



ConnecSenS

Configuration d'une passerelle LoRaWAN sur le réseau ConnecSenS

Modèles Kerlink :

- IoT Station 868



Historique des révisions

Rév.	Date	Modifications
2.0	Mai 2022	Mise à jour avec historique révisions (LR).
2.1	Aout 2022	Ajouts de notes en bas de documents concernant les problèmes VPN (LR)

Table des matières

I. Préparation du matériel.....	4
1) Matériel nécessaire.....	4
2) Récupération des ressources.....	5
a) Méthode 1 : Via la forge	5
b) Méthode 2 : Via GitHub Desktop.....	5
c) Méthode 3 : Via le wiki de Kerlink.....	6
II. Installation / Mise à jour des ressources	8
1) Mise à jour du firmware	8
2) Installation du Packet Forwarder.....	9
III. Configuration des ressources.....	10
1) Connexion à la passerelle	10
a.1) Méthode 1 : Connexion en série.....	10
a.2) Méthode 2 : Connexion SSH	12
b) Configuration du réseau GSM.....	13
c) Configuration du Packet Forwarder	14
d) Configuration du VPN	16
Annexes.....	18
1) Tutoriel : Branchement physique de la passerelle en vue de mise sous tension	18
2) Mise en route de la passerelle.....	19
3) Tutoriel : Changer l'adresse IP de l'interface réseau Ethernet.....	22
4) Monitoring VPN et autres concernant VPN.....	25
VPN.....	25
VPN.....	26

ATTENTION : Ce document contient des adresses IP ainsi que des identifiants de connexion CONFIDENTIELS. Merci de ne pas le rendre public et de contrôler son audience afin de ne pas compromettre la sécurité de l'infrastructure.

I. Préparation du matériel

1) Matériel nécessaire

Requis :

- 1x Passerelle Kerlink LoRa IoT Station 868
- 1x Wirgrid Debug Board v1
- 1x Câble RJ45
- 1x Clé USB vide, formatée en FAT32
- 1x PC (équipé d'un terminal serial / SSH)
- Accès à la forge du projet I-SITE Cap 20-25 / ConneCSenS

Conseillé :

- MobaXTerm (terminal serial / SSH utilisé ci-dessous)
- Microsoft Windows 10 (utilisé ci-dessous)
- Accès au wiki de Kerlink

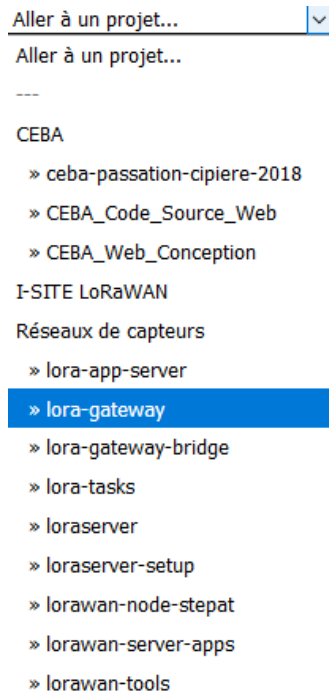
2) Récupération des ressources

a) Méthode 1 : Via la forge

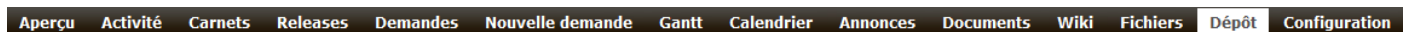
URL de la forge : <http://forge.clermont-universite.fr/login>

Identifiants : Vos identifiants ENT / Identifiants d'un compte invité¹

1 – Dans l'onglet « Aller à un projet » en haut à droite de la page, cliquez sur « lora-gateway ». Cet onglet contient toutes les ressources liées aux différents modèles de passerelles utilisés dans le cadre de l'I-SITE et de ConnecSenS.



2 – Dans la liste d'onglets en haut de page, cliquez sur « Dépôt »



3 – Dans la liste des dossiers à gauche, cliquez sur le « Kerlink », puis téléchargez les 3 packs en .zip (Pack Firmware Kerlink 3.3, Openvpn et SPF Kerlink)

b) Méthode 2 : Via GitHub Desktop

Il est possible de télécharger directement le dépôt de fichiers de la forge sur votre ordinateur grâce au logiciel « GitHub Desktop » disponible pour Windows, téléchargeable ici :

<https://desktop.github.com/>

Dépôt à cloner : <https://forge.clermont-universite.fr/git/lora-gateway>

Cette méthode vous permettra de disposer localement des fichiers plutôt que de les télécharger un par un, dans votre répertoire C:/User/Documents/GitHub/lora-gateway/.

¹ Si vous n'avez pas accès au projet « I-SITE LoRaWAN » sur la forge, merci de contacter Gil DE SOUSA (gil.de-sousa@irstea.fr)

c) Méthode 3 : Via le wiki de Kerlink

ATTENTION : Vous aurez tout de même besoin de récupérer le pack « Openvpn » avec l'une des méthodes précédentes, car il contient des clés uniques qui sont fournies par le Mésocentre, non par Kerlink. Cette méthode a avant tout pour but d'apprendre à récupérer les ressources nécessaires pour la mise à jour de la passerelle vers un firmware / un Packet Forwarder plus récent.

URL du wiki de Kerlink : <http://wikikerlink.fr/lora-station/doku.php>

Identifiants :

Username : cnrs-clermont

Password : Xft12PeWou

1 – Une fois loggé sur le wiki, dans la colonne de gauche, cliquez sur « Ressources ».

2 – Dans la section « 2.2. Firmware Links », cliquez sur la version qui vous intéresse.

3 – Dans la nouvelle page affichée, dans la section « 3.2. Download », téléchargez les fichiers « firmware (USB upgrade) et produsb file (USB upgrade). (Exemple ci-dessous pris avec la version 3.3, mais ce schéma est aussi viable avec la version 3.6 actuellement sortie.)

3.2. Download




- firmware (USB upgrade):  [usbflashdrive_wirmav2_wirnet_v3.3.zip](#)
- produsb file (USB upgrade):  [produsb_wirnet_v3.3.zip](#)
- firmware (network upgrade from v3.1 to v3.3 only):  [fwupgrade_wirmav2_wirnet_v3.3.tar.gz](#)
- script to create a custom network upgrade dota from v2.x to v3.x:  [create_dota_2x_wirnet3.sh](#)
- script to create a custom network upgrade dota from v3.1 to v3.3:  [create_fwupgrade.sh](#)

4 – Retournez en haut de la page, puis cliquez à nouveau sur « Ressources » dans le menu de gauche.

5 – Dans la section « 3.2.2. Semtech Packet Forwarder », sélectionnez la version qui vous intéresse.²

6 – Dans la nouvelle page affichée, dans la section « 3. Downloads », téléchargez le fichier « Dota Installation Package »

3. Downloads

- DOTA installation package:  [dota_spf_3.1.0-klk16_4.1.3-klk8_wirnet.tar.gz](#)
 - Md5sum: [f6e87530716a535291f342d2456b1aaf](#)
- Source files:  [spf-3.1.0-klk16.tar](#)
 - Md5sum: [ab5988429013c968f1d4eb5ce7a9da6a](#)
- Readme file:  [readme_3.1.txt](#)
- Packet forwarder protocol v1.3:  [Protocol.txt](#)
- JSON configuration file examples are available in the DOTA installation package.

² Le Semtech Packet Forwarder, abrégé SPF, est un outil standard présent sur l'écrasante majorité des passerelles LoRaWAN. L'autre version proposée, le « Kerlink Common Packet Forwarder », fonctionne aussi.

7 – Une troisième fois, retournez sur la page « Resources » accessible via le lien en haut à gauche de la page.

8 – Dans la section « 3.3. HAL », cliquez sur la version la plus récente (actuellement, Semtech HAL v4.1.3-klk8 (May 2018)).

9 – Dans la section « 3. Downloads », téléchargez le fichier « DOTA to upgrade the HAL ».

3. Downloads

- DOTA to upgrade the HAL: [custo_libloragw-fpga_4.1.3-klk8_wirnet.tar.gz](#)
 - Md5sum: f4e7de4c7a324ce1aa54d176801799a3
- Utils binaries: [libloragw-utils_4.1.3-klk8_wirnet.tar.gz](#)
 - Md5sum: 506d466fc0b2dbdc818518599d0a55e
- Source files: [libloragw-4.1.3-klk8.tar.gz](#)
 - Md5sum: fd6d0aca7e65ca72a0420ad5c7494bf3

II. Installation / Mise à jour des ressources

1) Mise à jour du firmware

1 – Décompressez à la racine de votre clé USB le « pack Firmware Kerlink 3.3 » (ou, si vous avez téléchargé les fichiers depuis le wiki de Kerlink, décompressez les deux .zip récupérés à l'étape 3). Le résultat doit être semblable à celui présenté ci-dessous.

Nom	Modifié le	Type	Taille
initramfs.cpio.gz.uboot	26/01/2018 14:07	Fichier UBOOT	1 178 Ko
prodbus.sh	21/02/2019 13:30	Shell Script	7 Ko
prodbus_wirnet_v3.3.md5	19/03/2018 09:59	Fichier MD5	1 Ko
rootfs.tar.gz	26/01/2018 14:07	gz Archive	9 262 Ko
script_uboot.img	26/01/2018 14:07	Fichier d'image disque	10 Ko
u-boot.bin	26/01/2018 14:07	Fichier BIN	142 Ko
ulmage	26/01/2018 14:07	Fichier	1 895 Ko
userfs.tar	26/01/2018 14:07	tar Archive	12 790 Ko
wirmaV2_wirnet_v3.3.md5	28/03/2018 17:31	Fichier MD5	1 Ko
wirmaV2_wirnet_v3.3.txt	14/02/2018 14:24	Document texte	2 Ko

2 – Mettez sous tension votre passerelle (appuyez sur le bouton « Test » sur la face avant pour savoir quand elle a fini de boot).





3 – Placez votre clé USB dans le port adéquat sur la face avant de la passerelle, puis, si les DEL sont éteintes, appuyez sur le bouton « Test ». Au bout de quelques secondes, vous devriez constater que les DEL « Mod1 » et « Mod2 » se mettent à clignoter. N'hésitez pas à rappuyer régulièrement sur le bouton « Test » afin de garder les DEL allumées. Il est important de ne pas retirer la clé USB avant la fin du processus.

4 – Lorsque vous vous êtes assuré que les DEL « MOD1 » et « MOD2 » ont cessé de clignoter, vous pouvez retirer la clé USB. Le firmware a été mis à jour.

2) Installation du Packet Forwarder

0 – Si vous avez utilisé votre clé USB pour mettre à jour le firmware, pensez à supprimer tous les fichiers avant de passer à la suite. Si votre clé USB est déjà vide, passez à l'étape suivante.

1 – Décompressez à la racine de votre clé USB le « Pack SPF Kerlink » (ou, si vous avez téléchargé les fichiers depuis le wiki de Kerlink, placez à la racine de votre clé vos deux fichiers « .tar.gz » respectivement téléchargés aux étapes 6 et 9, ainsi que le contenu du « produusb_wirnet_X.X.zip » téléchargé à l'étape 3. Le résultat doit être semblable à celui présenté ci-dessous.

Nom	Modifié le	Type	Taille
 custo_libloragw-fpga_4.1.3-klk8_wirnet.tar.gz	10/10/2018 10:54	gz Archive	105 Ko
 dota_spf_3.1.0-klk16_4.1.3-klk8_wirnet.tar.gz	10/10/2018 10:56	gz Archive	217 Ko
 produusb.sh	21/02/2019 13:30	Shell Script	7 Ko
 produusb_wirnet_v3.3.md5	19/03/2018 09:59	Fichier MD5	1 Ko

2 – Mettez sous tension votre passerelle (appuyez sur le bouton « Test » sur la face avant pour savoir quand elle a fini de boot).

3 – Placez votre clé USB dans le port adéquat sur la face avant de la passerelle, puis, si les DEL sont éteintes, appuyez sur le bouton « Test ». Au bout de quelques secondes, vous devriez constater que les DEL « Mod1 » et « Mod2 » se mettent à clignoter. N'hésitez pas à appuyer régulièrement sur le bouton « Test » afin de garder les DEL allumées. Il est important de ne pas retirer la clé USB avant la fin du processus.

4 – Lorsque vous vous êtes assuré que les DEL « MOD1 » et « MOD2 » ont cessé de clignoter, vous pouvez retirer la clé USB. Le logiciel a été installé.

III. Configuration des ressources

1) Connexion à la passerelle

a.1) Méthode 1 : Connexion en série

1 – Mettez la passerelle sous tension (en cas de doute, voir tutoriel dans la section « Annexes ») et ouvrez la face avant à l'aide d'un tournevis plat (enfoncer le tournevis plat dans la fente en haut de la face avant de la passerelle jusqu'à entendre un clic).³

2 – Branchez le câble USB du kit de debug sur l'un des ports USB du PC.

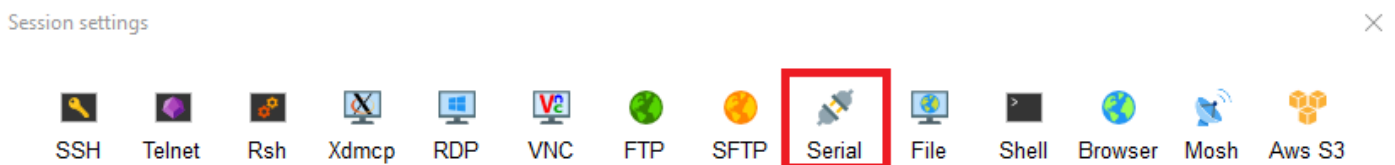
3 – Branchez l'autre bout du kit de debug (sortie 8 broches) dans le port « debug » de la passerelle (port rouge, au milieu à gauche. La sortie est dotée d'un détrompeur, qui doit se trouver vers le bas lors du branchement).

4 – Lancez MobaXTerm.

5 – Cliquez sur « Session » en haut à gauche de la fenêtre.

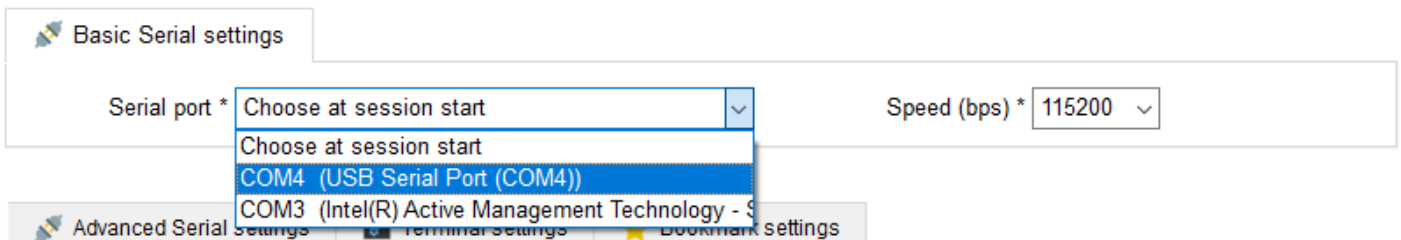


6 – Dans la fenêtre ouverte, cliquez sur « Serial »



7 – Dans « Basic Serial Settings », réglez :

- Serial Port : Indiquer le port sur lequel est branché le kit de debug (indiqué par l'identifiant « USB Serial Port »)
- Speed (bps) : 115200



7.5 – Normalement, les autres réglages sont à laisser par défaut. Cependant, vous pouvez tout de même vérifier les « Advanced Serial Settings » situés juste sous les « Basic Serial Settings » précédemment réglés. Ils doivent être ceux-ci (il s'agit de leur réglage par défaut, mais la connexion ne fonctionnera pas si un de ces paramètres est mal défini) :

³ Vous pouvez vérifier que la passerelle a été mise sous tension correctement en appuyant sur le bouton « test » de la passerelle. Les 2 LED « PWR » doivent s'allumer (LED verte fixe).

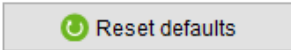
Serial engine: PuTTY (allows manual COM port setting) ▾

Data bits 8 ▾

Stop bits 1 ▾

Parity None ▾


Flow control Xon/Xoff ▾

 Reset defaults

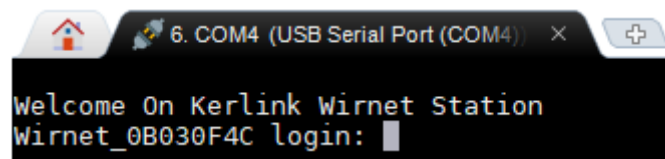
Execute macro at session start: <none> ▾

If you need to transfer files (e.g. router configuration file), you can use MobaXterm embedded TFTP server

["Servers" window --> TFTP server](#)



8 – Une fois tout ceci réglé, cliquez sur « OK » en bas de la fenêtre. Le terminal s'ouvre.



9 - Par défaut, les identifiants de la passerelle sont les suivants :

Login : root

Password : pdmk-« les7caractèresaprèsWirnet_ » (soit, dans cet exemple, pdmk-0B030F4C)

a.2) Méthode 2 : Connexion SSH

1 – Mettez la passerelle sous tension (en cas de doute, voir tutoriel dans la section « Annexes ». **ATTENTION, POUR CETTE CONNEXION, LES 8 FILS DOIVENT ÊTRE VISSÉS SUR LA PASSERELLE**), et connectez, grâce à un câble RJ45, l'autre port (DATA IN) de l'injecteur PoE à votre PC.

2 – Changez l'adresse IP de l'interface réseau Ethernet de votre PC connectée à votre passerelle à :

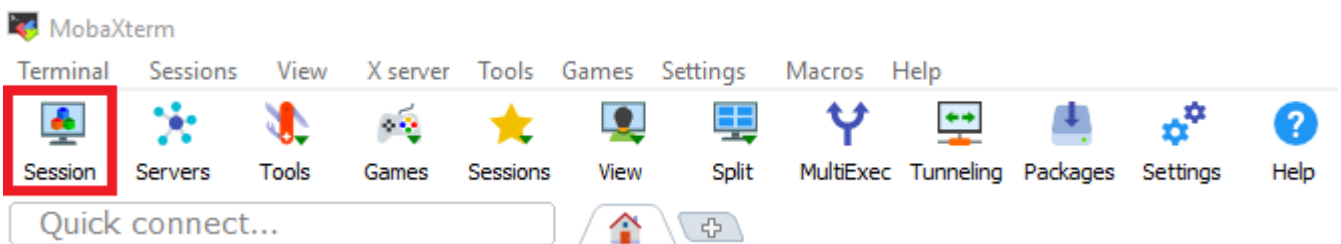
Adresse : 192.168.4.5

Maque : 255.255.255.0

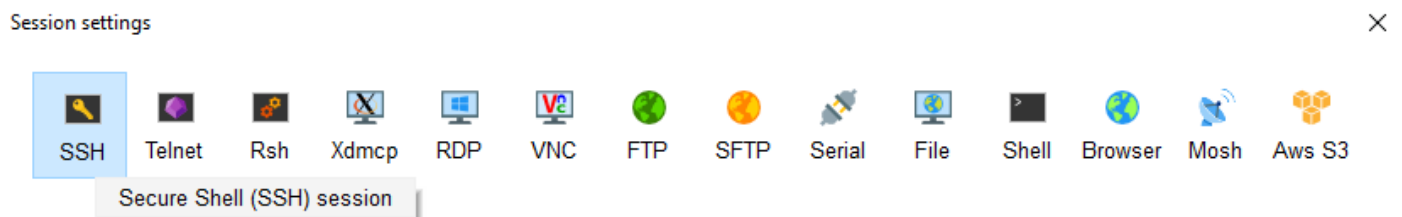
Un tutoriel pour connaître la procédure pour effectuer ce changement est disponible dans la section « Annexes ».

3 – Lancez MobaXTerm.

4 – Cliquez sur « Session » en haut à gauche de la fenêtre.



5 – Dans la fenêtre ouverte, cliquez sur « SSH ».

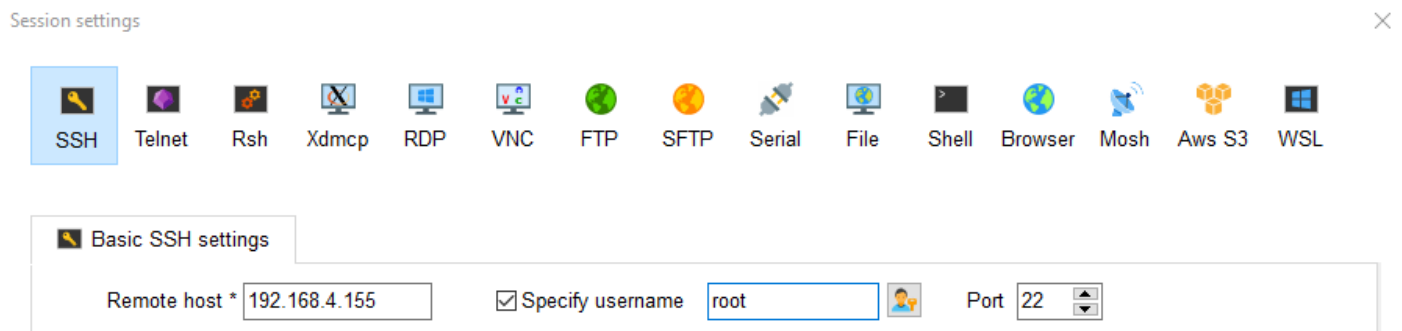


6 – Entrez les paramètres suivants :

- Remote host : 192.168.4.155

- Cochez « Specify Username », puis tapez « root »

- Port : 22 (par défaut)



7 – Cliquez sur « Ok ». Un terminal va s'ouvrir vous demandant un mot de passe. Si aucun terminal ne s'affiche, appuyez sur la touche « Entrée » pour l'afficher.

8 – Par défaut, les identifiants de la passerelle sont les suivants :

Login : root

Password : pdmk-« les7caractèresaprèsWirnet_ »

b) Configuration du réseau GSM

1 – Avec la passerelle hors tension, insérez la carte SIM de votre choix dans l’emplacement prévu sur la face avant de la passerelle.

2 – Mettez votre passerelle sous tension, et loggez-vous dessus [en série](#)⁴.

3 – Tapez la commande suivante :
vi /etc/sysconfig/network

4 – Appuyez sur la touche « i » de votre clavier pour passer en mode « input » dans le fichier ouvert.

5 – Modifiez les valeurs suivantes :

GPRSAPN=[APN de votre fournisseur d’accès GSM]

(APN actuellement utilisés :

SFR : sl2sfr

The Things Mobile : TM

Bouygues : objcoNPublic)

GPRSPIN=[Code PIN de votre carte SIM, sinon laisser vide après le =]

(PIN actuellement utilisés :

The Things Mobile : 1503)

```
# Selector operator APN
GPRSAPN=objcoNPublic
# Enter pin code if activated
GPRSPIN=
# Update /etc/resolv.conf to get dns facilities
GPRSDNS=yes
# PAP authentication
GPRSUSER=
GPRSPASSWORD=
```

Figure 1 : Exemple avec une carte SIM Bouygues

6 – Appuyez sur la touche « Echap » de votre clavier pour repasser en mode « commandes » dans le fichier ouvert.

7 – Tapez « :wq », puis appuyez sur « Entrée » pour enregistrer le fichier et en sortir.

8 – Faire un reboot ??

9 – Tapez la commande « ping 8.8.8.8 »

Si le « packet loss » est égal à 100%, la communication a échoué. Vérifier votre configuration GSM.

⁴ Les passerelles Kerlink sont conçues pour n’avoir qu’une interface capable de communiquer avec « l’extérieur » active à un instant T. Si vous vous connectez en SSH pour configurer le GSM, l’interface Ethernet prendra la priorité, l’interface PPP permettant la communication GSM restera donc systématiquement éteinte.

c) Configuration du Packet Forwarder

0 – Si ce n'est pas déjà fait, loggez vous sur la passerelle (en série ou SSH, pour cette étape ça n'a pas d'importance)

1 – Tapez « vi /mnt/fsuser-1/spf/etc/global_conf.json »

2 – Appuyez sur la touche « i » de votre clavier pour passer en mode « input » dans le fichier ouvert.

3 – Dans le fichier ouvert, modifiez les lignes suivantes :

```
"lorawan_public": false,  
"server_address": "127.0.0.1",
```

4 – Dans le même fichier, sous « gateway_conf », ajoutez la ligne :

```
"gateway_ID": "7276FF000[7 derniers caractères du numéro de série de la passerelle]",  
exemple : 7276FF000B0302D1
```

Votre fichier doit être semblable au fichier ci-contre.

5 – Appuyez sur la touche « Echap » de votre clavier pour repasser en mode « commandes » dans le fichier ouvert.

6 – Tapez « :wq », puis appuyez sur « Entrée » pour enregistrer le fichier et en sortir.

```

" SX1301_conf": {
  "lorawan_public": false,
  "antenna_gain": 0,
  "clksrc": 1,
  "radio_0": {
    "enable": true,
    "type": "SX1257",
    "freq": 867500000,
    "tx_enable": true,
    "tx_notch_freq": 129000,
    "tx_freq_min": 863000000,
    "tx_freq_max": 870000000
  },
  "radio_1": {
    "enable": true,
    "type": "SX1257",
    "freq": 868500000,
    "tx_enable": false
  },
  "chan_multiSF_0": { "enable": true, "radio": 0, "if": -400000 },
  "chan_multiSF_1": { "enable": true, "radio": 0, "if": -200000 },
  "chan_multiSF_2": { "enable": true, "radio": 0, "if": 0 },
  "chan_multiSF_3": { "enable": true, "radio": 0, "if": 200000 },
  "chan_multiSF_4": { "enable": true, "radio": 0, "if": 400000 },
  "chan_multiSF_5": { "enable": true, "radio": 1, "if": -400000 },
  "chan_multiSF_6": { "enable": true, "radio": 1, "if": -200000 },
  "chan_multiSF_7": { "enable": true, "radio": 1, "if": 0 },
  "chan_Lora_std": {
    "enable": true,
    "radio": 1,
    "if": -200000,
    "bandwidth": 250000,
    "spread_factor": 7
  },
  "chan_FSK": {
    "enable": true,
    "radio": 1,
    "if": 300000,
    "bandwidth": 125000,
    "datarate": 50000
  },
  "tx_lut_0": {"dig_gain": 0, "pa_gain": 0, "mix_gain": 8, "rf_power": 0}
},
"gateway_conf": {
  "gateway_ID": "7276FF000B0302FE",
  "server_address": "127.0.0.1",
  "serv_port_up": 1700,
  "serv_port_down": 1700,
  "keepalive_interval": 10,
  "stat_interval": 30,
  "push_timeout_ms": 100,
  "forward_crc_valid": true,
  "forward_crc_error": false,
  "forward_crc_disabled": false,
  "autoquit_threshold": 3,
  "gps_tty_path": "/dev/nmea"
}
}

```

```

- /mnt/fsuser-1/spf/etc/global_conf.json 59/59 100%

```


d) Configuration du VPN

0 – Si cela n’a pas déjà été fait précédemment, télécharger depuis la forge le dossier « openvpn » (selon la méthode décrite dans le chapitre 2) Récupération des ressources / sous-chapitre 1(via la forge)), et décompresser le pack sur votre ordinateur.

1 – Connectez-vous à la passerelle en SSH via MobaXTerm (voir Chapitre 3) Configuration des ressources, sous-chapitre 1) Connexion à la passerelle, paragraphe a.2) Méthode 2 : Connexion SSH)

2 - Glisser-déposer le dossier « openvpn » décompressé depuis le PC sur l’écran de MobaXTerm (ça aura pour effet d’initier la copie du dossier et de son contenu vers la passerelle).

3) Taper les commandes suivantes :

- mkdir /etc/openvpn
- mv openvpn/openvpn/* /etc/openvpn/
- rm /etc/init.d/network_functions
- mv openvpn/network_functions /etc/init.d/ »
- mkdir /mnt/fsuser-1/openvpn
- mv openvpn/fsuser-vpn/* /mnt/fsuser-1/openvpn/
- chmod +x /mnt/fsuser-1/openvpn/start_openvpn.sh
- vi /etc/sysconfig/network
 - o Appuyer sur « i » pour passer en input
 - Modifier les lignes (en bas du fichier) :
 - FIREWALL=yes
 - VPN=yes
 - o Appuyer sur « Echap » pour repasser en commande, puis taper « :wq » et Entrée
- vi /etc/init.d/firewall
 - o Appuyer sur « i » pour passer en input
 - Sous les lignes :
#allow KMS connections
iptables -A INPUT -p tcp --dport 35035 -j ACCEPT
 - Ajouter les lignes :
#allow VPN connection
iptables -A INPUT -p tcp -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
 - o Taper « Echap », « :wq », puis « Entrée »

4) Fermer la session SSH de MobaXTerm, retirer le câble RJ45 connectant le PC à l’injecteur PoE (celui reliant la passerelle à l’injecteur doit rester connecté pour des raisons d’alimentation. Les 8 fils peuvent rester connectés sans que ce soit gênant tant que la passerelle ne peut pas communiquer en Ethernet).

5) Appuyer sur le bouton « reset » présent sur la face « haut » de la passerelle.

ATTENTION : Il faudra vérifier tous les fichiers copiés depuis le pc sur la passerelle, notamment les fichiers de config du vpn, car ils sont tous susceptible d’avoir comme caractère à la fin de chaque ligne « ^M ». Be careful !

Commande linux pour chercher et remplacer une chaîne de caractères dans un fichier :

dos2unix "chemin/fichier"

```

#!/bin/sh

. /etc/profile
. /etc/sysconfig/network

set_rules()
{
    #DROP everything in INPUT (Let everything going out)
    iptables -P INPUT DROP
    ip6tables -P INPUT DROP

    #Allow everything on localhost interface
    iptables -A INPUT -i lo -j ACCEPT

    #Allow DHCP protocol on all interfaces
    iptables -A INPUT -p udp --dport 67:68 --sport 67:68 -j ACCEPT
    #Allow ICMP output (ping requests) on all interfaces
    iptables -A INPUT -p icmp -j ACCEPT
    #allow ICMP v6 on all interfaces
    ip6tables -A INPUT -p ipv6-icmp -j ACCEPT

    #allow DNS requests
    iptables -A INPUT -p udp --sport 53 -j ACCEPT
    iptables -A INPUT -p tcp --sport 53 -j ACCEPT

    #allow NTP
    iptables -A INPUT -p udp --dport 123 --sport 123 -j ACCEPT

    # Allow CoAP messages
    # iptables -A INPUT -p udp --dport 5683 -j ACCEPT

    #allow FTP input connections
    # iptables -A INPUT -p tcp --dport 21 -j ACCEPT
    # iptables -A INPUT -p udp --dport 21 -j ACCEPT

    #allow SSH input connections
    iptables -A INPUT -p tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p udp --dport 22 -j ACCEPT

    #allow KMS connections
    # iptables -A INPUT -p tcp --dport 35035 -j ACCEPT

    #allow VPN connection
    iptables -A INPUT -p tcp -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

    #allow specific rules
    for file in `find /etc -name "iptables_*.rules"`
    do
        echo "Applying config file ${file}"
        iptables-restore --noflush < "${file}"
    done
}

```

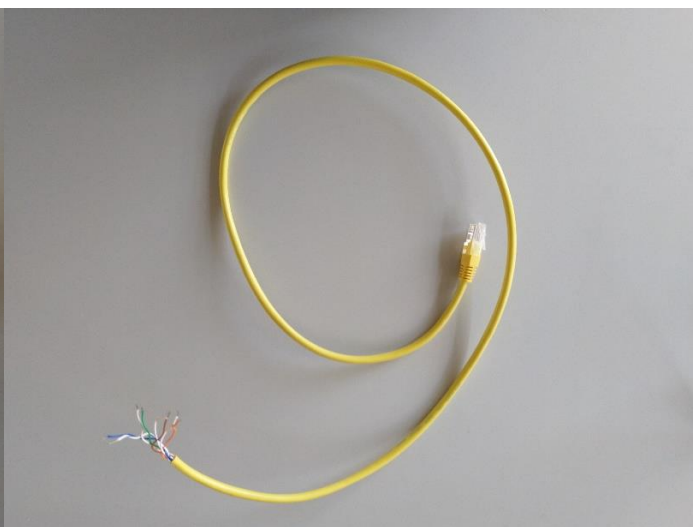
Annexes

1) Tutoriel : Branchement physique de la passerelle en vue de mise sous tension

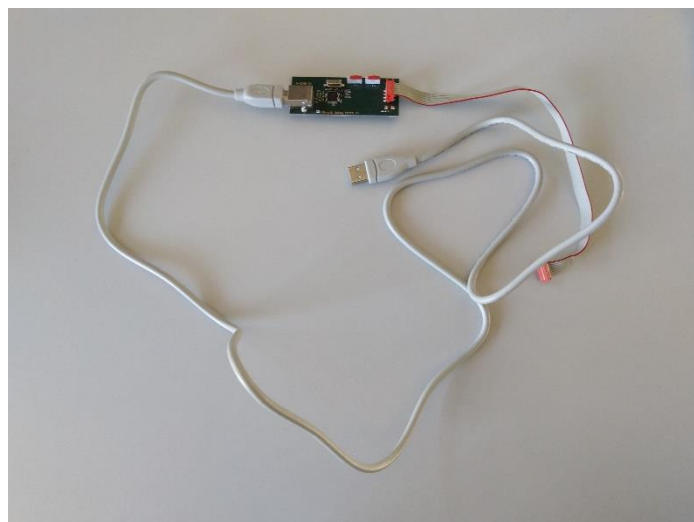
Matériel nécessaire :



Passerelle Kerlink



Câble RJ45 coupé, dénudé, étamé



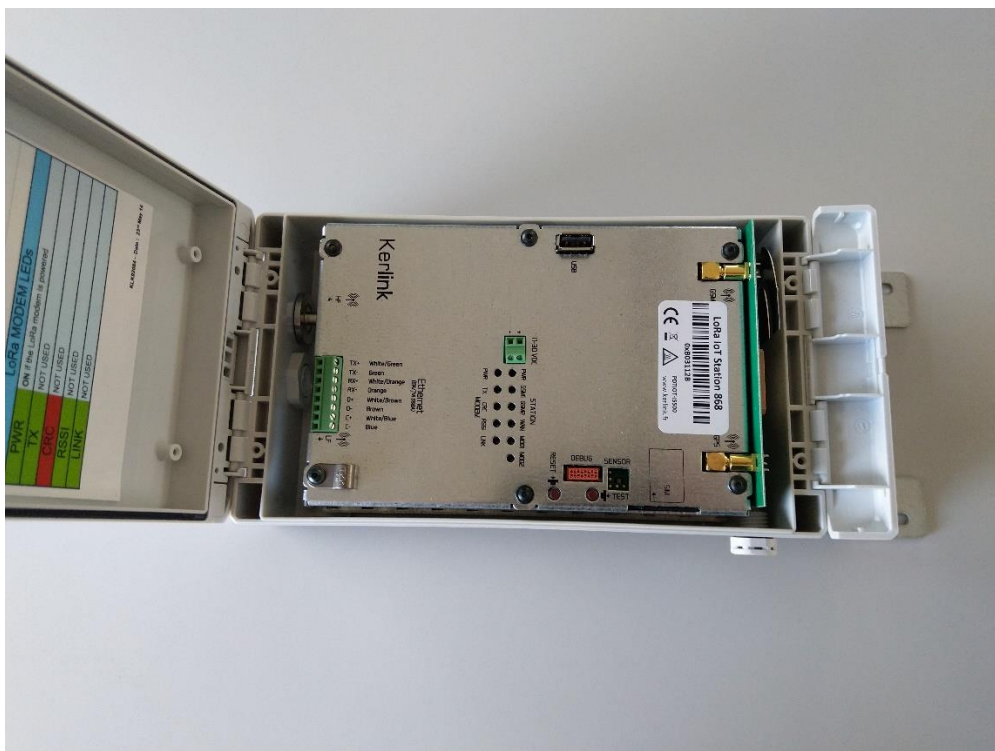
Wirgrid Debug Board



Injecteur PoE (sous tension)

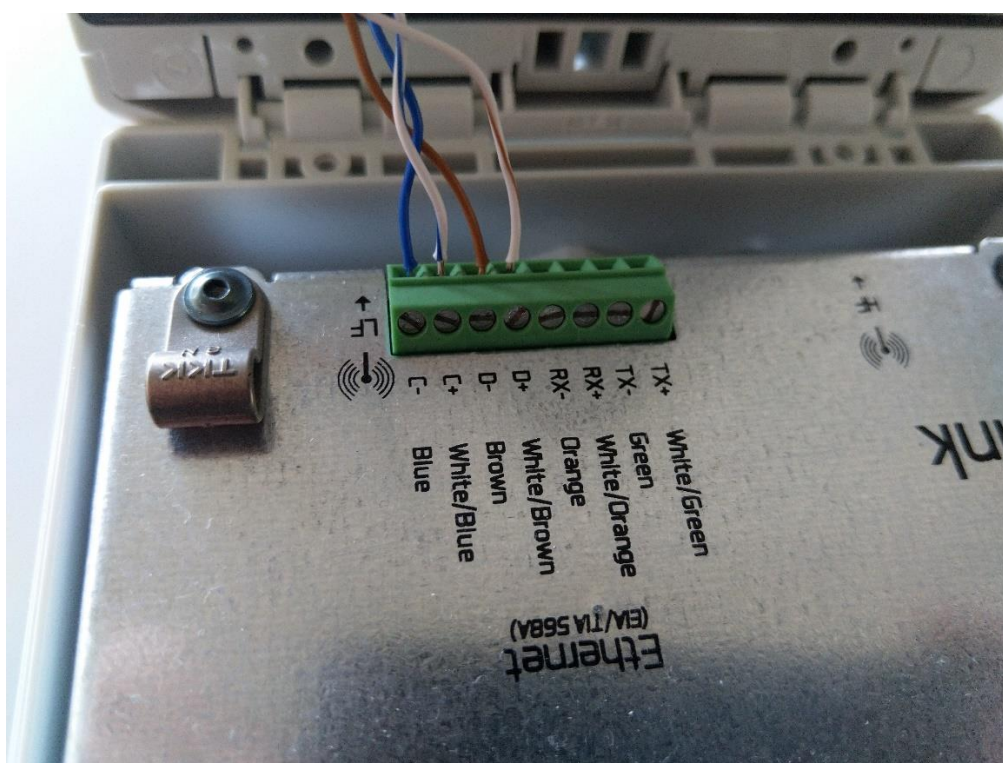
2) Mise en route de la passerelle

1) Enfoncez le petit tournevis plat dans l'une des encoches de la face supérieure de la passerelle jusqu'à entendre un « clic », et ouvrez cette dernière en soulevant le panneau de la face supérieure.



Passerelle ouverte

2) Insérez les 4 premiers fils dénudés du câble RJ45 (Bleu, Blanc / Bleu, Marron, Blanc / Marron) dans les emplacements d'alimentation de la passerelle (respectivement C-, C+, D-, D+)⁵, et vissez-les à l'aide du tournevis.

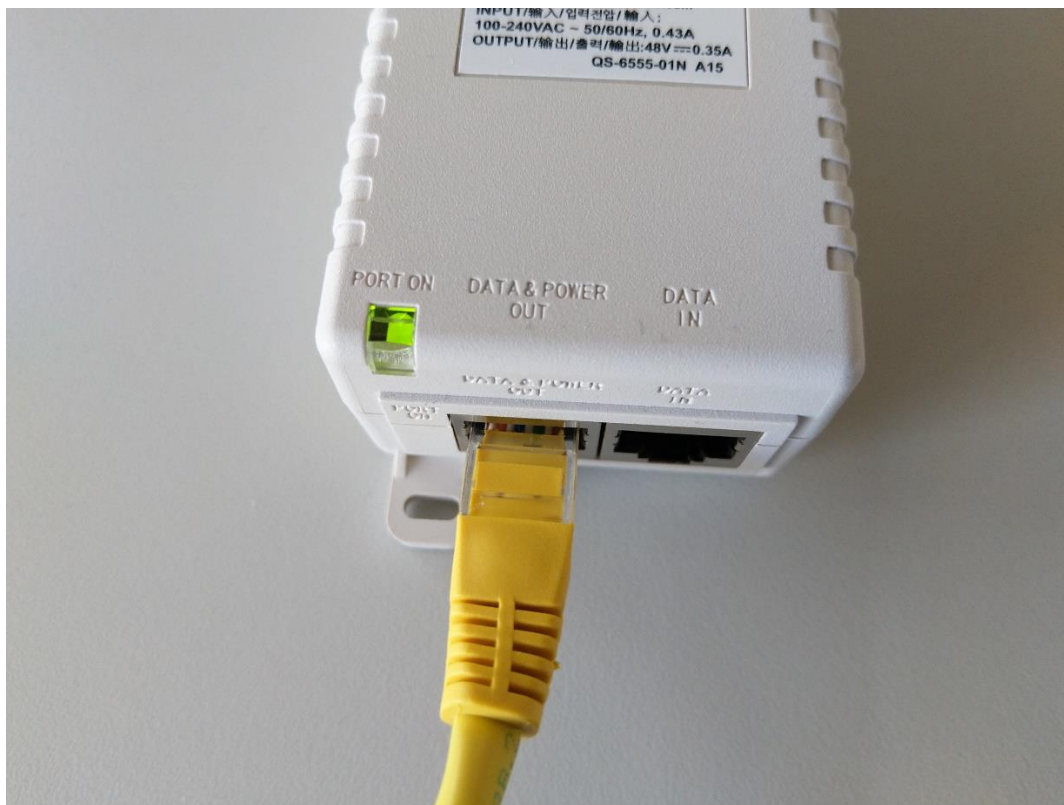


Fils vissés sur la passerelle

⁵ En cas de doute, les couleurs correspondantes à chaque emplacement sont indiqués sous ces derniers.

3) Si ce n'est pas déjà fait, mettez sous tension l'injecteur PoE⁶, et connectez l'autre extrémité du câble RJ45 au port « Data & Power Out » de l'injecteur. Si tout fonctionne bien, la DEL de l'injecteur passera de l'orange au vert.

Vous pouvez aussi vérifier que la passerelle est bien sous tension en appuyant sur son bouton « Test » de cette dernière. Si tout fonctionne bien, les deux DEL « PWR » doivent s'éclairer au vert de manière fixe.



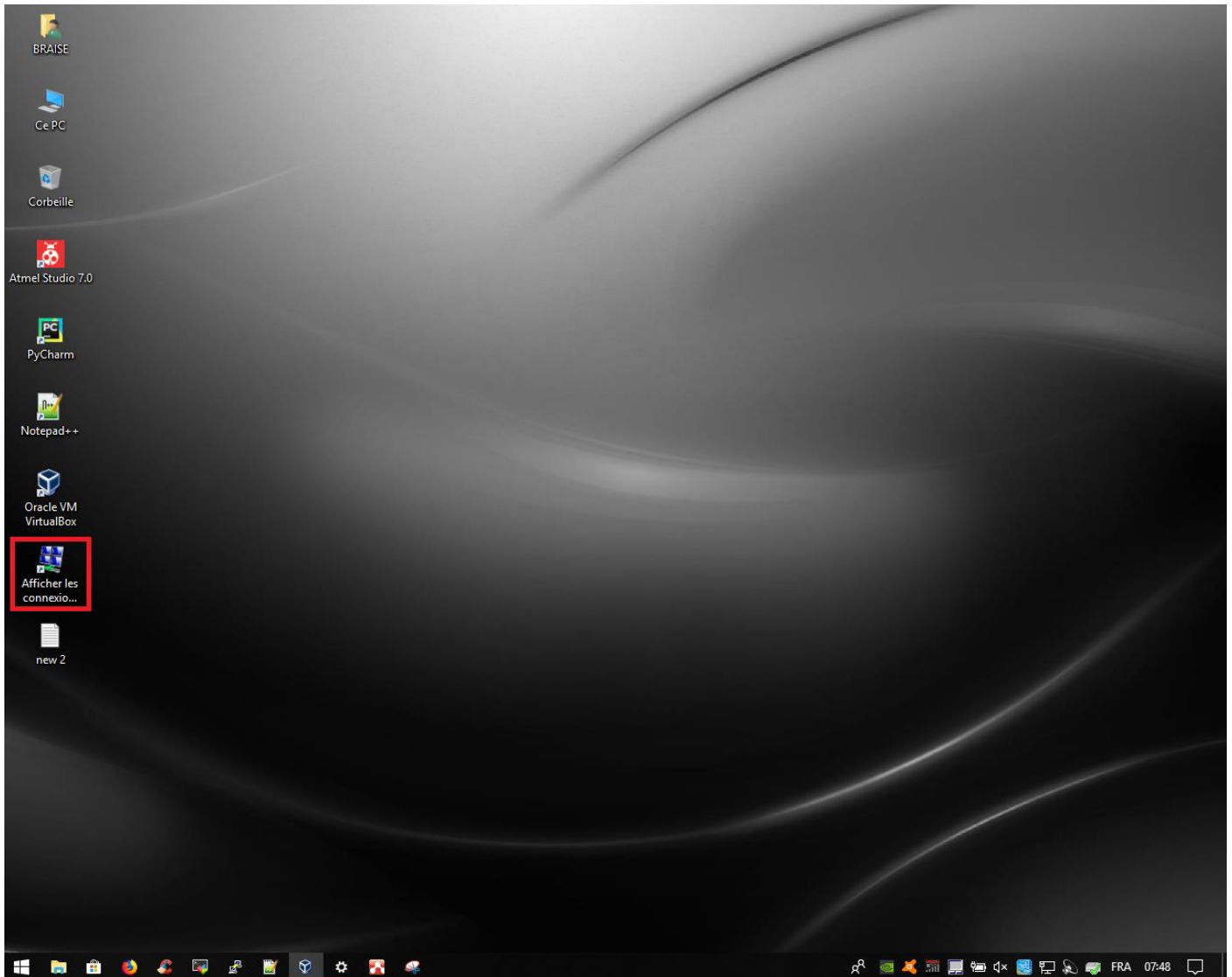
Injecteur PoE branché et fonctionnel

⁶ Le PoE, « Power Over Ethernet », est une technologie réseau permettant de faire passer du courant dans des câbles réseau, permettant ainsi de se passer d'un câble séparé pour mettre le matériel sous tension.

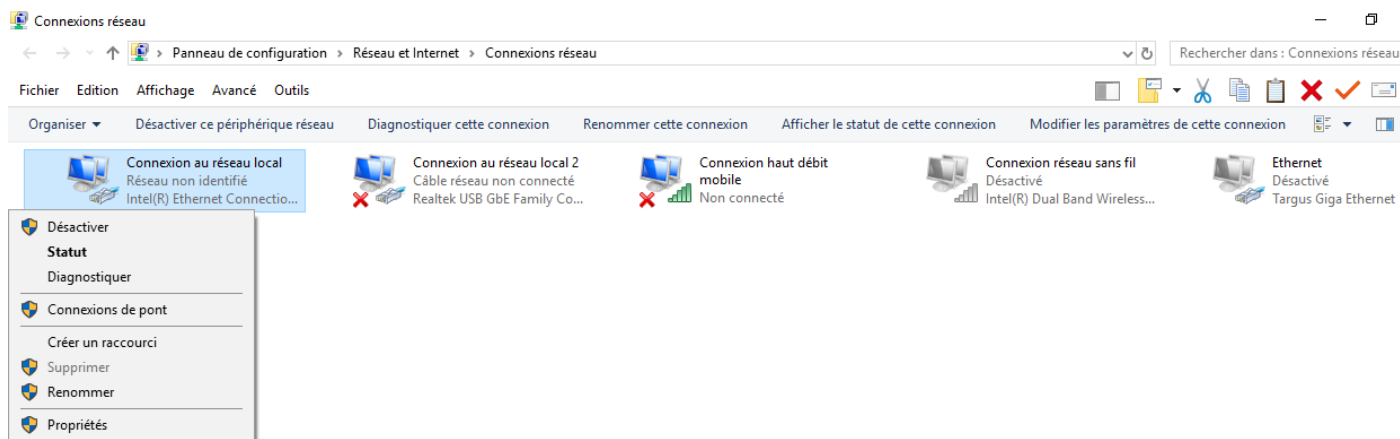
3) Tutoriel : Changer l'adresse IP de l'interface réseau Ethernet

1 – Sur le bureau, double-cliquez sur « Afficher les connexions réseau ».

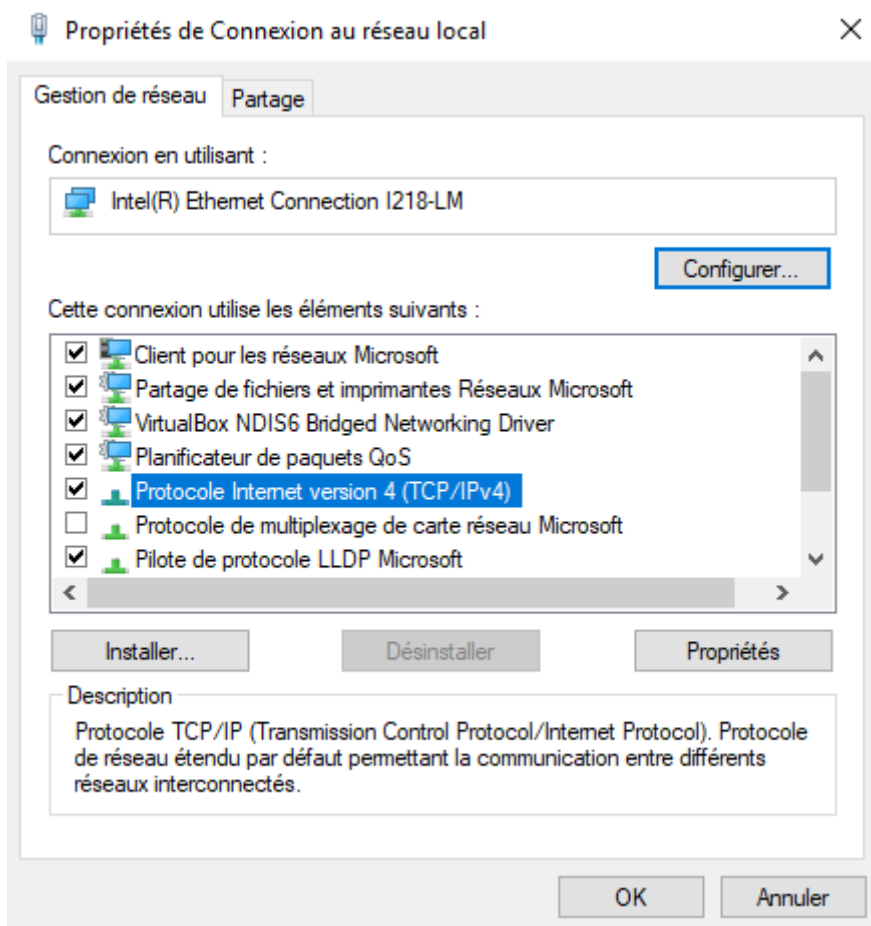
Si cette icône est absente, cliquez sur « Démarrer », tapez « Afficher les connexions réseau », puis cliquez sur le résultat.



2 – Dans la fenêtre ouverte, faites un clic droit sur l'interface « Connexion au réseau local »⁷ et cliquez sur « Propriétés ».



3 – Cliquez sur « Protocole Internet version 4 (TCP /IPv4), puis cliquez sur « Propriétés ».



⁷ Sur certaines versions de Windows, notamment les plus récentes, cette interface peut aussi s'appeler « Ethernet ».

4 - Cliquez sur « utiliser l'adresse IP suivante : », puis insérez les valeurs suivantes :

Adresse IP : 192.168.4.5

Masque de sous-réseau : 255.255.255.0

Puis, cliquez sur « OK » (vous pouvez aussi cocher la case « valider les paramètres en sortant », mais cela n'a pas d'incidence réelle sur l'efficacité de la configuration).

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 4 . 5

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : . . .

Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

OK Annuler

4) Monitoring VPN et autres concernant VPN

Note Richard février 22 ?

Mise à jour Laurent mai 22

VPN

Message de David G. :

« si ma mémoire est bonne, sur **le kerlink ZATU**, j'ai :

1. Créé un nouveau fichier `./mnt/fsuser-1/check_vpn.sh`, avec le contenu suivant :

Version pour GW trépied (mai 22, copie du fichier dans le répertoire) :

```
[root@Wirnet_0b030f4c fsuser-1]# more check_vpn.sh
#!/bin/bash
ping -c 1 -W 120 10.0.42.1 2>/dev/null 1>&2
ret=$?
if [ $ret -ne 0 ]
then
  pkill -2 /usr/sbin/openvpn
  pkill -15 /usr/sbin/openvpn
  pkill -9 /usr/sbin/openvpn
  /bin/bash /mnt/fsuser-1/openvpn/start_openvpn.sh &
fi
```

2. Ajouté une tâche récurrente de lancement de ce script

```
$ crontab -e
```

```
@ */1 * * * /bin/bash /mnt/fsuser-1/check_vpn.sh
```

Version pour GW trépied (mai 22) :

```
*/4 * * * * /bin/bash /mnt/fsuser-1/check_vpn.sh
```

VPN

Alors que ce n'est pas indiqué sur la doc d'Etienne, l'adresse du serveur doit être modifiée dans le fichier /mnt/fsuser-1/spf/etc/global_conf.json. Il faut mettre l'adresse 127.0.0.1 pour le serveur, comme ci-dessous :

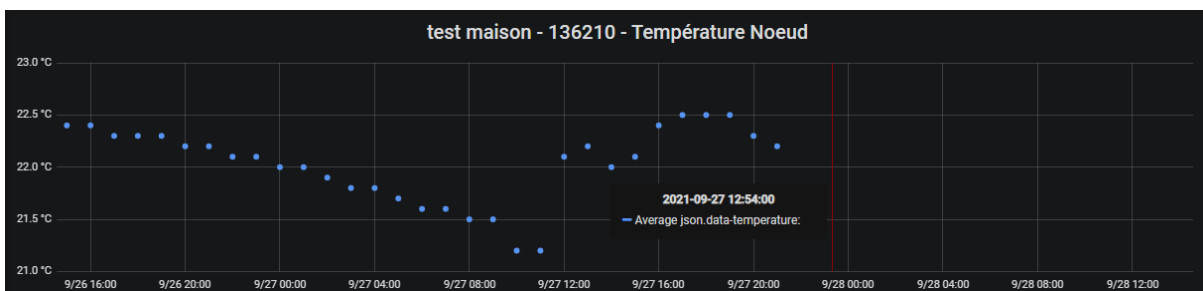
```
    "tx_lut_0": {"dig_gain": 0, "pa_gain": 0,
},
"gateway_conf": {
  "gateway_ID": "7276FF000B030F4C",
  "server_address": "127.0.0.1",
  "serv_port_up": 1700,
  "serv_port_down": 1700,
  "keepalive_interval": 10,
  "stat_interval": 30,
  "push_timeout_ms": 100,
  "forward_crc_valid": true,
  "forward_crc_error": false,
  "forward_crc_disabled": false,
  "autoquit_threshold": 3,
  "gps_tty_path": "/dev/nmea"
}
```

Service VPN ne se relance pas

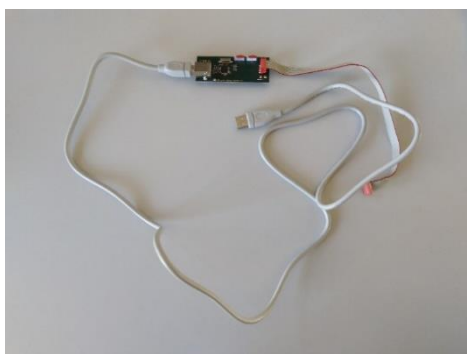
Note Richard

Problème :

- A partir du 27/09/2021 à 21h les données ne sont plus remontées au Mésocentre



- Accès à la passerelle via la carte de debug



Sur la console de la passerelle, je tape ifconfig pour vérifier les interfaces réseaux :

- Eth0, lo et pp0 sont présent
- Tun0 n'est pas lancé

Test secondaire :

- ping 8.8.8.8 OK
- ping 10.0.42.1 (Loraserver nécessitant un VPN) pas OK

Le service VPN n'est donc pas fonctionnel.

- Vérification des scripts permettant le redémarrage automatique du service VPN
 - Un script de monitoring (/mnt/fsuser-1/openvpn/start_openvpn.sh) surveille openvpn et le relance s'il quitte
 - Ce script est lancé parce que l'option **start autostart="y"** est mise dans le fichier /mnt/fsuser-1/openvpn/manifest.xml et **VPN=yes** est mis dans le fichier /etc/sysconfig/network

La configuration des scripts est OK !!

Pourquoi openvpn ne s'est pas relancé automatiquement ???

A faire confirmer mais d'après le script « start_openvpn.sh » en cas de crash du VPN, un fichier « exit_openvpn » doit être créé pour que le redémarrage du service soit effectué. Or dans notre cas, le fichier n'était pas présent. → Cause du problème ????

```
[root@wirnet_0b0302fe openvpn]# more /mnt/fsuser-1/openvpn/start_openvpn.sh
#!/bin/bash

trap "killall openvpn ; touch /tmp/exit_openvpn" SIGINT
killall openvpn || true

/usr/sbin/openvpn /etc/openvpn/client-openvpn.conf &
PID=$!
STATUS=0

STATUS=0

while ! [ -f /tmp/exit_openvpn -o $STATUS -eq 1 ]
do
    sleep 1
    kill -0 $PID
    STATUS=$?
done

rm -f /tmp/exit_openvpn
```

- Reboot la passerelle

Le service VPN est lancé

```
[root@wirnet_0b0302fe openvpn]# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:4B:08:03:02:FE
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:580 (580.0 B)
          Interrupt:29

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1%1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2637 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2637 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:198322 (193.6 KiB)  TX bytes:198322 (193.6 KiB)

ppp0     Link encap:Point-to-Point Protocol
          inet addr:10.109.141.223  P-t-P:10.109.141.223  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:1973 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2088 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:198059 (193.4 KiB)  TX bytes:230873 (225.4 KiB)

tun0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.0.42.7  P-t-P:10.0.42.7  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:722 errors:0 dropped:0 overruns:0 frame:0
          TX packets:784 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:31533 (30.7 KiB)  TX bytes:44060 (43.0 KiB)
```

Test :

- ➔ ping 8.8.8.8 OK
- ➔ ping 10.0.42.1 (Loraserver nécessitant un VPN) OK

Le service VPN est fonctionnel.

- Vérification de la fonctionnalité du monitoring et du redémarrage automatique des services

Tuer tous les process openvpn → killall openvpn (service VPN HS)

Au bout de quelques secondes le service VPN se relance sans soucis.

Le redémarrage des services à l'air fonctionnel