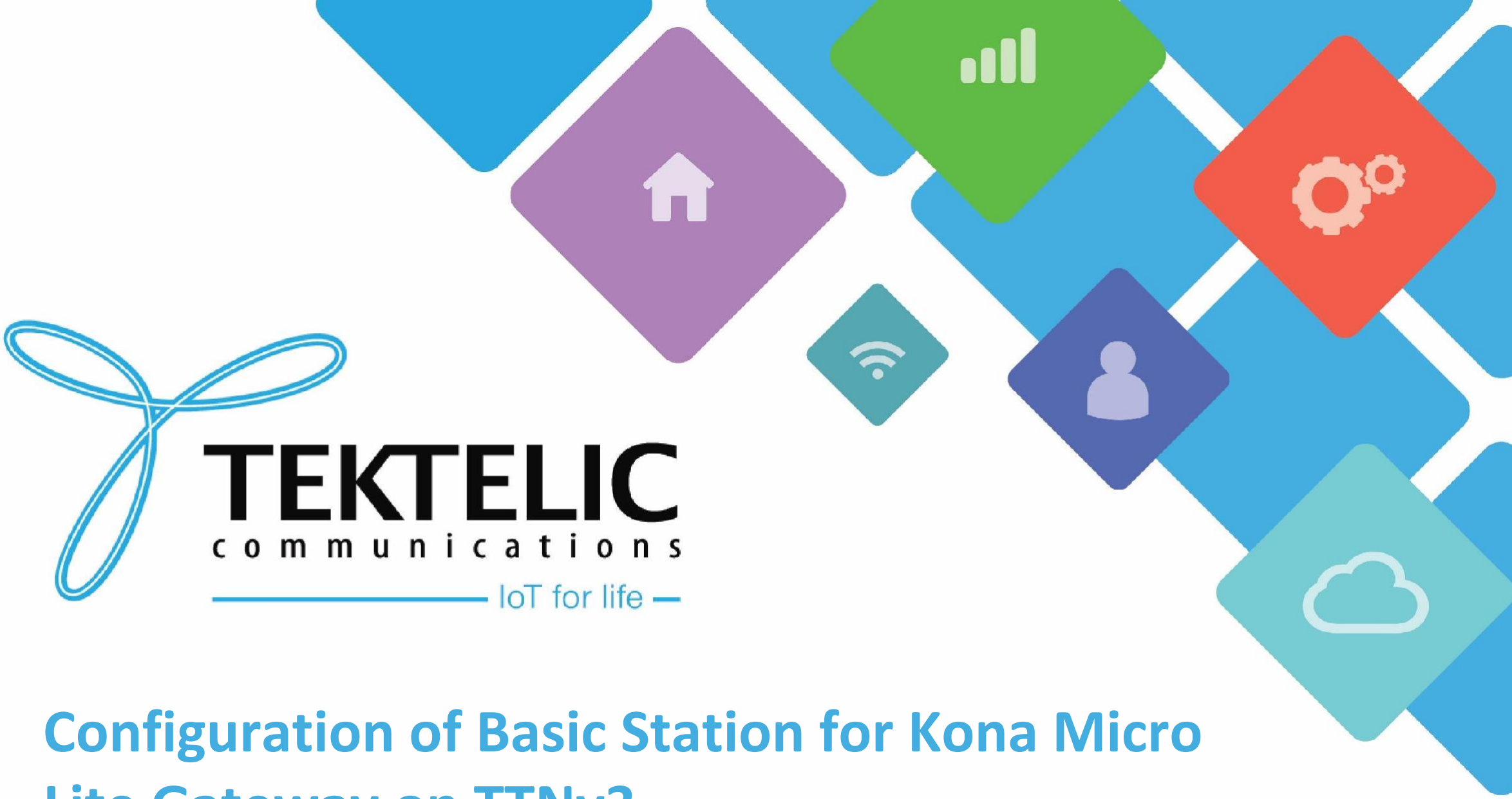

Configuration of Basic Station for Kona Micro Lite Gateway on TTNv3

Introduction

- Reference guide to configure Basic Station for Kona Micro Lite Gateway on TTNv3

- High-level process involves below stages.

1. Commissioning of Gateway on TTNv3
2. Generating Gateway API Keys
3. Configuration of CUPS
4. Uploading Basic Station file
5. Uploading configuration files
6. Uploading security certificates

Commissioning of Gateway on TTNv3

1. Login to TTN Network Server.

2. Go to Gateways page. Then Select **Add Gateway** button

3. Enter the **Gateway ID**, **Gateway EUI,** and **Gateway Name**.

4. Select the correct frequency plan based on your Gateway.

5. Select **Create Gateway**.

Certificates and Keys

To connect LoRaWAN Micro-Lite gateway to TTNv3, below list of certificates and keys will be required as outlined by TTNv3 here.

1. **cups.uri**
2. **cups.key**

Gateway API Keys

- Gateway API key that will be required from TTNv3 to connect the Micro-Lite GW:
    1. **CUPS API Key**
    2. **LNS API Key**

CUPS API Key:

A. Navigate to the API Keys menu of your gateway and select **Add API Key** again.

B. Enter a name for your key, select the following rights for your key.

C. CUPS require an API key for your gateway with the following rights:
- View gateway information
- Edit basic gateway settings
- Retrieve secrets associated with a gateway

D. You will see a screen that shows your newly created API Key. You now can copy it in your clipboard by pressing the copy button.

E. After saving the key in a safe place, press I have copied the key.

F. This is your **CUPS API key**.

Note:

- You will not be able to see this key again in the future. If you lose it, you can create a new one to replace it in the gateway configuration.

LNS API Key:

A. Navigate to the API Keys menu of your gateway and select **Add API Ke**.

B. Enter a name for your key, select the following rights for your key.

C. Enter a name for your key, select the “Link as Gateway to a Gateway Server for traffic exchange”, then click on Create API Key.

D. You will see a screen that shows your newly created API Key. You now can copy it in your clipboard by pressing the copy button.

E. After saving the key in a safe place, press I have copied the key.

F. This is your **LNS API key**.

Note:

- You will not be able to see this key again in the future. If you lose it, you can create a new one to replace it in the gateway configuration.

Configuration of CUPS

- To configure CUPS in The Things Stack to transmit the LNS API key when a gateway connects, TTN CLI is required.
- To download and install **TTN CLI (Use v3.10.1 and above)**. Please visit this link for instructions.
- After installation, Enter this command to login**: ttn-lw-cli login**
- Upon log-in, execute below commands.

Note:

Replace "**your-gateway-id**" with your gateway ID in The Things Stack and "**your-lns-api-key**" with the LNS API key you created in the last step:

- export GTW_ID="your-gateway-id"
- export LNS_KEY="your-lns-api-key" (#if this doesn't work then add "Bearer LNS-API-KEY")
- export SECRET=$(echo -n $LNS_KEY | xxd -ps -u -c 8192)
- ttn-lw-cli gateways update $GTW_ID --lbs-lns-secret.value $SECRET

Configuration of CUPS (cont.)

- If successful, you should receive a response as shown in Figure-1:


```
{
  "ids": {
    "gateway_id": "<gateway-id>"
  },
  "created_at": "2020-10-13T10:49:02.730Z",
  "updated_at": "2020-11-17T14:52:06.440Z",
  "version_ids": {

  },
  "lbs_lns_secret": {
    "key_id": "is/gateway-secrets-encryption-key",
    "value": "<encrpyted-base64-lns-api-key>"
  }
}
```


Figure-1 Successful configuration of CUPS

CUPS Certificates and Keys

1. cups.uri:

- This file should contain LNS Server Address: **https://<server-address>:443**
  - The server address is the network endpoint of The Things Stack CUPS.
  - It is a combination of the **protocol (https)**, **the server address**, and the **port**:

2. cups.key:

- You need TTN CLI to execute these commands after you login to CLI.
- This is a file which The Things Stack uses to verify the identity of your gateway.
- Use the following command to create a file called **cups.key**, replacing "**your-cups-api-key**" with the LNS API key you created above.

  - export CUPS_KEY="your-lns-cups-key"
  - echo "Authorization: Bearer $CUPS_KEY" | perl -p -e 's/\r\n|\n|\r/\r\n/g' > cups.key

Uploading Basic Station File

- Download latest version of Basic Station binary file for Kona Micro Lite gateway using this link.

- Use **TFTP client** to upload downloaded binary file of Basic Station on Kona Micro Lite gateway as shown in Figure-2 and reboot thegateway.

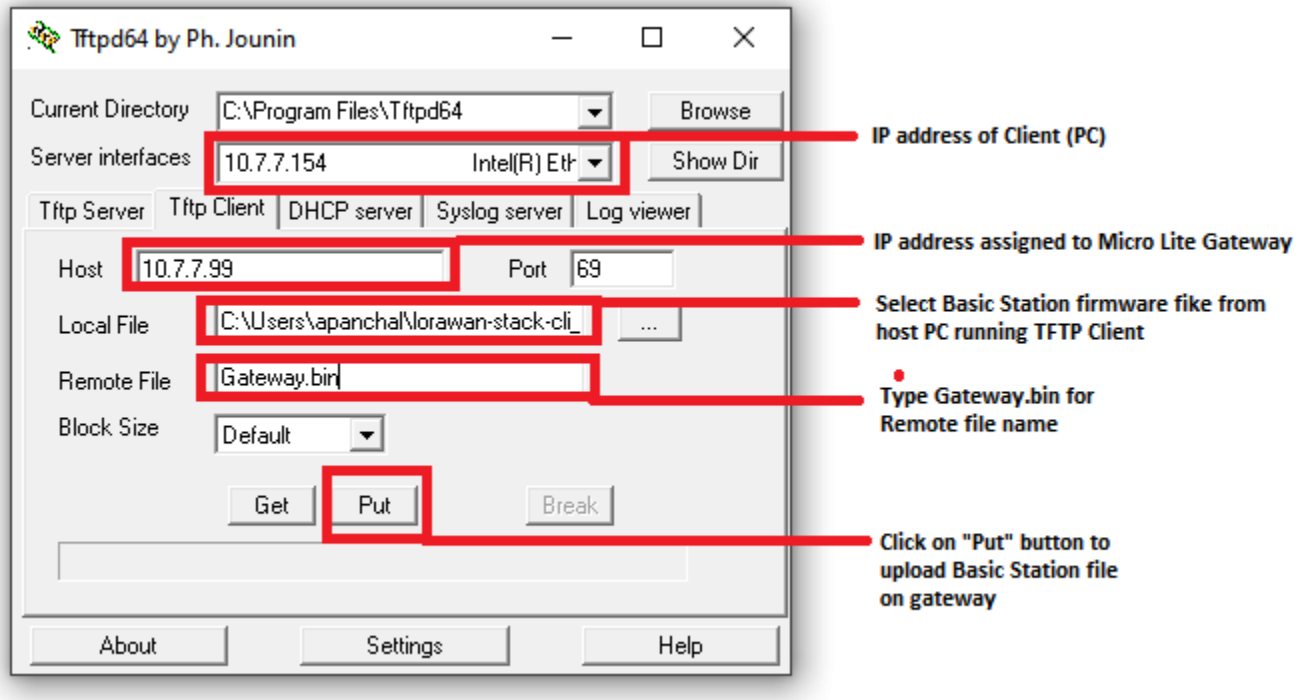

Figure-2 Uploading Basic Station binary

Updating Customer. json file

- To connect Kona Micro Lite Gateway to TTNv3, you will be required to modify existing **Customer.json** file.
- Modified **Customer.json** file will have a structure as shown in Figure-3.

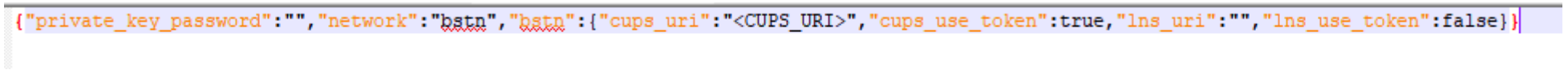

Figure-3 Customer.json file

- Sample Customer.json file can be downloaded using this link.
- After downloading this file, edit **cups_uri** value by contents of **cups.uri** file.

Uploading Customer.json File

- Use **TFTP client** to upload downloaded binary file of Basic Station on Kona Micro Lite gateway as shown in Figure-4 and reboot the gateway.

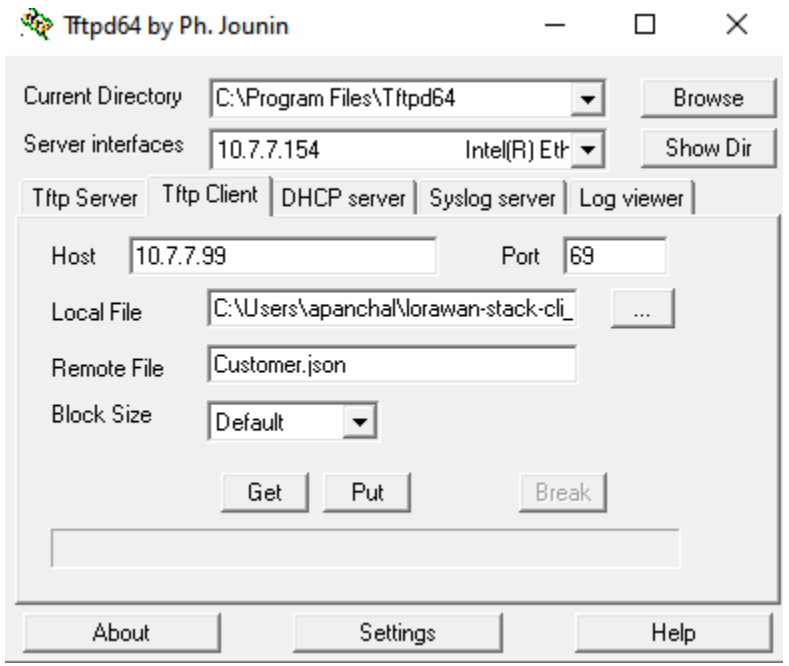

Figure-4 Uploading Customer.json file

CaRootCertificate.pem File

- **CaRootCertificate.pem** file can be downloaded using ISRG Root X1 certificate using this link.
- Save this downloaded file as **CaRootCertificate.pem** .
- After that, Use TFTP client to upload **CaRootCertificate.pem** file as shown in Figure-5 and reboot the gateway.

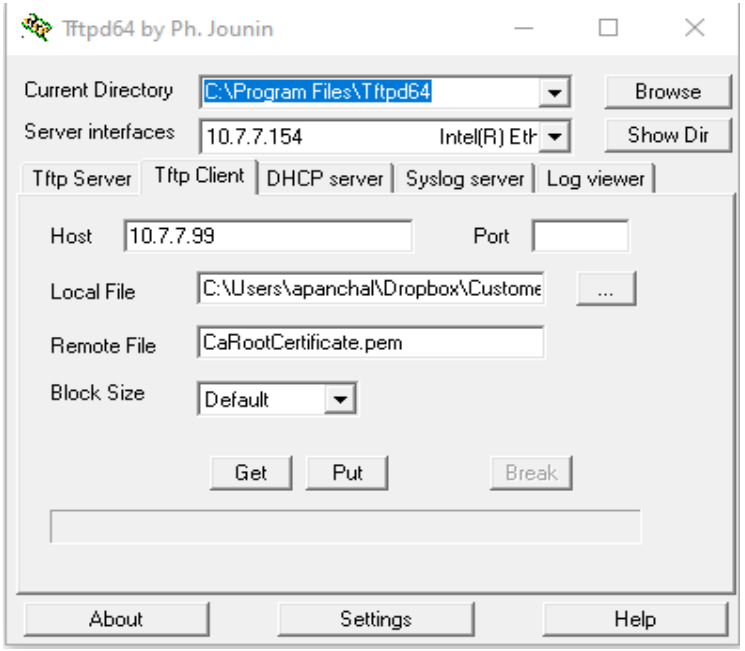

Figure-5 Uploading CaCertificate.pem file

PrivateKey.pem File

- **PrivateKey.pem** file is gateway specific and must be generated by combining **cups.key** file.
- To do so, copy contents from **cups.key** file and paste them in a new file.
- Save this file as **PrivateKey.pem** .
- After that, Use TFTP client to upload **PrivateKey.pem** file on Kona Micro Lite gateway as shown in Figure-6 and reboot the gateway.

PrivateKey.pem File (Cont…)

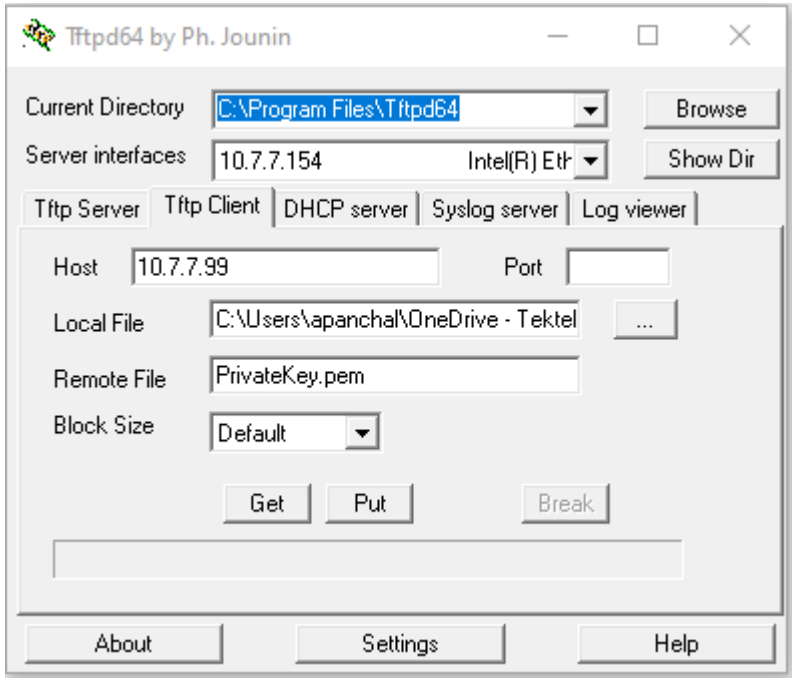

Figure-6 Uploading PrivateKey.pem file

- After reboot, you will be able to see gateway showing Connected on TTNv3.

Best-In-Class, Carrier Grade & Most Cost Effective Portfolio of Gateways, Network Server, Sensors & Applications