network must "form" it, before any other nodes are able to join and participate in it. The formation of a network includes selecting a network name and channel, setting the admin password (aka Network Passphrase or Commissioning Credential) generating a network key, extended PANID and PANID. This then becomes the active operational dataset of the network, and is shared between every node participating in the network.

The Thread network formation procedure only needs to be executed once for any given network. Once the network is formed, additional nodes can join the network, and be provided with the active operational dataset by following the commissioning process. If the network parameters need to be changed, then a commissioner can be used in order to reconfigure the active dataset.

To create a Thread network using the KNX IoT Hub's Border Router interface, follow the steps below:

1. Login to your hub, as described previously in this document.
2. Hover over "Thread" in the menu bar at the top, and click on "Overview".
3. Click on the "Create".
4. If you have some Thread knowledge, edit any of the fields to your liking. Otherwise, you can use the default values. Perhaps the most important decision to make at this stage, is which channel you want your Thread network to be on, which you can edit by clicking on "Advanced Settings" and modifying the input text field for "Channel". See this next section on how to select the best channel for your Thread network if you want to do that now, otherwise proceed with the default channel.

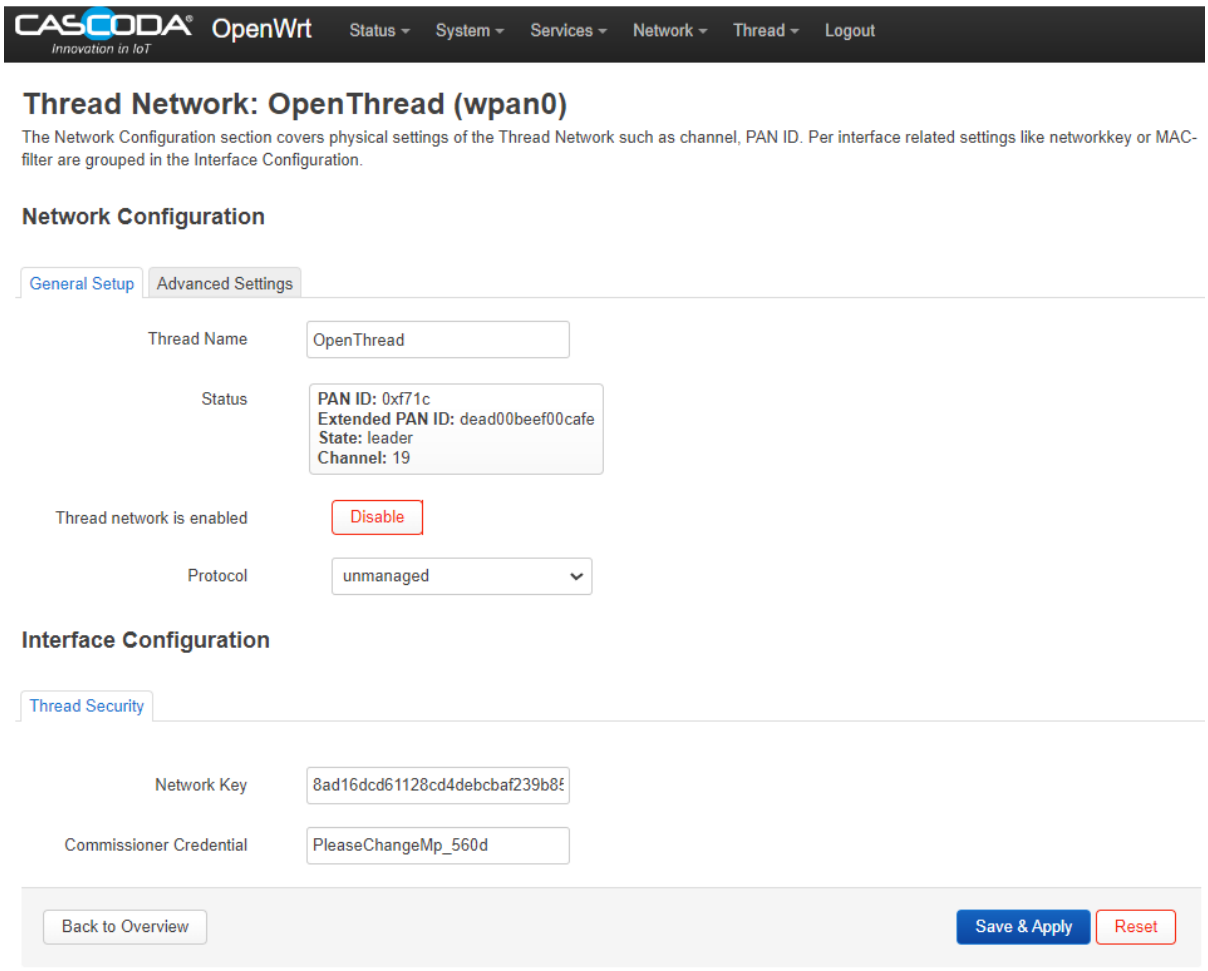


Fig 17: Creating the Thread Network.

5. Scroll down to the bottom and click on "Save & Apply".

6. Your Thread network should now be visible under "Thread - Overview"!

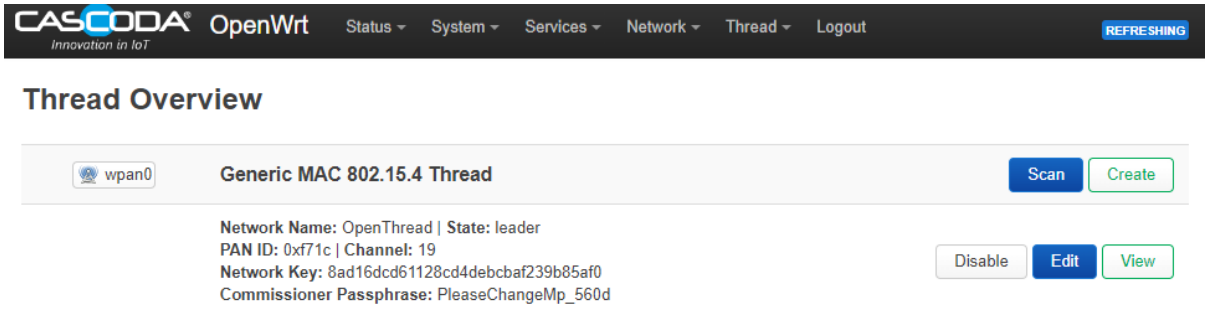


Fig 18: Thread Network overview.

6.1.2. Selecting the best channel for your Thread network

6.1.2.1. Background information

Both Wi-Fi and Thread operate in the 2.4 Hhz range, so they can interfere with each other. In Thread there are 16 channels, 11 to 26. Channel 26 is not recognised globally, so we advise against choosing this channel. Below is a graph illustrating how the Wi-Fi and Thread channels overlap and interfere.

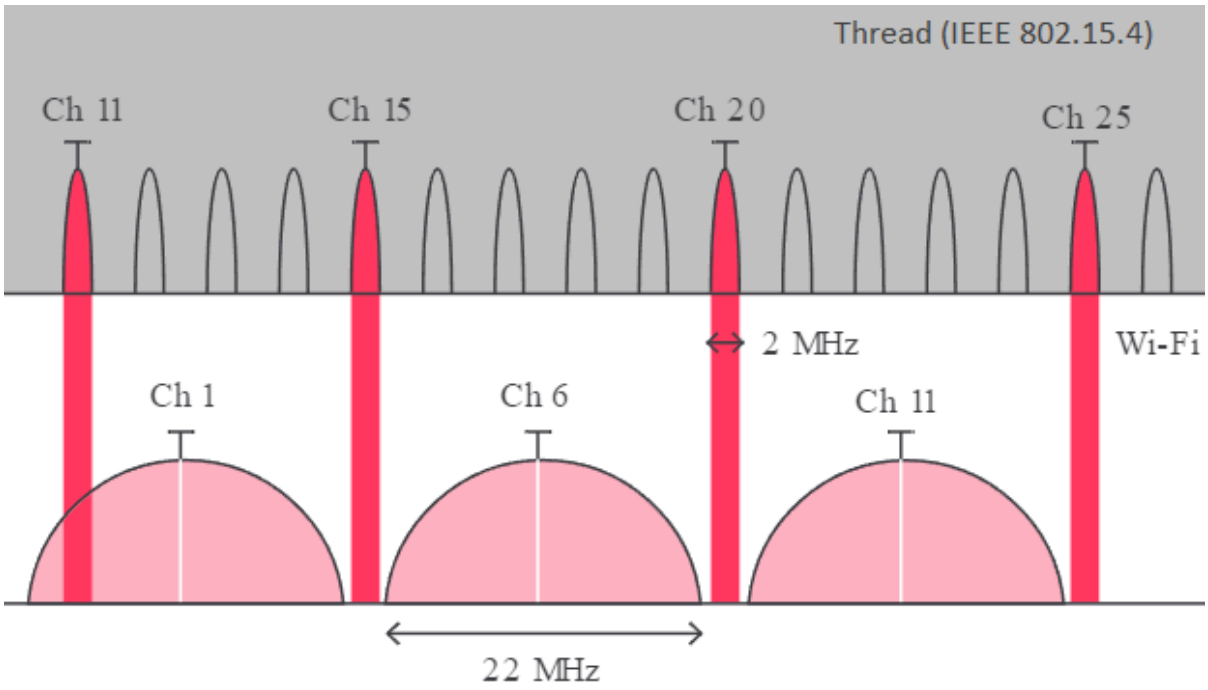
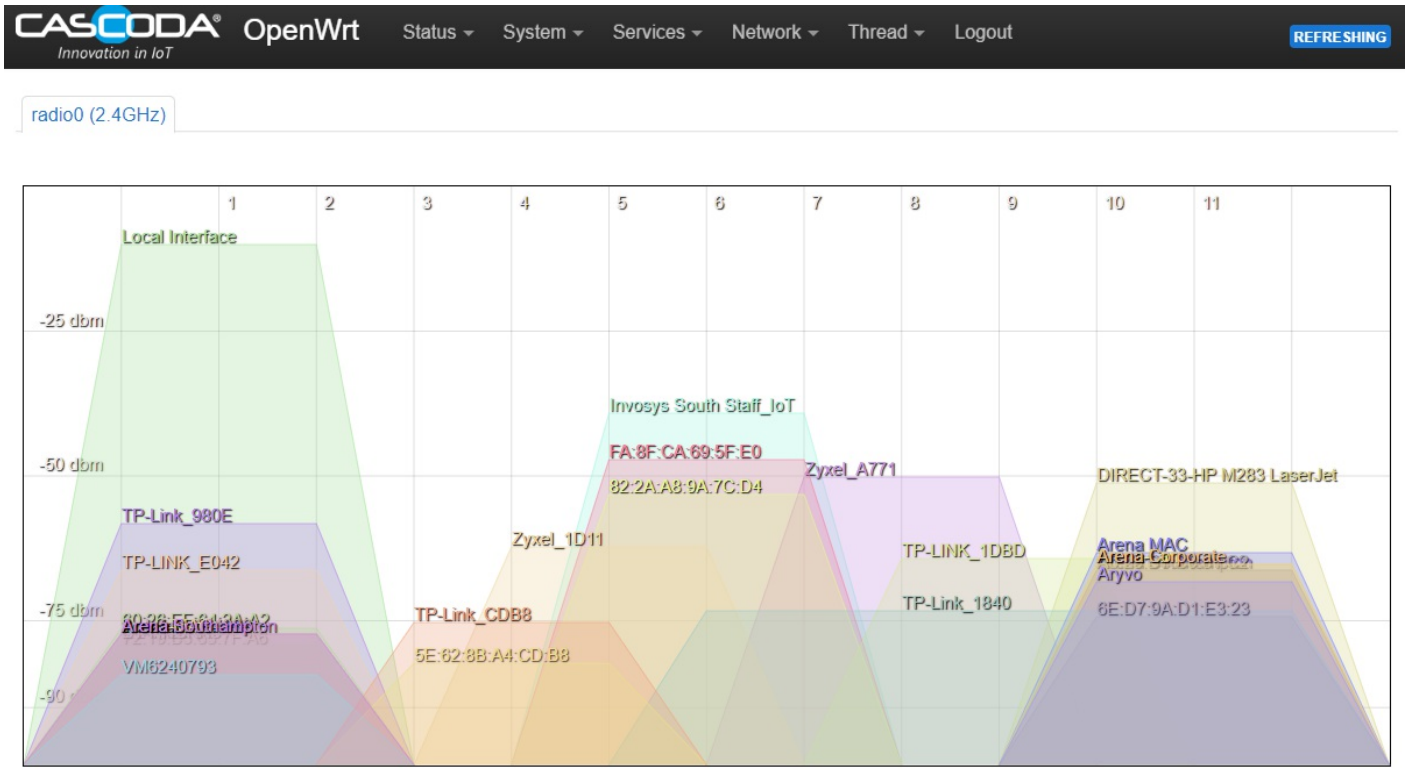


Fig 19: Thread Channels.

From the graph, you can see that in general the best Thread channels to pick are channels 11, 15, 20, and 25, because they fall within the troughs of the Wi-Fi channels occupancy.

6.1.2.2. Channel analysis

The KNX IoT Hub has a feature allowing us to view in real-time all the Wi-Fi networks and how they are occupying the different channels. Hover over "Status" on the top menu bar, and click on "Channel Analysis". The graph will take a few seconds to load. Once it loads, you will be able to see the different Wi-Fi access points, which channel they are occupying, and how strong the signal strength is. The graph updates every few seconds.



Signal	SSID	Channel	Channel Width	Mode	BSSID
-10 dBm	Local Interface	1	20 MHz	Master	00:C0:CA:B2:11:3A
-39 dBm	Invosys South Staff_IoT	6	20 MHz (40 MHz Intolerant)	Master	80:2A:A8:9A:7C:D4
-47 dBm	*hidden*	6	20 MHz	Master	FA:8F:CA:69:5F:E0

Fig 20: Example of Wi-Fi Channels.

You will notice that some areas are less dense than others. It is best to pick a Thread channel which lines up with those less dense areas. As shown in the graph previously, this will usually be channels 15, 20, and 25. Channel 15 is usually especially good, because it falls between Wi-Fi's channel 1 and channel 6.

Once you have determined the best Thread channel to use in terms of Wi-Fi interference, you can select that channel when you are creating your Thread network.

6.2. Commissioning devices to a Thread Network

In a Thread network, all communication is secured by a network-wide key. Without that key, a device cannot participate in the network. The network also has other parameters that must be consistent and can be configured, such as the extended PAN ID, admin password, channel and network name.

In Thread, the Commissioner is the user-controlled admin interface to the Thread network. The primary purpose of the Commissioner is to add new devices to the network by securely provisioning them with the network credentials. It can also be used to modify the network parameters safely after the network is formed. Multiple commissioners can control a Thread Network, but only one can be active at a time. The KNX IoT Hub, using its Thread Border Router functionality, can act as a Thread Commissioner.

The following instructions assume that you have already created a Thread network, as described previously in this document. To commission a new device onto that Thread network, first navigate to "Thread - Add Device" on the menu bar. On the page that loads, you will notice that there are two ways of entering your joiner credentials: either through QR Code Entry or Manual Entry.

6.2.1. QR code entry

1. Obtain the QR Code of your device. For e-paper products, it will be available in the "QR Code" menu. For other products, please check the casing, packaging, or installation/user manual.
2. Use a QR Code scanner to scan the QR Code into the input field, or alternatively use your computer's Webcam to scan the QR Code. NOTE: Using the webcam requires secure access, so you will have to connect to the border router via the https:// endpoint.

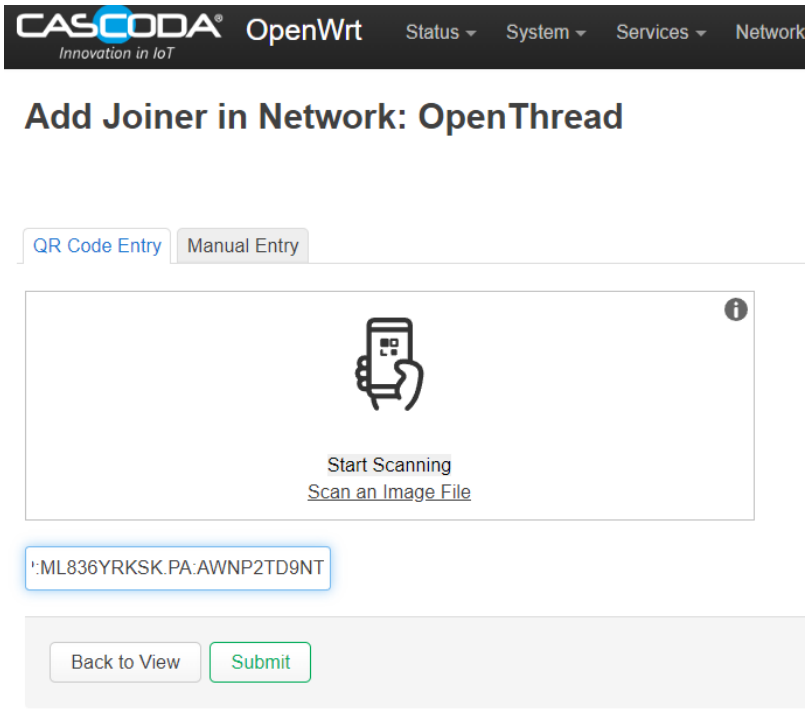


Fig 21: QR entry.

3. Press "Submit" to start the commissioning procedure and wait for the commissioning to complete. If this device is a direct neighbor to the hub, which would be the case if this is the first device that you are commissioning to the network, then you will see it show up in the "Neighbors" table. NOTE: There is a way to view the entire Thread network topology, including all devices that are not direct neighbors to the hub. This is shown in this section.

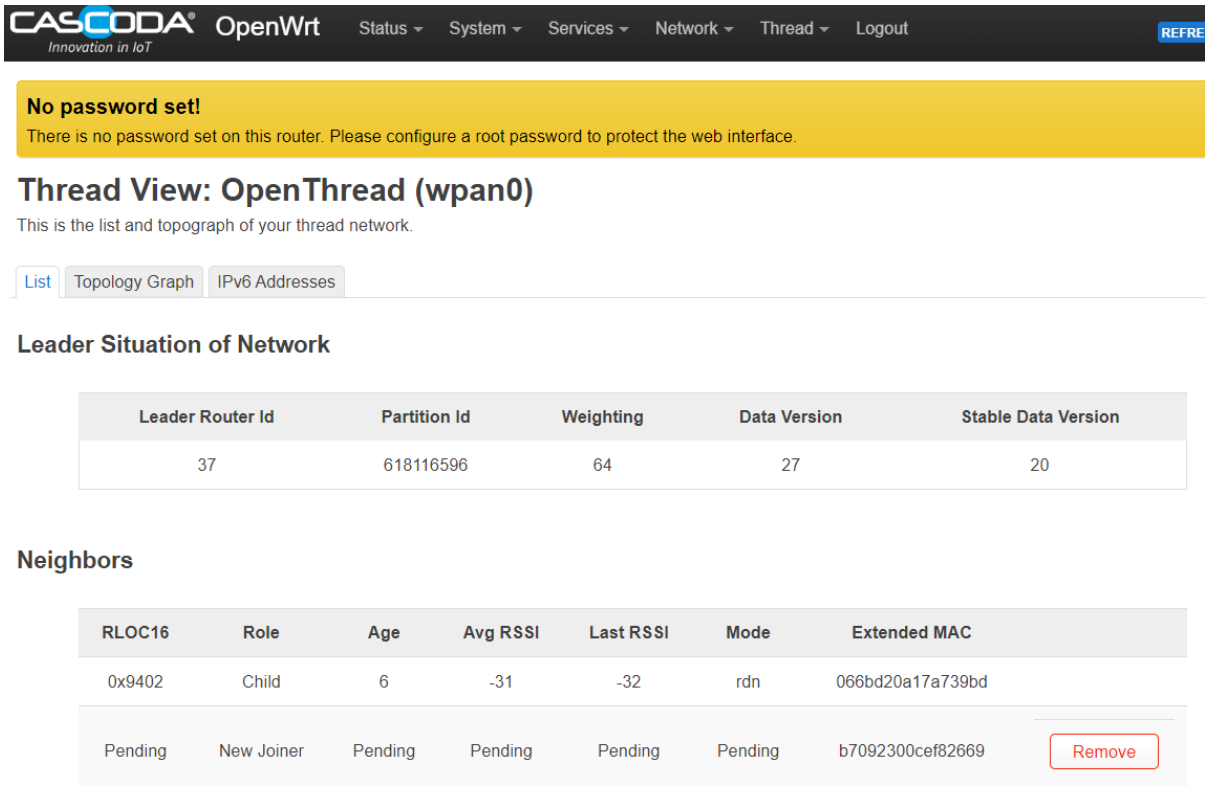


Fig 22: Thread Overview with Joiners.

6.2.2. Manual entry

NOTE! This method is more difficult, because you will have to acquire the joiner credentials, which is outside the scope of this guide. We always provide QR codes for our products, so commissioning with manual entry most likely won't be necessary. However, the option is available in case it is needed.

1. Navigate to the "Manual Entry" tab and enter the Network Passphrase/Admin Password and the Joiner Credential.

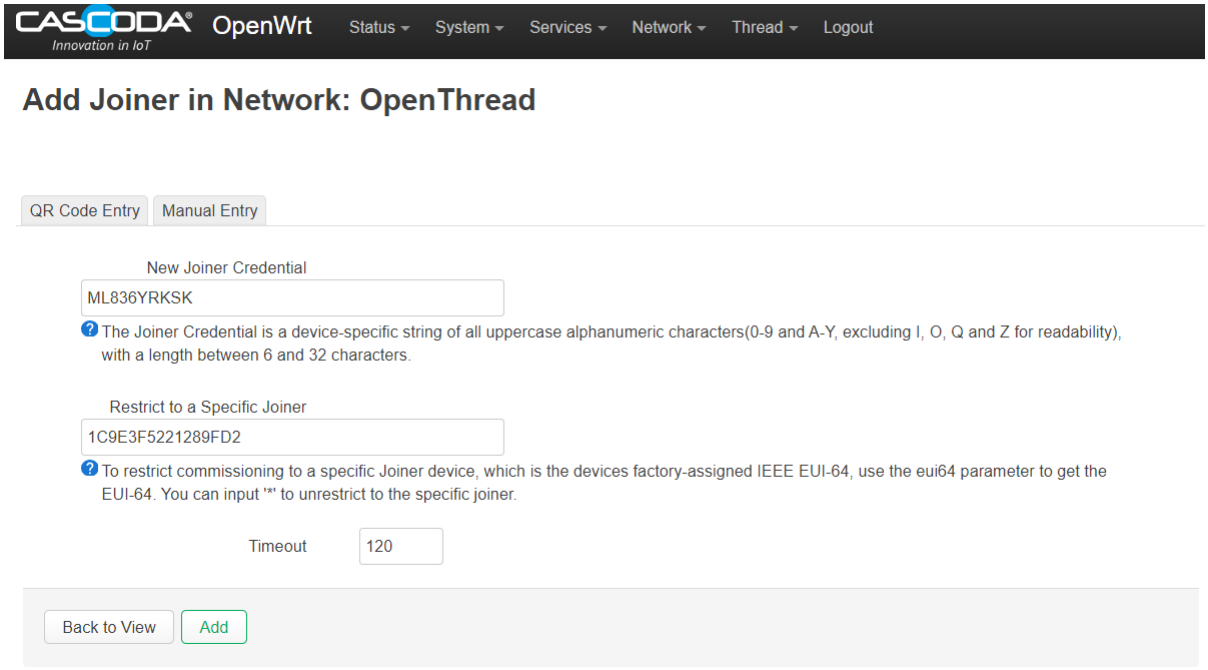


Fig 23: Manual entry for adding a Joiner.

2. Click "Add", and the commissioning process should begin. If this device is a direct neighbor to the hub, which would be the case if this is the first device that you are commissioning to the network, then you will see it show up in the "Neighbors" table. NOTE: There is a way to view the entire Thread network topology, including all devices that are not direct neighbors to the hub. This is shown in this section.

6.3. Thread network visualization and information

By navigating to "Thread - View", you access a page that allows you to view information about the Thread network and the devices that make it up. There are three tabs, each of which will be shown below, with an example network topology. Those three tabs are "List", "Topology Graph", and "IPv6 Addresses".

The topology that has been formed for demonstration purposes consists of the KNX IoT Hub (acting as a Border Router), three end devices, and two routing devices.

6.3.1. Topology Graph

Once on the "Thread - View" page, click on the "Topology Graph" tab. This allows you to view the exact current links between all Thread devices, updated in real time, with a slight delay (up to 10 seconds).

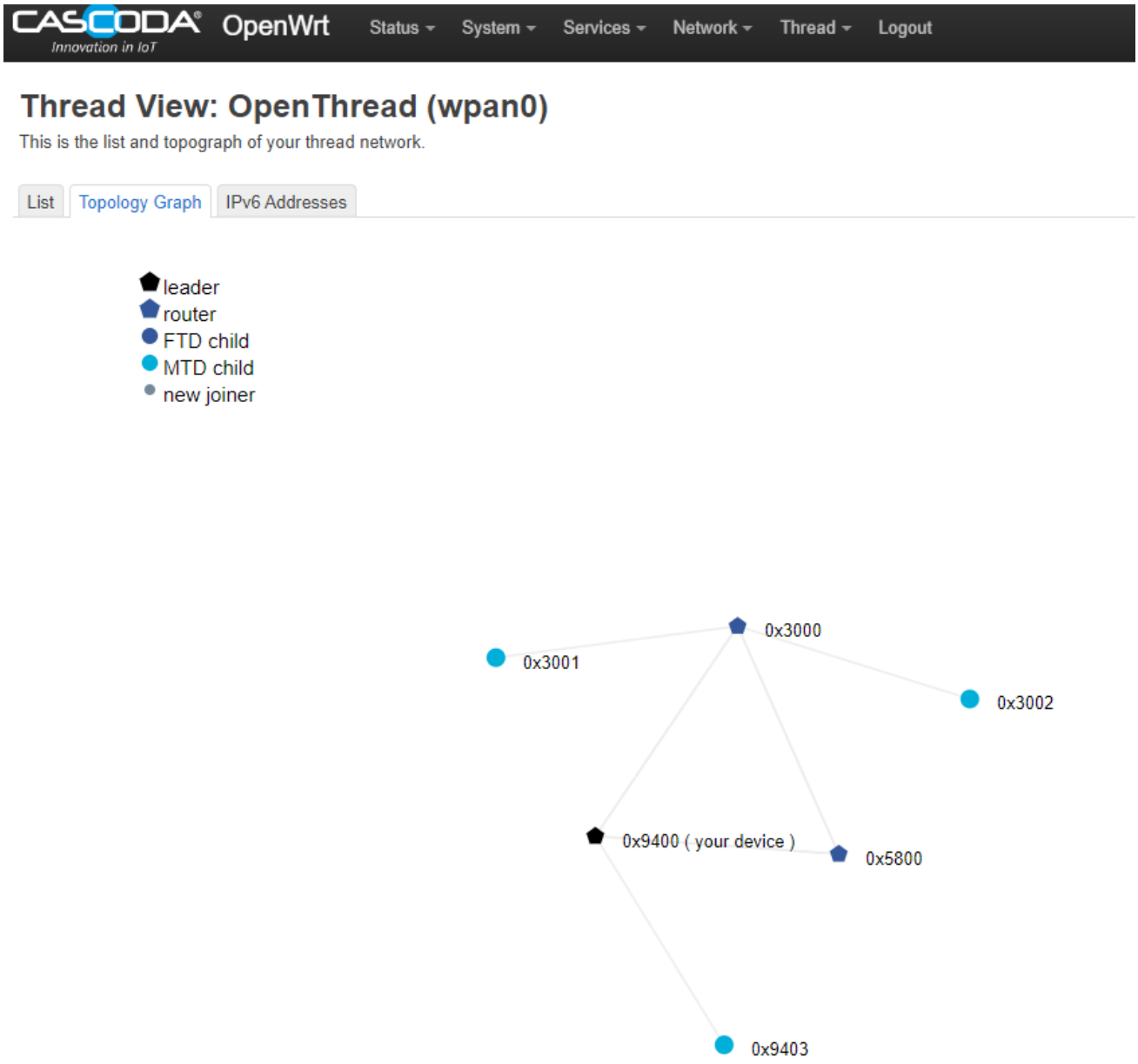


Fig 24: Thread Topology Graph.

6.3.2. Neighbor Table

Click on the "List" tab in order to view the neighbor table of the Border Router. Listed are all of the devices that have a *direct* link to the Border Router (so notice that not all devices that are shown in the Topology Graph are listed in that table).

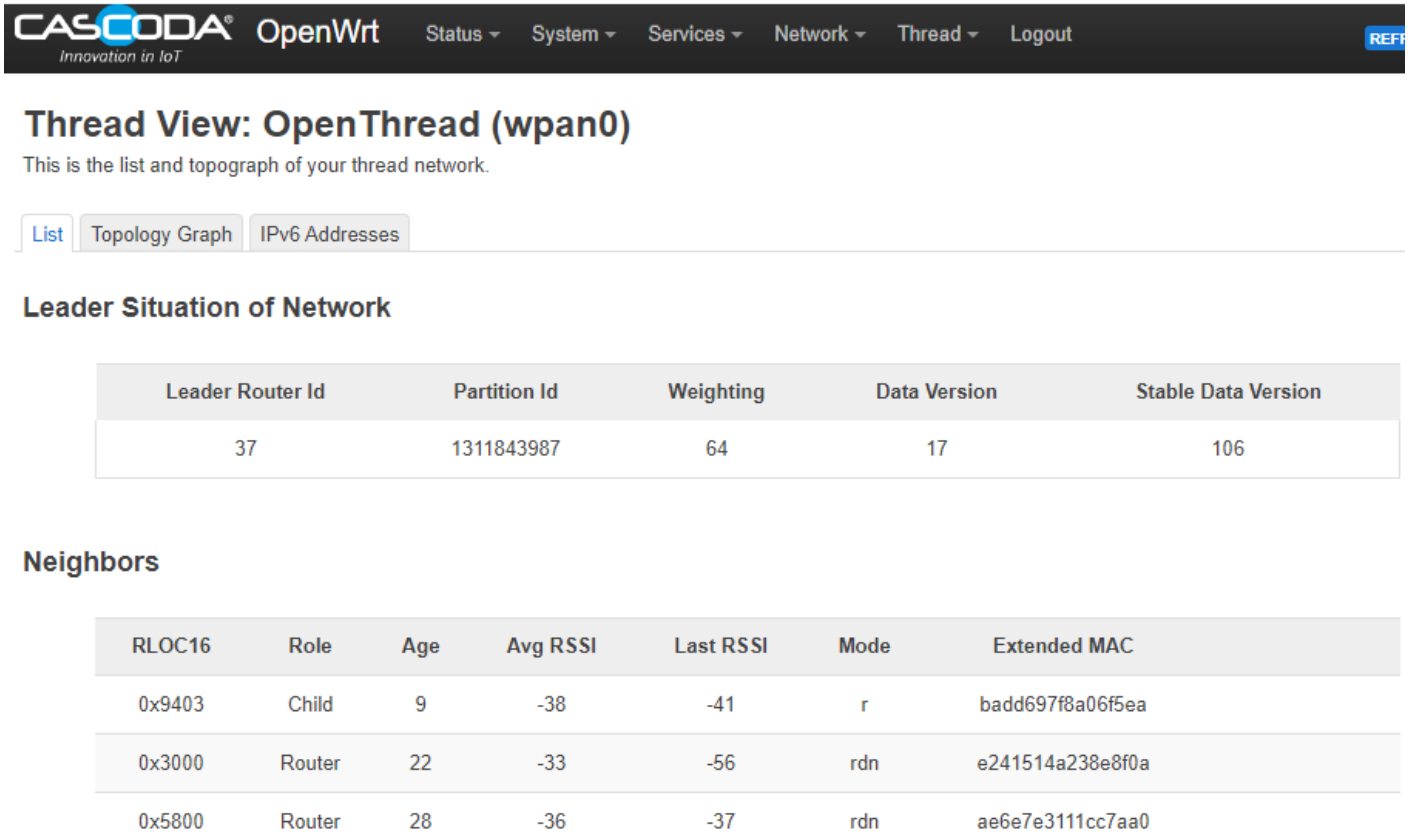


Fig 25: Thread Neighbor Table.

One very useful feature of the neighbor table, is that it shows the average RSSI, as well as the last RSSI for the device on that row. RSSI stands for Received Signal Strength Indicator, and it is a measure of the power present in the received radio signal. So by looking at this value, you are able to determine how good the signal strength is between the Hub and this particular device. The higher the number (closer to 0) the better, and as a rule of thumb, see the table below for an indication of how to interpret the values.

RSSI	Signal Strength
> -70 dBm	Excellent
-70 dBm to -85 dBm	Good
-86 dBm to -100 dBm	Fair
< -100 dBm	Poor
-110 dBm	No signal

Fig 26: RSSI overview.

6.3.3. IPv6 Addresses

Click on the "IPv6 Addresses" tab in order to view a table of all the Router devices, and their IPv6 addresses. Note that only router devices are shown in this table (so notice that not all devices that are shown in the Topology Graph are listed in that table).

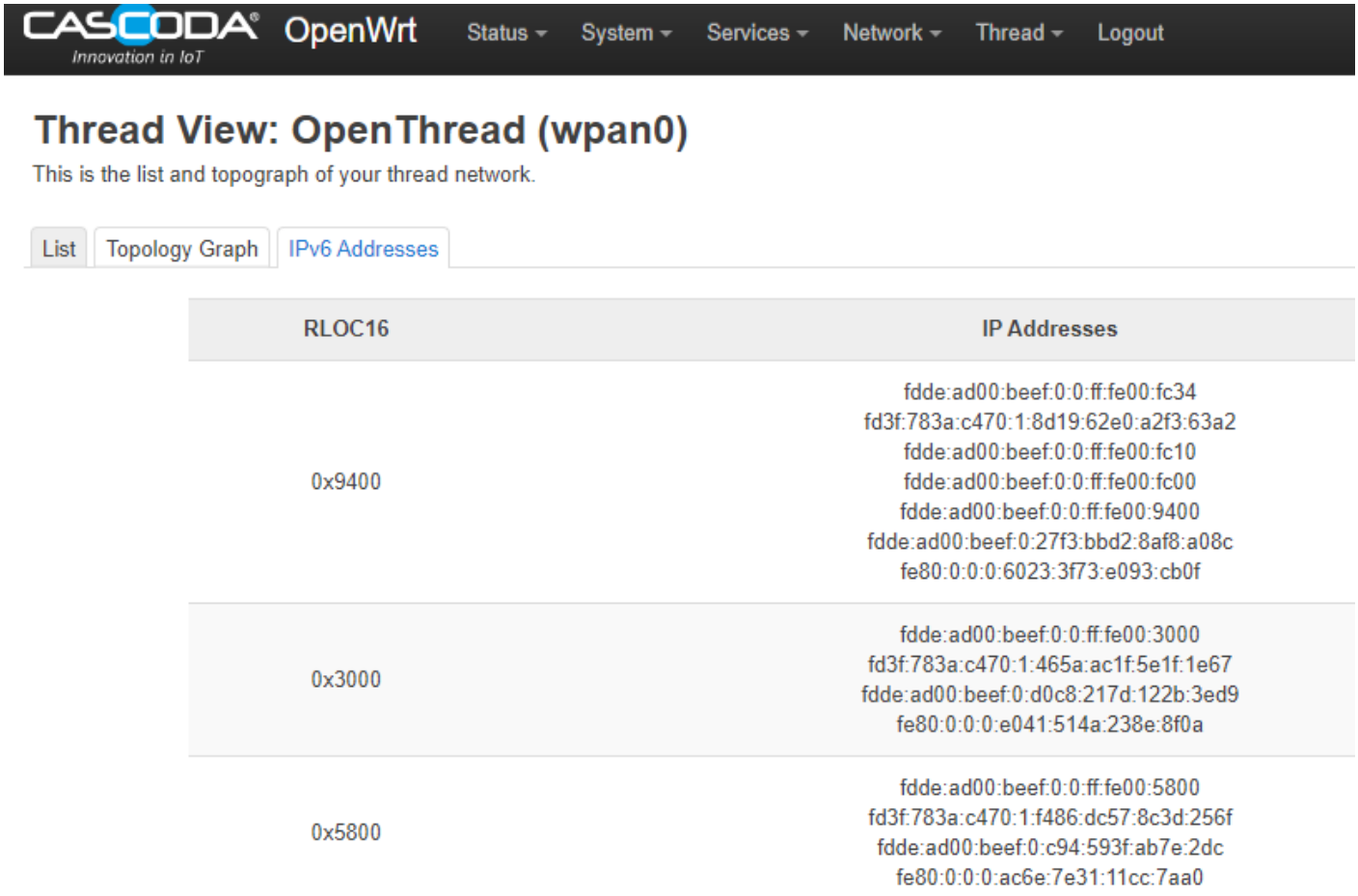


Fig 27: IPV6 address overview.

6.4. Rebooting

> **NOTE!** This is not part of the setup. This section is included for informational purposes.

To reboot the KNX IoT Hub, hover over "System" and click on "Reboot". This will take you to a screen asking you to confirm, click on "Perform reboot", then wait for the device to finish rebooting.

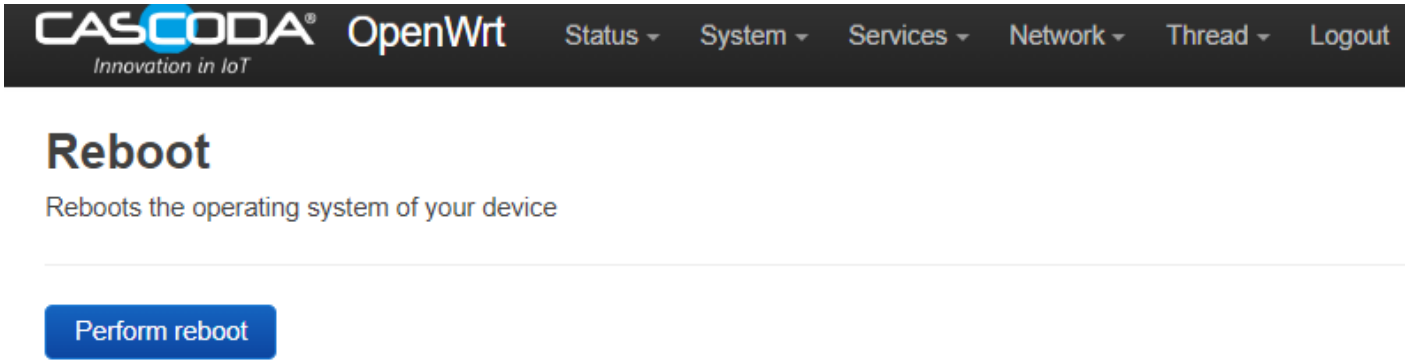


Fig 28: Reboot Screen.

6.4.1. Troubleshooting

6.4.1.1. Thread device does not join the Thread network

If the device does not join after two minutes, you may need to restart the Border Agent. To do so, navigate to "System - Startup", scroll down until you find "otbr-agent", then press "Restart". Once the restart is completed, try commissioning the device again.

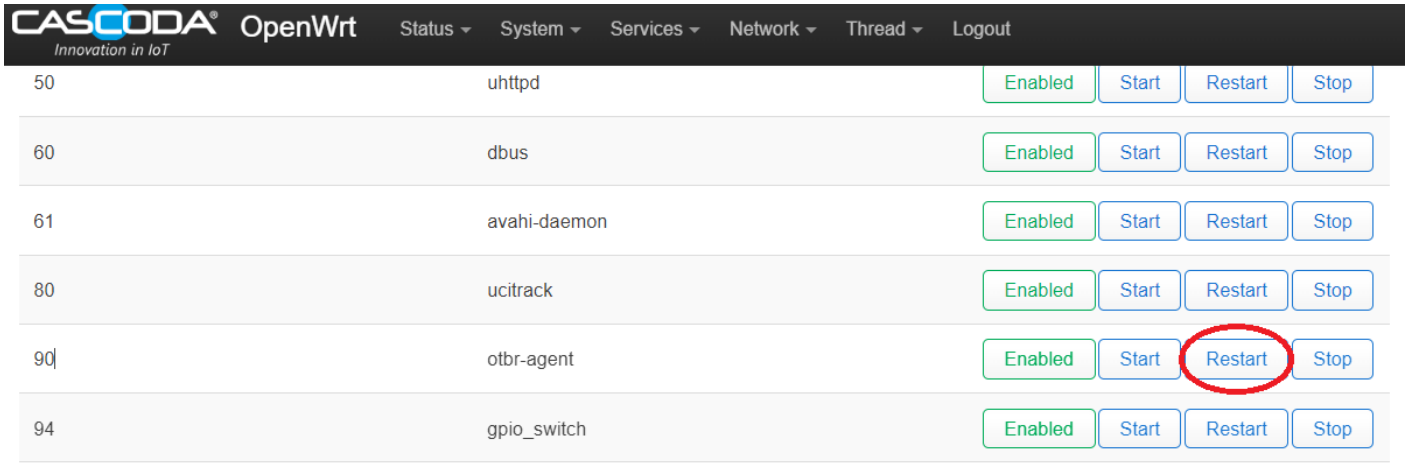


Fig 29: Restart service.

6.4.1.2. KNX IoT device is still listed but I have factory reset it

The discovery mechanism for KNX IoT is based on mDNS. When the device is factory reset, the mDNS service is NOT informed, e.g. the reset is executed out of bound. Hence the Hub still thinks the KNX IoT device is still on the network. The solution is to wipe the mDNS cache. This can be done by navigation to the "Thread - Overview" page and press the "Reset MDNS" button.

6.4.1.3. Troubleshooting failed downloads

Failed downloads can be caused by the IPv6 addresses allocated to the Hub by the upstream router. Please attempt the following steps:

1. Navigate to Network -> Interfaces.
2. Find the WAN6 Interface within the list, and press the corresponding "Edit" button.
3. Navigate to the Advanced Settings tab, uncheck "Delegate IPv6 prefixes" and set "IPv6 assignment length" to "disabled".
4. Press Save, then press Save and Apply
5. Restart the KNX IoT Hub and ETS.

If you are still having difficulties completing a download, you can additionally unplug any upstream Ethernet cables connected to the WAN interface, to ensure no global IPv6 addresses are allocated to the Hub.

6.4.1.4. Troubleshooting TP to IOT routing

IP to IOT routing failures can be caused by the IPv6 addresses allocated to the Hub by the upstream router.

For example Border Routers in **Switch Mode** allocate ULAs to devices on the local network, so that those devices can send routeable Thread frames. These addresses come from the prefix visible in Network -> Interfaces -> Global Network Options

Fig 30: Global network options.

A second border router attached to the same network (in **Router Mode**) will see this prefix and assign itself as a downstream router of that prefix, on the WAN interface. The problem is that in the default network configuration the router will also allocate an address matching that prefix on the LAN interface, which cannot be used to communicate to the Thread

network. Occasionally the KNX-IoT Router picks this incorrect address to talk to the Thread network, resulting in breakdown of communication from TP to IoT.

If a KNX IoT Router is not forwarding messages from the TP side to the Thread network, follow the following steps:

1. Navigate to Network -> Interfaces and click the Global network options tab. Make a note of the IPV6 ULA prefix, as you will be comparing it to other addresses.
2. Press the Interfaces tab and look at the addresses on the LAN interface. Ensure that all of the IPV6 addresses on this interface are either global (start with 2xxx:xxxx...) or ULAs with 1. the prefix written down in step 1

If you see any ULAs with a different prefix, the routing can be fixed by not delegating the ULA prefix:

1. Press Edit on the WAN6 interface lower down and navigate to Advanced Settings
2. Uncheck "Delegate IPV6 prefixes"
3. Press Save, then press Save and Apply at the bottom

7. Software Bill of Materials

This paragraph contains the list of used open source software in this product.

Name	Version	License
Cascoda OpenWrt	v.1.10	GPL-2.0
Cascoda SDK	0.25	BSD-3-Clause
tinycbor	v0.6.0	MIT
mbedtls	2.16.2	Apache-2.0
Openthread	knx-v1.0.0	BSD-3-Clause

Table 6: *List of Open Source*

7.1. Cascoda OpenWrt

- Description: Cascoda OpenWRT
- License: GPL-2.0
- Version: v1.10 (or later)
- URL: https://github.com/Cascoda/OpenWrt
- Notes: OpenWrt port for the KNX IoT Hub

7.2. Cascoda SDK

- Description: Cascoda development

- License: BSD-3-Clause
- Version: 0.25
- URL: https://github.com/Cascoda/cascoda-sdk
- Notes: Chili2D/S SDK, various drivers

7.3. tinycbor

- Description: CBOR implementation
- License: MIT
- Version: v0.6.0
- URL: https://github.com/intel/tinycbor
- Notes: used for CBOR encoding/decoding

7.4. mbedtls

- Description: security constructs
- License: Apache-2.0
- Version: 2.16.2
- URL: https://github.com/ARMmbed/mbedtls
- Notes: used for encryption/decryption

7.5. Openthread

- Description: OpenThread, IPv6
- License: BSD-3-Clause
- Version: knx-v1.0.0
- URL: https://github.com/Cascoda/openthread
- Notes: Cascoda's port of OpenThread