Espressif IoT SDK:

IOT_Demo(Light/Plug/Sensor)

Status	Released
Current version	V0.5
Author	Fei Yu
Completion Date	2014.9.24
Reviewer	Jiangang Wu
Completion Date	2014.9.24

[√] CONFIDENTIAL
[ ] INTERNAL
[ ] PUBLIC

Version Information

Date	Version	Author	Comments / Changes
2014.5.13	0.1	Jiangang Wu	Draft
2014.6.16	0.2	Fei Yu	Update commands
2014.7.10	0.3	Fei Yu	Add RPC
2014.8.14	0.4	Fei Yu	Update commands
2014.9.24	0.5	Fei Yu	Add WEP HEX curl introduction

Table of Contents

1. Foreword

Herein, we introduce the embedded application development based on Espressif IoT SDK. The IoT demo application showcases smart connectivity for three kinds of products: smart power plugs, lights and humidity-temperature sensors. In addition, our Espressif cloud server enables the reverse control of devices and data collection.

With the IoT demo, users can rapidly develop a variety of similar applications.

2. Overview

2.1. Source Code Layout

2.1.1. Folder “usr”

The IoT demo source code of is in the "usr" folder, and the details are as follows:

user_main.c — main file

user_webserver.c — provides REST light weighted webserver function

user_devicefind.c — provides device look-up function

user_esp_platform.c — based on application function of espressif server

user_json.c — json packet processing function

user_plug.c — plug function

user_light.c — pwm light function

user_humiture.c — humidity-temperature function

2.1.2. Folder “include”

Header files are stored in the include folder. The "user_config.h" define variables to select the platform and demo type to compile.

Example:

PLUG_DEVICE,LIGHT_DEVICE, SENSOR_DEVICE

SENSOR_DEVICE can be sub-divided into HUMITURE_SUB_DEVICE and FLAMMABLE_GAS_SUB_DEVICE.

2.1.3. Folder “driver”

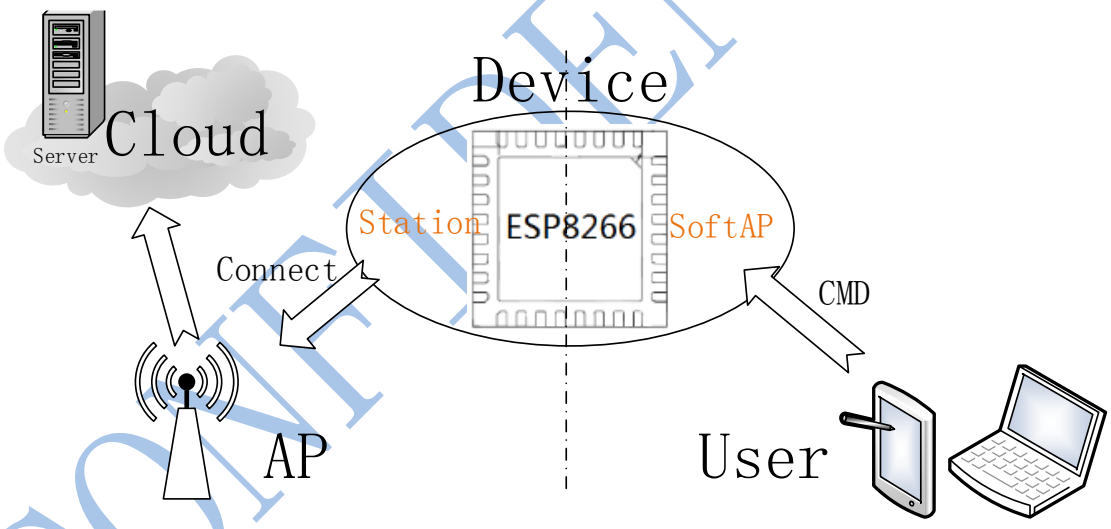
Our divers currently supports I2C Master,external buttons,PWM and Dual UART.

2.2. Operating Mode

The Wi-Fi operating mode in this IoT Demo is softAP + station -> station. By default, the setting is softfAP + station. Users can connect to the LAN via the softAP interface and send commands to connect to the router via the station interface. Through the softAP interface, the user can query the station connection status. After connection to the router is successfule, the device can be rebooted to station mode. (For more details, please refer to 3.1.2 Setting Connection Parameters)

By default, the SSID for softAP is ESP_XXXXXX,where XXXXXX are the last three bytes of the MAC address. The default encryption mode is WPA/WPA2.

In station mode, by pressing the button for 5 seconds, the device will be reset and restarted to initial softAP + station mode for reconfiguration.



2.3. Debugging Tools

The Cloud Server in the IoT Demo uses the REST architecture. When the PC is communicating with the IoT Demo device, curl commands can be used.

Download the specified version on http://curl.haxx.se/download.html . For use of curl commands here, please refer to the examples shown in "Windows curl".

If you use Linux curl or Cygwin curl, please refer to examples of the curl

command in "Linux/Cygwin curl".

Unless otherwise specified, both can be used.

Common errors in Curl:

1） Take note of the upper and lower case in the commands, otherwise the command may fail.

2） The number of spaces curl commands may cause it to fail.

3） Token generated on the Server is only for 1 device and cannot be shared.

4） Use the right command format for Linux/Cygwin or Windows Curl. Do not mix them up.

3. Functions for LAN

Default IP address of softAP mode is 192.168.4.1. In station mode the IP address is assigned by router. The IP address in the URL represents IP in softAP and station mode depending on which is required.

Espressif softAP needs a password to connect. The password format is as follows:

device's_softAPMAC_PASSWORD.

The password defined in esp_iot_sdk\app\include\user_config.h is the softAP's PASSWORD.

For example:

The "PASSWORD" defined in esp_iot_sdk_v.08 is v*%W>L<@i&Nxe!

The softAP MAC address of a device is 1a:fe:86:90:d5:7b

So the connection password is 1a:fe:86:90:d5:7b_v*%W>L<@i&Nxe!

3.1. General Functions

3.1.1. Get version information

```
curl -X GET http://ip/client?command=info
```

Response:

```
{
    "Version": {
        "hardware":"0.1",
        "software":"0.8.0"
    },
    "Device": {
        "product":"Plug",
         "manufacture", "Espressif Systems"
    }
}
```

3.1.2. Set connection parameter

Device initial state is softAP+station mode. Connect PC to LAN provided by device softAP's interface (password described above) and send curl to control device through PC.

- Set station mode

PCs send following command and connect device to the external network.

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -d '{"Request":{"Station":{"Connect_Station":{"ssid":"tenda","password":"1234567890","token": "1234567890123456789012345678901234567890"}}}}' http://192.168.4.1/config?command=wifi
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -d "{\"Request\":{\"Station\":{\"Connect_Station\":{\"ssid\":\"tenda\",\"password\":\"1234567890\",\"token\": \"1234567890123456789012345678901234567890\"}}}}" http://192.168.4.1/config?command=wifi
```

After the setup is completed, connect the device to the router in the command.

Note:

- The red token length field is a random hexademical string of 40 bytes. Device will send this random token to server for activation and identification
- Users use the same random token to apply for control access to the device from Espressif Server, so random token cannot be shared with other devices.

P.S.

If router(AP) config is **WEP HEX** , the password need to convert into HEX in curl.

For example:

SSID of router is "wifi_1", the password is "tdr0123456789" , encrypt as "WEP HEX", then

Linux/Cygwin curl：

```
curl -X POST -H Content-Type:application/json -d '{"Request":{"Station":{"Connect_Station":{"ssid":"wifi_1","password":"74647230313233343536373839","token": "1234567890123456789012345678901234567890"}}}}' http://192.168.4.1/config?command=wifi
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -d "{\"Request\":{\"Station\":{\"Connect_Station\":{\"ssid\":\"wifi_1\",\"password\":\"746472303132333435363738 39\",\"token\": \"12345678901234567890123456789012345678901234567890\"}}}}" http://192.168.4.1/config?command=wifi
```

During the connection，the command below can be sent through PC side to query the connection status of device

```
curl -X GET http://ip/client?command=status
```

Response：

```
enum {
    STATION_IDLE = 0,
    STATION_CONNECTING,
    STATION_WRONG_PASSWORD,
    STATION_NO_AP_FOUND,
    STATION_CONNECT_FAIL,
    STATION_GOT_IP
};
```

```
enum {
    DEVICE_CONNECTING = 40,
    DEVICE_ACTIVE_DONE,
    DEVICE_ACTIVE_FAIL,
    DEVICE_CONNECT_SERVER_FAIL
};
```

After connecting the PC side will send following command and change the device mode from softAP+station mode to station mode.

For the devices which support reverse control,such as switches, lights and so on, command is:

```
curl -X POST http://ip/config?command=reboot
```

For the devices which do not support reverse control, such as sensors, the command is:

```
curl -X POST http://ip/config?command=sleep
```

The sensor devices will wake up automatically after sleep 30s and mode will be changed to station mode.

➢ Set softAP parameters

Devices send following command and set parameters for softAP, such as ssid, password and so on.

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -d '{"Request":{"Softap":{"Connect_Softap":{"authmode":"OPEN","channel":6,"ssid":"ESP_IOT_SOFTAP","password":""}}}}' http://192.168.4.1/config?command=wifi
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -d "{\"Request\":{\"Softap\":{\"Connect_Softap\":{\"authmode\":\"OPEN\",\"channel\":6,\"ssid\":\"ESP_IOT_SOFTAP\",\"password\":\"\"}}}}" http://192.168.4.1/config?command=wifi
```

The devices need to be rebooted before changes take effect.

Note:

- authmode supports following modes: OPEN, WPAPSK, WPA2PSK, WPAPSK/WPA2PSK.
- password must be no less than 8 bytes.

3.1.3. Transformation of wifi mode

Since esp_iot_sdk_v0.9.2, transformation of wifi mode is as follow：

（1） Device initial state is softAP+station mode.

（2） Phone APP（or PC）connects to ESP8266 softAP，sends a command to make ESP8266 station connect to router（AP）.

（3） Connected to router（AP），ESP8266 tries to communicate with server for authentication. If succeed , ESP8266 changes to station mode.

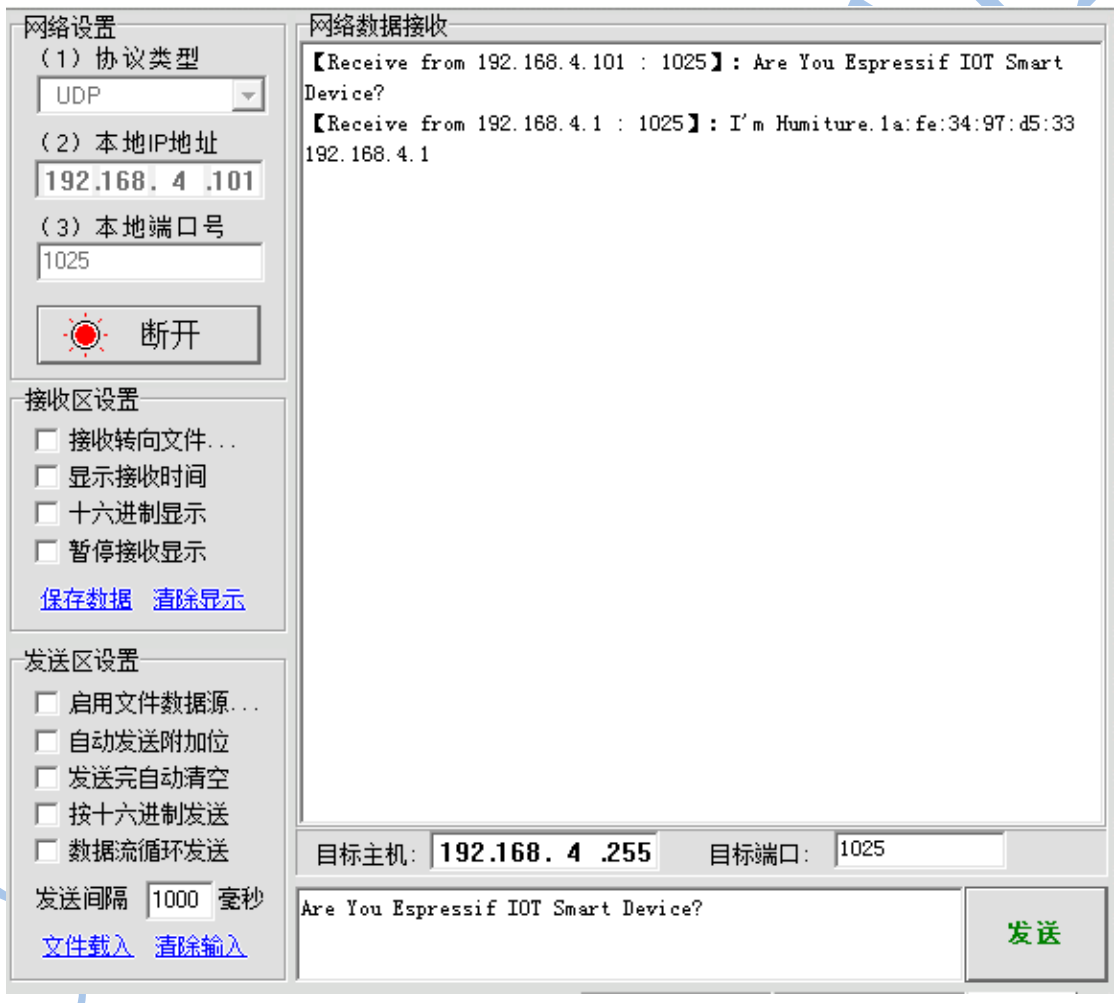
（4） After that, ESP8266 is in station mode, only if it is disconnected from the network, ESP8266 will convert into softAP + station mode again. Then restart from step (2), try to connect again.

If fail to connect to router(AP), ESP8266 will try another router(AP) which has been recorded. This function in source code defines as “#define AP_CACHE”.

3.2. Device search in LAN

Find devices by sending UDP broadcast packets to port 1025 to the LAN. The message sent is "Are You Espressif IOT Smart Device?". Devices will respond to the received UDP broadcast packets with a string.

This function can be tested by using the network debugging assistant, for example:



Response：

- Plug

  I'm Plug.xx:xx:xx:xx:xx:xxyyy.yyy.yyy.yyy

- Light

  I'm Light.xx:xx:xx:xx:xx:xxyyy.yyy.yyy.yyy

- Humidity and Temperature Sensor

I'm Humiture.xx:xx:xx:xx:xx:xxyyy.yyy.yyy.yyy

Where xx:xx:xx:xx:xx:xx is the device MAC address and yyy.yyy.yyy.yyy is the device IP address. There is no response for the wrong string.

3.3. Plug

3.3.1. Get Status

```
curl -X GET http://ip/config?command=switch
```

Response

```
{
    "Response": {
        "status": 0
    }
}
```

Status can be 0 or 1。

3.3.2. Set Status

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -d '{"Response":{"status":1}}' http://ip/config?command=switch
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -d "{\"Response\":{\"status\":1}}" http://ip/config?command=switch
```

status can be 0 or 1。

3.4. Light

3.4.1. Get Status

```
curl -X GET http://ip/config?command=light
```

Response

```
{
    "freq": 100,
        "rgb": {
```

```
            "red": 100,
            "green": 0,
            "blue": 0
        }
}
```

Range: freq can be 1~500 while red, green, blue can be 0~255.

3.4.2. Set Status

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -d '{"freq":100,"rgb":{"red":200,"green":0,"blue":0}}' http://ip/config?command=light
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -d "{\"freq\":100,\"rgb\":{\"red\":200,\"green\":0,\"blue\":0}}" http://ip/config?command=light
```

Range: freq can be 1~500 while red, green, blue can be 0~255.

3.5. Humidity-Temperature Sensor

The humidity-temperature sensor status can be obtained from Espressif Cloud Server through internet.

4. Functions for WAN

4.1. Espressif Cloud Serve

Specifications and details of the Espressif Cloud Server, including introduction of the APIs can be found on the server itself.

Note:

- “Device " refers to the operation which that the device runs by itself and needs no user intervention.
- "PC” refers to the commands that users can send to the device to run.

4.1.1. master-device-key

The Espressif Cloud server is designed such that each device needs to apply for a master device key from it and burned to 0x3e000 at SPI flash.

Please refer to the document Espressif Cloud Introduction.

4.1.2. Activation

➢ Device

After setting the ssid, password and random token through softAP interface, the device’s station interface will connect to router for activation. Once it gets IP address from router,it will try to connect to the server automatically for activation.

Activation requires a TCP packet to be send to the server (IP address 114.215.177.97, port 8000). Format of TCP packet:

```
{"path": "/v1/device/activate/", "method": "POST", "meta": {"Authorization": "token HERE_IS_THE_MASTER_DEVICE_KEY"}, "body": {"encrypt_method": "PLAIN", "bssid": "18:fe:34:70:12:00", "token": "1234567890123456789012345678901234567890"}}
```

HERE_IS_THE_MASTER_DEVICE_KEY is the device key stored in the SPI flash, and 1234567890123456789012345678901234567890 is the random token set in above section 3.1.2 set connection parameter.

Response

```
{"status": 200, "device": {device}, "key": {key}, "token": {token}}
```

➢ PC

After PC has configured the device's ssid, password and token, it needs to be connected to a router which has access to the internet and applies for device control from server.

Linux/Cygwin curl：

```
curl -X POST -H "Authorization:token c8922638bb6ec4c18fcf3e44ce9955f19fa3ba12" -d '{"token": "12345678901234567890123456789012345678901234567890"}' http://114.215.177.97/v1/key/authorize/
```

Windows curl：

```
curl -X POST -H "Authorization:token c8922638bb6ec4c18fcf3e44ce9955f19fa3ba12" -d "{\"token\": \"12345678901234567890123456789012345678901234567890\"}" http://114.215.177.97/v1/key/authorize/
```

Response：

```
{"status": 200, "key": {"updated": "2014-05-12 21:22:03", "user_id": 1, "product_id": 0, "name": "device activate share token", "created": "2014-05-12 21:22:03", "source_ip": "*", "visibly": 1, "id": 149, "datastream_tmpl_id": 0, "token": "e474bba4b8e11b97b91019e61b7a018cdbaa3246", "access_methods": "*", "is_owner_key": 1, "scope": 3, "device_id": 29, "activate_status": 1, "datastream_id": 0, "expired_at": "2288-02-22 20:31:47"}}
```

c8922638bb6ec4c18fcf3e44ce9955f19fa3ba12 is an example of user key, and users do need to fill in their own user key which can be obtained as follows:

1. Log into Espressif server http://iot.espressif.cn/
2. Sign in with username password
3. Click on Username at the top corner ->Set-up ->Developer.

e474bba4b8e11b97b91019e61b7a018cdbaa3246 is the device's owner key which will be used later to control the device at PC end.

4.1.3. Identification

After activation the device needs to send TCP packets to Espressif Cloud Server (IP address 114.215.177.97, port 8000). TCP packet format：

{"nonce": 560192812, "path": "/v1/device/identify", "method": "GET", "meta": {"Authorization": "token HERE_IS_THE_MASTER_DEVICE_KEY"}}

The function of this tcp packet is to help the device to confirm its identity. Each time the device reconnects to server, it should send such a packet. “nonce" is a batch of random numbers, the string behind token is the master device key.

The server replies to the device with when its identity is successfully confirmed with a data packet:

Response：

{"device": {"productbatch_id": 0, "last_active": "2014-06-19 10:06:58", "ptype": 12335, "activate_status": 1, "serial": "334a8481", "id": 130, "bssid": "18:fe:34:97:d5:33", "last_pull": "2014-06-19 10:06:58", "last_push": "2014-06-19 10:06:58", "location": "", "metadata": "18:fe:34:97:d5:33 temperature", "status": 2, "updated": "2014-06-19 10:06:58", "description": "device-description-79eba060", "activated_at": "2014-06-19 10:06:58", "visibly": 1, "is_private": 1, "product_id": 1, "name": "device-name-79eba060", "created": "2014-05-28 17:43:29", "is_frozen": 0, "key_id": 387}, "nonce": 560192812, "message": "device identified", "status": 200}

The identification process is required for plugs and lights application.

4.1.4. PING Server

To maintain the connection of socket under the circumstance that the device doesn’t need reverse control over a long period of time,the device needs to send TCP packets to Espressif Cloud Server (IP address 114.215.177.97, port 8000) every 50s in following format:

{"path": "/v1/ping/", "method": "POST","meta": {"Authorization": "token HERE_IS_THE_MASTER_DEVICE_KEY"}}

Response：

{"status": 200, "message": "ping success", "datetime": "2014-06-19 09:32:28", "nonce": 977346588}

PING is required in devices that need reverse control like plugs and lights.

4.1.5. Plug

- Device

During reverse control of devices, there are two cases:

（1）Device receives get command from the server which indicates that the

device needs to send his own status to the server. Format of device's get command sent from server:

{"body": {}, "nonce": 33377242, "is_query_device": true, "get": {}, "token": "e474bba4b8e11b97b91019e61b7a018cdbaa3246", "meta": {"Authorization": "token e474bba4b8e11b97b91019e61b7a018cdbaa3246"}, "path": "/v1/datastreams/plug-status/datapoint/", "post": {}, "method": "GET"}

Response

{"status": 200, "datapoint": {"x": 0}, "nonce": 33377242, "is_query_device": true}

（2）When device receives post command from the server, it indicates that the device needs to change his own status and server will send data packets for instructions. For example, "turn on the switch" command:

{"body": {"datapoint": {"x": 1}}, "nonce": 620580862, "is_query_device": true, "get": {}, "token": "e474bba4b8e11b97b91019e61b7a018cdbaa3246", "meta": {"Authorization": "token e474bba4b8e11b97b91019e61b7a018cdbaa3246"}, "path": "/v1/datastreams/plug-status/datapoint/", "post": {}, "method": "POST","deliver_to_device": true}

After the switch completes instruction, it will send a successful status update response to the server in the following format. The "nonce" used to sync request and response must be in consistent to the "nonce" in the control command previously sent from the server which represents that each control and response correspond to each other.

Response

{"status": 200, "datapoint": {"x": 1}, "nonce": 620580862, "deliver_to_device": true}

- PC

Get plug status

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" http://114.215.177.97/v1/datastreams/plug-status/datapoint/
```

Response：

{"status": 200, "nonce": 11432809, "datapoint": {"x": 1}, "deliver_to_device": true}

Set plug status

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" –d '{"datapoint":{"x":1}}' http://114.215.177.97/v1/datastreams/plug-status/datapoint/?deliver_to_device=true
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" –d "{\"datapoint\":{\"x\":1}}" http://114.215.177.97/v1/datastreams/plug-status/datapoint/?deliver_to_device=true
```

Response：

```
{"status": 200, "nonce": 11432809, "datapoint": {"x": 1}, "deliver_to_device": true}
```

4.1.6. Light

✧ Device

When handling reverse control of devices, there are two cases:

（1）When device receives get command from the server, it needs to send its own status to the server. The get command format as sent from server to device is as follows:

```
{"body": {}, "nonce": 8968711, "is_query_device": true, "get": {}, "token": "e474bba4b8e11b97b91019e61b7a018cdbaa3246", "meta": {"Authorization": "token e474bba4b8e11b97b91019e61b7a018cdbaa3246"}, "path": "/v1/datastreams/light/datapoint/", "post": {}, "method": "GET"}
```

Response:

```
{"nonce": 5619936, "datapoint": {"x": 100,"y": 200,"z": 0,"k": 0,"l": 50},"deliver_to_device": true}
```

（2）When device receives post command from the server, it needs to change its own status and complete instructions according to data packets from the server. The example given here is the switch on lights command:

```
{"body": {"datapoint": {"y": 200, "x": 100, "k": 0, "z": 0, "l": 50}}, "nonce": 5619936, "is_query_device": true, "get": {}, "token": "e474bba4b8e11b97b91019e61b7a018cdbaa3246 ", "meta": {"Authorization": "token e474bba4b8e11b97b91019e61b7a018cdbaa3246"}, "path": "/v1/datastreams/light/datapoint/", "post": {}, "method": "POST"
```

Response：

```
{"nonce": 5619936, "datapoint": {"x": 100,"y": 200,"z": 0,"k": 0,"l": 50},"deliver_to_device": true}
```

X = frequency, range 1~500. Y (red), Z (green), K (blue) indicate that the different colors of lights, range 0~255. L parameters are reserved.

✧ PC

Get light status

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" http://114.215.177.97/v1/datastreams/light/datapoint
```

Response

```
{"nonce": 5619936, "datapoint": {"x": 100,"y": 200,"z": 0,"k": 0,"l": 50},"deliver_to_device": true}
```

Set light status

Linux/Cygwin curl：

```
curl -X POST -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" –d '{"datapoint":{"x": 100, "y": 200, "z": 0, "k": 0,"l": 50}} ' http://114.215.177.97/v1/datastreams/light/datapoint/?deliver_to_device=true
```

Windows curl：

```
curl -X POST -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" –d "{\"datapoint\":{\"x\": 100, \"y\": 200, \"z\": 0, \"k\": 0, \"l\": 50}}" http://114.215.177.97/v1/datastreams/light/datapoint/?deliver_to_device=true
```

Response

```
{"nonce": 5619936, "datapoint": {"x": 100,"y": 200,"z": 0,"k": 0,"l": 50},"deliver_to_device": true}
```

X = frequency, range 1~500.

Y (red), Z (green), K (blue) indicate that the different colors of lights, range 0~255.

L parameters are reserved.

4.1.7. Humidity and Temperature Sensor

✧ Device

Upload data packets of this format:

```
{"nonce": 1, "path": "/v1/datastreams/tem_hum/datapoint/", "method": "POST", "body": {"datapoint": {"x": 35,"y": 32}}, "meta": {"Authorization": "token HERE_IS_THE_MASTER_DEVICE_KEY"}}
```

X = temperature, Y = humidity.

Device key after token. When upload successful, the server will respond as follows:

Response

```
{"status": 200, "datapoint": {"updated": "2014-05-14 18:42:54", "created": "2014-05-14 18:42:54", "visibly": 1, "datastream_id": 16, "at": "2014-05-14 18:42:54", "y": 32, "x": 35, "id": 882644}}
```

The last data update time will be contained in the response information.

✧ PC

The PC gets sensor information through two kinds of interfaces. Fonts in red are user's owner key.

1. Get the latest nformation:

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" http://114.215.177.97/v1/datastreams/tem_hum/datapoint
```

Notes: Above mentioned command will respond "remote device is disconnect or busy" since the sensor does not support reverse control.

2. Get historical data collected by sensor devices:

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token e474bba4b8e11b97b91019e61b7a018cdbaa3246" http://114.215.177.97/v1/datastreams/tem_hum/datapoints
```

4.1.8. User defined reverse control

The Espressif Cloud Server supports user defined reverse control actions. Send the action to the device with additional parameters and flexible reverse control can be realized. The command format is as follows:

Linux/Cygwin curl：

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token HERE_IS_THE_OWNER_KEY" 'http://114.215.177.97/v1/device/rpc/?deliver_to_device=true&action=your_custom_action&any_parameter=any_value'
```

Windows curl：

```
curl -X GET -H "Content-Type:application/json" -H "Authorization: token HERE_IS_THE_OWNER_KEY" "http://114.215.177.97/v1/device/rpc/?deliver_to_device=true&action=your_custom_action&any_parameter=any_value"
```

The user defined portion is marked red. Users can analyze the action and parameter in codes and define their own functions.

Device side receives following:

```
{"body": {}, "nonce": 872709859, "get": {"action": "your_custom_action", "any_parameter": "any_value", "deliver_to_device": "true"}, "token": "HERE_IS_THE_DEVICE_KEY", "meta": {"Authorization": "token HERE_IS_THE_DEVICE_KEY "}, "path": "/v1/device/rpc/", "post": {}, "method": "GET", "deliver_to_device": true}
```

Note: RPC commands can only realize flexible reverse control but does not save

history info. For example,users can define an action to control the fan to stop turning, but server will not record how many times the fan has turned or stopped.