RAS/IPL/SIG Guide de configuration 4.13

Cette documentation est également disponible en version web sur doc.etictelecom.com

TABLE OF CONTENTS

1. INTERFACES WAN

Les interfaces WAN (Wide Area Network) sont les interfaces exposées au réseau public. Ces interfaces sont protégées par le pare-feu du routeur. Pour plus d'informations sur les fonctionnalités de pare-feu, consultez la section Pare-feu.

Les chapitres suivants vous aideront à configurer les interfaces WAN.

1.1. ADSL

Cette section s'applique aux routeurs ci-dessous :

IPL-A, IPL-DAC, SIG-A

Accéder au menu ***Configuration > Interfaces WAN > ADSL***

Configuration du modem ADSL

Activer l'ADSL	Permet d'activer ou de désactiver l'interface ADSL
Modulation	La valeur par défaut est Multimode ; le modem s'adaptera à la modulation du modem FAI. Sinon, demandez à votre fournisseur la modulation à utiliser.
VPI ATM	La plage est `0 – 4095`. Laissez la valeur par défaut (8)
VCI ATM	La plage est `0 – 65535`. Laissez la valeur par défaut (35)
Multiplexage	Valeur `LLC` ou `VC`. Laissez la valeur par défaut (LLC)
Encapsulation	• `PPPoE` : PPP sur Ethernet • `PPPoA` : PPP sur ATM • `EoA` : Ethernet sur ATM • `IPoA` : IP sur ATM Un ensemble de paramètres IP est associé à chacune de ces d'encapsulation (voir le paragraphe suivant).

Configuration IP du WAN ADSL

La configuration IP dont dépend la ligne ADSL

1.1. ADSL

	PPPoE	PPPoA	EoA	IPoA
Priorité du WAN ADSL Ce paramètre définit la priorité du chemin lorsque plusieurs chemins sont sélectionnés (Cellulaire et Ethernet WAN, par exemple). Le routeur utilisera en premier l'interface ayant la priorité la plus élevée ; l'autre interface sera utilisée comme backup.	✔	✔	✔	✔
PPP login & **Mot de passe PPP** Saisissez le login et mot de passe du compte ADSL.	✔	✔		
Nom de service PPPoE C'est le nom du service fourni par l'opérateur. Habituellement, il n'est pas nécessaire de saisir ce paramètre	✔			
Obtenir une adresse IP automatiquement, **Adresse IP** & **Adresse IP distante** Laissez cette option sélectionnée si le fournisseur est censé attribuer une adresse IP au routeur via la ligne à chaque fois qu'il se connecte à Internet (par défaut). Sinon, désélectionnez cette option et saisissez l'adresse IP attribuée à l'interface ADSL ainsi que l'adresse IP du routeur distant.	✔	✔	✔	✔
Obtenir les adresses des serveurs DNS automatiquement, **Adresse serveur DNS primaire** & **Adresse serveur DNS secondaire** Laissez cette option sélectionnée si le fournisseur est censé fournir ces adresses automatiquement via la ligne (par défaut). Sinon, désélectionnez cette option et entrez l'adresse IP du serveur DNS principal et secondaire.	✔	✔	✔	✔
Activer la translation d'adresse (NAT) Si cette option est sélectionnée, l'adresse IP source de toute trame IP provenant d'un appareil connecté à l'interface LAN et acheminée vers l'interface ADSL, est remplacée par l'adresse IP WAN du routeur. **NOTE** Cochez cette case si un appareil de l'interface LAN doit établir une connexion avec un appareil connecté à Internet (serveur FTP, ...)	✔	✔	✔	✔

	PPPoE	PPPoA	EoA	IPoA
Activer le proxy ARP Cette fonction donne un accès direct au routeur distant pour les équipements de l'interface LAN. Laissez cette case décochée	✔	✔	✔	✔

Les informations saisies sur cette page doivent être fournies par le fournisseur Internet.

Ping de contrôle

Le routeur est capable d'envoyer périodiquement un message PING via une interface WAN vers une machine particulière. Si le PING reçoit une réponse, cette interface WAN est déclarée active avec la priorité déclarée. Si le message PING ne reçoit pas de réponse, cette interface WAN est désactivée.

Activer le PING de contrôle	Activer ou désactiver la fonction PING de contrôle
Adresse IP du serveur	Adresse IP de la machine à laquelle le message PING doit être transmis
Intervalle des PING	Période entre deux pings consécutifs
Nombre d'essais	Nombre d'échecs de messages PING avant de désactiver l'interface WAN

1.2. Cellulaire

Cette section s'applique aux routeurs ci-dessous :

IPL-C, IPL-DAC, SIG-C, RAS-C, RAS-EC, RAS-ECW

Pour certains modèles, deux cartes SIM peuvent être insérées dans le routeur pour permettre l'utilisation de deux réseaux cellulaires différents.

Le réseau correspondant sur la carte SIM numéro 1 est le réseau principal, tandis que l'autre est le réseau de secours.

Configuration de l'interface cellulaire

Accéder au menu ***Configuration > Interfaces WAN > Cellulaire***

Actif	Permet d'activer ou de désactiver l'interface cellulaire
Priorité de l'interface cellulaire	Ce paramètre définit la priorité du chemin lorsque plusieurs chemins sont sélectionnés (Cellulaire et Ethernet WAN, par exemple). Le routeur utilisera en premier l'interface ayant la priorité la plus élevée ; l'autre interface sera utilisée comme backup.

Carte SIM	Il est possible de sélectionner le numéro de carte SIM 1, ou le numéro de carte SIM 2 ou les deux : • `SIM1`: La SIM 1 est sélectionné (valeur par défaut) • `SIM2`: La SIM 2 est sélectionné • `SIM 1 backup sur SIM2`: La SIM 1 est utilisée en premier ; la SIM 2 sert de backup
MTU de l'interface (Paramètre avancés)	Maximum Transfer Unit, contrôle le plus gros paquet de données pouvant être transféré sans fragmentation, 1500 par défaut

Compteur de trafic cellulaire

Jour de réinitialisation	Lorsque ce jour du mois est atteint, le routeur réinitialise son compteur de trafic cellulaire. La valeur du compteur de données cellulaires est enregistrée chaque mois dans le journal ***Diagnostics>Statistiques>Utilisation des données***

Partage de données avec le serveur de licence Etic

Envoyer l'ICCID	Partage l'ICCID de la carte SIM au serveur de licence Etic. Cette option doit êter activée si vous souhaitez pouvoir visualiser la consommation des données de votre EticSIM dans votre espace client.

Commandes SMS

Certains textes de SMS envoyés au routeur agissent comme des commandes et déclenchent des actions sur le routeur. Seuls les utilisateurs avec leur numéro de téléphone enregistré dans le routeur peuvent déclencher ces commandes.

Ces commandes sont répertoriées dans le tableau ci-dessous.

`M2ME ON`	Active la connexion M2Me
`M2ME OFF`	Désactive la connexion M2Me
`CELL ON`	Active la data cellulaire
`CELL OFF`	Désactive la data cellulaire
`DOUT ON`	Met la sortie TOR à l'état ON (1)
`DOUT OFF`	Met la sortie TOR à l'état OFF (0)
`ACK XXXX`	Acquitte l'alarme dont l'identifiant est XXXX
`PING`	Renvoie "PONG" à l'émetteur

REBOOT	Redémarre le routeur

NOTE Ces commandes ne sont pas sensibles à la casse, i.e. `M2ME ON` aura le même effet que `m2me on`

Connexion au fournisseur de services mobiles

La mise en place de la carte SIM 1 ou de la carte SIM 2 est identique. Nous décrivons ci-après la configuration de la carte SIM 1.

SIM : Configuration du modem

Nom du point d'accès (APN)	Entrez le libellé de la passerelle (APN) vers Internet - ou vers d'autres services - fournis par le fournisseur de services mobiles.
Code PIN de la carte SIM	Saisissez le code PIN de la carte SIM. Tant que le code PIN n'a pas été correctement saisi, le voyant LED OPERATION clignote (couleur rouge).
Type de réseau	Le routeur est censé se connecter au meilleur relais cellulaire disponible. Cependant, dans des situations particulières, il peut être utile de forcer le Routeur à utiliser un service particulier. Ce paramètre permet de sélectionner soit le service LTE 4G, soit le service UMTS 3G soit le service GPRS-EDGE. La valeur par défaut est `Auto` ; dans ce cas, le routeur sélectionne la meilleure connexion disponible.

Interface IP cellulaire

Identifiant & **Mot de passe**:	Entrez le login et le mot de passe de l'abonnement. Ces paramètres ne sont généralement pas obligatoires.
Authentification avec PAP seul	Activer si vous nécessitez l'authentification PAP
Obtenir une adresse IP automatiquement	L'adresse IP de l'interface cellulaire du routeur est généralement attribuée par le fournisseur de services par voie hertzienne. Sinon, saisissez l'adresse IP attribuée à l'interface cellulaire du routeur.

Forcer un opérateur	Si cette option est cochée, un opérateur spécifique peut être choisi. Dans certains cas, il peut être intéressant de forcer la connexion cellulaire via un fournisseur de service spécifique. Par exemple pour éviter le roaming vers un opérateur étranger lors d'une installation en zone frontalière. Un opérateur doit être mentionné par son code pays mobile suivi du code réseau mobile de l'opérateur. Par exemple pour Orange (MNC=01) en France (MCC=208), le champ doit être renseigné avec le code "20801".

Paramètres partagés par les deux SIM

Obtenir les adresses des serveurs DNS automatiquement	Laissez cette case cochée si l'adresse IP des serveurs DNS est attribuée par un serveur DHCP. Sinon, décochez cette case et saisissez les adresses IP des serveurs DNS.
Activer la translation d'adresse (NAT)	Si cette option est sélectionnée, l'adresse IP source de toute trame IP provenant d'un périphérique connecté à l'interface LAN et acheminée vers l'interface WAN est remplacée par l'adresse IP WAN du routeur. **NOTE** Cochez cette case si un périphérique de l'interface LAN doit établir une connexion avec un périphérique connecté à Internet.

Fonctionnement de la SIM de backup

Chaque carte SIM peut être associée à un fournisseur de données mobiles différent.

Dans le texte suivant, le service cellulaire associé à la carte SIM 1 est appelé Réseau 1 et le service cellulaire associé à la carte SIM 2 Réseau 2.

À la mise sous tension, le réseau 1 est le premier à être testé.

Si le réseau 1 reste en panne pendant la période T1, le routeur bascule vers le réseau 2.
Si le réseau 2 fonctionne correctement, le routeur utilise ce réseau cellulaire au moins durant la période T3.
À l'expiration de cette période, le routeur revient au réseau 1 et vérifie s'il est disponible. Si ce n'est pas le cas, le routeur continue d'utiliser le réseau 2.

À tout moment, si le réseau 2 ne fonctionne pas correctement pendant la période de temps T2, le routeur bascule sur le réseau 1.

Les périodes de temps T1, T2 et T3 peuvent être configurées.

Nous conseillons de ne pas sélectionner des valeurs trop petites pour les paramètres T1, T2 et T3:

Example 1. Temps de commutation de la carte SIM

T1 Temps max de déconnexion SIM1 avant commutation = 20 mn + T1 Temps max de déconnexion SIM2 avant commutation = 20 mn + T3 Temps de connexion SIM2 avant de retester SIM1 = 12 heures

Timings du backup de SIM

Temps avant basculement sur SIM2	Voir au-dessus. Valeurs possibles : 5, 10, 20, 30, 60 mn
Temps avant rebasculement sur SIM1	Voir au-dessus. Valeurs possibles : 5, 10, 20, 30, 60 mn
Temps de connection sur SIM2 avant de retester SIM1	Voir au-dessus. Valeurs possibles : 1, 12, 24 heures, 5 jours, jamais.

Contrôle de la connexion cellulaire

En cas de défauts de connexion constatés, il peut être intéressant d'activer l'option de contrôle de la connexion cellulaire.

Le routeur peut vérifier périodiquement que la connexion cellulaire est correctement établie.

Cependant, chez certains fournisseurs de services mobiles ou dans des situations particulières, la connexion peut rester active alors que le service de transmission de données n'est pas fourni par le fournisseur de services mobiles.

C'est pourquoi le routeur est capable d'envoyer une requête ping à un serveur particulier pour vérifier si le service de données est réellement fonctionnel. Si il ne l'est pas, la connexion cellulaire est redémarré.

Pour implémenter cette fonction, entrez les paramètres ci-dessous.

Activer le PING de contrôle	Activer ou désactiver la fonction du PING de contrôle
Adresse IP ou Nom d'hôte du serveur:	Entrez l'adresse IP ou le nom d'hôte de l'appareil auquel le routeur enverra un message ICMP périodique (PING)
Intervalle des PING	Période entre deux pings consécutifs
Nombre d'essais	Entrer le nombre d'essais avant que la connexion PPP soit redémarrée.

NOTE

Si toutefois les problèmes persistent, il est possible de redémarrer l'alimentation du module cellulaire au lieu de relancer uniquement la connexion.
Pour ce faire, modifier le paramètre `p_wan_gsm_ping_ctrl_power_reset` par SSH à l'aide de la commande `set_params`.

Commande pour l'activation du reset de l'alimentation

```
$ set_params p_wan_gsm_ping_ctrl_power_reset.0 true
```

1.3. Ethernet

Cette section s'applique aux routeurs ci-dessous :

IPL-E, IPL-EW, IPL-DEC, SIG-E, RAS-E, RAS-EC, RAS-EW, RAS-ECW.

Elle s'applique également aux routeurs IPL-A ou IPL-C lorsque vous souhaitez utiliser l'interface RJ5 N°1 comme interface WAN au lieu de l'interface ADSL (IPL-A) ou de l'interface cellulaire (IPL-C).

Accéder au menu ***Configuration > Interfaces WAN > Ethernet***

Configuration du port WAN Ethernet

Speed / Duplex	Sélectionnez 10 ou 100 Mb/s en Half ou Full duplex. Par défaut, on utilise la valeur `Autonégociation` qui permet à l'interface d'adapter le débit par rapport à l'équipement branché sur ce WAN.

Configuration IP du port Ethernet WAN

Type de connexion	• La valeur `Ethernet` est la valeur par défaut. Elle doit être sélectionnée lorsqu'un autre routeur connecté à l'interface Ethernet/WAN du routeur Etic Telecom est en charge du routage des trames IP vers Internet • La valeur `PPPoE` ne doit être sélectionnée que dans des cas particuliers. Lorsqu'elle est sélectionnée, le routeur établit une connexion PPP sur Ethernet vers un fournisseur de services par exemple. Elle est utile lorsqu'un modem, ne prenant pas en charge PPPoE, est connecté au port Ethernet WAN du routeur. • La valeur `Désactivée` permet de désactiver ce port.

Interface WAN

Paramètre	Ethernet	PPPoE
Priorité du WAN Ethernet Ce paramètre définit la priorité de l'interface lorsque plusieurs interfaces sont activées (Cellulaire & WAN Ethernet, par exemple). Le routeur utilisera comme interface ayant la valeur la plus élevée; l'autre interface sera utilisée comme chemin de secours.	✔	✔
Identifiant PPP et **Mot de passe PPP** Entrez le login et le mot de passe de la connexion PPP		✔
Obtenir une adresse IP automatiquement, **Adresse IP**, **Masque de sous réseau** & **Passerelle par défaut** Laissez cette option cochée si l'adresse IP sur l'interface WAN est attribuée par un serveur DHCP. Sinon, décochez cette option et entrez l'adresse IP, le masque de réseau et l'adresse de passerelle par défaut de l'interface WAN.	✔	
Obtenir les adresses des serveurs DNS automatiquement, **Adresse serveur DNS primaire** & **Adresse serveur DNS secondaire** Laissez cette option cochée si l'adresse IP du serveur DNS est attribuée par un serveur DHCP. Sinon, décochez cette option et saisissez les adresses IP des serveurs DNS.	✔	✔
Connexions OpenVPN sortantes à travers un proxy Cocher cette option pour configurer un serveur proxy. Ce serveur proxy sera utilisé pour les connexions OpenVPN sortantes qui sont attachées à l'interface `Ethernet WAN`.	✔	
Activer la translation d'adresse (NAT) Si cette option est sélectionnée, l'adresse IP source de toute trame IP provenant d'un périphérique connecté à l'interface LAN et acheminée vers l'interface WAN est remplacée par l'adresse IP WAN du routeur. **NOTE** Cocher cette option si un périphérique de l'interface LAN doit établir une connexion avec un périphérique connecté à Internet (serveur FTP, ...)	✔	✔
Activer le proxy ARP Le routeur agit comme un proxy ARP. Laisser cette option décochée	✔	

Paramètre	Ethernet	PPPoE
MTU de l'interface Maximum Transfer Unit, contrôle le plus gros paquet de données pouvant être transféré sans fragmentation, 1500 par défaut	✔	
Seulement 1 WAN connecté à la fois Case à cocher pour n'avoir qu'un seul WAN connecté à la fois	✔	✔

Ping de contrôle

Le routeur est capable d'envoyer périodiquement un message PING par l'interface WAN vers une machine particulière. Si le PING répond, cette interface WAN est déclarée active et garde sa priorité. Si le message PING ne reçoit pas de réponse, cette interface WAN est désactivée.

Activer le PING de contrôle	Activer ou désactiver la fonction de contrôle PING
Adresse IP du serveur	Adresse IP de la machine à laquelle le PING est envoyé
Intervalle des PINGs	Laps de temps entre deux pings
Nombre d'essais	Nombre d'échecs de messages PING avant de désactiver l'interface WAN

1.4. Wi-Fi

Cette section s'applique aux routeurs ci-dessous:

IPL-EW, IPL-AW, IPL-CW, RAS-EW, RAS-ECW

NOTE Le scanner Wi-Fi permet de détecter les réseaux Wi-Fi aux alentours du routeur. Pour utiliser le scanner Wi-Fi, accéder au menu ***Diagnostic*** > ***Outils*** > ***Scans Wi-Fi***.

Configurez l'interface Wi-Fi en tant que client pour accéder à Internet

Accéder au menu ***Configuration*** > ***Interfaces WAN*** > ***Wi-Fi***. Ensuite, cochez la case **Activer le WAN Wi-Fi**.

Profils de connexion

Un tableau contient les différents profils Wi-Fi sur lesquels le routeur peut se connecter.

Activer	Permet d'activer ou de désactiver un profil de connexion

Rechercher les réseaux disponibles	Un bouton `Scanner` permet d'obtenir la liste des SSID vus par le produit ainsi que le niveau de signal en dBm pour chacun d'entre eux.
Nom du réseau (SSID)	Entrez le nom attribué au réseau Wi-Fi auquel le routeur doit se connecter. **CAUTION** Le SSID est sensible à la casse.
Authentification	Sélectionnez `WPA` ou `WEP` ou `Aucun` en fonction de la configuration du point d'accès.
Clé pré-partagée	Entrez la clé WPA ou WEP en fonction de la configuration du point d'accès.

Configuration IP WAN Wi-Fi

Priorité du WAN Wi-Fi	Ce paramètre définit la priorité de l'interface lorsque plusieurs interfaces sont activées (Cellulaire & WAN Ethernet, par exemple). Le routeur utilisera comme interface ayant la valeur la plus élevée; l'autre interface sera utilisée comme chemin de secours.
Obtenir une adresse IP automatiquement, **Adresse IP**, **Masque de sous réseau** & **Passerelle par défaut**	Laissez cette case cochée si l'adresse IP sur l'interface WAN est attribuée par un serveur DHCP. Sinon, décochez cette case et saisissez l'adresse IP, le masque de réseau et l'adresse de passerelle par défaut.
Obtenir les adresses des serveurs DNS automatiquement, **Adresse serveur DNS primaire** & **Adresse serveur DNS secondaire**	Laissez cette case cochée si les adresses IP des serveurs DNS sont attribuées par un serveur DHCP. Sinon, décochez cette case et saisissez les adresses IP des serveurs DNS.
Activer la translation d'adresse (NAT)	Si cette option est sélectionnée, l'adresse IP source de toute trame IP provenant d'un périphérique connecté à l'interface LAN et acheminée vers l'interface WAN est remplacée par l'adresse IP WAN du routeur. **NOTE** Cochez cette case si un appareil de l'interface LAN doit établir une connexion avec un appareil connecté à Internet (serveur FTP, ...)
Activer le proxy ARP	Le routeur agit comme un proxy ARP. Laisser cette option décochée

Activer sur fermeture de l'entrée TOR	Démarre le WAN Wi-Fi lorsque l'entrée TOR passe à l'état ON.

2. INTERFACES LAN

Les interfaces LAN (Local Area Network) sont les interfaces qui interconnectent les équipements au sein d'une zone limitée telle qu'une usine, une machine, un bâtiment.

2.1. Switch Ethernet

L'interface LAN se compose de 1 à 4 connecteurs Ethernet 10/100 BT RJ45 commutés.

Les chapitres suivants vous aideront à configurer l'interface LAN.

2.2. Ethernet et IP

Accéder au menu ***Configuration > Interface LAN > Ethernet et IP***

Réseau LAN

Adresse IP & **Masque de sous réseau**	Une adresse IP fixe doit être attribuée à l'interface LAN du routeur. Il s'agit de `192.168.0.128` par défaut. **NOTE** Cette adresse IP est également l'adresse IP du serveur d'administration du routeur
Passerelle par défaut	Si un autre routeur est connecté au réseau LAN donnant accès à d'autres réseaux et agissant comme passerelle par défaut pour le routeur, entrez son adresse ici. **NOTE** Laissez ce champ vide si aucun autre routeur n'est connecté au réseau LAN

Accès à distance

Si les PC des utilisateurs distants sont censés se connecter aux périphériques du réseau LAN, un pool d'adresses IP appartenant au réseau LAN doit leur être réservé.

CAUTION Les adresses réservées aux utilisateurs distants ne doivent pas être allouées à d'autres périphériques du réseau LAN.

Gestion automatique des adresses IP des utilisateurs distants	Si cette option est cochée, le routeur alloue automatiquement une adresse IP inutilisée du réseau LAN à un utilisateur distant lorsqu'il se connecte

Début de la plage d'adresses IP & **Fin de la plage d'adresses IP**	Si les adresses ne sont pas allouées automatiquement, ce sont les adresses IP fixes qui peuvent être allouées aux utilisateurs distants. Ces adresses IP doivent appartenir au domaine LAN

Example 2. Configuration LAN

	Adresse IP	**Remarque**
Réseau LAN	192.168.12.0 / 24	De 192.168.12.1 à 192.168.12.254
Adresse IP du routeur	192.168.12.1	
Début de la plage d'adresses IP	192.168.12.2	Dans cet exemple, deux utilisateurs distants peuvent se connecter simultanément au réseau LAN ; l'un recevra l'adresse IP 192.168.12.2 et l'autre 192.168.12.3.
Fin de la plage d'adresses IP	192.168.12.3	
Adresses IP disponibles pour les périphériques du réseau LAN	192.168.12.4 à 192.168.12.254	

CAUTION

Soyez prudent avec les adresses IP utilisées par l'interface LAN lors de la configuration des VPNs.

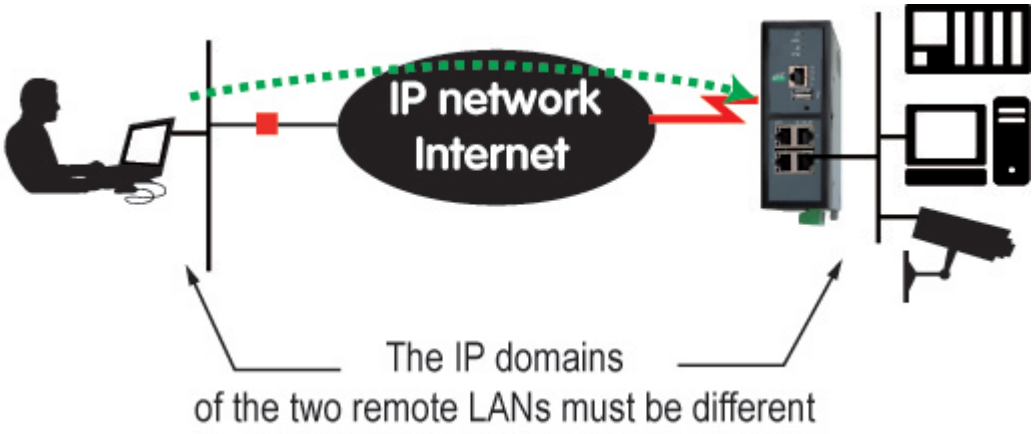


Figure 1. Cas 1: Connexion d'un utilisateur distant

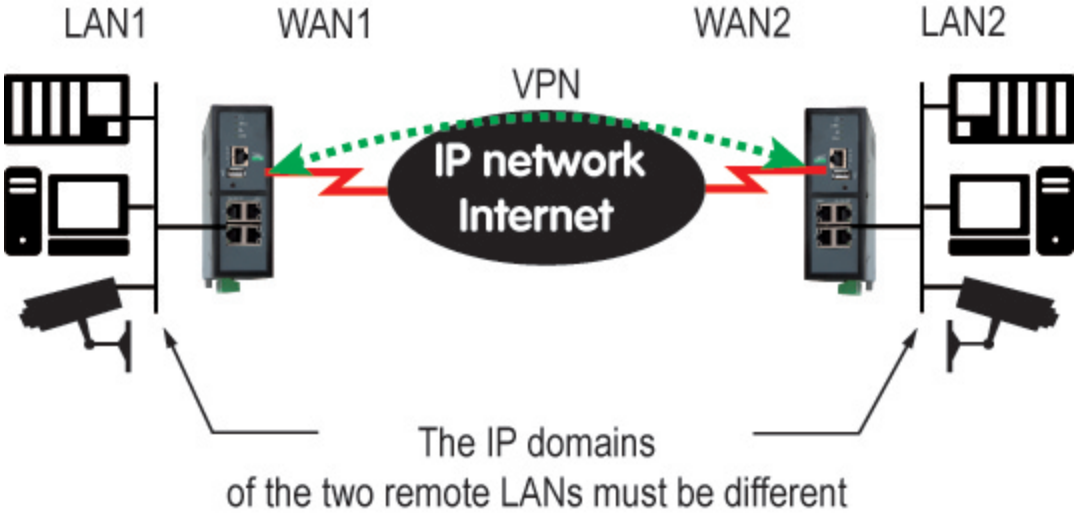


Figure 2. Cas 2 : VPN configuré entre 2 routeurs

Paramètres avancés

Configuration port 1/2/3/4	Désactiver un port LAN ou forcer un certain débit pour ce port, en Half ou Full Duplex. `Autonégociation` par défaut
Activer le relais DNS	Le routeur agit comme un DNS Forwarder. Activé par défaut
Serveur DNS primaire & **Serveur DNS secondaire**	Adresses IP des serveurs DNS à interroger
Activer le proxy ARP	Le routeur agit comme un proxy ARP. Désactivé par défaut
Adresse IP additionnelle & **Masque de sous réseau additionnel**	Ajouter une adresse IP à l'interface LAN, en plus de l'adresse principale
Désactiver ICMP redirect	Les paquets de redirection ICMP sont ignorés. Désactivé par défaut

2.3. Point d'accès Wi-Fi

Point d'accès Wi-Fi

Lorsque l'interface Wi-Fi est configurée comme point d'accès, les appareils connectés au routeur via ce réseau Wi-Fi appartiennent au réseau LAN.

Par conséquent, leur adresse IP appartient au domaine IP du réseau LAN.

Le module Wi-Fi peut être configuré soit comme un client, soit comme un point d'accès.

Configuration du point d'accès Wi-Fi

- Accéder au menu ***Configuration > Interface LAN > Point d'accès Wi-Fi***

SSID	Saisissez le nom attribué au réseau Wi-Fi auquel le routeur doit se connecter. **IMPORTANT** Le SSID est sensible à la casse.
Clé pré-partagée (mot de passe)	Saisissez la clé pré-partagée WPA (au moins 8 caractères)
Code pays	Les canaux RF alloués au service Wi-Fi ne sont pas les mêmes dans tous les pays. Voir Code pays. **WARNING** L'émission non autorisée sur des fréquences radio restreintes est passible de poursuites dans de nombreux pays.
Mode	Sélectionnez l'un des modes Wi-Fi disponible **NOTE** Le mode Wi-Fi sélectionné doit être saisi dans chaque client Wi-Fi (tablette, ...)
Activer ieee 802.11n (Haut débit)	Activer IEEE 802.11n haut débit. Désactivé par défaut
Canal	Entrez un numéro de canal. Il est préférable de sélectionner un canal inutilisé à l'emplacement où le routeur est installé **TIP** Utilisez le scanner Wi-Fi pour afficher les canaux utilisés par les réseaux Wi-Fi dans un emplacement (voir la section Diagnostics Scans Wi-Fi)
Activer sur fermeture de l'entrée TOR	Activer le point d'accès Wi-Fi uniquement lorsque l'état de l'entrée TOR est activé. Désactivé par défaut

Code pays

AD	Andorra
AE	United Arab Emirates
AL	Albania
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AW	Aruba
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados

BD	Bangladesh
BE	Belgium
BG	Bulgaria
BH	Bahrain
BL	Saint Barthélemy
BN	Brunei Darussalam
BO	Bolivia, Plurinational State of
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GD	Grenada
GE	Georgia
GL	Greenland
GR	Greece
GT	Guatemala

GU	Guam
HK	Hong Kong
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IR	Iran, Islamic Republic of
IS	Iceland
IT	Italy
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KH	Cambodia
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Macedonia, the former Yugoslav Republic of
MO	Macao
MT	Malta
MX	Mexico

MY	Malaysia
NL	Netherlands
NO	Norway
NP	Nepal
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SV	El Salvador
SY	Syrian Arab Republic
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad and Tobago
TW	Taiwan, Province of China
UA	Ukraine
US	United States
UY	Uruguay

UZ	Uzbekistan
VE	Venezuela, Bolivarian Republic of
VN	Viet Nam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

2.4. Liste des équipements

- Accédez au menu ***Configuration > Interface LAN > Liste des équipements***

Identification des équipements connectés au réseau LAN

Les équipements définis dans le produit sont censés être accessibles côté LAN.

Ils sont constitués d'un nom et d'une adresse IP pour les identifier, et sont le plus souvent utilisés pour accorder/restreindre l'accès aux opérateurs (utilisateurs distants).

Ajouter un équipement à la liste

- Cliquez sur le bouton **Ajouter**
- Attribuez un nom et une adresse IP à l'appareil

NOTE	Vous pouvez saisir l'adresse IP d'un équipement ou l'adresse IP d'un sous-réseau d'équipements

Example 3. Configuration de l'adresse IP de l'équipement

192.168.8.8 ou 192.168.8.8/29 (sous-réseau)

Nom d'hôte et nom de domaine

Dans ce menu, vous pouvez également modifier le nom d'hôte du produit. Deux champs doivent être remplis pour cela:

- **Nom du site**: nom d'hôte de votre produit
- **Nom du domaine** : nom du domaine dans lequel votre produit est censé se trouver

2.5. Serveur DHCP

Le routeur peut se comporter comme un serveur DHCP pour les appareils sur l'interface LAN.

Dans ce cas, un pool d'adresses doit être réservé ; les adresses du pool sont automatiquement distribuées aux périphériques du LAN agissant comme clients DHCP.

Les adresses du domaine LAN qui n'appartiennent pas à ce pool peuvent être attribuées comme adresses IP fixes à des périphériques particuliers.

NOTE	De nombreux périphériques de bureau Wi-Fi comme les tablettes ou les smartphones ne prennent pas en charge une adresse IP fixe.

Accéder au menu ***Configuration > Interface LAN > Serveur DHCP***

Configuration DHCP

Début de la plage d'adresses IP & **Fin de la plage d'adresses IP**	Entrez la première et la dernière adresse IP réservée au serveur DHCP.
Masque de sous réseau	Masque de sous réseau des adresses IP allouées
Passerelle par défaut	Si un autre routeur est connecté au réseau LAN donnant accès à d'autres réseaux, et faisant office de passerelle par défaut pour le routeur Etic Telecom, entrez l'adresse de ce routeur.
Serveur DNS primaire & **Serveur DNS secondaire**	Adresses IP des serveurs DNS à interroger

Associations DHCP MAC-IP

Vous pouvez lier une adresse IP à une adresse MAC, de sorte qu'un périphérique (identifié par son adresse MAC) se voit toujours attribuer la même adresse IP.

Nom du client	Nom permettant d'identifier le client (facultatif)
Adresse MAC du client	Adresse MAC du client *Example 4. MAC address* 12:34:56:78:9A:BC
Adresse IP du client	Adresse IP du client

3. CONNEXIONS VPN

Un VPN est un canal de communication sécurisé établi entre des appareils sur un réseau public ou privé. Le VPN utilise des techniques d'authentification et de chiffrement pour sécuriser la connexion et la protéger contre les écoutes clandestines ou la manipulation des données. Il s'agit du meilleur moyen d'interconnecter des réseaux via une connexion Internet.

Le routeur propose 2 technologies VPN : IPSec et OpenVPN.

3.1. IPSec

Un tunnel VPN IPSec permet de connecter deux réseaux de manière sécurisée et transparente : Chaque appareil du premier réseau peut échanger des données avec n'importe quel appareil de l'autre réseau.

- 15 connexions IPSec peuvent être établies par un `routeur IPL ou RAS`.
- 128 connexions IPSec peuvent être établies par un `routeur SIG`.
- 100 connexions IPSec peuvent être établies par une `SIG VM 100`.
- 1000 connexions IPSec peuvent être établies par une `SIG VM 1000`.

Principes IPSec

Le routeur qui initie le VPN IPSec est appelé l'initiateur ; l'autre est appelé le répondeur.

Un exemple des différentes adresses IP utilisées lors de la configuration est décrit par le schéma ci-dessous.

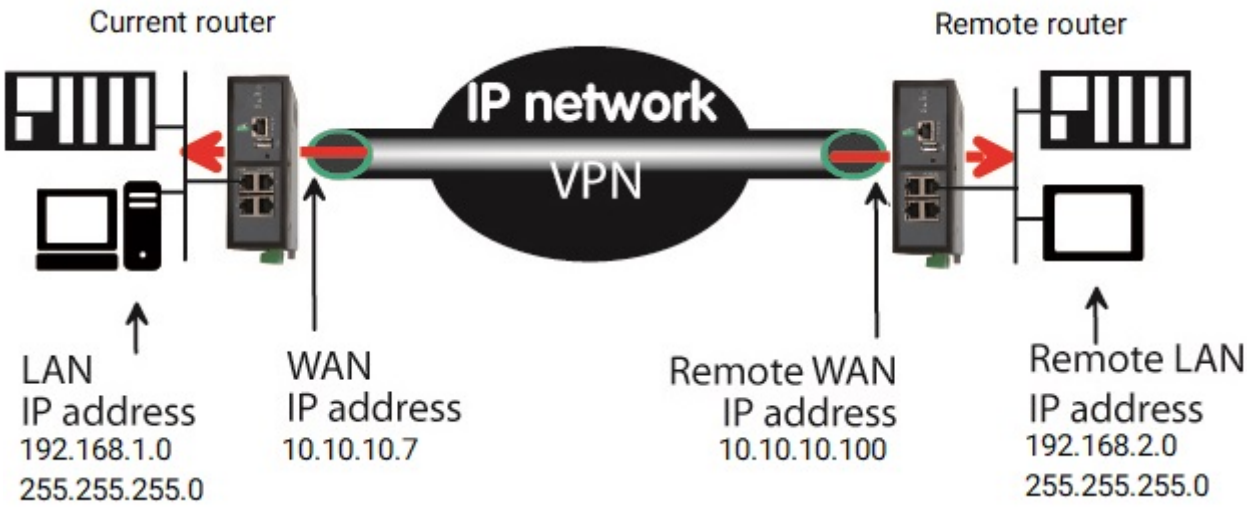


Figure 3. Schéma de connexion IPSec

Configuration de la connexion VPN IPSec

Acceder au menu ***Configuration > Réseau > Connexions VPN > Connexion IPSec***

Vous devez activer IPSec pour configurer les connexions. Le menu IPSec affiche des informations sur les connexions configurées.

Pour ajouter une connexion VPN IPSec, cliquez sur **Ajouter**.

Actif	Vous pouvez activer ou désactiver une connexion configurée
Paramètres avancés	Afficher les paramètres si une clé pré-partagée est utilisée et/ou des routeurs intermédiaires traduisent l'adresse IP source
Nom	Attribuer un nom unique à la connexion
Authentification par	Clé ou certificat pré-partagé
Connexion	Initiateur si le routeur actuel est censé initier le VPN
Activer le mode "route based"	`Route based` si activé / `Policy based` si désactivé. Voir le chapitre **Route based VS Policy based** pour plus d'explications.

Policy-based VS Route-based

Lorsque vous utilisez l'option IPSec `Policy-based`, le démon IPSec établit un tunnel uniquement pour les réseaux distants configurés. Une fois établi, tout le trafic correspondant à cette politique est chiffré et envoyé au routeur distant.

Lorsque vous utilisez l'option IPSec `Route-based`, le trafic envoyé au routeur distant est géré par les routes des réseaux. Cette option offre plus de flexibilité pour gérer de manière dynamique les réseaux accessibles via le tunnel.

Pour un simple tunnel de réseau à réseau, il est plus facile d'utiliser le mode `Policy-based` (mode `Route-based` désactivé)

IMPORTANT

En mode `Route-based`: Des routes statiques doivent être ajoutées dans le menu Routes statiques pour passer par le tunnel IPSec. Les champs **Adresse du réseau LAN distant** et **Masque du réseau LAN distant** doivent englober les routes statiques configurées.

Example 5. route-based

Pour associer les 2 routes statiques suivantes à un noeud IPSec :

- 10.1.21.0/24
- 10.1.30.0/24

Vous pouvez utiliser la configuration IPSec suivante :

- Adresse du réseau LAN distant : 10.1.16.0
- Masque du réseau LAN distant : 255.255.240.0

TIP

Pour envoyer tout le trafic du routeur via le tunnel (VPN comme passerelle par défaut):

1. Activez le mode `Route-based`
2. Définissez **Adresse du réseau LAN distant** sur 0.0.0.0/0 (doit être identique à celle du routeur homologue)
3. Définir une route statique pour atteindre le routeur distant (**Adresse IP WAN distante**/32 via la passerelle ou l'interface Internet)
4. Définir une route statique par défaut (0.0.0.0/0) via le VPN IPSec

Authentification IKE - Cas 1 : Utilisation d'un certificat

IMPORTANT Les deux certificats utilisés des participants doivent être délivrés par la même autorité

TIP Accéder au menu ***Configuration*** > ***Sécurité*** > ***Magasin de certificats*** pour ajouter des certificats personnalisés et des CRL.

Utiliser le certificat usine	Utiliser le certificat d'usine
Choisir un certificat personnalisé	Utiliser l'un de vos certificats personnalisés
Identité IKE locale	L'identité IKE doit être contenue dans le certificat, soit en tant que DN du sujet, soit en tant que subjectAltName. L'identité sera par défaut le DN du sujet du certificat si elle n'est pas spécifiée **NOTE** Les valeurs d'identité IKE sont spécifiées par la documentation StrongSwan. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Identité IKE distante	L'identité IKE doit être contenue dans le certificat distant, soit en tant que DN du sujet, soit en tant que subjectAltName. **NOTE** Les valeurs d'identité IKE sont spécifiées par la documentation StrongSwan. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Politique de révocation de certificat	Si aucune information sur la révocation du certificat entrant n'est disponible : `relaxed` l'acceptera, `strict` la refusera.

Authentification IKE - Cas 2 : Utilisation d'une clé pré-partagée

Utilisez une clé pré-partagée pour l'authentification ; elle doit être la même côté répondeur et initiateur.

Ces identifiants permettent de définir un VPN à clé pré-partagée même si des routeurs intermédiaires modifient l'adresse IP source. Le routeur recevant une trame IP vérifie l'ID IKE du routeur distant à la place de son adresse IP source.

Valeur clé	Valeur de la clé, elle doit être la même côté répondeur et initiateur.
Identité IKE locale (Paramètres avancés)	Identité IKE à utiliser pour le cycle d'authentification. Utilisé pour identifier le routeur actuel **NOTE** Les valeurs d'identité IKE sont spécifiées par la documentation StrongSwan. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Identité IKE distante (Paramètres avancés)	Identité IKE attendue pour le cycle d'authentification. Utilisé pour identifier le routeur distant **NOTE** Les valeurs d'identité IKE sont spécifiées par la documentation StrongSwan. https://docs.strongswan.org/docs/5.9/config/identityParsing.html

NOTE Le type d'ID IKE est spécifié par la documentation StrongSwan. https://docs.strongswan.org/docs/5.9/config/identityParsing.html

Section réseau

Réseau LAN local (Paramètres avancés)	Adresse IP du LAN local. Si vide, il s'agit du réseau local du routeur Ce champ est utilisé par les sélecteurs de trafic local à inclure dans l'association de sécurité CHILD *Example 6. Sur le schéma de connexion IPSec* 192.168.1.0

Masque du réseau LAN local (Paramètres avancés)	Masque de réseau du réseau LAN local. Si vide, il s'agit du LAN du routeur Ce champ est utilisé par les sélecteurs de trafic local à inclure dans l'association de sécurité CHILD *Example 7. Sur le schéma de connexion IPSec* 255.255.255.0
Adresse du réseau LAN distant	Adresse IP du réseau LAN distant Ce champ est utilisé par les sélecteurs de trafic local à inclure dans l'association de sécurité CHILD *Example 8. Sur le schéma de connexion IPSec* 192.168.1.0
Masque du réseau LAN distant	Masque de réseau du réseau LAN distant Ce champ est utilisé par les sélecteurs de trafic local à inclure dans l'association de sécurité CHILD *Example 9. Sur le schéma de connexion IPSec* 255.255.255.0
Adresse IP WAN distante	Adresse IP du routeur distant vers lequel le VPN doit se connecter *Example 10. Sur le schéma de connexion IPSec* 10.10.10.100

Section IKE Phase1

La phase 1 d'IKE effectue une authentification mutuelle entre les deux parties avec pour résultat final d'avoir des clés secrètes partagées. La même valeur doit être sélectionnée pour les deux routeurs.

Utiliser IKEv1 (Paramètres avancés)	Utiliser la version IKEv1. Cette version ne doit être utilisée que pour la compatibilité avec les appareils qui n'ont pas IKEv2.
Mode (Paramètres avancés)	Principal ou agressif. Le mode agressif ne doit être utilisé que pour la compatibilité avec les appareils qui l'utilisent. Le mode agressif n'est plus considéré comme sécurisé.

Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données. Valeur recommandée: Auto *Example 11. Valeurs possibles* AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, Auto
Algorithme d'authentification	Algorithme d'authentification. Valeur recommandée: Auto *Example 12. Valeurs possibles* MD5, SHA1, SHA-256, SHA-384, SHA-512, Auto
Groupe DH (Paramètres avancés)	Groupe Diffie-Hellman
Life time (Paramètres avancés)	Durée de vie de l'association IKE. Après cette période, l'étape 1 d'IKE est à nouveau exécutée.

Section IKE Phase 2

La phase 2 d'IKE a pour but de négocier les paramètres IPSec (paramètres généraux, chiffrement, durée de vie de l'association de sécurité...).
Le résultat de la phase 2 d'IKE est le tunnel chiffré entre les deux routeurs.

Protocole:	Protocole de transport IPSec. ESP assure l'authentification des routeurs et le chiffrement des données. L'ESP est désormais imposé sur les produits ETIC Telecom.
Algorithme de chiffrement	Valeur recommandée: Auto
Algorithme d'authentification	Valeur recommandée: Auto
PFS	Avec PFS désactivé, le matériel de chiffrement initial est créé pendant l'échange de clés dans la phase 1 de la négociation IKE. Dans la phase 2 de la négociation IKE, les clés de session de chiffrement et d'authentification seront extraites du matériel de clé initial. En utilisant PFS (Perfect Forwarding Secrecy), un matériel de clé entièrement nouveau sera toujours créé lors du changement de clé. Si une clé est compromise, aucune autre clé ne peut être dérivée à l'aide de ces informations
Groupe DH (Paramètres avancés et PFS activé)	Groupe Diffie-Hellman
Life time (Paramètres avancés)	Durée de vie de la clé phase 2

Section DPD

Un DPD est un message envoyé périodiquement de chaque point de terminaison à l'autre pour s'assurer que le VPN reste actif

Périodicité des messages "DPD keepalive"	Durée entre deux de ces requêtes
Délai de détection de perte de connexion	Durée maximale pendant laquelle une connexion VPN restera établie si aucun trafic ou aucun message de maintien en activité DPD n'est reçu du point distant
Lier le VPN au WAN :	Lier un VPN à un WAN afin que la connexion soit établie uniquement via ce WAN. L'option `Tous` peut ne pas fonctionner avec IKEv1.
Démarrer sur évenement	Le VPN démarre sur un événement spécifique. S'il est désactivé, le VPN est établi à la mise sous tension.
Démarrer seulement lorsque	Événement qui démarrera la connexion VPN *Example 13. Valeurs possibles* WAN cellulaire connecté, WAN cellulaire déconnecté, WAN Ethernet connecté, WAN Ethernet déconnecté, Entrée TOR ouverte, Entrée TOR fermée, aucun VPN connecté

3.2. OpenVPN

Un tunnel OpenVPN permet de connecter deux réseaux de manière sûre et transparente: Chaque appareil du premier réseau peut échanger des données avec les appareils du second réseau.

- 15 connexions OpenVPN entrantes + 15 connexions sortantes + 2 serveurs peuvent être définis pour un `routeur IPL ou RAS`.
- 128 connexions OpenVPN entrantes + 128 connexions sortantes + 4 serveurs peuvent être définis pour un `routeur SIG`.
- 100 connexions OpenVPN entrantes + 100 connexions sortantes + 4 serveurs peuvent être définis pour un `SIG VM 100`.
- 1000 connexions entrantes + 1000 sortantes OpenVPN + 4 serveurs peuvent être définis pour un `SIG VM 1000`.

Pour configurer les connexions OpenVPN, accéder au menu ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***OpenVPN***

Principes OpenVPN

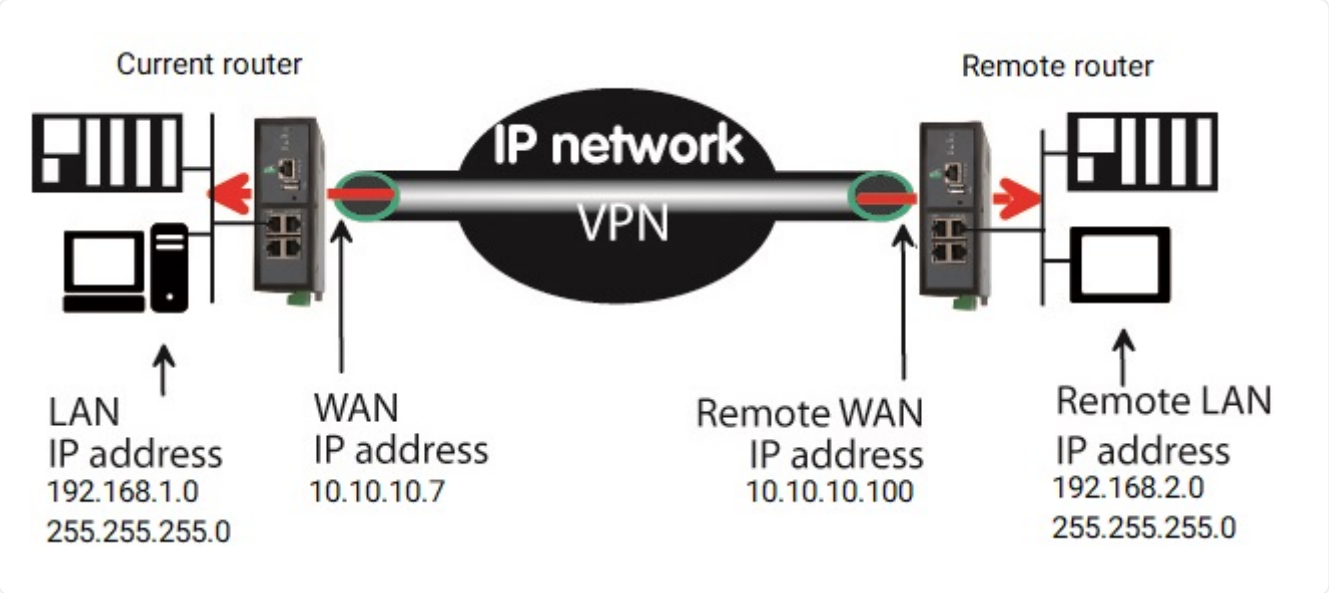
Le routeur qui initie la connexion est appelé le client VPN. Il configure une connexion sortante.

Le routeur qui reçoit la connexion est appelé le serveur VPN. Il configure les connexions entrantes.

Le routeur peut faire à la fois client VPN et serveur VPN.

Le domaine IP du LAN du client et du LAN du serveur doivent être différent.

Example 14. Connexion OpenVPN



Serveur OpenVPN

Si le routeur est configuré comme serveur VPN, cela signifie que le routeur doit recevoir au moins une connexion entrante. La configuration doit être effectuée en deux étapes :

1. Configuration des paramètres des serveurs OpenVPN
2. Configuration des connexions entrantes

Client OpenVPN

Si le routeur est configuré comme client VPN, l'installation consiste uniquement à configurer la connexion sortante.

Serveur

Sélectionnez le bouton **Ajouter** situé juste en dessous du tableau des serveurs VPN

IMPORTANT	Les certificats utilisés par chaque participant doivent être délivrés par la

même autorité

Consultez le menu ***Configuration*** > ***Sécurité*** > ***Magasin de certificats*** pour ajouter des certificats et des CRL personnalisés.

Actif	Activer ou désactiver une connexion
Nom	Nom unique de la connexion
Numéro de port	Numéro de port du protocole de transport **CAUTION** Le port doit être différent de celui utilisé par les serveurs d'accès distant
Protocole	UDP ou TCP
Périphérique réseau virtuel	TUN ou TAP. **NOTE** • TUN: Les données VPN sont envoyées sur la couche réseau (L3) • TAP: Les données VPN sont envoyées via la couche liaison de données (L2)
Utiliser le certificat usine	Utiliser le certificat d'usine
Choisir un certificat personnalisé	Utiliser un certificat personnalisé
Adresse réseau VPN & **Masque réseau VPN**	Le serveur OpenVPN attribue automatiquement une adresse IP au routeur client VPN. Laissez les valeurs par défaut 172.16.0.0 et 255.255.0.0 **CAUTION** Cette adresse IP VPN ne doit pas être confondue avec l'adresse IP de l'interface WAN.
Délai de détection de perte de connexion	Définit la période des messages de contrôle Un message de contrôle (également appelé message Keep-alive) est envoyé périodiquement par le serveur VPN pour s'assurer que le VPN doit rester actif. En conséquence, il définit la durée maximale pendant laquelle une connexion VPN restera établie avant d'être supprimée si aucune réponse au message de contrôle VPN n'est reçue du routeur distant. **CAUTION** La valeur doit être sélectionnée avec soin; si le VPN a été supprimé, pour une raison quelconque, le routeur attendra pendant cette période avant de relancer le VPN.
Délai de retransmission	Durée pendant laquelle le serveur attendra la réponse au message de contrôle de maintien en vie avant de le répéter.

Chiffrement	Algorithme utilisé pour chiffrer les données *Example 15. Valeurs possibles* AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, Auto
Authentification	Algorithme d'authentification *Example 16. Valeurs possibles* MD5, SHA1, SHA-256, SHA-384, SHA-512
Diffie Hellman	Groupe Diffie Hellman
Activer le protocole TLSv1 (Seulement pour la compatibilité)	Utiliser la version 1 de TLS. Cette version ne doit être utilisée que pour la compatibilité avec les anciens appareils. Si non coché, la version TLS est 1.2 minimum.
Désactiver la compression	Désactiver la compression
Activer tls-auth	Activer tls-auth
Clé tls-auth	Clé pour tls-auth
Activer tls-crypt	Activer tls-crypt
Clé tls-crypt	Clé pour tls-crypt
Activer tls-crypt-v2	Activer tls-crypt-v2, ne peut pas être utilisé avec tls-crypt et tls-auth
Clé tls-crypt-v2	Valeur de clé pour le serveur tls-crypt-v2
Priorité du serveur	Métrique utilisée pour toutes les routes poussées
Pousse la route locale aux clients VPN	Si cette option est activé, le serveur diffuse aux clients la route vers le domaine IP de son réseau local (adresse IP LAN et adresse IP supplémentaire LAN s'il y en a une)
Pousse les routes statiques aux clients VPN	Si cette option est activé, le serveur diffuse aux clients les routes statiques qui ont été configurées dans le serveur VPN

Pousse les routes des clients	Il existe deux solutions pour permettre à un appareil connecté à un routeur client VPN d'échanger des données avec un autre appareil connecté à un autre routeur client VPN. • La première consiste à définir une route statique dans les deux routeurs clients VPN. Un appareil connecté à un routeur client VPN peut échanger des données avec un appareil connecté au réseau LAN du serveur VPN, mais pas avec un appareil connecté à un autre routeur client VPN. • La seconde consiste à sélectionner l'option **Pousse les routes des clients**. Le serveur VPN diffuse à tous les clients VPN la route vers chacun d'eux. De cette façon, chaque appareil du réseau peut échanger des données avec chaque autre appareil. La définition de routes statiques n'est plus nécessaire.
Première et deuxième route spécifique à pousser:	Ces paramètres permettent de diffuser des routes spécifiques vers les clients.
Afficher les paramètres avancés	Afficher les paramètres avancés
tun-mtu	Maximum Transmission Units (Maximum Transmission Units)
fragment	Activez la fragmentation interne des paquets afin qu'aucun paquet UDP supérieur à cette valeur en octets ne soit envoyé.
mssfix	Annoncer aux sessions TCP sur le tunnel qu'elles doivent limiter la taille de leurs paquets d'envoi de telle sorte qu'une fois qu'OpenVPN les a encapsulés, la taille du paquet UDP résultant qu'OpenVPN envoie à son homologue ne dépassera pas cette valeur en octets.

Connexion sortante

Une connexion sortante est une connexion initiée par le routeur actuel.

- Sélectionnez le bouton **Ajouter** situé juste en dessous du tableau Connexion sortante.

IMPORTANT	Les certificats utilisés par chaque participant doivent être délivrés par la même autorité

Accéder au menu ***Configuration*** > ***Sécurité*** > ***Magasin de certificats*** pour ajouter des certificats et des CRL personnalisés.

Actif	Activer ou désactiver une connexion
Nom	Nom unique de la connexion
Identifiant	Login configuré des deux côtés de la connexion

Mot de passe	Mot de passe configuré des deux côtés de la connexion
Adresse IP du serveur VPN	Adresse IP publique ou nom de domaine ou adresse DynDNS ou NoIP. Une liste d'adresses séparées par le caractère ';' peut être utilisée. Si le port n'est pas défini, le port saisi dans le champ **Numéro de port** sera utilisé *Example 17. Liste d'adresses* 10.1.35.210;10.1.35.210:2194;10.6.66.102;10.6.66.102:1200
Adresse IP du serveur VPN de backup	Adresse IP de secours en cas de panne du serveur principal. Comme dans **Adresse IP du serveur VPN**, une liste peut être utilisée
Numéro de port	Numéro de port du protocole de transport **CAUTION** Le port doit être différent de celui utilisé par les serveurs d'accès distant
Protocole	UDP ou TCP
Périphérique réseau virtuel	TUN ou TAP. **NOTE** • TUN: Les données VPN sont envoyées sur la couche réseau (L3) • TAP: Les données VPN sont envoyées via la couche liaison de données (L2)
Utiliser le certificat usine	Utiliser le certificat d'usine
Choisir un certificat personnalisé	Utiliser un certificat personnalisé
Chiffrement	Algorithme utilisé pour chiffrer les données *Example 18. Valeurs possibles* AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, Auto
Authentification	Algorithme d'authentification *Example 19. Valeurs possibles* MD5, SHA1, SHA-256, SHA-384, SHA-512
Lier le VPN à une interface spécifique	Attacher un VPN à un WAN afin que la connexion ne soit établie que via ce WAN.

Activer le protocole TLSv1 (Seulement pour la compatibilité)	Utiliser TLS version 1. Cette version ne doit être utilisée que pour la compatibilité avec les anciens appareils. Si non coché, la version TLS est 1.2 minimum.
Démarrer sur évenement	Le VPN démarre sur un événement spécifique. S'il est désactivé, le VPN est établi à la mise sous tension.
Démarrer seulement lorsque	Événement qui démarrera la connexion VPN. *Example 20. Valeurs possibles* WAN cellulaire connecté, WAN cellulaire déconnecté, WAN Ethernet connecté, WAN Ethernet déconnecté, Entrée TOR ouverte, Entrée TOR fermée, aucun VPN connecté
Envoyer une alarme sur connexion/déconnexion	Envoyer une alarme à chaque connexion/déconnexion
Afficher les paramètres avancés	Afficher les paramètres avancés
Activer tls-auth	Activer tls-auth
Clé tls-auth	Valeur de la clé pour tls-auth
Activer tls-crypt	Activer tls-crypt
Clé tls-crypt	Valeur de la clé pour tls-crypt
Activer tls-crypt-v2	Activer tls-crypt-v2, ne peut pas être utilisé avec tls-crypt et tls-auth
Clé tls-crypt-v2	Valeur de la clé pour le client tls-crypt-v2
Désactiver la compression	Désactiver la compression

Passer par un proxy

Si votre routeur est derrière un proxy sur le WAN Ethernet, vous devez connecter le VPN à l'interface `WAN Ethernet`.
Configurez ensuite les paramètres du proxy dans la page ***Configuration*** > ***Interfaces WAN*** > ***Ethernet*** (voir la section WAN Ethernet).

Connexion entrante

Une connexion VPN entrante est une connexion reçue par le routeur configuré comme serveur VPN.

- Pour créer une connexion entrante, sélectionnez le bouton **Ajouter** situé juste en dessous du tableau Connexion entrante.

Actif	Activer ou désactiver une connexion

Nom	Nom unique de la connexion
Identifiant	Login configuré des deux côtés de la connexion
Mot de passe	Mot de passe configuré des deux côtés de la connexion
Adresse du réseau LAN distant	Adresse IP du LAN distant *Example 21. Adresse IP* 192.168.2.0
Masque du réseau LAN distant	Masque réseau du LAN distant *Example 22. Netmask* 255.255.255.0
Nom commun	'Nom commun' du certificat actif du routeur distant. **NOTE** Vous pouvez récupérer le nom commun du certificat dans le magasin de certificats.

4. ACCÈS À DISTANCE

Fournir un service d’accès à distance sécurisé nécessite trois étapes:

1. La configuration de la connexion à distance
2. Créer un utilisateur
3. Créer un opérateur avec ses droits d’accès

4.1. Avantages d’une connexion d’accès à distance

Utiliser une connexion à distance pour accéder à une machine offre les avantages suivants:

Identification des utilisateurs distants

Le login, le mot de passe et éventuellement le certificat de l’utilisateur distant sont vérifiés lors de l’établissement de la connexion.

Droits d’accès sélectifs

Des droits d’accès individuels peuvent être attribués à chaque utilisateur distant. L’utilisateur ne peut accéder qu’aux appareils du réseau ainsi autorisés.

Connexion transparente

Une fois la connexion à distance lancée, l’utilisateur distant reçoit automatiquement une adresse IP du réseau.

Chiffrement des données

Les données sont chiffrées de bout en bout.

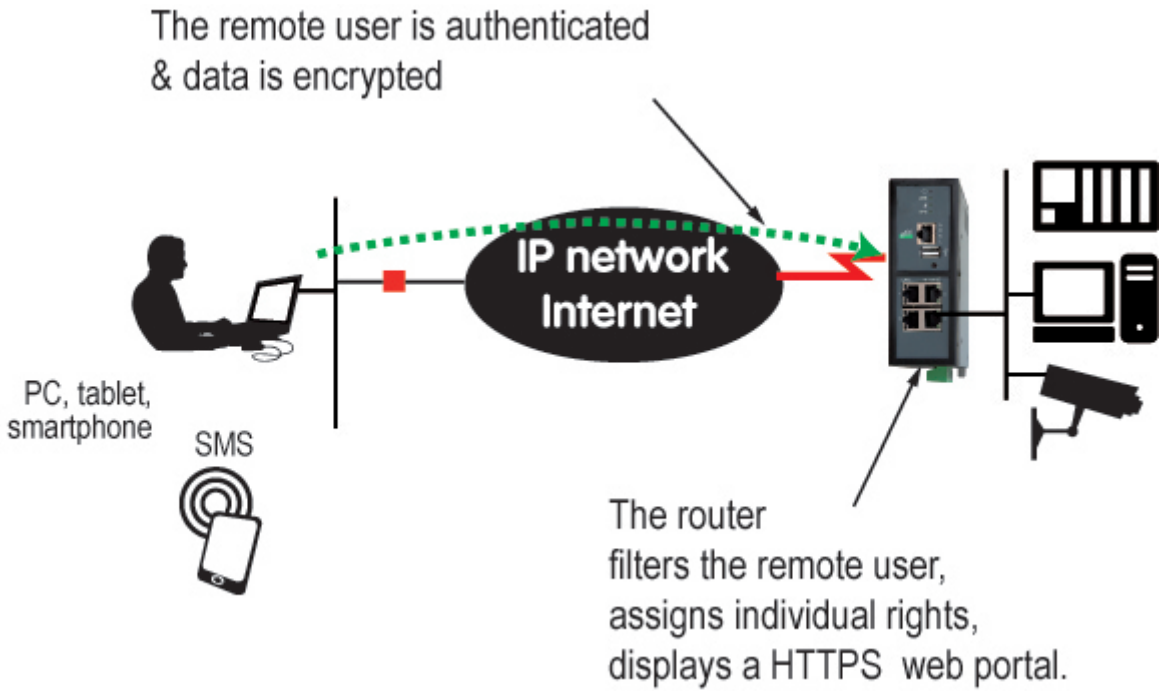


Figure 4. Chiffrement des données des accès distants

PC, tablette, smartphone

Les solutions apportées par le Routeur conviennent aussi bien aux PC ou tablettes Windows qu'aux smartphones (Android ou IOS).

4.2. Types de connexions d'accès à distance

Quatre types de connexions d'accès à distance peuvent être configurés. Ils peuvent tous être actifs en même temps.

	Authentification	Chiffrement
OpenVPN	Login/Password + Facultativement un certificat	Oui
PPTP	Login/Mot de passe	Oui
L2TP/IPSec	Login/Password + Clé pré-partagée ou certificat	Oui
HTTPS	Login/Mot de passe	Oui

La connexion HTTPS est principalement dédiée à l'accès distant sécurisé. Par exemple pour accéder à des pages HTML embarquées dans des PC de supervision, des IHM ou des automates; elle est décrite dans le chapitre suivant.

Lorsqu'un utilisateur distant établit une connexion, quel que soit son type, son identité est vérifiée (Login/Mot de passe).

4.3. Utilisateur distant OpenVPN

- Accéder au menu ***Configuration > Accès distant > Moyens d'accès***

Côté PC distant, on peut utiliser un client OpenVPN standard ou, si le PC fonctionne sous Windows, le logiciel M2Me_Client qui est simple à installer, configurer et utiliser.

Configurer la connexion OpenVPN

Sélectionnez l'option **Activer OpenVPN (OpenVPN)**

Numéro de port	Numéro de port utilisé
Protocole	UDP ou TCP **CAUTION** Assurez-vous que la combinaison Protocole + Numéro de port est utilisée uniquement par ce VPN. Elle doit être différente de celles prévues pour les PC.
Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données
Algorithme de hachage	Algorithme d'authentification
Activer le protocole TLSv1	Utilise TLS version 1. Cette version ne doit être utilisée que pour des raisons de compatibilité avec les anciens appareils. La version TLS est 1.2 minimum si elle n'est pas cochée.
Authentification des utilisateurs	**Login/mot de passe** ou **Login/mot de passe + Certificat**. Dans ce cas, le certificat du PC distant doit être saisi dans le menu Liste des opérateurs
Utiliser le certificat usine	Utiliser le certificat d'usine
Choisir un certificat personnalisé	Utiliser l'un de vos certificats personnalisés

4.4. Smartphones OpenVPN

- Accéder au menu ***Configuration > Accès distant > Moyens d'accès***

Il est possible de différencier la connexion d'un utilisateur distant depuis un PC et la connexion depuis un smartphone.

Configurer la connexion OpenVPN pour les smartphones

Sélectionnez l'option **Activer OpenVPN (OpenVPN) pour Smartphones**

Numéro de port	Numéro de port utilisé

Protocole	UDP ou TCP **CAUTION** Assurez-vous que la combinaison Protocole + Numéro de port est utilisée uniquement par ce VPN. Elle doit être différente de celles prévues pour les PC.
Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données
Algorithme de hachage	Algorithme d'authentification
Activer le protocole TLSv1	Utilise TLS version 1. Cette version ne doit être utilisée que pour des raisons de compatibilité avec les anciens appareils. La version TLS est 1.2 minimum si elle n'est pas cochée.
Authentification des utilisateurs	**Login/mot de passe** ou **Login/mot de passe + Certificat**. Dans ce cas, le certificat du PC distant doit être saisi dans le menu `Liste des opérateurs`
Utiliser le certificat usine	Utiliser le certificat d'usine
Choisir un certificat personnalisé	Utiliser l'un de vos certificats personnalisés

4.5. PPTP et L2TP/IPSec

- Accéder au menu ***Configuration > Accès distant > Moyens d'accès***

Connexion PPTP

WARNING L'utilisation de PPTP n'est plus recommandée en raison de problèmes de sécurité sur le protocole.

Sélectionnez l'option **Activer PPTP**

Si le PC distant est sous Windows, sélectionnez uniquement l'option `MS-CHAP V2`.

Connexion L2TP/IPSec

Sélectionnez l'option **Activer L2TP/IPSec**

Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données
Algorithme de hachage	Algorithme d'authentification
Authentification par	`Clé pré-partagée` ou `Certificat client`, dans ce cas, le certificat du PC distant doit être saisi dans le menu Liste des opérateurs.

4.6. Authentification multifacteur

Lors de l'authentification des opérateurs, le routeur vérifie le login et le mot de passe. Mais il peut également vérifier d'autres paramètres pour avoir une authentification multifacteur (MFA).

Login / Mot de passe + Certificat

Pour l'authentification avec login, mot de passe et certificat, le certificat de l'utilisateur est vérifié en suivant ces étapes :

1. Tout d'abord, il vérifie si l'opérateur a un CN de certificat (nom commun) dans sa description d'utilisateur
2. S'il existe un CN spécifié pour cet opérateur, le certificat entrant doit avoir le CN spécifié, sinon l'opérateur est rejeté
3. Si aucun CN n'est spécifié pour cet opérateur, il vérifiera dans la `Liste des certificats autorisés` (voir chapitre ci-dessous), le CN du certificat entrant doit être présent dans la liste, si ce n'est pas le cas, l'opérateur est rejeté

Liste des certificats autorisés

Dans le menu ***Configuration*** > ***Accès distant*** > ***Liste des opérateurs***

Actif	Activer ou désactiver un certificat
CN autorisés	Common name d'un certificat appartenant à un opérateur *Example 23. Common name* my_cert_cn
Commentaire	Commentaire pour savoir à quoi correspond ce certificat

5. M2ME_CONNECT

Tous les routeurs RAS sont concernés par cette section. Elle s'applique également à tous les autres routeurs, uniquement si l'option M2Me a été activée.

5.1. Description de M2Me_Connect

Le service M2Me_Connect simplifie la connexion d'un PC distant à une machine via Internet. C'est une solution lorsqu'une connexion directe PPTP ou OpenVPN est impossible.

Prenons l'exemple d'une machine constituée de plusieurs appareils formant un "réseau de machines" et connectée à un réseau d'entreprise via un routeur. Supposons qu'un expert souhaite se connecter à un ou plusieurs de ces appareils pour aider à leur réparation ou à la mise à jour d'un firmware.

La solution la plus simple serait d'établir une connexion à distance entre le PC distant et le routeur via le réseau de l'entreprise, l'accès Internet existant dans l'entreprise et Internet.

Plusieurs raisons rendent cette connexion difficile voire impossible, mais la principale est une raison de sécurité : il n'est généralement pas permis d'établir une connexion entrante depuis un PC connecté à Internet vers un appareil tel qu'un routeur connecté à l'intérieur d'un réseau d'entreprise.

Le service M2Me_Connect permet de contourner ce problème :

- Le PC ne se connecte pas directement au routeur ; le PC et le routeur se connectent tous deux au service "M2Me_Connect".
- Une fois que les deux parties ont été authentifiées par le service M2Me_Connect avec leur propre certificat, un VPN OpenVPN est établi de bout en bout du PC au routeur.
- L'identité de l'utilisateur distant est vérifiée par le routeur et s'assure qu'il appartient à la liste d'utilisateurs autorisés stockée dans le routeur.
- Enfin, des droits d'accès individuels sont attribués à l'utilisateur distant en fonction de son identité.

Figure 5. VPNs M2Me

Le VPN peut être transporté en UDP ou en TCP.

TIP Une fois la connexion M2Me démarrée, la LED M2Me clignote.

IMPORTANT	La Clé de produit du routeur est requise par le logiciel M2Me du PC distant. Vous pouvez la retrouver depuis le menu ***À propos*** du routeur.

5.2. Configurer la connexion M2Me

Pour donner accès à une machine aux utilisateurs distants via le service M2Me_Connect, il est nécessaire d'effectuer ces étapes:

1. Réaliser la configuration de la connexion M2Me décrite ci-dessous
2. Enregistrer au moins un utilisateur dans le menu ***Configuration*** > ***Sécurité*** > ***Utilisateurs***
3. Enregistrer au moins un opérateur dans le menu ***Configuration*** > ***Accès distant*** > ***Liste des opérateurs*** et attribuer des droits d'accès à ces opérateurs

Accédrer au menu ***Configuration*** > ***Accès distant*** > ***M2Me_Connect***.

Connexion au service M2Me_Connect

Cocher le paramètre **Actif** pour activer les paramètres de connexion M2Me.

Ports TCP & **UDP**	Entrer les ports UDP et TCP sélectionnés que le routeur utilisera pour monter le VPN M2Me. Le routeur va essayer de monter la connexion M2Me avec les ports UDP et TCP sélectionnés en commençant par UDP.
Accès direct à Internet (pas de proxy)	Si un serveur proxy filtre les connexions sortantes, décocher l'option et entrer les paramètres du serveur proxy
Type de proxy	Type de proxy du serveur (`HTTP`, `SOCKS5`)
Adresse et **Port**	Adresse IP et port du proxy
Authentification	Type d'authentification du proxy (`None`, `Basic`, `NTLM`) si le proxy est `HTTP`
Se connecter à la mise sous tension	Connection automatique au réseau M2Me à la mise sous tension
Connecter lorsque l'entrée TOR est fermée	Connection au réseau M2Me lorsque l'entrée TOR est fermée
Se connecter maintenant	Si le routeur ne se connecte pas automatiquement, appuyez sur ce bouton pour vous connecter au réseau M2Me

Connexion de bout en bout depuis le client PC M2Me

Configuration utilisée lorsque l'utilisateur final utilise un ordinateur.

Authentification des utilisateurs	`Login/Mot de passe` ou `Login/Mot de passe + Certificat`. Reportez-vous à Authentification multifacteur pour plus de détails
Utiliser le certificat usine	Utiliser le certificat usine pour la connexion M2Me de bout en bout
Choisir un certificat personnalisé	Certificat utilisé pour la connexion M2Me de bout en bout

Connexion de bout en bout depuis le client smartphone M2Me

Configuration utilisée lorsque l'utilisateur final utilise un smartphone ou une tablette.

Authentification des utilisateurs	`Login/Mot de passe` ou `Login/Mot de passe + Certificat`. Reportez-vous à Authentification multifacteur pour plus de détails
Utiliser le certificat usine	Utiliser le certificat usine pour la connexion M2Me de bout en bout
Choisir un certificat personnalisé	Certificat utilisé pour la connexion M2Me de bout en bout

6. ROUTAGE IP

6.1. Fonction de routage

Le routage permet de transférer des paquets IP d'un réseau à un autre. La destination des paquets et la table de **routage** du routeur permettent de déterminer vers quel réseau ils doivent être transférés, afin d'atteindre la destination finale.

Voici un exemple où le routage est utilisé:

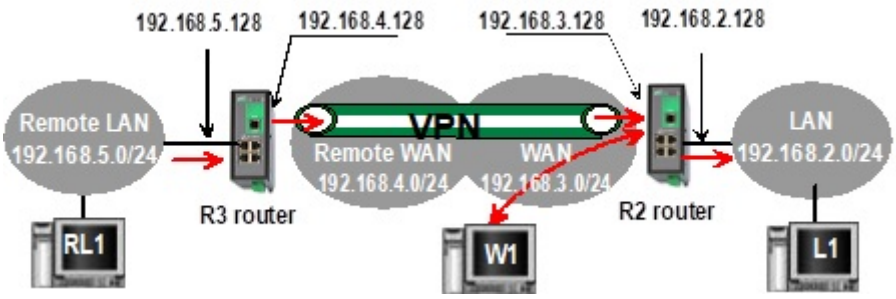


Figure 6. Routage de base

Une fois qu'une adresse IP a été attribuée au routeur R2 sur l'interface LAN et une autre sur l'interface WAN, le routeur est prêt à router les paquets:

- Entre les appareils connectés au réseau LAN distant comme RL1 et les appareils connectés au réseau LAN comme L1 via un VPN
- Entre les appareils connectés au réseau WAN comme W1 et les appareils connectés au réseau LAN comme L1

NOTE

- Les règles du pare-feu doivent être définies pour autoriser le transfert WAN vers LAN
- Une adresse de passerelle par défaut doit être renseignée dans chaque appareil des différents réseaux

6.2. Itinéraires statiques

Un routeur apprend dynamiquement les routes des réseaux qui lui sont directement connectés. Si vous voulez que votre routeur sache comment transférer un paquet pour une destination qui n'y est pas directement connectée, vous pouvez configurer des **routes statiques**.

Une route statique consiste à décrire un réseau de destination (adresse IP et masque réseau) et l'adresse IP du routeur voisin par lequel doivent transiter les paquets IP destinés à une destination.

Exemple de cas d'utilisation

Voici un exemple pour illustrer l'utilisation de routes statiques:

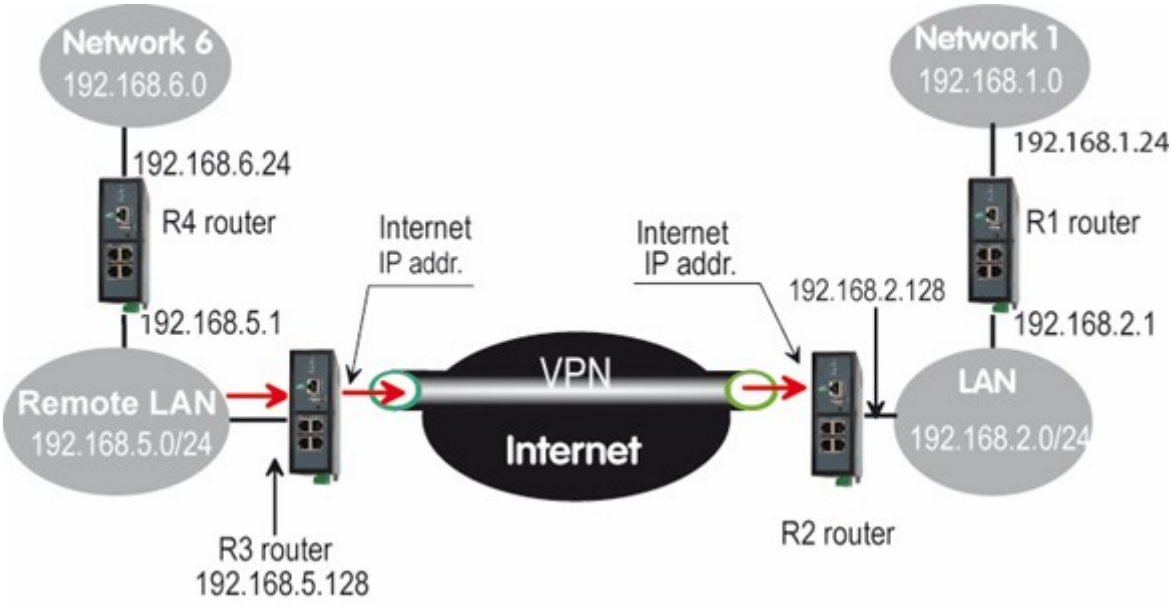


Figure 7. Exemple d'itinéraires statiques

Dans cet exemple, le routeur R2 est capable de router les paquets provenant du réseau `LAN` vers le réseau `WAN` de R2, ou vers le réseau `LAN distant`, sans aucune route statique. Ces routes ont été créées automatiquement par le routeur respectivement lorsque l'adresse IP WAN a été saisie et lorsque le VPN a été configuré.

Mais le routeur R2 n'est pas en mesure de router des paquets entre un périphérique appartenant au réseau `LAN` et un périphérique connecté au `Réseau 6`. Dans ce cas, il est nécessaire de saisir manuellement la route vers ce `Réseau 6`; cette route est appelée route statique.

Table 1. Tableau des routes statiques de R2, afin de pouvoir router vers les réseaux 1 et 6

Actif	Nom de la route	Adresse IP	Masque de réseau	Passerelle
Oui	Réseau 6	192.168.6.0	255.255.255.0	192.168.5.1
Oui	Réseau 1	192.168.1.0	255.255.255.0	192.168.2.1

Le même type de routes statiques doit être ajouté dans les autres routeurs afin qu'ils sachent comment transférer les paquets.

Configuration des routes statiques

Accéder au menu ***Configuration > Réseau > Routage > Routes statiques***

Dans ce menu, un tableau récapitule les routes statiques du produit, et si elles sont actives ou non.

Réseau de destination

Paramètres généraux des routes

Active	Activer ou désactiver cette route
Nom de la route	Nom pour vous permettre de décrire l'utilité de la route

Priorité	Priorité de la route (`1`:Haute - `255`:Faible)
Adresse IP & **Masque de sous-réseau**	Adresse IP et masque de réseau du réseau de destination

Chemin

Chemin par lequel doivent passer les paquets IP destinés à un réseau.

IMPORTANT	Choisissez une seule de ces options et laissez les autres vides lors de la création d'une route

Adresse IP de la passerelle	Adresse IP de la passerelle
Interface	Interface physique
Noeud OpenVPN entrant	Noeud OpenVPN (voir Connexion entrante)
Noeud OpenVPN sortant	Noeud OpenVPN (voir Connexion sortante)
Noeud IPSec	Noeud IPSec (voir IPSec)

6.3. Protocole RIP

RIP (« Routing Information Protocol ») est un protocole de routage qui permet à chaque routeur appartenant à un réseau d'acquérir les routes vers n'importe quel sous-réseau.

Le principe est le suivant :

Table de routage

Chaque routeur contient une table de routage.
Chaque entrée du tableau comprend l'adresse du sous-réseau de destination et l'adresse du routeur adjacent menant à ce sous-réseau.

Diffusion de la table de routage

Chaque routeur diffuse sa table

Mise à jour de la table de routage

Chaque routeur met à jour sa propre table en utilisant les tables reçues des autres.

Configuration du RIP

Accéder au menu ***Configuration*** > ***Réseau*** > ***Routage*** > ***RIP***.

Sélectionnez les options **Activer RIP sur le LAN** et **Activer RIP sur le WAN Ethernet**.

7. SUBSTITUTION D’ADRESSES

Chaque trame entrante ou sortante du routeur peut être traitée. Les fonctions NAT permettent de modifier les adresses des trames IP pour atteindre les équipements placés derrière le routeur.

7.1. Traduction d’adresse réseau (NAT)

Cette fonction s’applique aux trames IP émises par les appareils appartenant au réseau LAN et transmises au réseau WAN.

La fonction NAT consiste à remplacer l’adresse IP source de ces trames par l’adresse IP source du Routeur sur l’interface WAN.

Cette fonction est requise lorsqu’un appareil appartenant au réseau LAN doit se connecter à Internet (pour transmettre un fichier par FTP par exemple).

Pour activer la fonction NAT pour Ethernet par exemple. Selectionnez le menu ***Accueil*** > ***Configuration*** > ***Interfaces WAN*** > ***Ethernet***, puis cliquez sur **Activer la translation d’adresse (NAT)**.

7.2. Redirection de port

La redirection de port consiste à transférer des trames IP destinées à l’interface WAN du routeur IP vers un périphérique particulier de l’interface LAN à l’aide du numéro de port de destination.

Le critère de transfert est le numéro de port ; le numéro de port est utilisé comme champ d’adresse de destination supplémentaire.

Example 24. Exemple de redirection de port

Supposons que le PC nommé `W1` connecté au réseau WAN doive envoyer des trames au périphérique PLC1 connecté à un port Ethernet du routeur.

Si les tables de routage ne peuvent pas être enregistrées ni établir un VPN, la solution peut être d’utiliser la fonction Redirection de Port :

Lorsque W1 doit transmettre des trames à PLC1, il transmet les trames au routeur sur un numéro de port particulier.

Le routeur vérifie la trame, remplace l’adresse de destination par l’adresse IP de l’appareil sur l’interface LAN et modifie éventuellement le numéro de port.

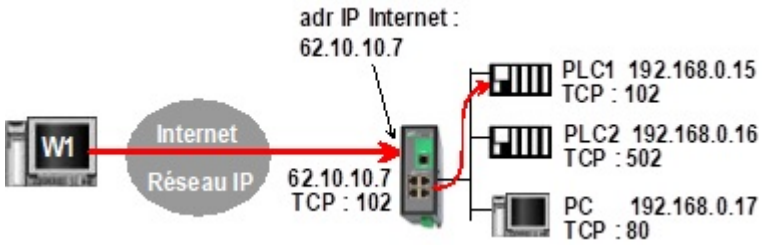


Figure 8. Exemple de redirection de port

Table 2. Exemple de configuration de redirection de port

IN	OUT	
Service entrant	Machine de destination	Service de destination
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

Configurer la redirection de port

Pour configurer une règle de redirection de port :

1. Accéder au menu ***Configuration > Réseau > Redirection de port***
2. Cliquez sur le bouton **Ajouter**,
3. Saisissez les caractéristiques des trames à transmettre :
   - **Adresse IP sources**
   - **Port**
4. Saisissez les caractéristiques de l'appareil vers lequel ces trames IP doivent être transmises :
   - **Machine de destination**
   - **Port**

7.3. NAT avancé

La fonction NAT avancée consiste à modifier les adresses IP source ou destination et le numéro de port des trames reçues par le Routeur sur son interface LAN ou WAN.

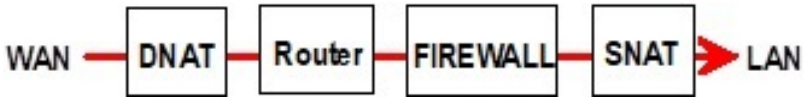
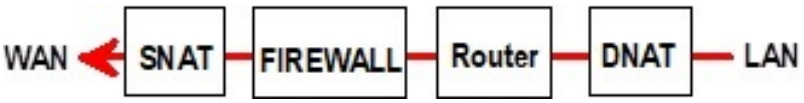
Il s'applique à toutes les trames reçues par le routeur sur l'une de ses deux interfaces à l'exception des paquets IP contenus dans les connexions d'un utilisateur distant.

Le NAT est composé de :

- La fonction DNAT qui consiste à remplacer le port de destination et l'adresse IP.
- La fonction SNAT qui consiste à remplacer l'adresse IP source.

Étant donné que les fonctions DNAT et SNAT modifient les adresses IP des paquets IP traités par le

routeur RAS-3G et que le pare-feu filtre ces trames, il est très important de comprendre dans quel ordre les différentes fonctions sont exécutées.

Direction	
WAN vers LAN	
LAN vers WAN	

Configuration

Pour définir les fonctions avancées de traduction d'adresse, accéder au menu ***Configuration*** > ***Réseau*** > ***NAT avancé***.

Créer une règle DNAT

1. Cliquez **Ajouter** sous la table **Règles DNAT**.
2. Sélectionnez **Active** pour activez la règle.
3. Saisissez les caractéristiques des trames IP qui doivent être modifiées par la règle DNAT :
   - **Adresse IP source** & **Adresse IP destination**
   - **Protocole** (TCP, UDP, ...)
   - **Port source** & **Port destination**
4. Entrez le nouveau port de destination et la nouvelle adresse IP.

Créer une règle SNAT

1. Cliquez **Ajouter** sous la table **Règles SNAT**.
2. Sélectionnez **Active** pour activez la règle.
3. Saisissez les caractéristiques des trames IP qui doivent être modifiées par la règle SNAT :
   - **Adresse IP source** et **Adresse IP destination** et **Protocole** (TCP, UDP, ...)
   - **Port source** & **Port destination** (champs en fonction du protocole sélectionné)
4. Entrez la **Nouvelle adresse IP source**.

7.4. NAT 1:1

NAT 1:1 (one-to-one) consiste à mapper l'adresse IP d'un périphérique sur le réseau LAN à une adresse IP appartenant à une interface WAN du routeur.

Cela signifie que lorsqu'un périphérique sur le WAN envoie des paquets à cette IP WAN, le routeur les renvoie à l'appareil sur le LAN avec son adresse IP LAN.

Sélectionnez le menu ***Configuration*** > ***Réseau*** > ***NAT 1:1***.

Activée	Activer ou désactiver la règle NAT
WAN sur lequel appliquer la règle	`WAN Ethernet` ou `WAN Wifi`
Adresse WAN à ajouter	Adresse IP ajoutée à l'interface WAN choisie
IP LAN à mapper sur le WAN	Adresse IP de l'appareil sur le LAN qui doit être accessible

CAUTION Les règles de pare-feu dont l'adresse de destination est l'IP WAN ou l'IP LAN d'une règle NAT 1:1 ne sont pas prises en compte

8. REDONDANCE VRRP

VRRP est un protocole qui permet à deux ou plusieurs routeurs sur le même réseau IP d'agir de manière redondante entre eux pour augmenter la disponibilité.

Le mécanisme est le suivant : Les routeurs placés en redondance ont chacun des adresses IP différentes, comme tout périphérique sur un réseau IP ; mais ils ont aussi une adresse IP commune appelée adresse IP virtuelle.

Cette adresse IP virtuelle et partagée est l'adresse IP qui doit être enregistrée dans différents périphériques réseau comme adresse de routeur par défaut.

De plus, un index de priorité (entre 1 et 255) est attribué à chacun des routeurs du groupe. Les routeurs du groupe élisent le routeur maître ; c'est celui qui a l'index de priorité le plus élevé. Il annoncera 255 comme index de priorité, tandis que les autres routeurs, que nous désignons comme routeurs de secours, resteront silencieux.

Le routeur maître prend en charge la fonction routeur ; il répond aux requêtes ARP envoyées par les périphériques réseau. De plus, il diffuse régulièrement un message de présence en utilisant l'adresse multicast 224.0.0.18 avec un numéro de protocole IP 112. Si le message n'est pas reçu, un nouveau routeur maître est élu.

NOTE Le routeur peut gérer ce protocole sur l'interface WAN et LAN.

8.1. Configuration VRRP

Accédez à la vue ***Configuration > Réseau > Redondance VRRP***

Activer VRRP sur le LAN	Cochez cette case pour activer VRRP sur l'interface LAN
Activer VRRP sur le WAN	Cochez cette case pour activer VRRP sur l'interface WAN
Id VRRP	Affecter un code d'identité au groupe de routeurs compris entre `1` et `255`. Tous les routeurs d'un même groupe doivent avoir le même code. Deux groupes différents ne peuvent pas avoir le même code
Adresse IP virtuelle	Adresse IP virtuelle commune à tous les routeurs du groupe. Tous les routeurs redondants doivent avoir la même adresse IP virtuelle
Priorité	Affecter un index de priorité au routeur compris entre `1` et `255`. L'index le plus élevé désigne le routeur ayant la priorité la plus élevée

Utiliser une adresse MAC virtuelle	Une adresse MAC virtuelle peut être associée à l'adresse IP virtuelle Ainsi, lorsqu'un périphérique réseau transmet une requête ARP, le maître du groupe VRRP répond toujours avec la même adresse MAC. L'adresse MAC utilisée est une adresse prévue à cet effet : 00-00-5E-00-01-XX, le dernier octet étant le numéro de groupe VRRP codé en hexadécimal

9. DÉLÉGATION D'AUTHENTIFICATION

9.1. Protection de l'authentification

Pour protéger le routeur des attaques par force brute, il existe un mécanisme permettant de bannir les utilisateurs pour l'authentification Web, SSH et VPN.

Ce mécanisme est configurable, il est basé sur le nombre de tentatives échouées et rend invalides toutes les tentatives d'authentification pour un utilisateur pendant une durée configurable.

Lorsqu'un utilisateur s'authentifie avec succès et n'a pas encore été banni, son compteur de tentatives se réinitialise à 0. Après avoir attendu la durée du bannissement, le compteur de tentatives se réinitialise à 0.

Accédez à la vue ***Configuration > Sécurité > Authentification***

Activé	Activer ce mécanisme. `Désactivé` par défaut
Nombre de tentatives ratées avant bannissement	Nombre de tentatives infructueuses pour un utilisateur avant qu'il ne soit banni. `10` par défaut
Durée du bannissement (minutes)	Nombre de minutes pendant lesquelles l'utilisateur restera banni. `10` par défaut

Un tableau est disponible à la vue > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Utilisateurs*** récapitulant les utilisateurs bannis de l'authentification, il est possible pour un Super administrateur de débannir un ou plusieurs utilisateurs de ce tableau grâce au bouton **Débannir l'utilisateur** situé juste en dessous du tableau.

9.2. Avertissement à l'authentification

Il est aussi possible d'afficher un message d'avertissement concernant l'utilisation du système afin de prévenir que l'accès réservé aux utilisateurs autorisés uniquement, que toute activité peut être surveillée et enregistrée, qu'une utilisation non autorisée est interdite et passible de sanctions.

Ce message est affiché sur les différentes interfaces d'authentification (Zone Administration, Zone Exploitation, Interface SSH)

Message d'avertissement avant l'authentification	Message à afficher sur les différentes interfaces d'authentification pour informer que l'accès est réservé aux utilisateurs autorisés uniquement.

9.3. Authentification déléguée

Etic Telecom fournit une fonctionnalité permettant à votre routeur de récupérer les utilisateurs depuis des serveurs d'authentification tels qu'Active Directory, FreeRADIUS ou OpenLDAP.

Dans les routeurs Etic Telecom, les utilisateurs sont divisés en 2 catégories : `Administrateurs`, qui

configurent les paramètres du routeur, et Opérateurs, qui accèdent au routeur via M2Me. Il y a donc 2 sections dans le menu de configuration pour l'authentification déléguée, une pour chaque catégorie.

Ce chapitre décrit la configuration à effectuer pour utiliser les utilisateurs de votre serveur sur le routeur, avec les droits et fonctions appropriés pour chacun d'eux.

Dans chaque section, vous avez la possibilité de mettre en cache les informations d'identification, de cette manière, si votre serveur est en panne, les utilisateurs peuvent toujours se connecter pendant un certain temps. Le cache est vidé au redémarrage et à l'arrêt du routeur.

NOTE	Concernant l'administration SSH déléguée, les administrateurs de votre serveur délégué devront s'authentifier deux fois lors de la première connexion. Les utilisateurs locaux avec le rôle de super-administrateur auront toujours un accès SSH au routeur.

Cas des Super Administrateurs locaux en mode délégué

Les utilisateurs locaux dotés du rôle de super-administrateur peuvent toujours se connecter au routeur avec leur compte local.

Si vous souhaitez refuser au super-administrateur local la connexion au routeur, vous pouvez désactiver le compte utilisateur lié au super-administrateur (voir la section Users).

9.4. Configuration de l'authentification EFM

Accédez à la vue ***Configuration*** > ***Sécurité*** > ***Authentification***. Le paramètre **Type d'authentification** doit être défini sur `EFM`.

Dans la section d'authentification pour les opérateurs, la case à cocher **Autoriser les connexions de secours** est disponible. Celle-ci permet aux utilisateurs définis localement comme Super Administrateur et Opérateur de s'authentifier lorsque l'EFM est indisponible.

9.5. Configuration de l'authentification RADIUS/TACACS+

Accédez à la vue ***Configuration*** > ***Sécurité*** > ***Authentification***. Le paramètre **Type d'authentification** doit être défini sur `RADIUS` ou `TACACS+`. Remplissez ensuite les paramètres de votre serveur.

Adresse IP du serveur ou nom d'hôte	Adresse IP ou nom d'hôte de votre serveur. **CAUTION** Assurez-vous que le routeur est capable d'effectuer la résolution DNS si vous utilisez un nom d'hôte.
Adresse IP ou nom d'hôte du serveur de sauvegarde	Adresse ou nom d'hôte de sauvegarde, au cas où le premier ne serait pas disponible. (Facultatif)

Port d'authentification	Port d'écoute de votre serveur RADIUS pour l'authentification. Le port par défaut est 1812.
Secret partagé	Secret partagé du serveur RADIUS.
Port du serveur	Port d'écoute de votre serveur TACACS+. Le port par défaut est 49.
Secret partagé	Secret partagé du serveur TACACS+.

Configurer les droits d'accès pour les administrateurs

Les administrateurs authentifiés via RADIUS ou TACACS+ disposent de droits d'accès configurables. Accédez à la vue ***Configuration*** > ***Accès distance*** > ***Groupes d'administrateurs***. Vous trouverez un tableau pour ajouter/supprimer/modifier des groupes.

Si vous souhaitez accorder l'accès aux administrateurs au routeur, vous devrez créer un groupe appelé `RADIUS_ETIC_TELECOM` pour RADIUS et `TACACS_PLUS_ETIC_TELECOM` pour TACACS+. Ce nom de groupe est conçu spécifiquement pour les administrateurs qui s'authentifient via RADIUS ou TACACS+ et en ajoutant/modifiant ce groupe, vous pouvez choisir le rôle de ces administrateurs.

Configurer les droits d'accès pour les opérateurs

Les opérateurs authentifiés via RADIUS ou TACACS+ ont des droits d'accès configurables, accédez à la vue ***Configuration*** > ***Accès distance*** > ***Groupes d'opérateurs***. Vous trouverez un tableau pour ajouter/supprimer/modifier des groupes.

Si vous souhaitez accorder l'accès aux opérateurs au routeur, vous devrez créer un groupe appelé `RADIUS_ETIC_TELECOM` pour RADIUS et `TACACS_PLUS_ETIC_TELECOM` pour TACACS+. Ce nom de groupe est conçu spécifiquement pour les opérateurs s'authentifiant via RADIUS ou TACACS+ et en ajoutant/modifiant ce groupe, vous pouvez choisir les droits d'accès.

9.6. Configuration de l'authentification LDAP

Accédez à la vue ***Configuration*** > ***Sécurité*** > ***Authentification***. Le paramètre **Type d'authentification** doit être défini sur `LDAP`. Remplissez ensuite les paramètres qui seront utilisés pour les requêtes vers votre serveur LDAP.

TIP Vous pouvez vérifier les journaux d'authentification LDAP dans le journal `Principal`

Adresse IP du serveur ou nom d'hôte	Adresse IP ou nom d'hôte de votre serveur. **CAUTION** • Assurez-vous que le routeur est capable d'effectuer une résolution DNS si vous utilisez un nom d'hôte. • Pour utiliser LDAPS, il peut être nécessaire de renseigner le nom d'hôte au lieu de l'adresse IP. *Example 25. Nom d'hôte du serveur* `monserveur.monentreprise.com`
Adresse IP ou nom d'hôte du serveur de sauvegarde	Adresse ou nom d'hôte de sauvegarde, au cas où le premier ne serait pas disponible. (Facultatif)
Port du serveur	Port d'écoute de votre serveur LDAP. Le port par défaut est 389.
DN du compte privilégié	Nom distinctif complet du compte LDAP utilisé pour effectuer les requêtes. (Les droits en lecture seule sur les branches nécessaires sont suffisants) *Example 26. DN du compte privilégié* `cn=admin,dc=monentreprise,dc=com`
Mot de passe du compte privilégié	Mot de passe du compte privilégié.
Type de serveur	Soit Active Directory, soit autre (OpenLDAP, etc...)
Domaine racine (Base DN) pour la recherche d'utilisateurs	Nom distinctif complet de la branche LDAP utilisée pour stocker les utilisateurs. (Les feuilles des utilisateurs doivent être directement en dessous) *Example 27. Domaine racine pour la recherche d'utilisateurs* `ou=utilisateurs,dc=monentreprise,dc=com`
Domaine racine (Base DN) pour la recherche de groupe	Nom distinctif complet de la branche LDAP utilisée pour stocker les groupes. (Les congés de groupe doivent être directement en dessous) *Example 28. Domaine racine pour la recherche de groupe* `ou=groupes,dc=monentreprise,dc=com`

Attribut utilisé pour identifier les utilisateurs	Attribut LDAP `utilisé dans le DN` (noms distinctifs) pour identifier les utilisateurs. *Example 29. Attribut utilisé pour identifier les utilisateurs* CN
Nom de domaine Active Directory	Nom de domaine (utilisé uniquement si le type de serveur est Active Directory) *Example 30. Nom de domaine* monentreprise.com
LDAP sur SSL	Utiliser ou non le protocole LDAPS **WARNING** LDAP sans SSL signifie que vos mots de passe sont visibles sur le réseau lors de l'authentification
Type de certificat	Certificat client ou certificat CA selon que le serveur LDAP nécessite une authentification mutuelle ou si seul le routeur doit l'authentifier
Certificat CA pour LDAPS	Choisissez un certificat dans la liste pour l'utiliser
Certificat pour LDAPS	Choisissez un certificat dans la liste pour l'utiliser

Les droits des utilisateurs qui s'authentifient via LDAP sont définis par leur appartenance à des groupes.

IMPORTANT Un utilisateur existant sur le serveur, mais ne disposant d'aucun groupe lui donnant des droits, n'aura pas accès au routeur.

Certains attributs sont vérifiés pour connaître l'appartenance des utilisateurs à des groupes. Sur l'objet utilisateur LDAP, l'attribut vérifié est `memberOf`. Sur l'objet groupe LDAP, les attributs vérifiés sont `member`, `memberUid` et `uniqueMember`.

Configurer les droits d'accès pour les opérateurs

Accédez à la vue ***Configuration > Accès distance > Groupes d'opérateurs***. Vous trouverez un tableau pour ajouter/supprimer/modifier des groupes. Pour chaque groupe, vous pouvez choisir les droits d'accès.

Configurer les fonctions pour les administrateurs

Accédez à la vue ***Configuration > Sécurité > Groupes d'administrateurs***. Vous trouverez un

tableau pour ajouter/supprimer/modifier des groupes. Vous pouvez ajouter le même groupe plusieurs fois si ce groupe a plusieurs rôles.

IMPORTANT	Le paramètre **Group name** est CASE-SENSITIVE et DOIT correspondre à l'attribut `CN` du groupe sur le serveur.

9.7. Différence entre Active Directory et les autres

Active Directory

Les connexions des utilisateurs qui s'authentifient via Active Directory sont leur `userPrincipalName`.

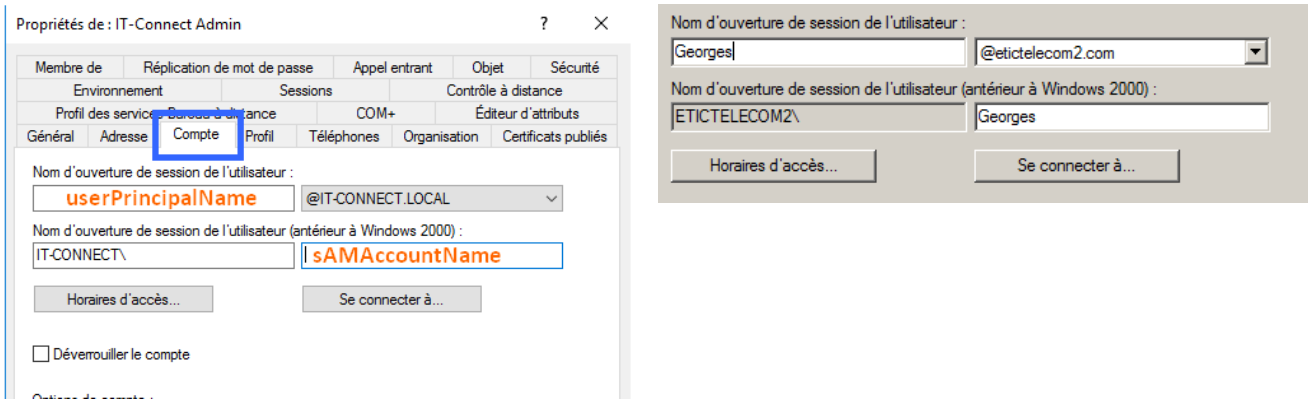


Figure 9. Configuration du serveur Active Directory

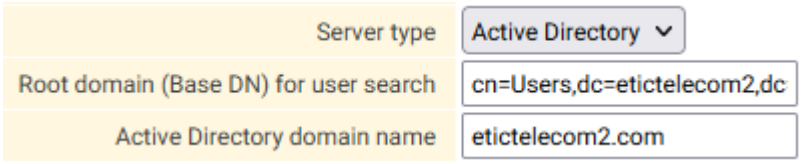


Figure 10. Configuration du routeur Active Directory

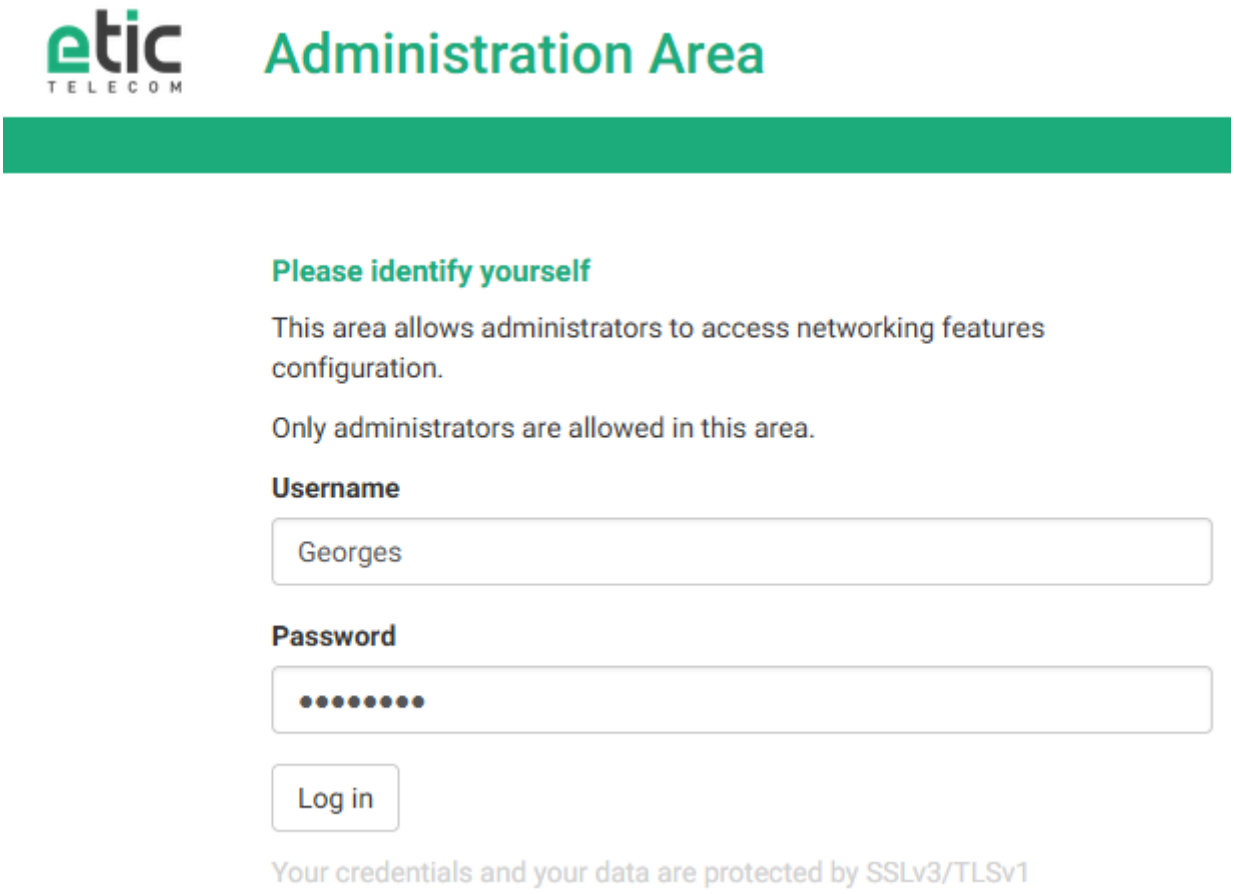


Figure 11. Connexion Web avec Active Directory

Autres

Les connexions des utilisateurs qui s'authentifient via d'autres types de serveurs, tels qu'OpenLDAP, sont les valeurs de l'attribut que vous avez défini dans la configuration du routeur, par exemple les valeurs de l'attribut `cn`.

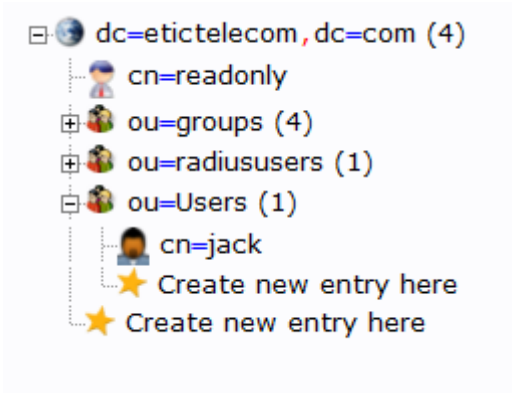


Figure 12. Configuration du serveur OpenLDAP

Figure 13. Configuration du routeur OpenLDAP

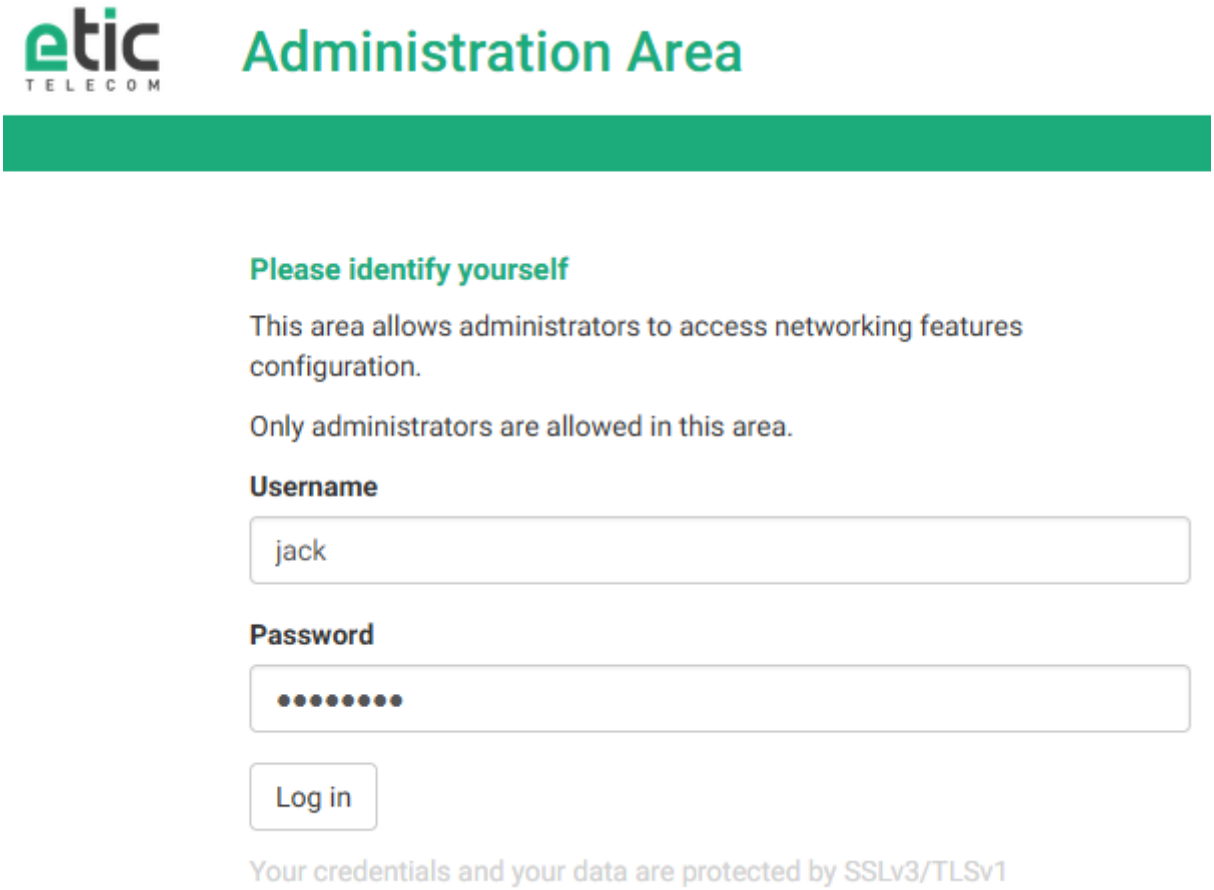


Figure 14. Connexion Web avec OpenLDAP

10. MAGASIN DE CERTIFICATS

10.1. Magasin de certificats

Etic Telecom fournit un magasin de certificats, vous permettant de gérer les certificats clients, les certificats des autorités de certification, les clés privées et les listes de révocation de certificats. Les programmes qui utilisent les informations de ce magasin de certificats sont OpenVPN, IPsec, LDAP, OPCUA, Syslog, FTP, MQTT, ...

Ce chapitre décrit comment configurer les certificats et les utiliser dans les routeurs.

NOTE	Le bundle CA, les certificats, les clés privées et la CRL ne sont **jamais** stockés dans les fichiers de configuration.

Paramètres d'usine

Le magasin de certificats contient toujours les certificats `factory_certificate_ca.crt` et `factory_certificate.crt` ainsi que la clé privée `factory_certificate.key`. Tous créés et signés par l'Infrastructure à clés publiques d'Etic Telecom pour identifier votre routeur sur les services proposés par Etic Telecom. Ils ne peuvent pas être supprimés.

10.2. Menu Magasin de certificats

Pour configurer le magasin de certificats, accéder au menu ***Configuration > Sécurité > Magasin de certificats***. Cette vue est divisée en 4 panneaux: Certificats CA, Certificats, Clés privées et CRL.

Ajout/Suppression

Dans ce menu, utilisez les boutons pour ajouter/supprimer des certificats x509, des clés privées et des CRL. Lorsque vous en ajoutez un dans le magasin de certificats, vous devez lui spécifier un nom, ce nom sera ensuite utilisé dans les autres menus pour y faire référence.

CAUTION	Les noms donnés aux certificats / clés privées / CRL doivent respecter certaines règles : 1. Être unique dans sa catégorie 2. Être adapté à un nom de fichier 3. Ne pas se terminer par `.rsa`, `.info` ou `.pub` pour les clés privées 4. Ne pas être utilisé par des certificats, des certificats CA et des clés pour les fichiers p12

L'ajout peut être effectué en important le fichier au format PEM.

Vous avez également la possibilité d'ajouter le contenu d'un fichier p12 en cliquant sur le bouton **Ajouter** du tableau des certificats. Le format d'importation doit être défini sur PKCS12 et vous pouvez choisir votre fichier p12 avec son mot de passe.

Clés privées

NOTE	L'importation au format PEM de clés privées cryptées n'est pas prise en charge par le routeur.

N'importez pas de clés privées dont la taille est trop petite pour OpenSSL, la plupart des fonctionnalités du routeur ne l'accepteront pas pour des raisons de sécurité.

Pour les clés privées, vous pouvez également les générer. Les types de clé que vous pouvez générer sont RSA de longueur 2048, 3072, 4096 ou ECDSA Prime256v1.

Demande de signature de certificat

Vous pouvez créer une demande de signature de certificat pour une clé spécifique. Sélectionnez la clé et cliquez sur **Faire une CSR**. Une page s'ouvrira vous permettant de spécifier les champs de votre CSR.

Ensuite, cliquez sur **Enregistrer**, et votre CSR s'affichera au format texte PEM. Il permet de signer un certificat pour une clé avec votre autorité de certification personnalisée.

Détails du certificat et de la CRL

Chaque tableau présente le détail des certificats, comme le nom commun du sujet (CN), le nom commun de l'émetteur et la date d'expiration du certificat. Pour les certificats clients, il est aussi indiqué si le certificat est lié à une clé privée ou non.

Il existe également un bouton **Afficher** pour les certificats pour afficher ses détails.

Pour chaque CRL, le menu affiche le nom commun de l'émetteur, la dernière mise à jour de la CRL et la prochaine mise à jour de la CRL.

10.3. Utilisation des certificats

Certaines fonctionnalités utilisent des certificats. Il y aura alors, dans l'interface de cette fonctionnalité, un paramètre qui vous permettra de choisir le certificat à utiliser.

Si cette fonctionnalité nécessite une authentification mutuelle, il faudra choisir un certificat client, si cela suffit à authentifier le serveur il y a la possibilité de choisir uniquement le certificat CA.

Pour les certificats clients, il est nécessaire d'avoir un certificat avec une clé privée ainsi que le certificat CA qui lui est lié.

TIP Si un certificat CA n'est pas auto-signé, vous pouvez concaténer chaque PEM de la CA intermédiaire à la CA racine lors de l'importation du certificat CA. De cette façon, toute la chaîne CA est disponible lors de l'utilisation de ce certificat.

TIP Pour diagnostiquer des problèmes, vous pouvez vérifier sur l'interface du magasin de certificats si votre certificat client a un lien vers une clé privée, et si l'émetteur du certificat client est dans la liste des certificats CA.

Example 31. LDAPS a besoin d'un certificat client, d'un certificat CA et d'une clé privée.

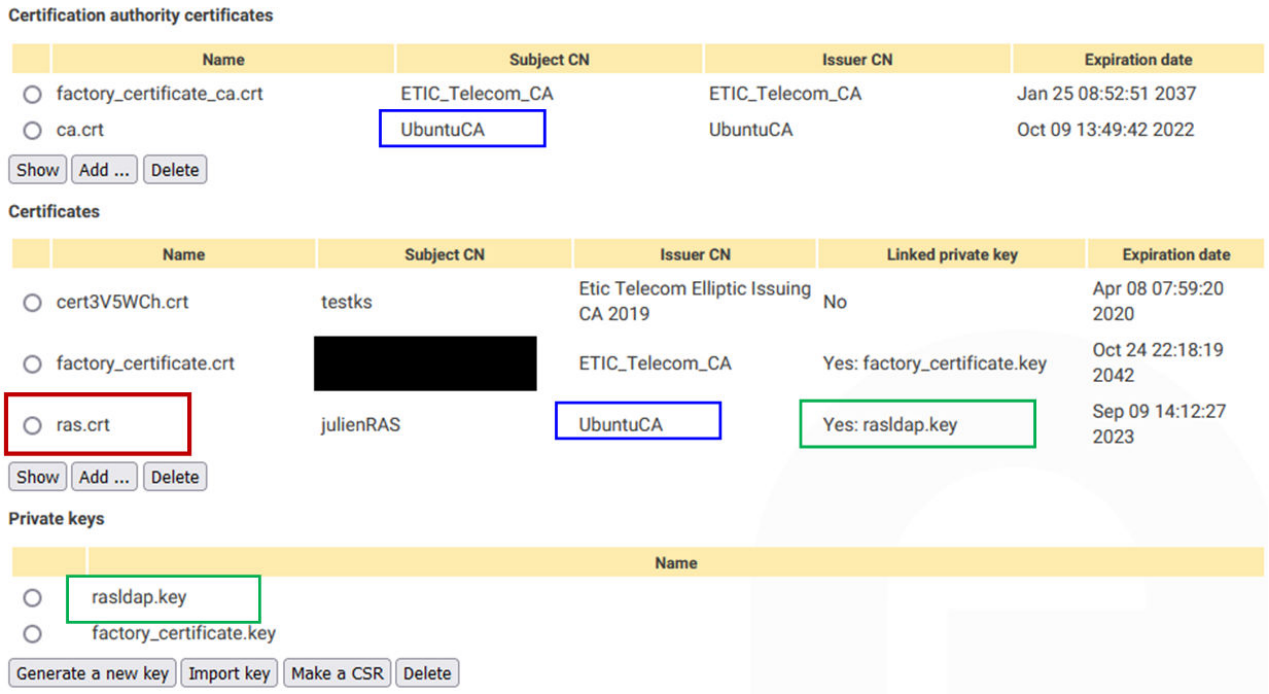


Figure 15. Configuration du magasin de certificats

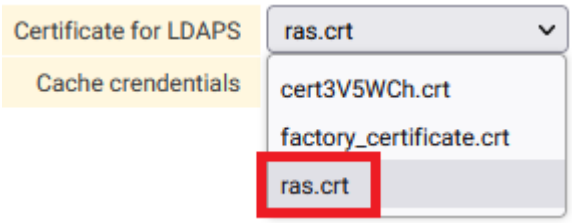


Figure 16. Configuration du certificat LDAP

Listes de révocation de certificats

OpenVPN et IPsec VPN (StrongSwan) peuvent vérifier si un certificat a été révoqué par une CRL. Pour OpenVPN, nous vous conseillons d'utiliser une CRL pour chaque autorité de certification.

CAUTION Il peut être nécessaire d'avoir les extensions x509v3 pour votre CRL, comme l'identifiant de la clé du sujet, pour fonctionner correctement.

10.4. CA bundle

Pour les outils datalogger et le serveur SMTP, vous devez spécifier les certificats CA auxquels vous faites confiance. Vous pouvez spécifier l'un de vos certificats personnalisés ou choisir le `Bundle de certificats CA de confiance`.

Ce bundle est un fichier contenant une liste de certificats CA de confiance de grandes entreprises. Il a été créé par le paquet Linux `ca-certificates`; ce paquet inclut les autorités de certification émises avec les navigateurs Mozilla pour permettre aux applications basées sur SSL de vérifier l'authenticité des connexions SSL.

Voici la liste de tous les certificats CA de confiance inclus dans ce fichier:

1. ACCVRAIZ1.crt
2. AC_RAIZ_FNMT-RCM.crt
3. Actalis_Authentication_Root_CA.crt
4. AffirmTrust_Commercial.crt
5. AffirmTrust_Networking.crt
6. AffirmTrust_Premium.crt
7. AffirmTrust_Premium_ECC.crt
8. Amazon_Root_CA_1.crt
9. Amazon_Root_CA_2.crt
10. Amazon_Root_CA_3.crt
11. Amazon_Root_CA_4.crt
12. Atos_TrustedRoot_2011.crt
13. Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
14. Baltimore_CyberTrust_Root.crt
15. Buypass_Class_2_Root_CA.crt
16. Buypass_Class_3_Root_CA.crt
17. CA_Disig_Root_R2.crt
18. CFCA_EV_ROOT.crt
19. COMODO_Certification_Authority.crt
20. COMODO_ECC_Certification_Authority.crt
21. COMODO_RSA_Certification_Authority.crt
22. Certigna.crt
23. Certum_Trusted_Network_CA.crt
24. Certum_Trusted_Network_CA_2.crt
25. Comodo_AAA_Services_root.crt
26. Cybertrust_Global_Root.crt

27. D-TRUST_Root_Class_3_CA_2_2009.crt
28. D-TRUST_Root_Class_3_CA_2_EV_2009.crt
29. DigiCert_Assured_ID_Root_CA.crt
30. DigiCert_Assured_ID_Root_G2.crt
31. DigiCert_Assured_ID_Root_G3.crt
32. DigiCert_Global_Root_CA.crt
33. DigiCert_Global_Root_G2.crt
34. DigiCert_Global_Root_G3.crt
35. DigiCert_High_Assurance_EV_Root_CA.crt
36. DigiCert_Trusted_Root_G4.crt
37. E-Tugra_Certification_Authority.crt
38. EC-ACC.crt
39. Entrust.net_Premium_2048_Secure_Server_CA.crt
40. Entrust_Root_Certification_Authority.crt
41. Entrust_Root_Certification_Authority_-_EC1.crt
42. Entrust_Root_Certification_Authority_-_G2.crt
43. GDCA_TrustAUTH_R5_ROOT.crt
44. GlobalSign_ECC_Root_CA_-_R4.crt
45. GlobalSign_ECC_Root_CA_-_R5.crt
46. GlobalSign_Root_CA.crt
47. GlobalSign_Root_CA_-_R2.crt
48. GlobalSign_Root_CA_-_R3.crt
49. GlobalSign_Root_CA_-_R6.crt
50. Go_Daddy_Class_2_CA.crt
51. Go_Daddy_Root_Certificate_Authority_-_G2.crt
52. Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt
53. Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt
54. Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt
55. Hongkong_Post_Root_CA_1.crt
56. ISRG_Root_X1.crt
57. IdenTrust_Commercial_Root_CA_1.crt
58. IdenTrust_Public_Sector_Root_CA_1.crt
59. Izenpe.com.crt
60. Microsec_e-Szigno_Root_CA_2009.crt
61. NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt

62. Network_Solutions_Certificate_Authority.crt
63. OISTE_WISeKey_Global_Root_GB_CA.crt
64. OISTE_WISeKey_Global_Root_GC_CA.crt
65. QuoVadis_Root_CA_1_G3.crt
66. QuoVadis_Root_CA_2.crt
67. QuoVadis_Root_CA_2_G3.crt
68. QuoVadis_Root_CA_3.crt
69. QuoVadis_Root_CA_3_G3.crt
70. SSL.com_EV_Root_Certification_Authority_ECC.crt
71. SSL.com_EV_Root_Certification_Authority_RSA_R2.crt
72. SSL.com_Root_Certification_Authority_ECC.crt
73. SSL.com_Root_Certification_Authority_RSA.crt
74. SZAFIR_ROOT_CA2.crt
75. SecureSign_RootCA11.crt
76. SecureTrust_CA.crt
77. Secure_Global_CA.crt
78. Security_Communication_RootCA2.crt
79. Security_Communication_Root_CA.crt
80. Staat_der_Nederlanden_EV_Root_CA.crt
81. Starfield_Class_2_CA.crt
82. Starfield_Root_Certificate_Authority_-_G2.crt
83. Starfield_Services_Root_Certificate_Authority_-_G2.crt
84. SwissSign_Gold_CA_-_G2.crt
85. SwissSign_Silver_CA_-_G2.crt
86. T-TeleSec_GlobalRoot_Class_2.crt
87. T-TeleSec_GlobalRoot_Class_3.crt
88. TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt
89. TWCA_Global_Root_CA.crt
90. TWCA_Root_Certification_Authority.crt
91. TeliaSonera_Root_CA_v1.crt
92. TrustCor_ECA-1.crt
93. TrustCor_RootCert_CA-1.crt
94. TrustCor_RootCert_CA-2.crt
95. USERTrust_ECC_Certification_Authority.crt
96. USERTrust_RSA_Certification_Authority.crt

97. XRamp_Global_CA_Root.crt
98. certSIGN_ROOT_CA.crt
99. ePKI_Root_Certification_Authority.crt
100. Certigna_Root_CA.crt
101. Entrust_Root_Certification_Authority_-_G4.crt
102. GTS_Root_R1.crt
103. GTS_Root_R2.crt
104. GTS_Root_R3.crt
105. GTS_Root_R4.crt
106. Hongkong_Post_Root_CA_3.crt
107. Microsoft_ECC_Root_Certificate_Authority_2017.crt
108. Microsoft_RSA_Root_Certificate_Authority_2017.crt
109. NAVER_Global_Root_Certification_Authority.crt
110. Trustwave_Global_Certification_Authority.crt
111. Trustwave_Global_ECC_P256_Certification_Authority.crt
112. Trustwave_Global_ECC_P384_Certification_Authority.crt
113. UCA_Extended_Validation_Root.crt
114. UCA_Global_G2_Root.crt
115. certSIGN_Root_CA_G2.crt
116. e-Szigno_Root_CA_2017.crt
117. emSign_ECC_Root_CA_-_C3.crt
118. emSign_ECC_Root_CA_-_G3.crt
119. emSign_Root_CA_-_C1.crt
120. emSign_Root_CA_-_G1.crt
121. AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt
122. ANF_Secure_Server_Root_CA.crt
123. Certum_EC-384_CA.crt
124. Certum_Trusted_Root_CA.crt
125. GlobalSign_Root_E46.crt
126. GlobalSign_Root_R46.crt
127. GLOBALTRUST_2020.crt

11. PARE-FEU

11.1. Principes du pare-feu

Un pare-feu filtre les paquets IP selon un ensemble de règles ordonnées:

1. Si c'est le cas, la décision est appliquée au paquet pour `Autoriser` ou pour `Interdire` selon la règle.
2. Si c'est le cas, la décision est appliquée au paquet. `Autoriser` ou `Interdire` selon la règle.
3. Si ce n'est pas le cas, le pare-feu vérifie s'il correspond à la deuxième règle ; et ainsi de suite.
4. Si le paquet ne correspond à aucune des règles du tableau, la politique par défaut est appliquée au paquet (`Autoriser` ou `Interdire`).

11.2. Règles de trafic WAN et VPN

Pour configurer les règles, accéder au menu ***Configuration > Sécurité > Pare-feu***

Cette section vous aide à créer des règles de pare-feu. Pour une meilleure organisation, les règles sont divisées en deux sections, toutes deux ayant la même structure.

Les **Règles pour le trafic WAN** filtrent les paquets transmis en dehors des VPN et les **Règles pour le trafic VPN** filtrent les paquets transmis à l'intérieur des VPN.

Le pare-feu est en charge de filtrer les trames IP entre les interfaces (LAN/WAN/VPN). Les deux sections peuvent filtrer les paquets entrants (depuis LAN/WAN/VPN).

Le trafic WAN vers LAN et le trafic LAN vers WAN sont considérés séparément, car la décision peut être différente pour un paquet provenant du WAN ou provenant du LAN. Par exemple, si la politique par défaut attribuée au trafic WAN vers LAN est `Interdire`, cela signifie qu'un paquet IP qui ne correspond à aucune des règles sera rejeté.

CAUTION	Les règles définies dans le tableau "Redirection de port" ne sont pas vérifiées par les règles de cette section. Ces paquets sont directement transférés vers le périphérique défini (voir Redirection de port)

Voici la description des paramètres avec leurs valeurs par défaut:

Politique par défaut LAN→WAN	`Autoriser` ou `Interdire`. Décision qui sera appliquée si un paquet ne correspond à aucune des règles du filtre. `Interdire` par défaut
Politique par défaut WAN→LAN	`Autoriser` ou `Interdire`. Décision qui sera appliquée si un paquet ne correspond à aucune des règles du filtre. `Interdire` par défaut
Activer le filtre anti Déni de Service (DoS)	Activer les règles de protection contre les attaques par déni de service. `True` par défaut

Activer les 'conntrack helpers' (Non recommandé)	Les assistants de suivi de connexion sont des modules qui fournissent un support pour le suivi et la manipulation de certains protocoles de la couche application au sein du sous-système de suivi de connexion (par exemple: FTP, H.323, SIP, PPTP, IRC). Il est désactivé par défaut pour des raisons de sécurité par défaut
Autoriser le ping	Accepter le ping sur l'interface WAN. Activé par défaut
Politique par défaut LAN → VPN	`Autoriser` ou `Interdire`. Décision qui sera appliquée si un paquet ne correspond à aucune des règles du filtre. `Autoriser` par défaut
Politique par défaut VPN → LAN	`Autoriser` ou `Interdire`. Décision qui sera appliquée si un paquet ne correspond à aucune des règles du filtre. `Autoriser` par défaut
Autoriser le trafic entre VPN	Autoriser le trafic provenant d'un VPN à être transféré vers un autre VPN. Activé par défaut

Dans ces sections, il y a des tableaux, chaque ligne étant une règle. Chaque règle du filtre est composée de plusieurs champs qui définissent un flux de données particulier et d'un autre champ qui est appelé le champ d'action.

Direction	La direction que prend le paquet *Example 32. Direction* `WAN ¬ LAN`
Action	`Autoriser` : autoriser les paquets concernés ou `Interdire` : rejeter les paquets concernés
Protocole	TCP, UDP, ICMP, AH, ESP, GRE, IGMP ou Tous pour tous les types de protocoles
Port source & **Port destination**	Numéro de port Si TCP ou UDP sélectionné, laisser vide si tous les ports sont concernés
Adresse IP source & **Adresse IP destination**	Adresses IP concernées, laisser vide si toutes les adresses sont concernées
Log	Les paquets correspondant à cette règle seront enregistrés dans le menu ***Diagnostics > Journaux > Pare-feu***

12. UTILISATEURS

Deux types d'utilisateurs peuvent accéder au routeur:

- `Opérateurs` qui ont besoin de droits d'accès au réseau
- `Administrateurs` qui configurent le routeur

Les deux sont liés à un `Utilisateur`.

12.1. Gestion des utilisateurs

Le routeur dispose d'un nouveau mécanisme de gestion des utilisateurs. Un utilisateur est une personne physique qui doit accéder au routeur, que ce soit pour le configurer ou pour se connecter à des équipements par son intermédiaire.

Les utilisateurs peuvent être définis dans l'écran ***Configuration*** > ***Sécurité*** > ***Utilisateurs***.

12.2. Créer un utilisateur

Pour enregistrer un nouvel utilisateur dans la liste des utilisateurs, cliquez sur le bouton **Ajouter** situé sous la liste des utilisateurs.

Actif	Activer ou désactiver un utilisateur
Nom complet	(Facultatif) Nom complet de la personne
Entreprise	(Facultatif) Entreprise à laquelle il appartient
Adresse E-mail	(Facultatif) Adresse e-mail, utilisé par Collect&Alert
Numéro de téléphone	(Facultatif) Numéro de téléphone au format international, utilisé par Collect&Alert *Example 33. Numéro de téléphone* +33611223344
CN du certificat utilisateur	(Facultatif) CN du certificat avec lequel cet utilisateur doit se connecter pour être accepté pour les connexions à distance. Laisser vide s'il n'y en a pas. Reportez-vous à Authentification multifacteur pour plus de détails
Nom d'utilisateur	Login de l'utilisateur, utilisé pour l'authentification. Celui-ci doit être unique, aucun nom d'utilisateur ne peut être utilisé deux fois
Mot de passe	Mot de passe de l'utilisateur, doit être robuste.

12.3. Gestion des opérateurs

Un opérateur est un `Utilisateur` qui doit accéder via le routeur.
Des droits d'accès individuels au réseau peuvent être attribués à chaque `Utilisateur`.

Créer un opérateur

Dans l'écran ***Configuration > Accès distant > Liste des opérateurs***, un administrateur peut définir un opérateur, en associant un `Utilisateur` à un ensemble de règles de pare-feu.

La liste des équipements du réseau LAN doit avoir été enregistrée au préalable.

Pour accorder des droits d'accès à un utilisateur distant:

1. Cliquez sur le bouton **Ajouter**.
2. Sélectionnez un `Utilisateur` dans la liste.
3. Sélectionnez un équipement dans la liste pour autoriser l'utilisateur distant à accéder à cet équipement.

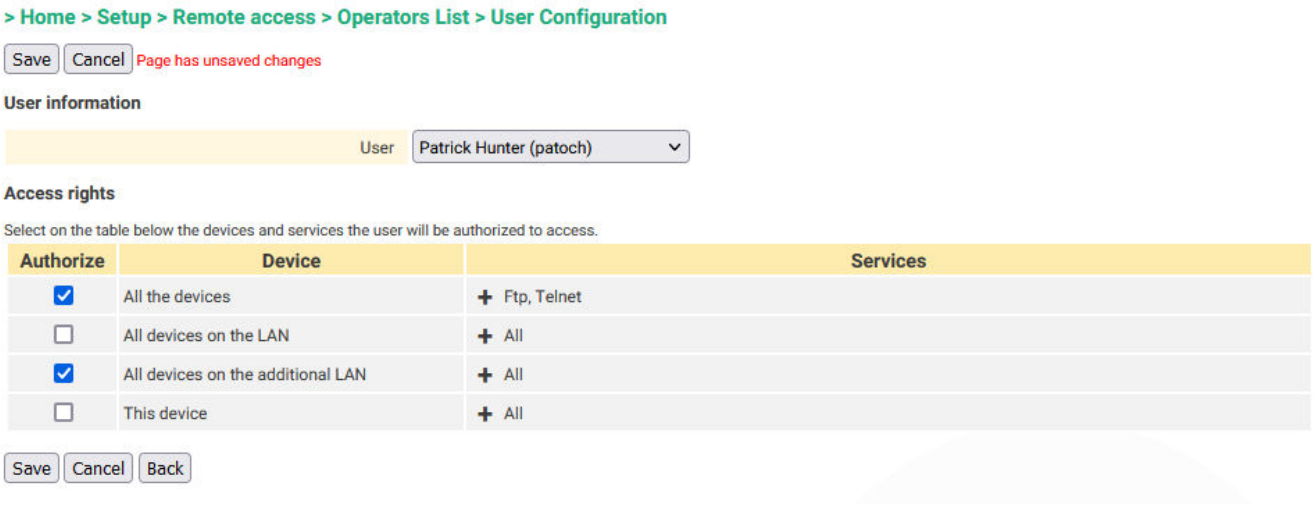


Figure 17. Écran de création d'opérateur

NOTE Un périphérique peut être un sous-réseau ou une adresse IP (reportez-vous à ***Configuration > Interface LAN > Liste des équipements***).

12.4. Administrateur et définition des rôles

Un administrateur est un utilisateur qui peut configurer le routeur. Il ne peut accéder qu'aux écrans autorisés par son rôle.

Pour protéger la section d'administration avec une authentification, accéder au menu ***Configuration > Sécurité > Droits d'administration***. Cochez **Protéger l'accès à la configuration par mot de passe**.

Créer un administrateur

Dans l'écran ***Configuration > Sécurité > Droits d'administration***, le Super administrateur peut créer un administrateur en associant un utilisateur à un rôle.

Figure 18. Ecran de création d'administrateur

6 rôles sont définis et permettent à l'utilisateur d'accéder à des écrans spécifiques. Ils sont définis dans la section `Liste des rôles`:

- Administrateur accès distant
- Administrateur télégestion
- Administrateur réseau
- Administrateur système
- Super administrateur
- Auditeur

NOTE	Au moins un super administrateur est requis sur le routeur. Si aucun super administrateur n'est défini, le routeur vous demandera d'en créer un.

Liste des rôles

Administrateur accès distant

- Gestion des utilisateurs
- Gestion de la liste des utilisateurs d'accès à distance
- Gestion de la liste des règles des utilisateurs d'accès à distance
- Création des utilisateurs
- Édition/suppression des utilisateurs non liés à un administrateur
- Édition de ses propres informations personnelles, à l'exception de son login

- Interfaces réseau et diagnostic de connexion M2Me
- Sauvegarde localement la configuration actuelle

Administrateur télégestion

Identique à Administrateur accès distant +

- Gestion du Datalogger
- Gestion Collect & Alert

Administrateur réseau

Identique à Administrateur accès distant +

- Accéder à tous les journaux en lecture seule sauf le journal d'audit
- Configuration et diagnostic des interfaces réseaux :
  - WAN
  - LAN
  - Serveurs d'accès à distance
  - VPNs (IPSec et OpenVPN)
  - Routes statiques
  - VRRP / RIP
  - Pare-feu / redirection de port / NAT / NAT 1:1
  - DNS dynamique
  - Passerelles
  - SMS / e-mails
- Magasin de certificats
- Outil Ping

Administrateur système

Identique à Administrateur réseau +

- Accéder et supprimer tous les journaux (sauf le journal d'audit qui est en lecture seule)
- Configuration et diagnostic de :
  - Gestion date/heure
  - Redémarrage périodique
  - Syslog distant
  - SNMP
  - Serveur ModBus / OPCUA
  - GPS

- Options logicielles
- Redémarrer
- Diagnostics avancés

Super administrateur

Identique à Administrateur système + Administrateur télégestion +

- Gestion déléguée de l'authentification
- Gestion Administrateur et Auditeur
- Gestion complète de la liste des utilisateurs
- Gestion complète des configurations : exporter, importer, sauvegarder, charger, ...
- Mettre à jour le firmware

Auditeur

- Accéder à tous les logs en lecture seule
- Édition de ses propres informations personnelles, à l'exception de son login

13. JOURNAUX

Plusieurs journaux sont disponibles pour superviser et aider à configurer le routeur.

Accédez à ***Diagnostics > Journaux*** pour y accéder.

Toutes les pages de journaux contiennent :

Filtrer	Accepte une `regexp` pour filtrer le contenu des journaux.
Bouton **Effacer**	Efface le journal. **CAUTION** Cette action efface les journaux `DANS` le routeur, cette opération ne peut pas être annulée.
Bouton **Rafraichir**	Recharger la page actuelle avec les journaux du routeur

NOTE Un mécanisme d'intégrité des logs a été mis en place sur le `Journal d'audit`. Lors de son affichage, une vérification est faite pour s'assurer que ce log n'a pas été altéré. Si c'est le cas, un message est affiché indiquant que la vérification a échoué.

Des balises sont placées dans les logs pour indiquer dans quel bloc de logs l'erreur a été identifiée.

13.1. Principal

Ce journal contient les principaux événements du routeur pour garantir le bon fonctionnement du système.

Des sections ont été définies pour aider à se concentrer sur une partie spécifique :

- SECURITY : Logs de sécurités comme l'authentification des utilisateurs sur le routeur
- CONFIGURATION : Tout ce qui concerne la configuration
- NETWORK : État ou changements des interfaces réseau
- SYSTEM : Événements internes du système
- HWMON : Surveillance du matériel
- GTW_RSIP : Gateway RSIP
- MESSAGING : Messagerie SMS et pagers
- DATALOGGER : Journaux spécifiques du Datalogger
- REMOTE_ACCESS : Événements d'accès à distance comme les connexions M2Me

13.2. OpenVPN

Journaux de tous les serveurs et clients OpenVPN. Chacun d'eux a son propre onglet.

13.3. IPSec

Tous les journaux d'IPSec.

13.4. Pare-feu

Journaux des règles du pare-feu. L'option **Log** doit être définie sur `Oui` dans l'écran ***Configuration*** > ***Sécurité*** > ***Pare-feu*** > ***Règle de filtrage trafic WAN*** pour que ces règles soient enregistrées.

13.5. Journal d'audit

Sont enregistrés :

- Les connexions utilisateur/administrateur et tentatives de connexion
- Toutes les actions (et tentatives) de l'administrateur qui modifient la configuration du routeur

Dans ce journal chaque action de chaque utilisateur est renseignée. C'est utile pour analyser ce qui a été effectué sur le routeur et vérifier la non-répudiation des actions sur le routeur.

Le bouton **Effacer** n'est pas disponible pour ce journal, car il sert à des fins de sécurité.

13.6. Avancé

Contient le journal principal. Mais aussi d'autres journaux provenant de composants internes.

13.7. Syslog

Pour configurer votre produit afin qu'il envoie ses journaux à un serveur Syslog distant de votre choix.

Accéder au menu ***Configuration*** > ***Système*** > ***Syslog*** et cochez l'option **Actif**.

Configuration du serveur distant Syslog

Adresse IP du serveur de log	Adresse IP et port du serveur Syslog vers lequel envoyer les journaux
Mode de transfert	• `Texte en clair` : les journaux sont transférés sous forme de texte en clair • `Authentification serveur` : les journaux sont chiffrés avec le certificat du serveur • `Authentification mutuelle` : les journaux sont chiffrés avec le certificat du serveur et signés avec une clé privée

Nom d'hôte du serveur	Seulement si `Authentification serveur` ou `Authentification mutuelle` Nom du serveur syslog. Ce champ doit correspondre au nom commun (CN) du certificat du serveur. **CAUTION** Les journaux sont chiffrés avec le certificat du serveur. L'autorité de certification qui a émis le certificat du serveur doit être présente dans les `Certificats d'autorité de certification` du `Magasin de certificats`.
Certificat	Seulement si `Authentification mutuelle`. Choisissez un certificat dans le `Magasin de certificats` pour signer les journaux. **CAUTION** Le certificat choisi doit être lié à une clé privée. Sinon, les journaux ne peuvent pas être signés.

Format des journaux envoyés au serveur distant

Les journaux envoyés à un serveur Syslog distant sont formatés comme suit:

```
${ISODATE} ${UNIQID} ${PROGRAM} ${FACILITY} (${LEVEL}) | ${MSG}
```

Voici un exemple de traces:

```
...
2025-07-04T16:15:51+02:00 9164560d@00000000000000dc   daemon_starter   local1
(info) |       NETWORK: LAN: lan4 is Down
2025-07-04T16:16:07+02:00 9164560d@00000000000000df   daemon_starter   local1
(info) |       NETWORK: LAN: lan2 Up 100Mb/s Full Duplex
2025-07-04T16:16:27+02:00 9164560d@00000000000000e0         dropbear authpriv
(info) | Child connection from 192.168.0.20:61448
2025-07-04T16:16:28+02:00 9164560d@00000000000000e1         dropbear authpriv
(notice) | Auth succeeded with blank password for 'root' from 192.168.0.20:61448
2025-07-04T16:18:49+02:00 9164560d@00000000000000e2   gui_backend.py   local3
(info) | User 'admin' has authenticated to the Admin Web interface
2025-07-04T16:19:02+02:00 9164560d@00000000000000e3   gui_backend.py   local3
(info) | User 'admin' set params into the configuration
2025-07-04T16:19:04+02:00 9164560d@00000000000000e4        committer   local3
(info) | Changed parameters: {u'p_https_appserver_2_enable.0': u'false'}
...
```

La FACILITY local1 correspond au journal Principal. local3 correspond au journal Journal d'audit.

Configuration du serveur Syslog distant

Suivant la configuration de votre serveur, il peut être nécessaire d'ajouter flags(no-parse) pour afficher le texte brut reçu.

14. INTERFACE UTILISATEUR

Plusieurs interfaces sont disponibles sur le produit pour permettre à un utilisateur d'interagir avec celui-ci.

Il peut s'agir d'interfaces d'administration pour configurer le produit, ou d'opération pour qu'un exploitant puisse utiliser certaines fonctionnalités du produit.

14.1. Page web d'administration

La page Web d'administration permet aux administrateurs de configurer le produit et ses fonctionnalités.

Configuration

Ce serveur web peut aussi être configuré, aller à la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Droits d'administration*** pour le configurer.

Protéger l'accès à la configuration par mot de passe	Utiliser un compte avec login/mot de passe afin d'accéder à la page web d'administration. `True` par défaut
Protocoles à utiliser pour la configuration	`HTTP seulement`, `HTTPS seulement` ou `HTTP et HTTPS`. Il est conseillé d'utiliser `HTTPS seulement`
Port HTTPS d'administration (4433)	Port TCP utilisé pour le serveur Web d'administration. C'est 4433 par défaut
Le port TCP 80 redirige vers la Zone Administration	Lorsque le portail WEB et le serveur d'applications sont désactivés, cette case à cocher permet de rediriger les requêtes vers le port 80 vers le port d'administration HTTP ou HTTPS
Utiliser le certificat usine auto-signé	Utiliser un certificat auto signé pour le serveur web. `True` par défaut
Choisir un certificat personnalisé	Utiliser l'un de vos certificats personnalisés
Activer l'accès via EticNet (HTTPS seulement)	Permet d'accéder au serveur d'applications via EticNet. `False` par défaut
Activer l'accès par le WAN (HTTPS seulement)	Permet d'accéder à la page web depuis les interfaces WAN. `False` par défaut

La page web fonctionne avec des sessions, si un utilisateur connecté reste inactif pendant 10 minutes, il est automatiquement déconnecté de la page web.

WARNING	Lors d'un changement de certificat du serveur web d'administration, il est probable que votre navigateur bloque l'accès et vous affiche une page blanche. Pour prendre en compte le nouveau certificat, veuillez rafraichir la page de

votre navigateur avec son cache (`Ctrl + F5` dans la plupart des navigateurs).

Si vous utilisez le certificat auto-signé, après un retour configuration usine, le certificat du serveur web sera renouvelé par un nouveau.

14.2. Page web d'exploitation

Ce serveur HTTPS peut se comporter comme une passerelle HTTPS vers HTTP pour donner un accès à distance sécurisé aux pages HTML/HTTP(S) des équipements sur le LAN.

Il faut dans un premier temps créer des opérateurs avant de pouvoir accéder à cette page.

La page Web d'exploitation permet aux opérateurs d'accéder à la liste des serveurs HTML auxquels ils ont le droit d'accéder, ainsi qu'aux variables Collect&Alert si le produit en est équipé. Si l'opérateur reste inactif pendant 10 minutes, il est automatiquement deconnecté de la page web.

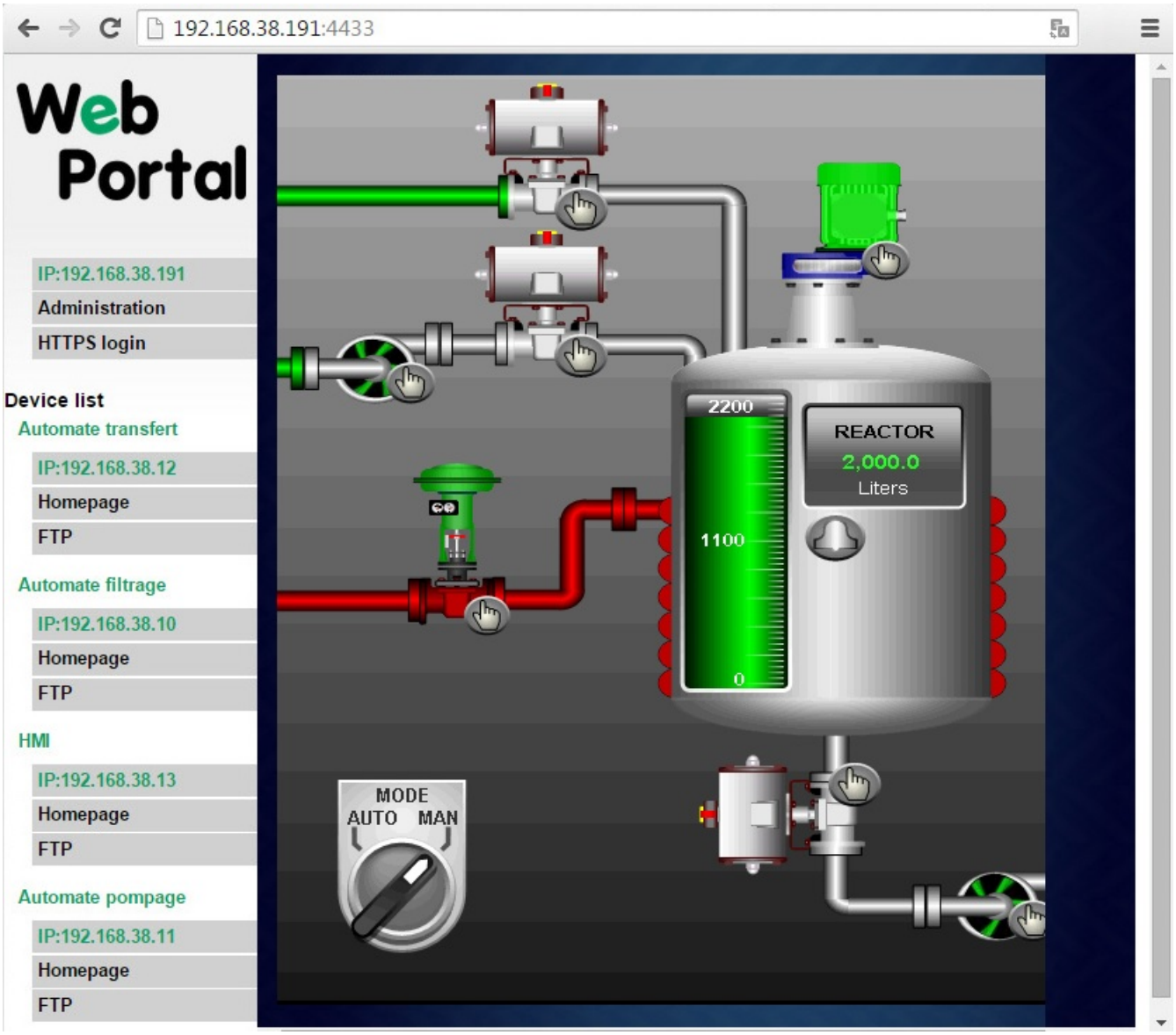


Figure 19. Page HTML HTTP intégrée

Configuration

Ce serveur web peut aussi être configuré, aller à la page > ***Accueil*** > ***Configuration*** > ***Accès distant*** > ***Moyens d'accès*** pour le configurer. Le serveur fonctionne sur le port TCP 443.

Activer le serveur d'applications HTTPS	Permet d'activer/désactiver le serveur web. `False` par défaut
Accès au serveur d'applications HTTPS par le WAN	Permet d'accéder au serveur d'applications via les interfaces WAN. `False` par défaut
Serveur d'application HTTPS accessible via EticNet	Permet d'accéder au serveur d'applications via EticNet. `True` par défaut **CAUTION** Cette option doit être activée pour permettre la connexion depuis l'application Smartphone.
Utiliser le certificat usine auto-signé	Utiliser un certificat auto-signé pour le serveur. Nous vous recommandons de décocher cette case et d'utiliser l'un de vos certificats. `True` par défaut
Choisir un certificat personnalisé	Utiliser l'un de vos certificats personnalisés

WARNING

Lors d'un changement de certificat du serveur web d'opération, il est probable que votre navigateur bloque l'accès et vous affiche une page blanche. Pour prendre en compte le nouveau certificat, veuillez rafraichir la page de votre navigateur avec son cache (`Ctrl + F5` dans la plupart des navigateurs).

Si vous utilisez le certificat auto-signé, après un retour configuration usine, le certificat du serveur web sera renouvelé par un nouveau.

Accéder au portail d'exploitation à travers M2Me par Smartphone

Pour faciliter l'accès aux équipements et autres pages depuis l'application M2Me Smartphone, il est possible de configurer une liste de liens qui seront directement disponibles après la connexion.

Aller à la page > ***Accueil*** > ***Configuration*** > ***Interface LAN*** > ***Portail WEB***, et activer l'option **Afficher le portail web**.

Ensuite créer des liens:

Nom	Nom qui sera affiché dans le portail Web
URL	URL associée au lien

En cliquant sur le lien, vous serez redirigé directement vers l'URL configurée.

Vous pouvez par exemple indiquer la page Collect & Alert. Ainsi, sur l'application Smartphone, vous aurez un lien qui vous redirigera directement vers la page des synaptiques, où vous pouvez lire et écrire les variables des automates configurés.

14.3. Interface en ligne de commande SSH

Le produit met à disposition un serveur SSH afin de permettre aux administrateurs de gérer le produit et ses fonctionnalités. Pour le configurer aller à la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Droits d'administration***

Activer le serveur SSH	Activer/désactiver le serveur SSH `True` par défaut
Clé publique SSH (pour login sans mot de passe)	Clé publique pour l'authentification SSH

Le serveur permet de gérer plusieurs sessions SSH, chacune avec des identifiants et des clés de session négociés lors de la phase d'échange de clés. Ceux-ci sont supprimés à la fin d'une session. Une session peut être fermée par un utilisateur en utilisant les touches `Ctrl`+`D`.

Le serveur utilise des suites de chiffrement fortes et sécurisées pour les communications.

Pour copier des fichiers dans le produit, vous pouvez utiliser `scp` dans le répertoire `/tmp` qui est le seul répertoire avec accès en écriture. Les fichiers copiés sur le SSH verront leurs capacités d'exécution supprimées pour des raisons de sécurité.

Liste des commandes SSH

Un sous-ensemble de commandes Linux est disponible, ainsi qu'un ensemble de commandes Etic Telecom qui vous aideront à configurer et à utiliser votre appareil.

Toutes ces commandes ont une aide à laquelle vous pouvez accéder avec l'argument `--help`.

Commandes	Description
m2me	Démarrer ou arrêter M2Me
test_smsemail	Procéder au test d'envoi de sms et d'email
stor	Changer la sortie vers un état spécifique
test_ftpc	Tester le client FTP
shdsl_testmode	Tester le mode SHDSL
shdsl_dotest	Appeler SHDSL socrates
shdsl_pmms	Lire les pmms SHDSL
get_external_ssh_users	Obtenir la liste des utilisateurs qui se sont déjà connectés une fois à l'interface SSH à partir d'un serveur d'authentification délégué
clear_external_ssh_users	Effacer la liste des utilisateurs qui se sont déjà connectés une fois à l'interface SSH à partir d'un serveur d'authentification délégué

14.3. Interface en ligne de commande SSH

Commandes	Description
sw_upgrade	Mettre à jour le logiciel avec un code
fw_upgrade	Mettre à jour le firmware avec une archive
get_upgrades_list	Obtenir la liste des versions de mises à jour disponibles en ligne
upgrade_from_eticnet	Mettre à jour la version à partir du serveur Eticnet
set_date_time	Régler la date et l'heure
unban_user	Débannir un utilisateur banni de l'authentification par le mécanisme de protection
simplify_hotline_remote_access	Simplifiez l'accès à distance à la hotline pendant une période donnée.
display_view	Afficher les paramètres utilisés dans les vues
delete_row	Supprimer une ligne dans un groupe de paramètres de la configuration actuelle
add_row	Ajouter une ligne dans un groupe de paramètres
edit_row	Editer une ligne dans un groupe de paramètres
swap_rows	Échanger la position de deux lignes dans un groupe de paramètres
get_groups_params	Obtenir les paramètres d'un groupe de la configuration actuelle
get_params	Afficher la valeur des paramètres de la configuration actuelle
get_status	Afficher les statuts du produit
get_groups_status	Obtenir les valeurs d'un groupe de statuts
set_params	Modifier des paramètres de la configuration actuelle
set_first_superadmin	Définir le premier super administrateur
reset_hotline_passwd	Réinitialiser le mot de passe de la hotline
config_list	Lister les configurations enregistrées
config_load	Charger une configuration
config_save	Enregistrer une configuration 'Utilisateur'
config_delete	Supprimer une configuration 'Utilisateur'
config_upload	Uploader une configuration 'Utilisateur'
config_load_fac	Recharger la configuration d'usine
config_export	Exporter une configuration

Commandes	Description
make_csr_request	Effectuer une demande CSR pour une clé privée spécifique
get_cert_infos	Obtenir les détails d'un certificat
generate_private_key	Générer une clé privée
import_private_key	Importer une clé privée au format x509
delete_private_key	Supprimer une clé privée
add_crl	Ajouter une liste de révocation de certificats au format x509
delete_crl	Supprimer une liste de révocation de certificats
add_cert	Ajouter un certificat au format x509
add_pkcs12	Ajouter un fichier PKCS12
delete_cert	Supprimer un certificat
role_add	Ajouter un ou plusieurs rôles d'administrateur personnalisés
role_list	Lister les rôles d'administrateur ou afficher leur description
role_delete	Supprimer un rôle d'administrateur personnalisé
get_log	Afficher un log

Aide des commandes

m2me

```
$ m2me --help
m2me : Start or stop M2Me

usage : m2me <expected_state>

  expected_state : START / STOP. start or stop the m2me on the device
```

test_smsemail

```
$ test_smsemail --help
test_smsemail : Proceed to the test of sending sms and email

usage : test_smsemail
```

stor

```
$ stor --help
stor : Change output to a specific state

usage : stor <expected_state>

  expected_state : ON / OFF. Switch ON or switch OFF the stor
```

test_ftpc

```
$ test_ftpc --help
test_ftpc : Test FTP client

usage : test_ftpc
```

shdsl_testmode

```
$ shdsl_testmode --help
shdsl_testmode : Test SHDSL mode

usage : shdsl_testmode
```

shdsl_dotest

```
$ shdsl_dotest --help
shdsl_dotest : Call SHDSL socrates

usage : shdsl_dotest <command>

  command   : Command to pass to socrates. help (without --) as command for more
information
```

shdsl_pmms

```
$ shdsl_pmms --help
shdsl_pmms : Read SHDSL pmms

usage : shdsl_pmms
```

get_external_ssh_users

```
$ get_external_ssh_users --help
get_external_ssh_users : Get the list of users who have already logged in once to the
```

```
SSH interface from a delegated authentication server

usage : get_external_ssh_users
```

clear_external_ssh_users

```
$ clear_external_ssh_users --help
clear_external_ssh_users : Clear the list of users who have already logged in once to
the SSH interface from a delegated authentication server

usage : clear_external_ssh_users
```

sw_upgrade

```
$ sw_upgrade --help
sw_upgrade : Upgrade software with a code

usage : sw_upgrade <code>

       code : Code provided by Etic Telecom to upgrade your device
```

fw_upgrade

```
$ fw_upgrade --help
fw_upgrade : Upgrade firmware with an archive

usage : fw_upgrade <fw_path> [end_upgrade] [config_file]

    fw_path : Path of the firmware archive to upgrade to
end_upgrade : (Optionnal - Default : True) End the action and clean the pending status
in database : True / False
config_file : (Optionnal - Default : '') Load a configuration file after the upgrade
```

get_upgrades_list

```
$ get_upgrades_list --help
get_upgrades_list : Get a list of available upgrades version online

usage : get_upgrades_list
```

upgrade_from_eticnet

```
$ upgrade_from_eticnet --help
upgrade_from_eticnet : Upgrade version from Eticnet server
```

```
usage : upgrade_from_eticnet <version> [config_file]

version_file : Version file to upgrade to. Use cmd 'get_upgrades_list' to get the
possible version files available
 config_file : (Optionnal - Default : '') Load a configuration file after the upgrade
```

set_date_time

```
$ set_date_time --help
set_date_time : Set the date and time

usage : set_date_time <date_time>

  date_time : Date/Time to set. Format shall be YYYY-MM-DD_HH:mm
```

unban_user

```
$ unban_user --help
unban_user : Unban a banned user from authentication by the protection mechanism

usage : unban_user <ip>

  user            : User to unban.
```

simplify_hotline_remote_access

```
$ simplify_hotline_remote_access --help
simplify_hotline_remote_access : Simplify hotline remote access for an amount of time.
This will disable hotline password requirement, and enable remote access VPN even if
you have not defined an operator for it

usage : simplify_hotline_remote_access [nb_minutes]

 nb_minutes       : (Optionnal - Default: 60 - Range [1 - 480]) Number of minutes to
simplify hotline remote access.
```

display_view

```
$ display_view --help
display_view : Display parameters descriptions used in views

usage : display_view [view] ...

  views     : 0-N view(s) to display
```

delete_row

```
$ delete_row --help
delete_row : Delete a row in current configuration

usage : delete_row <group_name> <row_index>

  group_name  : Name of the group where to deleted the row
  row_index   : Index of the row to delete
```

add_row

```
$ add_row --help
add_row : Add a row in a group of parameters

usage : add_row <group_name> <param_name param_value> [param_name param_value] ...

  group_name              : Name of the group where to add rows
  param_name param_value  : 1-N couples of <param_name param_value> to add in a group
```

edit_row

```
$ edit_row --help
edit_row : Edit a row in a group of parameters

usage : edit_row <group_name> <row_index> <param_name param_value> [param_name
param_value] ...

  group_name              : Name of the group where to add rows
  row_index               : Index of the row to edit
  param_name param_value  : 1-N couples of <param_name param_value> to add in a group
```

swap_rows

```
$ swap_rows --help
swap_rows : Swap two rows in a group of parameters

usage : swap_rows <group_name> <row_index_1> <row_index_2>

  group_name      : Name of the group where to swap rows
  row_index_(1|2) : Indexes of the rows to swap
```

get_groups_params

```
$ get_groups_params --help
```

```
get_groups_params : Get parameters of a group in the configuration

usage : get_groups_params <group> ...

  group : 1-N group(s) to display
```

get_params

```
$ get_params --help
get_params : Get parameters in the configuration

usage : get_params <param> ...

  param : 1-N param(s) to display
```

get_status

```
$ get_status --help
get_status : Get statuses of the product

usage : get_status <status>.<index> ...

  status       : 1-N status to display
  index        : Index of the specified status to get (0-N)
```

get_groups_status

```
$ get_groups_status --help
get_groups_status : Get statuses of a group of status

usage : get_groups_status <group> ...

  group : 1-N group(s) to display
```

set_params

```
$ set_params --help
set_params : Set parameters in the configuration

usage : set_params <param_name param_value> [param_name param_value] ...

  param_name param_value  : 1-N couples of <param_name param_value> to add in the
configuration
```

set_first_superadmin

```
$ set_first_superadmin --help
set_first_superadmin : Set first superadmin

usage : set_first_superadmin <login> <password>

     login     : Login of the Super Administrator.
  password     : Password of the Super Administrator. Password must follow the
following rules:
                 * One lowercase letter
                 * One uppercase letter
                 * One number
                 * One special character in the subset: &#{}[]@!?_ *+=~$%
                 * Minimum of 8 characters
                 * Maximum of 50 characters
```

reset_hotline_passwd

```
$ reset_hotline_passwd --help
reset_hotline_passwd : Reset hotline password

usage : reset_hotline_passwd [password_length]

  password_length : (Optionnal - Default : 12) Length of the generated password.
```

config_list

```
$ config_list --help
config_list : List saved configurations

usage : config_list [config_types]

  config_types    : types of configuration to display : Reference / User / Builder
```

config_load

```
$ config_load --help
config_load : Load a configuration

usage : config_load <conf_filename> [config_type] [edition_mode]

  conf_filename   : File name of the configuration to load
  config_type     : (Optionnal - Default : User) location of the configuration to load
: Reference / User / Builder
  edition_mode    : (Optionnal - Default : False) start edition mode : True / False
                    edition mode : Configuration has to be validated with option
```

```
<commit> to apply it
```

config_save

```
$ config_save --help
config_save : Save a 'User' configuration

usage : config_save <conf_name>

  conf_name     : Name of the saved configuration. Will be located in the User space
```

config_delete

```
$ config_delete --help
config_delete : Delete a 'User' configuration

usage : config_delete <conf_name>

  conf_name     : Name of the exported configuration. Will appear in the User space
```

config_upload

```
$ config_upload --help
config_upload : Upload a 'User' configuration

usage : config_upload <file_path> <conf_name> [force] [decryption_secret]

  file_path  : Path of the configuration file to upload
  conf_name  : Name of the configuration in User space
  force      : (Optionnal - Default : False) force upload file : True / False. Bypass
illformed configuration
  decryption_secret  : (Optionnal) Secret to decrypt password in the configuration
```

config_load_fac

```
$ config_load_fac --help
config_load_fac : Reload factory configuration

usage : config_load_fac
```

config_export

```
$ config_export --help
onfig_export : Export the configuration
```

```
usage : config_export <conf_filename> <destination_file> <secret_encryption>
[encryption_key] [config_type]

  conf_name         : Configuration name to export
  destination_file  : Output file destination
  secret_encryption : Encrypt or not the secrets : encrypt / no_encryption
  encryption_key    : (Only if <secret_encryption> is `encrypt`) Key to encrypt
configuration's secrets
  config_type       : (Optionnal - Default : User) location of the configuration :
Reference / User / Builder
```

make_csr_request

```
$ make_csr_request --help
make_csr_request : Make a CSR request for a specific private key

usage : make_csr_request <private_key> [common_name] [country] [organization]
[organizational_unit] [locality] [state]

  private_key : The private key to make the CSR for
  common_name : (Optionnal) Set Common Name (CN)
      country : (Optionnal) Set Country (C)
 organization : (Optionnal) Set Organization (O)
 organizational_unit : (Optionnal) Set Organizational Unit (OU)
     locality : (Optionnal) Set Locality (L)
        state : (Optionnal) Set State (S)

# If you don't want a specific field. Leave it empty with ""
```

get_cert_infos

```
$ get_cert_infos --help
get_cert_infos : Get details of a certificate

usage : get_cert_infos <certificate> [CA]

  certificate : Certificate to retrieve information
           CA : (Optionnal - Default : False) Look in Certification Authorities
certificates : True / False
```

generate_private_key

```
$ generate_private_key --help
generate_private_key : Generate a private key

usage : generate_private_key <pk_name> <algo> [algo_param]
```

```
    pk_name : Name of the private key
       algo : Private Key Algorithm (Possible value : rsa / ecdsa)
 algo_param : (Optionnal) Depending of the algorithm choosen
                rsa   : (Default : 2048) length of the key (Possible value : [2048,
3072, 4096])
                ecdsa : (Default : Prime256v1) curve to use (Possible value :
[Prime256v1])
```

import_private_key

```
$ import_private_key --help
import_private_key : Import a private key in x509 format

usage : import_private_key <key_name> <key_path>

   key_name : Name of the private key
   key_path : Private key file path
```

delete_private_key

```
$ delete_private_key --help
delete_private_key : Delete a private key

usage : delete_private_key <private_key>

  private_key : The private key to delete
```

add_crl

```
$ add_crl --help
add_crl : Add a certificate revocation list in x509 format

usage : add_crl <crl_name> <crl_path>

   crl_name : Name of the certificate revocation list
   crl_path : CRL file path
```

delete_crl

```
$ delete_crl --help
delete_crl : Delete a certificate revocation list

usage : delete_crl <crl_name>
```

```
     crl_name : The CRL to delete
```

add_cert

```
$ add_cert --help
add_cert : Add a certificate in x509 format

usage : add_cert <cert_name> <cert_path> [CA]

  cert_name : Name of the certificate
  cert_path : Certificate file path
         CA : (Optionnal - Default : False) Insert in Certification Authorities
certificates : True / False
```

add_pkcs12

```
$ add_pkcs12 --help
add_pkcs12 : Add a PKCS12 file

usage : add_pkcs12 <pkcs12_name> <pkcs12_file> <pkcs12_password>

      pkcs12_name : Name of the Pkcs12
      pkcs12_file : PKCS12 file path
  pkcs12_password : password of the pkcs12
```

delete_cert

```
$ delete_cert --help
delete_cert : Delete a certificate

usage : delete_cert <cert_name> [CA]

  cert_name : The certificate to delete
         CA : (Optionnal - Default : False) Delete in Certification Authorities
certificates : True / False
```

role_add

```
$ role_add --help
role_add : Add administrator custom role(s)

usage : role_add <file_path>

  file_path  : Absolut path of the file with the customs roles to add
  overwrite  : (Optionnal - Default : False) Overwrite custom roles if it exists
```

```
already
```

Les rôles personnalisés doivent être décrits au format `json`.
Ce format est une `list` de rôle. Chaque rôle est un `dict` contenant les paramètres suivants :

role_name	Nom interne du rôle. 50 caractères maxmimum, doit être en minuscule et commence par `p_custom_role_`
local_fr	Texte affiché en français
local_en	Texte affiché en anglais
func_permissions	Définir un niveau de permission pour chaque fonction : • `20`: lecture • `30`: écriture Les fonctions `func_superadmin`, `func_admin`, `func_firmconf` ne peuvent être définies qu'en lecture.

Custom role file example

```
[
    {
        "role_name": "p_custom_role_group_a",
        "local_fr": "Administrateur A",
        "local_en": "Administrator A",
        "func_permissions": {
            "func_generic": 30,
            "func_biwan": 20,
            "func_wan_eth": 20,
            "func_wan_br": 20,
            "func_wan_ip": 20,
            "func_diagnostics": 20,
            "func_logs": 20,
            "func_net_stat": 20,
            "func_diag_ifaces": 20,
            "func_vpn_node": 20,
            "func_tls_node": 20,
            "func_tools": 20,
            "func_firmconf": 20,
            "func_product_def": 20
        }
    },
    {
        "role_name": "p_custom_role_group_b",
        "local_fr": "Administrateur B",
        "local_en": "Administrator B",
        "func_permissions": {
            "func_generic": 30,
            "func_biwan": 30,
```

```
            "func_wan_eth": 30,
            "func_wan_gsm": 30,
            "func_wan_br": 30,
            "func_wan_ip": 30,
            "func_diagnostics": 30,
            "func_logs": 30,
            "func_net_stat": 30,
            "func_diag_ifaces": 30,
            "func_vpn_node": 30,
            "func_tls_node": 30,
            "func_tools": 30,
            "func_firmconf": 20,
            "func_product_def": 20
        }
    }
]
```

role_list

```
$ role_list --help
role_list : List administrator roles or display their description

usage : role_list [role_name]

   role_name : (Optionnal - Default : Empty) If empty, display role_name of all roles
                            If role_name is provided, display the role in a json
format
```

role_delete

```
$ role_delete --help
role_delete : Delete an administrator custom role

usage : role_delete <role_name>

   role_name  : Custom role to delete
       force  : (Optionnal - Default : False) Delete the role even if administrators
use it
```

get_log

```
$ get_log --help
get_log : Get a specific log

usage : get_log <type> [display] [specific_log]

         type : Log type. Possible values : user / advanced_user / audit / firewall /
```

```
vpn / m2me / charon / gsm_ext_counter_log / gsm_ext_log / gsm_counter_log / gsm_log
      display : (Optionnal - Default : all) Display the whole log or output appended
data as the file grows: all / follow
 specific_log : (Optionnal - Only for type = vpn) A pair of param. Choose between
server/client log and a configuration. Ex : server 1
```

Lecture du log serveur OpenVPN 0 exemple

```
$ get_log vpn follow server 0
```

15. DNS DYNAMIQUE

Les services EticDNS, DynDNS ou NoIP permettent de se connecter à distance à un routeur via Internet même si l'adresse IP de ce routeur est dynamique.

L'adresse IP du routeur doit être une adresse IP publique.

Par exemple, si un PC distant doit se connecter à un routeur cellulaire RAS-EC ou IPL-C, les solutions EticDNS, DynDNS ou NoIP ne seront utiles que si l'adresse IP attribuée par le fournisseur de services de données mobiles à "l'antenne" du routeur est une adresse IP publique.

15.1. EticDNS

En créant un compte sur l'Espace Client du site Etic Telecom, vous pouvez gérer votre routeur et lui attribuer un nom de domaine pour son WAN Principal.

Le routeur doit être accessible via Internet.

15.2. Étape 1: Attribution d'un nom de domaine

Réservez un nom de domaine sur le site Web Dynamic DNS de votre choix.

15.3. Étape 2: Configuration du routeur

Accéder au menu ***Configuration > Réseau > DNS dynamique***. Cochez ensuite l'option **Activer**.

Service de DNS dynamique	Sélectionnez `EticDNS`, `dyndns.org` ou `NoIP`. **NOTE** Si vous choisissez `EticDNS`, les paramètres suivants seront directement connus par Etic Telecom
Identifiant du compte utilisateur DNS dynamique	Identifiant de votre compte attribué par votre service DNS dynamique
Mot de passe	Mot de passe de votre compte attribué par votre service DNS dynamique
Hostname	Nom de domaine attribué par votre service DNS dynamique *Example 34. Nom de domaine* mymachine.eticdns.com

16. ALARME E-MAIL OU SMS

Tous les modèles de Routeurs sont capables de transmettre des alarmes SMS ou e-mail lorsqu'un événement se produit.

Accéder au menu ***Configuration*** > ***Système*** > ***SMS/e-mail*** et activer l'option **Actif**.

Chaque envoi de SMS ou d'e-mail est consigné dans les journaux, ainsi que la personne/le processus qui a déclenché cet envoi.

Message	Type de message : SMS ou E-mail
Source de l'alarme	Sélectionnez l'événement: • `Entrée TOR: passage à l'état fermé` • `Entrée TOR: passage à l'état ouvert` • `Entrée TOR: passage à l'état ouvert ou fermé` • `VPN connecté/déconnecté`
Numéro de téléphone (Message SMS)	Entrez le numéro de téléphone mobile. Si vous utilisez le serveur M2Me et le pack SMS, le numéro doit avoir l'indicatif du pays. Par exemple, `0033` ou `+33` pour la France. Il est possible de renseigner plusieurs numéros séparés par une virgule.
Emetteur de l'e-mail (Message E-mail)	Entrez l'émetteur de l'e-mail.
Destinataire de l'alarme (Message E-mail)	Entrez les destinataires de l'e-mail. Il est possible de renseigner plusieurs destinataires séparés par une virgule.
Objet (Message E-mail)	Entrez l'objet de l'e-mail d'alarme.
Texte à envoyer	Entrez le contenu du message d'alarme.

16.1. Section client SMTP

Etic Telecom fournit des services SMTP qui peuvent être utilisés pour envoyer des messages d'alarme sans configuration supplémentaire.

Accéder au menu ***Configuration*** > ***Système*** > ***Messagerie***.

Sélectionnez **Utiliser le serveur M2Me pour envoyer les e-mails** pour envoyer les messages d'alarme via le service Etic Telecom.

Vous pouvez également utiliser le serveur SMTP de votre choix. Désélectionnez la case précédente

et configurez les paramètres suivants:

Serveur SMTP	Le serveur SMTP de destination
Port	Le port sur lequel le serveur SMTP écoute
Sécurité de la connexion	Le chiffrement utilisé: `Aucun`, `StartTLS` ou `TLS`
Utiliser le certificat utilisateur	Sélectionner le certificat issu du magasin de certificat qui sera utilisé pour chiffrer la connexion
Source de la CA	Si la CA pour l'authentification du serveur est issu du magasin de certificat ou du bundle fourni avec le routeur (voir la section CA bundle)
Certificat CA du serveur SMTP	La CA du magasin de certificat pour l'authentification du serveur
Méthode d'authentification	Le moyen d'authentification sur le serveur
Nom d'utilisateur et **Mot de passe**	Nom de l'utilisateur et mot de passe pour l'authentification sur le serveur

16.2. SNMP

Le routeur est un agent SNMP; il est conforme à la norme MIB et peut transmettre des traps SNMP sur des événements configurables.
Il peut également envoyer des traps à un gestionnaire SNMP.

Configuration SNMP

Accéder au menu ***Configuration > Système > SNMP***

Les propriétés suivantes sont utilisées aussi bien par l'agent SNMP que pour identifier l'envoi des traps.

Nom du système	`syslocation` de l'agent SNMP. Permet également d'identifier l'origine des traps par le gestionnaire.
Localisation du système	`sysname` de l'agent SNMP. Permet également d'identifier l'origine des traps par le gestionnaire.

Configuration de l'agent SNMP

Activer	Activer l'agent SNMP
Version de protocole SNMP	Version SNMP à utiliser. `SNMP version 1 et 2c` ou `SNMP version 3`
Nom de communauté	Il s'agit du nom partagé entre chaque agent et le gestionnaire SNMP. L'agent SNMP ne répond qu'aux requêtes d'un gestionnaire qui s'identifie par ce nom (uniquement dans `SNMP version 1 et 2c`)

Nom d'utilisateur	Nom de l'utilisateur SNMP (uniquement dans `SNMP version 3`)
Algorithme d'authentification	Algorithme d'authentification (uniquement dans `SNMP version 3`) *Example 35. Valeurs possibles* MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512
Mot de passe	Mot de passe de l'utilisateur SNMP (uniquement dans `SNMP version 3`)
Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données (uniquement dans `SNMP version 3`) *Example 36. Valeurs possibles* AES-256-CBC, AES-192-CBC, AES-128-CBC, DES
Clé de chiffrement	Clé utilisée pour chiffrer les données (uniquement dans `SNMP version 3`)
Surveiller le statut du backup OpenVPN	Le serveur VPN peut surveiller l'état des clients VPNs primaires et de backup via SNMP. Ces données sont affichées dans le tableau récapitulatif de la page ***Diagnostics > État du réseau > Connexions VPN > OpenVPN***
Nom du VPN principal	Nom du premier VPN à surveiller
Nom du VPN secondaire	Nom du second VPN à surveiller

Configuration de l'envoi des traps

Démarrage produit - Cold start	Envoyer un trap SNMP au démarrage
Redémarrage passerelle - WarmStart	Envoyer un trap SNMP au redémarrage de la passerelle (routeur avec liaison série uniquement)
Passerelle serveur RawTCP connectée - LinkUp	Envoyer un trap SNMP à la connexion de la liaison IP vers série (routeur avec liaison série uniquement)
Passerelle serveur RawTCP déconnectée - LinkDown	Envoyer un trap SNMP à la déconnexion de la liaison IP vers série (routeur avec liaison série uniquement)
Adresse IP du premier gestionnaire SNMP	Adresse IP du gestionnaire SNMP à laquelle les traps SNMP seront envoyés
Adresse IP du second gestionnaire SNMP	Adresse IP du second gestionnaire SNMP à laquelle les traps SNMP seront envoyés
Version de protocole SNMP	Idem à l'agent SNMP
Nom de communauté	Idem à l'agent SNMP

Nom d'utilisateur	Idem à l'agent SNMP
engineID	Spécifier `engineID` pour définir l'entité SNMP. Un hexadécimal entre 5 et 32 octets est attendu. Le paramètre doit commencer par `0x`.
Algorithme d'authentification	Idem à l'agent SNMP
Mot de passe	Idem à l'agent SNMP
Algorithme de chiffrement	Idem à l'agent SNMP
Clé de chiffrement	Idem à l'agent SNMP

17. SERVEUR MODBUS TCP

17.1. Configuration du serveur Modbus TCP

Etic Telecom met à disposition un serveur Modbus TCP permettant de réaliser des requêtes pour récupérer diverses données collectées par le produit. Mais aussi pour déclencher des fonctionnalités sur le produit. La liste complète des données disponibles est présentée dans la section `Spécification des registres et de leur contenu`.

Accéder au menu ***Configuration*** > ***Système*** > ***Serveur Modbus***. Cochez l'option **Activer** et entrez un numéro de port TCP libre pour le serveur Modbus. Si vous ne spécifiez pas de numéro de port, le port 502 est utilisé par défaut.

Les machines connectées au produit pourront envoyer des requêtes Modbus TCP sur le port spécifié précédemment et ainsi récupérer le contenu des registres demandés.

17.2. Lecture et écriture des registres Modbus

Certains registres sont faits pour être lus ; ils affichent des états pour le produit. D'autres sont conçus pour que vous puissiez écrire à l'intérieur pour des fonctionnalités spécifiques. Ces registres sont détaillés dans le chapitre `Spécification des registres et de leur contenu`.

- Pour lire les registres, envoyez une requête Modbus `Read Holding Registers (FC=3)`.
- Pour écrire sur les registres, envoyez une requête Modbus `Write Multiple Registers (FC=16)` ou `Write Single Register (FC=6)`.
- Pour écrire sur les bobines, envoyez une requête Modbus `Write Single Coil (FC=5)` ou `Force Multiple Coils (FC=15)`.

Fonctionnalité d'envoi de SMS et d'e-mails

Les registres suivants sont dédiés aux options des messages :

- **Registers 500-549:** Expéditeur du message
- **Registers 550-599:** Destinataire du message
- **Registres 600-649:** Objet du message
- **Registres 650-773:** Texte du message

```
Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 500
```

Figure 20. Capture Wireshark d'une requête Modbus pour écrire l'expéditeur du message

Étapes depuis l'automate

1. Écrivez des caractères (ASCII, Latin-1, UTF-8) en commençant par le premier registre de chaque

option.

- Chaque option doit être remplie pour envoyer un e-mail. Uniquement Destination et Texte pour les SMS.
- Le serveur Modbus lira les registres jusqu'à ce qu'il trouve un registre de valeur 0x00. Les registres Expéditeur, Destination et Sujet sont donc limités à 99 caractères.

2. Écrire à l'intérieur des bobines Modbus pour déclencher l'envoi du message.
   - Le réglage de la bobine à l'adresse 0 sur l'état ON enverra un SMS.
   - Le réglage de la bobine à l'adresse 1 sur l'état ON enverra un e-mail.

Table 3. Contenu des registres pour l'expéditeur "ETIC Telecom" : chaque registre contient 2 caractères ; la première lettre est sur le LSB et la seconde sur le MSB.

Registre	500	501	502	503	504	505	506
Registre @	40501	40502	40503	40504	40505	40506	40507
8-bit ASCII	TE	CI	T	le	ce	mo	
Hexadecimal	0x5445	0x4349	0x5420	0x6c65	0x6365	0x6d6f	0x0000
Decimal	21573	17225	21536	27749	25445	28015	0

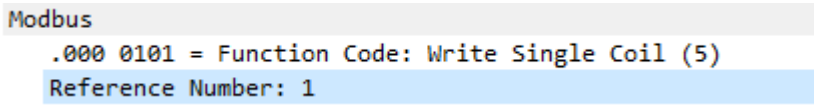


Figure 21. Capture Wireshark d'une requête d'écriture Modbus de l'expéditeur d'un message

17.3. Spécification des registres et de leur contenu

Register 10 Address: 40011

NodeID: 255

Cartographie des registres

Registre	Contenu	Type	Détails
10-13	Latitude de la localisation GPS	LREAL (-1.79e+308 ... 1.79e+308)	Unité : ° • Registre 10 - bit 0: LSB (bit le moins significatif) • Registre 13 - bit 15: MSB (bit le plus significatif)

17.3. Spécification des registres et de leur contenu

Registre	Contenu	Type	Détails
14-17	**Longitude de la localisation GPS**	LREAL (-1.79e+308 ... 1.79e+308)	Unité : ° • Registre 14 - bit 0: LSB • Registre 17 - bit 15: MSB
18-19	**Altitude de la localisation GPS**	REAL (-3.40e+38 ... 3.40e+38)	Unité : mètres • Registre 18 - bit 0: LSB • Registre 19 - bit 15: MSB
20-21	**Vitesse de la localisation GPS**	REAL (-3.40e+38 ... 3.40e+38)	Unité : m/s • Registre 20 - bit 0: LSB • Registre 21 - bit 15: MSB
22	**Précision de la localisation GPS**	UINT16 (0 ... 65535)	Unité : mètres
...			
30	**État de l'entrée numérique**	BITMAP	bit 0 - État de l'entrée (0 désactivé / 1 activé)
31	**État de la sortie numérique**	BITMAP	bit 0 - État de la sortie (0 désactivé / 1 activé)
32	**Alimentation 1**	UINT16 (0 ... 65535)	Unité : dV
33	**Alimentation 2**	UINT16 (0 ... 65535)	Unité : dV
34	**Température interne**	INT16 (-32768 ... 32767)	Unité : °C
...			
40	**Statut du WAN Principal**	UINT16 (0 ... 65535)	0: Aucun / 1: ADSL / 2: Ethernet / 3: Cellulaire / 4: Wi-Fi
41	**Statut du WAN ADSL**	BITMAP	• bit 0: Statut ADSL (0 désactivé / 1 activé) • bit 1: ADSL connecté (0 disconnected / 1 connected)
42	**Statut du WAN Ethernet**	BITMAP	• bit 0: Statut Ethernet (0 désactivé / 1 activé) • bit 1: Ethernet connecté (0 disconnected / 1 connected)
43	**Statut du WAN Cellulaire**	BITMAP	• bit 0: Statut Cellulaire (0 désactivé / 1 activé) • bit 1: Cellulaire connecté (0 disconnected / 1 connected)

Registre	Contenu	Type	Détails
44	**Statut du WAN Wi-Fi**	BITMAP	• bit 0: Statut Wi-Fi (0 désactivé / 1 activé) • bit 1: Wi-Fi connecté (0 désactivé / 1 activé) • bit 2: Auto-DNS WAN Wi-Fi (0 désactivé / 1 activé)
…			
50	**WAN ADSL débit descendant**	UINT16 (0 … 65535)	Unité : kbits/s
51	**WAN ADSL débit montant**	UINT16 (0 … 65535)	Unité : kbits/s
52-53	**WAN ADSL SNR Margin descendant**	REAL (-3.40e+38 … 3.40e+38)	Unité : dB
54-55	**WAN ADSL SNR Margin montant**	REAL (-3.40e+38 … 3.40e+38)	Unité : dB
…			
70	**WAN Cellulaire Niveau de signal**	INT16 (-32768 … 32767)	Unité : dBm
71-72	**WAN Cellulaire SNR**	REAL (-3.40e+38 … 3.40e+38)	Unité : dBm • Registre 71 - bit 0: LSB • Registre 72 - bit 15: MSB
73	**WAN Cellulaire octets reçus**	UINT16 (0 … 65535)	Unité : Mégaoctets
74	**WAN Cellulaire octets transmis**	UINT16 (0 … 65535)	Unité : Mégaoctets
75-76	**WAN Cellulaire octets totaux**	UINT32 (0 … 4294967295)	Unité : Mégaoctets
…			
80	**WAN Wi-Fi Fréquence**	UINT16 (0 … 65535)	Unité : MHz
81	**WAN Wi-Fi Niveau de signal**	INT16 (-32768 … 32767)	Unité : dBm
…			

17.3. Spécification des registres et de leur contenu

Registre	Contenu	Type	Détails
90	**États des interfaces LAN**	BITMAP	• bit 0…1 - état du port LAN Ethernet 0 ◦ 00 désactivé ◦ 10 activé/déconnecté ◦ 11 activé/connecté • bit 2…3 - état du port LAN Ethernet 1 • bit 4…5 - état du port LAN Ethernet 2 • bit 6…7 - état du port LAN Ethernet 3
91	**Statut du LAN Wi-Fi**	BITMAP	• bit 0: Statut du LAN Wi-Fi (0 désactivé / 1 activé) • bit 1: LAN Wi-Fi 802.11n (0 désactivé / 1 activé) • bit 2: LAN Wi-Fi actif sur entrée TOR (0 désactivé / 1 activé)
92	**État de l'accès à distance M2Me**	BITMAP	• bit 0: M2Me actif (0 désactivé / 1 activé) • bit 1: M2Me connecté (0 disconnected / 1 connected) • bit 2: M2Me proxy (0 désactivé / 1 activé)
93	**M2Me Nombre d'utilisateurs distants connectés**	UINT16 (0 … 65535)	
…			
100-109	**États VPN OpenVPN entrants**	BITMAP[10]	bit X: VPN n° X connecté (0 déconnecté-pas créé / 1 connecté)
110-119	**États VPN OpenVPN sortants**	BITMAP[10]	bit X: VPN n° X connecté (0 déconnecté-pas créé / 1 connecté)
120-129	**États VPN IPsec**	BITMAP[10]	bit X: VPN n° X connecté (0 déconnecté-pas créé / 1 connecté)
…			
500-549	**Expéditeur du message**	STRING[50]	50 registres conçus pour écrire 99 caractères (ASCII, Latin-1, UTF-8) - Non utilisé pour les SMS
550-599	**Destinataire du message**	STRING[50]	50 registres conçus pour écrire 99 caractères (ASCII, Latin-1, UTF-8) - Doit être un numéro de téléphone ou une adresse e-mail valide
600-649	**Objet du message**	STRING[50]	50 registres conçus pour écrire 99 caractères (ASCII, Latin-1, UTF-8) - Non utilisé pour les SMS

Registre	Contenu	Type	Détails
650-773	**Texte du message**	STRING[123]	123 registres conçus pour écrire 246 caractères (ASCII, Latin-1, UTF-8)

18. SERVEUR OPC UA

18.1. Configuration du serveur OPC UA

Etic Telecom fournit un serveur OPC UA qui met à disposition différents états et données collectées par le produit. La liste complète des données disponibles est présentée dans la section `Spécification des nœuds du serveur OPC UA`.

Accéder au menu ***Configuration*** > ***Système*** > ***Serveur OPC UA***. Cochez l'option **Actif** et choisissez votre politique de sécurité. Si `Accepter tous les certificats du client` est activé le serveur ne vérifiera pas le certificat client.

18.2. Lecture des noeuds OPC UA

Pour accéder au serveur OPC UA, nous utilisons UaExpert Client disponible sur (https://www.unified-automation.com/downloads/opc-ua-clients.html). Le serveur OPC UA est accessible sur une URL spécifique. L'URL est structurée comme suit :

- Identifiant de protocole "opc.tcp://"
- Adresse IP du routeur: 192.168.0.128
- Numéro de port TCP: 5040

Exemple d'URL: "opc.tcp://192.168.0.128:5040"

- Après avoir lancé le client expert UA, pour ajouter une nouvelle connexion à un serveur OPC UA, cliquez sur le bouton + dans la barre d'outils. Une nouvelle fenêtre de dialogue s'ouvre. Double-cliquez sur < Double-cliquez pour ajouter un serveur >.

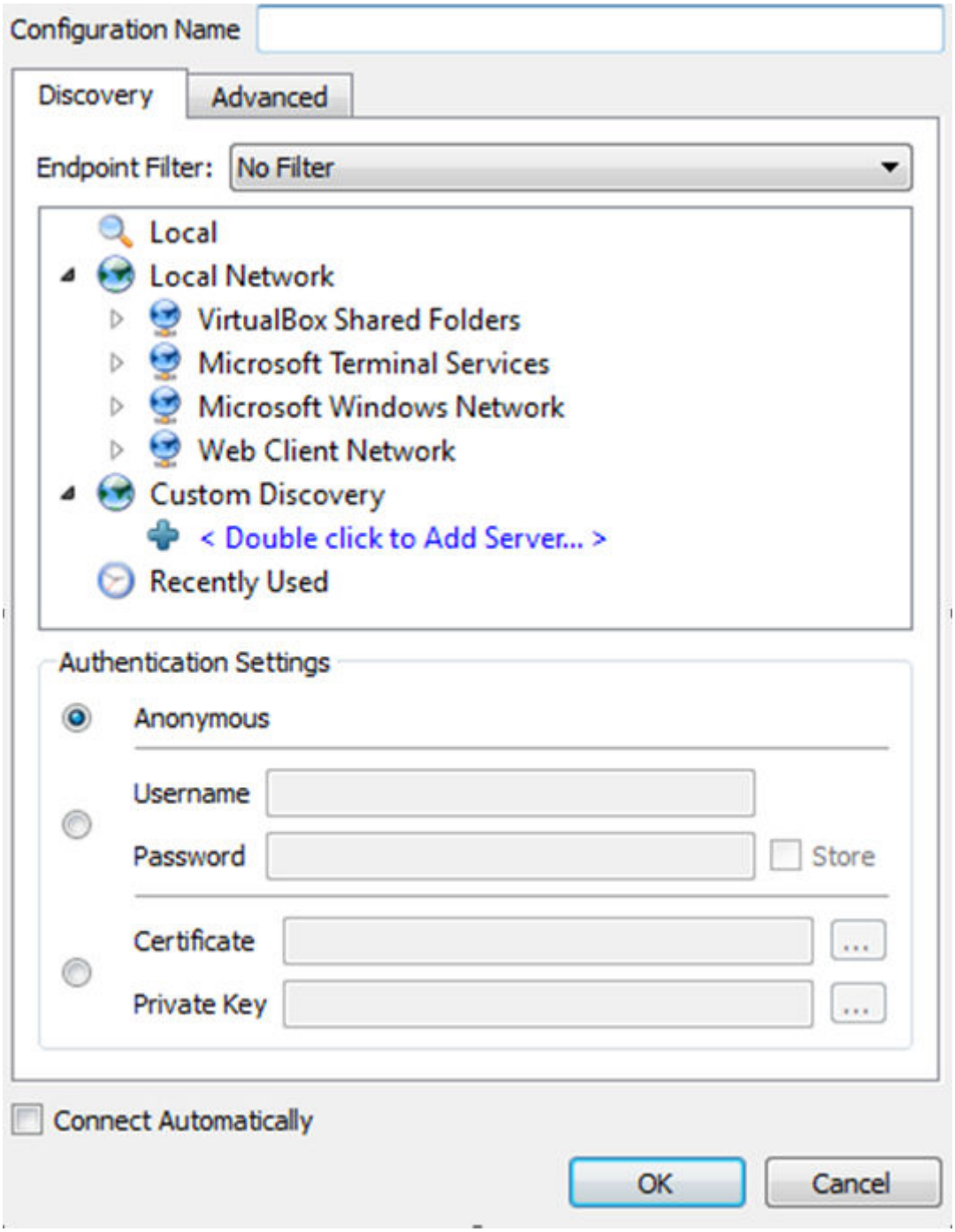


Figure 22. Menu de UAExpert Client pour ajouter un nouveau serveur

- Une fois l'URL ajoutée, le serveur et tous les points de terminaison qu'il fournit sont affichés.
- Choisissez un point de terminaison et confirmez avec OK. Le serveur est maintenant répertorié dans la fenêtre de projet et vous pouvez vous connecter à l'aide du connecteur dans la barre d'outils
- Dans la fenêtre de l'espace d'adressage, vous pouvez voir l'espace d'adressage du serveur actuellement sélectionné.

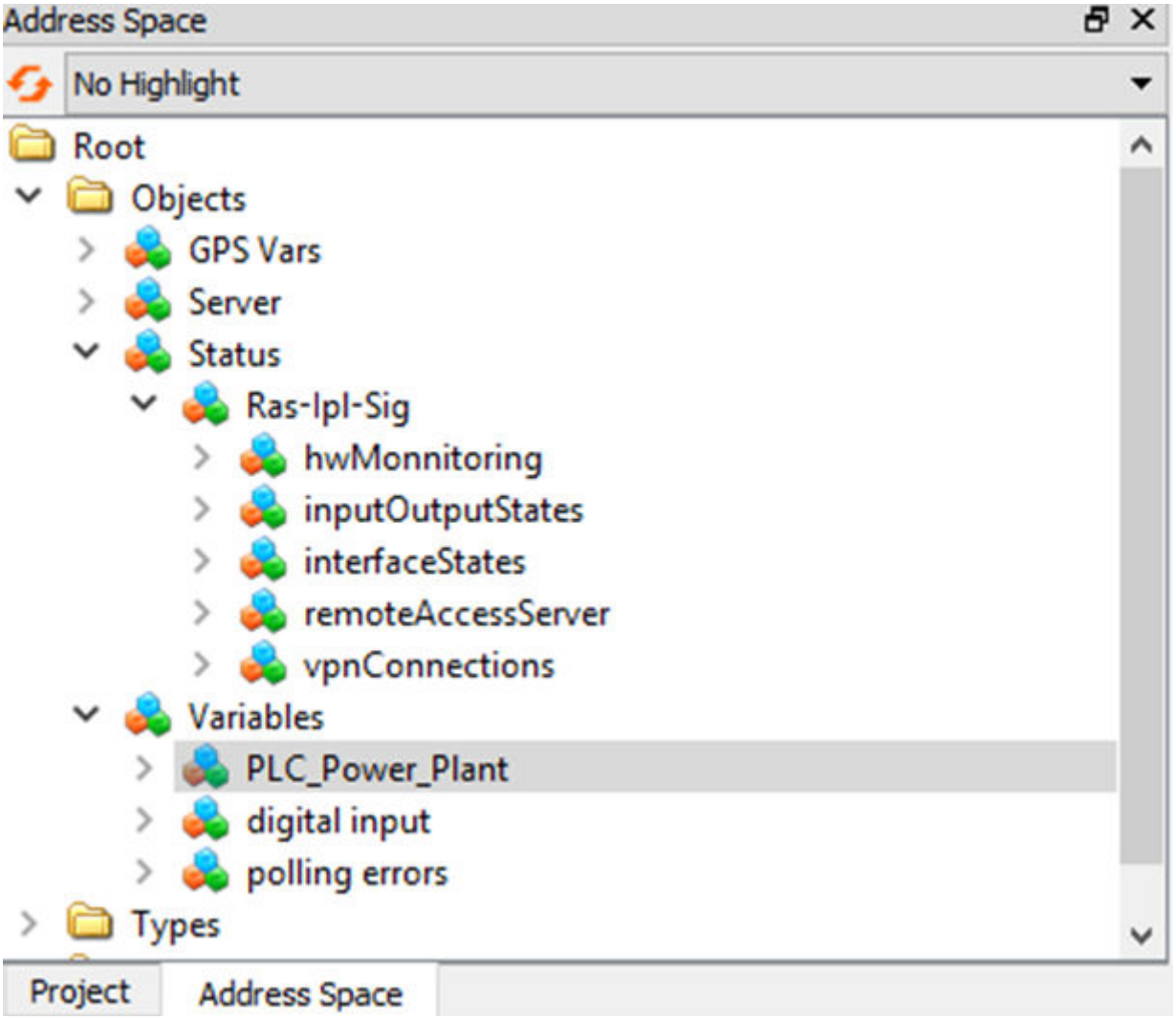


Figure 23. Fenêtre d'espace d'adressage UA Expert Client

18.3. Spécification des noeuds du serveur OPC UA

- Informations sur l'état du matériel :

  status_hwmon_alim1: Power supply 1: ns=2;s=status_hwmon_alim1

  status_hwmon_alim2: Power supply 1: ns=2;s=status_hwmon_alim2

  status_hwmon_temp : Internal temperature: ns=2;s=status_hwmon_temp
- États des entrée/sortie:

  status_etor_state: State of input: ns=2;s=status_etor_state

  status_stor_state: State of output: ns=2;s=status_stor_state
- États des interfaces réseau:
  - LAN
    - Ports LAN

      status_lan(n)_state: status of Ethernet LAN port (n): ns=2;s=status_lan1_state
    - État LAN WIFI:

status_wifi_lan_macadd: WIFI LAN Mac Address: ns=2;s=status_wifi_lan_macaddr

status_wifi_lan_client_signal: WIFI LAN quality signal: ns=2;s=status_wifi_lan_client_signal

status_wifi_lan_client_authorized: WIFI LAN client authorized: ns=2;s=status_wifi_lan_client_authorized

- WAN
  - État WAN ADSL:

    status_wan_adsl_is_connected: WAN ADSL connected: ns=2;s=status_wan_adsl_is_connected

    status_adsl_modem_state : [.etic-param]

    status_wan_adsl_priority: ADSL priority: ns=2;s=status_wan_adsl_priority

    status_wan_adsl_ip_interface: ADSL interface IP address: ns=2;s=status_wan_adsl_ip_interface

    status_adsl_dn_att: adsl downstream attenuation: ns=2;s=status_wan_adsl_dn_att

    status_adsl_dn_snrm: downstream snr margin: ns=2;s=status_wan_adsl_dn_snmr

    status_adsl_up_att: adsl upstream attenuation: ns=2;s=status_wan_adsl_up_att

    status_adsl_up_snrm: upstream snr margin: ns=2;s=status_wan_adsl_up_snmr
  - État WAN cellulaire

    status_wan_gsm_is_connected: WAN GSM connected: ns=2;s=status_wan_gsm_is_connected

    status_wan_gsm_priority: GSM priority: ns=2;s=status_wan_gsm_priority

    status_wan_gsm_operator: GSM operator: ns=2;s=status_wan_gsm_operator

    status_wan_gsm_cid: GSM cell ID: ns=2;s=status_wan_gsm_cid

    status_wan_gsm_lac: GSM location Area Identity: ns=2;s=status_wan_gsm_lac

    status_wan_gsm_ecio: GSM EC/IO: ns=2;s=status_wan_gsm_ecio

    status_wan_gsm_byte_trans : GSM Bytes transmitted: ns=2;s=status_wan_gsm_byte_trans

    status_wan_gsm_byte_recvd : GSM Bytes received: ns=2;s=status_wan_gsm_byte_recvd
  - État WAN Ethernet

    status_wan_eth_is_connected: WAN Ethernet connected: ns=2;s=status_wan_eth_is_connected

    status_wan_eth_is_priority : [.etic-param]

    status_wan_eth_state: WAN Ethernet state: ns=2;s=status_wan_eth_state

    status_wan_eth_ip_interface: Ethernet interface IP address: ns=2;s=status_wan_eth_ip_interface
  - État WAN WIFI

status_wan_wifi_is_connected: WAN WIFI connected: ns=2;s=status_wan_wifi_is_connected

status_wan_wifi_is_priority: WAN WIFI priority: ns=2;s=status_wan_wifi_priority

status_wan_wifi_mode: WAN WIFI mode: ns=2;s=status_wan_wifi_mode

status_wan_wifi_bss: Access point MAC address: ns=2;s=status_wan_wifi_bss

status_wan_wifi_freq: WAN WIFI Frequency (MHz): ns=2;s=status_wan_wifi_freq

status_wan_wifi_signal: WAN WIFI Signal: ns=2;s=status_wan_wifi_signal

status_wan_wifi_ssid: WAN WIFI ssid: ns=2;s=status_wan_wifi_ssid

- DNS

status_wan_applied_dns1: DNS1 applied: ns=2;s=status_wan_applied_dns1

status_wan_applied_dns2: DNS2 applied: ns=2;s=status_wan_applied_dns2

status_wan_applied_dns3: DNS1 applied: ns=2;s=status_wan_applied_dns3

- États des serveurs d'accès à distance :
  - États M2Me

status_m2me_connected: M2Me connected: ns=2;s=status_m2me_connected

status_m2me_ip: M2Me IP address: ns=2;s=status_m2me_ip

status_m2me_state: M2Me IP state: ns=2;s=status_m2me_state

status_m2me_port: M2Me Port: ns=2;s=status_m2me_port

status_m2me_protocol : [.etic-param]

  - Utilisateurs distants:

status_vpn_users_name: Remote user name: ns=2;s=status_vpn_users_name0

status_vpn_users_connected: Remote user connected: ns=2;s=status_vpn_users_connected0

status_vpn_users_ipaddr: Remote user IP address: ns=2;s=status_vpn_users_ipaddr0

  - status_nb_remote_users

status_nb_remote_users: number of connected remote users: ns=2;s=status_nb_remote_users

- Connexions VPN:
  - Ipsec

status_vpn_ipsec_nodes_name: VPN Ipsec name: ns=2;s=status_vpn_ipsec_nodes_name0

status_vpn_ipsec_nodes_connected: VPN Ipsec connected: ns=2;s=status_vpn_ipsec_nodes_connected0

status_vpn_ipsec_nodes_wan_addr: VPN in WAN address: ns=2;s=status_vpn_ipsec_nodes_wan_addr0

status_vpn_iosec_nodes_lan_addr: VPN in WAN address: ns=2;s=status_vpn_ipsec_nodes_lan_addr0

  - OpenVpn
    - Connexions entrantes

status_vpn_in_nodes_name: VPN in name: ns=2;s=status_vpn_in_nodes_name0

status_vpn_in_nodes_connected: VPN in connected: ns=2;s=status_vpn_in_nodes_connected0

status_vpn_in_nodes_wan_addr: VPN in WAN address: ns=2;s=status_vpn_in_nodes_wan_addr0

status_vpn_in_nodes_lan_addr: VPN in WAN address: ns=2;s=status_vpn_in_nodes_lan_addr0

- Connexions sortantes

status_vpn_out_nodes_name: VPN out name: ns=2;s=status_vpn_out_nodes_name0

status_vpn_out_nodes_connected : [.etic-param]

status_vpn_out_nodes_wan_addr: VPN out WAN address: ns=2;s=status_vpn_out_nodes_wan_addr0

status_vpn_out_nodes_lan_addr: VPN out WAN address: ns=2;s=status_vpn_out_nodes_lan_addr0

- Localisation GPS:

Altitude: GPS Location altitude: ns=0;i= 11030

Latitude: GPS Location latitude: ns=0;i= 11010

Longitude: GPS Location Longitude: ns=0;i= 11020

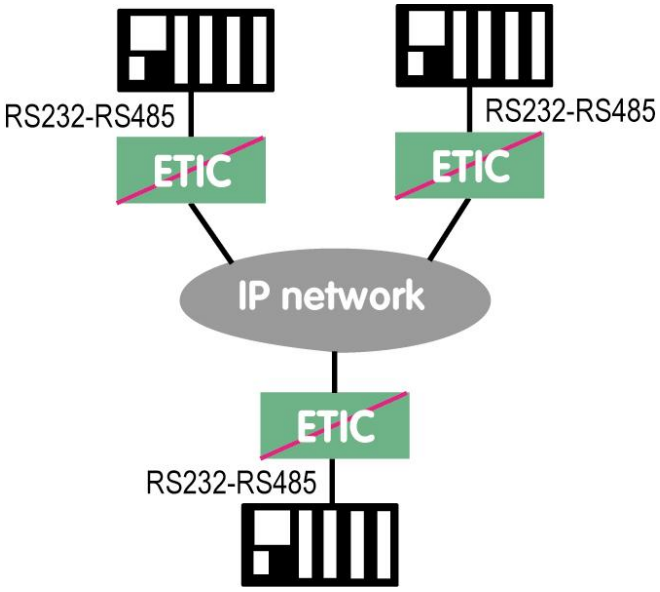
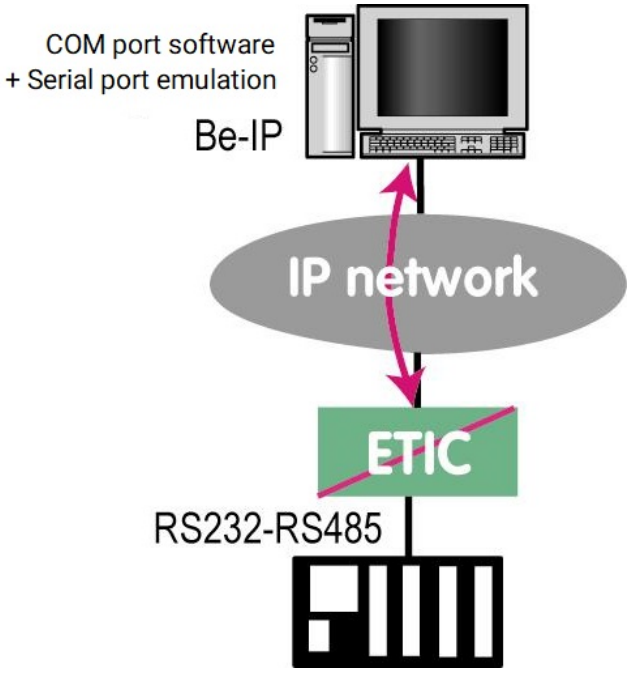
:leveloffset!:

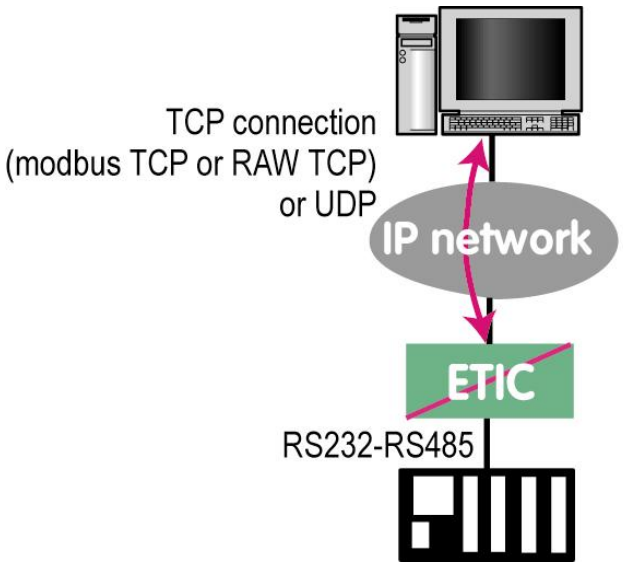
19. PASSERELLES SÉRIE VERS IP

Selon le modèle, le Routeur propose 2 ports série : 2 RS232, ou 1 RS232 et 1 RS485, ou 1 RS422 isolé ou 1 RS485 isolé.

Une passerelle peut être attribuée à chaque port série.

Une passerelle série permet d'utiliser le réseau IP pour transporter des données série entre plusieurs appareils série ou directement avec des appareils connectés au réseau Ethernet.

* Communication entre appareils série	
* Communication entre un périphérique série et un PC via un logiciel d'émulation de port COM	

* Communication entre les appareils série et une application logicielle PC capable d'encapsuler les données série en UDP ou TCP (comme une application logicielle Modbus TCP par exemple)	

Pour réaliser les fonctions décrites ci-dessus, plusieurs types de passerelles sont disponibles.

19.1. Modbus

La passerelle Modbus permet de connecter des appareils série RS232-RS485 maître ou esclaves à un ou plusieurs appareils Modbus TCP connectés au réseau IP

Glossaire

Un client Modbus TCP est un équipement connecté au réseau Ethernet et capable de transmettre des requêtes Modbus à un équipement serveur Modbus TCP qui répondra.

Plusieurs clients Modbus peuvent envoyer des requêtes au même serveur Modbus TCP.

Un serveur Modbus TCP est un équipement connecté au réseau Ethernet et capable de répondre aux requêtes Modbus à un client Modbus TCP.

Un serveur TCP peut répondre à plusieurs clients TCP.

Un équipement Modbus maître est un équipement connecté à une liaison série asynchrone et capable d'envoyer des requêtes à un équipement esclave Modbus connecté au même réseau série.

Un équipement Modbus esclave est un équipement connecté à une liaison série asynchrone et capable de répondre aux requêtes Modbus connectées au même réseau série.

Adresse Modbus : Adresse comprise entre 0 et 254 attribuée à chaque participant à un réseau Modbus.

NOTE	L'adresse Modbus ne doit pas être confondue avec l'adresse IP d'un équipement Modbus.

Sélection d'une passerelle Modbus client ou serveur

Sélectionnez la passerelle serveur Modbus pour connecter des équipements esclaves au port série du produit.

Sélectionnez la passerelle client Modbus pour connecter un équipement maître au port série du produit.

Attribution d'une passerelle Modbus à un port série

La passerelle client (ou serveur) Modbus peut être affectée au port série COM1 ou COM2.

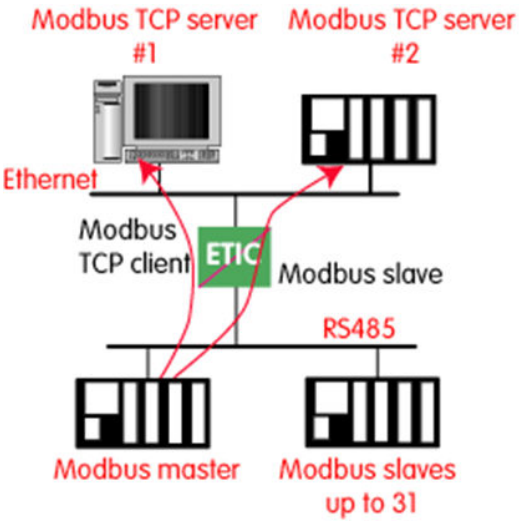
La passerelle client Modbus peut être affectée à un port série (par exemple COM1) tandis que la passerelle serveur Modbus est affectée à l'autre port (par exemple COM2).

Passerelle client Modbus

Cette passerelle permet de connecter un maître Modbus série à l'interface série du produit.

La passerelle peut être connectée à plusieurs serveurs Modbus TCP sur le réseau IP

D'autres esclaves peuvent être connectés à l'interface série.



Comment fonctionne la passerelle client Modbus

Pour accéder à un serveur Modbus TCP sur le réseau IP, une table de correspondance entre une adresse d'esclave Modbus et une adresse IP est définie ; ainsi lorsque le maître Modbus envoie une requête à l'esclave Modbus à l'adresse A, la table de correspondance permet de transmettre la requête à l'adresse IP correspondante.

De plus, le champ d'adresse Modbus de la trame Modbus TCP est défini sur A.

La table de mappage peut contenir 32 lignes permettant à un maître Modbus d'adresser 32 serveurs sur le réseau IP.

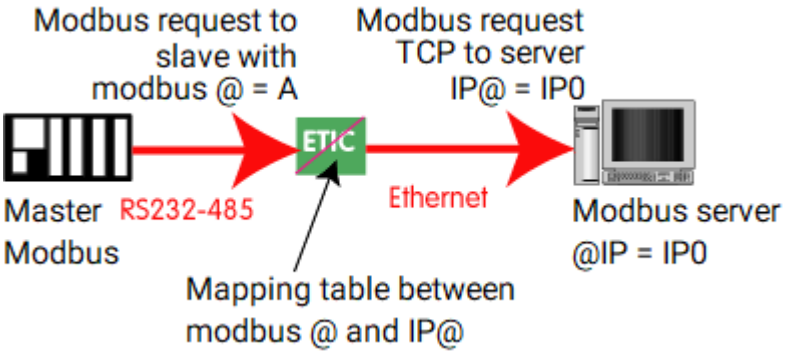


Figure 24. Table de mappage Modbus

Configurer la passerelle

Accéder au menu ***Configuration*** > ***Passerelles*** > ***IP-RS*** > ***Modbus*** > ***Client Modbus***, puis cochez l'option **Activer le client Modbus**.

Paramètre **Port COM**:

Sélectionnez la liaison série 1 ou 2 du produit.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Protocol Modbus**:

Sélectionnez RTU (hexa) ou ASCII

Paramètre **Temps inter-caractères**:

Définissez le délai maximum que la passerelle devra attendre entre la récepetion des caractères reçu d'un paquet de réponse Modbus.

Paramètre **Timeout d'inactivité TCP**:

Définissez le temps pendant lequel la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Port TCP**:

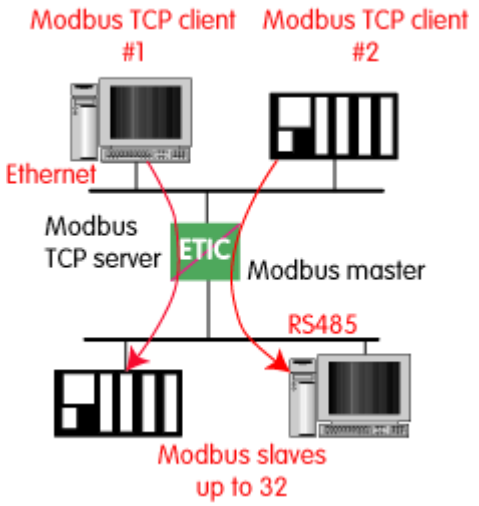
Définissez le numéro de port que la passerelle doit utiliser. Le port Modbus TCP par défaut est 502.

Paramètre **Esclave Modbus**:

La table permet de mapper une adresse d'esclave Modbus à une adresse IP.

Passerelle serveur Modbus

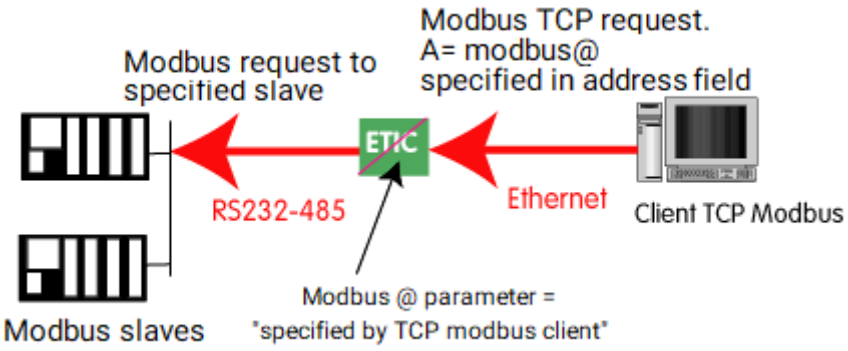
Cette passerelle permet de connecter des esclaves Modbus série à l'interface série du produit. Jusqu'à 32 esclaves peuvent être connectés au port RS485.



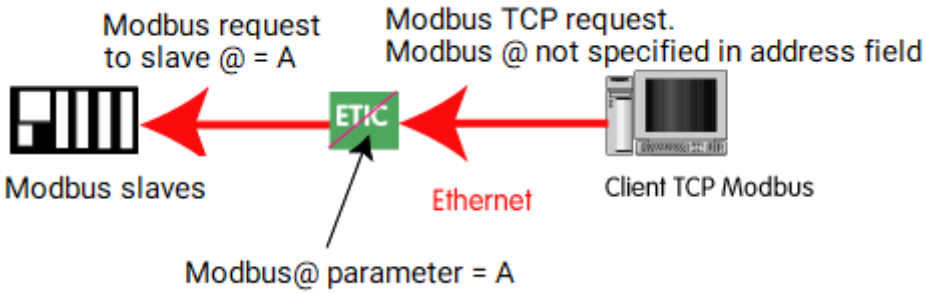
Fonctionnement de la passerelle serveur Modbus

Un client Modbus TCP envoie un client Modbus TCP à la passerelle.
La passerelle se comporte comme un maître sur la liaison série. Elle transcode et transmet la requête sur la liaison série.
L'adresse esclave Modbus de la requête est :

- Soit l'adresse contenue dans le champ adresse Modbus TCP; dans ce cas, plusieurs esclaves peuvent être adressés sur la liaison série.



- Soit une adresse fixe configurée dans la passerelle (voir ci-dessous) ; dans ce cas, un seul esclave peut être adressé sur la liaison série.



CAUTION	Plusieurs clients TCP Modbus peuvent envoyer des requêtes aux esclaves sur la liaison série. Il faut néanmoins veiller à ne pas saturer la liaison série car son débit est bien inférieur à celui de la liaison Ethernet.

Configurer la passerelle

Accéder au menu ***Configuration*** > ***IP-RS*** > ***Passerelles*** > ***Modbus*** > ***Serveur Modbus***, puis cochez l'option **Activer le serveur Modbus**.

Paramètre **Port COM**:

Sélectionnez la liaison série 1 ou 2 du produit.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Protocol Modbus**:

Sélectionnez RTU (hexa) ou ASCII.

Paramètre **Activer la fonction proxy/cache**:

Si cette fonction est active, une requête est envoyée à un esclave uniquement si la même requête n'a pas été envoyée depuis un certain temps. Ce temps est défini par le paramètre **rafraîchissement du cache**.

Paramètre **Rafraîchissement du cache**:

Définit le temps minimum entre deux requêtes identiques adressées à un esclave.

Paramètre **Temps inter-caractères**:

Définissez le délai maximum que la passerelle devra attendre entre la récepetion des caractères reçu d'un paquet de réponse Modbus.

Paramètre **Adresse esclave Modbus**:

Si la valeur "0" est sélectionnée, la passerelle utilise l'adresse Modbus spécifiée par le client Modbus TCP pour adresser l'esclave Modbus sur la liaison série; jusqu'à 32 esclaves peuvent être adressés sur la liaison série.

Si une valeur particulière est sélectionnée (1 à 255), la passerelle envoie toutes les requêtes à l'esclave sélectionné ; un seul esclave peut être adressé sur la liaison série.

Paramètre **Timeout d'inactivité TCP**:

Définissez le temps pendant lequel la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Temps d'attente réponse esclave**:

Définissez le temps que la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Port TCP**:

Définissez le numéro de port que la passerelle doit utiliser. Le port Modbus TCP par défaut est 502.

Paramètre **Nombre de réitérations locales**:

Définissez le nombre de fois que la passerelle répétera une requête en cas d'absence de réponse de l'esclave.

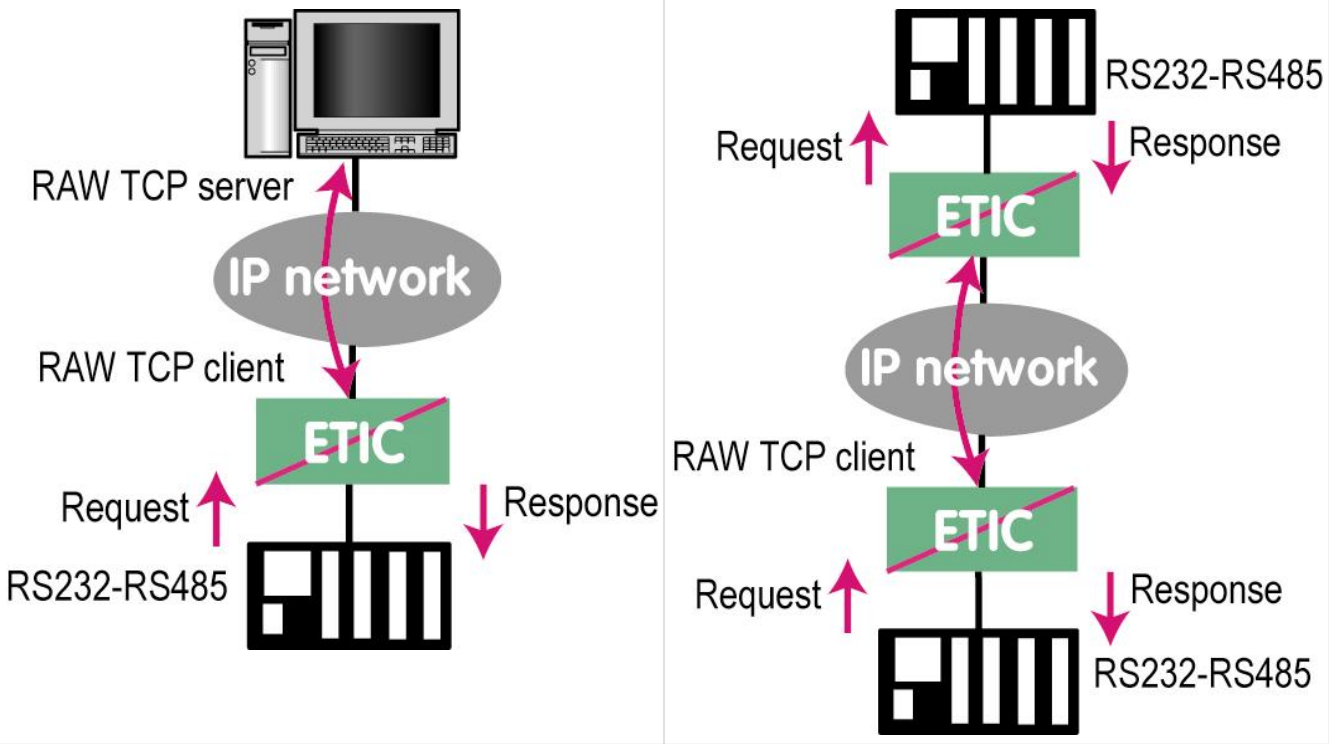
19.2. RAW TCP

Client Raw TCP

La passerelle client Raw peut être utilisée si un périphérique série "maître" doit envoyer des requêtes à un périphérique esclave (également appelé serveur) situé sur le réseau IP.

Le serveur peut être soit une passerelle Etic Telecom, soit un PC incluant un serveur TCP logiciel.

Table 4. Passerelle client RAW TCP



Pour configurer la passerelle client Raw, sélectionnez ***Configuration*** > ***Passerelles*** > ***IP-RS*** > ***Transparent*** > ***Raw client COMx***, puis cochez l'option **Activer**.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Taille du buffer de réception**:

Définissez la longueur maximale d'une chaîne asynchrone que la passerelle stockera avant de la transmettre au réseau IP.

Paramètre **Timeout fin de trame RS**:

Configurez le délai que la passerelle attendra avant de déclarer complète une chaîne reçue du périphérique asynchrone.

Une fois déclarée terminée, la passerelle transmettra la chaîne au réseau IP.

Paramètre **Timeout d'inactivité TCP**:

Définit le temps pendant lequel la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Port TCP**:

Définissez le numéro de port que la passerelle doit utiliser.

CAUTION	Si deux passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même numéro de port TCP.

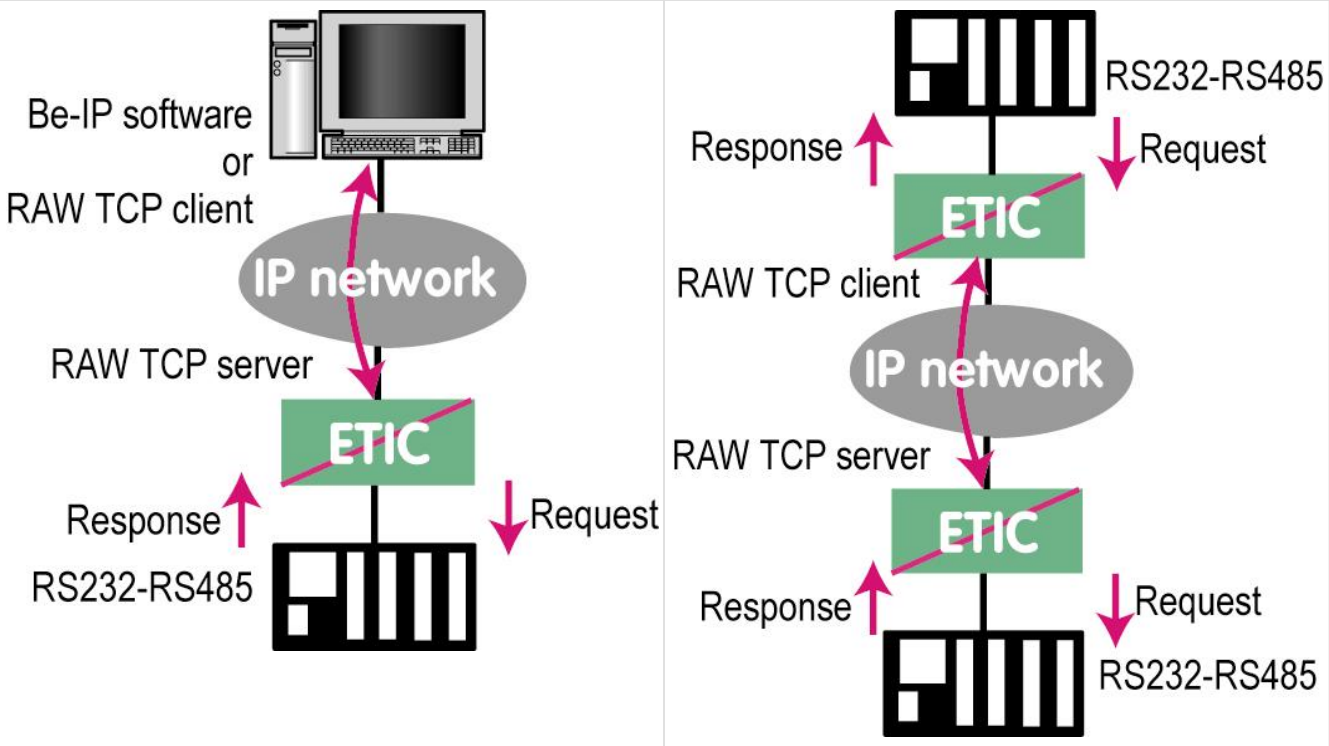
Paramètre **Addresse IP serveur**:

Définissez l'adresse IP du serveur Raw. La passerelle se connectera à ce serveur et lui enverra les données reçues sur la liaison série.

Passerelle du serveur Raw

Cette passerelle peut être utilisée si un périphérique esclave série doit répondre à des requêtes provenant de périphériques situés sur le réseau IP et agissant comme un maître (également appelé client TCP).

Table 5. Passerelle du serveur Raw



Pour configurer le serveur de passerelle RAW, sélectionnez ***Configuration*** > ***Passerelles*** > ***IP-RS*** > ***Transparent*** > ***Raw server COMx***, puis cochez l'option **Activer**.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Taille du buffer de réception**:

Définissez la longueur maximale d'une chaîne asynchrone que la passerelle stockera avant de la transmettre au réseau IP.

Paramètre **Timeout fin de trame RS**:

Configurez le délai que la passerelle attendra avant de déclarer complète une chaîne reçue du périphérique asynchrone.

Une fois déclarée terminée, la passerelle transmettra la chaîne au réseau IP.

Paramètre **Timeout d'inactivité TCP**:

Définit le temps pendant lequel la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Port TCP**:

Définissez le numéro de port que la passerelle doit utiliser.

CAUTION	Si deux passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même numéro de port TCP.

19.3. UDP brut

La passerelle UDP RAW permet de connecter ensemble un groupe d'appareils série ou IP via un réseau IP. Le groupe peut inclure des appareils IP s'ils disposent des logiciels capables de recevoir ou de transmettre des données série encapsulé en UDP.

Les données série transmises par chaque appareil sont transmises à tous les autres appareils série via le réseau IP.
Une table d'adresses IP définit la liste des appareils appartenant au groupe.
Les données série sont encapsulées dans le protocole UDP.

Le datagramme UDP est envoyé à toutes les adresses IP de destination stockées dans la table.

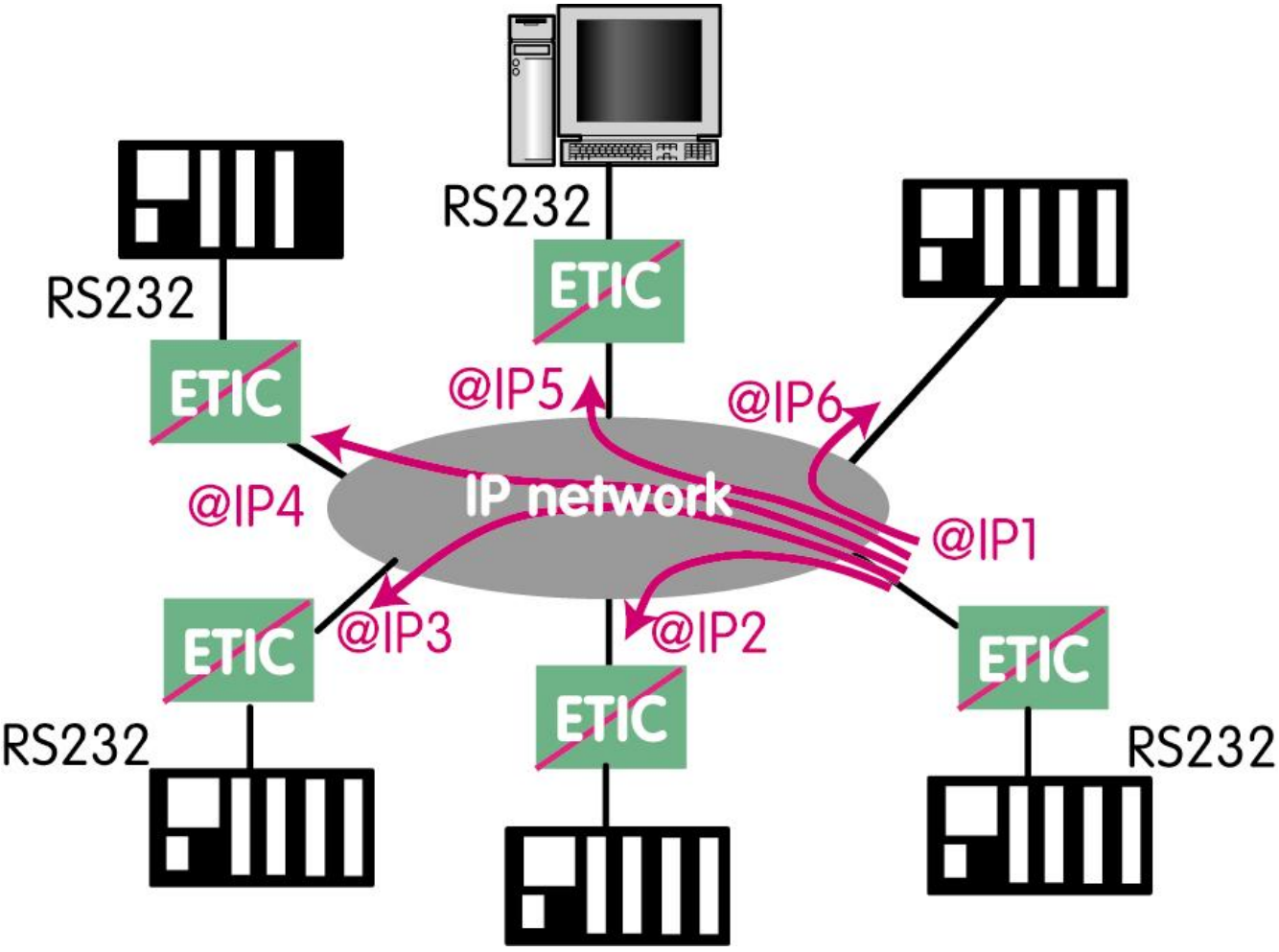


Figure 25. Passerelle UDP RAW

Accéder au menu ***Configuration*** > ***Passerelles*** > ***IP-RS*** > ***Transparent*** > ***Raw UDP COMx***, puis cochez l'option **Activer le client Modbus**.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Taille du buffer de réception**:

Définissez la longueur maximale d'une chaîne asynchrone que la passerelle stockera avant de la transmettre au réseau IP.

Paramètre **Timeout fin de trame RS**:

Configurez le délai que la passerelle attendra avant de déclarer complète une chaîne reçue du périphérique asynchrone.

Une fois déclarée terminée, la passerelle transmettra la chaîne au réseau IP.

Paramètre **Port UDP**:

Définit le numéro de port que la passerelle doit utiliser.

CAUTION	Si deux passerelles du même type sont actives sur les deux ports série, elles ne

peuvent pas utiliser le même numéro de port UDP.

Paramètre **Destination**:

Ce tableau stocke les adresses IP des passerelles vers lesquelles les données série, encapsulées dans UDP, doivent être envoyées.
Un numéro de port UDP différent peut être saisi pour chaque adresse IP de destination.

19.4. Raw multicast

Cette passerelle est conçue pour connecter un appareil série à plusieurs appareils sur un réseau IP.

Elle utilise le protocole `multicast` qui peut délivrer simultanément une trame IP à plusieurs périphériques sans augmenter le trafic: les données RS232 sont transmises dans une trame IP avec une adresse IP particulière appelée adresse multicast; tous les abonnés à cette adresse peuvent recevoir la trame.

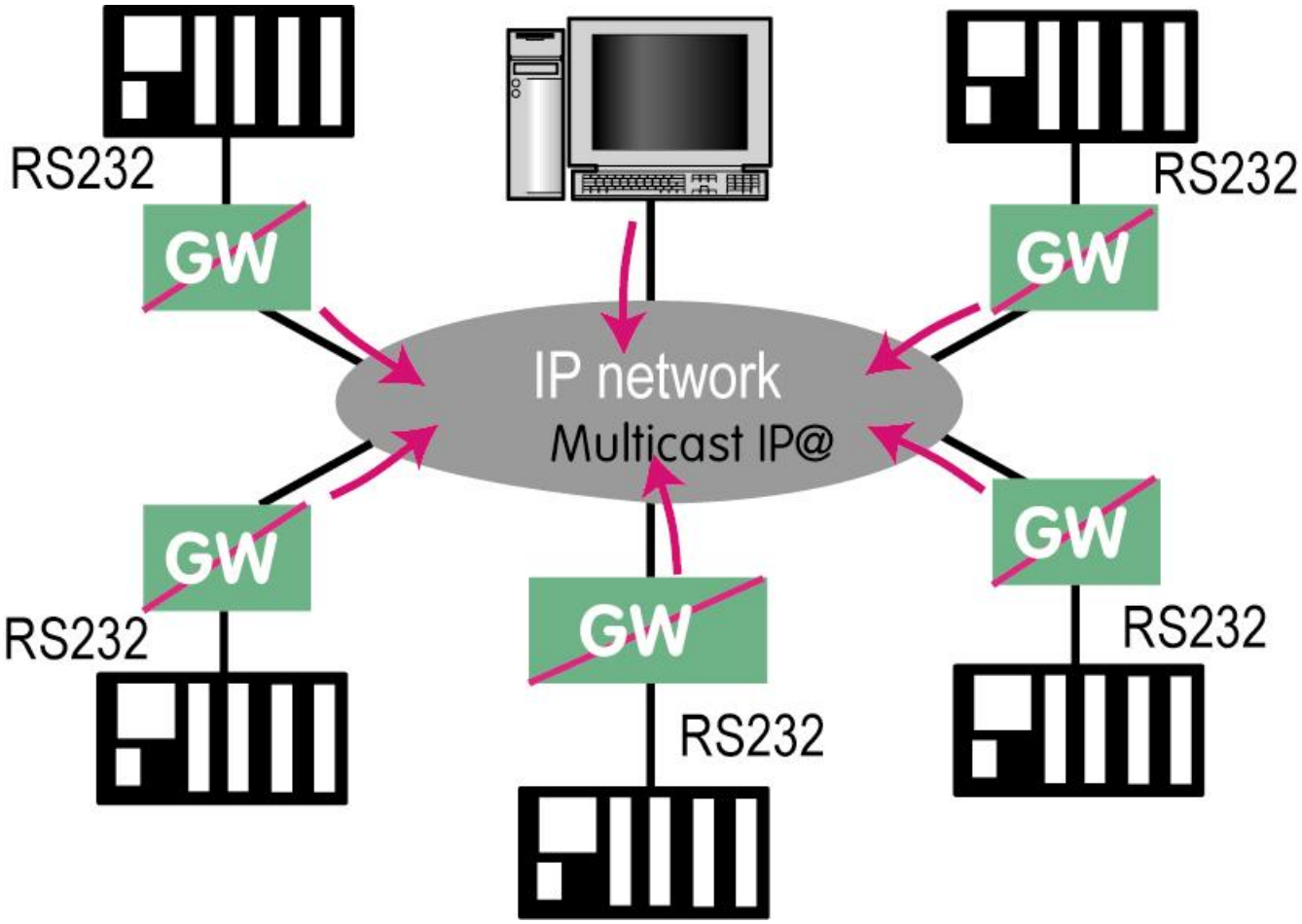


Figure 26. Passerelle Raw multicast

Configurer la passerelle

Accéder au menu ***Configuration*** > ***Passerelles*** > ***IP-RS*** > ***Transparent*** > ***Raw Multicast COMx***, puis cochez l'option **Activer**.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Taille du buffer de réception**:

Définissez la longueur maximale d'une chaîne asynchrone que la passerelle stockera avant de la transmettre au réseau IP.

Paramètre **Timeout fin de trame RS**:

Configurez le délai que la passerelle attendra avant de déclarer complète une chaîne reçue du périphérique asynchrone.

Une fois la chaine déclarée terminée, la passerelle transmettra la chaîne au réseau IP.

Paramètre **Port UDP**:

Définit le numéro de port que la passerelle doit utiliser.

CAUTION	Si deux passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même numéro de port UDP.

Paramètre **Adresse IP du groupe multicast**:

Définissez l'adresse IP attribuée au groupe multicast conformément aux règles IANA.

19.5. Unitelway

La passerelle Unitelway permet de connecter un automate maître Unitelway à un réseau IP.

Elle permet notamment d'effectuer la télémaintenance d'un automate Schneider Electric RS485 via un réseau IP.

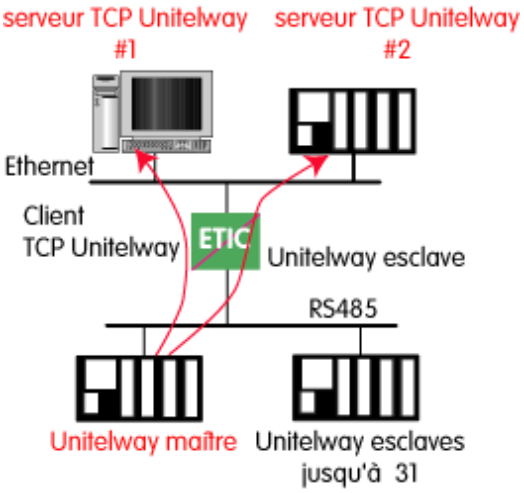


Figure 27. Passerelle Unitelway

Configurer la passerelle

Accéder au menu ***Configuration > Passerelles > IP-RS > Unitelway***, puis cochez l'option **Activer**.

Paramètre **Port COM**:

Sélectionnez la liaison série 1 ou 2 du produit.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Adresse Xway**:

Adresse de la passerelle dans le réseau Xway.

Paramètre **Timeout d'inactivité TCP**:

Définit le temps que la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Esclaves Unitelway**:

Mapping entre l'adresse de chaque esclave Unitelway émulé par la passerelle et les adresses IP et XWAY de l'appareil sur Ethernet.

19.6. Telnet

Cette passerelle permet à un PC exécutant un client Telnet de se connecter à un équipement connecté à la liaison série du Routeur.

Le débit et le format des caractères sur la liaison série peuvent être contrôlés selon la norme RFC2217.

Configurer la passerelle

Sélectionnez ***Configuration*** > ***Passerelles***> ***IP-RS*** > ***Telnet***, puis cochez l'option **Activer**.

Paramètre **Port COM**:

Sélectionnez la liaison série 1 ou 2 du produit.

Paramètres **Débit binaire, Parité, Données, Bits d'arrêt**:

Permet de définir le débit et le format de la liaison série asynchrone.

Paramètre **Timeout d'inactivité TCP**:

Définit le temps pendant lequel la passerelle attendra avant de déconnecter la liaison TCP si aucun caractère n'est détecté.

Paramètre **Port TCP**:

Définit le numéro de port que la passerelle doit utiliser.

19.7. USB

Passerelle USB

La passerelle USB vers IP est capable de transférer le trafic IP des appareils connectés au réseau Ethernet vers un périphérique USB.

Sur l'interface USB, le routeur se comporte comme un hôte USB et un client PPP.

Le périphérique USB connecté à l'interface USB du routeur doit se comporter comme un serveur PPP.

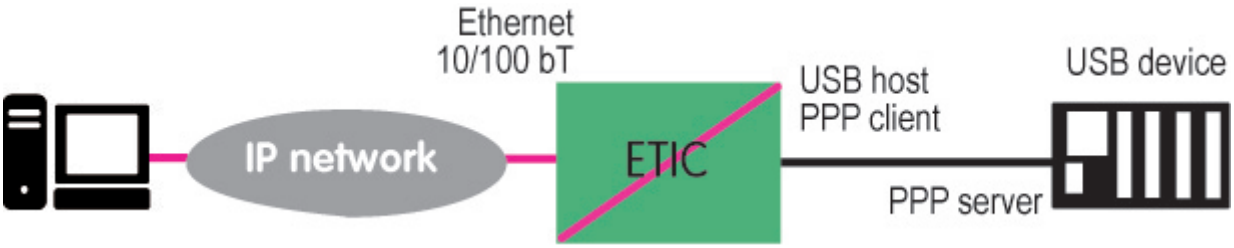


Figure 28. Passerelle USB

Adresse IP de destination; cas principal

Lorsqu'un équipement, connecté au réseau Ethernet, doit transmettre des données au périphérique USB, l'adresse de destination des trames IP qui doivent être transmises au périphérique USB doit être une adresse IP spécifique attribuée à la passerelle USB du routeur (voir la configuration ci-dessous).

Adresse IP de destination ; cas Modbus

Si aucune adresse IP spécifique n'est attribuée à la passerelle USB (voir ci-dessous), le routeur transmet uniquement le trafic Modbus TCP à l'interface USB.
L'adresse IP de destination des trames IP doit être l'adresse IP LAN du routeur.

Configuration

Accéder au menu ***Configuration*** > ***Passerelles*** > ***USB***, puis cochez **Activer**.

Option **Utiliser une adresse IP spécifique**:

Si seulement le trafic Modbus TCP doit être transféré vers le périphérique USB, cette option ne doit pas être sélectionnée.
Si d'autres types de trafic doivent être transférés, activer cette option.

Paramètre **Adresse IP spécifique**:

Si seulement le trafic Modbus TCP doit être transmis à l'interface USB, aucune adresse IP ne doit être saisie.

Si d'autres types de trafic doivent être transférés vers le périphérique USB, une adresse IP supplémentaire doit être attribuée au routeur.

Cette adresse appartient au réseau connecté à l'interface LAN du routeur. Il s'agit de l'adresse IP de la passerelle USB.

Elle sera utilisée comme adresse IP de destination des trames IP qui doivent être transmises au périphérique USB.

Option **Autoriser l'accès depuis l'interface WAN**:

Il est nécessaire de cocher cette option si le PC est connecté au réseau via l'interface WAN du routeur.
Ce n'est pas nécessaire si le PC distant est connecté au routeur via un VPN ou via l'interface LAN.

20. COLLECT & ALERT

L'option Collect&Alert disponible sur les routeurs RAS et IPL permet de superviser à distance un ou plusieurs automates. Les automates Modbus TCP et OPCUA UA peuvent être adressés. En combinant avec les passerelles série vers IP, le Modbus RTU peut également être supervisé.

Les routeurs sont capables de communiquer avec les automates et lire leurs registres. De ces valeurs, il est possible de :

- Afficher dans la page d'exploitation la valeur actuelle des variables, et les écrire
- Configurer des alarmes pour recevoir un email/sms en cas de dépassement de seuil
- Générer un rapport contenant l'évolution des variables

20.1. Variables et Synoptiques

Pour visualiser/écrire les registres des automates accessibles depuis le routeur, il est nécessaire de configurer la communication entre les deux.

La configuration se décompose en plusieurs points:

- La source de données : configuration de l'accès à un serveur de données (OPC UA ou ModBus)
- Les variables : rattachées à une source de données, elles correspondent à un ou plusieurs registres
- Les synoptiques : permettent l'affichage des variables à des opérateurs sur la page d'exploitation

Pour aider à la configuration, il est possible de voir l'état des sources de données et des variables dans la page ***Collect&Alert > Etat des serveurs***.

Source de données

Accéder au menu ***Collect&Alert > Sources de données***. Vous pouvez y configurer de nouvelles sources de données.

Activée	Activer ou désactiver la source de données
Nom de la source de données	Nom pour identifier la source de données
Le type de la source de données	`ModBus` ou `OPC UA`

Les paramètres suivants sont dépendants du type de la source de données.

ModBus

Période d'échantillonnage (secondes)	Intervalle entre 2 lectures de la source de données
Timeout (par variable)(secondes)	Timeout de la lecture d'une variable. Attention, une lecture est faite par variable.
Adresse IP du serveur ModBus	Adresse IP du serveur ModBus
Port serveur	Port du serveur ModBus
Esclave ModBus ou Unit ID	Esclave ModBus ou Unit ID où lire les registres sur le serveur
Lecture bit	Code à utiliser pour la lecture d'un bit de l'automate
Lecture mot 16 bits	Code à utiliser pour la lecture d'un mot de 16 bits
Lecture double mot (32 bits)	Code à utiliser pour la lecture d'un mot de 32 bits
Lecture nombre à vigule flottante 32 bits	Code à utiliser pour la lecture d'un float de 32 bits

OPC UA

Intervalle d'émission (secondes)	Intervalle entre 2 lectures de la source de données
Adresse IP du serveur OPC UA	Adresse IP du serveur OPC UA
Port serveur	Port du serveur OPC UA
Authentification Utilisateur/Mot de passe	Permet de configurer une connexion au serveur avec Login et mot de passe. Si désactivé, le serveur doit accepter les connexions anonymes.

Le mode de sécurité des connexions OPCUA est `None`.

Variable

Accéder au menu ***Collect&Alert*** > ***Variables***. Vous pouvez créer des variables associées à des sources de données.

Nom	Nom de la variable
Type de variable	`ModBus`, `Entrée TOR` ou `OPC UA`
Source de données	(OPC UA, ModBus) source de données dans laquelle sera lue la variable
NodeID Namespace Index	(OPC UA) Namespace dans le serveur OPC UA où trouver la variable
NodeID Type de l'Identifiant	(OPC UA) Type de l'identifiant de la variable
NodeID L'Identifiant	(OPC UA) Identifiant de la variable. Chaine de caractères ou numérique suivant le type

Adresse du registre	(ModBus) Le registre de la variable. Si la variable est sur 2 registres (32bits), le registre suivant sera également utilisé.

Type de variable

La variable peut être de différents types:

- Bit
- Bit dans mot (uniquement ModBus)
- Entier 16 bits non signé
- Entier 16 bits signé
- Entier 32 bits non signé
- Entier 32 bits signé
- Flottant 32 bits

Suivant le type, des champs sont disponibles. Les principaux sont:

Nombre de décimales	Nombre de décimales après la virgule à afficher
Gain	Multiplicateur de la valeur lue dans le registre
Offset	Décalage de la valeur lue dans le registre. Appliqué après le gain
Unité	Unité correspondante
Valeur à 0	Valeur à afficher dans le cas où le bit est à 0
Valeur à 1	Valeur à afficher dans le cas où le bit est à 1

Déclencher une alarme

Il est possible d'associer une alarme à chaque variable. Si la condition configurée est atteinte, alors une alarme est levée.

Déclenchement alarme	Configuration de la condition de déclenchement de l'alarme
Acquittement nécessaire	L'alarme doit être explicitement acquittée même si la condition n'est plus vérifiée
Description du défaut	Description qui sera associée à l'alarme

Il est possible d'associer une alerte à ces alarmes pour prévenir par email et/ou sms un destinataire (voir la page Cycles d'alerte)

Gestion des droits d'écriture d'une variable

La gestion des droits d'écriture d'une variable se fait à l'aide des rôles Collect & Alert. Voir la page Ecriture d'une variable.

Synoptiques

Un synoptique regroupe un ensemble de variables, provenant d'une ou plusieurs sources de données. Cela permet de visualiser les variables sur la page d'exploitation. Cette page est accessible aux opérateurs (voir la page Page web d'exploitation).

Accéder au menu ***Collect&Alert > Synoptiques*** pour les créer.

20.2. Ecriture d'une variable

Les variables sont associées à une source de données, et pointent vers un registre de ce dernier. Voir la page Variables et Synoptiques pour la configuration entre le registre d'un automate et une variable.

La gestion des droits d'écriture d'une variable se fait à travers les Rôles et Exploitants Collect & Alert. Accéder au menu ***Collect&Alert > Droits des Exploitants C&A*** pour les configurer.

NOTE	Lors de l'écriture d'une variable OPCUA, une nouvelle connexion au serveur est utilisée. Le serveur OPCUA doit donc accepter au minimum 2 connexions simultanément pour pouvoir lire et écrire les variables.

Configuration de l'écriture d'une variable

Rôles Collect & Alert

Dans la définition d'une variable, il est possible d'indiquer quel rôle peut écrire cette dernière. Un rôle peut donc avoir les droits d'écriture sur un ensemble de variables.

Un rôle est seulement défini par un identifiant unique.

Identifiant du rôle	Nom du rôle

Exploitants Collect & Alert

Un exploitant Collect & Alert est l'association entre un utilisateur et un rôle Collect & Alert. Un utilisateur peut avoir plusieurs rôles, ce qui permet une configuration fine de qui peut écrire telle ou telle variable.

Un exploitant est donc composé d'un utilisateur et d'un rôle.

Rôle Collect & Alert	Nom du rôle associé à l'exploitant
Utilisateur	Utilisateur qui aura les droits d'écriture sur les variables de ce rôle

Ecriture d'une variable

Une fois les rôles et exploitants configurés, l'écriture des variables se fait par le portail d'exploitation. La variable doit être associée à un Synoptique pour être visible dans le portail d'exploitation.

Pour accéder au portail d'exploitation, l'exploitant Collect & Alert doit également être configuré en tant qu'Opérateur. Voir la page Gestion des opérateurs.

20.3. Cycles d'alertes

Les alertes Collect & Alertes sont associées à une ou plusieurs variables.

Si l'une des ces variables atteint sa condition de déclenchement d'alarme, alors, une alerte est levée et les destinataires sont prévenus.

Pour ajouter une alerte, accéder au menu ***Collect&Alert > Cycles d'alerte***

Nom	Nom de l'alerte
Variables déclenchant le cycle d'alerte	Ensemble des variables qui déclenchent l'alerte
Destinataires des messages d'alerte	Les utilisateurs à contacter en cas d'alerte
Type	Type de canal à utiliser : Email et/ou SMS
Nombre de rappels	Nombre de rappels à envoyer tant que l'alerte n'a pas été acquittée
Périodicité des rappels (minutes)	Temps entre les rappels

Acquittement des alertes

Une fois déclenchée, une alerte doit être acquittée si la variable est configurée comme telle.

L'acquittement peut se faire de différentes manières :

- Par entrée TOR si l'option **Acquittement global par entrée TOR** est activée
- Par la page d'administration ***Collect&Alert > État des alertes***
- Par le portail d'exploitation ***Collect&Alert > Alarmes***

21. MIRRORING DISTANT ERSPAN

21.1. Principe du mirroring

Le mirroring permet de copier le trafic d'un port vers un autre port. Cela permet d'analyser le trafic réseau avec différents outils d'analyse comme WireShark.

ERSPAN (Encapsulated Remote SPAN) permet de transférer le réseau vers un réseau distant. Les trames réseaux sont encapsulées dans un tunnel GRE (Generic Routing Encapsulation). L'analyse du réseau local peut donc être faite sur une machine distante.

21.2. Configuration

- Le Mirroring est aujourd'hui disponible uniquement sur les produits de la gamme 100.
- ERSPAN est disponible en version 1.
- Le réseau mirroré est le réseau local.

Accéder au menu ***Configuration > Réseau > ERSPAN***

Adresse source	Adresse source pour encapsuler les données
Adresse destination	Adresse de destination où transférer le trafic du LAN
Clé GRE	Clé du tunnel GRE
Identifiant du tunnel	Identifiant du tunnel ERSPAN
Débit maximal	Limite de débit du mirroring

22. DIAGNOSTIC

Lors de la configuration de votre produit, vous devrez peut-être effectuer des vérifications pour vous assurer que votre configuration fonctionne. Certains outils sont disponibles dans l'interface d'administration pour vous aider à les faire.

22.1. Journaux

Voir la section Gestion des journaux

22.2. État du réseau

Accéder au menu ***Diagnostic > État du réseau***

Interfaces	État de vos interfaces WAN/LAN et ainsi que les DNS actifs. Vous pouvez visualier des informations sur les différentes priorités, débits de données, atténuation, délais, SNR, ... de chaque interface disponibles Champ Statut du modem ADSL: • Connected: Le modem ADSL est connecté • Showtime tc sync: Le modem ADSL est connecté • Full init: Phase de négociation de la connexion • Handshake: Contact établi avec l'ATU-C (DSLAM), ATU-C détecté • Silent: Aucun ATU-C détecté • Idle: Modem prêt, aucun ATU-C détecté • Exception: Le modem était connecté, une erreur (câble débranché en général) a provoqué une déconnexion
M2Me	Statut de la connexion au service M2Me
Utilisateurs distants	Liste des opérateurs actuellement connectés
Connexions VPN	Statut de votre VPN OpenVPN/IPSec (lesquels sont connectés, depuis quand...)
Routes	Table ARP, la table de routage et de routage étendu de votre routeur
Baux DHCP	Une table qui affiche les baux DHCP actuels. Chaque ligne correspond à un bail: Nom d'hôte du client, adresse MAC, adresse IP allouée et date d'expiration du bail

22.3. Statistiques

Accéder au menu ***Diagnostic > Statistiques***

Bins ADSL	Utilisation des bins du modem ADSL

Statistiques ADSL	Visualier l'historique des erreurs montantes/descendantes/de connexion de la connexion ADSL
Cellulaire	Journaux d'ID de cellule (CID) / Qualité du signal (SQ) / Rapport signal/bruit (SNR) / Octets reçus / Octets envoyés
Données cellulaires	Journaux du total des octets reçus et envoyés

22.4. Outils

Accéder au menu ***Diagnostic > Outils***

Ping	Entrer l'adresse IP de destination
Scans Wi-Fi	Le scanner Wi-Fi affiche des informations sur les réseaux Wi-Fi disponibles: adresse MAC du point d'accès / SSID / niveau de réception (dBm) / numéro de canal **NOTE** Le scanner Wi-Fi ne peut fonctionner que si l'interface Wi-Fi est enregistrée en tant que client Wi-Fi (et non en tant que point d'accès Wi-Fi)

22.5. Matériel

Accéder au menu ***Diagnostic > Matériel***

Entrées/Sorties	Vérifier l'état de l'entrée/sortie numérique. Contrôler l'état de la sortie numérique
Surveillance matérielle	Surveiller la tension des alimentations et la température interne

22.6. GPS

Accéder au menu ***Diagnostic > GPS***

Obtener les informations du GPS disponibles.

22.7. État des passerelles

Accéder au menu ***Diagnostic > État des passerelles***

Cette page affiche l'état actuel des paramètres de la passerelle, le nombre d'octets, le nombre de trames échangés et le nombre de trames en erreur.

Le menu **Visualisation des données série** permet d'afficher le trafic RX et TX sur la liaison série.

22.8. Diagnostic avancé

Cette section est destinée au service SAV d'Etic Telecom lorsque des problèmes sont particulièrement difficiles à analyser avec d'autres outils.

22.9. Diagnostic visuel

A la mise sous tension, la LED RUN  est rouge pendant environ 20 secondes lors de l'initialisation du produit.

Puis la LED devient verte et clignote pendant 30 secondes. Elle finit par rester verte fixe lorsque le produit est prêt.

Si la LED reste rouge après ce délai, le produit est probablement défectueux ; Contactez le SAV.

22.10. Commandes SSH

Commandes utiles

Si vous accédez à SSH avec un super administrateur, vous pourrez utiliser les commandes Linux utiles pour les diagnostics réseau.

Certaines commandes peuvent être bridées pour ne pas empiéter sur les fonctionnalités et la sécurité du firmware. Par exemple, `ifconfig eth0 192.168.0.128` ne fonctionnera pas.

Commande	Description
ifconfig	Afficher les adresses IP utilisées (vous ne pouvez pas modifier les adresses IP)
route	Afficher les itinéraires du routeur (vous ne pouvez pas ajouter de routes)
ping	Ping d'adresses
traceroute	Déterminer le chemin emprunté par les paquets
iperf	Tester les performances du réseau
tcpdump	Analyser les paquets

23. MAINTENANCE

Gestion des configurations	Enregistrer/restaurer une configuration, télécharger une configuration ou revenir à la configuration d'usine.
Mises à jour du logiciel	Vérifiez les mises à jour disponibles et mettez à jour le firmware
Options logicielles	Ajouter des options logicielles au routeur
Redémarrage	Forcer le redémarrage du routeur
Erreurs de paramètres	Résumé des erreurs de paramètres sur la configuration actuelle

23.1. Gestion des configurations

Les configurations des produits peuvent être sauvegardées et chargées.
Tous les paramètres sont concernés sauf le magasin de certificats :

CAUTION	Les certificats, clés privées et CRL ne sont pas sauvegardées dans les fichiers de configuration, mais les paramètres qui pointent vers eux y sont toujours. Vous devez ajouter des certificats et des clés privées dans le magasin de certificats du produit avant d'importer le fichier de configuration.

Accéder au menu ***Maintenance > Gestion des configurations***.

Enregistrer une configuration

Pour enregistrer une configuration, choisissez un nom dans le champ **Nom de la configuration** et cliquez sur le bouton **Enregistrer**.

Charger une configuration

NOTE	`Super administrateur` uniquement

Sélectionnez une configuration dans la liste des configurations, puis cliquez sur **Charger**.
Le produit appliquera toute la configuration enregistrée. Lorsque la LED verte cesse de clignoter, le produit est entièrement reconfiguré.

Mode édition

Ce mode est utile pour vérifier ce que contient une configuration. Ou pour définir un lot de paramètres sans que le produit ne se reconfigure à chaque paramètre.

En cliquant sur **Editer** au lieu de **Charger**, la configuration sera affichée, mais pas appliquée.
Le mode édition est activé et des modifications peuvent être apportées à la configuration.

Vous pouvez décider d'**Appliquer** la configuration, ou d'**Annuler** les changements en cours.

Exporter une configuration

NOTE	`Super administrateur` uniquement

Sélectionnez une configuration dans la liste des configurations, puis cliquez sur **Exporter vers le PC**.

La configuration peut contenir des mots de passe qui doivent être chiffrés. Remplissez la fenêtre contextuelle avec un mot de passe pour chiffrer ces valeurs. Si vous ne le saisissez pas, les mots de passe seront en texte clair dans le fichier exporté.

WARNING	Le mot de passe de chiffrement vous sera demandé si vous importez cette configuration ultérieurement

Importer une configuration

NOTE	`Super administrateur` uniquement

Pour importer une configuration depuis votre ordinateur:

1. Renseignez le **Nom de la configuration** à enregistrer dans le produit
2. Fournissez la **Clé de déchiffrement des secrets** si vous avez chiffré les mots de passe pendant la phase d'exportation
3. Sélectionnez le fichier depuis votre ordinateur en cliquant sur le bouton **Parcourir**

23.2. Mise à jour du Firmware

La mise à jour du firmware peut être effectuée localement ou à distance.

Si l'opération de mise à jour du firmware échoue, par exemple si la connexion échoue, le routeur redémarre avec le firmware actuel.

Une fois la mise à jour du firmware effectuée, le routeur restaure les paramètres actuels. Sauf si vous avez spécifié une configuration spécifique à appliquer.

Accéder au menu ***Maintenance > Mises à jour du logiciel***.

Mise à jour à l'aide d'un fichier local

Si le fichier de mise à jour pour mettre à jour le firmware se trouve sur votre ordinateur, vous pouvez:

1. Cliquer sur le bouton **Mettre à jour en utilisant un fichier de mise à jour** et sélectionnez l'archive du firmware,

2. Cliquez sur **Mettre à jour**.

NOTE	Le fichier de mise à jour doit être signé par Etic Telecom afin d'être valide. Tout autre fichier sera rejeté.

Mise à jour Internet

Recherchez automatiquement sur Internet la dernière version du firmware de votre produit:

1. Cliquer sur le bouton **Récupérer les mises à jour disponibles**,
2. Cliquer sur **Mettre à jour** pour la mise à jour que vous souhaitez installer.

Appliquer une configuration après la mise à jour

NOTE	`Super administrateur` uniquement

En cas de downgrade du firmware, la configuration actuelle peut ne pas être valide.

Un fichier de configuration peut être spécifié pour être appliqué après la mise à niveau du firmware du produit.
Les fichiers de configuration disponibles dans le menu ***Maintenance > Gestion des configurations*** sont affichés dans la liste.
La version de la configuration est affichée pour chacun d'eux.

CAUTION	Assurez-vous de choisir une configuration avec une version inférieure ou égale du firmware que vous installez.

24. REDÉMARRAGE PÉRIODIQUE

Il est possible de configurer un redémarrage périodique du routeur.

Accéder au menu ***Configuration > Système > Redémarrage périodique***.

Activer le redémarrage périodique	Activation du redémarrage périodique
Période de redémarrage	Temporalité du redémarrage. Quotidien, hebdomadaire ou mensuel
Heure de redémarrage	Heure à laquelle redémarrer le produit

NOTE

Le redémarrage périodique permet de s'assurer que le routeur redémarre régulièrement.

Pour le redémarrage hebdomadaire, il se fait le dimanche. Pour le redémarrage mensuel, il se fait le 1er du mois. Si le routeur a déjà redémarré dans la journée, alors le redémarrage périodique ne sera pas enclenché à l'heure configurée.

25. AUTHENTIFICATION DU SUPPORT HOTLINE

La hotline Etic Telecom ne peut accéder à votre produit sans votre accord.

Lorsque vous sollicitez l'assistance du support hotline Etic Telecom, vous devez effectuer l'une de ces deux opérations pour permettre à l'équipe d'accéder à votre produit:

- Fournir le mot de passe de la hotline généré à partir de la page d'administration
- Désactivez temporairement le mot de passe de la hotline requis en simplifiant la connexion

WARNING	Nous vous recommandons fortement de générer au préalable un mot de passe d'accès à distance.

25.1. Génération de mot de passe hotline pour le support Etic Telecom

Accéder au menu ***Configuration*** > ***Sécurité*** > ***Droits d'administration***.

Bouton **Générer un nouveau mot de passe pour le SAV**:

Générer un nouveau mot de passe et l'afficher. Il ne s'affichera qu'une seule fois, mais vous pouvez réinitialiser un nouveau mot de passe à tout moment.
Si vous le communiquez à l'équipe hotline Etic Telecom, nous vous recommandons de réinitialiser un nouveau mot de passe une fois le support terminé.

25.2. Simplifiez temporairement la connexion de la hotline Etic Telecom à votre routeur

Simplifier la connexion à la hotline Etic Telecom permettra de :

- activer le VPN d'accès à distance même si vous n'avez pas défini d'opérateur pour celui-ci
- rendre le mot de passe de la hotline non nécessaire. Les utilisateurs distants doivent toujours disposer d'un mot de passe unique, exclusif à Etic Telecom, pour accéder à votre produit.

Vous pouvez l'effectuer par l'une de ces deux actions :

- Maintenir le bouton avant pendant 10 secondes
- Accéder au menu ***Configuration*** > ***Sécurité*** > ***Droits d'administration*** et cliquer sur **Simplifier**.

La hotline Etic Telecom peut désormais accéder à votre produit pendant une heure ou jusqu'à son redémarrage.

Vous pouvez désactiver cette fonctionnalité en accédant au menu ***Configuration*** > ***Sécurité*** > ***Droits d'administration*** et en sélectionnant **Désactiver le bouton poussoir autorisant l'accès distant au SAV Etic Telecom**.

26. ASSISTANCE TÉLÉPHONIQUE ET SHOWROOM VIRTUEL

26.1. Assistance téléphonique

N'hésitez pas à contacter le +33 4 76 04 20 05 ou hotline@etictelecom.com

26.2. Showroom virtuel

En surfant sur notre site WEB www.etictelecom.com (Support/Virtual Showroom) vous pourrez apprendre à configurer une Machine Access Box (à savoir un produit RAS).

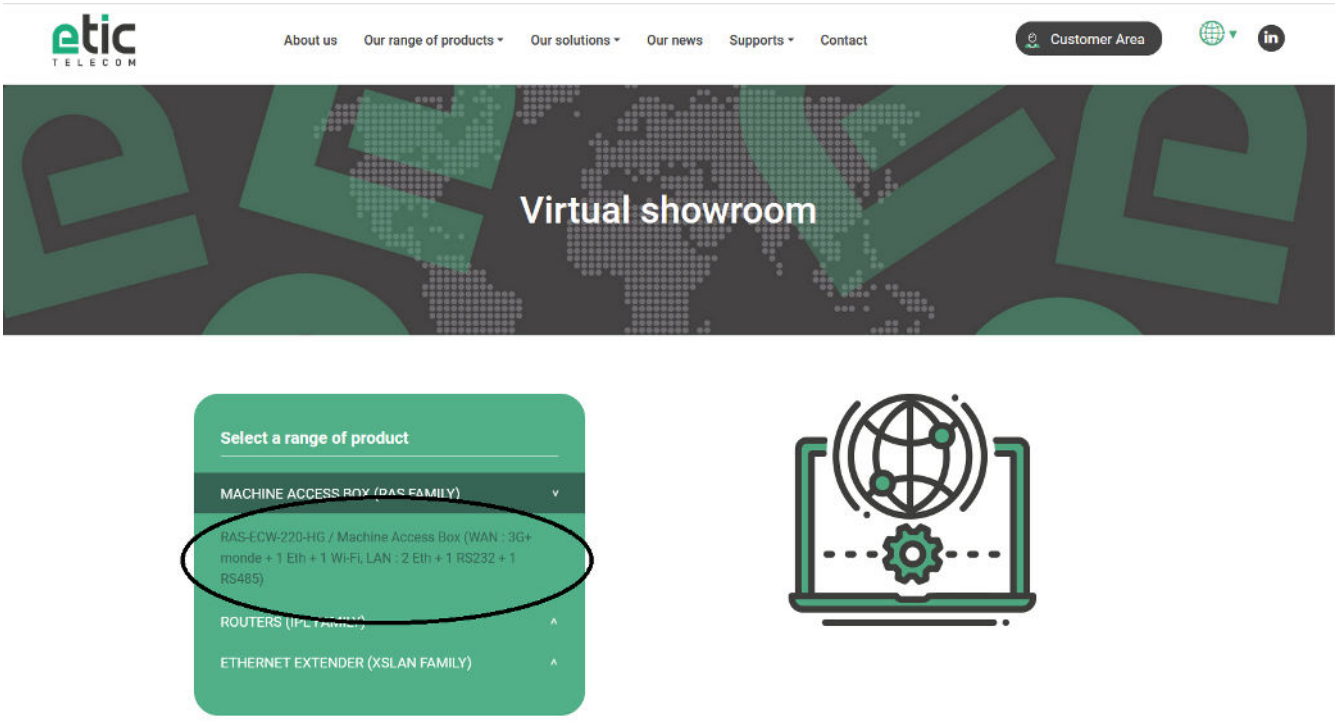


Figure 29. Accès au showroom virtuel

27. APPAIRAGE AVEC LE EFM

27.1. Gestion de flotte de routeurs

ETIC Telecom dispose d'un produit nommé le **EFM** qui permet de faire une gestion de flotte de routeurs ETIC Telecom.

27.2. Configuration de l'appairage

Pour faire partie d'une flotte gérée par un EFM, le routeur doit être configuré pour spécifier par quel EFM il sera géré. Pour cela, il faut accéder au menu ***Accueil*** > ***Configuration*** > ***Système*** > ***EFM*** et remplir les paramètres suivants :

Activer	Activer la gestion du routeur par un EFM
Identifiant unique de l'organisation	Identifiant unique de l'organisation auquel appartient le routeur
Votre identifiant personnel unique	Votre identifiant personnel unique
Adresse IP ou Nom d'hôte du EFM	Adresse IP ou nom d'hôte de votre EFM. Par défaut, c'est le nom d'hôte du EFM SaaS d'ETIC Telecom **WARNING** Assurez-vous que le routeur est capable d'effectuer la résolution DNS si vous utilisez un nom d'hôte.
Clé produit du EFM	Clé produit du EFM. Par défaut, c'est la clé produit du EFM SaaS d'ETIC Telecom
Description	Description du routeur pour avoir des détails sur son utilisation (Optionnel)
Latitude	Latitude de la position GPS du routeur (Optionnel)
Longitude	Longitude de la position GPS du routeur (Optionnel)

27.3. Authentification par EFM

Il est possible de renseigner `EFM` comme type d'authentification pour les Administrateurs et les Opérateurs. Voir la section EFM de la page Délégation d'authentification pour plus de détails.