TELETASK

Home Automation

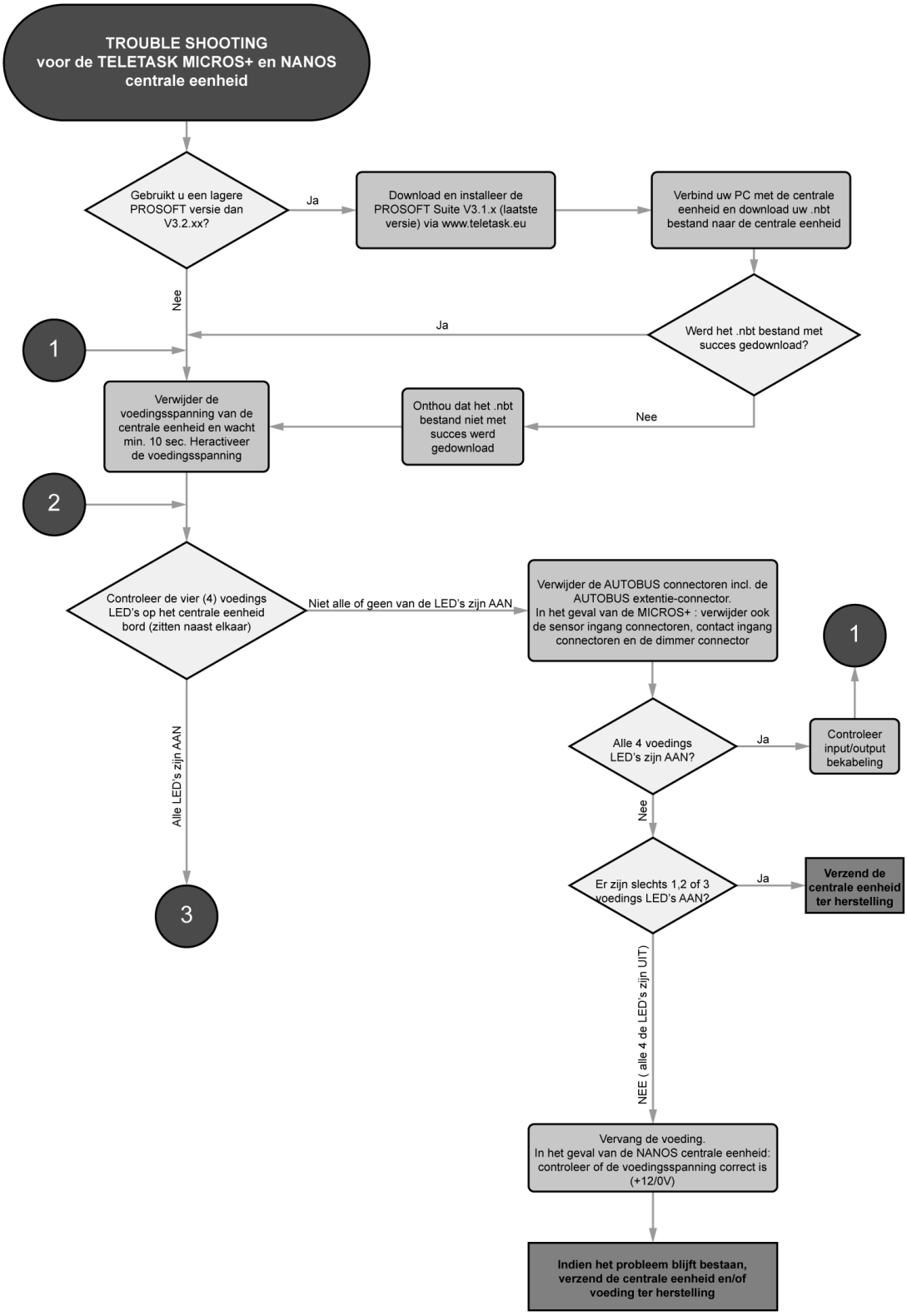
Support & Troubleshooting

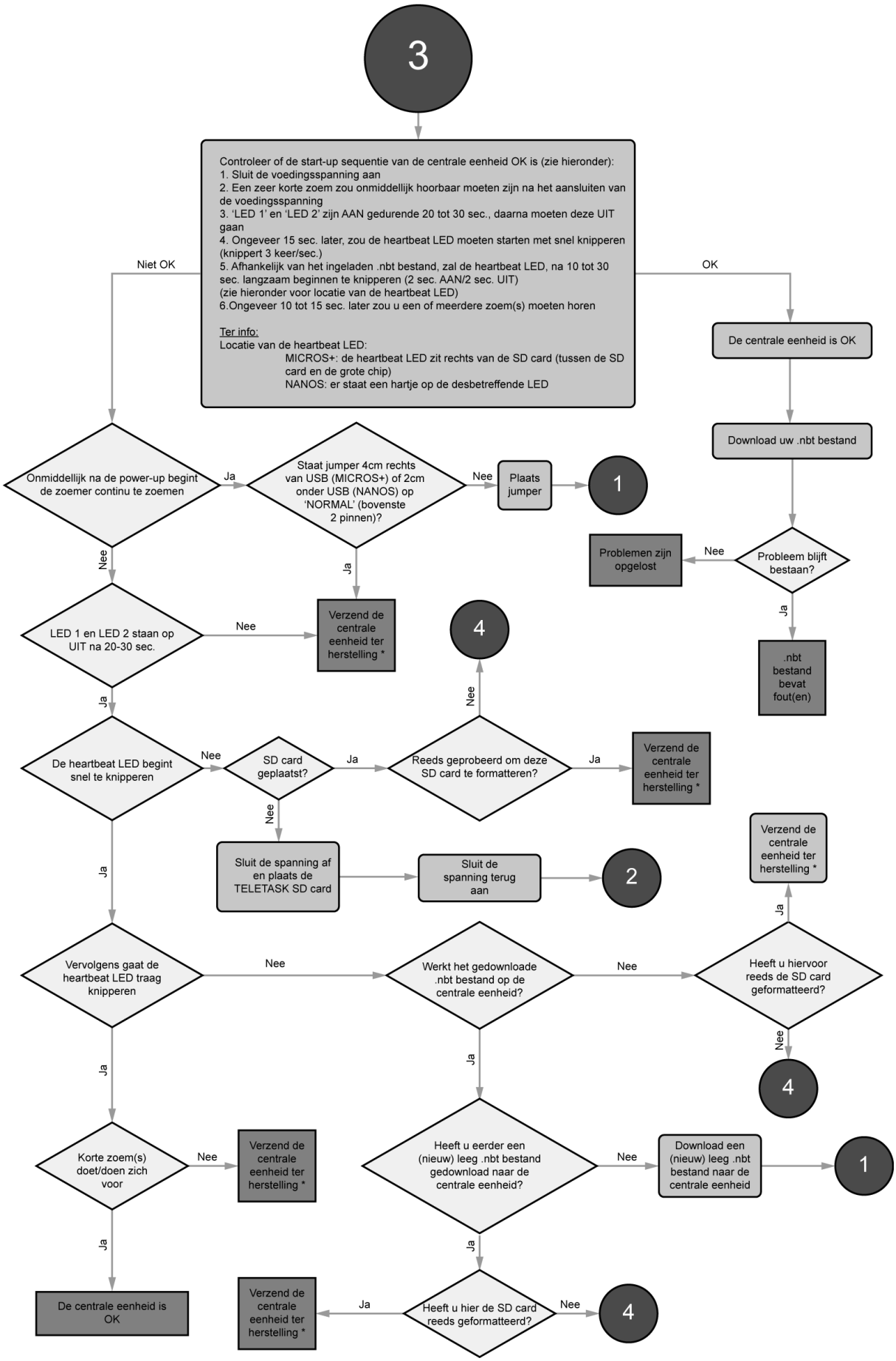
+ Tips & tricks

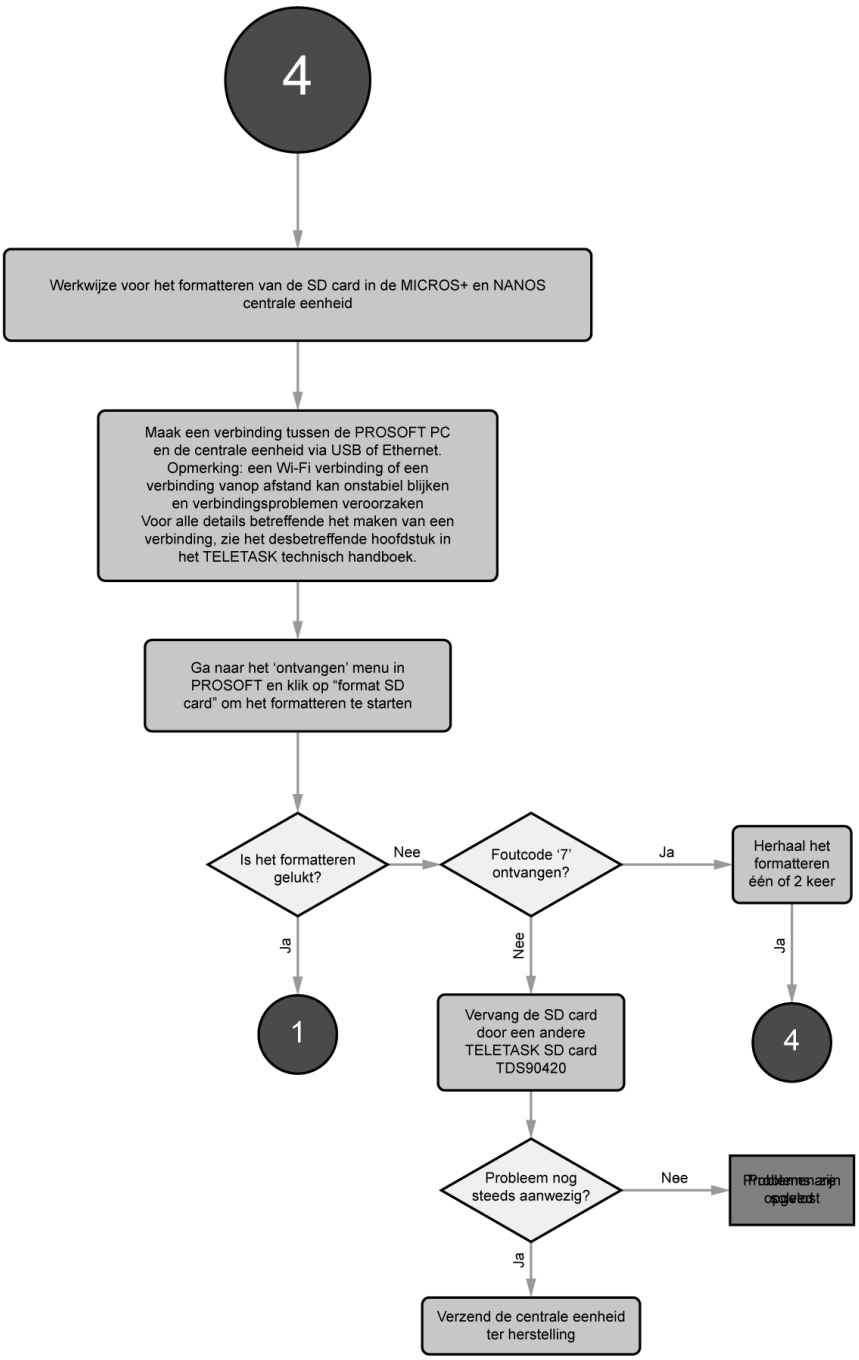
Versie: 25 April 2013

Inhoudstabel

1 Problemen oplossen met de MICROS+ en NANOS




3
Controleer of de start-up sequentie van de centrale eenheid OK is (zie hieronder):
1. Sluit de voedingsspanning aan
2. Een zeer korte zoem zou onmiddellijk hoorbaar moeten zijn na het aansluiten van de voedingsspanning
3. 'LED 1' en 'LED 2' zijn AAN gedurende 20 tot 30 sec., daarna moeten deze UIT gaan
4. Ongeveer 15 sec. later, zou de heartbeat LED moeten starten met snel knipperen (knippert 3 keer/sec.)
5. Afhankelijk van het ingeladen .nbt bestand, zal de heartbeat LED, na 10 tot 30 sec. langzaam beginnen te knipperen (2 sec. AAN/2 sec. UIT)
(zie hieronder voor locatie van de heartbeat LED)
6.Ongeveer 10 tot 15 sec. later zou u een of meerdere zoem(s) moeten horen
Ter info:
Locatie van de heartbeat LED:
MICROS+: de heartbeat LED zit rechts van de SD card (tussen de SD card en de grote chip)
NANOS: er staat een hartje op de desbetreffende LED
Niet OK
OK
De centrale eenheid is OK
Download uw .nbt bestand
Onmiddellijk na de power-up begint de zoemer continu te zoemen
Ja
Staat jumper 4cm rechts van USB (MICROS+) of 2cm onder USB (NANOS) op 'NORMAL' (bovenste 2 pinnen)?
Nee
Plaats jumper
1
Nee
Ja
Problemen zijn opgelost
Nee
Probleem blijft bestaan?
Ja
.nbt bestand bevat fout(en)
LED 1 en LED 2 staan op UIT na 20-30 sec.
Nee
Verzend de centrale eenheid ter herstelling *
4
Ja
Nee
De heartbeat LED begint snel te knipperen
Nee
SD card geplaatst?
Ja
Reeds geprobeerd om deze SD card te formatteren?
Ja
Verzend de centrale eenheid ter herstelling *
Nee
Sluit de spanning af en plaats de TELETASK SD card
Sluit de spanning terug aan
2
Verzend de centrale eenheid ter herstelling *
Ja
Ja
Vervolgens gaat de heartbeat LED traag knipperen
Nee
Werkt het gedownloade .nbt bestand op de centrale eenheid?
Nee
Heeft u hiervoor reeds de SD card geformatteerd?
Nee
4
Ja
Ja
Korte zoem(s) doet/doen zich voor
Nee
Verzend de centrale eenheid ter herstelling *
Heeft u eerder een (nieuw) leeg .nbt bestand gedownload naar de centrale eenheid?
Nee
Download een (nieuw) leeg .nbt bestand naar de centrale eenheid
1
Ja
Ja
De centrale eenheid is OK
Verzend de centrale eenheid ter herstelling *
Ja
Heeft u hier de SD card reeds geformatteerd?
Nee
4


4
Werkwijze voor het formatteren van de SD card in de MICROS+ en NANOS centrale eenheid
Maak een verbinding tussen de PROSOFT PC en de centrale eenheid via USB of Ethernet. Opmerking: een Wi-Fi verbinding of een verbinding vanop afstand kan onstabiel blijken en verbindingsproblemen veroorzaken Voor alle details betreffende het maken van een verbinding, zie het desbetreffende hoofdstuk in het TELETASK technisch handboek.
Ga naar het 'ontvangen' menu in PROSOFT en klik op "format SD card" om het formatteren te starten
Is het formatteren gelukt?
Nee
Foutcode '7' ontvangen?
Ja
Herhaal het formatteren één of 2 keer
Ja
Nee
Ja
1
Vervang de SD card door een andere TELETASK SD card TDS90420
4
Probleem nog steeds aanwezig?
Nee
Ja
Verzend de centrale eenheid ter herstelling

TROUBLE SHOOTING (*/**/***)
voor een MICROS+ en NANOS centrale eenheid.

*****

Vastgesteld probleem:
in uitzonderlijke gevallen, begint de zoemer onmiddellijk met zoemen na de power-up

Mogelijke oorzaak van het probleem:
de weerstand R33 dient 18k ohm te zijn in plaats van 10k ohm

Oplossing:
verzend de centrale eenheid ter herstelling (de R33 10k ohm moet vervangen worden door de 18 k ohm resistor)

Betrokken centrale eenheden:
MICROS+ : serienummer xxxxx0101 to xxxxx0611
NANOS: serienummer xxxxx0101 to xxxxx015

******

Vastgesteld probleem:
in uitzonderlijke gevallen start de heartbeat LED na de power-up niet met knipperen

Mogelijke oorzaak van het probleem:
probleem met de SD card connector
de weerstand R20 dient te worden vervangen (56K dient te worden vervangen door 6K8)

Oplossing:
verzend de centrale eenheid ter herstelling
(de SD card en/of de R20 moeten vervangen worden)

2 Richtlijnen voor het verdeelbord (NL)

Het bekabelen van een VerdeelBord (VB) uitgerust met TELETASK interfaces is niet verschillend van eender welk VB. Aangezien er zowel laagspanning (110-400V) als extra laagspanning (vooral 12-24V) toestellen in een typische domotica VB zit, dienen deze beiden zoveel mogelijk gescheiden van elkaar gehouden te worden. CE regulering en algemene kwaliteit verplicht de paneel/VB-installateur een simpele maar zeer belangrijke regel te volgen: breng alle laag spanningsdraden/kabels aan de ene kant van het VB en alle extra-lage spanningsdraden/kabels aan de andere kant van het VB.

Bijvoorbeeld de laagspanning rechts (van beneden tot boven). De extra-lage spanningsdraden aan de andere kant, in dit geval de linkse zijde van het VB.

Voordat u het VB kiest, dient u te weten of u een NANOS dan wel een MICROS+ centrale zal gebruiken. Bij het gebruiken van een NANOS zijn er geen specifieke opmerkingen omdat dit een standaard DIN-rail eenheid betreft. Indien u een MICROS+ centrale eenheid zal gebruiken, dient u te beslissen of u deze centrale eenheid intern of extern het VB zal installeren.

1. Voor kleine installaties met MICROS+ en tot 10 DIN-rail TELETASK interfaces (zoals TDS12116, TDS13500, TDS13524...), raden wij aan om een standaard (kunststof of metalen) VB te gebruiken en de MICROS+ ernaast te plaatsen (links of rechts).

Figuur 1: MICROS+ naast het DB

2. Voor gemiddelde en grote installaties waar u meerdere interfaces (en zekeringen en andere componenten) dient te installeren in het VB, raden wij u aan om één of meerdere grote industriële VB kasten te gebruiken. Meestal zijn deze in metalen uitvoering.

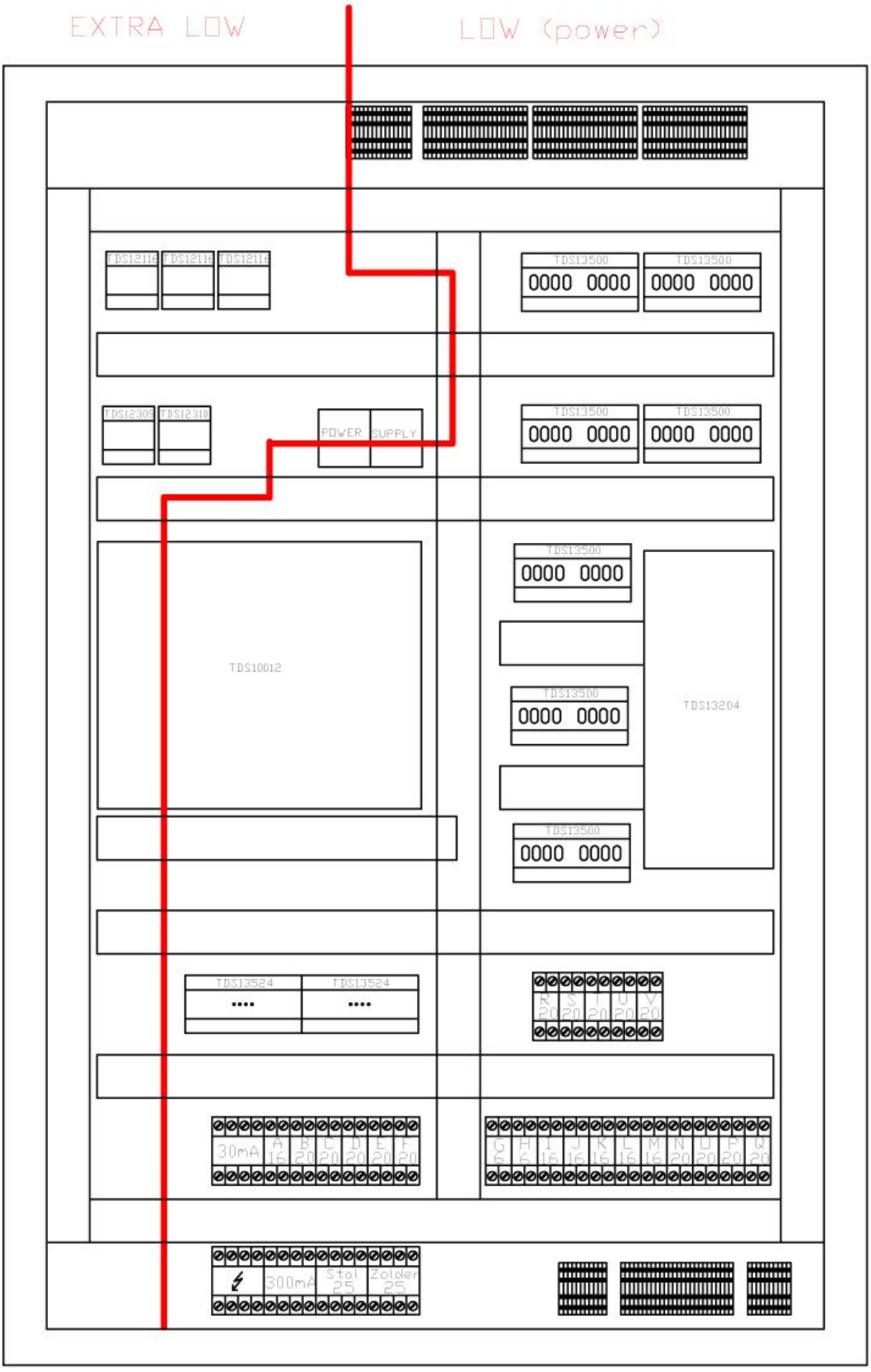
De MICROS+ wordt dan geplaatst in het VB. Houdt er rekening mee dat de MICROS+ in- en uitgangen aan de onderzijde van zijn behuizing zitten. De extralaag spanningsdraden (contactingangen, sensoringangen, AUTOBUS verbindingen…) zitten aan de linkse zijde (een grote opening) en de laagspanningsdraden (uitgang relaiscontacten voor 12-250 Volt) dienen door de ronde uitbreekbare openingen op dezelfde bodemplaat maar middenrechts geplaatst te worden. Dit past bij een VB dat op dezelfde manier bekabeld werd (extralaagspanning links).

Opmerking voor de installatie van de MICROS+: voor het vlot bedraden, opstarten en bedienen dient u de behuizing op ooghoogte te plaatsen. Dit betekent dat de onderkant van de MICROS+ tussen de 100 en 170 cm van de grond dient verwijderd te zijn.

Algemeen kunnen de zekeringen onderaan het VB geplaatst worden aangezien de niet gecontroleerde circuits (vb. Circuits voor frigo’s, diepvriezers waarbij de AAN/UIT functie niet bestuurd wordt door het TELETASK systeem) niet dienen verbonden te worden via schroefklemmen (zie ook hieronder het gebruik van DIN-rail schroefklemmen).

U bekomt de kortst mogelijke manier van bekabeling door uw energiekabels die van onderaan komen rechtstreeks te verbinden met de zekering, in dit geval zou deze in het onderste gedeelte van het VB geïnstalleerd moeten zijn.

Figuur 2: Duidelijk overzicht tussen ingang- en uitgangkabels



Figuur 3: Verdeling tussen extra-lage- en lage spanningsinterfaces.

Kabelgoten:

Wij raden het gebruik van een brede kabelgoot links en rechts van het VB aan voor het op en neer brengen van de kabels en draden in het VB. Het kan noodzakelijk zijn om een grotere kabelgoot te voorzien voor de 110-250V bekabeling dan voor de extra-lage spanningsbekabeling (signaal). Sommige installateurs zullen het panel in twee delen of zones verdelen.

Enkel extra-laagspanning en signaal interfaces in het linkse gedeelte van het VB en laagspanning in het rechtse gedeelte. In dergelijk geval kan u een kabelgoot links voorzien voor de extra-lage spanning, een kabelgoot in het midden en een kabelgoot aan de rechtse zijde van het VB voor laagspanning bedrading.

Opmerking: extra-lage spanningsbedrading is niet enkel nodig voor TELETASK maar kan ook gebruikt worden voor andere geplaatste systemen in het VB zoals videodeurtelefoon systeem, beveiliging, IT uitrusting, enz.…

Een andere manier voor het werken in grote VB is het werken met zons: een zone voor domotica, een zone voor videodeurtelefoon en een zone voor zekering. Dit is eveneens een goede manier van werken.

Hoe het ook zij, het is absoluut nodig dat de extra-lage spannings- en laagspanningsdraden en -kabels geïsoleerd van elkaar geplaatst worden. Een algemene regel is om de kabels/draden minstens 5 cm van elkaar te plaatsen. Dus indien u twee kabelgoten parallel heeft geplaatst, dienen deze op minimum 5 cm van elkaar geplaatst te zijn.

Aarding:

Het is zeer belangrijk om een goede aardingsverbinding met de centrale eenheid te hebben. Het volledige netwerk van de centrale eenheid en de AUTOBUS shieldings (naar alle interfaces, touch panels,…) is gebaseerd op een goede centrale aardingsverbinding in de MICROS+ centrale eenheid.

Verbind altijd de hoofd VB-aarding direct met de aardingsverbinding van uw elektrische installatie. Gebruik hiervoor de interne schroef in de MICROS+ behuizing in de rechter onderhoek. In het geval van een NANOS centrale eenheid, net zoals bij de MICROS+, is het de aardingsverbinding van de NANOS die het centrale aardingspunt vormt.

Figuur 4: MICROS (oude versie) Centrale eenheid

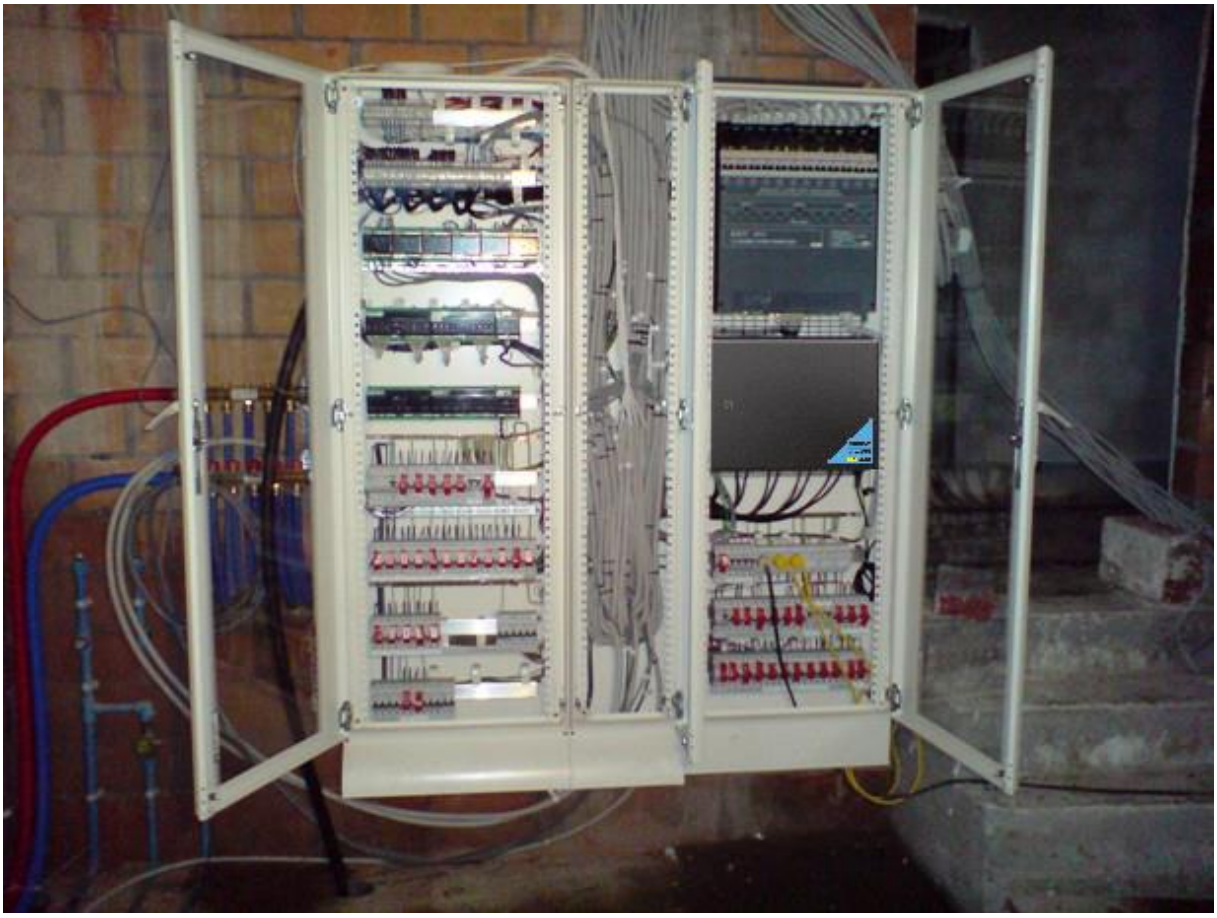
DIN-rail schroefklemmen:

Voor middelgrote en grote VB is het aanbevolen om de onderste en bovenste DIN-rails te gebruiken voor het installeren van de schroefklemmen. Via deze klemmen kunnen alle verbindingen tussen het VB en het gebouw gemaakt worden. Op deze manier kan de paneelbouwer (VB-bouwer) het VB volledig voor-bedraden alvorens het op de locatie te brengen. Het vermijdt ook stofvorming in het VB tijdens de opbouw van het huis/gebouw.

De meeste elektriciens gebruiken extra draden in hun kabels tussen de standaard contacten/drukknoppen en de contactingangen in het VB. Deze ingangen zitten in de MICROS+ centrale eenheid (32) of in een digitale ingangsinterface zoals de TDS12116 (16 kanalen ingang voltage vrije contact interface). Om het teveel aan kabels/draden in de MICROS+ eenheid te vermijden, dient u enkel de gebruikte draden met de schroefklemmen te verbinden met de DIN-rail en verbindt u de extra draden niet.

Vervolgens gebruikt u 3 multi-draad kabels (6 paar) om van de DIN-rail schroefklemmen naar de MICROS+ contactingangen te gaan. Het zal het bedraden veel gemakkelijker en sneller maken en de hoogste kwaliteit/betrouwbaarheid opleveren. Een standaard DIN-rail is 24 eenheden breed. De TDS13500/TDS113501/TDS13524 interfaces zijn 10 eenheden breed. Dit betekent dat u bijvoorbeeld 2 x TDS13500 naast elkaar kan plaatsen en dan nog 4 eenheden beschikbaar heeft voor 2x2 zekeringen die elk de nodige stroom voor elke TDS13500 interface kunnen voorzien (indien 16/20Amp voldoende is om alle verbonden circuits op de TDS13500 te voeden).

Voorbeeld Verdeelbord:



Figuur 5: Voorbeeld verdeelbord

- Het verdeelbord is verdeeld in duidelijk verdeelde zones.

- Er is een goed overzicht en een overzichtelijke bekabeling.

- De schroefklemmen en circuitbrekers zitten boven- en onderaan het verdeelbord.

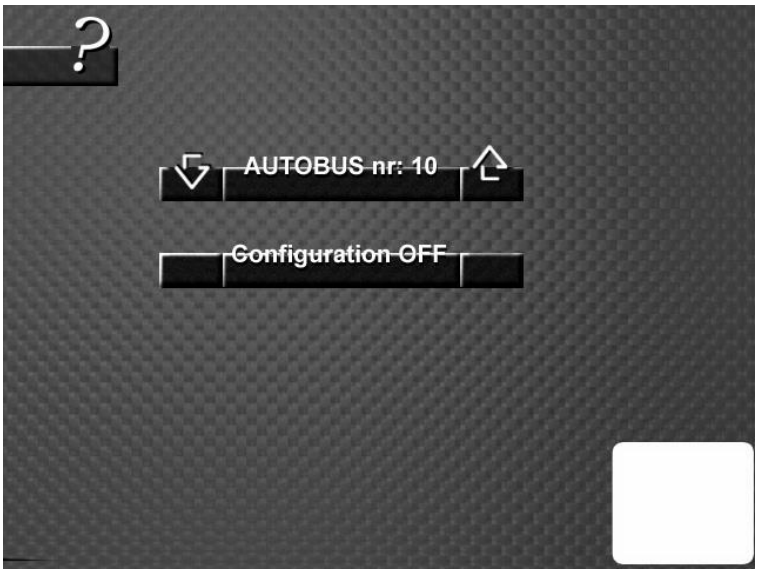
Tip: Indien de MICROS+ aan de linkse zijde van het VB wordt geplaatst, vermijdt u kruisende extra-lage spanningskabels en lage spanningskabels. Op deze manier kunnen de ingang-/sensor-/AUTOBUS-kabels via de linkse kabelgoot lopen en alle voedingsdraden kunnen dan via de middelste en rechtse kabelgoot lopen!

3 SERVUS TDS12110 Kalibratie aanraakscherm

3.1 Hoe de kalibratie van het aanraakscherm starten?

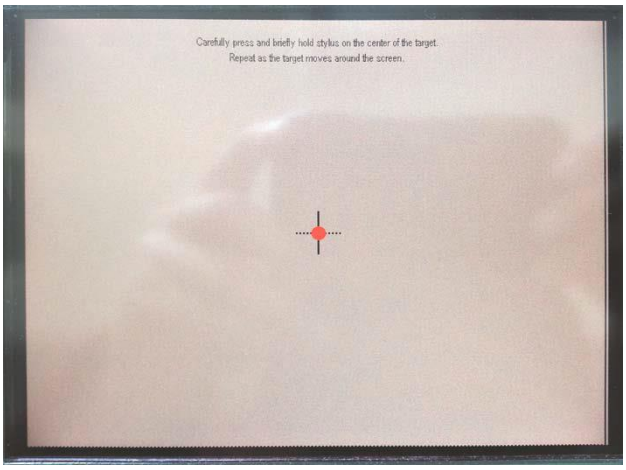
Kies het “Settings Menu” vanuit het startscherm.

Druk op de verborgen “Kalibratieknop” in de hoek rechtsonder van het aanraakscherm.

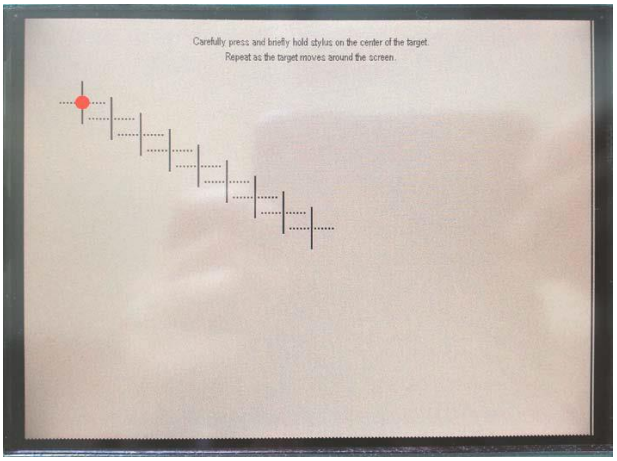


Volg de instructies op het scherm en raak de 5 noodzakelijke kalibratiepunten aan (het midden van het laatste kruis) door middel van een stylus (niet met je hand).

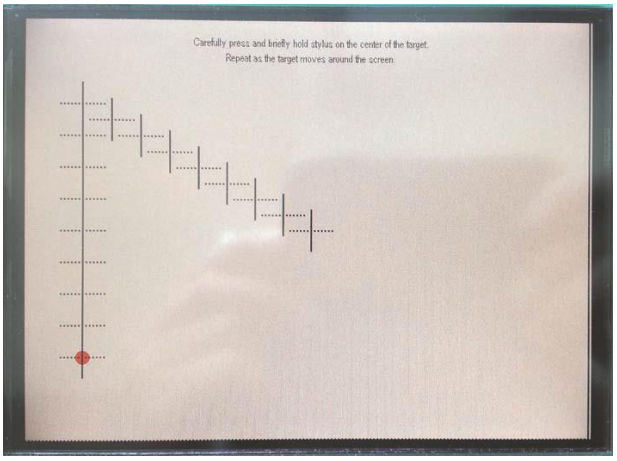
1.



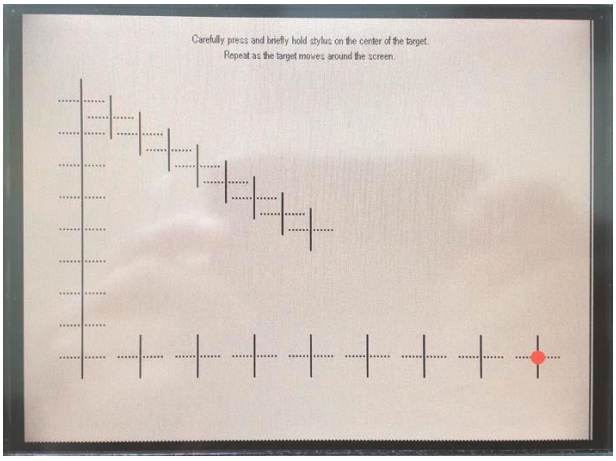
2.



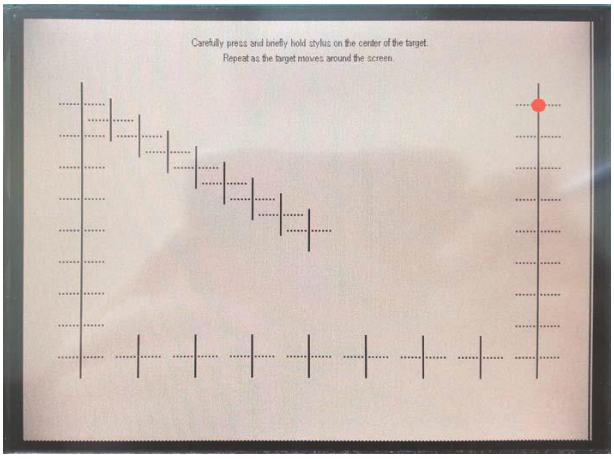
3.



4.



5.



3.2 Kalibratie opslaan

Nadat je het laatste 5de punt hebt geselecteerd met een stylus, zal de SERVUS vragen om het midden van het scherm aan te raken om zo de kalibratie te bevestigen en op te slaan. Als je binnen de 30 seconden niet op het midden van het scherm drukt, zal de kalibratie beëindigd en de aanpassingen ongedaan gemaakt worden.

4 AURUS-TFT hardware matig resetten

4.1 Inleiding

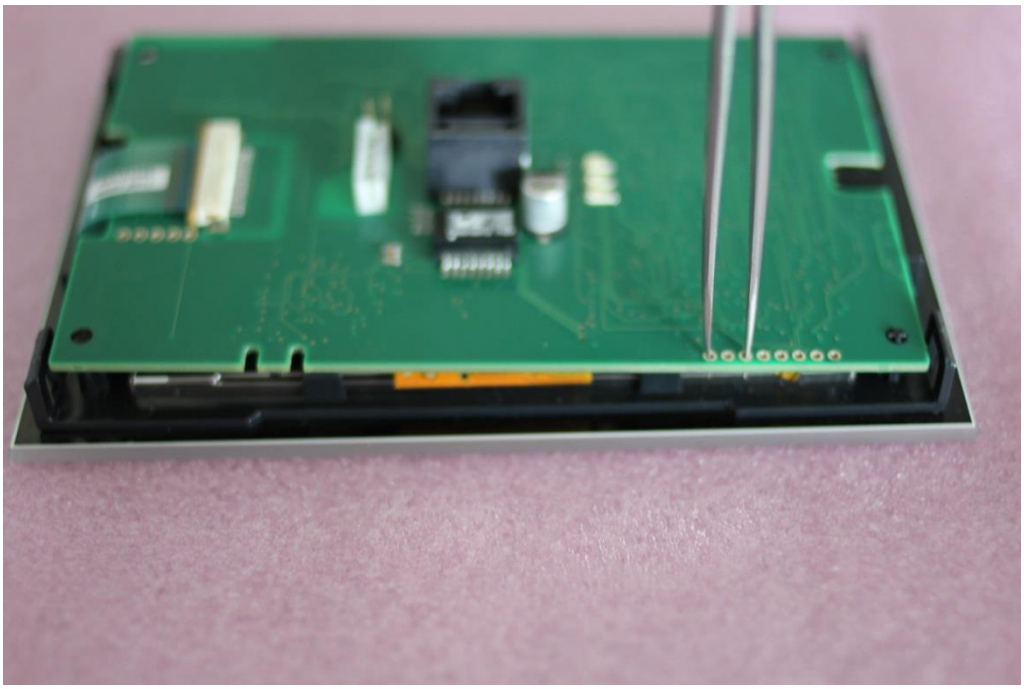
Bij uitzonderlijke gevallen kan het zich voordoen dat de AURUS-TFT blijft hangen bij het opstart scherm. Indien dit zich blijft voordoen na het loskoppelen en het terug steken van de AUTOBUS kabel, kan volgende procedure de AURUS-TFT terug brengen naar de fabrieksinstellingen.

Dit is enkel van toepassing bij AURUS-TFT met serienummer groter dan *****0256.

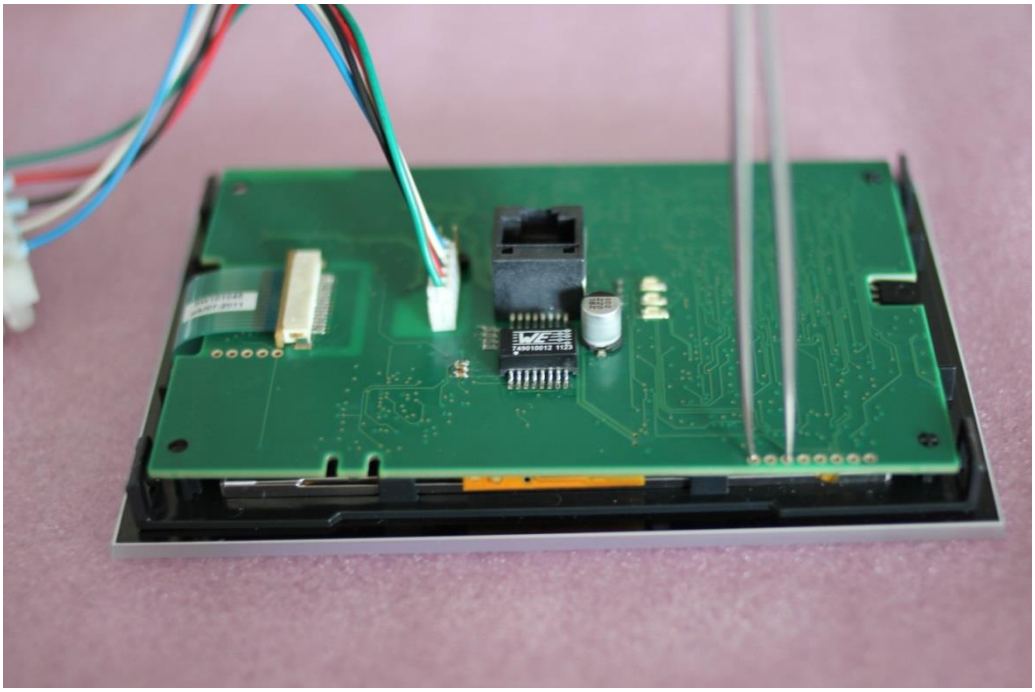
4.2 Hoe een AURUS-TFT resetten naar fabrieksinstellingen?

1. Controleer eerst en vooral of de laatste vier cijfers van het serienummer groter is dan 0256.
2. Plaats de AURUS-TFT omgekeerd met het glas naar beneden op een zacht oppervlak.
3. Verwijder de behuizing van de AURUS-TFT door voorzichtig met een platte schroevendraaier de binnenste lipjes in de hoeken naar binnen te duwen terwijl je de behuizing naar boven trekt. Herhaal dit voor de 4 hoeken.

4. Als de behuizing is verwijderd, verbindt dan door middel van een pincet of een draadje de eerste en de derde opening zoals weergegeven op onderstaande figuur:



5. Sluit de AUTOBUS terug aan met de openingen nog steeds met elkaar verbonden.



6. De AURUS-TFT start nu op in de ‘bootloader’. Verwijder de pincet of het draadje en laat de AURUS-TFT upgraden via AUTOBUS.

7. De AURUS-TFT is nu terug ingesteld naar de fabrieksinstellingen en heeft van de Centrale eenheid de laatste updates gekregen. Indien de problemen blijven aanhouden, neem dan contact op met uw TELETASK distributeur.

5 GEVALSTUDIES

5.1 DoIP - VPN Integratie

5.1.1 Inleiding

Dit document beschrijft hoe u een thuisnetwerk kan instellen voor het gebruik van op afstand van een TELETASK ‘GUI’, ‘GUI+’ of ‘iSGUI’.

Om een veilige verbinding te realiseren adviseren wij een VPN (Virtual Private Network) verbinding. De voordelen hiervan zijn:

- Universeel (standaard opzet dat kan gedaan worden met producten van verschillende router fabrikanten).
- Veilig (encrypted).
- De GUI configuratie is dezelfde voor lokaal gebruik als voor gebruik van op afstand.

Het principe van VPN is eenvoudig. Het verbindt (virtueel) vanop afstand uw laptop of Smartphone met uw thuisnetwerk (LAN). Hiervoor hebt u het volgende nodig: of een "Static IP address" of een "Dynamic DNS" address. Een static(statisch)- IP adres is de eenvoudigste en aangewezen oplossing, een “Dynamic DNS” (dynamisch) adres is een (mogelijks goedkoper) alternatief. Dit kan wisselen van land tot land.

Het instellen van een VPN verbinding verloopt volgens volgende stappen:

- Installeer thuis een router met ingebouwde VPN server
- Zet daarop een VPN verbinding op, via uw PC
- Test de VPN verbinding

Voor het opzetten van een VPN router oplossing is de nodige ICT en netwerk kennis vereist. Indien u geen ervaren specialist bent, raden we u aan om de onderstaande taken te laten uitvoeren door uw ICT leverancier.

5.1.2 Dynamic DNS (DynDNS)

5.1.2.1 Inleiding

Dynamic DNS is een dienst waarmee uw VPN router zijn (dynamisch; wijzigend) IP adres zendt naar een vaste server (met vast IP-adres) op het internet opdat u toegang zou kunnen hebben tot uw VPN router, van gelijk waar op het internet.

Er zijn verschillende providers voor deze dienstverlening. Eén van de meest gekende is www.DynDNS.org. In dit hoofdstuk zullen we een DynDNS account aanmaken en de VIGOR 2130 router configureren om te werken via deze account.

5.1.2.2 Creëer een DynDNS account

Een DynDNS account creëren is noodzakelijk om gebruik te maken van de DynDNS service.

- Open een browser en surf naar www.DynDNS.org.
- Maak een account aan en vul de gevraagde informatie in.
- Eenmaal uw account werd geactiveerd, kan u inloggen.
- Geef een "Hostname" in, selecteer het type service "Host with IP address", klik op de "Use auto detected IP address" link, en klik op "Create Host" (het is aanbevolen om deze stappen uit te voeren op de locatie waar de centrale eenheid werd geplaatst).

5.1.3 Network Range

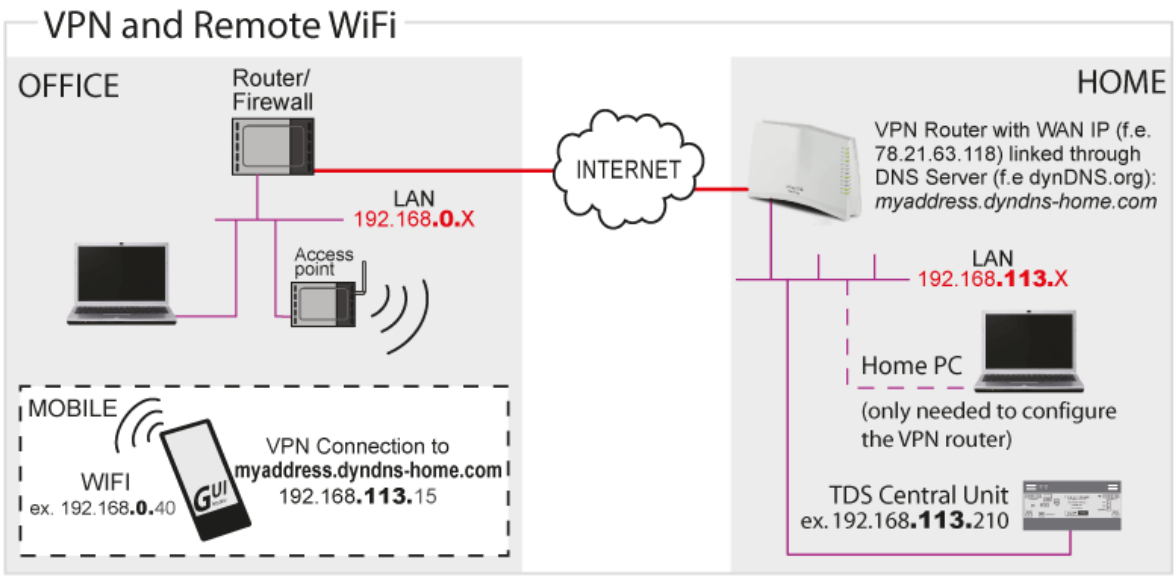
☝ **BELANGRIJK: Bij het gebruik van een VPN verbinding vanop het netwerk dient u er steeds voor te zorgen dat het netwerk waarmee u zich verbindt en het netwerk van waarop u zich verbindt een verschillende IP subnet hebben (in de meeste gevallen betekent dit dat de eerste 3 getallen niet gelijk zijn (192.168.1.1 en 192.168.1.100 zitten in hetzelfde subnet, 192.168.0.1 zit in een ander subnet, net zoals 10.0.1.1)**

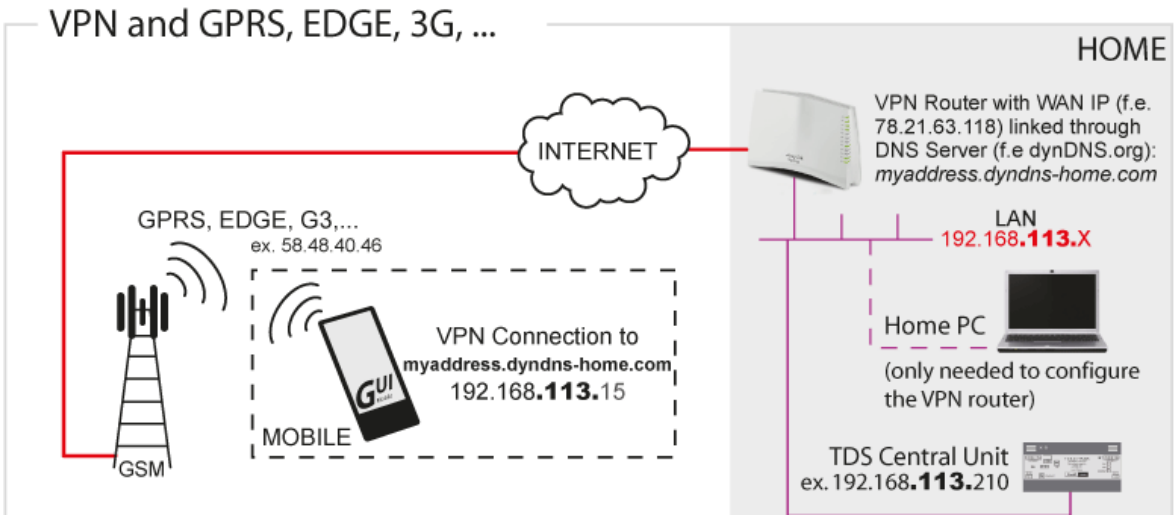
Voorbeeld: wanneer u uw privaat netwerk hebt geconfigureerd in de rij 192.168.1.xxx en u heeft een GUI op uw Smartphone dan zal u geen problemen ondervinden bij het verbinden via een GPRS/EDGE/3G/HSDPA/4G verbinding. Wanneer u een vakantiewoning heeft (die beschikt over een internetverbinding) kan u deze verbinden met uw centrale eenheid door het gebruik van de LAN van uw vakantiewoning, maar u moet er zeker van zijn dat de netwerkrij van uw vakantiewoning verschillend is van 192.168.1.xxx.

De meeste residentiële en kleine bedrijfsnetwerken, zitten in het bereik 192.168.X.X met 192.168.1.X en 192.168.0.X als meest gebruikte. Aangezien je veelal niet weet met welke netwerken je via VPN jouw netwerk zal verbinden, is het aangewezen om een willekeurig nummer te kiezen voor het derde stuk van het IP adres (vb.: 192.168.**113**.X).

☝ **Neem een ander nummer dan 168 of 10 als derde stuk van het IP adres aangezien deze in conflict kan komen met het virtuele netwerk die via USB connectie met de TELETASK Centrale eenheid wordt opgesteld.**

Hier is een tekening van een basis installatie (De thuis-PC is enkel in de tekening opgenomen ter illustratie van een praktisch thuisnetwerk. De PC is enkel tijdelijk nodig voor het configureren van de VPN router):





5.1.4 Installeer een router met ingebouwde VPN server

5.1.4.1 Inleiding

Er zijn heel wat routers op de markt met een ingebouwde VPN server en het is onmogelijk om alle types hier op te sommen.

Daarom hebben we bij TELETASK zelf enkele types getest en geven we u hierbij een gedetailleerde installatie procedure voor één van de (volgens onze mening) meest betrouwbare en eenvoudig te installeren router, namelijk de VIGOR 2130 van DrayTek. Verderop staan ook de installatiestappen van de SnapGear SG300 router. Deze router is niet langer beschikbaar maar voor zij die deze router al hadden, blijft deze informatie in het document.

De installatie van een VPN verbinding is voor andere type routers ongeveer hetzelfde, maar wanneer u beslist een ander type router te gebruiken, gelieve rekening te houden met de volgende bemerkingen:

- Alhoewel PPTP (een protocol voor VPN) een standard is kan de specifieke toepassing van merk tot merk verschillen (bij router en toestel). Controleer dus op voorhand of het toestel (vb. PC of Smartphone) compatible is met de router.
- Er zijn verschillende types data encryptie dus controleer de specificaties van je (mobiel) toestel nauwkeurig bij het kiezen van de VPN router. Ga na of deze compatible zijn.
- TELETASK kan geen support leveren voor elk type router. Indien u extra hulp nodig hebt, gelieve contact te nemen met uw lokale router verkoper (voor VIGOR check www.draytek.com).

5.1.5 VIGOR 2130 Configuratie

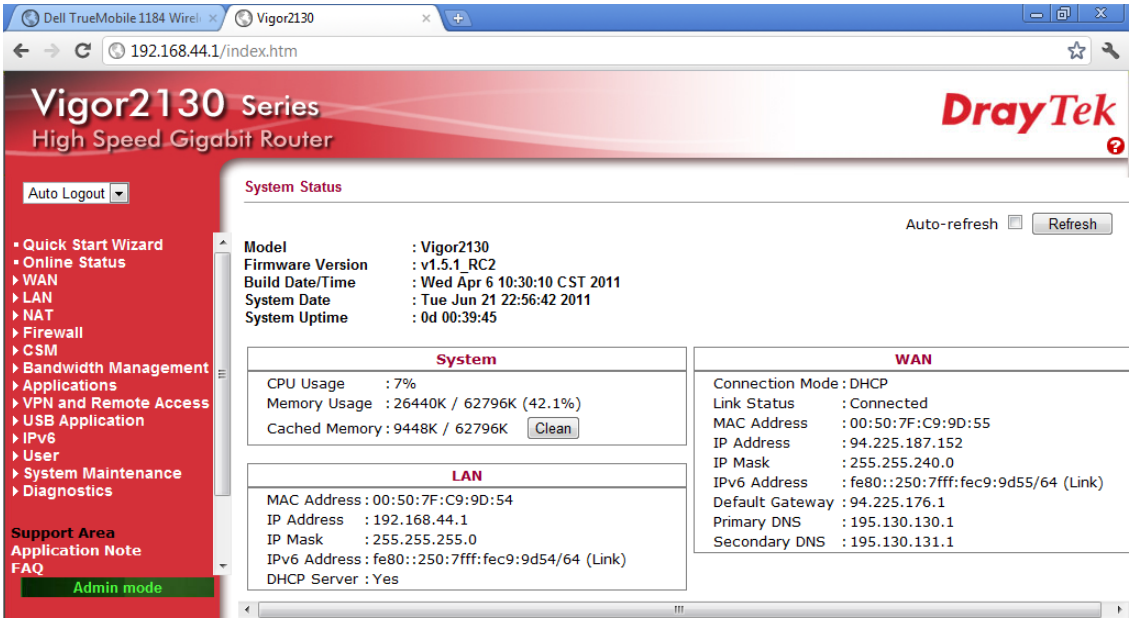
In dit deel van het document staat de term 'VIGOR' voor de VIGOR 2130 serie router. Voor deze documentatie is de standaard VIGOR 2130 gebruikt. Er bestaan ook versies met ingebouwde WiFi en andere functionaliteiten.

5.1.5.1 Algemene instellingen

Verbindt de VIGOR met een computer via één van de LAN poorten van de VIGOR en sluit de WAN poort van de VIGOR aan op het internet.

Het standaard IP adres van de VIGOR is 192.168.1.1. Wanneer je deze invult in een browser, kom je op de login pagina. Het standaard login en paswoord zijn 'admin' (zonder de aanhalingstekens).

Na het inloggen zie je een soortgelijke pagina:

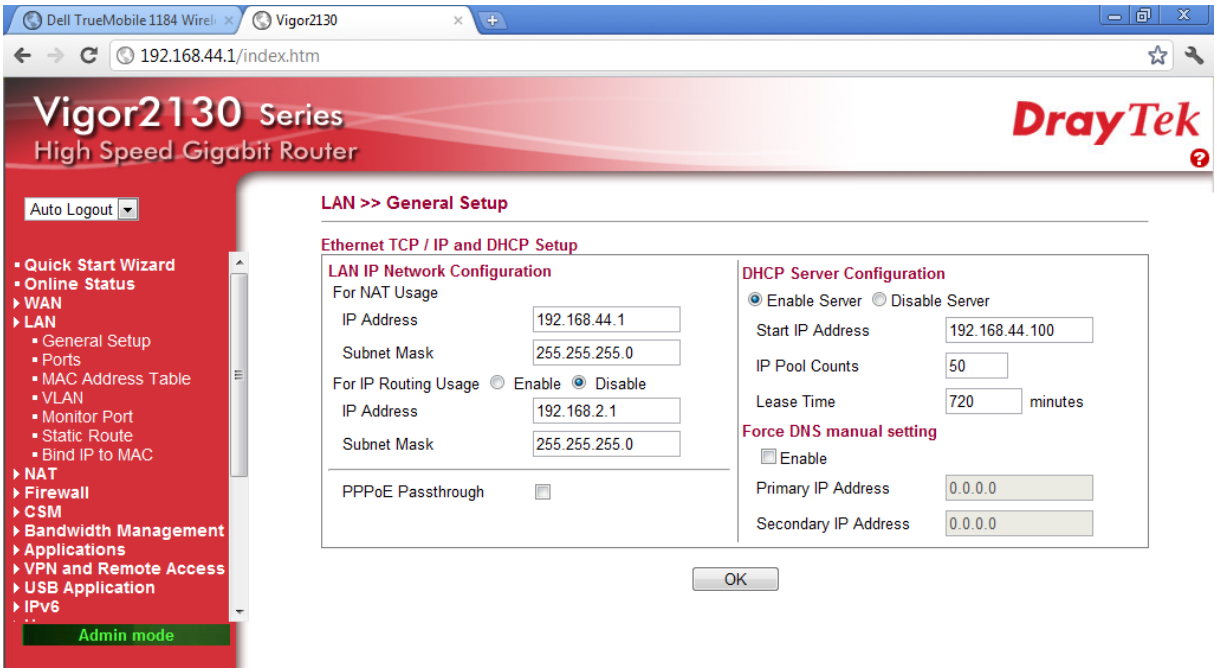


Ter info: de Firmware versie van de VIGOR waarvoor deze handleiding is geschreven is v1.5.1_RC2. Er kunnen kleine verschillen optreden bij andere versies.

Het is aangewezen om te starten met de 'Quick Start Wizard' (bovenste item in de linker kolom). Deze zal de tijdzone, een nieuwe administrator paswoord en enkele basis instellingen betreffende de internet connectie, instellen (vraag de correcte informatie bij je Internet Provider). In de meeste gevallen zullen de standaard ingevulde waardes OK zijn.

5.1.5.2 LAN Instellingen

Zoals eerder aangegeven is het netwerkbereik van je netwerk belangrijk voor VPN. Om het netwerkbereik aan te passen, klik 'LAN' > 'General Setup'.

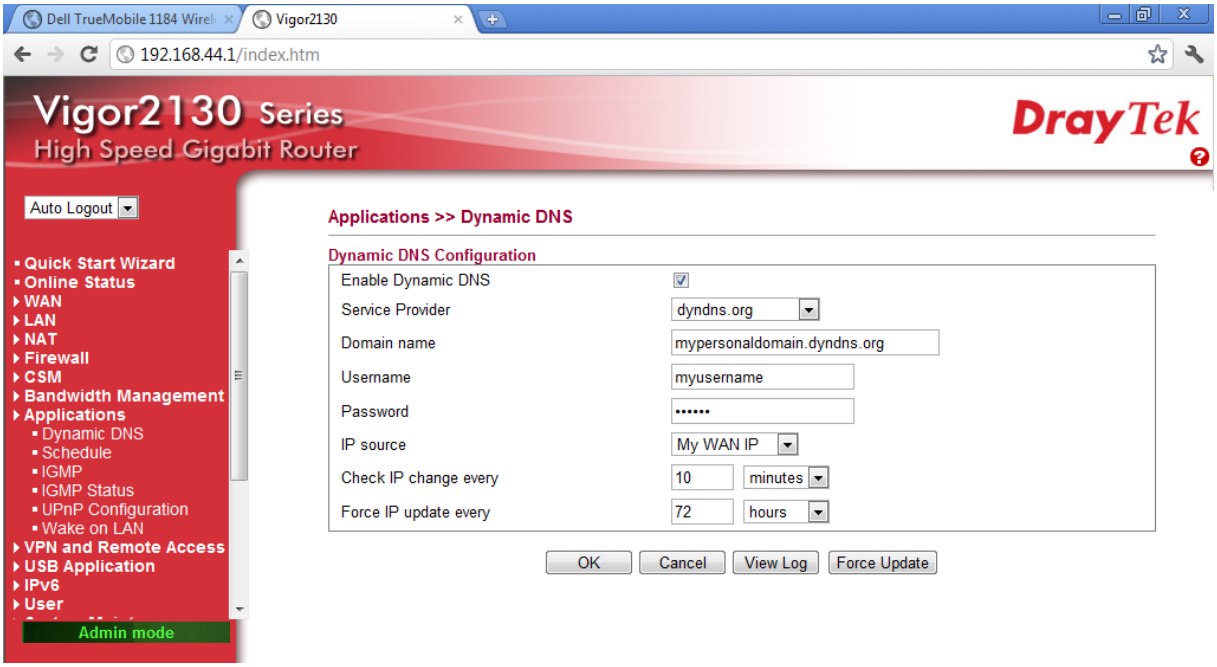


In de 'LAN IP Network Configuration' stel je het derde nummer van het IP adres in naar wens. Onder 'DHCP server Configuration' moet je bij de 'Start IP Address' een adres in het zelfde netwerkbereik invullen.

Opmerking: het 'Start IP Address' samen met de 'IP Pool Counts', vormen het bereik van IP adressen die toegewezen kunnen worden aan computers die verbonden zijn aan het netwerk (in dit voorbeeld zijn de adres 192.164.44.100 tot en met 192.168.44.150). Het is belangrijk dat je toestellen zoals de TELETASK DoIP centrale eenheid, een IP camera, een netwerk printer, een netwerkschijf,… **niet** met één van deze IP adressen instelt.

5.1.5.3 Dynamic DNS instellingen

Om de DynDNS in te stellen op de VIGOR klik 'Applications' > 'Dynamic DNS'.



- Vink het 'Enable Dynamic DNS' aan
- Vul het domein naam in dat je geregistreerd hebt bij de provider (in dit voorbeeld mypersonaldomain.dyndns.org)
- Vul de login en het paswoord in die je gebruikt voor de DynDNS registratie met de provider
- Selecteer de juiste instelling voor 'IP source': kies voor 'My WAN IP' als de VIGOR rechtstreeks met het internet is verbonden, kies voor 'My Internet IP' als er een kabel/DSL modem-router tussen de VIGOR en het internet zitten (zie opmerking hier onder).
- De rest van instellingen zijn normaal gezien OK

☝ **Opmerking: als er een kabel/DSL modem-router tussen de VIGOR en het internet zit moet je de volgende stappen ondernemen om alles vlot te laten werken. In de geval zal het WAN IP adres van de VIGOR aan 'private IP address' zijn (in het bereik van 10.x.x.x, 172.16.x.x tot 172.31.x.x of 192.168.x.x). Als de VIGOR zijn IP adres (vb.: 192.168.1.x) zou doorgeven aan jouw dynamic IP-address host, zou dit niet werken aangezien dit een 'private IP address' is. Om dit op te lossen moet je de VIGOR instellen zodat hij zijn 'internet IP address' en niet zijn lokaal 'My WAN IP address' gebruikt.**
Om het mogelijk te maken om vanaf het internet met de VIGOR te kunnen verbinden, moet de kabel/DSL modem-router voorzien worden van port-forwarding. Stuur poort 1723 door naar het WAN IP-adres van de VIGOR VPN router. Het is ook aanbevolen om de WAN IP adres van de VIGOR statisch te zetten (vb.: 192.1.0.2). Raadpleeg je internet provider voor meer details voor het instellen van port-forwarding van de kabel/DSL modem-router.

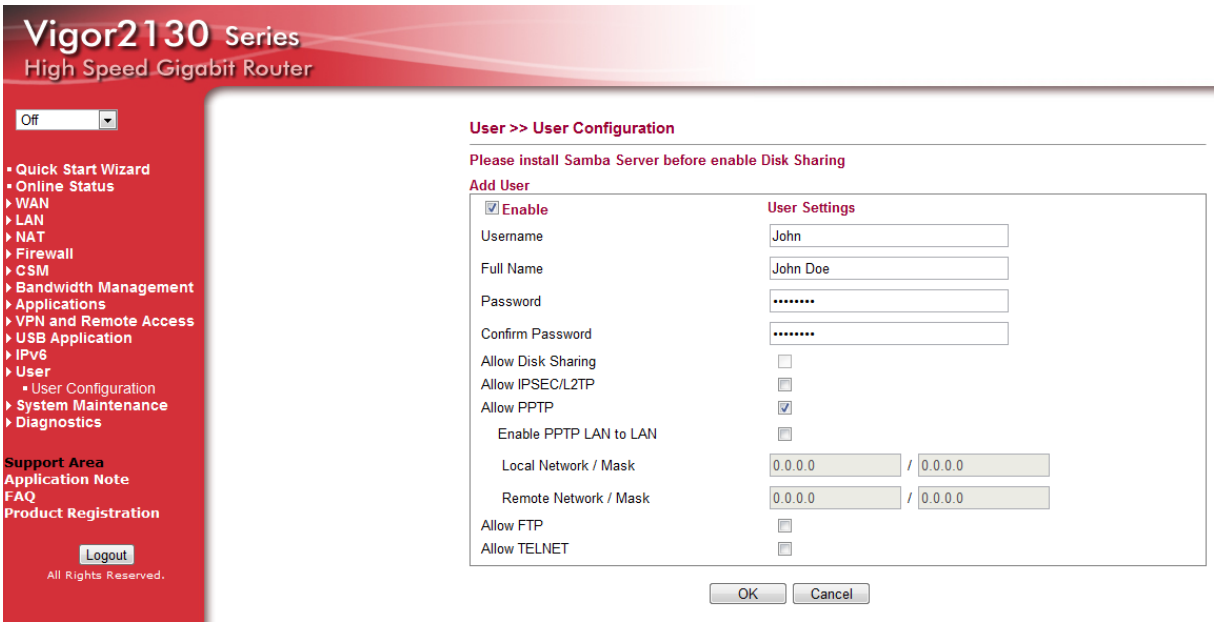
☝ **BELANGRIJKE OPMERKING: Dit is niet het zelfde als rechtstreeks port-forwarden naar de Centrale Eenheid! Er wordt nog steeds gebruik gemaakt van de beveiligde VPN verbinding. Je gebruikt hier enkel het port-forwarden om vanop het internet rechtstreeks met je VIGOR VPN router te verbinden.**

5.1.5.4 Toevoegen van gebruikers

Voordat we de VPN server kunnen opzetten, moeten er eerst gebruikers toegevoegd worden. Elke gebruiker heeft zijn eigen gebruikersnaam en paswoord om te verbinden met de VPN server (en kan verschillende privileges hebben).

Om een gebruiker toe te voegen, klik 'User' → 'User Configuration'

Je zal dit scherm zien:



- Vink het 'Enable User Settings' aan

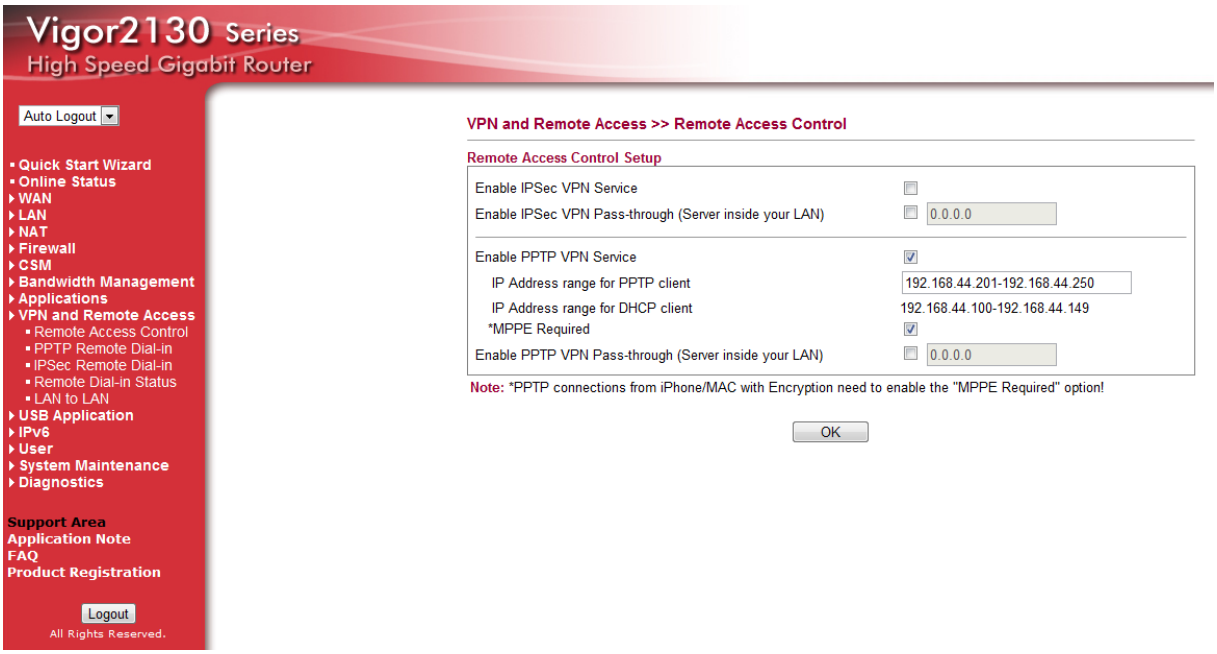
Vul in:

- Username: een naam voor de gebruiker om in te loggen op de VPN (elke gebruiker moet een unieke naam hebben)
- Full name: de volledige naam van de gebruiker (enkel ter info)
- Password: het paswoord voor de gebruiker
- Vink aan: 'Allow PPTP field'
- Klik OK

Herhaal deze stappen voor alle gebruikers.

5.1.5.5 VPN server instellingen

We zijn nu klaar om de VPN server zelf, in te stellen. Klik op 'VPN and Remote Access' → 'Remote Access Control'.



Pas de volgende instellingen aan:

- Vink uit: ‘Enable IPSec VPN Service’
- Vink aan: ‘Enable PPTP VPN Service’
- Als je van plan bent om Apple toestellen (zoals iPhone, iPad, etc.) te gebruiken, vink dan ‘MPPE Required’ aan

Opmerking: zoals de DHCP server, heeft de VPN server ook aan waaier van IP adressen van welke het een IP adres geeft aan een toestel dat een VPN verbinding maakt. Zorg er dus voor dat toestellen die fysisch op het netwerk zitten, geen statisch IP adres hebben in het IP adres bereik van de ‘IP Address range for PPTP client’.

Klik OK om de instellingen op te slaan. De VIGOR is nu klaar om binnenkomende VPN connecties toe te laten.

5.1.6 Installeer de SG300 VPN router (niet meer verkrijgbaar)

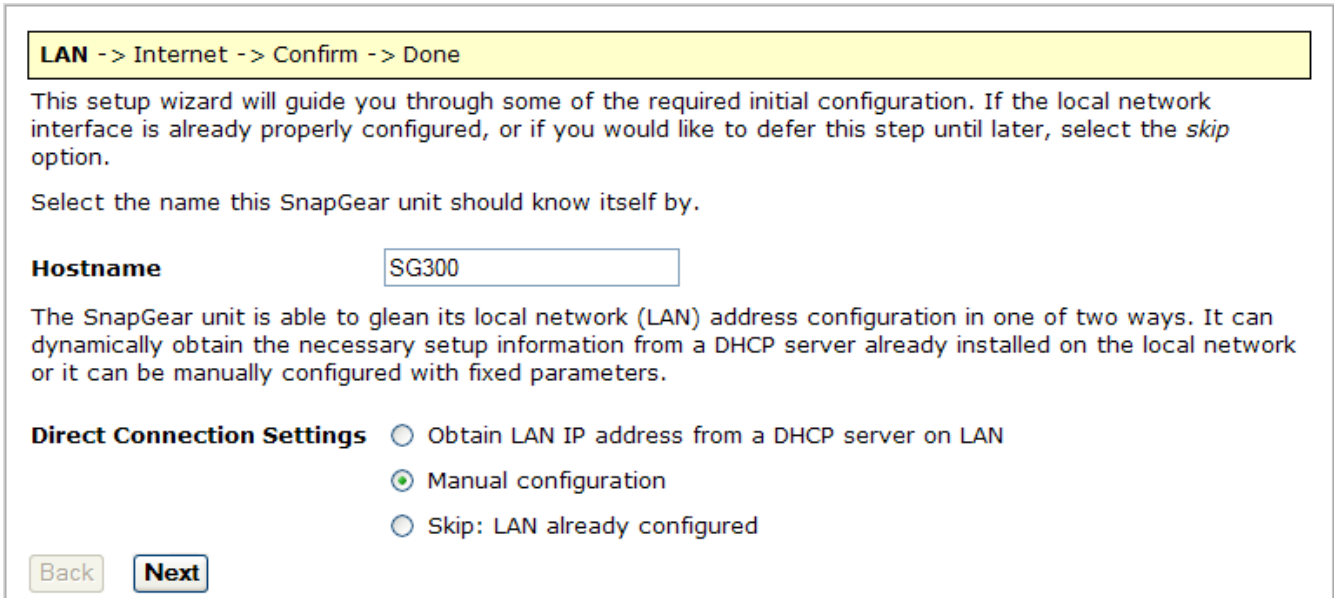
Van zodra u de laptop hebt verbonden met de LAN zijde van de SnapGear router, opent u de browser en surft u naar de SG300. U geeft het kernpaswoord in (dit is niet standaard geconfigureerd). Merk op dat de default LAN verbinding van de SG300 statisch is geconfigureerd op 192.168.0.1

De snelste manier om uw Router/Firewall te installeren is het gebruik van de ‘Quick Setup Wizard’.

Volgende schermen zullen verschijnen op uw configuratie-PC:

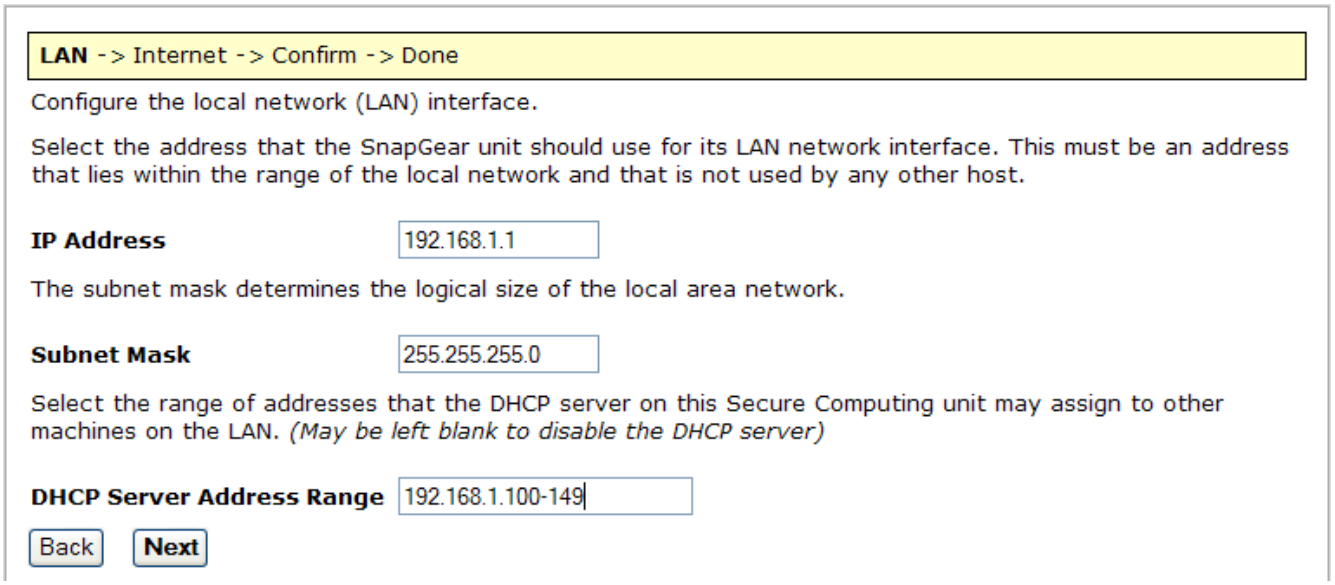
- Quick Setup
- Manual LAN Configuration
- ISP connection

5.1.6.1.1 Quick Setup



In de meeste gevallen zal 'Manual configuration' de correcte setting zijn omdat de SG300 het enige apparaat zal zijn dat zal fungeren als een DHCP server.

5.1.6.1.2 Manuele LAN Configuratie



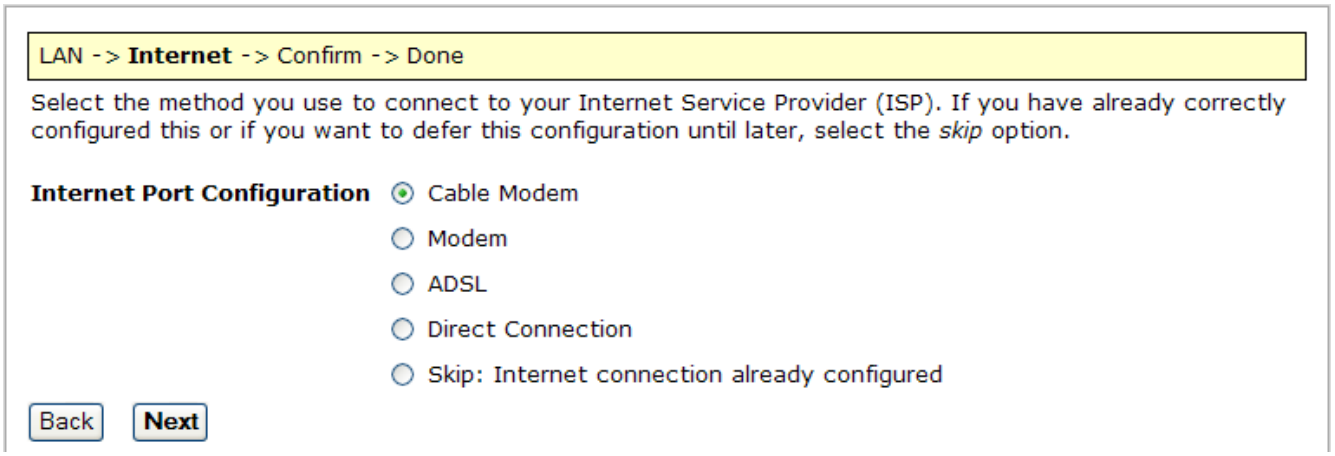
In dit geval veronderstellen we dat we het private netwerk zullen configureren in de rij: 192.168.1.xxx en kiezen we voor het LAN IP-Adres van de SG300: 192.168.1.1

BELANGRIJK: Bij het gebruik van een VPN verbinding vanop het netwerk dient u er steeds voor te zorgen dat het netwerk waarmee u zich verbindt en het netwerk van waarop u zich verbindt een

verschillende IP subnet hebben (in de meeste gevallen betekent dit dat de eerste 3 nummers niet gelijk zijn (192.168.1.1 en 192.168.1.100 zitten in hetzelfde subnet, 192.168.**0**.1 zit in een ander subnet, net zoals **10**.**0**.1.1)

Voorbeeld: wanneer u uw privaat netwerk hebt geconfigureerd in de rij 192.168.1.xxx en u heeft een GUI op uw Smartphone dan zal u geen problemen ondervinden bij het verbinden via een GPRS/EDGE/3G verbinding. Wanneer u een vakantiewoning heeft (die beschikt over een internetverbinding) kan u deze verbinden met uw centrale eenheid door het gebruik van de LAN van uw vakantiewoning, maar u moet er zeker van zijn dat de netwerkrij van uw vakantiewoning verschillend is van 192.168.1.xxx.

5.1.6.1.3 ISP Verbinding



Hier dient u de correcte verbinding met het internet te kiezen,

indien u deze niet kent, neem contact op met uw Internet Service Provider (in de meeste gevallen is de optie 'Direct Connection' correct).

Na het afwerken van de wizard zal u het IP-Adres in uw browser moeten wijzigen naar 192.168.1.1 om verder te gaan met de configuratie.

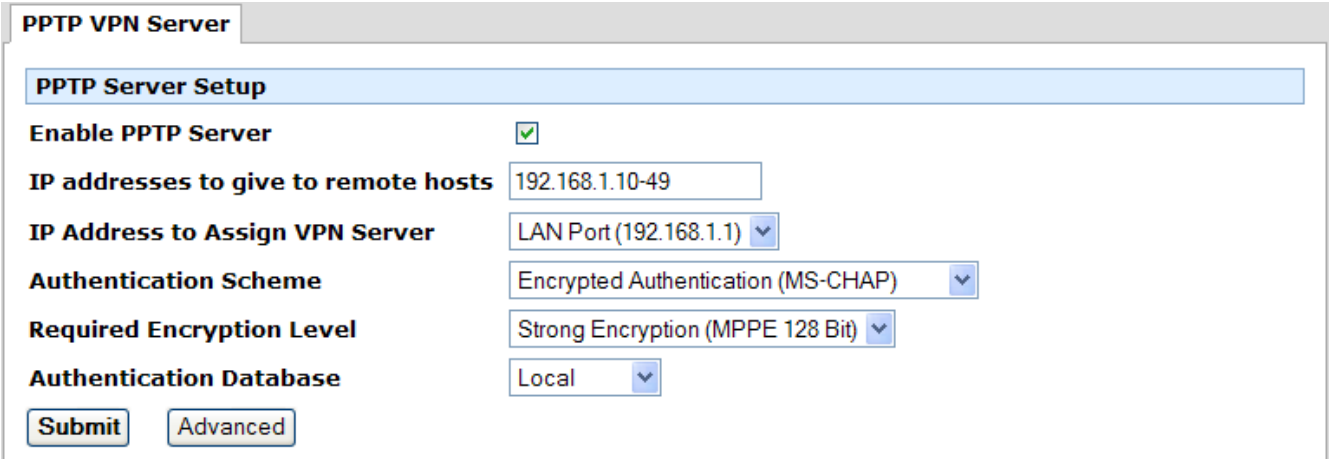
5.1.6.1.4 VPN Configuratie

In de voorgaande stap heeft u de basis- netwerkinstellingen geconfigureerd. Nu kunnen we starten met het instellen van de actuele VPN server.

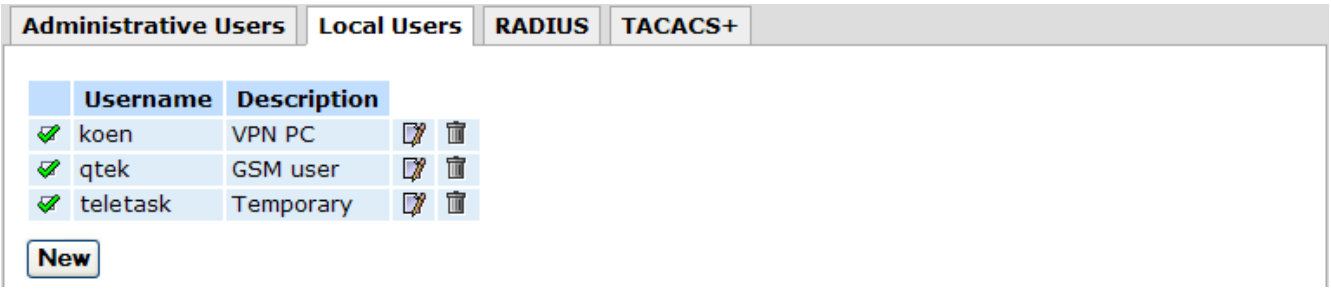
- Klik links onder op VPN on PPTP VPN Server
- Controleer de optie "Enable PPTP Server"
- Kies voor het "Authentication Scheme" "Encrypted Authentication (MS-CHAP), dit betekent dat de apparaten die de MS-CHAP (of MS-CHAP v2) gebruiken, kunnen verbonden worden.

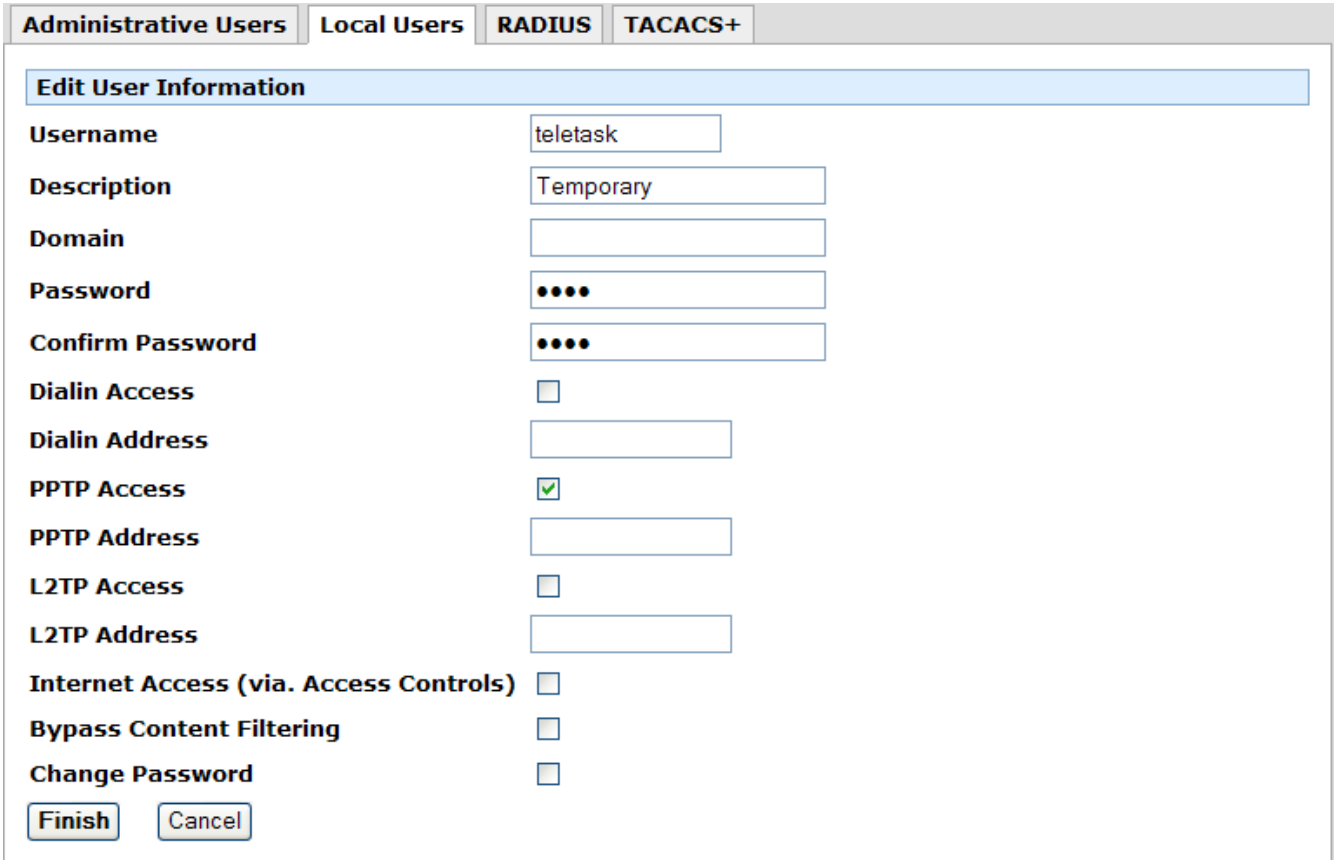
Wanneer er enkel PC's waarop Windows Vista loopt en/of Smartphones die werken met Windows mobile V6 worden gebruikt, kan u de optie "Encrypted Authentication (MS-CHAP v2)" hier kiezen.

- Laat de rest van de settings zoals ze staan en klik op 'Submit'.



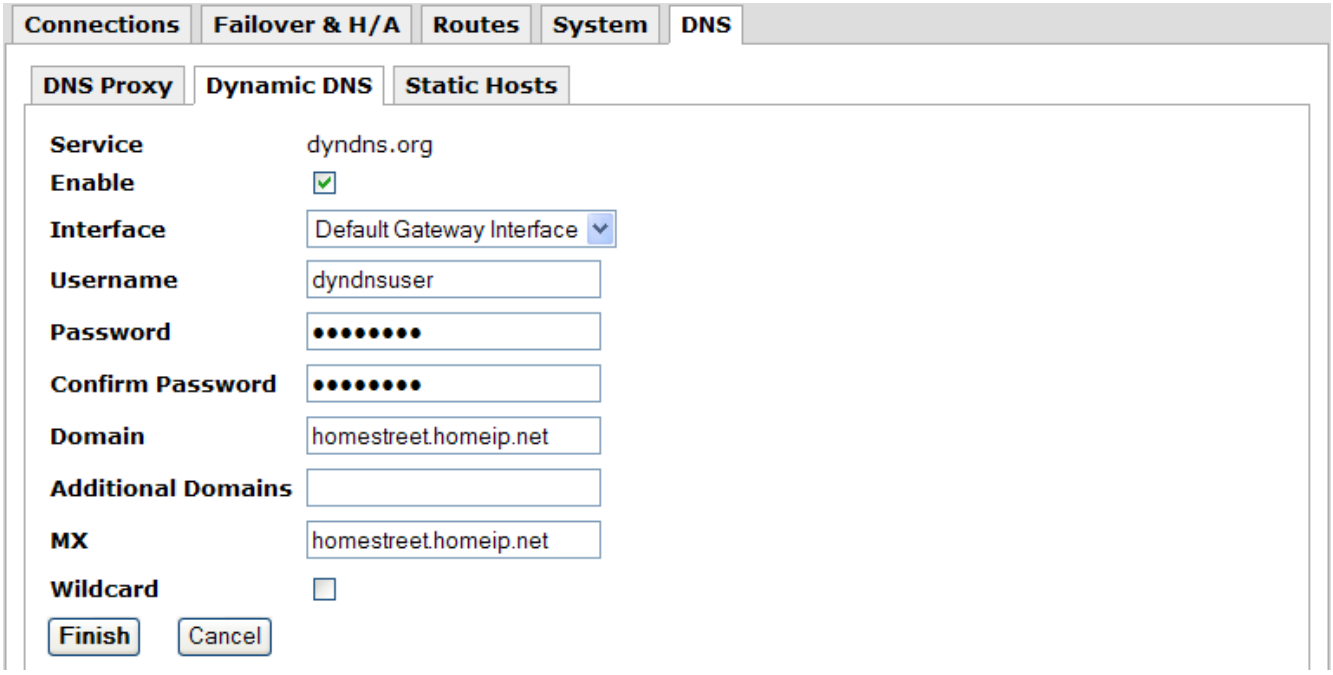
- Klik links onder System on User en kies de tabtoets 'Local Users'.
- Klik 'New', vul naam, beschrijving en paswoord in.
- Wees er zeker van dat de optie"PPTP access" is aangevinkt.
- Klik 'Finish'.





5.1.6.1.5 Instellen van een DynDNS in de SG300

- Klik links op Network Setup onder NETWORK SETUP en kies de tabtoets DNS en dan de tabtoets pagina Dynamic DNS .
- Selecteer "dyndns.org" uit de lijst en klik “New”
- Vink de "Enable" optie aan
- Geef uw DynDNS username paswoord en Domain in (in het onderstaande voorbeeld habben we een DynDNS account met username 'dyndnsuser' en hostname 'homestreet.homeip.net')
- klik "Finish"



5.1.7 Installeer een client VPN connectie

Nu de router werd geïnstalleerd en de Dynamic DNS werd geactiveerd, kunnen we een VPN verbinding vanop afstand installeren. In deze stap zullen we een VPN verbinding opstarten met Windows XP (voor Windows Vista zijn de te nemen stappen identiek). Wanneer u een VPN verbinding wenst op te starten vanop een Windows Mobile apparaat, stellen we voor om eerst een PC verbinding aan te maken (om de werking van de VPN server te testen) en pas daarna de verbinding vanop uw Windows Mobile apparaat op te starten. Indien hulp nodig betreffende het opzetten van een VPN verbinding vanop een mobiel apparaat, zie de installatiehandleiding voor de 'GUI for Smartphones'.

Opstarten van een verbinding met Windows XP. Neem de volgende stappen:

- Ga naar Start > Configuration panel > Network connections.

- Klik op ‘Create a new connection’.

- Kies: to make a connection to the network at my workplace en klik "Next".

- Kies VPN connection en klik "Next"

- Geef het een naam waardoor u weet dat dit de verbinding met uw (clients) huis betreft en klik "Next"

- Als Host name of IP adres, geeft u de hostname die u configureerde op de Dyn DNS (in het door ons gebruikte voorbeeld was dit 'homestreet.homeip.net'). Indien u een statisch IP adres heeft, geeft u nu uw IP adres in.
- Klik "Next", en dan "Finish" in het volgende scherm.De laptop kan nu verbonden worden met uw "home network"

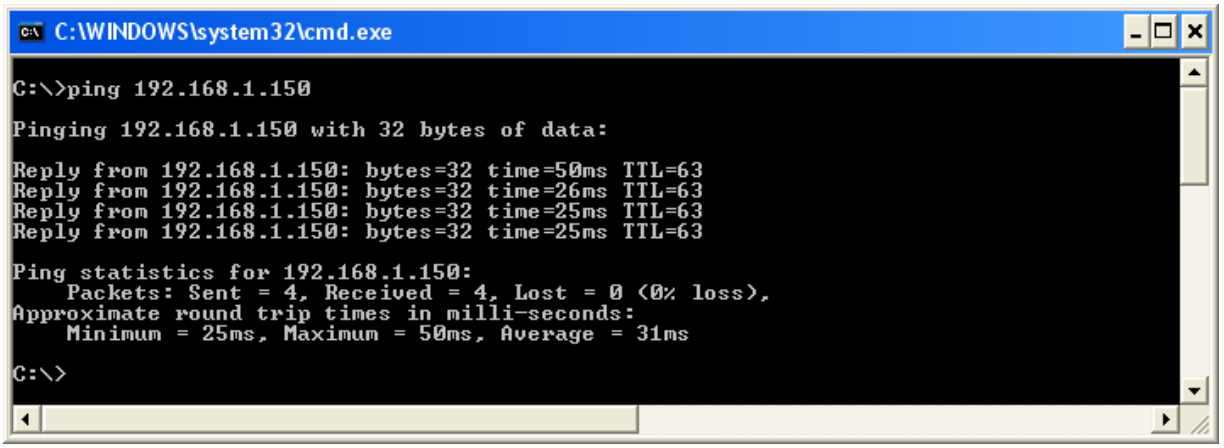
5.1.8 Test de VPN verbinding

In dit hoofdstuk zullen we eerst de verbinding testen en dan uitleggen hoe u de TELETASK GUI via een VPN verbinding kan gebruiken.

5.1.8.1 Test de VPN verbinding

- Open uw VPN verbinding met "Start", "Connect to".
- Geef uw User name en paswoord in (deze die u heeft gecreëerd in de router –zie hoofdstuk “VPN verbinding”).
- Klik connect

- Om de verbinding te testen, stellen we u voor om een ping naar het IP adres van uw installatie thuis (vb uw MICROS+) te sturen. Wanneer u alles correct hebt geïnstalleerd zou dit moeten werken.



5.1.8.2 Gebruik van de TELETASK GUI via een VPN verbinding

Zoals vermeld in de inleiding, is één van de voordelen van een VPN verbinding dat de configuratie voor lokaal gebruik en gebruik vanop afstand exact dezelfde is. Daarom dient hetzelfde IP adres ingegeven te worden in de eigenschappen van de GUI (of iSGUI) alsook hetzelfde poortnummer, net zoals u doet bij het lokaal gebruik van de GUI.

Dus u kan uw GUI laten werken vanop uw laptop thuis, u neemt de laptop mee naar het werk, op vakantie en u laat de GUI werken vanop afstand op identieke wijze als u thuis zou doen.

Het enige waaraan u moet denken is te klikken op "Connect to" en u verbinden met uw huisnetwerk alvoor u start met de GUI te laten werken vanop afstand. Voor de GUI for Smartphones is het nog eenvoudiger, het opent namelijk automatisch de VPN verbinding wanneer nodig. Meer informatie desbetreffende kan u terugvinden in de handleidingen van de GUI en GUI for Smartphones.