



# TELETASK

**Home Automation**

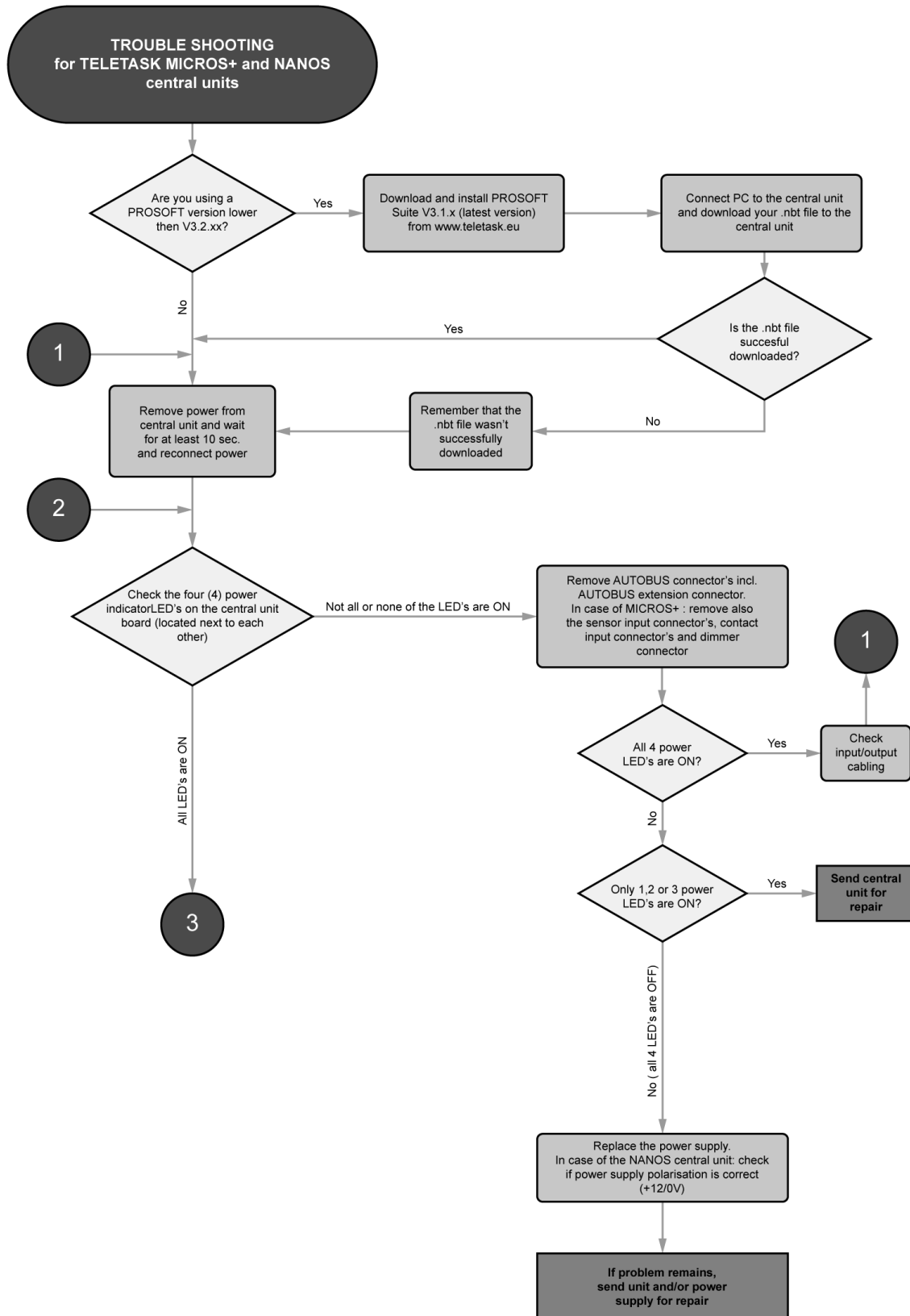
## **Support & Troubleshooting + Tips & tricks**

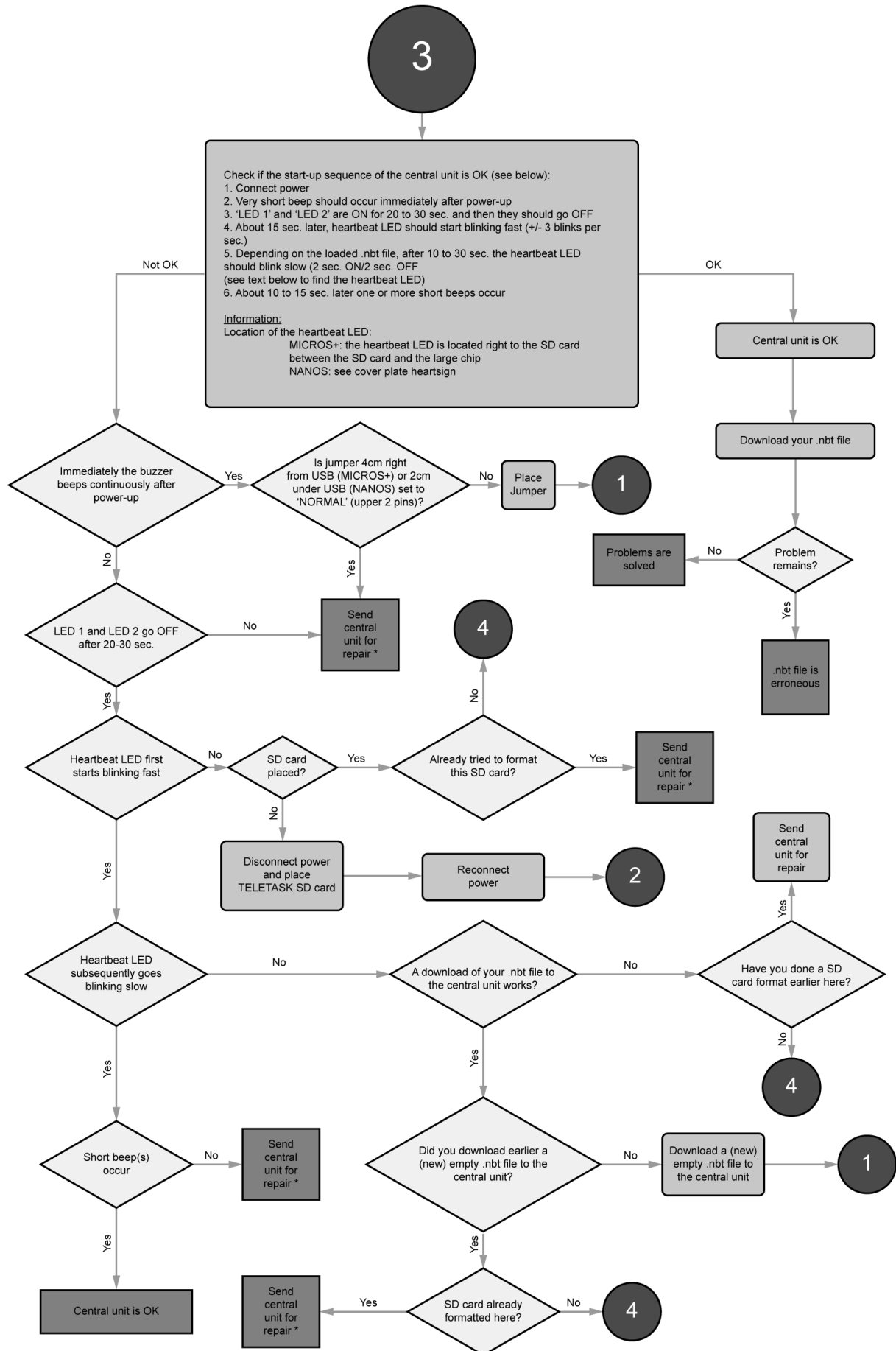
**Version: May 8, 2024**

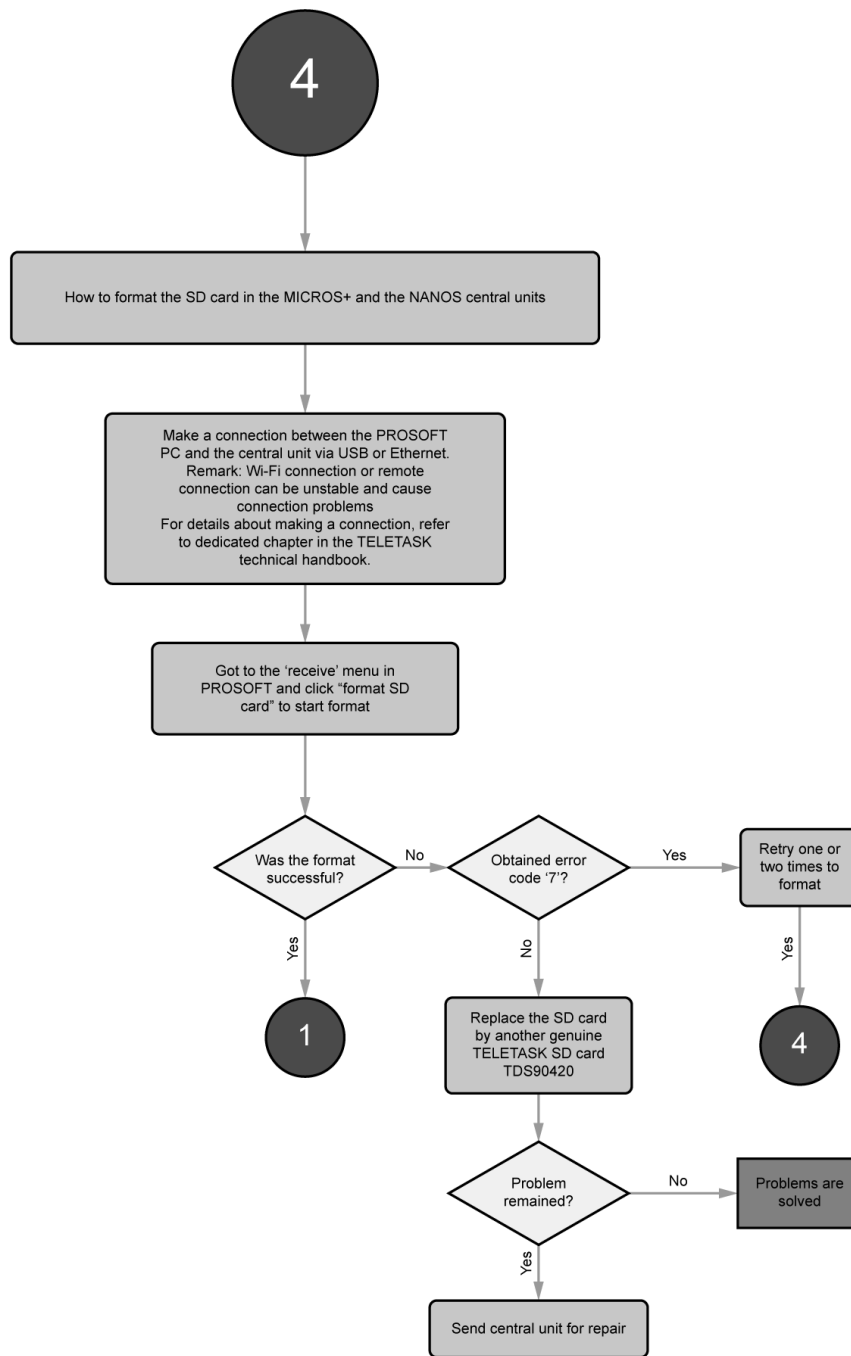
# Table of Contents

1	Trouble shooting MICROS+ and NANOS.....	3
2	Replacing MICROS+ power supply with a TDS10134 DIN rail power supply.....	7
2.1.1	The different actions step by step .....	7
3	Distribution board recommendations.....	11
4	SERVUS TDS12110 Touch Screen Calibration.....	17
4.1	How to start touch screen calibration? .....	17
4.2	Finalizing Calibration.....	19
5	AURUS-TFT hardware reset.....	20
5.1	Intro.....	20
5.2	How to reset an AURUS-TFT to factory settings? .....	20
6	Case Studies.....	23
6.1	DoIP – VPN Integration .....	23
6.1.1	Introduction.....	23
6.1.2	Dynamic DNS (DynDNS).....	23
6.1.3	Network Range .....	24
6.1.4	VPN routers .....	25
6.1.5	Set up a VIGOR 2130.....	26
6.1.6	Setup a SG300 (not available anymore) .....	30
6.1.7	Setting-up a client-VPN connection.....	36
6.1.8	Test the VPN connection .....	41
6.1.9	Using a TELETASK GUI over the VPN connection .....	42
6.2	How to control a CEILING SWEEP FAN.....	43

# 1 TROUBLE SHOOTING MICROS+ AND NANOS







## TROUBLE SHOOTING (\*/\*\*/\*\*\*) for a MICROS+ and a NANOS central unit.

\*

Occurred problem:

in exceptional case, the buzzer immediately beeps continuously after the power up.

Possible reason:

the resistor R33 must be 18k ohm instead of 10k ohm

Solution:

send for repair to replace the R33 10k ohm m(ust be replaced by a 18 k ohm resistor)

Involved central units:

MICROS+ : serial number xxxxx0101 to xxxxx0611

NANOS: serial number xxxxx0101 to xxxxx0151

\*\*

Occurred problem:

in exceptional cases the heartbeat LED never blinks after the power up

Possible reason:

problem with the SD card connector  
resistor R20 is to be exchanged (56K has to be replaced by 6K8)

Solution:

send for repair to replace the SD card and/or R20

## 2 REPLACING MICROS+ POWER SUPPLY WITH A TDS10134 DIN RAIL POWER SUPPLY.



The work instructions below are exclusively for a qualified electrician.



The intention is that we arrive at the result as shown in the picture on the left. The TDS10134 power supply is placed at the top right of the MICROS+ cabinet on a DIN rail instead of the 'old' power supply under the sealing cap (photo above).

How to do this

### 2.1.1 The different actions step by step

**IMPORTANT !!: First, remove the supply voltage from the distribution board and from all connected components. Only after all tensions have been disconnected, you can start and work safely.**

Open the MICROS+ case with a beard lock key.





Remove the protective hood from the power supply by unscrewing the two M3 bolts with a star screwdriver.

You no longer need the hood. You have to recycle it with metal waste.



Now you can see the power supply to be replaced with the connection to the 230VAC input + the grounding on the right and the 12V output to the MICROS board on the left.



Carefully pull the 230V power connector and also the grounding connection from the PCB on the right.

Then do the same on the left side with the 12V power connector (with red and black wire).





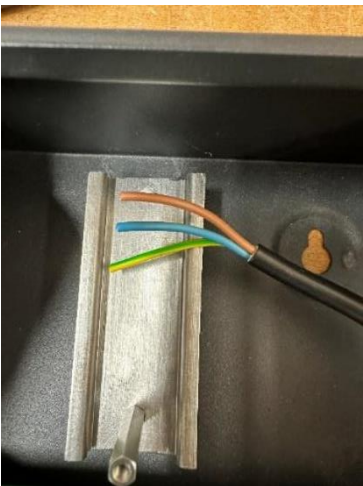


Now unscrew the two stainless steel spacers (30mm) by turning them counterclockwise with a flat wrench or socket wrench.

Keep one spacer with lock washer and one bolt with lock washer for later.



Now pull the PCB off the housing. Be careful with the white plastic support at the top right because we will use it again later (so just leave it on).



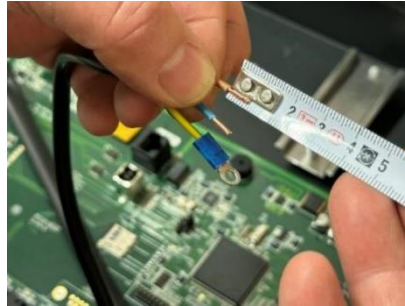
- Now cut a piece of DIN rail about 8 cm long and drill two holes in the middle at exactly 6.5 cm apart. The top hole should be 4mm in diameter and the bottom diameter should be 3mm.

- Install the DIN rail with the largest hole (4mm) facing up, provided that you use the existing white spacer for the 4mm hole and at the bottom of the press socket M3. Secure the DIN rail with the remaining stainless steel spacer with a locking ring between the DIN rail and the spacer bushing.

- Place the TDS10134 power supply on the rail, with the 230V input on the right side.



Cut both connectors (left and right of the power supply) from the wires and dismantle all five wires over a length of 7 mm.



Connect the two 230V wires to the power supply ("L"=brown wire; "N" = blue wire).

Apply a crimping eye (blue type) to the ground wire and connect it on top of the stainless steel spacer socket and secure with the M3 bolt with lock washer.



Now also connect the two (red and black) wires to the output of the power supply.

! Please note that the red wire must be connected to the +12V (top screw) and the black wire to the 0V connection (bottom screw).

The replacement is now complete. You can switch the power supply back ON.

### 3 DISTRIBUTION BOARD RECOMMENDATIONS

The wiring of the distribution board (DB), equipped with TELETASK interfaces is not different to any other DB. As there are both low-voltage (110-400V) and extra low-voltage (mainly 12-24V) devices in a typical Home Automation DB, these two should be kept away from each other as much as possible. CE regulations and general quality oblige the panel/DB- builder to hand a simple but very important rule: bring all low voltage wires/cables at one side of the DB and the extra-low voltage wires/cables at the other side.



For example low voltage at the right (from below and from above). The extra-low voltage wires at the opposite side, in this case at the left side of the DB.

Before you select the DB you need to know if you are going to use the NANOS or MICROS+ central unit. With NANOS there are no special remarks because this is a standard DIN-rail unit. If you use a MICROS+ central unit, you need to decide if you want this central unit going to be installed external or internal in the DB.

1. for small installations with MICROS+ and up to 10 DIN-rail TELETASK interfaces (like TDS12116, TDS13500, TDS13524...), we recommend to use a standard (plastic or metal) DB and have the MICROS+ installed beside of it (left or right).



Figure 1: MICROS+ outside distribution board



2. For medium and large installation where you have more interfaces (and circuit breakers and other components) to be installed in the DB, we recommend to use one or more large industrial DB cabinets. Most of them are metal plate based.

The MICROS+ is then mounted in the DB. Keep in mind that the MICROS+ in- and outputs are at the bottom side of its housing. The extra-low voltage wires (contact inputs, sensor inputs, AUTOBUS connections..) are at the left side (one large hole) and the low-voltage (output relay contacts for 12-250Volt) are to be made through the round break-out holes on the same bottom plate but the mid- to right side. This fits with a DB which is wired in the same way (extra-low voltage to the left).

Remark for MICROS+ installation: for easy wiring, start-up and servicing, mount the housing at eye level height. This means underside of the MICROS+ housing at about 100 to max. 170 cm from ground level.

Generally, circuit breakers can be mounted below in the DB because the non-controlled circuits (circuits like the ones to freezers, refrigerators which are not on/off controlled by the TELETASK system) do not need to be connected over screw terminals (see also below about using DIN-rail screw terminals).

So you obtain the shortest cabling to power cables coming from below by connecting them directly with the concerned circuit breaker, which in this case should be installed in the lower part of the DB.



**Figure 2: Clear division between input and output cables**

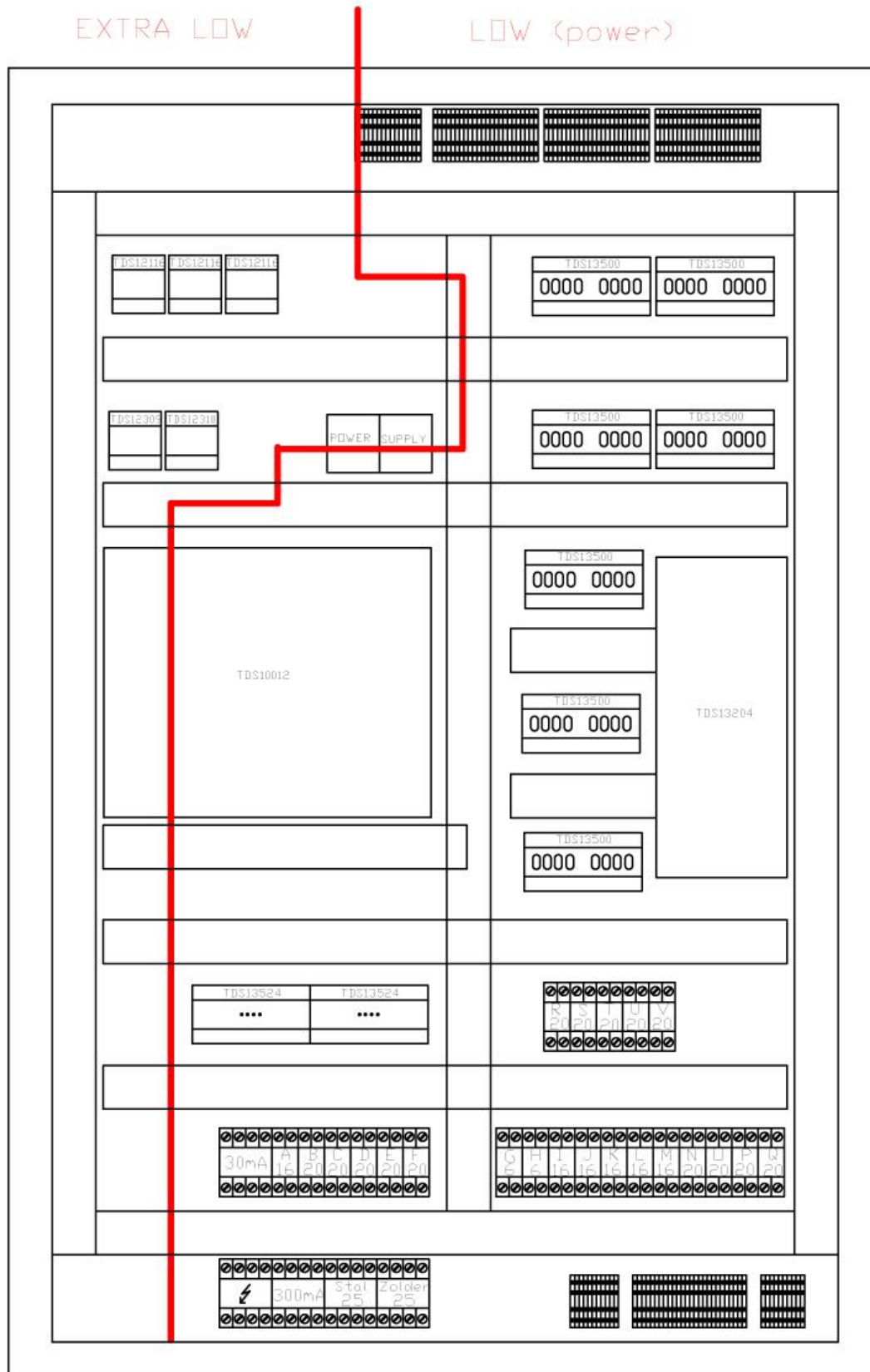


Figure 3: Division between extra-low and low voltage interfaces

**Cable trays:**

To have the necessary trays for bringing the wires and cables up/down in the DB, we recommend using a wide cable tray at the left and at the right side of the DB. It may be necessary to have a larger cable tray for the 110-250V cabling than for the extra-low voltage (signal) cabling. Some panel builders will divide the panel in two parts or in zones.

Only extra-low voltage and signal interfaces in the left part of the DB and low-voltage at the right. In such case, you can have a cable tray left for extra-low voltage and a tray in the middle and at the right of the DB for low voltage wiring.

Remark: extra-low voltage wiring is not only for TELETASK, but may also be applicable for other systems placed in the DB like video-door phone system, security, IT equipment, etc...

Another way of working in large DB's is using zones: A zone for Home Automation, a zone for video-door phone and a zone for circuit breakers. This is also a possible way of working.

Any how, you need to arrange that extra-low voltage and low voltage wires and cables are mounted isolated from each other. A general rule is keeping cables/wires away from each other at least 5 cm. So if you have two cable trays in parallel keep a distance of 5 cm between them.

**Earthing:**

It is very important to have a correct earth connection to the central unit. The whole network of central unit and AUTOBUS shieldings (to all interfaces, touch panels...) is based on a good central earth connection in the MICROS+ central unit.

Always connect the main DB- earth connection directly to the earth connection of your electrical installation. Use the internal screw in the MICROS+ housing at the lower-right corner. In case of the NANOS central unit, like on the MICROS+, it is the earth connection on the NANOS which becomes the central earth point.



Figure 4: MICROS (old version) Central unit

**DIN-rail screw terminals:**

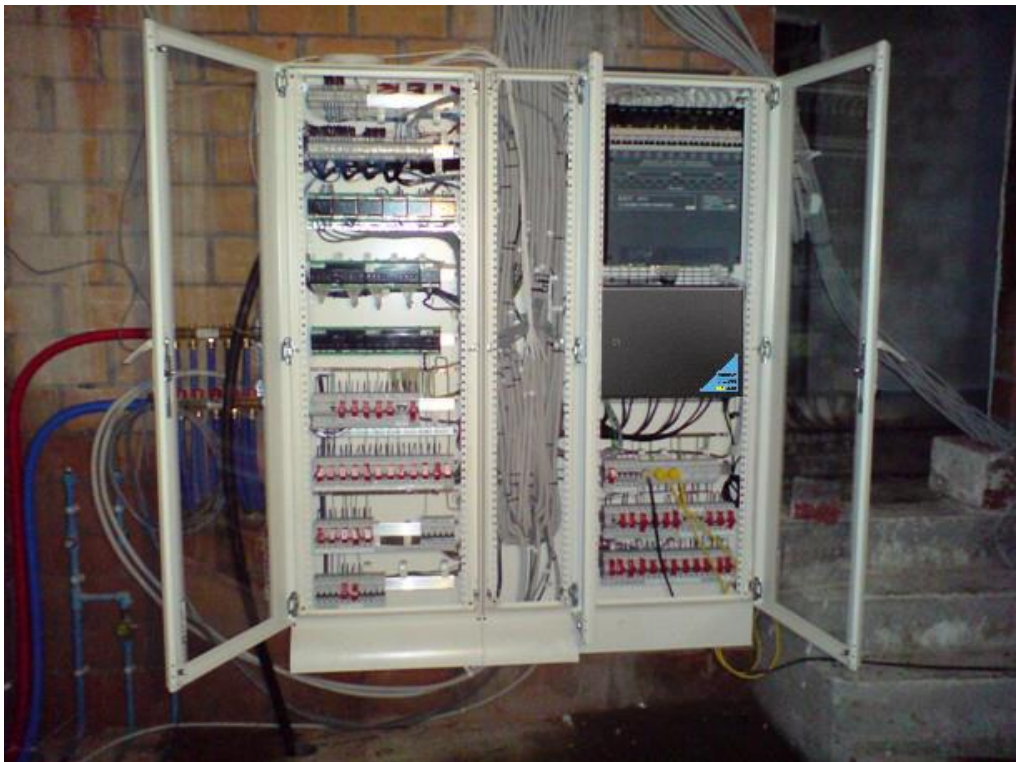
For medium- and large DB's it is recommended to use the lowest and highest DIN-rail for mounting screw terminals. All connections between the DB and the building can be made over these terminals. This way, the panel builder (DB-builder) can fully pre-wire the DB before bringing it at site. It also avoids dust getting in the DB during the construction of the house/building.

Most electrical contractors use spare wires in their cable between standard contacts/push-buttons and the contact inputs in the DB. These inputs can be in the MICROS+ central unit (32) or on digital input interfaces like TDS12116 (16 channel input voltage free contact interface). To avoid having to many cables/wires coming in the MICROS+ unit, you only connect the used wires to the DIN-rail screw terminals and keep the spare wires unconnected.

Then you use for example 3 multi-wire cables (6pair) to go from the DIN-rail screw terminals to the MICROS+ contact inputs. It will make wiring much more simple, faster and obtain the highest quality/reliability.

A standard DIN-rail is 24 units wide. The TDS13500/TDS113501/TDS13524 interfaces are 10 units wide. It means you can mount for example 2 x TDS13500 beside of each other and have 4 units available for 2x2 circuit breakers which can each supply the power to each individual TDS13500 interface (if 16/20Amp is enough to power all connected circuits on the TDS13500).

***Example distribution board:***



**Figure 5: Example distribution board - placing the MICROS+ at the left would have been better.**

- The distribution board is divided in zones with a clear division.
- Good overview and clean wire arrangement.



- Screw terminals and circuit breakers at the top and bottom of the board.

**Tip: By placing the MICROS+ at the left side of the cabinet you avoid crossing extra-low voltage cable and low voltage cables. This way the input-/sensor-/AUTOBUS-cables can be run through a left cable tray and all power wires can be run through the middle and right cable tray!**

## 4 SERVUS TDS12110 TOUCH SCREEN CALIBRATION

### 4.1 How to start touch screen calibration?

Choose the “Settings Menu” from the main menu buttons.

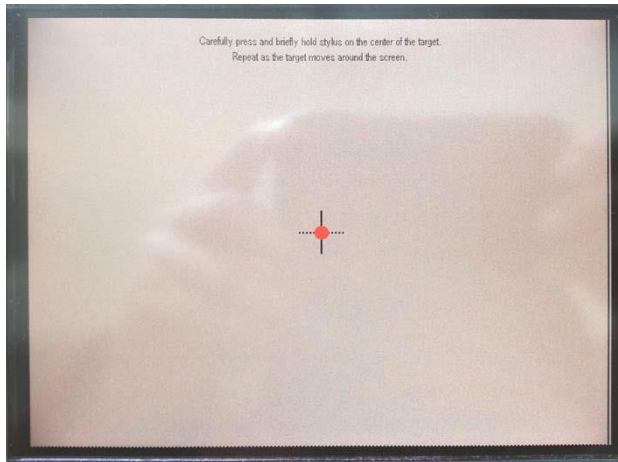


Push the hidden “Calibration Button” on the lower right side of the touch screen.

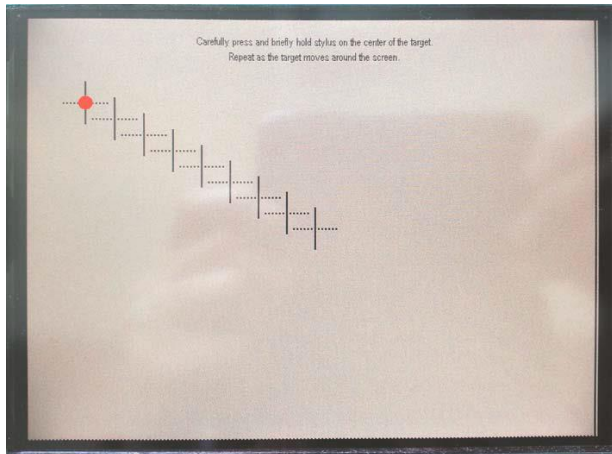


Follow the instructions and touch each of the required 5 calibration points (center of the last cross) with a stylus (not your hand), to recalibrate the SERVUS touch screen.

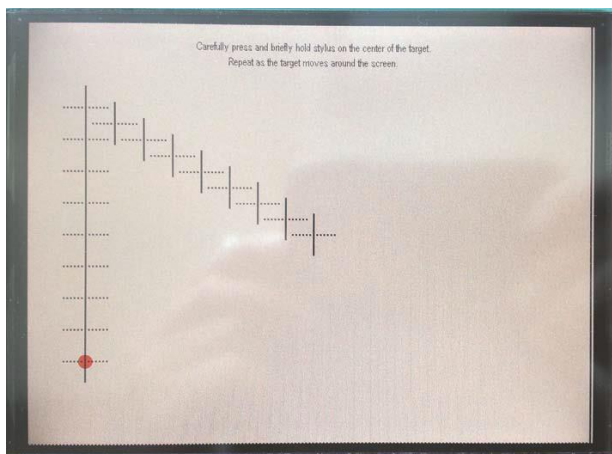
1.



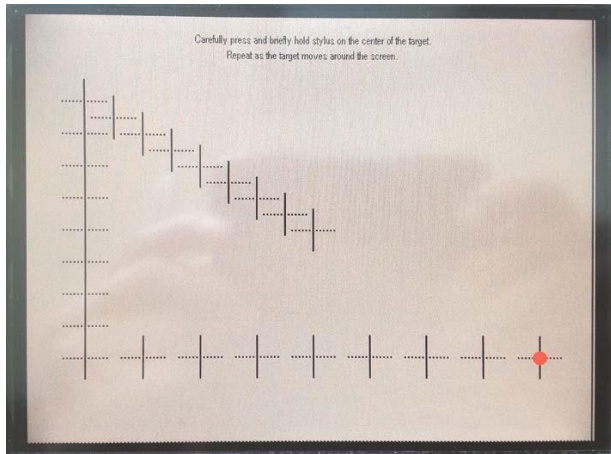
2.



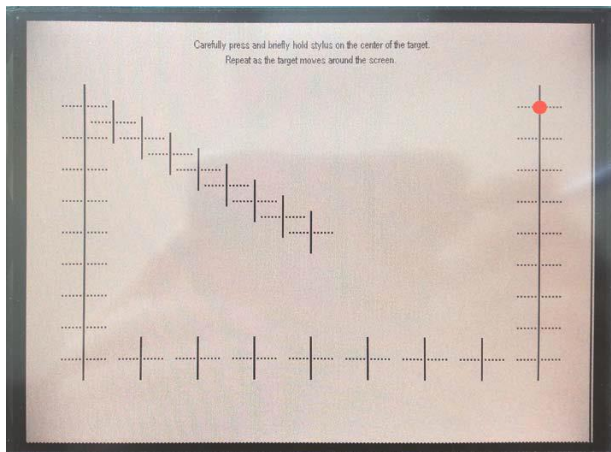
3.



4.



5.



## 4.2 Finalizing Calibration

After you touched the fifth and therefore final calibration point with the stylus, the program will ask you to touch the center of the screen, to confirm and save the calibration data. If you do not touch the center of the screen for confirmation within 30s, the calibration will be aborted and the new calibration data will be discarded.

## 5 AURUS-TFT HARDWARE RESET

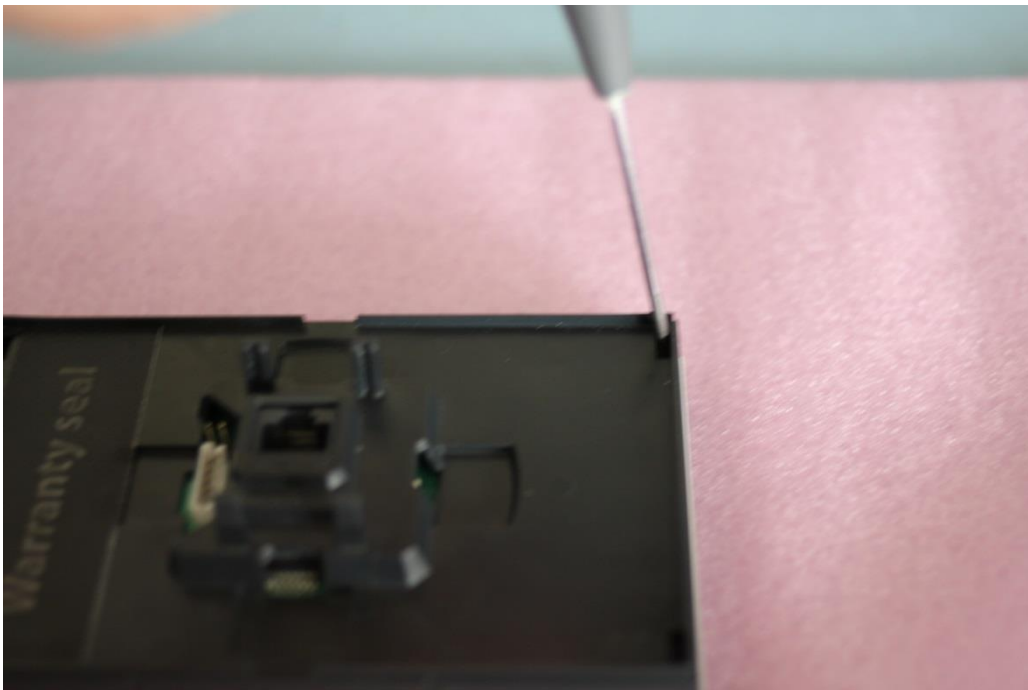
### 5.1 Intro

In some exceptional cases it can be that the AURUS-TFT hangs in the start-up screen. If this is still the case when the AUTOBUS cable is removed and reconnected, then the following instructions can bring the AURUS-TFT back to factory settings.

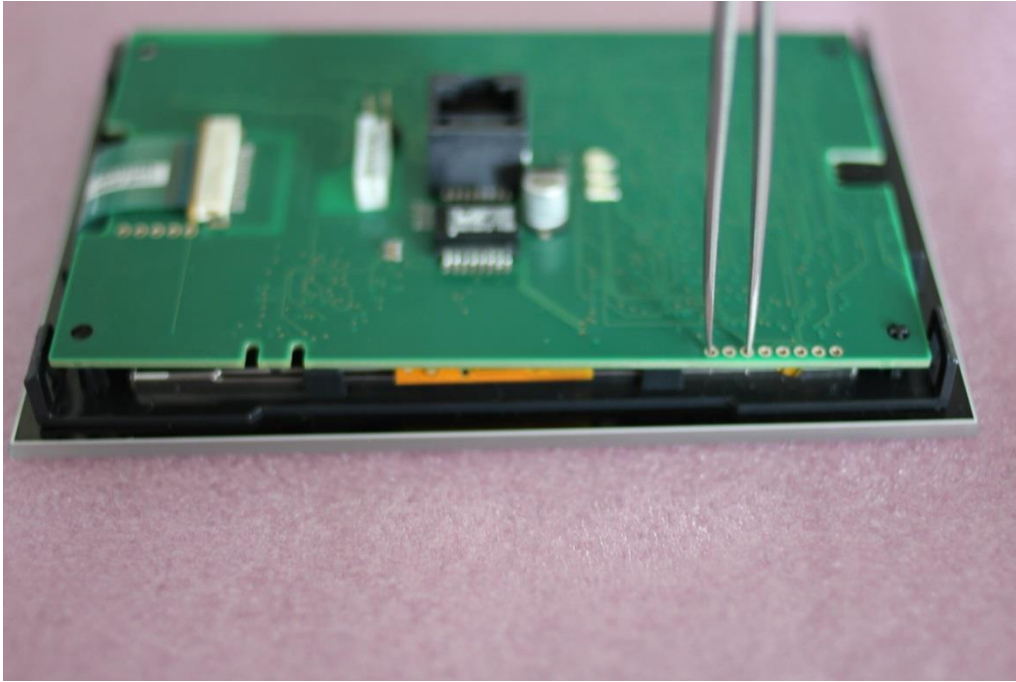
This is only applicable for AURUS-TFT versions with serial number bigger than \*\*\*\*\*0256.

### 5.2 How to reset an AURUS-TFT to factory settings?

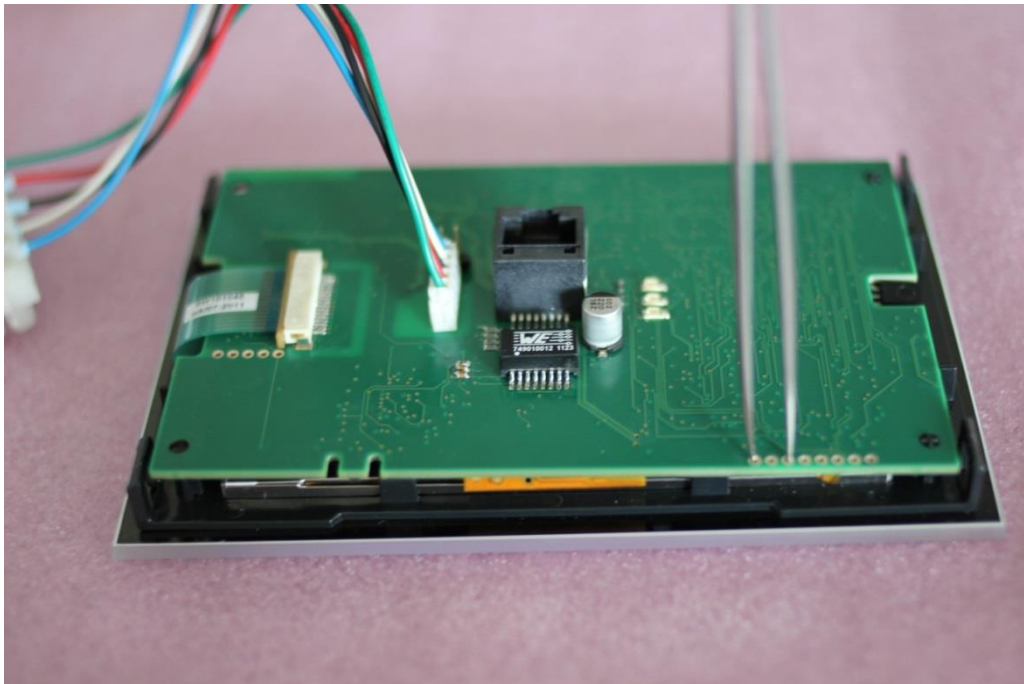
1. First of all, check if the last four digits of the serial number is bigger than 0256.
2. Put the AURUS-TFT downwards on a soft surface.
3. Remove the backcover of the AURUS-TFT by gentle pushing the inner snaps in the corners towards the center with a flat screwdriver, while pulling the backcover upwards. Repeat this for the four corners.



4. With the backcover removed, connect the first and third hole with a tweezer or a wire, like shown on the picture below.



5. Reconnect the AUTOBUS cable with the holes still connected.



6. The AURUS-TFT will now startup in the 'bootloader' screen. Remove the tweezer or wire and let the AURUS-TFT continue the upgrade process via AUTOBUS.





7. The AURUS-TFT is now back to factory setting and has received the latest updates of the Central unit. If the problems remain than contact your TELETASK distributor.



## 6 CASE STUDIES

### 6.1 DoIP – VPN Integration

#### 6.1.1 Introduction

This document describes how you can set up a home network for the use of a GUI, GUI+ or iSGUI which is to be run from a remote (away) location.

To do this, TELETASK advises to use a VPN (Virtual Private Network) connection. The advantages of VPN are:

- Universal (available from different brands)
- Protected against unwanted access (data is encrypted).
- GUI configuration is the same for both local and remote use.

The principle of VPN is easy: From a remote location it adds your laptop or Smartphone (virtually) to your home network (LAN). For this you need either a "Static IP address" or a "Dynamic DNS" address. A static IP address is the most easy and preferred solution, but Dynamic DNS can be an alternative (probably cheaper) solution. This may vary from country to country.

To set up a VPN connection the following steps are needed:

- Setting up a router (at home) with embedded VPN server
- Setting up a VPN connection on it via your PC or mobile device
- Test the VPN connection

Setting up a VPN router solution needs ICT skills and network knowhow. If you are not an experienced professional, TELETASK recommends that you consult your ICT supplier.

#### 6.1.2 Dynamic DNS (DynDNS)

##### 6.1.2.1 Intro

Dynamic DNS is a service with which your VPN router regularly sends its dynamic (changing) IP address to a dedicated server on the internet with a static (known and never changing) IP address, so you can have access to your VPN router from anywhere on the internet.

There are several providers of this service one of the most known is [www.DynDNS.org](http://www.DynDNS.org). In this chapter we will create a DynDNS account, and set up the VIGOR 2130 to work with this account.

### 6.1.2.2 Create a DynDNS account

Creating a DynDNS account is necessary to use the DynDNS service.

- Open a browser and go to [www.DynDNS.org](http://www.DynDNS.org).
- Create an account and complete the required information.
- Once your account has been activated you can log in.
- Enter a "Hostname", select the service type "Host with IP address", click on the "Use auto detected IP address" link, and click "Create Host" (it is advised to perform this step at the location where the TELETASK central unit is placed).

### 6.1.3 Network Range



**IMPORTANT:** When using a VPN connection from a network you must make sure that the network to which you are connecting and the network from which you are connecting are in a different IP subnet (in most cases this means that the 3 first numbers are not the same, 192.168.1.1 and 192.168.1.100 are in the same subnet, 192.168.0.1 is in a different subnet and so is 10.0.1.1)

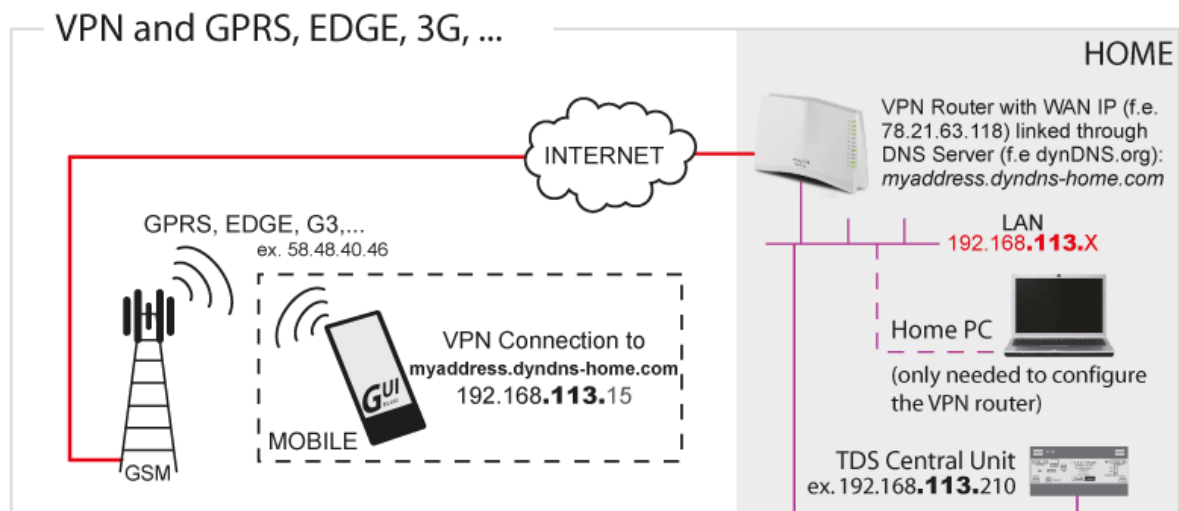
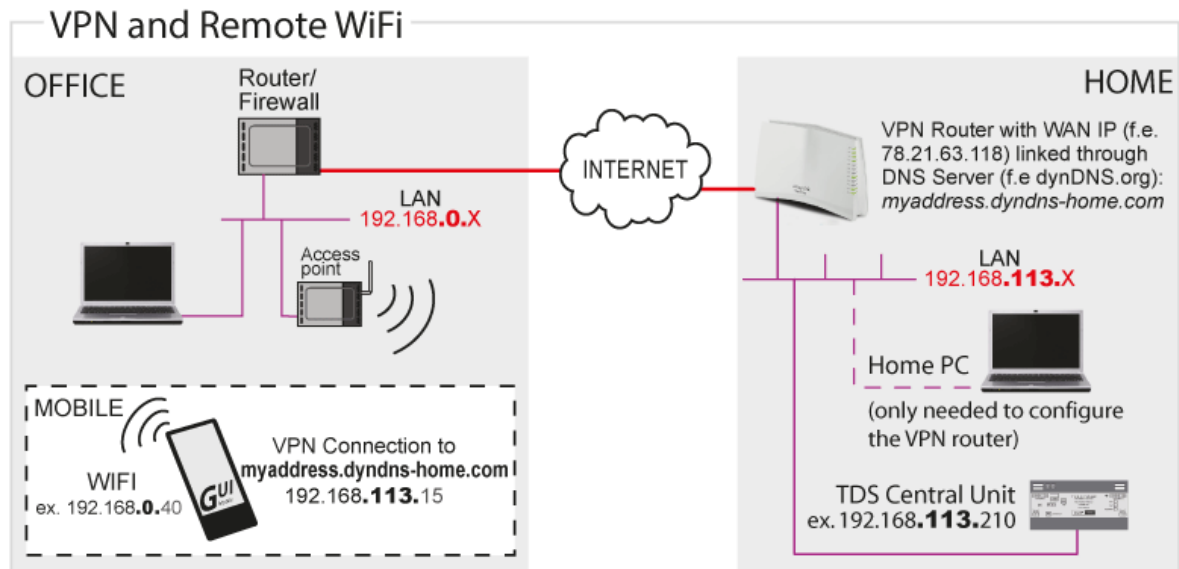
Example: If you have configured your private network in the range 192.168.1.xxx and you have an iSGUI on your Smartphone, you will not have a problem when connecting over a GPRS/EDGE/3G/HSDPA connection. If you have a holiday home (with an internet connection) you can connect to your TELETASK central unit using the WLAN of your holiday home but you must make sure that the network range in your holiday home is different from 192.168.1.xxx.

Most residential and small business networks are in the range 192.168.X.X with 192.168.1.X and 192.168.0.X being the most used by far. As you do not necessary know from which networks you will connect to your network using VPN it is advisable to choose an arbitrary number for the third part of the IP address e.g 192.168.113.X.



**Do not use 168 or 10 as third number because this may interfere with the virtual network that is set up over the USB connection to your TELETASK central unit.**

Basic drawing of the setup (the PC at home is not needed and is just added as a practical example of a home network. The PC is only temporarily needed for the configuration of the VPN router):



#### 6.1.4 VPN routers

There are a lot of routers available on the market with an embedded VPN server and it is impossible to give instructions for all the different types.

Therefore at TELETASK we have tested some of these types and give you a detailed installation procedure for (in our opinion) a reliable, easy to install and well priced router: the VIGOR 2130 from DrayTek.

This document also contains detailed info for setting up a SnapGear SG300 router. This router is no longer available but for the people who already has purchased this device the information is not removed from this document..

For other types of routers, the steps for setting up a VPN connection are more or less the same, but if you decide to use another type of router please note:

- Although PPTP (a protocol for VPN) is a standard, the specific implementation may vary from brand to brand (router and device). So check if the device (e.g. PC or SmartPhone) is compatible with the router.
- There are different types of data encryption so check the specifications of you (mobile) device when choosing a router. Make sure that they are compatible.
- TELETASK can't offer support on any type of router. If you need help, please contact your local router supplier (for VIGOR check [www.draytek.com](http://www.draytek.com)).

### 6.1.5 Set up a VIGOR 2130

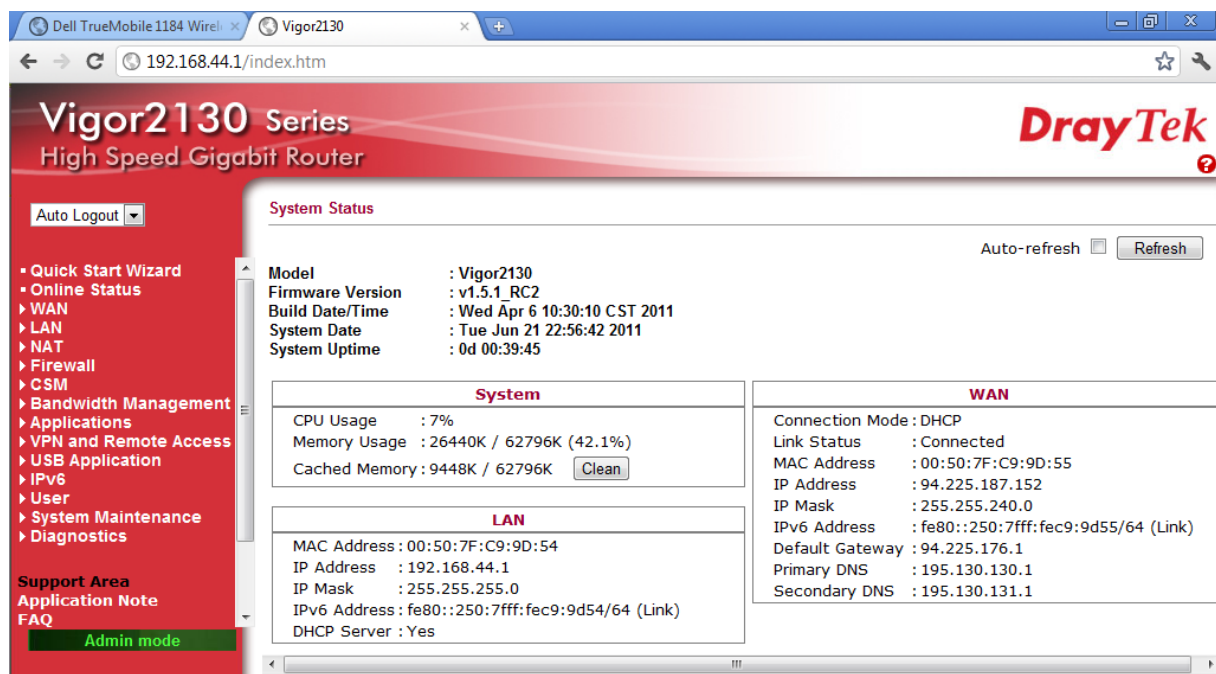
In this part of the document the term 'VIGOR' refers to a VIGOR 2130 series router. For this document the standard VIGOR 2130 is used, but versions with integrated WiFi and other functionalities are also available.

#### 6.1.5.1 General settings

To get started for Setting up a VIGOR, just connect your computer with one of the LAN ports of the VIGOR and the WAN port of the router with the internet.

The default IP address for the VIGOR is 192.168.1.1, when you enter this address in a browser, a login page appears, the default IP address and password are 'admin' (without the quotes).

After login you will see a page like this:



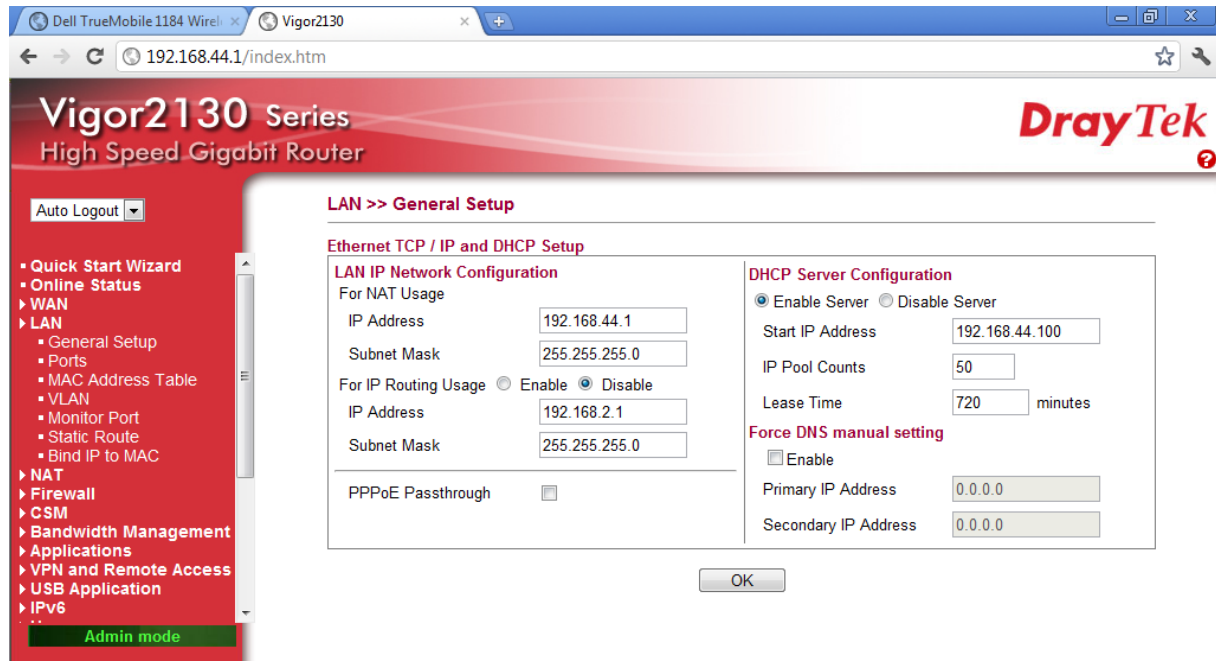
Remark: the Firmware version of the VIGOR for which this manual is written is v1.5.1\_RC2. Small differences may appear if the version of your VIGOR is different.

It is recommended that you start with the 'Quick Start Wizard' (top item in the bar at the left). This will set up the time zone, the new administrator password and some basic settings regarding the

internet connection (ask your Internet Service Provider for the correct info). In most cases the default values are OK.

### 6.1.5.2 LAN Settings

As stated before, the network range of your network is important for VPN. To change the network range, click 'LAN', 'General Setup'



In the 'LAN IP Network Configuration', change the third number of the IP address to your wish. You also need to change the 'Start IP Address' in the 'DHCP server Configuration' accordingly so that it is in the same network range.

Remark: the 'Start IP address' together with the 'IP Pool Counts', determine a range of IP addresses that can be assigned by the router to computers which are connected to the network (In the example, these are the addresses 192.168.44.100 – 192.168.44.150). So it is important that you do not assign one of these addresses statically to a device such as a TELETASK DoIP central unit, an IP camera, a network printer, a network hard disk,...

### 6.1.5.3 Dynamic DNS settings

To set up DynDNS on the VIGOR click 'Applications', 'Dynamic DNS'. You will see a page like this:

- Check the 'Enable Dynamic DNS' field
- Select the correct service provider (in this example dyndns.org)
- Enter the Domain name you have registered with the service provider (in this example mypersonaldomain.dyndns.org)
- Enter the Username and Password used for the DynDNS registration with the service provider.
- Select the correct setting for IP source: 'My WAN IP' in case your VIGOR is directly connected to the internet, 'My Internet IP' in case there is a cable modem/router from you internet provider between the VIGOR and the internet (see remark below).
- The rest of the settings are normally OK.



**Remark:** In case you have a cable modem/router between your VIGOR and the internet, you have to take additional steps to make thing work. In this case the WAN IP address of your VIGOR will be a 'private IP address' (in the rages 10.x.x.x, 172.16.x.x to 172.31.x.x or 192.168.x.x). If the VIGOR would update this IP address (e.g.: 192.168.1.x) to your dynamic IP-address host, but this would not work as this is a 'private IP address'. To solve this you need to set the VIGOR to use his 'internet IP address', and not his local 'My WAN IP address'.

To make it possible to connect to your VIGOR VPN router from the internet, you need to enable port-forwarding on you cable/DSL modem-router. Forward the port 1723 to the WAN IP-address of your VIGOR VPN router. It also advised to set the WAN IP address of your VIGOR VPN router static. (e.g. 192.1.0.2). For detail on how to set up port forwarding on your cable/DSL modem-router, contact you internet provider.



**IMPORTANT REMARK:** This is not the same as port-forwarding directly to the Central Unit! You are still using a secure VPN connection and you are only using the Port-forwarding to go from the internet directly to your VIGOR VPN router.

### 6.1.5.4 Adding Users

Before we can set up the VPN server, users must be added. Each user has its own username and password to connect to the VPN server (and can have different privileges).

To add a user, click 'User', 'User Configuration

You will see this screen:

**Vigor2130 Series**  
High Speed Gigabit Router

Off

- Quick Start Wizard
- Online Status
- WAN
- LAN
- NAT
- Firewall
- CSM
- Bandwidth Management
- Applications
- VPN and Remote Access
- USB Application
- IPv6
- User
  - User Configuration
- System Maintenance
- Diagnostics

**Support Area**  
Application Note  
FAQ  
Product Registration

Logout  
All Rights Reserved.

**User >> User Configuration**

Please install Samba Server before enable Disk Sharing

**Add User**

☒ **Enable**

**User Settings**

Username: John

Full Name: John Doe

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Allow Disk Sharing: ☐

Allow IPSEC/L2TP: ☐

Allow PPTP: ☒

Enable PPTP LAN to LAN: ☐

Local Network / Mask: 0.0.0.0 / 0.0.0.0

Remote Network / Mask: 0.0.0.0 / 0.0.0.0

Allow FTP: ☐

Allow TELNET: ☐

OK Cancel

- Check the 'Enable User Settings' field

Fill in:

- Username: a name for the user to log into the VPN (all users must have a unique name)
- Full Name: the full name of the user (only to simplify user management)
- Password: the password for the user
- Check the "Allow PPTP field"
- Click OK

Repeat these steps for all users.

### 6.1.5.5 Setup VPN server

Now we are ready to set up the VPN server itself, click on 'VPN and Remote Access', 'Remote Access Control'.



Adjust the following settings:

- Uncheck 'Enable IPsec VPN Service'
- Check 'Enable PPTP VPN Service'
- If you plan to use Apple devices (iPhone/iPod touch/iPad or Mac) Check '\*MPPE Required'



**Remark:** like the DHCP server, the VPN server also has a pool of IP addresses from which it gives an IP address to a device that makes a VPN connection. So make sure that no devices that are physically on the network have a static IP address in the 'IP Address range for PPTP client'

Click 'OK' to save the settings, your VIGOR is now ready to accept incoming VPN connections.

### 6.1.6 Setup a SG300 (not available anymore)



Once you have connected your laptop to the LAN side of the SnapGear router, open a browser and browse to the SG300, enter the root password (this is not standard configured).

Remark that the default LAN setup of the SG300 is static configured on 192.168.0.1

The easy way to set up your Router/Firewall is to use the 'Quick Setup Wizard'.

Following screens will appear on your configuration-PC:

- Quick Setup
- Manual LAN Configuration
- ISP connection

#### 6.1.6.1 Quick Setup

**LAN -> Internet -> Confirm -> Done**

This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the *skip* option.

Select the name this SnapGear unit should know itself by.

**Hostname**

The SnapGear unit is able to glean its local network (LAN) address configuration in one of two ways. It can dynamically obtain the necessary setup information from a DHCP server already installed on the local network or it can be manually configured with fixed parameters.

**Direct Connection Settings**

☐ Obtain LAN IP address from a DHCP server on LAN

☒ Manual configuration

☐ Skip: LAN already configured

In most cases 'Manual configuration' will be the correct one, because the SG300 will be the only device that will act as a DHCP server.

### 6.1.6.2 Manual LAN Configuration

**LAN -> Internet -> Confirm -> Done**

Configure the local network (LAN) interface.

Select the address that the SnapGear unit should use for its LAN network interface. This must be an address that lies within the range of the local network and that is not used by any other host.

**IP Address**

The subnet mask determines the logical size of the local area network.

**Subnet Mask**

Select the range of addresses that the DHCP server on this Secure Computing unit may assign to other machines on the LAN. *(May be left blank to disable the DHCP server)*

**DHCP Server Address Range**

In this case we assume that we will configure the private network in the range: 192.168.1.xxx and choose for the LAN IP-Address of the SG300 192.168.1.1

### 6.1.6.3 ISP Connection

**LAN -> Internet -> Confirm -> Done**

Select the method you use to connect to your Internet Service Provider (ISP). If you have already correctly configured this or if you want to defer this configuration until later, select the *skip* option.

**Internet Port Configuration**

- ☒ Cable Modem
- ☐ Modem
- ☐ ADSL
- ☐ Direct Connection
- ☐ Skip: Internet connection already configured

Select the correct connection to the internet, if you don't know, contact your Internet Service Provider (in most cases 'Direct Connection' is correct).

After finishing the wizard you will have to change the IP-Address in your browser to 192.168.1.1 to continue the configuration.

#### 6.1.6.4 VPN Configuration

In the previous step you have configured the basic network settings. Now you can start setting up the actual VPN server.

- Click on the left side under VPN on PPTP VPN Server
- Check the option "Enable PPTP Server"
- For the "Authentication Scheme" choose "Encrypted Authentication (MS-CHAP)", this means that devices using MS-CHAP or better (MS-CHAP v2) can connect. If only PC's running Windows Vista and/or Smartphones running Windows mobile V6 are used, you can select the option "Encrypted Authentication (MS-CHAP v2)" here.
- Leave the rest of the settings to their default values and click 'Submit'.

**PPTP VPN Server**

**PPTP Server Setup**

**Enable PPTP Server** ☒

**IP addresses to give to remote hosts**

**IP Address to Assign VPN Server**

**Authentication Scheme**

**Required Encryption Level**

**Authentication Database**

- Click on the left side under 'System on User' and choose the tab page 'Local Users'.
- Click 'New', fill in a name, description and Password
- Make sure the option "PPTP access" is check-marked
- Click finish

Administrative Users	Local Users	RADIUS	TACACS+																				
<table border="1"> <thead> <tr> <th></th> <th>Username</th> <th>Description</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>koen</td> <td>VPN PC</td> <td></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>qtek</td> <td>GSM user</td> <td></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>teletask</td> <td>Temporary</td> <td></td> <td></td> </tr> </tbody> </table>					Username	Description			<input checked="" type="checkbox"/>	koen	VPN PC			<input checked="" type="checkbox"/>	qtek	GSM user			<input checked="" type="checkbox"/>	teletask	Temporary		
	Username	Description																					
<input checked="" type="checkbox"/>	koen	VPN PC																					
<input checked="" type="checkbox"/>	qtek	GSM user																					
<input checked="" type="checkbox"/>	teletask	Temporary																					
<input type="button" value="New"/>																							

Administrative Users	Local Users	RADIUS	TACACS+
<div> <div>Edit User Information</div> <div> <div>Username</div> <div>teletask</div> </div> <div> <div>Description</div> <div>Temporary</div> </div> <div> <div>Domain</div> <div></div> </div> <div> <div>Password</div> <div>••••</div> </div> <div> <div>Confirm Password</div> <div>••••</div> </div> <div> <div>Dialin Access</div> <div><input type="checkbox"/></div> </div> <div> <div>Dialin Address</div> <div></div> </div> <div> <div>PPTP Access</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>PPTP Address</div> <div></div> </div> <div> <div>L2TP Access</div> <div><input type="checkbox"/></div> </div> <div> <div>L2TP Address</div> <div></div> </div> <div> <div>Internet Access (via. Access Controls)</div> <div><input type="checkbox"/></div> </div> <div> <div>Bypass Content Filtering</div> <div><input type="checkbox"/></div> </div> <div> <div>Change Password</div> <div><input type="checkbox"/></div> </div> <div> <div><input type="button" value="Finish"/></div> <div><input type="button" value="Cancel"/></div> </div> </div>			

#### 6.1.6.5 Setting up Dynamic DNS in SG300

- Click on the left side on Network Setup under NETWORK SETUP and choose first tab page DNS and then tab page 'Dynamic DNS'
- Select "dyndns.org" from the dropdown list and click "New"
- Check the "Enable" option
- Enter your DynDNS username password and Domain (in the example below we have created a DynDNS account with username 'dyndnsuser' and hostname 'homestreet.homeip.net')
- Click "Finish"

Connections Failover & H/A Routes System **DNS**

DNS Proxy Dynamic DNS Static Hosts

	Interface	Service	Domain	Status		
✓	Default Gateway Interface	dyndns.org	leliestraat.homeip.net	Active		

**New** TZ0

Connections Failover & H/A Routes System **DNS**

DNS Proxy Dynamic DNS Static Hosts

Service dyndns.org

Enable ☒

Interface Default Gateway Interface

Username dyndnsuser

Password

Confirm Password

Domain homestreet.homeip.net

Additional Domains

MX homestreet.homeip.net

Wildcard ☐

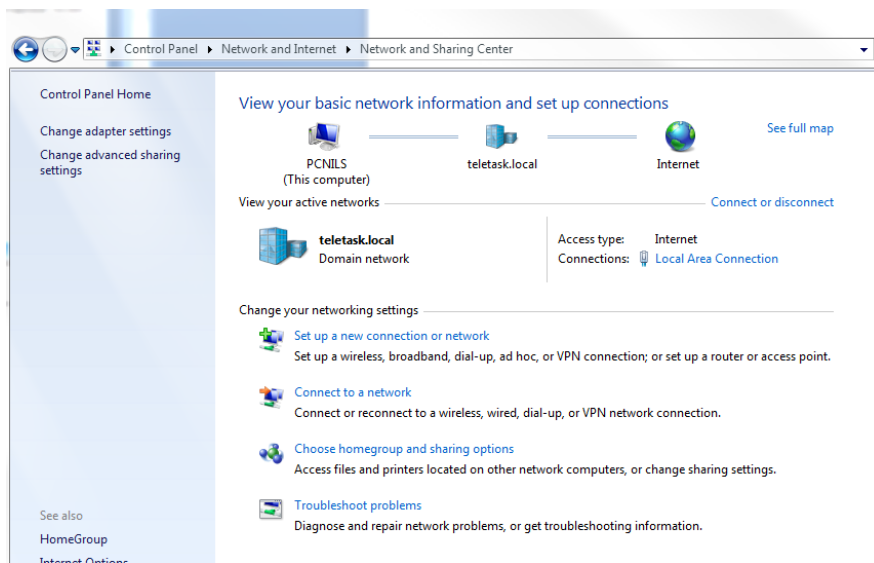
**Finish** **Cancel**

## 6.1.7 Setting-up a client-VPN connection

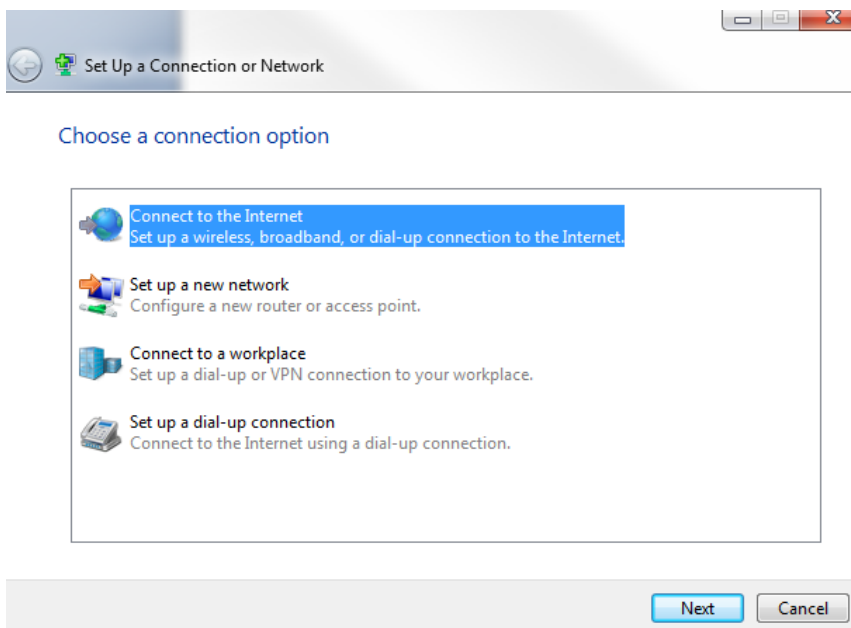
Now that the VPN-router is set-up, and the Dynamic DNS is activated, we can set up a VPN connection from a remote location. In this step we will set up a VPN connection using Windows 7 (for Windows Vista and XP the steps are the same). If you want to set up a VPN connection from a mobile device we suggest to first set up a PC connection (to test if the VPN server is working) and then set up the connection from your Mobile device. For help about setting up a VPN connection from a mobile device see the iSGUI installation manual.

### 6.1.7.1 Setting-up a client-VPN connection on Windows 7

- Go to Start > Control panel > Network and Internet > Network and Sharing center

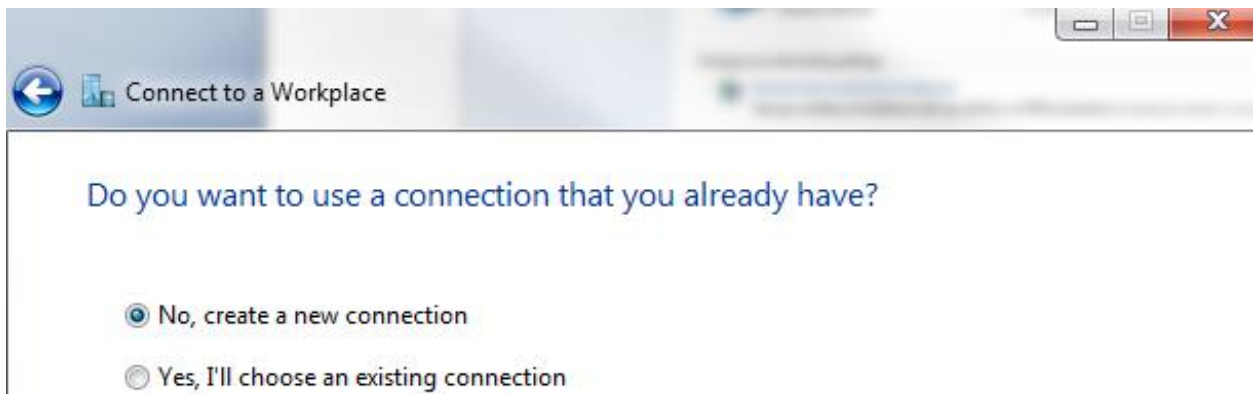


- Click on 'Set up a new connection or network.'

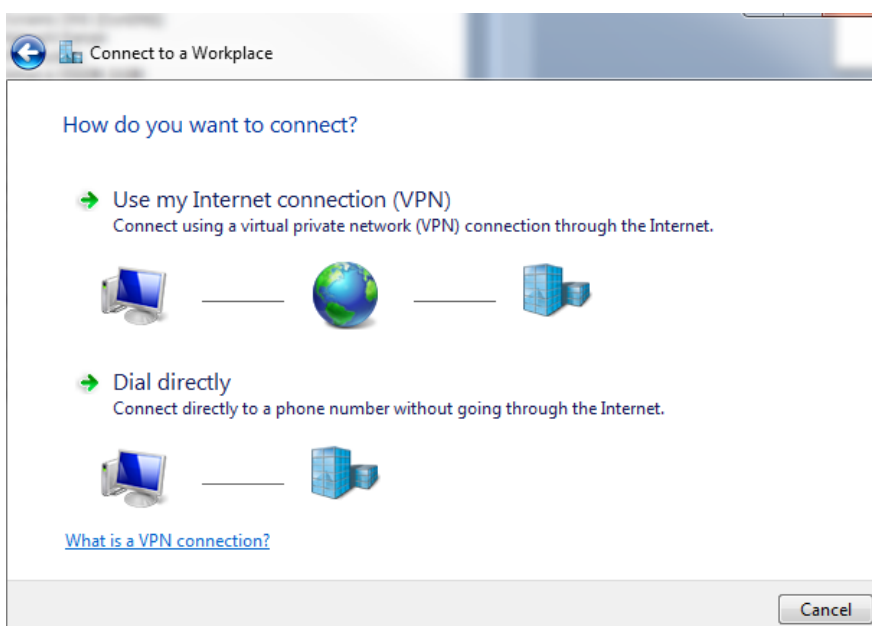


- Select "Connect to a workplace" and click "Next".

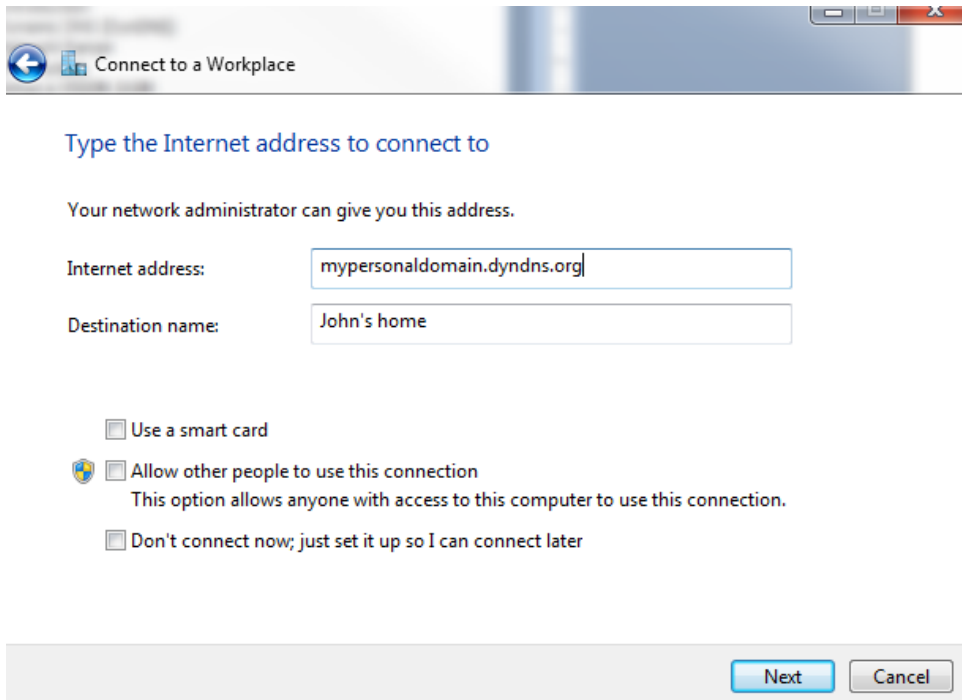




- Select 'No, create a new connection' and click next (depending on your system this step can be skipped).

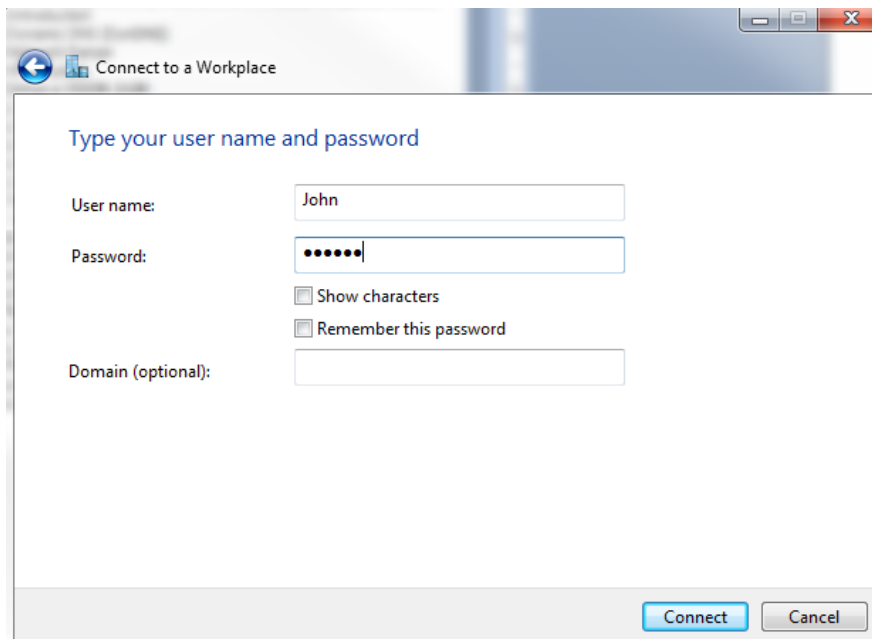


- Click 'Use my Internet connection (VPN)'



The screenshot shows a Windows-style dialog box titled "Connect to a Workplace". The main heading is "Type the Internet address to connect to". Below this, a message states: "Your network administrator can give you this address." There are two text input fields: "Internet address:" containing "mypersonaldomain.dyndns.org" and "Destination name:" containing "John's home". Below these fields are three checkboxes: "Use a smart card" (unchecked), "Allow other people to use this connection" (unchecked) with a sub-note "This option allows anyone with access to this computer to use this connection.", and "Don't connect now; just set it up so I can connect later" (unchecked). At the bottom right are "Next" and "Cancel" buttons.

- Enter the IP address or the DynDNS name in the 'Internet address' field
- Give it a name by which you know that this is a connection to your (clients) home and click "Next"

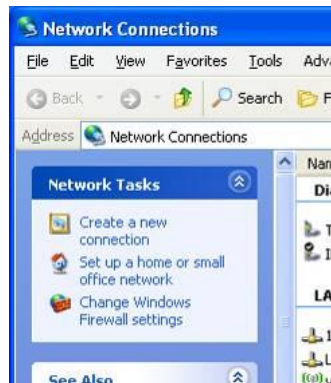


The screenshot shows the same "Connect to a Workplace" dialog box, but at the "Type your user name and password" step. The "User name:" field contains "John". The "Password:" field contains masked characters "•••••". Below the password field are two checkboxes: "Show characters" (unchecked) and "Remember this password" (checked). The "Domain (optional):" field is empty. At the bottom right are "Connect" and "Cancel" buttons.

- Enter the user name and Password as configured in the VPN router
- Click 'Connect' (The first time you connect will take some time)

### 6.1.7.2 Setting-up a client-VPN connection on Windows XP

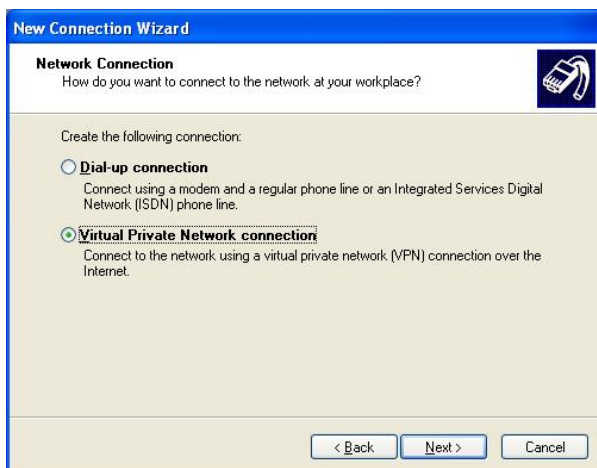
- Go to Start > Configuration panel > Network connections.



- Click on 'Create a new connection'.



- Choose to make a connection to the network at my workplace and click "Next".

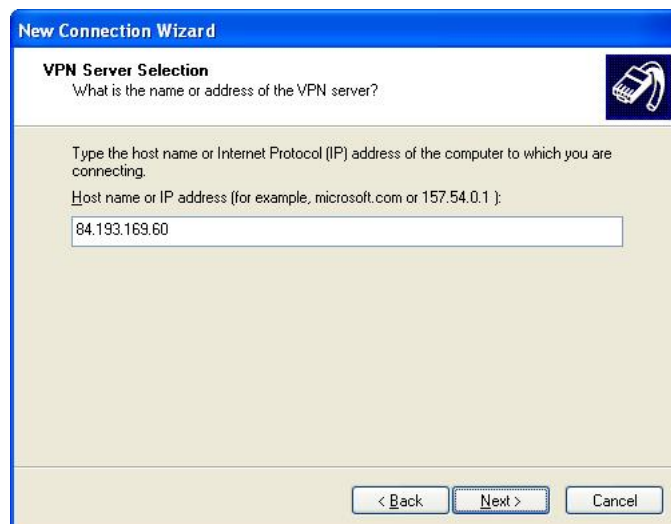


- Choose VPN connection and click "Next"



The screenshot shows the 'New Connection Wizard' dialog box with the 'Connection Name' step selected. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section 'Connection Name' is highlighted. The text 'Specify a name for this connection to your workplace.' is displayed. Below this, a text box contains 'Home-Network'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Give it a name by which you know that this is a connection to your (clients) home and click "Next"



The screenshot shows the 'New Connection Wizard' dialog box with the 'VPN Server Selection' step selected. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section 'VPN Server Selection' is highlighted. The text 'What is the name or address of the VPN server?' is displayed. Below this, a text box contains '84.193.169.60'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- As Host name or IP address, you give the hostname that you configured on DynDNS (in the example we used in "Setting up DynDNS in SG300" this would be 'homestreet.homeip.net'). If you have a static IP address enter your IP address here.
- Click "Next", and then "Finish" in the next screen. Now the laptop is ready to connect to your "home network"

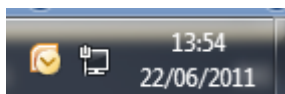


## 6.1.8 Test the VPN connection

In this chapter we will first test the connection and then explain how to use a TELETASK GUI over the VPN connection.

### 6.1.8.1 Test the VPN connection on Windows 7

The VPN connection is already tested while setting up. To disconnect or connect again, click the network icon in the notification area.



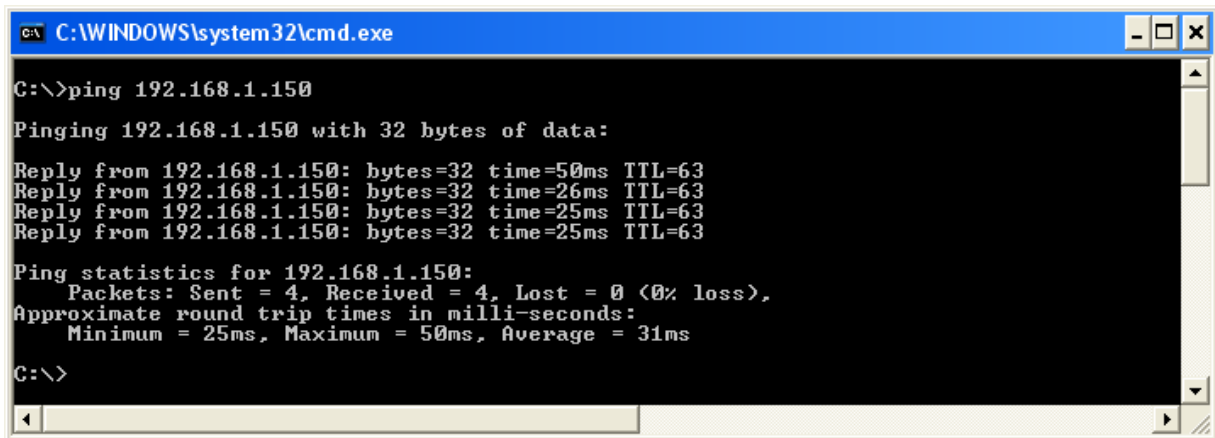
### 6.1.8.2 Test the VPN connection on Windows XP

- Open your VPN connection with "Start", "Connect to".
- Enter the User name and password that you have created in the router (in the chapter "VPN configuration")
- ...and click 'connect'



Ping

- To test the connection, we suggest you to do a ping to the IP address of the equipment at your home (e.g. the TELETASK 'MICROS+' or 'NANOS' DoIP central unit). If you have set up everything correctly this should work



```
C:\WINDOWS\system32\cmd.exe

C:\>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:

Reply from 192.168.1.150: bytes=32 time=50ms TTL=63
Reply from 192.168.1.150: bytes=32 time=26ms TTL=63
Reply from 192.168.1.150: bytes=32 time=25ms TTL=63
Reply from 192.168.1.150: bytes=32 time=25ms TTL=63

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 50ms, Average = 31ms

C:\>
```

### 6.1.9 Using a TELETASK GUI over the VPN connection

As said in the introduction, one of the benefits of a VPN connection is that the configuration for local and remote usage is exactly the same. So in the properties of the GUI+ (or iSGUI) you need to enter the same IP address and port number as if you would use the GUI locally.

So you can run your GUI+ on your laptop at home, take your laptop with you to work, holiday, etc... and run the GUI+ from the same laptop on the remote site without changing any settings.

All you need to think about is click the "Connect to" button and connect to your home network before starting the GUI+ on a remote location.



## 6.2 How to control a CEILING SWEEP FAN



This article is written for CEILING SWEEP FAN's with single coil (2 wires + earth connection only).

There are several ways to control an AC ceiling sweep fan with the TELETASK system:

1. **On/off control (full speed or off).**

This can be obtained by using a single power output contact, MICROS+ Central unit a relay (250V/10Amp) or a TDS13500 (250V/16Amp) or TDS13501 (10Amp/250V) relay output.

2. **Multi-speed control with the Ceiling Sweep Fan Interface (TDS13522).**

For more information, see the TDS13522 Datasheet or the Technical handbook.

3. **Multi-speed control with a power dimmer (not recommended).**

Continuous speed control is possible but will induce a humming noise of the ceiling fan. (not for use in low noise rooms). REMARK: make sure it is not possible to dim the ceiling sweep fan below 40%! Make use of a step function instead to define different speed levels.