

Titan Router

V6 Firmware

Application note 63

Using a TITAN-based device to read an
IEC Electricity Meter

60870-5-102

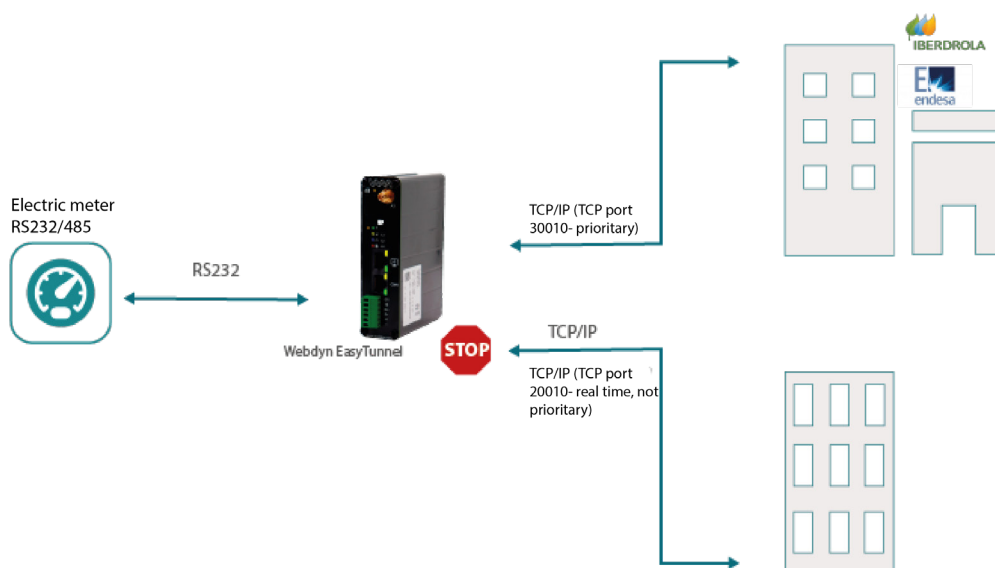
via the multiple IP-RS232 gateway
with Connection Priority

1. Scenario details

TITAN-based devices have all the typical functions of a 4G/3G/2G router, as well as a series of additional features that make them one of the best performing devices on the market. One of the additional benefits is the ability to create IP-RS232 gateways with **connection priority**, particularly for reading IEC 60870-5-102 electricity meters

2. Example scenario description

- There is an Electricity Meter (IEC 60870-5-102) with the RS232 serial port (9600,8,N,1)
- The aim is to configure the TITAN-based device to create an IP-RS232 gateway and to read the meter in real-time via an IP from a specific location. The connection will be made through the TCP 20010 port
- The electricity supply company will also connect via IP communications to carry out a daily meter reading. This will be done through the TCP 30010 port. This connection through the TCP 30010 port will be prioritised over the TCP 20010 port. Therefore, when an connection from an electricity supply company enters the TCP 30010 port, real-time communications via the TCP 20010 port will need to be suspended until the IP connection of the electricity supply company through the TCP 30010 port is complete.



3. Configuring the corresponding serial port

You need to configure the RS232 serial port of the TITAN-based device first, since this port will be used to read the meter. These values coincide with those of the configuration of the meter's serial port, which in this example is 9600,8,N,1.

As in this example, the aim is to read the meter through an IP connection, so you must configure a TCP server gateway. The TCP 20010 port is to be used for the IP connection for real-time readings while the TCP 30010 port is the electricity supply company's preferred connection.

To do this, access the **"Serial Settings - Serial Port1-232"** menu and configure the screen as follows:

The screenshot shows the webdyn TITAN configuration interface. The left sidebar contains a menu with categories: Mobile, Ethernet, Firewall, Serial Settings, External Devices, and Other. Under Serial Settings, 'Serial Port1-RS232' is selected and highlighted with a red box. The main panel is titled 'Serial Gateway > Com1 Settings'. It contains several configuration fields: Baudrate (9600), Data bits (8), Parity (none), Stop bits (1), Flow Control (none), and Timeout ms (50). These fields are grouped by a red box. Below these fields are three checkboxes: 'Allow local embedded AT commands', 'Allow remote embedded AT commands', and 'Allow incoming GSM call (CSD Data Call)'. A red box highlights the 'Function' section, which is set to 'Serial - IP Gateway (TCP Server)'. This section includes fields for 'TCP Local Port' (20010), 'Timeout' (300), and 'TCP Local Priority Port' (30010). A red box also highlights the 'Temporal client RS232' checkbox, which is unchecked.

4. Configuring the Mobile section

Since CSD calls are not required in this scenario, you are advised to set the device to "auto" mode (rather than "forced" (to 2G), such as for when CSD calls are required). Go to the **"Mobile - Basic Settings"** menu to correctly configure the network. The correct configuration is shown in the image below. In this configuration, the 4G/3G/2G WAN interface is enabled (so that the device obtains an IP) and the APN, username and password of the SIM card are all specified.

★ **Mobile**

○ Status

○ **Basic Settings**

○ Keep Online

★ **Ethernet**

○ Basic Settings

★ **Firewall**

○ Authorized IPs

★ **Serial Settings**

○ Serial Port1-RS232

○ Serial Port2-RS485

○ Serial Port3-RS232

○ SSL Certificates

★ **External Devices**

○ Logger configuration

○ ModBus Devices

○ Generic Serial Device

○ Temperature Sensor

○ IEC102 Meter

★ **Other**

○ AT Command

○ DynDns

○ Private DynDns

○ Sms control

○ Periodic Autoreset

○ Time Servers

○ Remote Console

○ Snmp

▶ **Mobile ▶ Basic Settings**

Mobile WAN: Enabled (IP active) Enable Wireless WAN interface

Sim Mode: SIM1 Sim selection

SIM1 APN: movistar.es SIM Card 1 APN

SIM1 Username: MOVISTAR SIM Card 1 username

SIM1 Password: SIM Card 1 password

SIM1 Pin: SIM Card 1 PIN

SIM1 Auth: Auto SIM card 1 authentication

SIM2 APN: SIM Card 2 APN

SIM2 Username: SIM Card 2 username

SIM2 Password: SIM Card 2 password

SIM2 Pin: SIM Card 2 PIN

SIM2 Auth: Auto SIM card 2 authentication

Network selection: Auto (4G/3G/2G) network selection

DNS selection: Get DNS from Operator



5. Other configurations

You also have the option to configure SMS messages on the TITAN-based device in case you need to perform any future action on it (such as a configuration change, a remote reset, a status reading, etc.) from any location. You can configure SMS messages from the **"Other -SMS control"** menu.

The image below shows a configuration where SMS messages are enabled, with a header (password) containing the text "mtx" and all phone numbers authorised (from where an AT command is sent via SMS). If you only want authorised telephones to send AT commands via SMS, do not check the "all phones" box and enter the authorised telephone numbers in full (for example, +34666123456).

With this in mind, if you need to check the coverage remotely, for example, you can send an SMS containing the text "mtx at+csq" and you will receive an SMS message with the requested information.

It may also be useful if your SIM card provides you with a public IP address (or accessible IP) and you have enabled the Telnet or SSH console to send AT commands to the device remotely and avoid unauthorised access. This can be done from the **"Other - Remote console"** menu. Try not to use standard ports for Telnet (23) and SSH (22) if you are using a SIM card with a public IP address. This will also avoid unwanted traffic. You can also use the **"Firewall - Authorized IPs"** menu section to authorise access to the remote console only from authorised IP addresses.



- ★ Mobile
 - Status
 - Basic Settings
 - Keep Online
- ★ Ethernet
 - Basic Settings
- ★ Firewall
 - Authorized IPs
- ★ Serial Settings
 - Serial Port1-RS232
 - Serial Port2-RS485
 - Serial Port3-RS232
 - SSL Certificates
- ★ External Devices
 - Logger configuration
 - ModBus Devices
 - Generic Serial Device
 - Temperature Sensor
 - IEC102 Meter
- ★ Other
 - AT Command
 - DynDns
 - Private DynDns
 - **Sms control**

Other > SMS control

SMS function

AT : ☒ enabled

AT header:

Authorized phone numbers: ☒ all phones

Send AT Commands by SMS allowed (you can reboot the device, get IP Wan, get GSM RSSI, change configuration, ...)

Header of at commands

All Phones are allowed

Authorized number 1

Authorized number 2

Authorized number 3

Authorized number 4

Authorized number 5

Authorized number 6


Authorized number 7


Authorized number 8

Authorized number 9

Authorized number 10

It may also be useful if your SIM card provides you with a public IP address (or accessible IP) and you have enabled the Telnet or SSH console to send AT commands to the device remotely and avoid unauthorised access. This can be done from the **"Other - Remote console"** menu. Try not to use standard ports for Telnet (23) and SSH (22) if you are using a SIM card with a public IP address. This will also avoid unwanted traffic. You can also use the **"Firewall - Authorized IPs"** menu section to authorise access to the remote console only from authorised IP addresses.

 **webdyn**
flexitron group

 **TITAN**
"Makes your APPLICATION happen"

★ **Mobile**

● Status

● Basic Settings

● Keep Online

★ **Ethernet**

● Basic Settings

★ **Firewall**

● Authorized IPs

★ **Serial Settings**

● Serial Port1-RS232

● Serial Port2-RS485

● Serial Port3-RS232

● SSL Certificates

★ **External Devices**

● Logger configuration

● ModBus Devices

● Generic Serial Device

● Temperature Sensor

● IEC102 Meter

★ **Other**

● AT Command

● DynDns

● Private DynDns

● Sms control

● Periodic Autoreset

● Time Servers

● Remote Console

● Snmp

▶ **Other ▶ Remote Console (TCP Server)**

Enabled: ☒

Enable remote console

TCP port:

TCP port for remote console

Username:

Username of your account

Password:

Password of your account (min 8 char)

SSH: ☒

Enable SSH security

SAVE CONFIG

6. Once the configurations are complete

Once you have completed the aforementioned configurations, you should re-start the TITAN-based device so that it can begin to operate with the new configuration. To do so, please go to the **"Other - reboot"** menu.

Any questions?

Please send us an email to iotsupport@mtxm2m.com