TELETASK

Home Automation

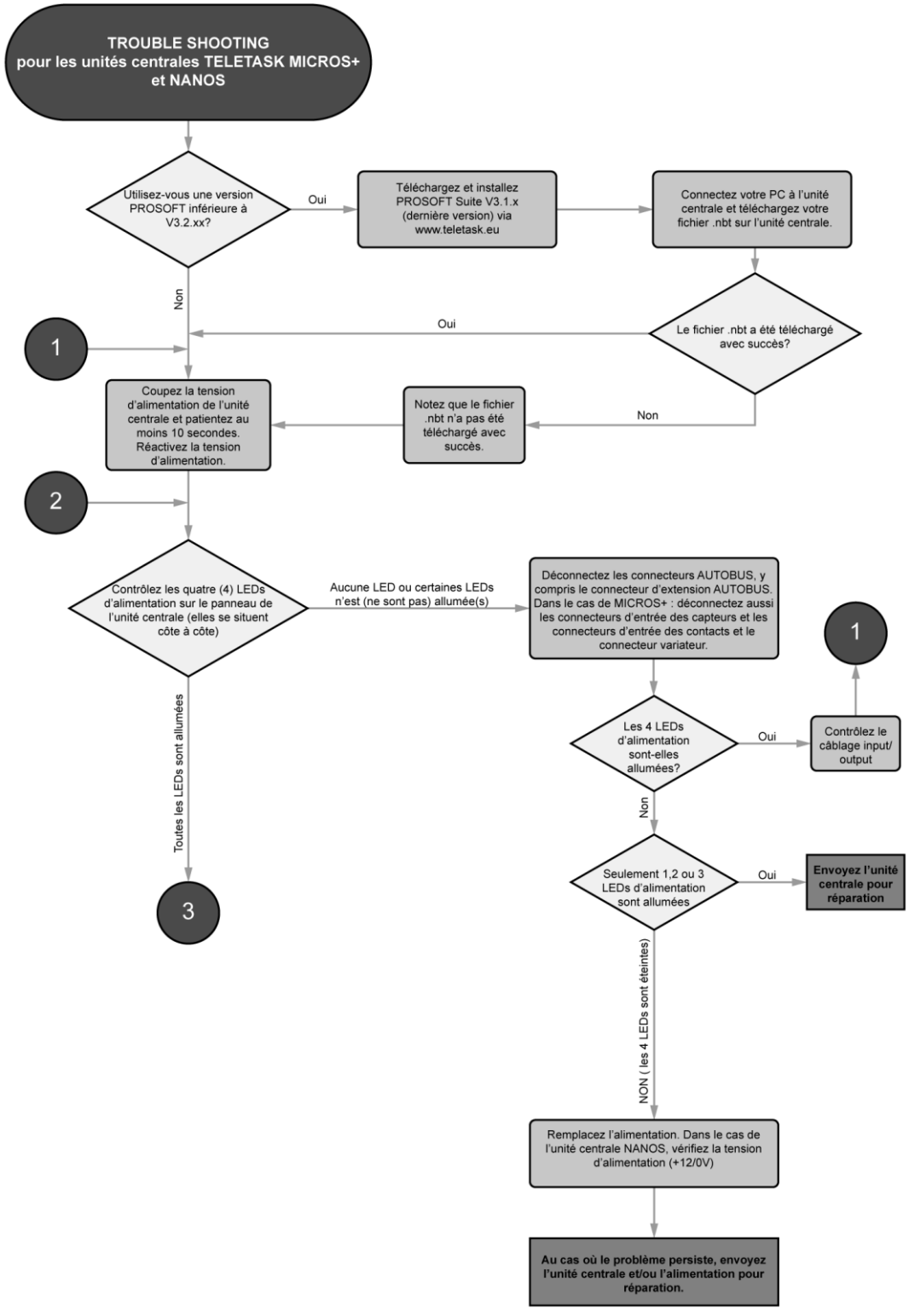
Support & Troubleshooting

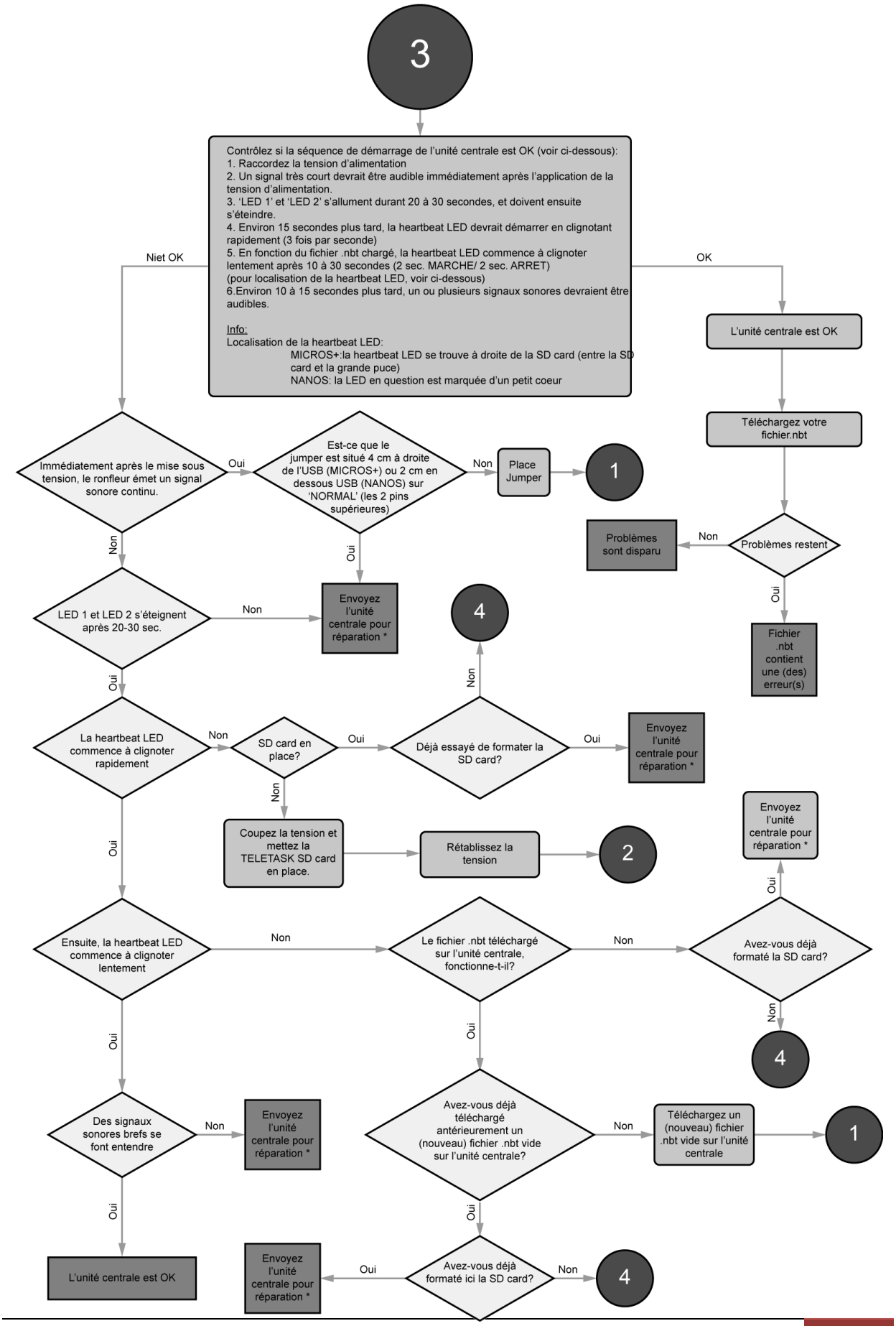
+ Tips & tricks

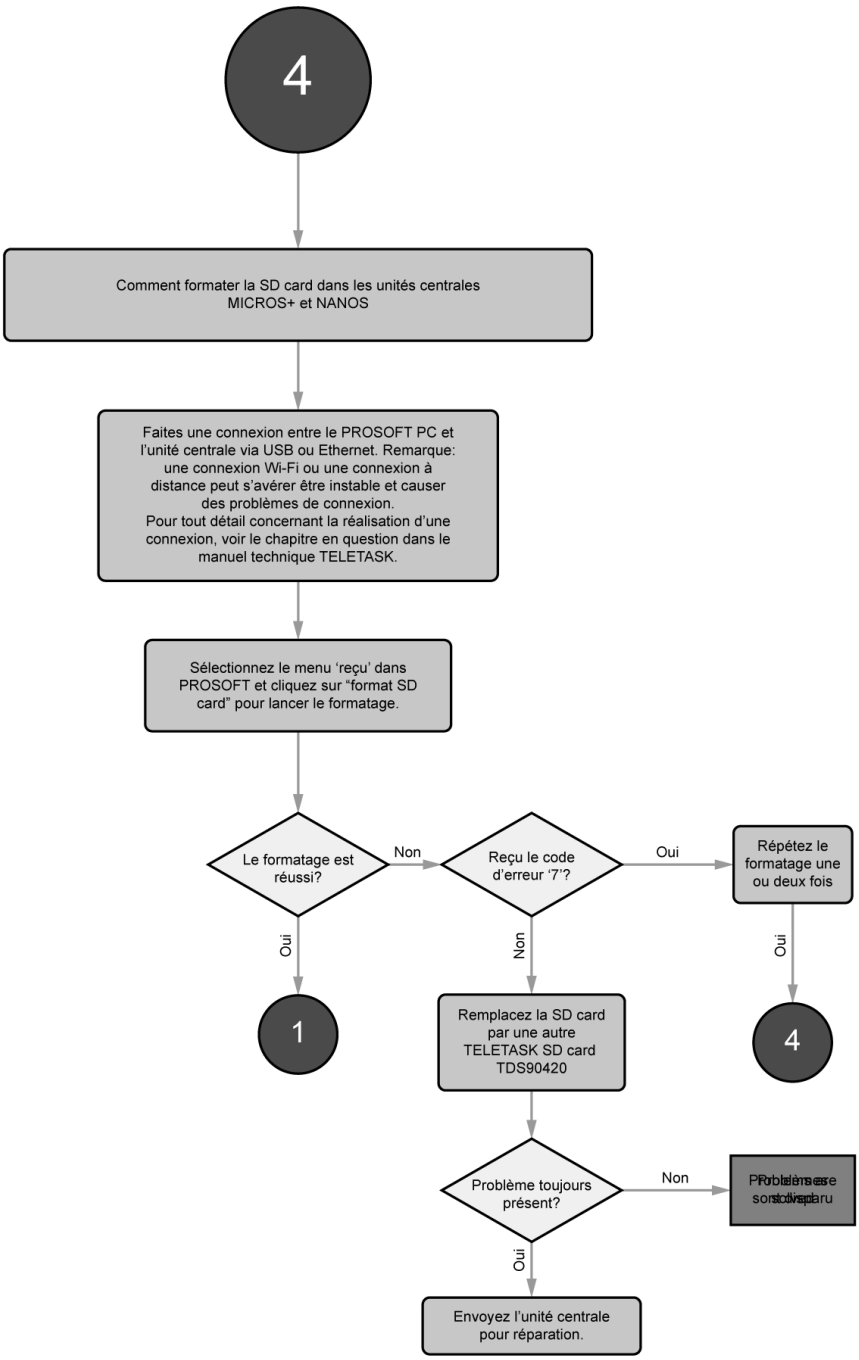
Version: 11 Juin 2013

Table des Matieres

1 Trouble shooting MICROS+ et NANOS




3
Contrôlez si la séquence de démarrage de l'unité centrale est OK (voir ci-dessous):
1. Raccordez la tension d'alimentation
2. Un signal très court devrait être audible immédiatement après l'application de la tension d'alimentation.
3. 'LED 1' et 'LED 2' s'allument durant 20 à 30 secondes, et doivent ensuite s'éteindre.
4. Environ 15 secondes plus tard, la heartbeat LED devrait démarrer en clignotant rapidement (3 fois par seconde)
5. En fonction du fichier .nbt chargé, la heartbeat LED commence à clignoter lentement après 10 à 30 secondes (2 sec. MARCHE/ 2 sec. ARRET)
(pour localisation de la heartbeat LED, voir ci-dessous)
6.Environ 10 à 15 secondes plus tard, un ou plusieurs signaux sonores devraient être audibles.
Info:
Localisation de la heartbeat LED:
MICROS+:la heartbeat LED se trouve à droite de la SD card (entre la SD card et la grande puce)
NANOS: la LED en question est marquée d'un petit coeur
Niet OK
OK
L'unité centrale est OK
Téléchargez votre fichier.nbt
Problèmes restent
Non
Problèmes sont disparu
Oui
Fichier .nbt contient une (des) erreur(s)
Immédiatement après le mise sous tension, le ronfleur émet un signal sonore continu.
Oui
Est-ce que le jumper est situé 4 cm à droite de l'USB (MICROS+) ou 2 cm en dessous USB (NANOS) sur 'NORMAL' (les 2 pins supérieures)
Non
Place Jumper
1
Non
Oui
LED 1 et LED 2 s'éteignent après 20-30 sec.
Non
Envoyez l'unité centrale pour réparation *
4
Oui
La heartbeat LED commence à clignoter rapidement
Non
SD card en place?
Oui
Déjà essayé de formater la SD card?
Oui
Envoyez l'unité centrale pour réparation *
Non
Non
Coupez la tension et mettez la TELETASK SD card en place.
Rétablissez la tension
2
Oui
Envoyez l'unité centrale pour réparation *
Oui
Ensuite, la heartbeat LED commence à clignoter lentement
Non
Le fichier .nbt téléchargé sur l'unité centrale, fonctionne-t-il?
Non
Avez-vous déjà formaté la SD card?
Non
4
Oui
Oui
Des signaux sonores brefs se font entendre
Non
Envoyez l'unité centrale pour réparation *
Avez-vous déjà téléchargé antérieurement un (nouveau) fichier .nbt vide sur l'unité centrale?
Non
Téléchargez un (nouveau) fichier .nbt vide sur l'unité centrale
1
Oui
Oui
L'unité centrale est OK
Envoyez l'unité centrale pour réparation *
Oui
Avez-vous déjà formaté ici la SD card?
Non
4


4
Comment formater la SD card dans les unités centrales MICROS+ et NANOS
Faites une connexion entre le PROSOFT PC et l'unité centrale via USB ou Ethernet. Remarque: une connexion Wi-Fi ou une connexion à distance peut s'avérer être instable et causer des problèmes de connexion. Pour tout détail concernant la réalisation d'une connexion, voir le chapitre en question dans le manuel technique TELETASK.
Sélectionnez le menu 'reçu' dans PROSOFT et cliquez sur "format SD card" pour lancer le formatage.
Le formatage est réussi?
Non
Reçu le code d'erreur '7'?
Oui
Répétez le formatage une ou deux fois
Oui
Non
Oui
1
Remplacez la SD card par une autre TELETASK SD card TDS90420
4
Problème toujours présent?
Non
Oui
Envoyez l'unité centrale pour réparation.

TROUBLE SHOOTING (*/**/***)
pour une unité centrale MICROS+ et NANOS.

*****

Problème constaté:
dans des cas exceptionnels, le ronfleur démarre immédiatement après la mise sous tension

Cause probable:
la valeur de la résistance R33 doit être 18k ohm au lieu de 10k ohm

Solution:
envoyez l'unité centrale pour réparation (la résistance R33 10k ohm doit être remplacée par une résistance de 18k ohm).

Unités centrales concernées:
MICROS+: numéros de série xxxxx0101 à xxxxx0611
NANOS: numéros de série xxxxx0101 à xxxxx0151

******

Problème constaté:
dans des cas exceptionnels, la heartbeat LED ne commence pas à clignoter après la mise sous tension

Cause probable:
problème avec le connecteur de la SD card
la résistance R20 doit être remplacée (56K à remplacer par 6K8)

Solution:
envoyez l'unité centrale pour réparation (la SD card et/ou R20 doivent être remplacées)

2 Distribution board recommendations (EN)

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. Take care 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 trough 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 bewteen input and output cables

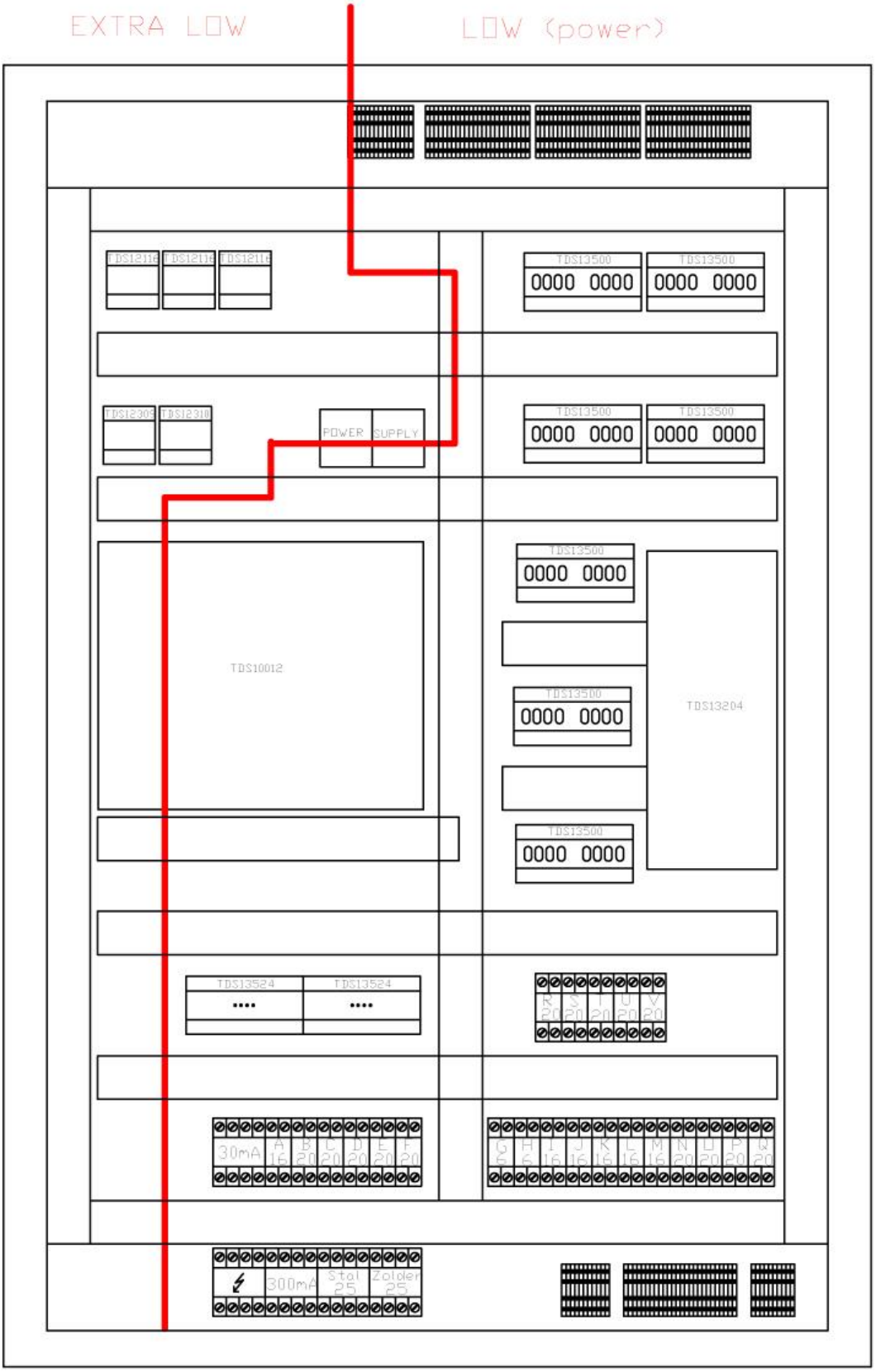


Figure 3: Division between extra-low and low voltage interfaces

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 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 parrallel 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...) are 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 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 brakers 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:

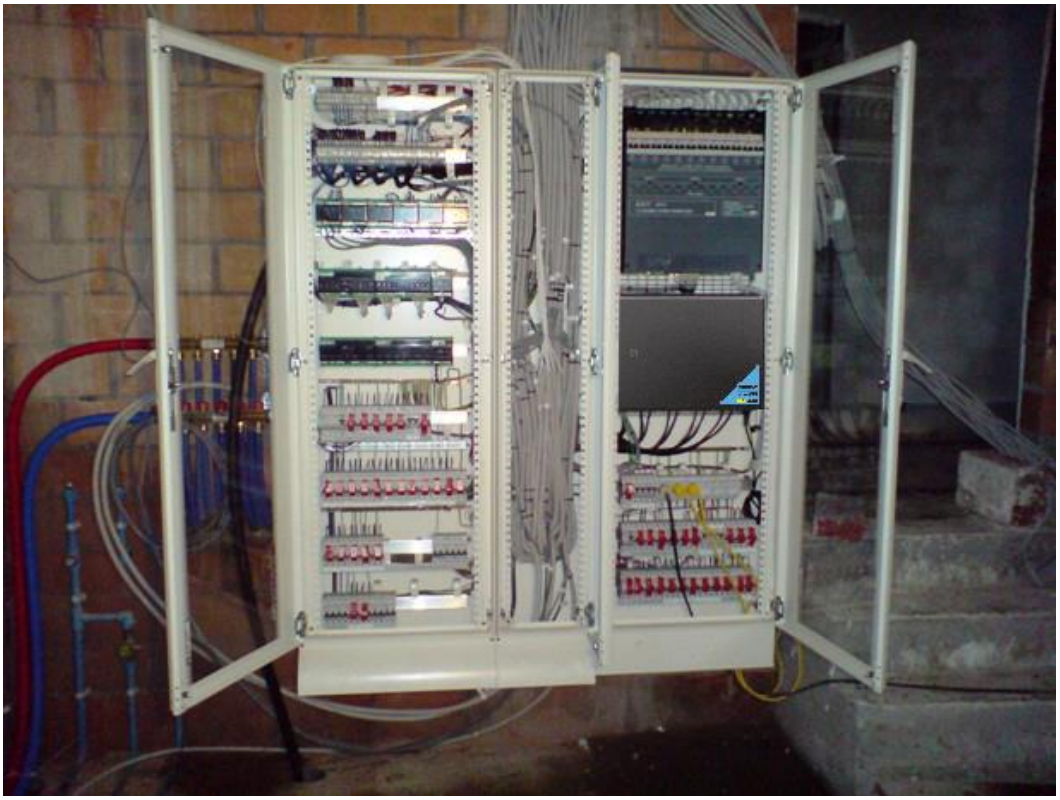


Figure 5: Example distribution board

- The distribution board is divided in zones with a clear division.

- Good overview and clean wire arrangment.

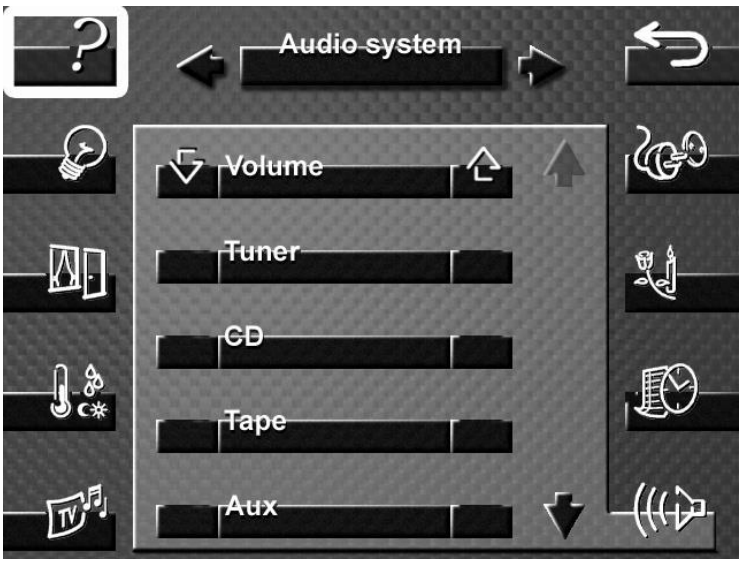
- screw terminals and circuit breakers at the top and bottom of the board.

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-cabels can be run through a left cable tray and all power wires can be run through the middle and right cable tray!

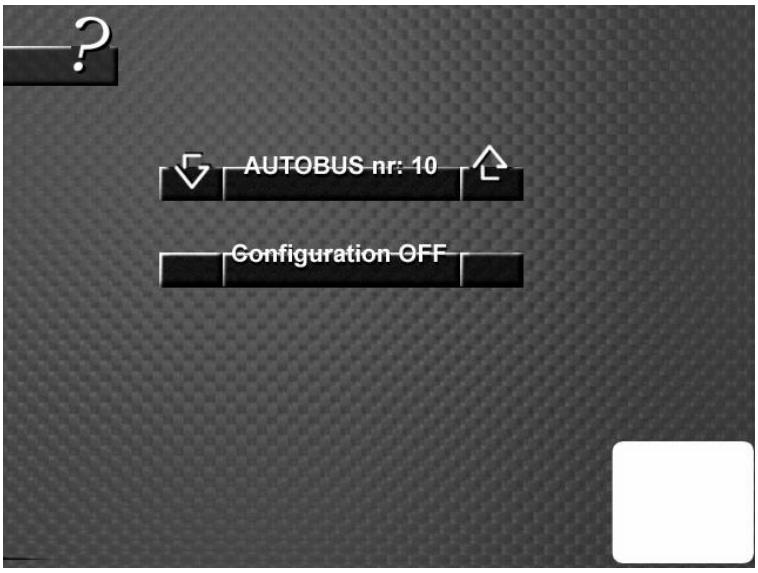
3 Etalonnage de l’écran tactile SERVUS TDS12110

3.1 Comment démarrer l’étalonnage de l’écran tactile?

Choisissez "Menu Paramètres" parmi les boutons du menu principal.

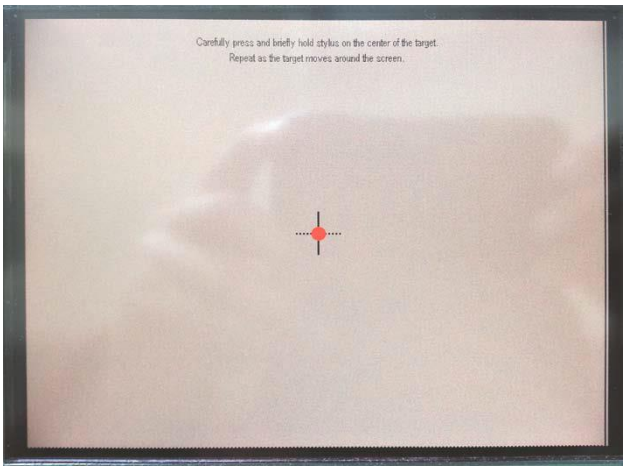


Appuyez sur le bouton "Etalonnage" caché sur le côté inférieur droit de l'écran tactile.

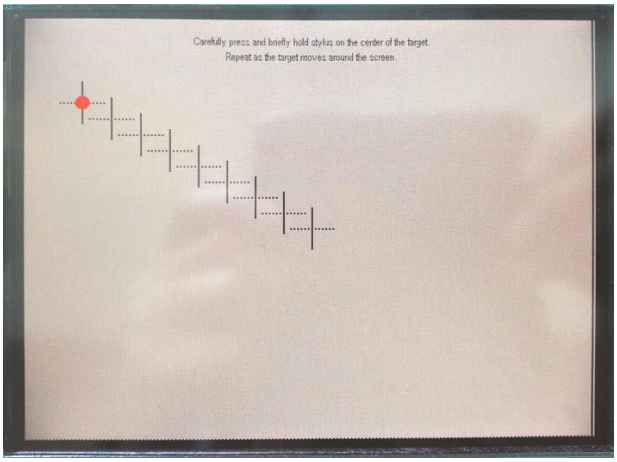


Suivez les instructions et touchez chacun des 5 points d'étalonnage requis (centre de la dernière croix) avec un stylet (et non avec le doigt), pour étalonner l'écran tactile du SERVUS.

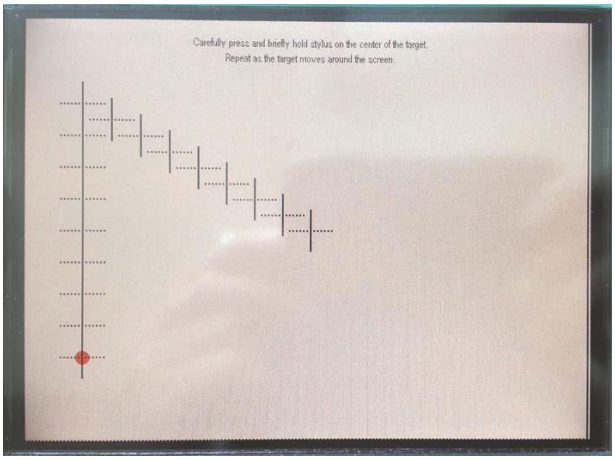
1.



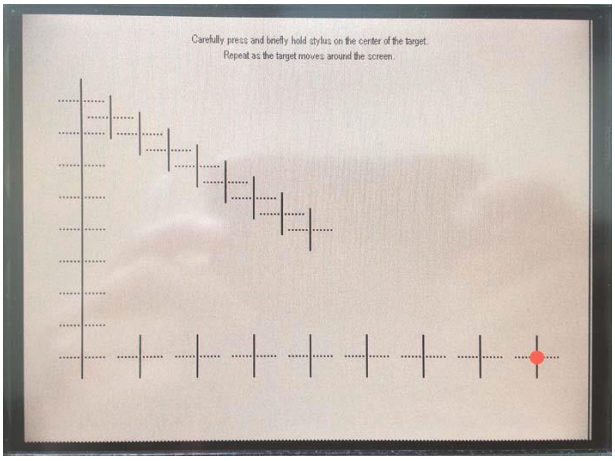
2.



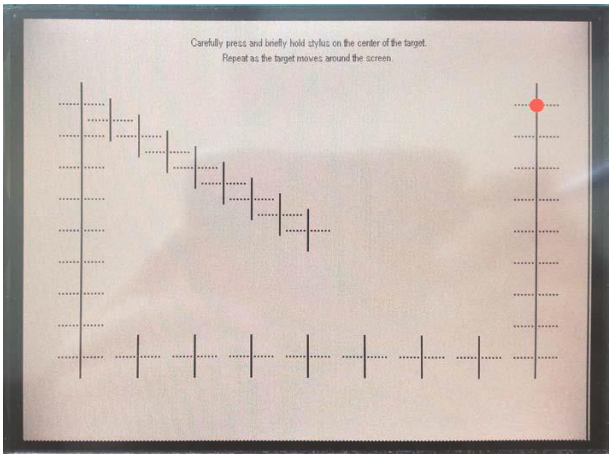
3.



4.



5.



3.2 Terminer l'étalonnage

Après avoir touché le cinquième et dernier point d'étalonnage avec le stylet, le programme vous demandera de toucher le centre de l'écran, pour confirmer et sauver les données d'étalonnage. Si vous ne touchez pas le centre de l'écran dans les 30 secondes, l'étalonnage sera annulé et les données ne seront pas sauvegardées.

4 AURUS-TFT hardware reset

4.1 Intro

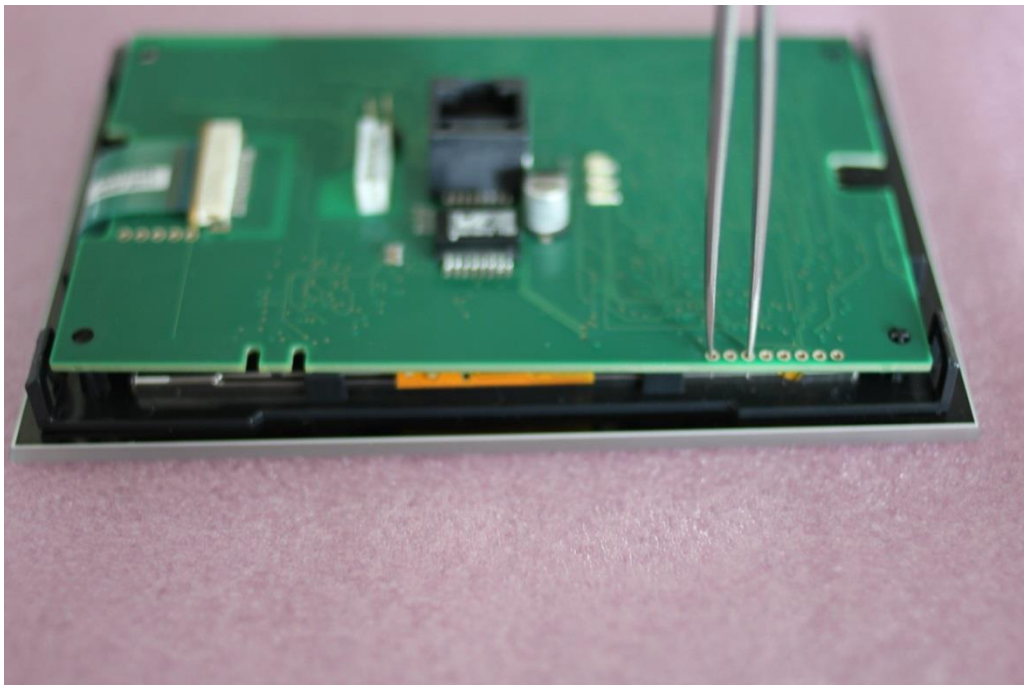
Dans certains cas exceptionnels, il se peut que l'AURUS-TFT soit bloqué sur l'écran de démarrage. Si, après avoir débranché et rebranché le câble AUTOBUS, le problème persiste les instructions ci-dessous permettent de restaurer les réglages usine de l'AURUS-TFT.

Cette procédure s'applique uniquement aux AURUS-TFT ayant un numéro de série supérieur à ***** 0256.

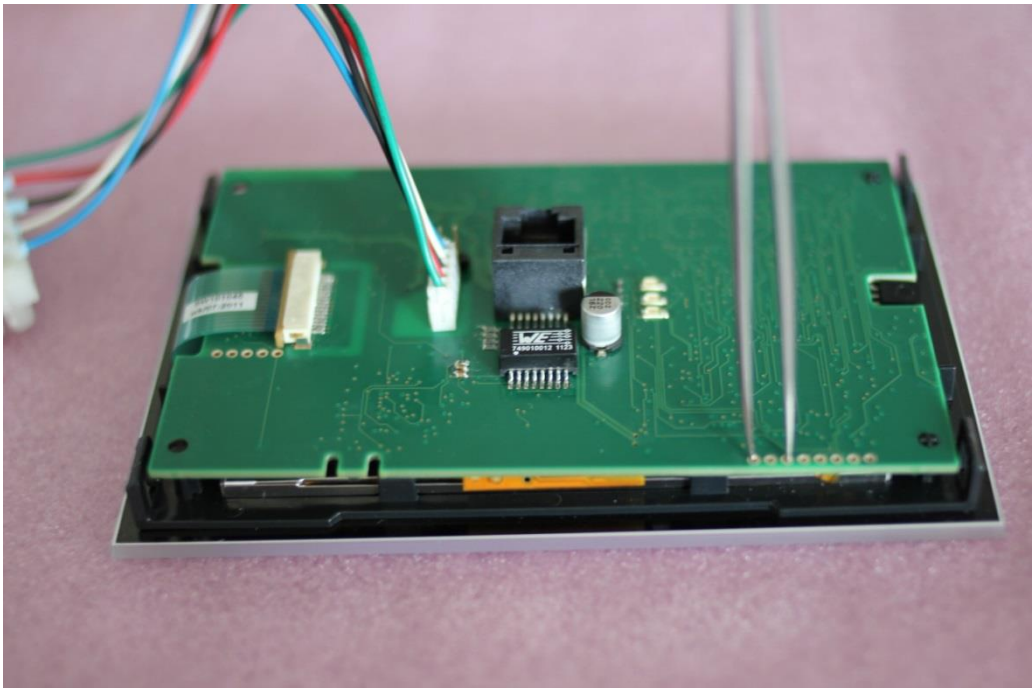
4.2 Comment restaurer les réglages usine d'un AURUS-TFT?

1. Tout d'abord, vérifiez que les quatre derniers chiffres du numéro de série soient plus grands que 0256.
2. Mettez l'AURUS-TFT à l'envers sur une surface douce.
3. Retirez en douceur le cache arrière de l'AURUS-TFT en poussant le clip de l'angle vers le centre avec un tournevis plat, tout en tirant le cache arrière vers le haut. Répétez cette opération pour les quatre coins.

4. Une fois le cache arrière retiré, branchez le premier et le troisième trou à l'aide d'une pince à épiler ou d'un fil, comme indiqué sur l'image ci-dessous.



5. Rebranchez le câble AUTOBUS avec les trous encore connectés.



6. L'AURUS-TFT va maintenant démarrer sur un écran de chargement. Retirez la pince à épiler ou le fil et laissez l'AURUS-TFT poursuivre le processus de mise à niveau via AUTOBUS.

7. Les réglages usine ont été rétablis sur l'AURUS-TFT et il a reçu les dernières mises à jour de l'unité centrale. Si les problèmes persistent, contactez votre distributeur TELETASK.

5 ETUDES DE CAS

5.1 Intégration DoIP – VPN

5.1.1 Introduction

Ce document décrit la manière de mettre en place un réseau domestique pour l'utilisation d'un GUI, GUI + ou iSGUI devant être utilisé à distance.

Pour ce faire, TELETASK conseille d'utiliser une connexion VPN (Virtual Private Network). Les avantages du VPN sont:

- Universel (disponible sur différentes marques)
- Protection contre les accès non autorisés (les données sont cryptées).
- L'interface graphique de configuration est la même que l'utilisation soit locale ou distante.

Le principe du VPN est simple: depuis un emplacement distant, il ajoute (virtuellement) votre ordinateur portable ou votre Smartphone à votre réseau domestique (LAN). Pour cela, vous avez besoin, soit d'une "adresse IP statique", soit d'une adresse "DNS dynamique". Une adresse IP statique est la solution la plus facile et le plus pratique, mais l'adresse DNS dynamique peut être une solution alternative (probablement moins cher). Cela peut varier d'un pays à l'autre.

Pour mettre en place une connexion VPN suivez les étapes suivantes:

- Mettre en place un routeur (à la maison) avec le serveur VPN intégré
- Configurer une connexion VPN sur ce routeur via votre PC ou votre appareil mobile
- Tester la connexion VPN

Mettre en place un routeur VPN demande des compétences TIC et des compétences réseau. Si vous n'êtes pas un professionnel expérimenté, TELETASK vous recommande de consulter votre fournisseur TIC.

5.1.2 DNS Dynamique (DynDNS)

5.1.2.1 Intro

Le DNS dynamique est un service auquel votre routeur VPN envoie régulièrement son adresse IP dynamique (variable) sur un serveur dédié sur internet avec une adresse IP statique (connue et invariable). Ainsi, vous pouvez avoir accès à votre routeur VPN de n'importe où sur Internet.

Il existe plusieurs fournisseurs de ce service. L'un des plus connus est www.DynDNS.org. Dans ce chapitre, nous allons créer un compte DynDNS, et mettre en place le VIGOR 2130 pour travailler avec ce compte.

5.1.2.2 Create a DynDNS account

Créer un compte DynDNS est nécessaire pour utiliser le service DynDNS.

- Ouvrez votre navigateur et allez sur www.DynDNS.org.
- Créer un compte et remplir les informations demandées.
- Une fois que votre compte a été activé, vous pouvez vous connecter.
- Entrez un "Nom d'hôte", sélectionnez le type de service "hôte avec l'adresse IP", cliquez sur le lien "Utiliser des adresses IP détectées automatiquement" et cliquez sur "Créer l'hôte" (il est conseillé d'effectuer cette étape sur le site où l'unité centrale TELETASK est installée).

5.1.3 Plage réseau

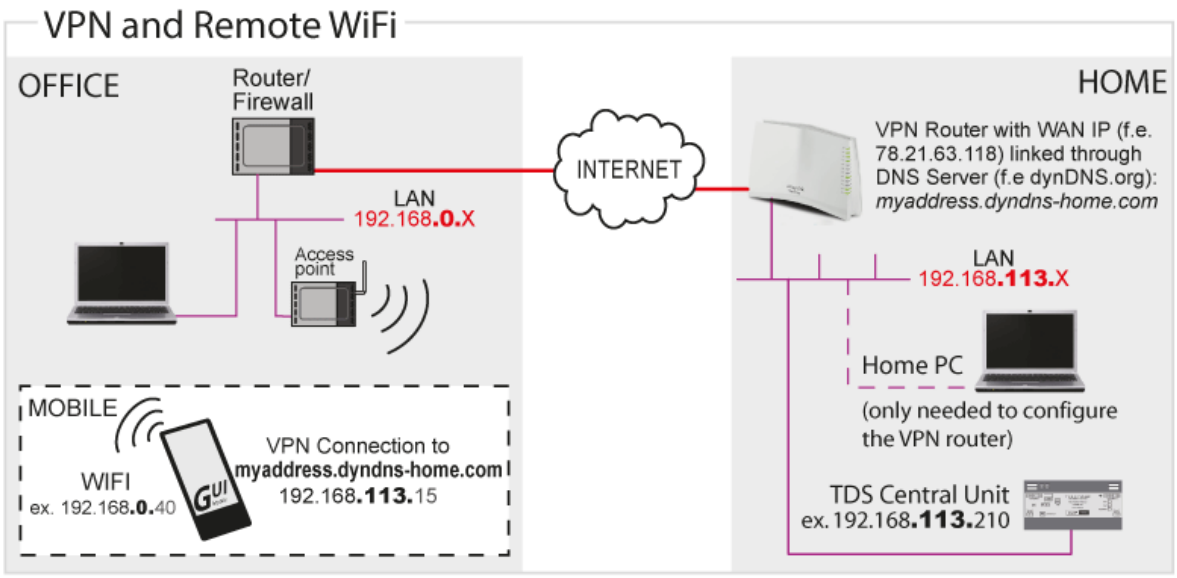
☝ **IMPORTANT: Lorsque vous utilisez une connexion VPN à partir d'un réseau, vous devez vous assurer que le réseau auquel vous vous connectez et le réseau à partir duquel vous vous connectez sont dans un sous-réseau IP différent (dans la plupart des cas, cela signifie que les 3 premiers chiffres sont différents, 192.168.1.1 et 192.168.1.100 sont dans le même sous-réseau 192.168.0.1 est dans un sous-réseau différent. De même pour 10.0.1.1)**

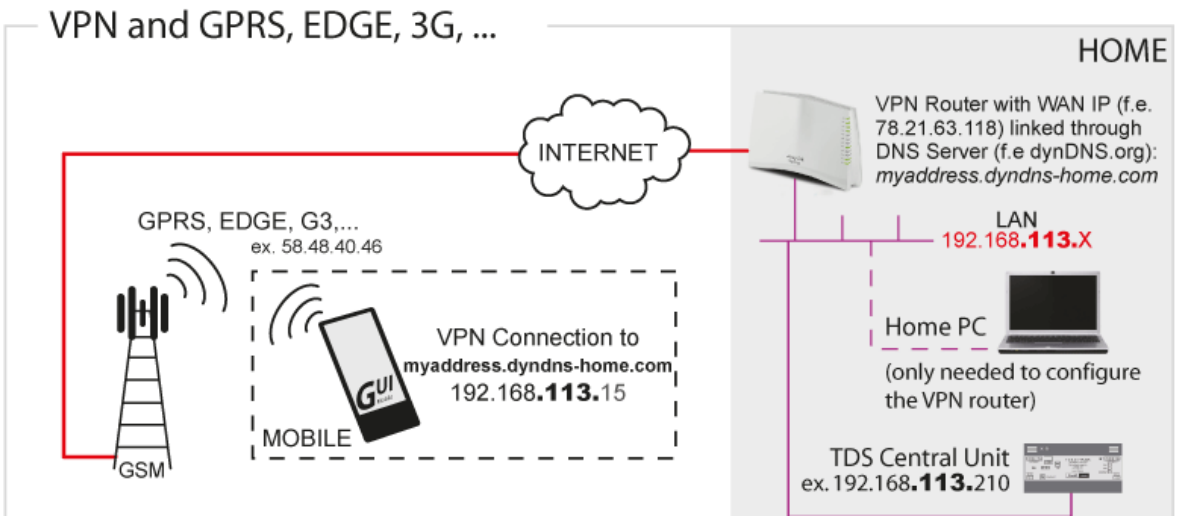
Exemple: Si vous avez configuré votre réseau privé à la plage 192.168.1.xxx et que vous avez iSGUI sur votre Smartphone, vous n'aurez aucun problème lors d'une utilisation à travers une connexion GPRS/EDGE/3G/HSDPA. Si vous avez une maison secondaire (avec une connexion Internet), vous pouvez vous connecter à votre unité centrale TELETASK en utilisant le Wifi de votre maison secondaire, mais vous devez vous assurer que la plage du réseau de votre maison secondaire est différente de 192.168.1.xxx.

La plupart des réseaux résidentiels et des petites entreprises sont dans les plages 192.168.XX, 192.168.1.X et 192.168.0.X étant de loin les plus utilisées. Comme vous n'avez pas besoin de savoir quels réseaux vous connecter à votre réseau à l'aide d'un VPN, il est conseillé de choisir un nombre arbitraire sur la troisième partie de l'adresse IP. Par exemple 192.168.113.X.

☝ **Ne pas utiliser 168 ou 10 comme troisième numéro, car ça pourrait interférer avec le réseau virtuel qui est mis en place via la connexion USB à votre unité centrale TELETASK.**

Schéma type d'une installation (le PC côté maison n'est pas nécessaire. Il est simplement là à titre d'exemple d'un réseau domestique. Le PC est nécessaire temporairement pour la configuration du routeur VPN):





5.1.4 Routeurs VPN

Il ya de nombreux routeurs disponibles sur le marché avec un serveur VPN intégré et il est impossible de fournir les instructions pour chaque type de routeur.

C'est pourquoi, chez TELETASK, nous avons testé certains de ces routeurs afin de vous donner une procédure d'installation détaillée pour (à notre avis) un routeur fiable, facile à installer et pas trop cher : le VIGOR 2130 de DrayTek.

Ce document contient également des informations détaillées pour la mise en place d'un routeur SG300 SnapGear. Ce routeur n'est plus disponible sur le marché, mais pour ceux qui ont déjà acheté cet appareil, l'information n'est pas retirée de ce document.

Pour les autres types de routeurs, les étapes à suivre pour configurer une connexion VPN sont plus ou moins les mêmes, mais si vous décidez d'utiliser un autre type de routeur, veuillez noter:

- Bien que PPTP (un protocole de VPN) soit une norme, la mise en œuvre spécifique peut varier d'une marque à l'autre (routeur et périphérique). Aussi, vérifier si l'appareil (par exemple un PC ou Smartphone) est compatible avec le routeur.

- Il existe différents types de cryptage de données afin de vérifier les spécifications de votre appareil (mobile) lors du choix d'un routeur. Assurez-vous qu'ils sont compatibles.

- TELETASK ne peut pas apporter un support sur tout type de routeur. Si vous avez besoin d'aide, contactez s'il vous plaît votre fournisseur local (pour VIGOR allez sur www.draytek.com).

5.1.5 Installer un VIGOR 2130

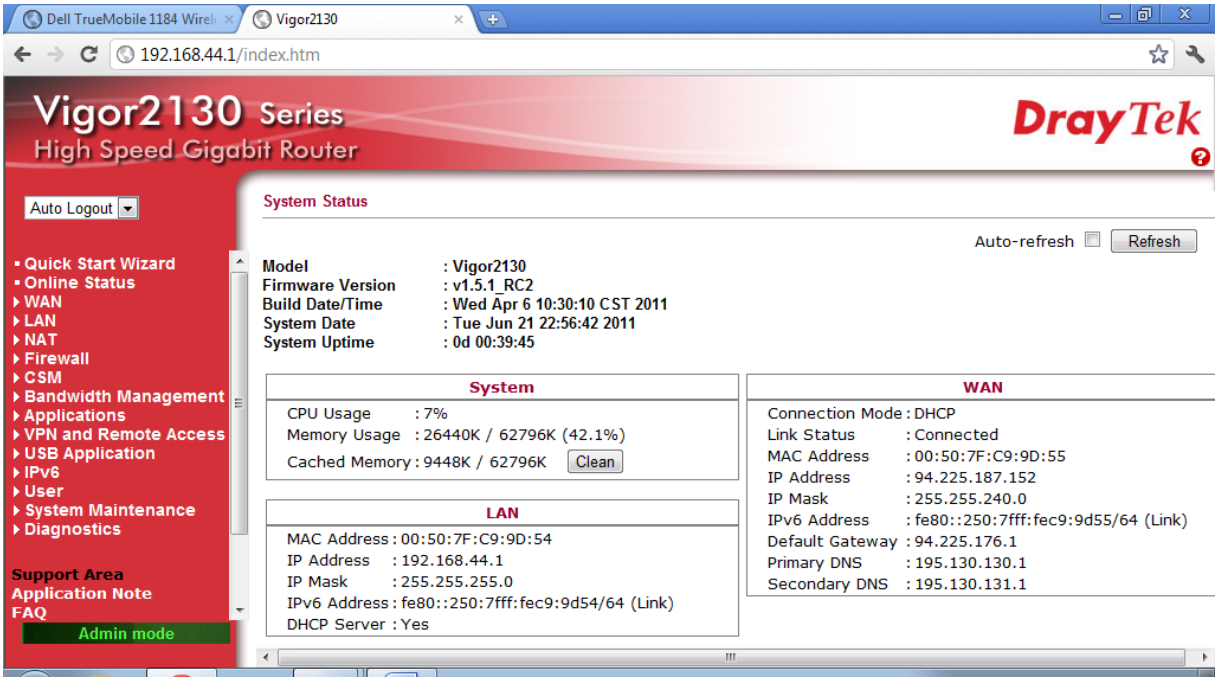
Dans cette partie du document, le terme «VIGOR» se réfère à la série de routeur VIGOR 2130. Pour ce document, le VIGOR 2130 standard est utilisé, mais des versions avec Wifi intégré et d'autres fonctionnalités sont également disponibles.

5.1.5.1 Paramètres généraux

Pour commencer l'installation d'un VIGOR, il suffit de connecter votre ordinateur à un des ports LAN du VIGOR et de connecter le port WAN du routeur à Internet.

L'adresse IP par défaut du VIGOR est 192.168.1.1, lorsque vous entrez cette adresse dans un navigateur, une page de connexion apparaît, l'adresse IP par défaut et mot de passe sont «admin» (sans les guillemets).

Suite à la connexion, vous verrez une page comme celle-ci:

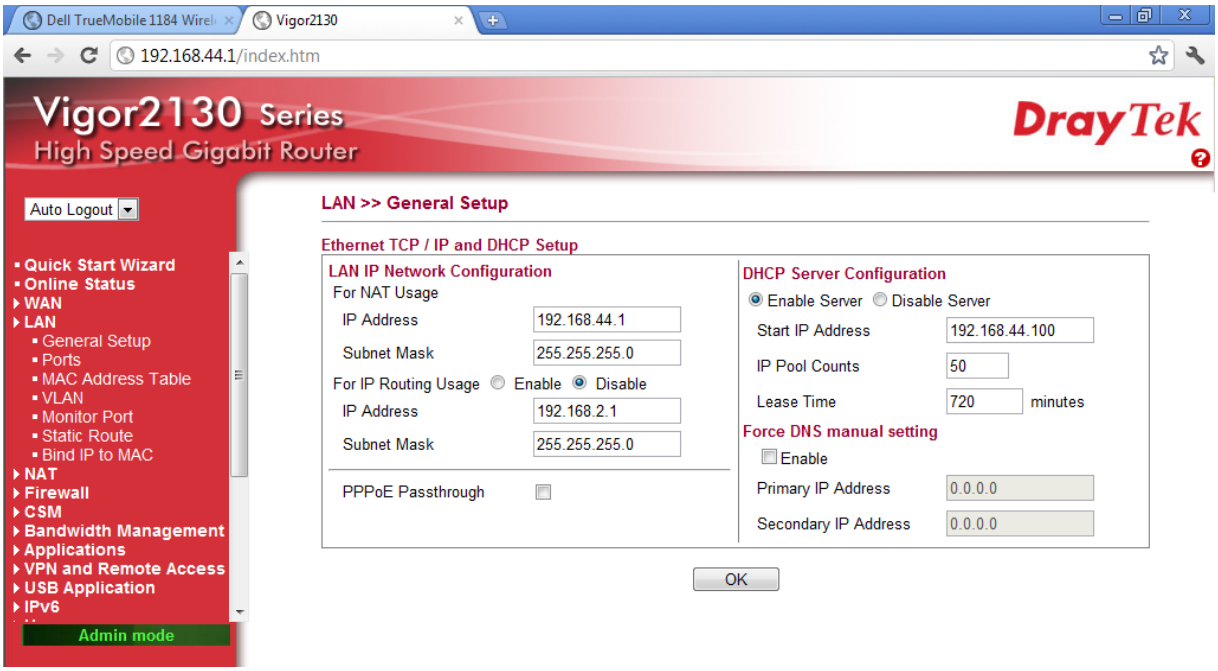


Remarque: la version du firmware du VIGOR pour lequel ce manuel est écrit est v1.5.1_RC2. De légères différences peuvent apparaître si la version de votre VIGOR est différente.

Il est recommandé de commencer avec le «Quick Start Wizard » (élément en haut dans la barre à gauche). Il va vous permettre de régler le fuseau horaire, le nouveau mot de passe administrateur et quelques réglages de base concernant la connexion internet (demandez à votre fournisseur de services Internet pour obtenir les informations correctes). Dans la plupart des cas, les valeurs par défaut sont correctes.

5.1.5.2 Paramètres LAN

Comme indiqué précédemment, la plage réseau de votre réseau est importante pour les VPN. Pour modifier la plage du réseau, cliquez sur «LAN», «Configuration générale»

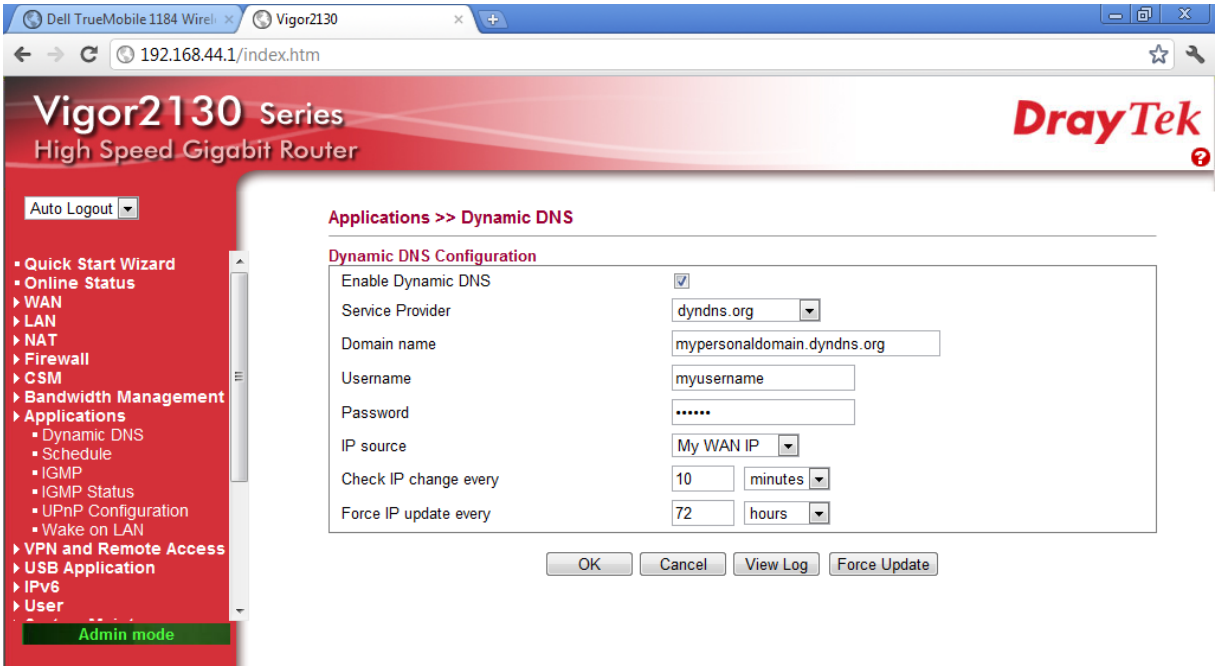


Dans la «Configuration du réseau IP LAN», modifier le troisième numéro de l'adresse IP selon votre souhait. Vous devez également modifier «l'adresse de début» dans la «Configuration du serveur DHCP» de sorte qu'il se trouve dans la même plage réseau.

Remarque: l'adresse de début associée avec le «IP Pool Counts», déterminer une plage d'adresses IP pouvant être attribuées par le routeur aux ordinateurs qui sont connectés au réseau (dans l'exemple, il s'agit des adresses 192.168.44.100 - 192.168.44.150). Il est donc important que vous ne donniez pas une de ces adresses en mode statique à un périphérique tel qu'une centrale TELETASK DoIP, une caméra IP, une imprimante réseau, un disque dur réseau, ...

5.1.5.3 Paramètres DNS dynamiques

Pour configurer DynDNS sur le VIGO, cliquez sur «Applications», «DNS Dynamique». Vous verrez une page comme celle-ci:



- Cochez la case «Activer DNS dynamique»
- Sélectionnez le fournisseur de service (dans cet exemple dyndns.org)
- Entrez le nom de domaine que vous avez enregistré chez le fournisseur de services (dans cet exemple, mypersonaldomain.dyndns.org)
- Entrez le nom d'utilisateur et le mot de passe utilisés pour l'enregistrement DynDNS chez le fournisseur de service.
- Sélectionnez le bon réglage pour l'adresse IP source: «Mon IP WAN» dans le cas où votre VIGOR est directement connecté à Internet, «Mon IP Internet» dans le cas où il y a un modem-routeur câble/ADSL de votre fournisseur d'accès entre le VIGOR et Internet (Voir la remarque ci-dessous).
- Les autres paramètres sont normalement corrects.

Remarque: Dans le cas où vous avez un modem-routeur câble/ADSL entre votre VIGOR et Internet, vous devez réaliser des réglages complémentaires pour le faire fonctionner. Dans ce cas, l'adresse IP WAN de votre VIGOR sera une «adresse IP privée» (dans les plages 10.xxx, 172.16.xx à 172.31.xx ou 192.168.xx). Si le VIGOR modifiait cette adresse IP (ex: 192.168.1.x) avec une adresse IP dynamique fourni par votre modem-routeur, cela ne fonctionnerait pas car il s'agit d'une «adresse IP privée». Pour résoudre ce problème, vous devez configurer le VIGOR pour qu'il utilise son «adresse IP internet», et non son «adresse IP WAN» locale.
Pour qu'il soit possible de se connecter à votre routeur VPN VIGOR depuis Internet, vous devez activer le routage de port sur votre modem-routeur câble/ADSL. Transférer le port 1723 à l'adresse IP WAN de votre routeur VPN VIGOR. Il est également conseillé de définir en statique l'adresse IP WAN de votre routeur VPN VIGOR. (Par exemple 192.1.0.2). Pour plus de détails sur la façon de configurer la redirection de port sur votre modem-routeur câble/ADSL, contactez votre fournisseur d'accès Internet.

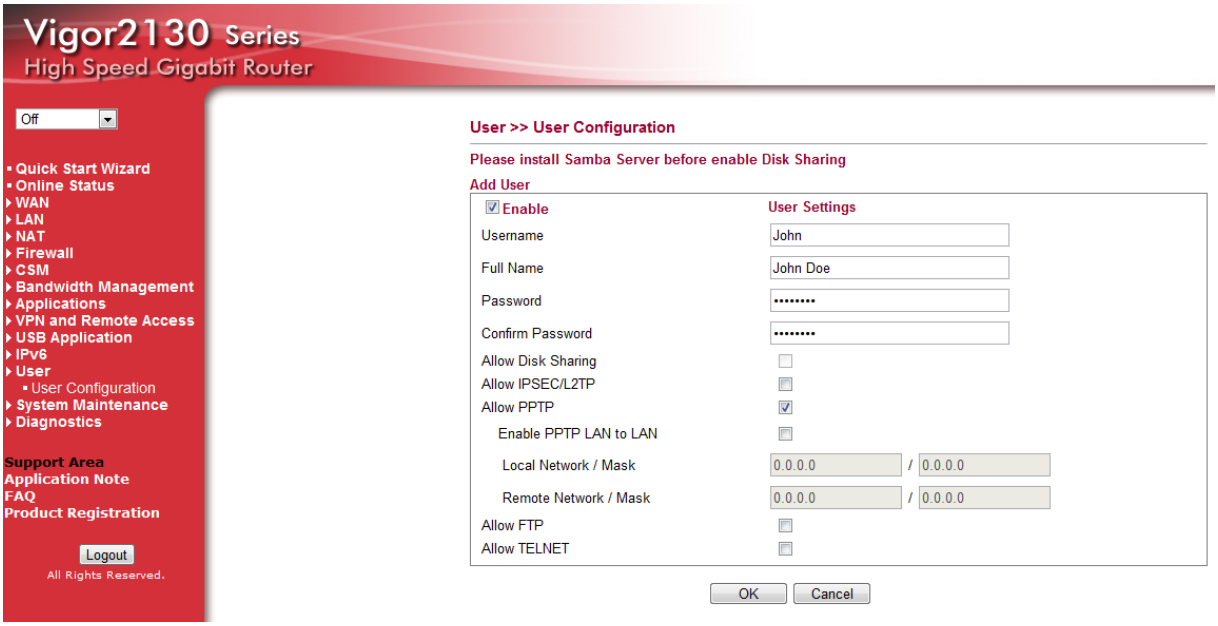
REMARQUE IMPORTANTE: C'est différent du routage de port directement vers l'unité centrale! Vous utilisez toujours une connexion VPN sécurisée et vous utilisez uniquement le routage de port pour passer directement d'Internet à votre routeur VPN VIGOR.

5.1.5.4 Ajout d'utilisateurs

Avant que nous puissions mettre en place le serveur VPN, des utilisateurs doivent être créés. Chaque utilisateur dispose de ses propres nom d'utilisateur et mot de passe pour se connecter au serveur VPN (et peut avoir des privilèges différents).

Pour ajouter un utilisateur, cliquez sur «User», «Configuration utilisateur»

Vous verrez cet écran:



- Cochez la case «Enable User Settings»

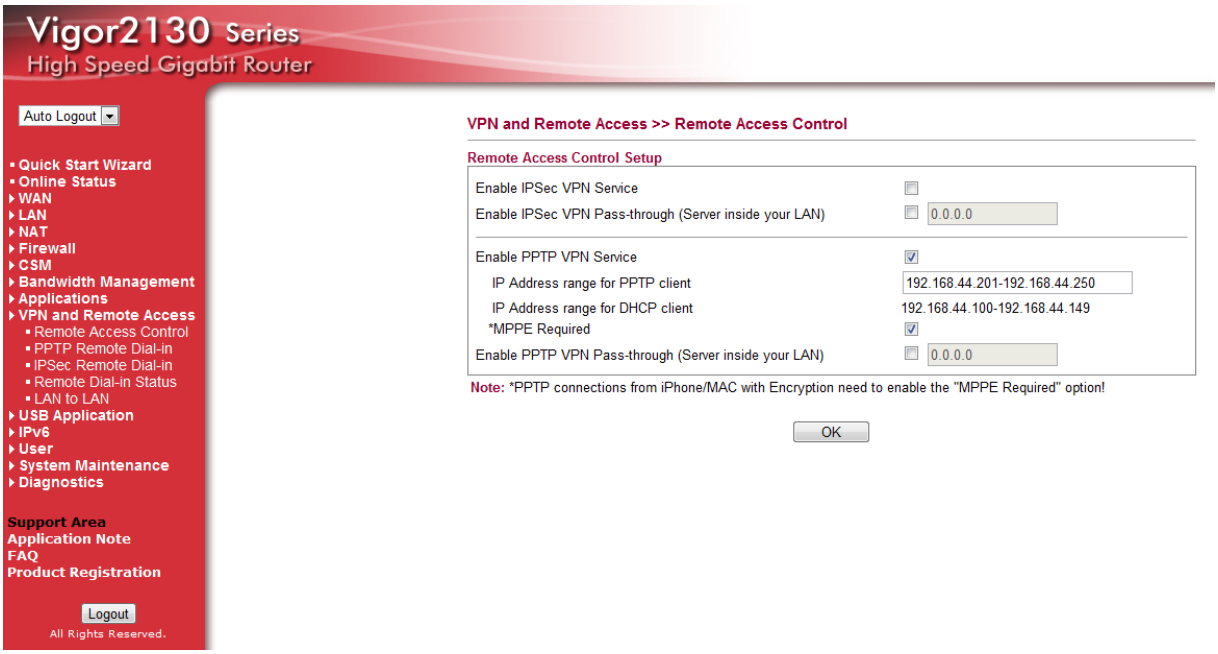
Remplissez:

- Nom d'utilisateur: Un nom pour l'utilisateur qui va se connecter au VPN (tous les utilisateurs doivent avoir un nom unique)
- Nom complet: le nom complet de l'utilisateur (uniquement pour simplifier la gestion des utilisateurs)
- Mot de passe: le mot de passe de l'utilisateur
- Cochez la case "PPTP Autorisé"
- Cliquez sur OK

Répétez ces étapes pour tous les utilisateurs.

5.1.5.5 Configuration du serveur VPN

Maintenant, nous sommes prêts à mettre en place le serveur VPN lui-même, cliquez sur «VPN et accès à distance», «Contrôle d'accès à distance».



Réglez les paramètres suivants:

- Décochez la case “Activer service VPN IPSec”
- Cochez la case “Activer service VPN PPTP”
- Si vous prévoyez d'utiliser des appareils Apple (iPhone / iPod touch / iPad ou Mac) Cochez “* MPPE required”

☝ **Remarque: comme un serveur DHCP, le serveur VPN a également un pool d'adresses IP à partir desquelles il donne une adresse IP à un dispositif qui établit une connexion VPN. Assurez-vous donc qu'aucun des périphériques qui sont physiquement sur le réseau n’a une adresse IP statique dans la «plage d'adresses IP pour client PPTP»**

Cliquez sur «OK» pour enregistrer les paramètres, votre VIGOR est maintenant prêt à accepter les connexions VPN entrantes.

5.1.6 VPN au moyen du routeur VPN SnapGear SG300 (plus disponible)

Accéder à distance à une unité centrale DoIP en toute sécurité.

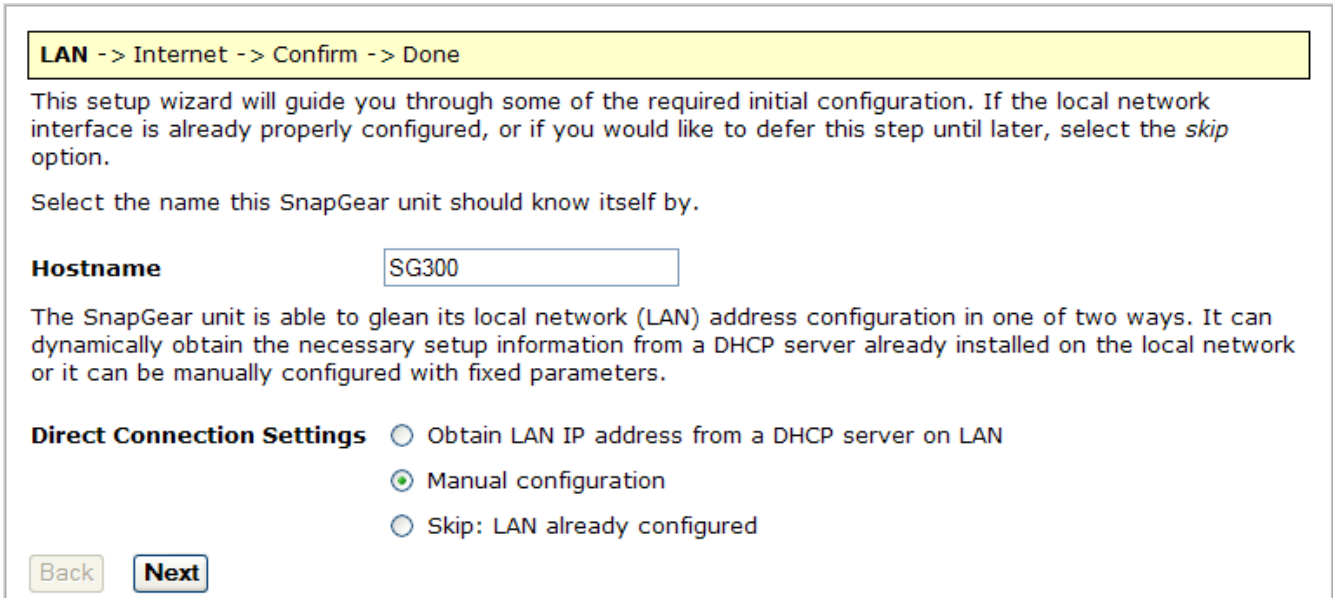
Dès que vous avez relié l'ordinateur portable au côté LAN du routeur SnapGear, ouvrez le navigateur et surfez vers le SG300. Vous introduisez le mot de passé-clé (celui-ci n'est pas configuré d'office). Notez que la connexion LAN par défaut du SG300 est configurée d'office sur 192.168.0.1.

La façon la plus rapide d'installer votre router/firewall est l'emploi du 'Quick Setup Wizard'.

Les écrans suivants apparaîtront sur votre PC de configuration:

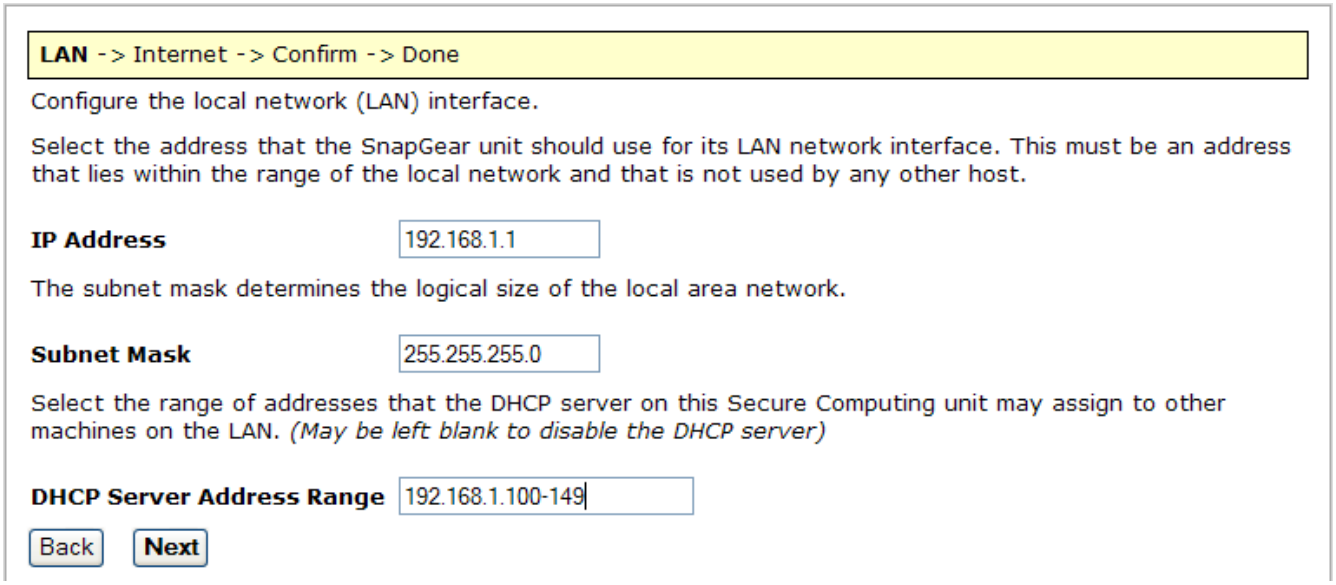
- Quick Setup
- Manual LAN Configuration
- ISP connection

5.1.6.1.1 Quick Setup



Dans la plupart des cas, 'Manual configuration' sera la sélection correcte, puisque SG300 sera le seul appareil qui fonctionnera comme serveur DHCP.

5.1.6.1.2 Configuration LAN manuelle

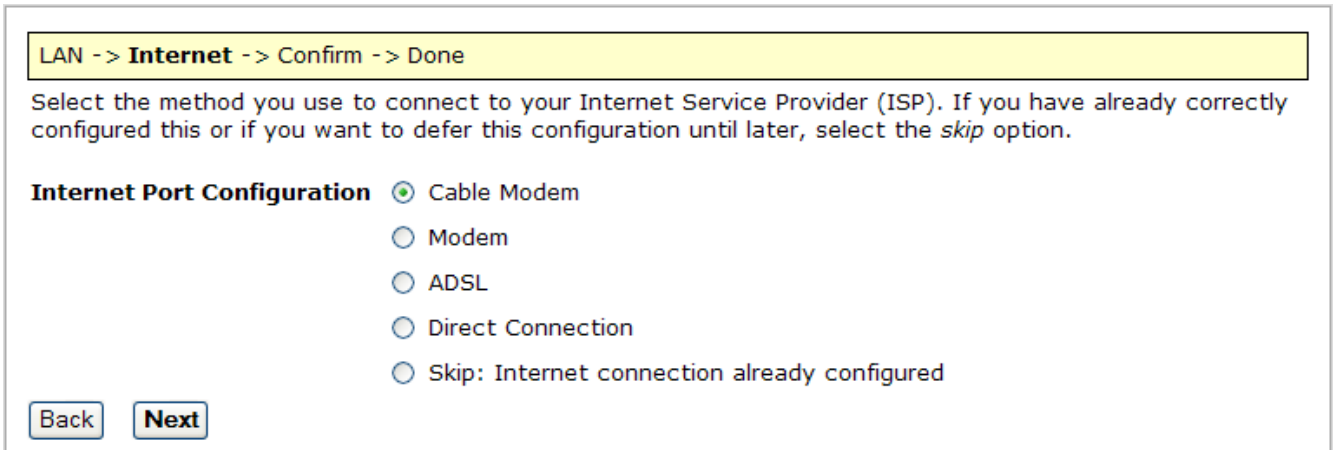


Dans ce cas, nous supposons que nous configurerons le réseau privé dans la série 192.168.1.xxx et nous choisissons 192.168.1.1 pour l'adresse LAN IP du SG300.

IMPORTANT: lors de l'usage d'une connexion VPN depuis le réseau, veillez à ce que le réseau sur lequel vous vous connectez et le réseau depuis lequel vous vous connectez aient un subnet IP différent. Dans la plupart des cas, cela signifie que les 3 premiers chiffres ne sont pas les mêmes. (192.168.1.1 et 192.168.1.100 appartiennent au même subnet, tandis que 192.168.**0**.1 est dans un autre subnet, de même que **10**.**0**.1.1).

Exemple: si vous avez configuré votre réseau privé dans la série 192.168.1.xxx et vous avez un GUI sur votre Smartphone, vous n'aurez pas de problèmes pour connecter via une connexion GPRS/EDGE/3G. Lorsque vous avez une maison de vacances qui dispose d'une connexion Internet, vous pouvez relier celle-ci à votre unité centrale par l'intermédiaire du LAN de votre maison de vacances, mais il faut que la série du réseau de votre maison de vacances soit différente de 192.168.1.xxx.

5.1.6.1.3 Connexion ISP



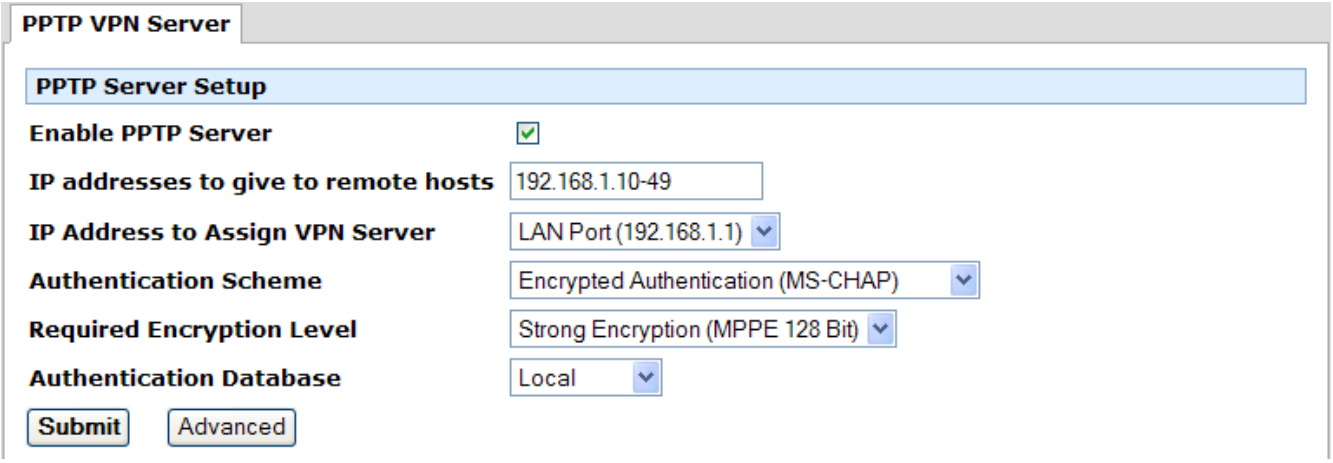
Ici vous devez choisir la connexion correcte avec Internet. Si vous ne la connaissez pas, contactez votre Internet Service Provider (dans la plupart des cas, l'option 'Direct Connection' est correcte).

Aprés avoir achevé le wizard, vous devez modifier l'adresse IP dans votre navigateur sur 192.168.1.1 pour poursuivre la configuration.

5.1.6.1.4 Configuration VPN

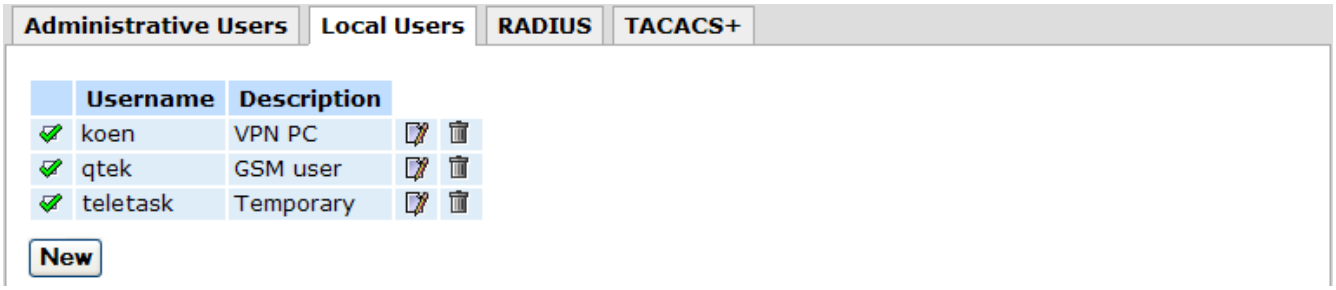
Dans l'étape précédente, vous avez configuré le réseau basique. Nous pouvons entamer maintenant la configuration du serveur VPN en question.

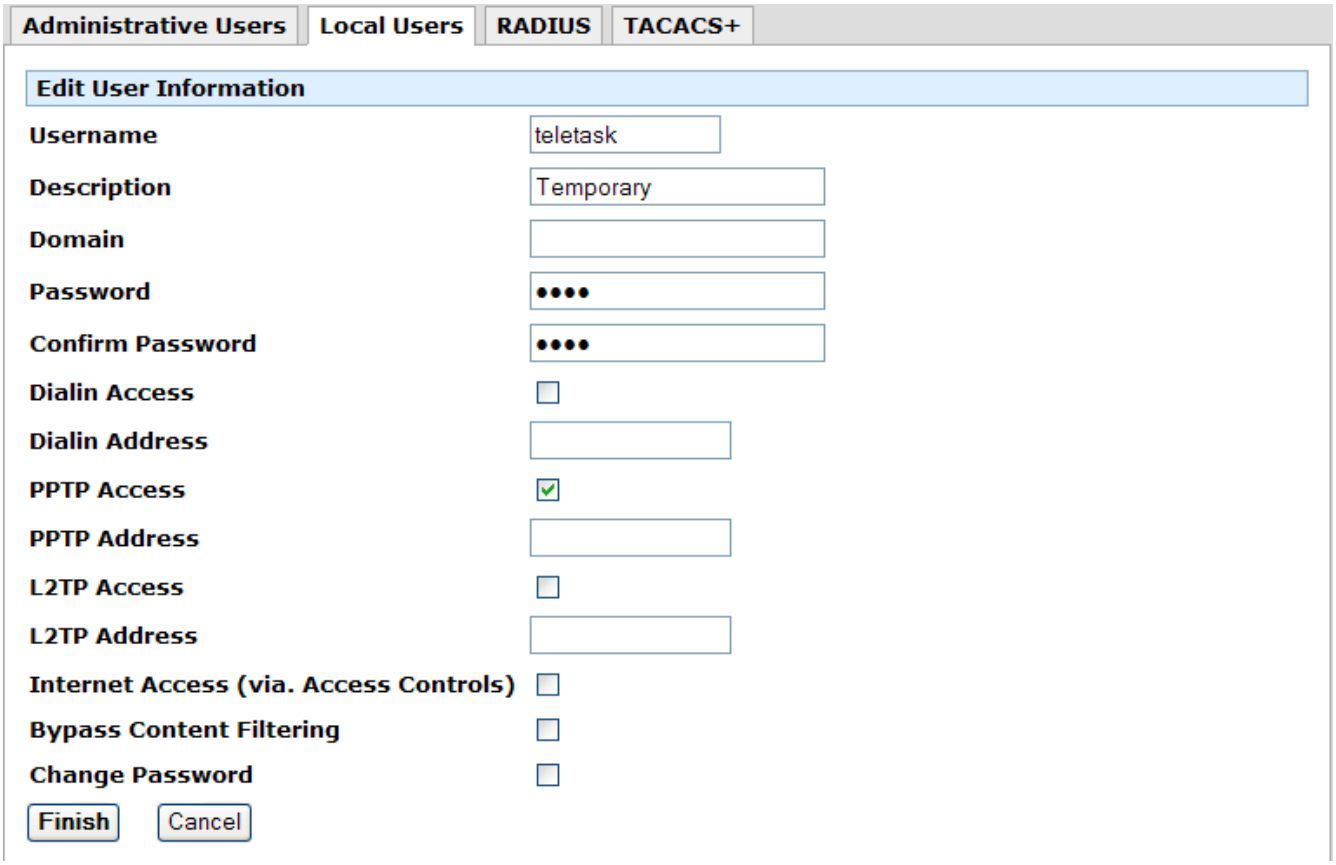
- Cliquez en bas à gauche sur "VPN on PPTP VPN Server"
- Contrôlez l'option "Enable PPTP Server"
- Sélectionnez le "Authentication Scheme" "Encrypted Authentication (MS-CHAP), ce qui signifie que les appareils qui utilisent MS-CHAP (ou MS-CHAP v2), peuvent être connectés. Au cas où seuls des ordinateurs fonctionnant sous Windows Vista et/ou des Smartphones qui fonctionnent avec Windows mobile V6 sont en service, vous pouvez choisir ici l'option "Encrypted Authentication (MS-CHAP v2)"
- Ne modifiez pas le reste des réglages et cliquez sur 'Submit'.



- Cliquez à gauche sous "System on User" et choisissez l'onglet 'Local Users'.
- Cliquez 'New', entrez nom, description et mot de passe

- Vérifiez que l'option "PPTP access" est cochée.
- Cliquez 'Finish'.





5.1.6.2 DNS Dynamique

5.1.6.2.1 Introduction

Dynamic DNS est un service qui permet à votre routeur d'envoyer son adresse IP (dynamique, changeante) à un serveur fixe (à adresse IP fixe) sur Internet, pour que vous puissiez accéder à votre routeur VPN depuis n'importe où sur Internet, sans devoir disposer d'une adresse IP statique (onéreuse).

Il y a plusieurs fournisseurs donnant accès à ce service. Un des mieux connus est www.DynDNS.org. Dans ce chapitre nous instaurerons un compte DynDNS gratuit et installerons le SG300 pour travailler via ce compte.

5.1.6.2.2 Créer un compte DynDNS dynamique

Créer un compte DNS dynamique est indispensable pour pouvoir se servir du service DynDNS. Avec un compte DynDNS vous pouvez créer 1 adresse DynDNS gratuite.

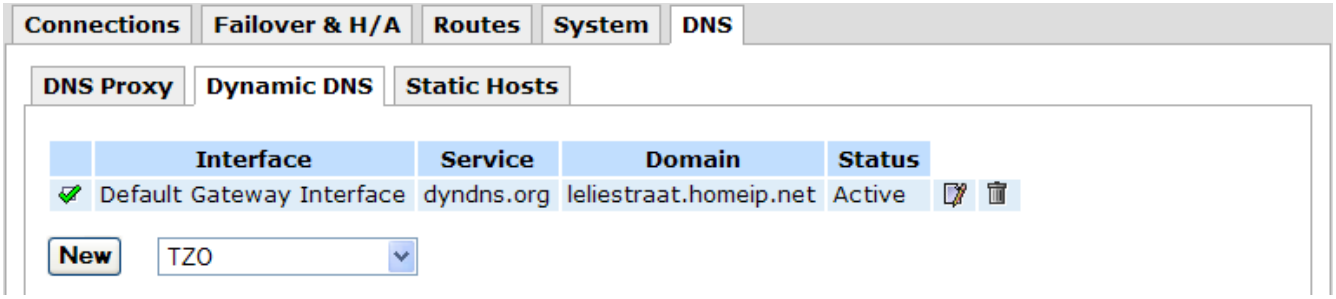
Ouvrez un navigateur et surfez vers www.DynDNS.org.

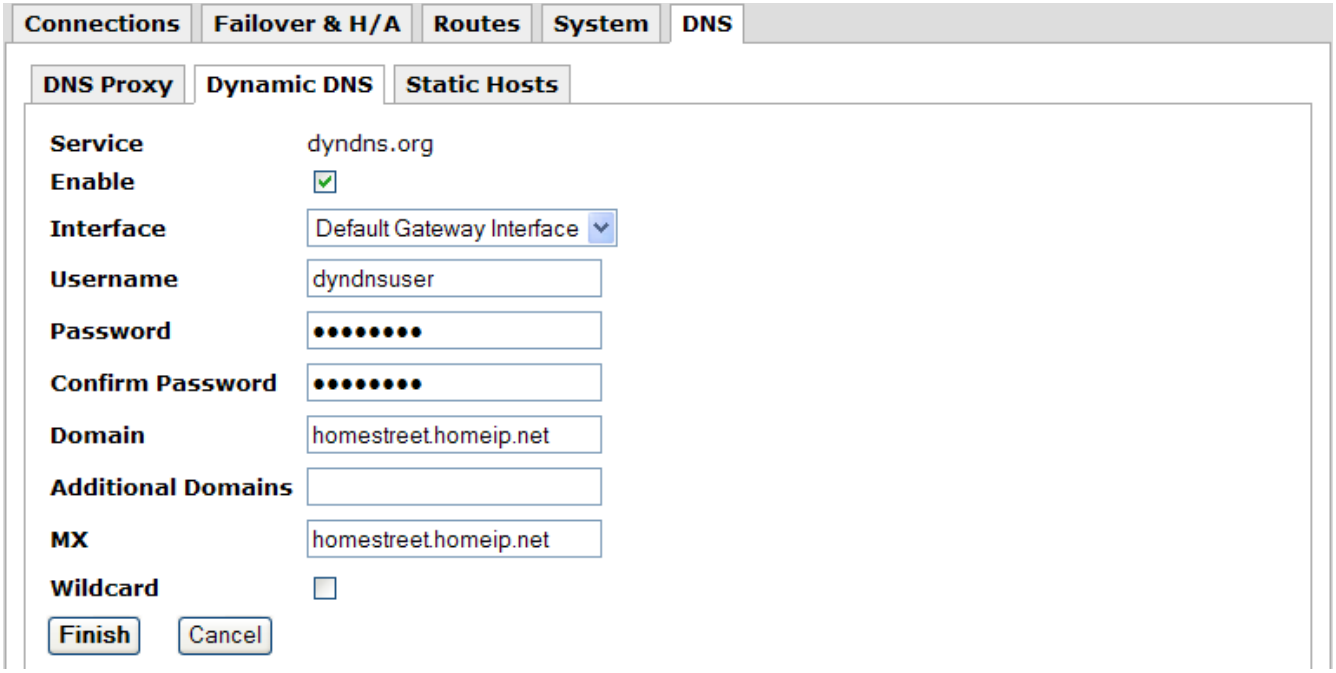
- Cliquez sur le lien "Create account" sur cette page et introduisez les informations demandées.
- Vous recevrez un message de confirmation avec "Account information confirmation", ouvrez-le et cliquez sur le lien de confirmation (si vous ne recevez pas le message, contrôlez votre fichier Junk Mail)
- Une fois votre compte activé, vous pouvez entrer. Cliquez sur "Services", "Dynamic DNS", "Get Started".
- Introduisez un "Hostname", sélectionnez le type de service "Host with IP address", cliquez sur le lien "Use auto detected IP address", et cliquez sur "Create Host" (il est recommandé d'effectuer ces étapes sur la location où l'unité centrale a été installée).

5.1.6.2.3 Installer un DynDNS dans le SG300

- Cliquez à gauche sur Network Setup sous NETWORK SETUP, sélectionnez l'onglet DNS et ensuite l'onglet page Dynamic DNS .
- Sélectionnez "dyndns.org" dans la liste et cliquez “New”
- Cochez l'option "Enable"

- Introduisez votre nom d'utilisateur et mot de passe DynDNS et Domain (dans l'exemple ci-dessous nous avons un compte DynDNS avec nom d'utilisateur 'dyndnsuser' et nom d'hôte 'homestreet.homeip.net')
- Cliquez sur "Finish"



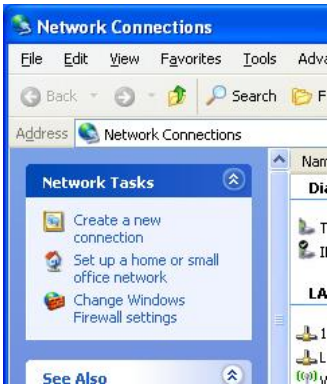


5.1.7 Installer une connexion client VPN

Le routeur étant installé et le Dynamic DNS étant activé, nous pouvons maintenant installer à distance une connexion VPN. Dans la présente étape, nous allons ouvrir une connexion VPN avec Windows XP (pour Windows Vista, les étapes à parcourir sont les mêmes). Si vous désirez ouvrir une connexion VPN à partir d'un appareil Windows Mobile, nous proposons de créer d'abord une connexion PC (pour tester le fonctionnement du serveur VPN) et seulement ensuite ouvrir la connexion depuis votre appareil Windows Mobile. Si vous avez besoin d'aide pour ouvrir une connexion VPN depuis un appareil mobile, consultez le manuel d'installation de 'GUI for Smartphones'.

Ouvrir une connexion avec Windows XP. Suivez les étapes suivantes:

- Allez sur Start > Configuration panel > Network connections.

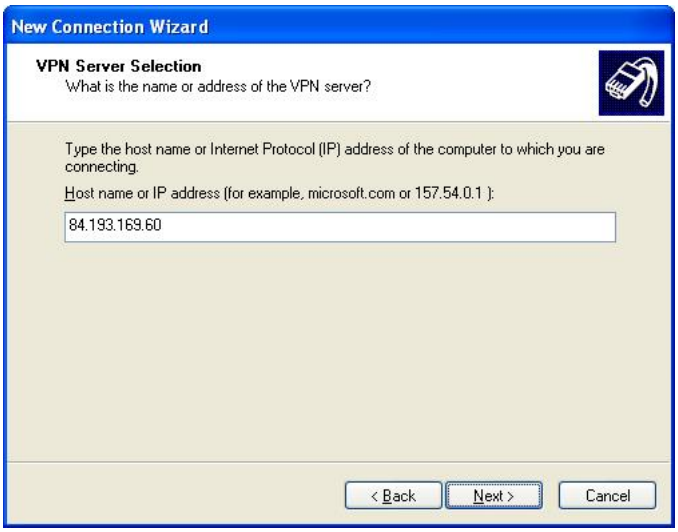


- Cliquez sur 'Create a new connection'.

- Sélectionnez: 'Connect to the network at my workplace' et cliquez "Next".

- Sélectionnez 'Virtual Private Network connection' et cliquez "Next"

- Donnez-la un nom pour que vous sachiez qu'il s'agit de la connexion avec votre maison (client) et cliquez "Next".



- Introduisez comme nom d'hôte ou adresse IP, le nom d'hôte que vous avez configuré sur le DynDNS ('homestreet.homeip.net' dans l'exemple précité). Si vous avez une adresse IP statique, introduisez maintenant votre adresse IP.
- Cliquez "Next", et ensuite "Finish" dans l'écran suivant. L'ordinateur portable peut maintenant être relié à votre "home network".

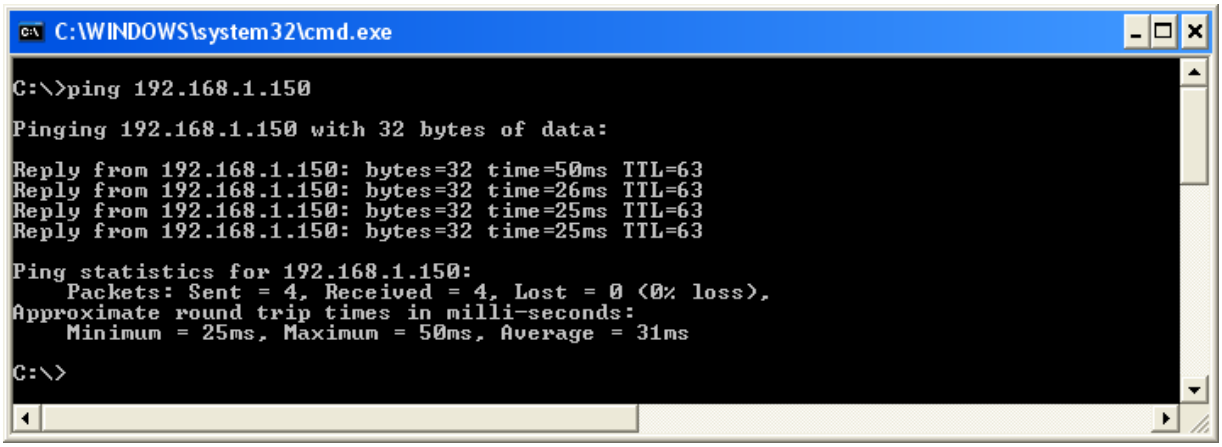
5.1.8 Testez la connexion VPN

Dans ce chapitre, nous allons d'abord tester la connexion et ensuite expliquer comment vous pouvez utiliser le TELETASK GUI via une connexion VPN.

5.1.8.1 Tester la connexion VPN

- Ouvrez votre connexion VPN par "Start", "Connect to".
- Introduisez votre nom d'utilisateur et mot de passe (ceux que vous avez créés dans le routeur – voir chapitre "Configuration VPN").
- Cliquez "Connect"

- Pour tester la connexion, nous vous proposons d'envoyer un ping à l'adresse IP de votre installation locale (p. ex. votre MICROS+). Si tout a été installé correctement, cela devrait réussir.



5.1.8.2 Usage du TELETASK GUI via une connexion VPN

5.1.8.3

Comme annoncé dans l'introduction, un des avantages d'une connexion VPN est que la configuration pour usage local et celle pour usage à distance sont exactement identiques. Dès lors, la même adresse IP doit être introduite dans les caractéristiques du GUI (ou GUI for Smartphones), ainsi que le même numéro de port, tout comme pour l'usage local du GUI.

Vous pouvez donc faire fonctionner votre GUI depuis votre portable à la maison, vous prenez votre portable avec vous au bureau, en vacances et vous pouvez faire fonctionner votre GUI à distance de la même façon comme si vous étiez à la maison. N'oubliez pas de cliquer sur "Connect to" et de vous relier à votre réseau local avant de démarrer le GUI à distance. Pour le GUI for Smartphones, c'est encore plus simple: il ouvre notamment la connexion VPN automatiquement si besoin est. Vous trouverez de plus amples informations dans les manuels de GUI et GUI for Smartphones.