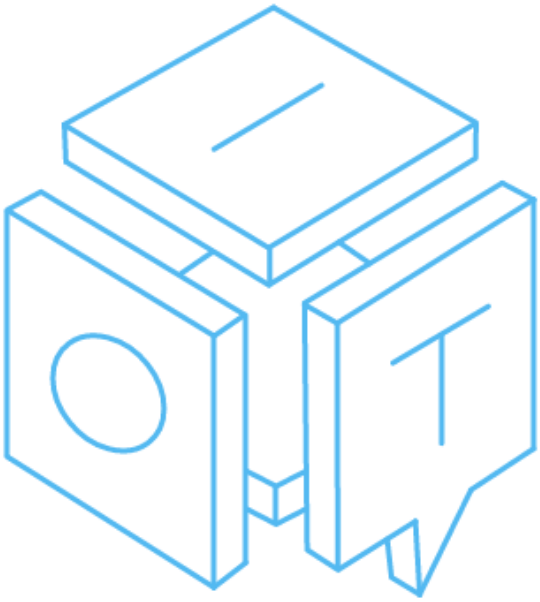
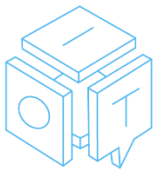
Installation quick guide

NB-IoT on the trial T-Mobile network





DOCUMENT PROPERTIES

CREATION DATE: 9-2-2017

LAST UPDATE: 14-3-17

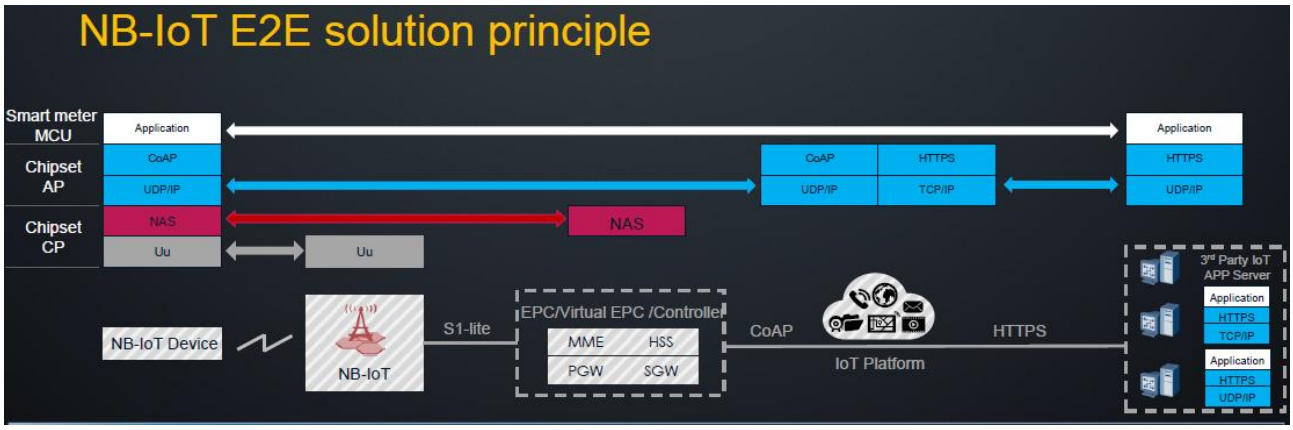
AUTHOR: ERIC BARTEN, THEES BRONS

Contents

Introduction to NB-IoT 4
Overview of the installation steps 5
Module commands 10
Security certificates for using the API 12

Introduction to NB-IoT

The picture below provides a high level overview of the network set-up of the T-Mobile IoT network:



It is important to understand that data transfer to and from the device does not happen directly. In between is the T-Mobile IoT platform, which provides an Application Programming Interface (API) towards end-user applications.

This means that in order to send data end-end, devices need to be registered on this IoT platform, and the type of application data needs to be defined.

This is different from a traditional M2M set-up, where the device receives an (internal) IP address from the network and a direct connection can be established.

Overview of the installation steps

This installation manual describes the steps necessary to connect to the trial IoT network of T-Mobile. As a prerequisite, it is assumed that the test set-up consists of the following elements:

> *Laptop/desktop with programmable board plus NB-IoT module connected to com port, with the test SIM-card from T-Mobile installed and located in area with NB-IoT coverage*
>
> *(please contact T-Mobile for the latest coverage information or visit the Proefrit section on forum.things.nl).*
>
> *This quick guide only focuses on the software side of setting up an NB-IoT connection. Please review the documentation from your module manufacturer on how to connect the module to your programmable board (the pin layout of most modules is the same as current market models working on GPRS or 3G).*

High level steps:

- Retrieve the IMEI number of your device
- Set up Postman or another API program with the correct environment variables (certificates, app ID en app key)
- POST Login to API to retrieve access token
- POST Register device to create new device with IMEI and a name
- PUT Set device info to set manufacturer, devicetype and model of your device **(should be exactly the same as the manufacturer, devicetype and model in your device template in Ocean Connect!)**.
- Use the appropriate AT commands to establish a network attach (use SP8 Neul firmware)
- Use AT+NMGS=<length>,<data> to send your Hello World!
- GET device data history to retrieve your Hello World! via the API

The NB-IoT Trial network Github can be found on https://github.com/tmnl-iot/proefrit

Detailed steps

1. Use your com software to connect to the NEUL module (for example Qcom for Quectel modules).

2. Use the appropriate AT command to retrieve your device information, especially the IMEI number of your module is important for the IoT platform.

3. Use the appropriate AT commands to establish a network attach with the T-Mobile IoT network.

Specific information on module / modem set-up can be found in Chapter "Module commands"

4. Log in with your Ocean Connect credentials (provided by email) on https://160.44.193.219:8843/#/login

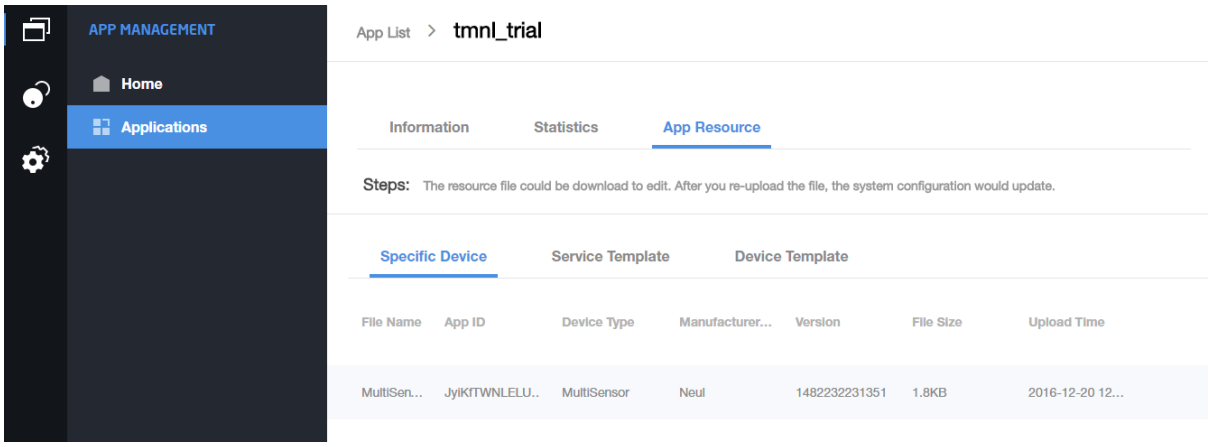
5. On your dashboard you will see two main menus: App management and Device Management.

6. Go to App Management > Applications and click on the default app that was created on your account (app name is nbiot_yourcompany).

7. Copy the different IP addresses that are needed in your set-up (see screenshot, needed in next steps):

   - Application Docking IP-address (not necessary, only when running own Ocean Connect instance)
   - Devices Docking IP-address (use this IP address in your AT commands)

8. Go to App Management > Applications > yourAppId > App Resource



9. In some cases there will be a service and device template which was already created for you (during workshop or other event), this will only transport RAW data from your device to the API.

10. If there is no template, you must upload your own device and service templates (for example to transfer different data types). Use the upload button to upload a zip file containing your service and device template (this zip file needs to contain the files devicetype-capability.json and servicetype-capability.json both in the appropriate folder). This will define which kind of devices you will use and which kind of data they will transmit.

    Please make sure that the filename is in the right format:
    devicetype_manufacturer_model.zip

    An example ZIP file can be found on the Github repository, in the folder /device templates.

    Specific details on how to create your own device and service templates can be found in Huawei IoT Platform Interworking Guide for NB-IoT.doc (available in the repository)

If your devices are able to make a network attach and send the raw data, the final steps are to retrieve this data via the North API.

In this quick guide we will show how this can be done by using the program Postman (download on https://www.getpostman.com/ , please use the program and not the Chrome plugin), which can be used to test and simulate your application talking to our API.

In the Github repository you can download our Postman collection and environment variables, with the example code.

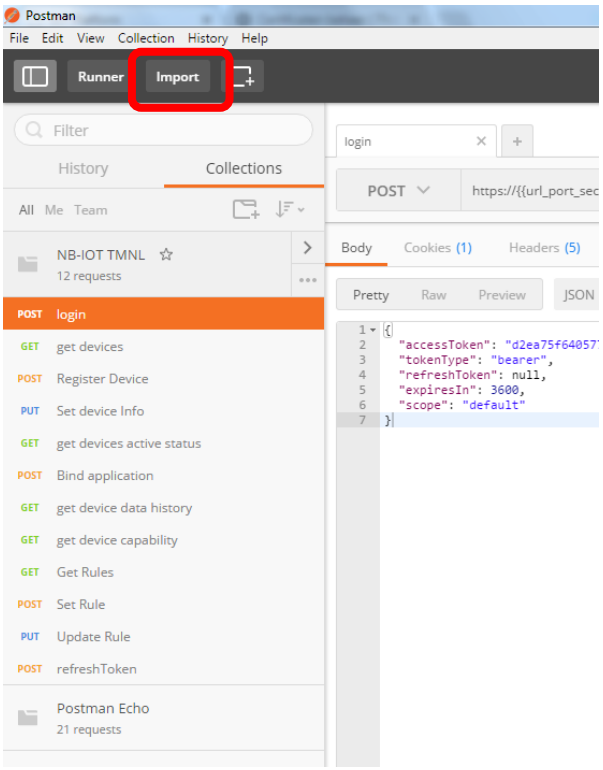
Postman can also convert this collection into for example Python or PHP scripts.

Please follow the steps below to use Postman:

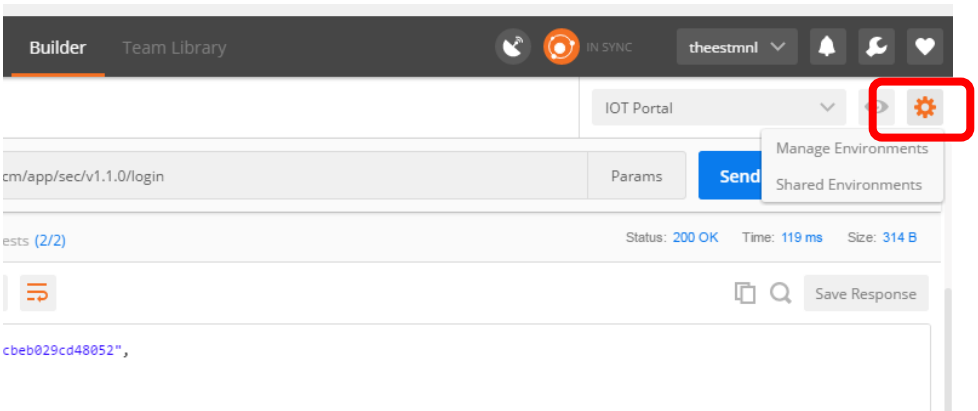
11. Attached in the email is the file cert.zip containing the security certificates to connect to the Ocean Connect API. For use within Postman, you need to use the *.crt and *.key file. If you want to split the PKCS12 fileyourself into these two files, you can find instructions on how to do this in the chapter “Security certificates”.

12. Please see chapter Security Certificates on how to import the certificates into Postman (use Settings > Certificates).

13. Import the TMNL postman collection NB-IOT TMNL.postman_collection.json (download from repository)



14. Download the environment variables from the repository and select the environment settings icon.



15. Select manage environments > import > select the json file downloaded from the forum (environment json)

16. Click on IOT portal to edit the variables, enter your appID and Secret (send in email)

17. You should now be able to use the POST Login, to get an access token from the API. This access token you can enter into the environment variables (our Postman collection has a script to do this automatically).

18. With the access token entered, you should be able to use;

    GetDevices – in case you already have devices registered

    Register device – to register the IMEI (please enter the IMEI in the fields VerifyCode and NodeID)

    SetDeviceInfo – to set additional info of your device, like its name. It is essential that you use exactly the same name for Manufacturer, Devicetype and Model!
    You can find these names in Ocean Connect under App Management > Applications > yourAppId > App Resource

    Please note the following: the default template which was created for you contains a typo, you have to use this typo Dector instead of Detector in order for it to work…

    Your code in Set DeviceInfo should look like (if you have not changed the default template):

```
{
   "name":"YourName" ,
   "endUserId":"Eric",
   "mute":"FALSE",
   "manufacturerId":"fangle",
   "manufacturerName":"fangle",
   "location":"NL_DH",
   "deviceType":" Geomagnetic",
   "protocolType":"CoAP",
   "model":" VehicleDector "
}
```

    In the current trial set-up, you need to switch off SSL certificates check in the general Postman settings.

19. To send data from the device, use the AT+NMGS=+NMGS=<length>,<data>

    <length> Decimal length of message.

    <data> Data to be transmitted in hexstring format.

And collect the data via GET device data history

Module commands

All AT commands are based on the Neul chipset. The complete Neul documentation can be found on the repository (restricted access).

To check hardware and firmware version:

Connect USB to Serial;

Use 9600 Baud, 8 bits , 1 stop, Parity: None

Reset ;	Nuel Ok
Switch On;	AT+CFUN=1
Manufacturer;	AT+CGMI
Model;	AT+CGMM
Firmware;	AT+CGMR
IMEI;	AT+CGSN=1
IMSI;	AT+CIMI

Each command should give a response, if not check your set-up. If no IMSI is returned, please check your SIM card, it has been noticed that some test SIM cards are not working.

Note: Please verify the firmware revision number anything equal or higher than SP11 will not work on the trial network.

Note: SP8 has the support for extended network coverage, which will improve the signal reception in areas with less coverage.

To establish network attach:

Connect USB to Serial;

9600 Baud, 8 bits , 1 stop, Parity: None

Reset ;	Nuel Ok
Switch On;	AT+CFUN=1
Set IP;	AT+NCDP=172.16.0.36
Set APN;	AT+CGDCONT=1,"IP", "parking.donas.nb-iot.com"
Attach;	AT+COPS=1,2,"12345"
Wait for IP;	AT+CGPADDR=1

Note: Newer Firmware versions (SP8) require a slightly different approach.

By default these modules have auto connect configured. The CDP must be set before connection to the network is performed. (From the manual; Set the module to minimum functionality (issuing AT+CFUN=0 command) before sending the NCDP command).

So there are two steps:

1) Turn off Autoconnect;

```
AT+NCONFIG=AUTOCONNECT,FALSE
```

2) Perform the connect sequence

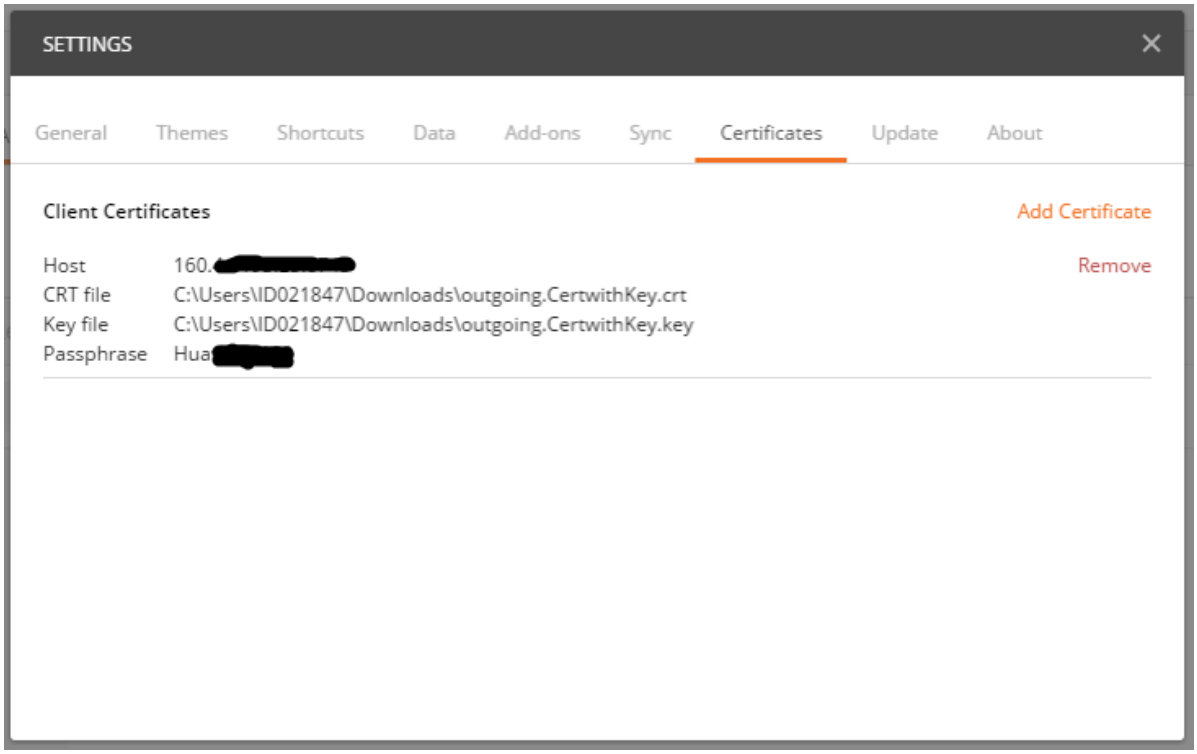
Reset ;	Nuel Ok
Set IP;	AT+NCDP=172.16.0.36
Set APN;	AT+CGDCONT=1,"IP", "parking.donas.nb-iot.com"
Switch On;	AT+CFUN=1
Attach;	AT+COPS=1,2,"12345"
Wait for IP;	AT+CGPADDR=1

Please be aware that these settings only apply for the T-Mobile trial network, the production network will have different APN and IP addresses.

Security certificates for using the API

In your account info email the file cert.zip was attached. Use the file outgoing.CertwithKey.pkcs12

Visit https://www.sslshopper.com/ssl-converter.html en select the pkcs12 file.

- Choose current certificate type PKCS12
- Choose Type To Convert To for PEM
- Enter as PFX password the keystore password from the account set-up email
- Click convert certificate.
- A file is downloaded with the PEM extension.
- Make a copy of this file and give one copy the new extension .key and the other the extension .crt
- In Postman, click in the top right on Settings > Certificates
- Choose Add certificate enter the following information and files:
- the North API IP address and port number from the email
- upload the CRT and KEY files
- Passphrase is the truststore password from the email

Postman now has the right settings and certifcates in order to connect to the API: