Unified BSP Upgrade via TEKTELIC CORE / OAM

Introduction

Reference guide to upgrade BSP on Kona GW using **TEKTELIC CORE Network Server or TEKTELIC OAM.**

Table of contents:

Prerequisites

This guide will assume that you are familiar with operating and navigating through a Linux environment. For a guide with ease of access, please see the BSP upgrade guide using KonaFT.

Requirements:

- FTP Program (such as FileZilla or WinSCP)

- Terminal program (such as TeraTerm or PuTTY)

- Kona Gateway connected to TEKTELIC CORE / OAM via MQTT bridge

- Access via SSH (or Reverse SSH for file management purposes)

Prerequisites

To upgrade the Kona Gateway BSP through Tektelic CORE / OAM, the gateway will need to be connected via MQTT Bridge.

- To verify if the MQTT Bridge is configured or not, click on the **Gateway Info** option. It should list all the information as shown in Figure-1.

- Gateways connected via UDP cannot be updated through this guide.

Kona Gateway	BSP versions that supports TEK MQTT
Kona Micro GW	v2.3.4 and onwards
Kona Macro GW	v3.1.5 and onwards
Kona Mega GW	V3.3.0 and onwards
Kona Enterprise GW / Micro PoE	Any version works.

Table-1 List of BSP version with TEK MQTT Bridge for Kona GW

Prerequisites (Continued)
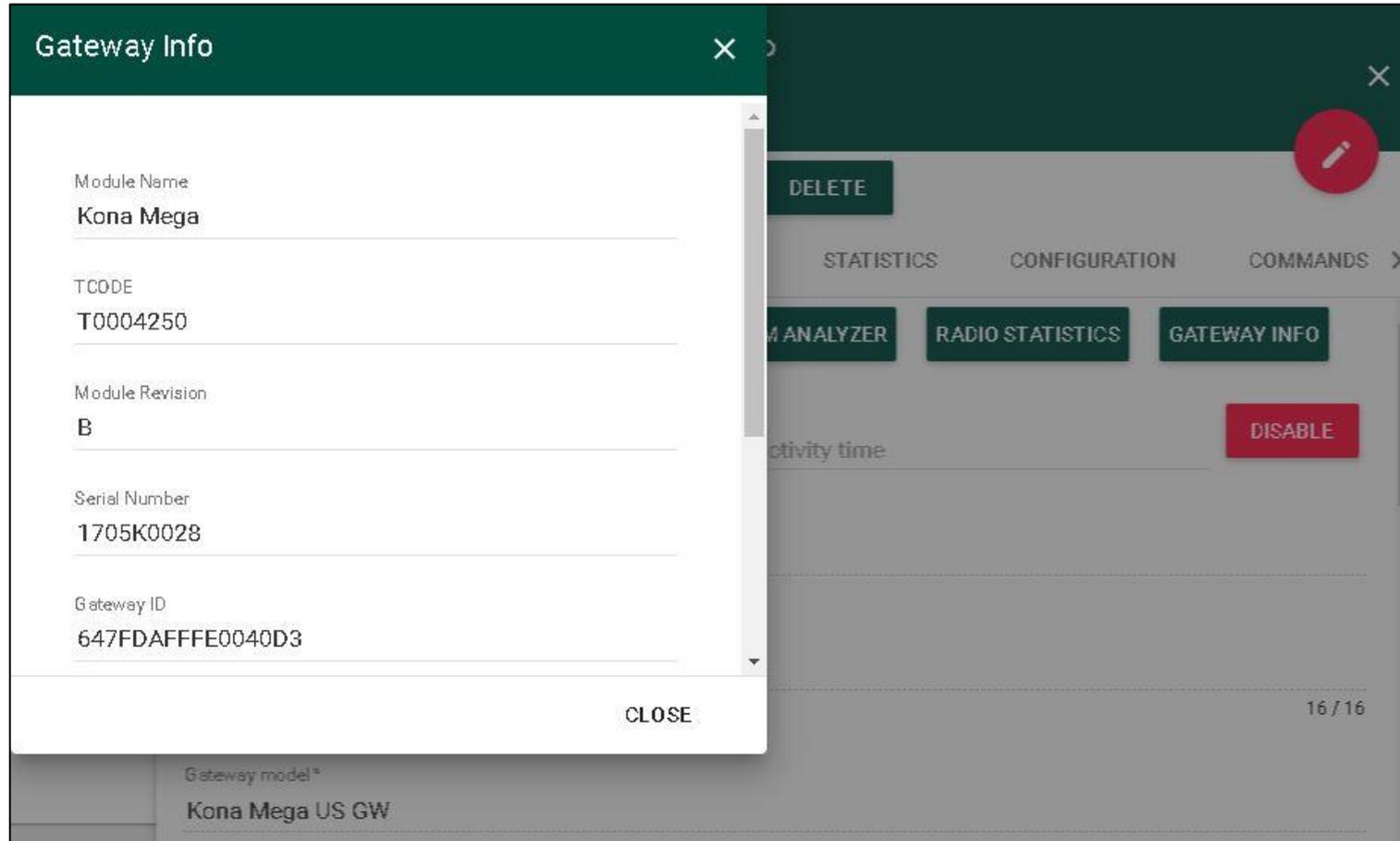
Figure-1 Gateway Information

Prerequisites (Continued)

To determine the current BSP version on the gateway, there are two methods.

<u>Tektelic Network Server/OAM:</u>

1. Go to **SW Management** tab

2. Click on **Read Versions**

3. In the list, verify the information in third row mentioned against **Release** shown in Figure-2. It will report the BSP version found on the gateway.

<u>On the Gateway:</u>

1. SSH into the gateway with the appropriate credentials. See the table below for details.

2. Enter the command: ***system_version***

Username	Password	Notes
root	9-Digit Serial number of the Gateway (i.e. 1618B0052)	• Applies to gateways with serial numbers that start with 21 and below.
admin	9-Digit Serial number of the Gateway (i.e. 1618B0052)	• Commonly found on **older ENTERPRISE gateways.**
admin	Random string of characters provided on the test report.	• Applies to gateways with serial numbers that start with 22 and above. • **Some units in this category may still have root as the user and the serial number as the default password.**

Table-2 Username and Password

Prerequisites (Continued)

Figure-2 SW Management tab

Prerequisites (Continued)

- All Kona gateways will be using a **unified BSP upgrade package** moving forward starting with **BSP v7.0.X.**
- Kona gateways will need to be on a specified BSP (seen below) before upgrading to the unified BSP.
- If your gateway is not on the initial BSP version, **use the legacy upgrade guide before proceeding.**

Gateway	Initial BSP Version	Final BSP Version
Kona Micro	v4.0.5 or newer	v7.0.x
Kona Micro PoE	v5.1.1 or newer	v7.0.x
Kona Macro	v6.1.4 or newer	v7.0.x
Kona Mega	v5.0.6 or newer	v7.0.x
Kona Enterprise	v2.1.2 or newer	v7.0.x

Table-3 Universal BSP upgrade

Download Upgrade Package

All BSP upgrade packages can be found on the TEKTELIC FTP server. You can find out [the latest releases here.](#) Instructions to access the FTP are as follows:

1. Configure your FTP client (such as [FileZilla](#) or [WinSCP](#)) to **"Use explicit FTP over TLS if available".**

| Protocol: | FTP - File Transfer Protocol |
| Encryption: | Use explicit FTP over TLS if available |
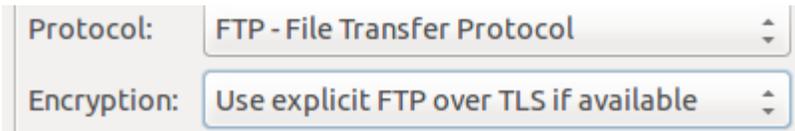
Figure-3 FTP client settings

2. Use the following credentials to access the server.
   - Site: **74.3.134.34**
   - Username: **customer**
   - Password: **vU6_ATR3**

3. Navigate to the **"Universal_Kona_SW"** directory and download the BSP package of your choice.

Upload Upgrade Package

To upload the newly downloaded BSP onto GW using TEKTELIC Network Server:

1. Go to the File Transfer tab by scrolling right to **File Transfer** tab

2. Click on the **Browse** option to locate the BSP upgrade zip file located on the system. Check mark the **Decompress** option seen next to the Upload File option.

3. Once located the files, click on **Upload File** option to upload the zip file as shown in Figure-2.

NOTE: Uploading the zip file can take up to 30 minutes.
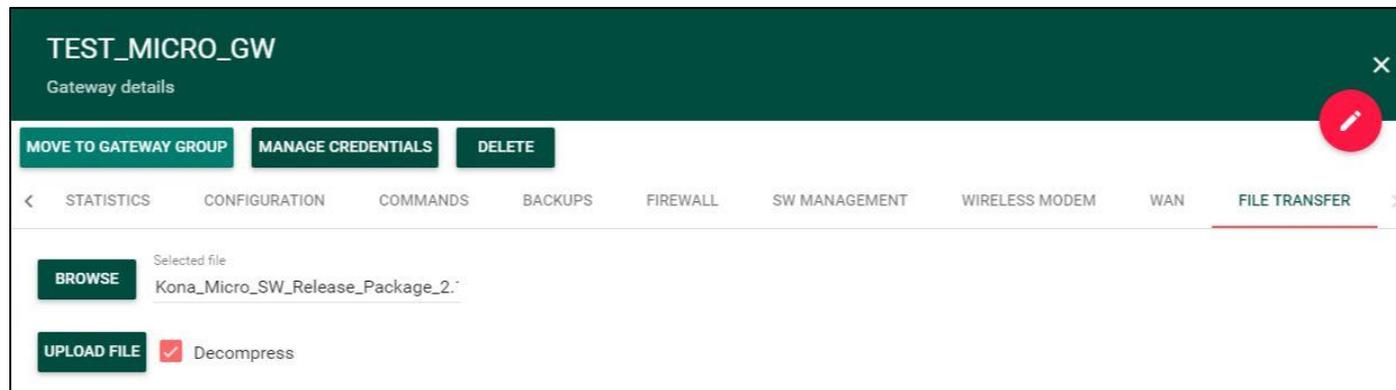
Figure-4 File Transfer

Configuration

Once the upgrade package has been uploaded to the gateway, the gateway needs to know where the files are.

1. Go to **Configuration** tab. Screen shown in Figure-3 will appear.

2. Click **the pencil icon** of the **Upgrade Servers row** to edit it.

3. Upon clicking the pencil, screen shown in Figure-4 will appear.

4. Unselect the **Use group configuration** option and Select **JSON** in **Content** Type field.

5. Copy text from the file "universal-upgrade.txt" (found here) and paste it under **Content.**

6. Click on **Save.**

NOTE: Files uploaded from Tektelic NS/OAM will be placed in /lib/firmware/ as opposed to /lib/firmware/bsp/ in other BSP upgrade guides. Please ensure the upgrade files are in the locations specified by the configuration file or vice versa.

Configuration (Continued)

Figure-5 Upgrade Servers

Configuration (Continued)

Figure-6 Configuration

SW Management

With the files uploaded onto the gateway, the gateway upgrade can be initiated.

1. Go to the **SW Management** tab.

2. Click on **Read Upgradable** option. It will list down all the packages which needs to be upgraded shown in Figure-5.

3. Click on **Upgrade BSP** option to upgrade the version of BSP on the GW.

4. While BSP is upgrading, Upgrade status message will display the status of the process.

5. Upon successful BSP upgrade, **BSP Upgrade Succeeded** message will be shown. Alternatively, clicking on BSP Status can also provide the information on BSP upgrade. Upon successful upgrade, message shown in Figure-7 will appear.

NOTE: BSP Upgrade may take up to 15-30 minutes.

SW Management (Continued)

Figure-7 SW Management

SW Management (Continued)

To verify the BSP Upgrade, [please follow the instructions to determine the new BSP version of the gateway.](#)

NOTE: If you are accessing the gateway via SSH and it is still undergoing the upgrade process, ***DO NOT*** modify nor administer any changes to the gateway.

To install additional packages (such as **geolocation for Kona Macro** or **Basic Station**) follow the steps below:

1. Click on the **checkbox beside the Component** you wish to install.

2. Click on **Install Selected.**

NOTE:

- For **Geolocation features**, the Component name is **"gl".**

- For the **Tektelic Basic Station**, the Component name is **"tektelic-bstn".**

SW Management (Continued)

Figure-8 BSP Upgrade

SW Management (Continued)

Figure-9 SW Management tab

Conserving Gateway Space

When a gateway requires multiple BSP upgrades, you will need to remove the upgrade files and backup created. This will ensure that the gateway will have enough space to create a backup and perform the upgrade. **If the gateway does not have enough space to perform an upgrade or backup the system, the upgrade will throw an error and will not proceed.**

Because each new BSP release may contain new versions of the packages, they will not overwrite existing upgrade files. Hence, we will always recommend removing upgrade package and associated files.

To check how much space you have on your gateway, run the following command: **df**
Generally, having 50% space free in **ubi0:rootfs** is enough to commence an upgrade.

```
root@kona-micro         :~# df
Filesystem              1K-blocks      Used Available Use% Mounted on
ubi0:rootfs                256512    229880     26632  90% /
devtmpfs                   242764        12    242752   0% /dev
tmpfs                      255168       104    255064   0% /run
tmpfs                       65536       492     65044   1% /var/volatile
ubi1:log                   192852     14136    173880   8% /var/lib/logs
```

Figure-10 SW Management tab

Conserving Gateway Space (cont.)

When managing your gateway through TEKTELIC CORE/OAM, _all files, upgrade package, and backups_ can _only_ be removed through _SSH_.

When a package is uploaded through TEKTELIC CORE/OAM, the package is uploaded to the directory **/dev/shm**
- To remove the upgrade package, run the following command: **sudo rm /dev/shm/<upgrade-package-name>.zip**

All BSP upgrade files can be found in the following folder: **/lib/firmware/**
- To remove the upgrade files, run the following command: **sudo rm -rf /lib/firmware/[folder name]**
- To see the names of folders, please use the command: **ls /lib/firmware**

Backups are always created as part of the BSP upgrade process. When doing multiple intermediate upgrades, backups should also be removed to conserve space.
1. Log into the gateway via SSH.
2. See the list of available backups: **system-backup -L**
3. Remove backups as desired: **system-backup –D [backup number]**

Reverse SSH

Customers who have deployed gateways in remote environments will still have to access the gateway through Reverse SSH. This is a process where the remote gateway connects to a proxy SSH server.

Remote Gateway

Proxy SSH Server

Your local PC

Network Server tells remote gateway to connect to Proxy Server

You connect to the Remote Gateway through the Proxy Server
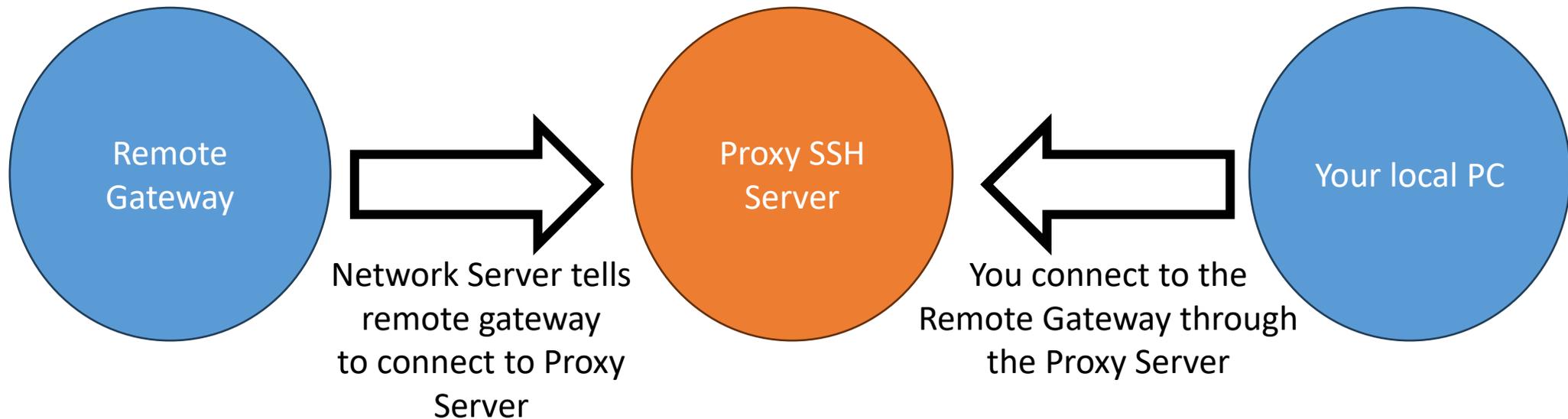
Reverse SSH (cont.)

To set up a Reverse SSH connection, follow the instructions below.

1. Navigate to the Commands tab of your gateway.

2. Set command to "Establish reverse SSH session".

3. Configure details indicated.

4. Finalize by clicking Execute.

If the connection was successful, the **"status"** will be **"ok".**

Figure-11 Reverse SSH configuration

Reverse SSH (cont.)

With the remote gateway connected to the Proxy Server, the final step is to connect to the Remote gateway.

1. Log into the Proxy Server via SSH.

2. Run the following command below:
    - *ssh root@localhost/9000 -y -y*
    - **Note: Some elements of this command can change depending on how you configured the connection in the previous slide.**
        - **root** is the Username of the Remote Gateway and can be **admin**
        - **9000** is the default Reverse SSH Port seen in the previous slide.

3. Log into your Remote Gateway with regular gateway credentials.

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