



RAS / IPL / SIG

GUIDE DE CONFIGURATION

Les familles de produits RAS, IPL et SIG sont fabriquées par

ETIC TELECOM

**13 Chemin du vieux chêne
38240 MEYLAN
FRANCE**

En cas de difficulté dans la mise en œuvre du produit, vous pouvez vous adresser à votre revendeur, ou bien contacter notre service support :

TEL : + (33) (0)4-76-04-20-05
E-mail : hotline@etitelecom.com
web : www.etitelecom.com

PRESENTATION.....	7
1 But du document.....	7
2 Fonctions principales des Routeurs	7
PREPARER LE PARAMETRAGE	11
1 Connexion du PC en vue de la configuration	11
1.1 Introduction.....	11
1.2 Première configuration.....	12
1.3 Modification ultérieure de la configuration	12
2 Accès au serveur d'administration par l'interface WAN	13
3 Opérations avec HTTPS	13
4 Retour temporaire à la configuration usine.....	14
5 Restitution de la configuration usine	14
6 Protection de l'accès au serveur d'administration.....	15
7 Etapes de configuration	15
PARAMETRAGE	17
1 Configuration de l'interface Ethernet / WAN	17
2 Configuration de l'interface ADSL.....	19
2.1 Paramètres « modem ADSL »	19
2.2 Paramètres "Configuration IP du WAN ADSL"	20
3 Configuration de l'interface cellulaire.....	21
3.1 Configuration de la carte SIM 1 ou de la carte SIM2.....	21
3.2 Cas où deux cartes SIM sont utilisées en secours l'une de l'autre.....	22
3.3 Configuration du contrôle de la connexion cellulaire	23
4 Interface Wi-Fi / WAN	24
5 Interface LAN	25
5.1 Principes de configuration.....	25
5.2 Paramètres « Ports Ethernet »	26
5.3 Paramètres « Réseau LAN ».....	26
5.4 Paramètres « Accès distant »	27
5.5 Paramètres « Paramètres avancés ».....	27
5.6 Serveur DHCP	28
5.7 Liste des équipements du réseau LAN	29
6 Interconnexion de routeurs au moyens de VPNs IPSec.....	30
6.1 Présentation.....	30
6.2 Paramétrage d'une connexion VPN IPSec	31
7 Connexion VPN de type OpenVPN.....	36
7.1 Présentation.....	36
7.2 Client et serveur OpenVPN.....	37
7.3 Authentification des participants à une connexion VPN	37
7.4 Règles du paramétrage	37
7.5 Paramétrage du serveur OpenVPN	38
7.6 Configurer les connexions OpenVPN entrante	40
7.7 Configurer une connexion OpenVPN sortante	41

TABLE DES MATIERES

8	Paramétrer le routeur pour secourir une liaison défailante	44
8.1	Basculement sur détection de perte de la liaison ADSL	45
8.2	Secours de connexion OpenVPN (Mode standard)	46
8.3	Secours de connexion OpenVPN (Mode Eco)	50
8.4	Secours de connexion IPSec	53
9	Routage IP	56
9.1	Fonctions de base	56
9.2	Route statique	56
9.3	Protocole RIP	58
10	Substitution d'adresses (NAT, Redirection de port, NAT avancé)	59
10.1	Translation d'adresse (NAT)	59
10.2	Redirection par port	59
10.3	Substitution généralisée d'adresses IP (NAT avancé)	61
11	Redondance VRRP	64
11.1	Principe	64
11.2	Configuration	64
12	Publier l'adresse IP du routeur sur l'Internet	66
12.1	Principe	66
12.2	Paramétrage	67
13	Connexion distante	68
13.1	Avantages de la connexion distante	69
13.2	Types de connexions distantes	70
13.3	Paramétrage d'une connexion distante de type OpenVPN	71
13.4	Paramétrage d'une connexion OpenVPN pour smartphone	72
13.5	Paramétrage d'une connexion distante de type PPTP	72
13.6	Paramétrage d'une connexion distante de type L2TP / IPSec	73
14	Portail sécurisé (HTTPS) pour smartphone, tablette ou PC	74
14.1	Présentation	74
14.2	Configuration	75
14.3	Accéder au portail HTTPS par l'Internet	75
15	M2Me_Connect pour la prise en main de machine à distance	76
15.1	Présentation	76
15.2	Paramétrage d'une connexion au service M2Me_Connect	77
16	Enregistrer les utilisateurs distants autorisés	79
16.1	Présentation	79
16.2	Définir des utilisateurs	80
17	Définir les droits d'accès des utilisateurs	81
18	Configuration du pare-feu	82
18.1	Présentation du pare-feu	82
18.2	Filtre principal	83
19	Ajouter un certificat	85
20	Alarmes	86
20.1	Transmettre un email ou un SMS	86
20.2	Alarmes SNMP	87
21	Passerelles série IP	88
21.1	Présentation des types de passerelles	88
21.2	Passerelle Modbus	89

21.3	Passerelle Raw TCP.....	94
21.4	Passerelle « Raw UDP ».....	96
21.5	Passerelle « Raw Multicast ».....	97
21.6	Passerelle « Unitelway ».....	98
21.7	Passerelle « Telnet ».....	99
21.8	Passerelle USB.....	100

DIAGNOSTICS ET MAINTENANCE.....101

1	Diagnostic visual de défaut de fonctionnement	101
2	Menu Diagnostic	101
2.1	Journaux	101
2.2	Etat de l'interface WAN du routeur	102
2.3	Etat des passerelles série	103
2.4	Outils « Ping ».....	103
2.5	Outil « Scanner Wi-Fi ».....	103
3	Sauvegarde et chargement d'un fichier de paramètres	104
4	Mise à jour du firmware.....	105

PRESENTATION

1 But du document

Le présent document décrit comment configurer les familles de routeurs IP RAS, IPL et SIG fabriqués par ETIC TELECOM.

Il s'applique en particulier aux modèles listés ci-dessous (liste non exhaustive ; consulter le catalogue) :

Boitier d'Accès Machine Ethernet	RAS-E
Boitier d'Accès Machine cellulaire	RAS-EC, RAS-C
Boitier d'Accès Machine Wi-Fi	RAS-EW
Boitier d'Accès Machine cellulaire et Wi-Fi	RAS-ECW
Routeur à interface Ethernet	IPL-E
Routeur ADSL	IPL-A
Routeur cellulaire	IPL-C
Routeur à interface Wi-Fi	IPL-EW
Routeur ADSL et cellulaire	IPL-DAC
Routeur à interface Ethernet et cellulaire	IPL-DEC
Serveur concentrateur de VPN Ethernet	SIG-E
Serveur concentrateur de VPN Cellulaire	SIG-EC
Serveur concentrateur de VPN ADSL	SIG-A

Dans ce document, le nom "Routeur" concerne aussi bien les produits RAS, IPL que SIG.

2 Fonctions principales des Routeurs

Routage

Le Routeur offre une large gamme de solutions de routage qui peuvent être mises en œuvre selon le besoin pour assurer la communication entre les machines de chaque réseau à connecter :

- Routes statiques, pour atteindre des réseaux nichés,
- Translation d'adresse (NAT, DNAT, port forwarding),
- Protocole automatique d'échange de table de routage (RIP),
- Gestion de nom de domaine DNS et DynDNS.

VPN IPSec et OpenVPN pour la sécurité

Le Routeur permet d'établir des tunnels VPN de type IPSec ou OpenVPN.

Il peut se comporter en client ou en serveur VPN.

La connexion VPN garantit un niveau élevé de performance et de sécurité

Transparence : Etabli entre deux routeurs, le VPN assure l'interconnexion transparente des deux réseaux en sorte que toute machine de l'un des réseaux peut communiquer avec une machine de l'autre réseau.

Authentification : Le routeur qui établit le VPN est authentifié par celui qui l'accepte et toute autre connexion est rejetée.

Confidentialité : Les données sont cryptées.

PRESENTATION

On choisira IPSec lorsque le routeur IPL-A doit établir un VPN avec un serveur VPN IPSec déjà installé.

On préférera OpenVPN lorsque le trafic VPN doit être routé au travers de routeurs intermédiaires pour profiter de la grande souplesse de cette technique.

Serveur d'accès distant pour PC, tablette et smartphone

Le Routeur fait également fonction de serveur d'accès distant permettant à un groupe d'utilisateurs distants enregistrés dans la liste d'utilisateurs d'accéder aux machines du réseau avec des droits maîtrisés.

De plus, le portail HTTPS accueille les utilisateurs de PC, tablettes et smartphones en mode HTTPS pour les rediriger en sécurité vers les serveurs HTTPS ou HTML que leur identité autorise.

Prise en main de machine à distance par le service M2Me

Le Routeur permet de raccorder une machine à l'internet et au service M2Me_Connect pour permettre sa prise en main de façon simple et sûre.

Le PC de l'utilisateur distant est télé-porté sur le réseau de la machine en sorte que l'utilisateur distant peut agir sur chacun des équipements de la machine comme s'il était sur place.

Firewall

Le Routeur dispose d'un firewall « SPI » qui inspecte les paquets en permanence.

Il permet de rejeter les tentatives de connexions non authentifiées sur l'Internet.

Il permet également d'attribuer des droits maîtrisés (@IP et N° de port de destination autorisés) aux trames IP reçues au travers d'un tunnel VPN.

Redondance VRRP en cas de panne du routeur :

En cas de panne, le Routeur peut se déclarer en stand-by en sorte qu'un autre routeur prenne le relais avec un fonctionnement identique.

Secours automatique de la ligne ADSL par un réseau cellulaire

L'IPL-DAC possède une interface ADSL et une interface cellulaire.

Il permet de véhiculer les données par l'interface la plus prioritaire tant qu'elle fonctionne normalement (l'ADSL en général) ou bien par l'autre interface (le réseau cellulaire en général, en secours).

Secours automatique d'un réseau privé VPN par un réseau cellulaire

L'IPL-DEC possède une interface WAN Ethernet et une interface cellulaire.

Il permet de véhiculer les données par l'interface la plus prioritaire tant qu'elle fonctionne normalement (Ethernet en général) ou bien par l'autre interface (le réseau cellulaire en général, en secours).

Interface Wi-Fi optionnel (point d'accès ou client)

Le Routeur peut être équipé d'une interface Wi-Fi 2.4 et 5GHz (selon modèle).

L'interface Wi-Fi peut fonctionner comme point d'accès pour permettre le raccordement de clients Wi-Fi (automate équipé d'une interface Wi-Fi, tablette, Webcam ...) ou bien en client Wi-Fi.

SNMP

Le Routeur est agent SNMP; il répond à la MIB2 standard et transmet un trap SNMP lorsque des événements paramétrables surviennent.

DNS

Le système DNS permet au Routeur d'établir une connexion avec un autre routeur même si l'un, l'autre ou les deux routeurs ne possèdent pas une adresse IP connue.

Le principe du DNS consiste à désigner un routeur destinataire d'une connexion par un nom de domaine (par exemple « etictelecom » est un nom de domaine) plutôt que par son adresse IP.

Serveur DHCP

Sur l'interface LAN, le Routeur peut se comporter en serveur DHCP.

Configuration

Le Routeur se configure au moyen d'un navigateur HTML (HTTP ou HTTPS).

EticFinder

Le logiciel ETICFinder permet de détecter simplement tous les produits de marque ETIC connectés à un segment Ethernet pour afficher leur adresse MAC ainsi que l'adresse IP qui leur est attribuée sur le réseau.

Passerelle série

Certaines références possèdent une passerelle série (RS232 ou RS485 ou RS422 ou USB).

La passerelle fonctionne suivant l'un des modes suivants :

- Raw TCP client ou serveur

- Raw UDP

- Telnet

- Modbus maître ou esclave

- Unitelway

PREPARER LE PARAMETRAGE

1 Connexion du PC en vue de la configuration

1.1 Introduction

Le Routeur se configure au moyen d'un PC équipé d'un navigateur Web. Aucun logiciel complémentaire n'est nécessaire.

Aide en ligne :

Pour la plupart des pages du serveur d'administration une aide est accessible en cliquant le ? situé en haut à droite de la page.

Adresse du serveur d'administration :

A la livraison, l'adresse IP du serveur web d'administration est 192.168.0.128.

Configuration :

La première configuration s'effectue de préférence en connectant le PC directement au connecteur LAN Ethernet.

Les modifications ultérieures peuvent être en plus effectuées à distance.

Restitution de l'adresse IP usine :

L'adresse IP usine 192.168.0.128 peut être restituée en enfonçant le bouton poussoir placé sur la partie supérieure du produit.

Protection d'accès au serveur d'administration :

Si vous ne parvenez pas à accéder au serveur d'administration, c'est probablement que l'accès en a été limité pour des raisons de sécurité ou pour d'autres raisons.

Format des adresses réseau :

Dans la suite du texte on appelle « adresse réseau », l'adresse IP de valeur la plus basse du réseau.

Par exemple si le netmask est 255.255.255.0, l'adresse réseau est X.Y.Z.0.

Caractères autorisés :

Les caractères accentués ne peuvent être saisis.

PREPARER LE PARAMETRAGE

1.2 Première configuration

Etape 1 : Créer ou modifier la connexion TCP/IP du PC

Attribuer au PC une adresse IP différente mais cohérente avec l'adresse IP usine du Routeur ; par exemple, l'adresse 192.168.0.1 pour le PC.

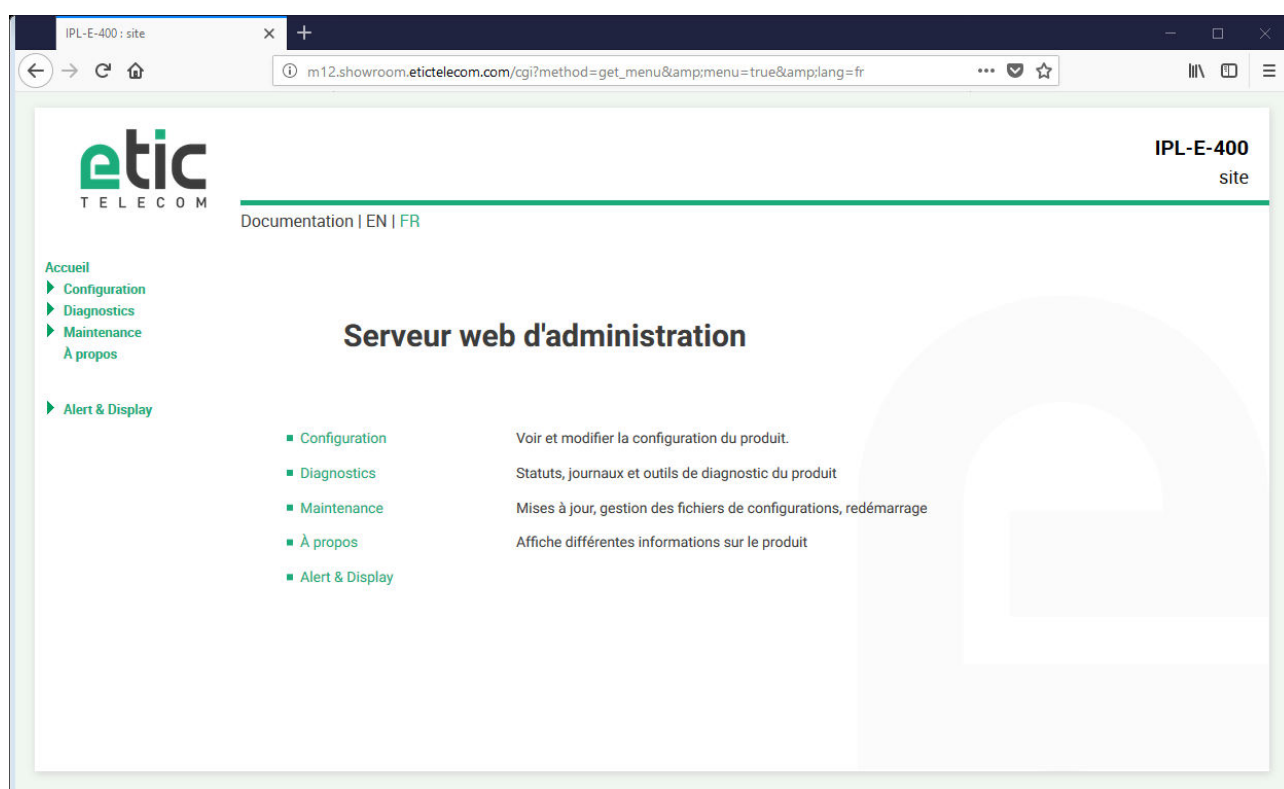
Etape 2 : Connecter le PC au Routeur

Connecter directement le PC au Routeur au moyen d'un câble Ethernet droit ou croisé.

Etape 3 : Lancer le navigateur

Lancer le navigateur puis saisir l'adresse IP du Routeur : 192.168.0.128

La page d'accueil du serveur d'administration s'affiche.



Note : A la première configuration, l'accès au serveur d'administration n'est pas protégé.

1.3 Modification ultérieure de la configuration

Par la suite, le serveur d'administration du Routeur est accessible depuis l'interface LAN à l'adresse IP attribuée au produit ou à travers une connexion distante.

Par défaut, l'accès au serveur d'administration depuis l'interface WAN n'est pas autorisé.

2 Accès au serveur d'administration par l'interface WAN

Pour autoriser l'accès au serveur d'administration par l'interface WAN,

- Dans le menu, choisir **Configuration > Sécurité > Droits d'administration**.
- Saisir le nom d'utilisateur et le mot de passe.
- Sélectionner le protocole à utiliser pour la configuration **HTTPS seulement** ou **HTTP et HTTPS**.
- Cocher la case **Activer l'accès par le(s) WAN**.

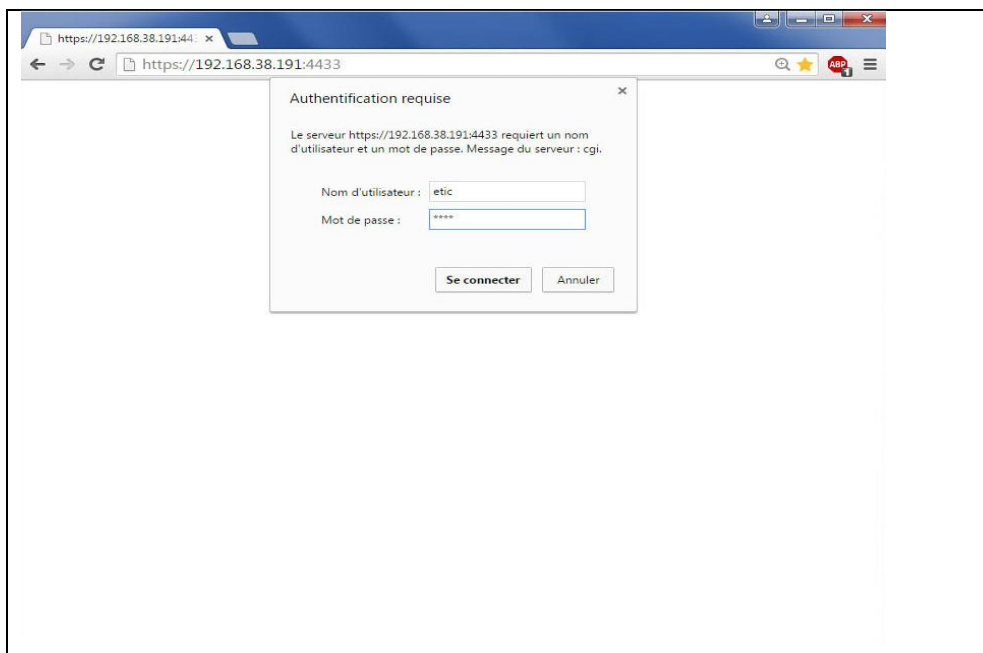
Le serveur d'administration est accessible au moyen d'un navigateur dans le mode HTTPS par l'interface WAN ou l'interface LAN.

3 Opérations avec HTTPS

Une fois que le mode HTTPS a été sélectionné, procéder comme indiqué ci-dessous :

Le N° de port attribué au serveur d'administration est le N°4433

- Ouvrir le navigateur et saisir l'adresse IP du serveur d'administration du Routeur :
Exemple : <https://192.168.38.191:4433>.
- Cliquer **Continuer** lorsque le navigateur affiche un message d'avertissement.
- Saisir le nom d'utilisateur et le mot de passe qui ont été programmés pour protéger l'accès au serveur d'administration.



La page d'accueil du serveur d'administration s'affiche.

PREPARER LE PARAMETRAGE

4 Retour temporaire à la configuration usine

Au cas où l'adresse IP du Routeur ne pourrait être identifiée, ou bien en cas d'impossibilité d'accéder au serveur d'administration à la suite d'une erreur de configuration ou parce que le mot de passe a été oublié, il est possible de restituer la configuration Usine sans pour autant perdre la configuration courante.

- Appuyer sur le bouton poussoir B2 situé à l'arrière du produit avec une pointe de tournevis par exemple,
- Maintenir le bouton-poussoir enfoncé pendant environ 3 secondes
- Le voyant  clignote rapidement en rouge.
- Le serveur d'administration devient accessible à l'adresse IP Usine (192.168.0.128), en HTTP et sans mot de passe. La configuration appliquée temporairement est la configuration Usine. Cependant la configuration courante n'est pas perdue et c'est celle qui est toujours visible dans les pages du serveur d'administration.
- Après avoir pris connaissance de l'adresse IP ou changé des paramètres de la configuration enregistrée, appuyer à nouveau sur le bouton-poussoir ou bien mettre le produit hors tension puis à nouveau sous tension.
- Le produit devient à nouveau accessible à l'adresse IP enregistrée.

Note :

Si l'adresse IP du Routeur n'est pas connue, on peut utiliser le logiciel **EticFinder**.

Ce logiciel détecte tous les produits de marque ETIC sur un réseau local. Après avoir lancé le logiciel, cliquer sur le bouton « Search », puis, lorsque la liste de produits s'affiche, double-cliquer sur l'adresse du produit pour accéder à son serveur html.

5 Restitution de la configuration usine

Il est possible de restituer définitivement la configuration Usine au moyen du bouton poussoir B2 de la face arrière, ou bien en utilisant le serveur d'administration. Dans ce cas, la configuration courante sera perdue, sauf si elle a été sauvegardée dans un fichier.

Pour restituer la configuration Usine au moyen du bouton poussoir,

- Mettre le Routeur hors tension,
- Appuyer sur le bouton poussoir B2 situé à l'arrière du produit avec une pointe de tournevis par exemple,
- Mettre sous tension tout en maintenant le bouton poussoir enfoncé 10 secondes.

Le voyant  passe au rouge ; le Routeur s'initialise et la configuration Usine est restituée.

Note : On peut aussi restituer la configuration Usine depuis le menu **Maintenance > Gestion des configurations** du serveur d'administration.

6 Protection de l'accès au serveur d'administration

- Dans le menu, choisir **Configuration > Sécurité > Droits d'administration**
- Saisir le nom d'utilisateur et le mot de passe qui protègent l'accès au serveur d'administration.
- Cocher la case **Protéger l'accès au site web par mot de passe**

En cas de perte du nom d'utilisateur et du mot de passe d'accès au serveur d'administration, il faut [revenir temporairement à la configuration usine](#) ; l'accès au serveur d'administration est alors libre.

7 Etapes de configuration

Pour configurer le produit, nous conseillons de procéder comme suit :

- Configurer l'interface LAN
- Configurer l'interface WAN
- Configurer les fonctions de routage
- Configurer les VPN
- Configurer l'accès distant
- Configurer le pare-feu
- Configurer les passerelles série

PARAMETRAGE

1 Configuration de l'interface Ethernet / WAN

Le présent paragraphe s'applique aux routeurs suivants :
IPL-E, IPL-EW, IPL-DEC, SIG-E, RAS-E, RAS-EC, RAS-EW, RAS-ECW.

Il s'applique aussi aux routeurs IPL-A ou IPL-C lorsque l'on souhaite utiliser l'interface RJ5 N°1 comme interface WAN au lieu de l'interface ADSL (IPL-A) ou l'interface cellulaire (IPL-C).

- Sélectionner le menu Configuration > Interface WAN

Case à cocher « Type de WAN » :

Choisir la valeur « Ethernet » pour désigner le port Ethernet N°1 comme interface WAN.

Paragraphe « Configuration du WAN Ethernet »

Paramètre « Speed / Duplex » :

Sélectionner 10 ou 100 Mb/s et full ou half duplex.

Paragraphe « Configuration IP du WAN Ethernet »

Case à cocher « Activer » :

Sélectionner la case à cocher

Case à cocher « PPPoE » :

PPPoE assure l'établissement d'une connexion PPP (point to point protocol) entre le port Ethernet N°1 du Routeur et un fournisseur de service (FAI) sur l'internet via un modem connecté au port Ethernet du Routeur.

Cette solution permet à l'interface Ethernet du Routeur de recevoir une adresse IP publique de l'Internet ce qui peut être utile lorsque l'on utilise IPSec par exemple, ou que l'on souhaite mettre en œuvre des fonctions de redirection de port.

Ne pas sélectionner cette case, sauf dans le cas très particulier décrit ci-dessus.

PARAMETRAGE

	Ethernet	Ethernet et PPPoE
Paramètre « priorité du WAN Ethernet» (valeur 0 à 100) : Ce paramètre définit la priorité de l'interface par rapport aux autres interfaces du Routeur. Plus la valeur est faible plus l'interface est prioritaire.	●	●
Paramètres « PPP login» et « mot de passe PPP »: Saisir l'identificateur et le mot de passe du compte Internet.		●
Case à cocher « Obtenir une adresse IP automatiquement »: Cocher cette case si l'adresse IP de la ligne est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP attribuée au Routeur ainsi que celle du serveur distant.	●	
Case à cocher « Obtenir les adresses des serveurs DNS automatiquement»: Cocher cette case si l'adresse des serveurs DNS est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP des serveurs DNS primaires et secondaires.	●	●
Case à cocher « Translation d'adresse NAT»: Cocher cette case pour que le Routeur substitue son adresse IP publique à l'adresse IP source de l'équipement du réseau LAN lors d'une transaction vers l'Internet.	●	●
Case à cocher « Activer le Proxy-Arp »: Cette fonction permet de rendre l'équipement distant (BRAS / broadband remote access server) accessible depuis le LAN. Laisser cette case désactivée sauf sur demande de la hotline.	●	●

2 Configuration de l'interface ADSL

Le présent paragraphe s'applique aux routeurs suivants :
IPL-A, IPL-DAC, SIG-A

- Sélectionner le menu Configuration > Interface WAN

Case à cocher « Type de WAN »

Choisir la valeur « ADSL »

2.1 Paramètres « modem ADSL »

La valeur des paramètres de la ligne ADSL doit être fournie par l'opérateur Télécom.

Paramètre « Modulation »

Il définit la modulation ADSL à utiliser. Le choix « multimode » permet au routeur de s'auto-adapter à la modulation imposée par le fournisseur d'accès Internet.

Paramètre « VPI » et « VCI » (Virtual Path Identifier/Virtual Channel Identifier)

Les valeurs VPI = 8 et VCI = 35 sont les valeurs couramment utilisées.

Paramètre « Multiplexage »

Les modes VC et LLC sont disponibles.

Paramètre « Encapsulation »

Les encapsulations suivantes peuvent être sélectionnées :

PPPoE : PPP over Ethernet

PPPoA : PPP over ATM

EoA : Ethernet over ATM, RFC1483/RFC2684 Bridged

IPoA : Routed IP over ATM, RFC1483 Routed

A chacun de ces types est associé un lot de paramètres « IP » décrits au paragraphe ci-dessous.

PARAMETRAGE

2.2 Paramètres "Configuration IP du WAN ADSL"

Les paramètres à saisir dépendent de la valeur du paramètre « encapsulation » du paragraphe précédent.

	PPPoE	PPPoA	EoA	IPoA
Paramètre « priorité du WAN ADSL » (valeur 0 à 100) : Ce paramètre définit la priorité de l'interface ADSL par rapport aux autres interfaces (Cellulaire ou Ethernet N°1). Plus la valeur est faible plus l'interface est prioritaire. En conséquence, si l'on affecte une haute priorité à l'interface ADSL (valeur faible) et une basse priorité à l'interface cellulaire (valeur élevée), les trames IP sont transmises prioritairement par l'interface ADSL et, en secours par l'interface cellulaire.	●	●	●	●
Paramètres « PPP login » et « mot de passe PPP » : Saisir l'identificateur et le mot de passe du compte Internet.	●	●		
Paramètres « Nom du service PPPoE » : C'est le nom du service fourni par l'opérateur télécom. Il est indiqué avec le nom et le mot de passe de connexion. Il n'est habituellement pas nécessaire de le saisir.	●			
Case à cocher « Obtenir une adresse IP automatiquement » : Cocher cette case si l'adresse IP de la ligne est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP attribuée au routeur ETIC ainsi que celle du serveur distant.	●	●	●	●
Case à cocher « Obtenir les adresses des serveurs DNS automatiquement » : Cocher cette case si l'adresse des serveurs DNS est attribuée par l'opérateur à travers la ligne. Autrement, décocher cette case et saisir l'adresse IP des serveurs DNS primaires et secondaires.	●	●	●	●
Case à cocher « Translation d'adresse NAT » : Cocher cette case pour que le routeur ETIC substitue son adresse IP publique à l'adresse IP source de l'équipement du réseau LAN lors d'une transaction vers l'Internet.	●	●	●	●
Case à cocher « Activer le Proxy-Arp » : Cette fonction permet de rendre l'équipement distant de la ligne ADSL (BRAS / broadband remote access server) accessible depuis le LAN. Laisser cette case désactivée sauf sur demande de la hotline.	●	●	●	●

3 Configuration de l'interface cellulaire

Le présent paragraphe s'applique aux routeurs suivants :
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 d'un deuxième réseau cellulaire en cas de panne du premier.

- Sélectionner le menu Configuration > Interface WAN

Case à cocher « Type de WAN » :

Choisir la valeur « Cellulaire ».

Paramètre « Priorité » :

Le paramètre « priorité » permet de hiérarchiser la priorité entre plusieurs routes pouvant agir en secours l'une de l'autre.

En l'absence de route de secours, saisir la valeur 10.

Remarque : plus la valeur est élevée (1 à 100) moins la route est prioritaire.

Paramètre « Carte SIM » :

Il est possible de sélectionner la carte SIM N°1, ou bien la carte SIM N°2, ou bien les deux.

Paramètre carte SIM	
Valeur	
SIM1	La carte SIM placée dans le logement 1 est sélectionnée
SIM2	La carte SIM placée dans le logement 2 est sélectionnée
SIM 1, backup sur SIM2	Le routeur utilise la carte SIM N°1 en priorité et, en cas de défaut de fonctionnement du réseau cellulaire, il utilise la carte SIM N°2 Dans ce cas, les temporisations de basculement d'un réseau à l'autre doivent être réglées.

3.1 Configuration de la carte SIM 1 ou de la carte SIM2

On décrit ci-dessous la configuration de la carte SIM du logement 1.

La configuration de la carte SIM du logement 2 est identique.

Paragraphe « SIM1 : Configuration du modem »

Paramètre « Chaîne d'initialisation du modem » :

Ce paramètre permet de modifier, dans des cas particuliers, la chaîne d'initialisation transmise par le routeur à son modem cellulaire.

Laisser ce champ vide sauf indication de la hotline.

Paramètre « Nom du point d'accès (APN) » :

Le réseau cellulaire est connecté à d'autres réseaux, l'internet ou un réseau privé, au travers d'une passerelle appelée APN.

La ou les passerelles utilisables doivent être désignées par l'opérateur Télécom dans le contrat d'abonnement. Dans le cas contraire, on peut se reporter au site web de l'opérateur.

Entrer le nom de l'APN associé à la carte SIM (par exemple websfr ou orange business).*

PARAMETRAGE

Paramètre « Code PIN » :

Saisir le code PIN de la carte SIM.

Paramètre « Type de réseau cellulaire » :

Les infrastructures (c'est-à-dire les relais) 4G, 3G et GPRS sont différentes les unes des autres. Ce paramètre permet de forcer le routeur à utiliser une de ces 3 infrastructures.

Paramètre « Type de réseau cellulaire »	
Valeur	
Auto	Si la valeur « Auto » est sélectionnée, le routeur choisit le relais qui assure la meilleure efficacité de transmission (valeur par défaut).
4G	S'il est nécessaire de forcer l'utilisation du réseau 4G, sélectionner la valeur 4G
3G	Idem
GPRS	Idem

Paragraphe « SIM1 : Configuration IP du WAN cellulaire »

Paramètres «login» et « Password» :

Saisir l'identificateur et le mot de passe du compte Internet.

Remarque sur les réseaux cellulaires, il n'est habituellement pas nécessaire de saisir ces paramètres.

Case à cocher « Obtenir une adresse IP automatiquement » :

Ce champ doit être laissé vide sauf dans le cas où une adresse IP fixe est attribuée au Routeur sur le réseau cellulaire.

Case à cocher « Obtenir les adresses des serveurs DNS automatiquement» :

Cocher cette case si l'adresse des serveurs DNS est attribuée par l'opérateur à travers la ligne.

Case à cocher « Translation d'adresse NAT»:

Cocher cette case pour que le Routeur substitue son adresse IP publique à l'adresse IP source de l'équipement du réseau LAN lors d'une transaction vers l'Internet.

3.2 Cas où deux cartes SIM sont utilisées en secours l'une de l'autre

Le routeur IPL-C comporte deux logements pour carte SIM.

Chaque carte SIM peut être associée à un abonnement différent ; l'un chez un opérateur et l'autre chez un autre opérateur.

Dans la suite du texte, on nomme « réseau 1 » le réseau cellulaire associé à la carte SIM N°1, et « réseau 2 » le réseau associé à la carte SIM N°2.

Le réseau 1 est le réseau testé à la mise sous tension du Routeur.

En cas de défaillance du réseau 1 confirmée durant le temps T1, le Routeur bascule sur le réseau 2.

Si le réseau 2 fonctionne correctement, le Routeur y reste au minimum pendant le temps T3 ; à l'issue de ce temps, le Routeur interrompt la communication sur le réseau 2, teste le réseau 1 et retourne sur le réseau 1 s'il est à nouveau disponible.

A tout moment, si le réseau 2 ne fonctionne pas correctement et après confirmation pendant le temps T2, le Routeur retourne sur le réseau 1.

Les temporisations T1, T2 et T3 peuvent être réglées.

Paramètre T1 «Temps avant basculement sur SIM2» :

Saisir le temps de confirmation d'indisponibilité du réseau 1 au-delà duquel le Routeur bascule sur le réseau 2.

Valeur : 5, 10, 20, 30, 60 mn

Paramètre T2 «Temps avant re-basculé sur SIM1» :

Saisir temps de confirmation d'indisponibilité du réseau 2 au-delà duquel le Routeur bascule sur le réseau 1.

Valeur : 2, 5, 10, 20 mn

Paramètre T3 «Temps de connexion sur SIM2 avant de re-tester SIM1» :

Saisir le temps minimum durant lequel le Routeur demeure sur le réseau 2, s'il fonctionne correctement.

Valeur : 1, 12, 24 heures, 5 jours, jamais

Remarque :

Il est conseillé de donner à T3 une valeur longue (12 heures par exemple); en effet, si le réseau 2 fonctionne correctement, il n'est pas nécessaire de retourner immédiatement sur le réseau 1.

3.3 Configuration du contrôle de la connexion cellulaire

Le Routeur contrôle la connexion au réseau cellulaire en testant le fonctionnement de la connexion PPP au serveur de l'opérateur du réseau cellulaire. Cette technique est la technique normale de vérification du fonctionnement de la liaison.

Cependant, il a été constaté que, sur certains réseaux ou à certains moments, la connexion PPP pouvait être déclarée active alors que le service de transmission de données n'était pas rendu par l'opérateur de réseau cellulaire.

C'est la raison pour laquelle le Routeur peut vérifier le fonctionnement du service en transmettant un message ICMP (PING) vers un serveur distant.

Si le message n'obtient pas de réponse, et après réitération, le routeur initialise son module de transmission de données 4G / 3G.

Cette fonction ne doit être activée que si un dysfonctionnement est constaté.

Paramètre «Adresse IP du serveur» :

Saisir l'adresse IP du serveur vers lequel le message ICMP (PING) doit être transmis.

Paramètre «Intervalle des PING» :

Saisir la période de transmission des PING

Paramètre «Nombre d'essais» :

Saisir le nombre de tests infructueux successifs avant de réinitialiser le module de transmission de données 4G / 3G.

4 Interface Wi-Fi / WAN

Le présent paragraphe s'applique aux routeurs suivants :
IPL-EW, IPL-AW, IPL-CW, RAS-EW, RAS-ECW

L'interface Wi-Fi du Routeur doit être paramétré en client Wi-Fi (et pas un point d'accès).

Lorsque l'interface Wi-Fi est sélectionnée comme interface WAN, le voyant Wi-Fi s'éclaire et le voyant de niveau de réception indique la qualité de la liaison avec le point d'accès.

Pour sélectionner l'interface Wi-Fi,

- Sélectionner le menu Configuration > Interface WAN
- Sélectionner le type de WAN « Wi-Fi »

Paramètre « Nom de réseau Wi-Fi (SSID) » :

Saisir un libellé libre qui désigne le réseau Wi-Fi.

Paramètre « Authentification » :

Choisir le mode d'authentification WPA ou WEP ou le mode non sécurisé (non recommandé).

Paramètre « Clé partagée » :

Saisir la clé WPA ou WEP du réseau.

Elle est fixée par le point d'accès Wi-Fi.

Paramètre « Priorité du WAN Wi-Fi » :

Saisir la valeur 10.

Case à cocher « Obtenir une adresse IP automatiquement » :

Cocher cette case si l'adresse IP est attribuée par le point d'accès Wi-Fi.

Autrement, décocher cette case et saisir l'adresse IP attribuée au Routeur sur cette interface, le masque de sous-réseau et l'adresse IP de la passerelle par défaut.

Case à cocher « Obtenir les adresses des serveurs DNS automatiquement » :

Cocher cette case si l'adresse des serveurs DNS est attribuée par le point d'accès Wi-Fi.

Autrement, décocher cette case et saisir l'adresse IP des serveurs DNS primaires et secondaires.

Case à cocher « Translation d'adresse NAT » :

Cocher cette case pour que le Routeur substitue l'adresse IP qui lui a été attribuée sur le réseau Wi-Fi à l'adresse IP source de l'équipement du réseau LAN lors des transactions sur le réseau Wi-Fi

Remarque :

Le scanner Wi-Fi du Routeur permet d'identifier les réseaux Wi-Fi détectés par le Routeur.

Pour utiliser le scanner Wi-Fi, sélectionner le menu Diagnostic > Outils > Scan Wi-Fi.

(Voir le chapitre Diagnostic de la présente notice).

5 Interface LAN

5.1 Principes de configuration

Switch Ethernet

L'interface LAN est constituée de 2 ou 4 prises Ethernet switchées.

Cette interface est désignée par « interface LAN » dans la suite du texte ; et le réseau qui y est directement raccordé est appelé « réseau LAN ».

Les ports Ethernet peuvent être paramétrés pour former un hub au lieu d'un switch.

Adresse IP du routeur sur l'interface LAN

Une adresse IP fixe doit être attribuée à l'interface LAN du Routeur.

Serveur DHCP

Le Routeur peut être serveur DHCP pour les équipements du réseau local (LAN).

Réserve d'adresses pour les utilisateurs distants

Si le Routeur est aussi utilisé pour permettre à des utilisateurs distants d'échanger des données avec les équipements du réseau local au moyen d'une connexion distante (PPTP ou TLS ou L2TP) , une plage d'adresses IP du réseau local doit leur être réservée.

Les adresses de cette plage ne doivent donc pas être attribuées aux équipements du réseau local.

Exemple :

Désignation	Adresse IP	Observations
Réseau LAN	192.168.12.0	Les adr. des équipements du réseau vont de 192.168.12.1 à 192.168.12.254
Netmask	255.255.255.0	
Interface LAN Routeur	192.168.12.1	L'adr IP du Routeur sur le réseau LAN est 192.168.12.1
Début de plage utilisateurs distants	192.168.12.2	2 utilisateurs distants pourront se connecter simultanément au réseau LAN. L'un recevra l'adresse 192.168.12.2 et l'autre 192.168.12.3. Ces 2 adresses ne peuvent pas être attribuées à d'autres équipements du réseau LAN
Fin de plage utilisateurs distants	192.168.12.3	
Adresses disponibles pour les équipements du réseau local	192.168.12.4 à 192.168.12.254	

Nom des équipements raccordés au réseau LAN

Il est possible d'attribuer un nom à chaque équipement ou groupe d'équipements connectés à l'interface LAN.

Ce nom permet ensuite de définir les droits d'accès des utilisateurs distants.

Interface Wi-Fi optionnelle

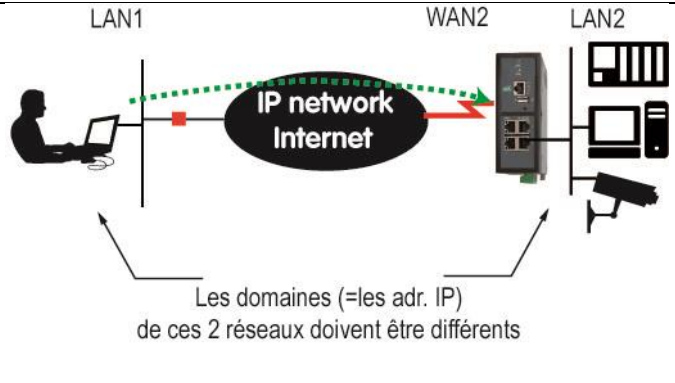
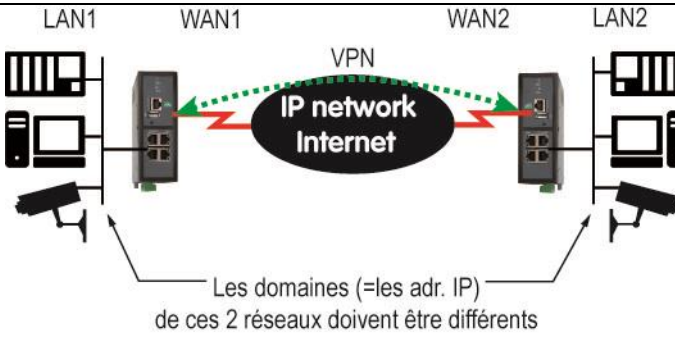
L'interface Wi-Fi optionnelle vient compléter l'interface LAN lorsqu'elle est configurée en « Point d'accès ».

Les équipements qui se connectent en Wi-Fi appartiennent au réseau LAN.

En particulier, les adresses IP de ces équipements font partie du domaine IP du réseau LAN.

PARAMETRAGE

Règles d'attribution de l'adresse IP de l'interface LAN

Cas d'une connexion distante Le plan d'adresses IP du réseau du PC distant d'une part, et du réseau LAN d'autre part, doivent être disjoints.	
Cas d'un VPN établi avec un autre routeur Le plan d'adresses IP du réseau distant d'une part, et du réseau LAN d'autre part, doivent être disjoints.	

Menu Ethernet et IP

- Sélectionner le menu Configuration > Interface LAN > Ethernet & IP

5.2 Paramètres « Ports Ethernet »

Case à cocher « Activer le mode hub » :

Si cette case est cochée, le switch Ethernet devient un hub ; les trames Ethernet sont diffusées sur tous les ports.

5.3 Paramètres « Réseau LAN »

Paramètre « Adresse IP » :

Saisir l'adresse IP attribuée à l'interface LAN du Routeur.

Paramètre « Masque de sous-réseau » (netmask) :

Saisir le netmask du réseau LAN.

Exemple : Le netmask d'un réseau de 254 stations est 255.255.255.0.

Paramètre « Passerelle par défaut » :

Si un autre routeur est raccordé au réseau LAN et si ce routeur est le routeur par défaut du Routeur (ETIC), saisir son adresse. Cette adresse doit faire partie du domaine du réseau LAN.

Remarque : Ne rien saisir si aucun autre routeur n'est connecté au réseau LAN.

5.4 Paramètres « Accès distant »

Case à cocher « Gestion automatique des adresses IP des utilisateurs distants » :

Si cette case est cochée, une adresse IP non utilisée du réseau LAN est attribuée au PC d'un utilisateur distant lorsqu'il se connecte.

Pour attribuer cette adresse, le Routeur vérifie au moyen de requêtes appropriées qu'elle n'est pas attribuée par ailleurs à un équipement du réseau LAN.

Décocher la case pour fixer la plage des adresses du réseau LAN réservée aux utilisateurs distants.

Remarque : La plage doit comporter autant d'adresses que l'on souhaite d'accès simultanés.

Paramètre « Début de la plage d'adresses IP » :

Saisir l'adresse IP du début de la plage

Paramètre « Fin de la plage d'adresses IP » :

Saisir l'adresse IP de la fin de la plage

5.5 Paramètres « Paramètres avancés »

Pour afficher ces paramètres, cocher la case « paramètres avancés ».

Paramètres « Configuration port 1 » à « Configuration port 4 »:

Les ports 1 à 4 (ou 1 à 2) du switch Ethernet sont à détection automatique de débit ; cependant, dans des cas particuliers, il peut être utile de fixer leur comportement ou encore de désactiver certains ports pour des raisons de sécurité.

Valeur	Observation
Auto-négociation	Le switch négocie le débit et le mode de fonctionnement du port Ethernet
100 M full duplex	
10 M full duplex	
100 M half duplex	
10 M half duplex	
Désactivé	Le fonctionnement du port Ethernet est désactivé

Paramètre « Serveur DNS primaire » :

Saisir l'adresse IP du serveur DNS principal.

Paramètre « Serveur DNS secondaire » :

Saisir l'adresse IP du serveur DNS secondaire.

Case à cocher « Activer proxy ARP » :

Proxy-Arp permet au routeur de simuler sur son interface LAN le comportement d'un équipement situé sur son interface WAN afin que les trames IP puissent effectivement être routées du LAN vers le WAN.

Cette fonction peut être nécessaire, par exemple, lorsque des équipements possédant une adresse IP du domaine du LAN, sont connectés à l'interface WAN.

Cette fonction n'est pas nécessaire habituellement.

PARAMETRAGE

Paramètre « Adresse IP additionnelle » et « Masque de sous-réseau additionnel » :

Il est possible d'attribuer une seconde adresse IP à l'interface LAN du Routeur.

Dans ce cas, le routeur appartient aux deux réseaux IP.

Case à cocher « Désactiver ICMP redirect » :

ICMP est un protocole de même niveau que IP.

Il permet aux équipements de gérer les erreurs survenant sur le réseau.

ICMP redirect est un des messages de ICMP.

Lorsque plusieurs routeurs sont présents sur l'interface LAN, et qu'un équipement fait appel à tort au Routeur (ETIC) pour router les trames IP vers un autre réseau, « ICMP redirect » permet au Routeur (ETIC) de transmettre à cet équipement la route adaptée (c'est-à-dire l'adresse IP d'un autre routeur du réseau LAN).

5.6 Serveur DHCP

La fonction serveur DHCP permet de réserver une plage d'adresses IP du domaine du réseau LAN.

Les adresses de cette plage sont automatiquement attribuées aux équipements du réseau LAN configurés en client DHCP lorsqu'ils en font la demande.

Les adresses extérieures à cette plage peuvent être attribuées de manière fixe aux autres équipements du réseau.

Remarque :

Lorsque le Routeur est équipé de l'option Wi-Fi et qu'il est configuré en point d'accès afin de permettre la connexion d'équipements Wi-Fi tels qu'un PC, une tablette ou un smartphone, il est conseillé de sélectionner la fonction serveur DHCP sur l'interface LAN ; en effet, de nombreux équipements de ce type ne fonctionnent que lorsqu'un serveur DHCP attribue les adresses IP.

- Sélectionner le menu Configuration > Interface LAN > Serveur DHCP

Case à cocher « Activer le serveur » :

Si cette case est cochée, le Routeur se comporte en serveur DHCP sur l'interface LAN.

Paramètre « Début de la plage d'adresses IP » :

Saisir l'adresse IP du début de la plage que le Routeur peut attribuer aux équipements du réseau LAN.

Paramètre « Fin de la plage d'adresses IP » :

Saisir l'adresse IP de la fin de la plage que le Routeur peut attribuer aux équipements du réseau LAN.

Paramètre « Masque de sous-réseau » :

Saisir le masque du réseau LAN

Paramètre « Passerelle par défaut » :

Saisir l'adresse IP de la passerelle par défaut sur l'interface LAN (s'il en existe une).

Paramètre « Serveur DNS primaire » :

Saisir l'adresse IP du serveur DNS secondaire.

Paramètre « Serveur DNS secondaire » :

Saisir l'adresse IP du serveur DNS secondaire.

Remarque : les 4 paramètres ci-dessus sont les mêmes que ceux qui ont été saisis préalablement (menu Ethernet et IP) ; ils doivent être saisis à nouveau si le serveur DHCP est utilisé.

5.7 Liste des équipements du réseau LAN

Cette page permet de désigner par un nom et une adresse IP les équipements connectés au réseau LAN.

Il est nécessaire de désigner les équipements du réseau LAN qui doivent être rendus sélectivement accessibles aux utilisateurs distants.

- Sélectionner le menu Configuration > Interface LAN > Liste des équipements

192.168.38.191:8080/cgi?method=get_menu&menu=true&lang=fr

etlc **IPL-CW-220** site

> Accueil > Configuration > Interface LAN > Liste des équipements

Nom du site: site
 Nom de domaine: site
☐ Afficher le portail web

Liste des équipements

	Nom	Adresse IP
⊗	Automate filtrage	192.168.38.10
⊗	Automate pompage	192.168.38.11
⊗	Automate transfert	192.168.38.12
⊗	HMI	192.168.38.13

Afficher Modifier Supprimer Ajouter... Copier et modifier A Y

Enregistrer Annuler

Pour désigner un équipement du réseau :

- Cliquer le bouton « Ajouter »,
- Attribuer un nom et une adresse IP du réseau LAN à l'équipement.

Remarque : On peut aussi attribuer à un équipement un nom et un ensemble d'adresse IP appartenant au même sous réseau.

Exemple : 192.168.38.8/29 pour désigner la plage d'adresses IP allant de 192.168.38.8 à 192.168.38.15

6 Interconnexion de routeurs au moyens de VPNs IPSec

6.1 Présentation

Chaque connexion IPSec est un tunnel établi entre 2 routeurs.

Ce tunnel VPN permet de connecter deux réseaux de façon sûre et transparente : Lorsque le tunnel est établi entre 2 routeurs, chaque équipement du premier réseau peut échanger des trames IP avec chaque équipement du second.

Sur un IPL ou un RAS, 10 connexions VPN IPSec peuvent être créées.

Sur un SIG, 100 connexions VPN IPSec peuvent être créées.

Sur un SIG VM, 500 connexions VPN IPSec peuvent être créées.

Le fonctionnement de chaque connexion IPSec est réglé individuellement ce qui permet une grande souplesse d'utilisation.

- **Authentification**

L'authentification réciproque des deux routeurs participants à la connexion peut être réalisée au moyen d'une clé partagée ou de certificats.

Utilisation d'une clé partagée :

La clé partagée est, comme son nom l'indique, un code identique enregistré dans les deux routeurs participant à la connexion. La clé partagée doit être produite par le routeur initiateur auprès du routeur répondeur pour autoriser la connexion.

Utilisation de certificats :

Un certificat X509 est enregistré en usine dans le routeur. Il est produit par l'autorité de certification enregistrée par ETIC TELECOM.

Si nécessaire, il est possible d'enregistrer d'autres types de certificat dans le routeur (voir paragraphe enregistrement de certificats).

Le certificat peut être utilisé pour l'authentification réciproque des routeurs.

Dans ce cas, le routeur initiateur de la connexion présente son certificat au routeur répondeur. Réciproquement, le routeur répondeur s'authentifie auprès de l'initiateur.

- **Utilisation de IPSec lorsque l'adr. IP source est modifiée le long du trajet (NAT ou adresse IP dynamique)**

Pour garantir l'authenticité de l'initiateur du tunnel, chacun des deux routeurs du tunnel IPSec vérifie si l'adresse IP source n'a pas été modifiée au cours du cheminement dans le réseau.

Pour cette raison, IPSec nécessite un paramétrage particulier lorsque le routeur initiateur ou répondeur est installé de telle sorte que les trames IP franchissent des nœuds (routeurs intermédiaires dans le trajet), qui modifient l'adresse IP source.

C'est ce que font, par exemple, les routeurs d'entreprise à l'interface avec l'Internet.

Pour pallier cette difficulté, deux solutions sont possibles :

Solution 1 : Utiliser des certificats et pas une clé partagée.

Solution 2 : Si l'on utilise une clé partagée,

il faut d'une part attribuer un code d'identité à chaque routeur (IKE ID),

Ce code identifie chaque routeur IPSec auprès de l'autre routeur.

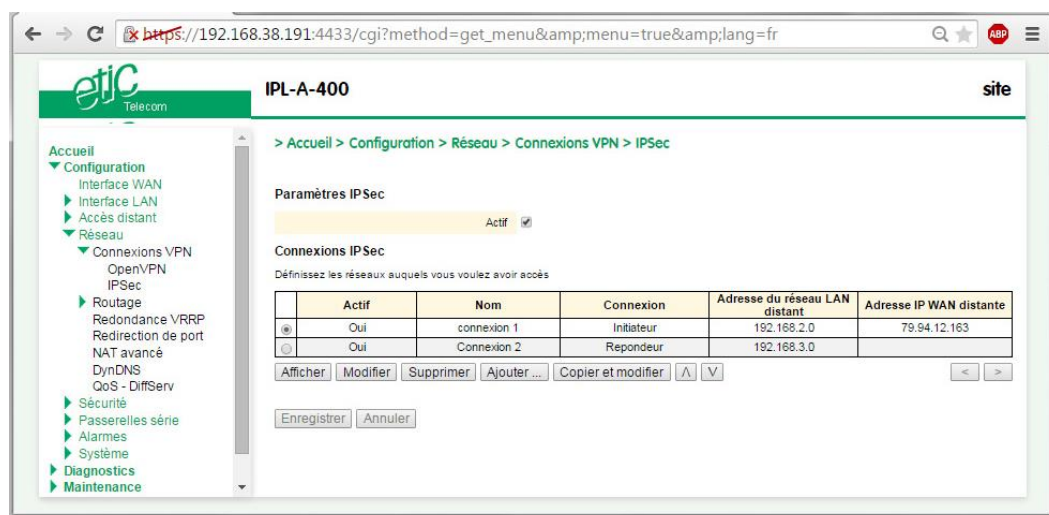
Il faut donc saisir dans chaque routeur le paramètre « IKE ID » du routeur (paramètre « IKE ID local ») et le paramètre « IKE ID » du routeur distant (paramètre IKE ID distant).

et d'autre part sélectionner le mode « Aggressive mode » (paragraphe IKE phase 1 dans la page de paramétrage IPSec).

6.2 Paramétrage d'une connexion VPN IPSec

- Sélectionner le menu « **Configuration** », puis « **Réseau** », puis « **Connexions VPN** ».

L'écran des connexions VPN s'affiche.



PARAMETRAGE

Pour ajouter une connexion VPN IPSec, cliquer « Ajouter ».

L'écran d'une nouvelle connexion VPN IPSec s'affiche.

etic Telecom **IPL-A-400** **site**

Paramètres avancés ☒

Nom: connexion1

Indiquez la méthode d'authentification utilisée pour les connexions IPSec.
ATTENTION:
- Si le produit est situé derrière un routeur qui effectue de la translation d'adresse ou redirection de port (DNAT) et que vous souhaitez configurer le produit en connexion entrante, alors vous devez obligatoirement choisir une authentification par certificat numérique.

Authentification par: Clé pré partagée

Sélectionner le type de connexion (entrante ou sortante) que vous souhaitez configurer.
Connexion: Initiateur

IKE authentication

Attention : la clé pré partagée est globale pour le produit. Elle est donc identique à celle des connexions utilisateurs utilisant L2TP/IPSec. Vous pouvez laisser ce champ vide et définir des clés différentes pour chaque connexion. (Dans ce cas les clés sont définies dans la page de configuration des connexions distantes.)

Valeur clé: ***** Mots de passe identiques

IKE ID local: azertyuiop

IKE ID distant: azertyuiop

Réseau

Saisir les informations concernant le réseau distant.

Adresse du réseau LAN distant: 192.168.2.0

Masque du réseau LAN distant: 255.255.255.0

Adresse IP WAN distante: 79.94.12.163

IKE Phase 1

Mode: Main mode

Algorithme de cryptage: AES 256

Algorithme d'authentification: SHA1

Groupe DH: Groupe 2

Life time: 8 heures

IKE Phase 2

Indiquez le protocole utilisé pour les connexion IPSec. ESP est conseillé, avec le protocole AH, il n'y a pas de chiffrement mais seulement de l'authentification.

Protocole: ESP

Algorithme de cryptage: AES 128

Algorithme d'authentification: SHA1

Utilisation de la PFS (Perfect Forward Secrecy) : modifier cette valeur seulement pour certains cas d'interopérabilité

PFS: ☒

Groupe DH: Groupe 2

Life time: 8 heures

DPD Timeout

La détection DPD (Dead Peer Detection) permet de détecter un homologue mort et, en cas de détection, de supprimer les associations de sécurité IKE et IPSec de cet homologue.

Périodicité des messages "DPD keepalive": 30 s

Délai de détection de perte de connexion: 2 minutes

Lier le VPN au WAN: WAN ADSL

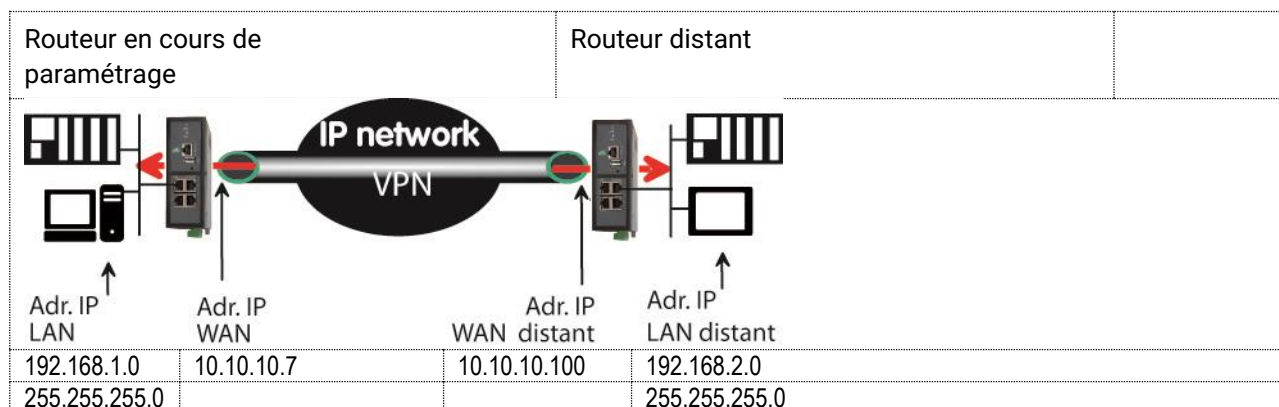
Démarrer sur événement: ☒

Démarrer seulement lorsque: WAN ADSL connecté

Enregistrer Annuler Retour

- Sélectionner la case cocher « Activer » et éventuellement « Paramètres avancés ».
- Attribuer un nom à la connexion.

Les différentes adresses IP auxquelles il est fait référence sont décrites ci-dessous :



Paramètre « Authentification » :

Deux choix sont possibles : Certificat numérique X509 ou Clé partagée.

Paramètre « Connexion » :

Sélectionner la valeur « Initiateur » si la connexion est établie à l'initiative du Routeur en cours de paramétrage.

Sélectionner la valeur « Répondeur » si la connexion est établie à l'initiative du routeur distant vers le Routeur en cours de paramétrage.

Paragraphe authentification – Cas du choix Certificat numérique

Paramètre « Mon SubjectAlt name » :

Entrez la valeur du champ 'SubjectAltName' du certificat actif du Routeur.

Si l'on utilise le certificat enregistré en usine dans le Routeur, il s'agit du champ Email.

Paramètre « SubjectAlt name distant » :

Entrez la valeur du champ 'SubjectAltName' du certificat actif du Routeur distant.

Pour les certificats ETIC, il s'agit du champ Email.

Paragraphe authentification – Cas du choix clé partagée

Paramètre « Clé » :

Saisir la valeur de la clé partagée nécessaire pour l'authentification du Routeur.

la clé, comme son nom l'indique, est identique sur les deux routeurs participant au VPN.

Paramètre « IKE ID local » :

Nom utilisé par le produit pour s'identifier pendant la phase 1.

Il est nécessaire de le remplir si on utilise une clé partagée et dans le cas où un des Routeurs (ETIC) est lui-même placé derrière un autre routeur qui translate les adresses source (fonction NAT).

Paramètre « IKE ID distant » :

Nom utilisé par le produit pour identifier son pair pendant la phase 1. Il est nécessaire de le remplir si on utilise une clé partagée et dans le cas où un des Routeurs (ETIC) est lui-même placé derrière un autre routeur qui translate les adresses source (fonction NAT).

Paragraphe Réseau

Paramètres « Adresse du réseau LAN distant » et « Netmask distant » :

Saisir l'adresse et le netmask du réseau distant (exemple 192.168.2.0 et 255.255.255.0)

Paramètres « Adresse WAN distant » (uniquement si le routeur est initiateur du VPN) :

Saisir l'adresse WAN du routeur distant.

Remarque :

Cette adresse est l'adresse du routeur vers lequel le VPN doit être établie.

Elle ne doit être saisie que si la connexion est de type « initiateur ».

PARAMETRAGE

Paragraphe IKE phase 1

IKE est le protocole d'échange de clés. Il se déroule en deux phases.

La phase 1 de IKE est la phase d'établissement d'un canal de sécurité.

La phase 2 est la phase de négociation des paramètres de cryptage des données échangées par les routeurs.

Ce paragraphe permet de choisir les paramètres de la phase 1.

Paramètre « Mode » :

Les modes « Main » et « Agressive » sont proposés.

Le mode « Agressive » est un mode moins sécurisé.

Paramètres «Algorithme de cryptage » :

Sauf difficulté particulière, on sélectionnera le choix « Auto ».

AES offre une meilleure sécurité par que 3DES.

Paramètres «Algorithme d'authentification» :

Sauf difficulté particulière, on sélectionnera le choix « Auto ».

SHA1 offre une meilleure sécurité par que MD5.

Paramètres «Groupe DH» (uniquement si la case « paramètres avancés » a été cochée) :

Groupe utilisé lors de l'échange de clefs Diffie-Hellman (DH). Le DH est l'étape 1 de la phase 1 et permet aux pairs de se mettre d'accord sur un secret partagé. Le DH a besoin qu'un groupe (au sens structure algébrique) soit défini et identique sur les pairs pour fonctionner. Plus le groupe est grand, plus la sécurité est élevée, au détriment du temps d'établissement du VPN. Recommandé : groupe 2.

La même valeur doit être choisie dans les 2 routeurs participant au VPN.

Paramètres «Life-time» (uniquement si la case « paramètres avancés » a été cochée) a été cochée) :

Saisir la durée de vie de la clé.

Paragraphe IKE phase 2

La phase 2 de IKE est la phase de négociation des paramètres de cryptage des données échangées par les routeurs.

Paramètres «Protocole» :

Préférer ESP à AH.

ESP assure confidentialité, intégrité et authentification des paquets échangés par les routeurs.

AH assure intégrité et authentification mais pas la confidentialité (ou cryptage).

Paramètres «Algorithme de cryptage » :

Sauf difficulté particulière, on sélectionnera le choix « Auto ».

AES offre une meilleure sécurité par que 3DES.

Paramètres «Algorithme d'authentification» :

Sauf difficulté particulière, on sélectionnera le choix « Auto ».

SHA1 offre une meilleure sécurité par que MD5.

Case à cocher «PFS» :

PFS (Perfect forward Secrecy) garantit qu'un attaquant ayant enregistré des échanges chiffrés à un instant donné et parvenant à obtenir les secrets cryptographiques à une date ultérieure ne puisse pas pour autant déchiffrer les enregistrements.

Le renouvellement périodique de la clé renforce la sécurité.

Paramètres «Groupe DH» (uniquement si la case « PFS a été cochée) :

Groupe utilisé lors de l'échange de clefs Diffie-Hellman (DH). Le DH est l'étape 2 de la phase 1 et permet aux pairs de se mettre d'accord sur un secret partagé. Le DH a besoin qu'un groupe (au sens structure algébrique) soit défini et identique sur les pairs pour fonctionner. Plus le groupe est grand, plus la sécurité est élevée, au détriment du temps d'établissement du VPN. Recommandé : groupe 2.

La même valeur doit être choisie dans les 2 routeurs participant au VPN.

Paramètres «Life-time» (uniquement si la case « PFS a été cochée) :

Saisir la durée de vie de la clé de la phase 2.

Paragraphe DPD time-out

Paramètre « Période des messages DPD Keepalives » :

Le VPN est entretenu périodiquement par chaque routeur ; pour ce faire, et en l'absence de données à émettre, chaque routeur transmet une trame de maintien du VPN.

Ce paramètre fixe la période d'envoi de la trame de maintien du VPN par le routeur.

Paramètre « Délai de détection de perte de connexion » :

Ce paramètre fixe le délai maximum d'attente d'un message Keep-alive.

Une fois ce délai échu, et en l'absence de réception du message Keep alive, le routeur coupe le VPN.

7 Connexion VPN de type OpenVPN

7.1 Présentation

Chaque connexion VPN de type OpenVPN est un tunnel établi entre deux routeurs.

Ce tunnel VPN permet de connecter deux réseaux de façon sûre et transparente : Lorsque le tunnel est établi entre 2 routeurs, chaque équipement du premier réseau peut échanger des trames IP avec chaque équipement du second.

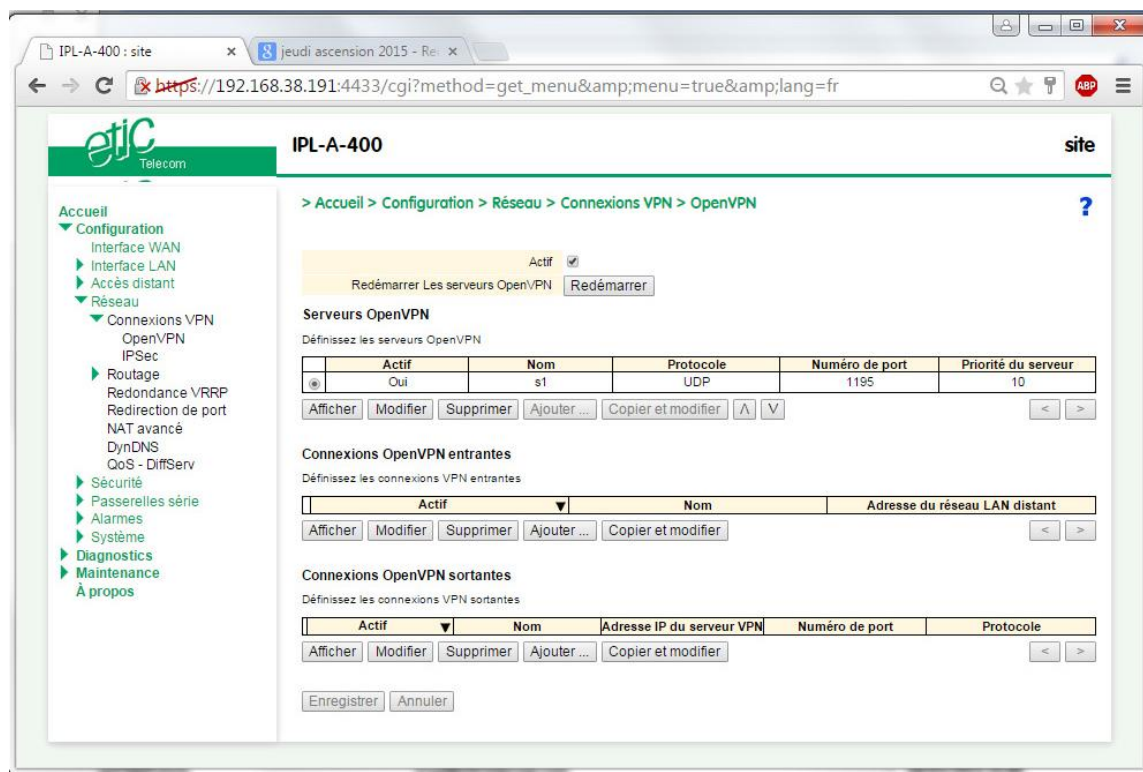
Sur un IPL ou un RAS, 10 connexions OpenVPN peuvent être créées.

Sur un SIG, 100 connexions OpenVPN peuvent être créées.

Sur un SIG VM, 500 connexions OpenVPN peuvent être créées.

- Pour configurer les connexions OpenVPN, sélectionner le menu Configuration > Réseau > OpenVPN.

L'écran des connexions VPN s'affiche.



7.2 Client et serveur OpenVPN

Client OpenVPN

Le routeur qui initie la connexion VPN est appelé le client OpenVPN ; il initie une connexion sortante.

Serveur OpenVPN

Le routeur qui accepte la connexion VPN est appelé le serveur OpenVPN. il accepte une connexion entrante.



Le routeur initie la connexion VPN
Pour ce routeur, la connexion est sortante
Ce routeur est le client VPN

Le routeur accepte la connexion VPN
Pour ce routeur, la connexion est entrante
Ce routeur est le serveur VPN

7.3 Authentification des participants à une connexion VPN

Chaque Routeur est livré avec un certificat émis par ETIC TELECOM.

Lorsqu'il initie la connexion VPN, le routeur client VPN, s'identifie auprès du serveur VPN en présentant son Identifiant et mot de passe et s'authentifie en présentant un extrait de son certificat.

Ces informations doivent donc être enregistrées dans le routeur serveur VPN afin qu'il puisse accepter la connexion entrante.

7.4 Règles du paramétrage

Paramètres d'identification du client VPN

Les paramètres qui caractérisent chaque connexion VPN sont enregistrés dans le serveur VPN : Identifiant, mot de passe, extrait du certificat du client OpenVPN, N° de port de destination et protocole de transport du VPN (UDP ou TCP).

Paramètres techniques de la connexion VPN

Le N° de port, le protocole de transport, les valeurs des paramètres de chiffrement (Blowfish, AES 256, AES192, AES128, 3DES) et d'authentification (MD5, SHA1) doivent être identiques dans le serveur VPN et dans tous les clients abonnés au même serveur VPN.

Adresses IP des réseaux distants connectés au moyen du VPN

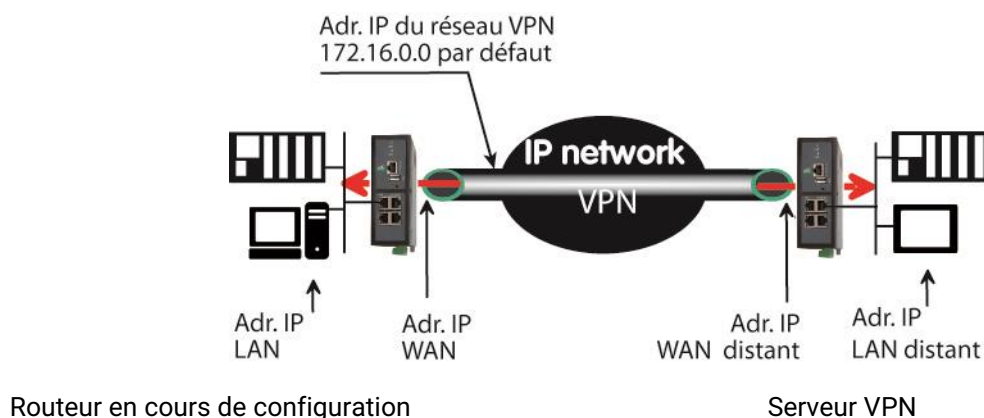
Le réseau « LAN » et le réseau « LAN distant » doivent être différents.

Plus généralement, si plusieurs routeurs établissent chacun un VPN vers le même serveur, les domaines des réseaux doivent tous être différents.

Par exemple :

Réseau LAN :	192.168.1.0	netmask 255.255.255.0
Réseau LAN distant :	192.168.2.0	netmask 255.255.255.0

PARAMETRAGE



Configuration d'une connexion VPN entrante

Pour configurer une connexion entrante, il faut tout d'abord configurer la fonction « serveur VPN » puis déclarer la ou les connexions entrantes.

Configuration d'une connexion VPN sortante

Pour configurer une connexion sortante, il est inutile de configurer le serveur VPN.

7.5 Paramétrage du serveur OpenVPN

Le serveur VPN doit être configuré uniquement lorsque le Routeur doit accepter une ou plusieurs connexions entrantes provenant des clients VPN.

Après avoir configuré le serveur VPN, il faut déclarer les connexions entrantes (voir paragraphe suivant).

- Sélectionner le menu Configuration > Réseau > OpenVPN, puis cliquer le bouton « Ajouter » situé sous le tableau intitulé « Serveur VPN ».

(Paramètres « Numéro de port » et « protocole » :

On choisira de préférence le protocole UDP plutôt que TCP pour une meilleure efficacité.

Remarques :

Tous les clients VPN raccordés au serveur VPN doivent utiliser le N° de port et le protocole.

Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour la connexion des utilisateurs distants.

Paramètres « Adresse réseau VPN » et Masque réseau VPN :

Le tunnel VPN une fois établi est équivalent à une liaison par câble Ethernet. Chaque extrémité du tunnel doit avoir une adresse IP. Il s'agit d'une adresse IP appartenant à un réseau privé et nécessaire pour le fonctionnement du tunnel, mais non visible pour les applications. Cette adresse IP ne doit pas être confondue avec l'adresse IP du routeur.

Paramètre « Délai de détection de perte de connexion » :

En l'absence de données à émettre, le VPN est entretenu périodiquement par le client VPN au moyen d'un paquet de contrôle.

A l'issue de ce délai, en l'absence de réception d'un acquittement au paquet de contrôle de la part du serveur,

le VPN est déconnecté par le client. Le client peut alors tenter de le rétablir par la même interface ou bien par une interface de secours.

Ce paramètre fixe la période d'envoi du paquet de contrôle.

Prenons un exemple :

Si on fixe ce paramètre à 15 minutes, et en cas d'interruption de la connexion VPN, elle ne sera détectée par le client qu'à l'issue de ce délai.

Si on fixe la valeur à 1 mn, le temps d'interruption ne sera que de 1 mn au maximum., mais la transmission du paquet de contrôle à intervalle réduit peut engendrer un trafic gênant ou coûteux sur un réseau cellulaire.

Paramètre « Délai de retransmission » :

C'est le délai au bout duquel le Routeur ré-émet le paquet de contrôle de connexion en l'absence d'acquittement.

Paramètres « Chiffrement » & « Authentification » :

Les algorithmes de cryptage et de hachage proposés sont tous d'un haut niveau de sécurité.

Par défaut, choisir Blowfish et MD5.

Paramètre « Priorité du serveur » :

Laisser la valeur 10.

Paramètre « Pousse la route locale aux clients VPN » :

Laisser cette case cochée.

Dans ce cas, le serveur indique à tous les clients VPN qu'il faut passer par le VPN pour atteindre le réseau LAN du serveur.

Paramètre « Pousse les routes statiques aux clients VPN » :

Dans ce cas, le serveur indique à tous les clients VPN qu'il faut passer par le VPN pour atteindre les réseaux accessibles par les routes statiques du serveur VPN.

Paramètre « Pousse les routes aux clients VPN » :

Cette fonction est utile pour permettre à un équipement raccordé à un client VPN d'échanger des données avec un autre équipement raccordé à un client VPN (client to client).

Le serveur VPN a connaissance de la route qui mène à chaque réseau raccordé à chaque routeur client VPN.

- Si cette case n'est pas sélectionnée, un équipement raccordé à un routeur client VPN peut échanger des trames IP avec un équipement raccordé au serveur VPN.
Mais il ne peut pas échanger des trames IP avec un équipement raccordé à un autre routeur client VPN.

Pour que des équipements raccordés à deux routeurs clients VPN différents puissent échanger des trames, il faut enregistrer une route statique dans chaque routeur client VPN, ou bien cocher la case.

- Si cette case est sélectionnée, le serveur diffuse ces routes vers tous les clients.
Ainsi, tout équipement raccordé à un routeur client VPN peut échanger des trames IP avec tout autre équipement raccordé à un autre routeur sans qu'il soit nécessaire de programmer des routes.

Paramètre « 1ere route spécifique à pousser / adresse IP et netmask » :

Envoie aux clients les chemins : "la valeur du paramètre" via "le VPN"

Paramètre « 2eme route spécifique à pousser / adresse IP et netmask » :

Envoie aux clients les chemins : "la valeur du paramètre" via "le VPN"

PARAMETRAGE

7.6 Configurer les connexions OpenVPN entrante

Après avoir déclaré le serveur VPN (paragraphe précédent), il faut déclarer chacune des connexions entrantes afin de permettre au serveur d'identifier les clients VPN.

Les paramètres à saisir sont l'identificateur, le mot de passe et l'extrait du certificat du client, mais aussi le domaine IP du réseau distant afin de rendre possible le routage d'un client à un autre ou du serveur aux clients.

- Pour créer une connexion entrante, cliquer le bouton « **Ajouter** » placé sous le tableau des connexions entrantes.

The screenshot shows a web browser window with the URL `https://192.168.38.191:4433/cgi?method=get_menu&menu=true&lang=fr`. The page title is "IPL-A-400" and the breadcrumb trail is "> Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexion OpenVPN". The left sidebar contains a navigation menu with categories: Accueil, Configuration (Interface WAN, Interface LAN, Ethernet et IP, Serveur DHCP, Liste des équipements), Accès distant, Liste des utilisateurs, Droits d'accès, Moyens d'accès, Réseau (Connexions VPN, OpenVPN, IPSec), Routage (Redondance VRRP, Redirection de port, NAT avancé, DynDNS, QoS - DiffServ), and Sécurité (Pare-feu). The main content area is for configuring an OpenVPN connection. It includes a checkbox for "Actif" (checked), a "Nom" field, and a section for authentication: "Indiquez l'identifiant et le mot de passe avec lesquels le routeur distant devra s'authentifier". This section has fields for "Identifiant", "Mot de passe", and "Mots de passe identiques". Below this are fields for "Adresse du réseau LAN distant" and "Masque du réseau LAN distant". At the bottom, there is a section for the certificate: "Entrez ici le nom commun du certificat que le routeur distant devra utiliser pour s'identifier" with a "Nom commun" field. At the very bottom are buttons for "Enregistrer", "Annuler", and "Retour".

- Sélectionner la case à cocher « Actif » et attribuer un nom à la connexion.

Paramètres « Identifiant et mot de passe » :

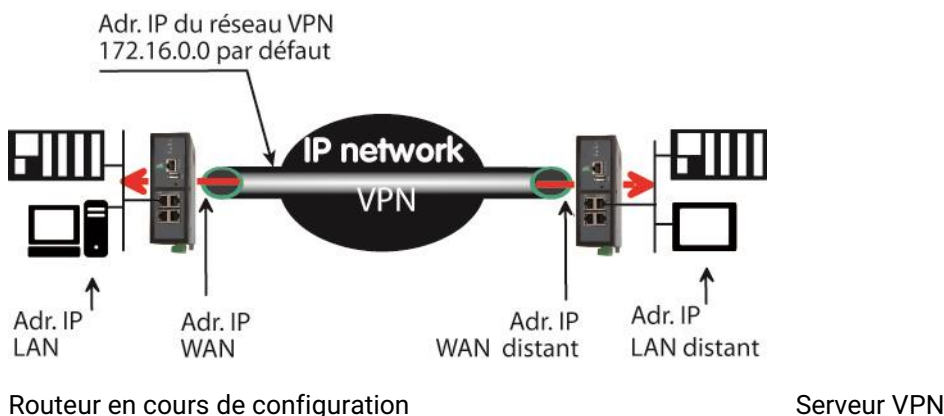
Saisir l'identifiant et le mot de passe qui seront présentés par le routeur distant pour s'authentifier.

Paramètres « Adresse IP du LAN distant » & « Masque du réseau LAN distant » :

Saisir l'adresse du réseau LAN du routeur distant.

Paramètre « Nom commun » :

Entrez la valeur du champ 'SubjectAltName' du certificat actif du routeur distant.
Pour les certificats émis par ETIC TELECOM, il s'agit du champ Email.



7.7 Configurer une connexion OpenVPN sortante

Une connexion sortante est une connexion VPN établie à l'initiative du routeur.

- Pour créer une connexion sortante, cliquer le bouton « **Ajouter** » placé sous le tableau des connexions sortantes.

- Sélectionner la case à cocher « Actif » et attribuer un nom à la connexion.

Paramètres « Identifiant et mot de passe » :

Saisir l'identifiant et le mot de passe qui seront utilisés par le routeur pour s'authentifier auprès du serveur VPN en complément du certificat.

Remarque : Cet identifiant et ce mot de passe devront donc être enregistrés dans la connexion entrante du serveur VPN.

Paramètre « Adresse IP du serveur VPN » :

PARAMETRAGE

C'est l'adresse vers laquelle le tunnel VPN doit être établi.

Cette adresse peut être soit l'adresse IP fixe Internet du routeur distant, soit son nom de domaine sur DynDns.org ou NoIP, soit son nom de domaine.

Paramètre « Adresse IP du serveur VPN de backup » :

Ce paramètre permet de désigner un serveur VPN de secours.

Si le serveur principal n'est pas accessible le routeur IPL établit le VPN avec le serveur de secours.

En l'absence de serveur VPN de secours, laisser ce champ vide.

Paramètres « Numéro de port » et « protocole » :

On choisira de préférence le protocole UDP plutôt que TCP pour une meilleure efficacité.

Paramètres « Chiffrement » & « Authentification » :

Les algorithmes de cryptage et de hachage proposés sont tous d'un haut niveau de sécurité (par exemple l'ancien algorithme DES n'est pas proposé).

Toutefois, AES offre une meilleure sécurité par rapport à 3DES, de même que SHA-1 par rapport MD5.

Paramètres « lier le VPN à une interface spécifique » :

Note : Les interfaces proposées dépendent du modèle de Routeur.

Lier le VPN à l'interface ADSL

- Pour forcer l'établissement du VPN vers l'interface ADSL, sélectionner la valeur « WAN ADSL ».

Lier le VPN à l'interface cellulaire

- Pour forcer l'établissement du VPN vers l'interface cellulaire, sélectionner la valeur «WAN cellulaire».

Lier le VPN à l'interface Ethernet N°1 déclarée comme WAN à la place du cellulaire

- Pour forcer l'établissement du VPN vers l'interface Ethernet N°1 (si elle a été sélectionnée comme WAN à la place du cellulaire), sélectionner la valeur «WAN Ethernet».

Lier le VPN à l'interface Ethernet LAN

- Pour forcer l'établissement du VPN vers l'interface LAN, sélectionner la valeur «LAN Ethernet».

Secourir la défaillance de l'interface la plus prioritaire par une autre interface (IPL-DAC)

Trois interfaces IP peuvent être actives simultanément l'interface ADSL, l'interface cellulaire (ou Ethernet WAN en remplacement) et l'interface LAN.

- Pour secourir l'interface la plus prioritaire (ADSL par exemple) par une interface moins prioritaire (cellulaire par exemple), sélectionner la valeur « Tous ».

En cas de défaillance de la liaison ADSL, le Routeur désactive la route correspondante ; le VPN est aiguillé par le réseau cellulaire.

Case à cocher « Démarrer sur événement » :

Le VPN est habituellement établi par le routeur dès la mise sous tension.

Cependant, il peut être intéressant de pouvoir commander l'établissement du VPN ; par exemple pour mettre en œuvre des fonctions de secours (voir paragraphe paramétrage de la fonction de secours).

Il est possible de déclencher l'établissement du VPN sur l'un des événements suivants :

- WAN connecté
- WAN déconnecté
- WAN Ethernet connecté
- WAN Ethernet déconnecté
- Entrée digitale fermée
- Entrée digitale ouverte

Case à cocher « Envoyer une alarme sur connexion / déconnexion » :

Ce VPN génère un événement qui peut être traité dans la page web "alarmes, sms/email" lorsque on choisit comme source d'alerte connexion / déconnexion VPN.

8 Paramétrer le routeur pour secourir une liaison défailante

Le présent paragraphe s'applique au routeur IPL-DAC qui permet de secourir une ligne ADSL et cellulaire.

Remarque préliminaire :

Dans le paragraphe ci-dessous, et pour plus de simplicité, on décrit les fonctions et le paramétrage du secours en désignant comme interface principale l'interface ADSL et l'interface cellulaire comme interface de secours ; mais l'inverse est possible ; il est aussi possible de raccorder un modem routeur externe à l'interface Ethernet N°1 au lieu d'utiliser l'interface cellulaire intégrée.

Une utilisation du routeur IPL-DAC est le secours de liaison ADSL par le réseau cellulaire ; 4 solutions de secours sont proposées.

Dans le cas de la solution 1, le routeur bascule lorsque l'interface ADSL (ou plus généralement l'interface la plus prioritaire) est déclarée Down. Il transmet alors sur l'interface moins prioritaire.

Dans le cas des solutions 2, 3 ou 4, le routeur établit 2 connexions VPN ; l'une sur l'interface ADSL et l'autre en secours sur l'interface cellulaire.

Le routeur bascule le trafic lorsque le VPN de l'interface ADSL est déconnecté.

scénario	Critère de basculement	Critère de basculement	Observation
	Aller	Retour	
1	Interface ADSL déconnecté	Interface ADSL connecté	Solution simple et universelle Ne fonctionne pas avec tunnel IPSec
2	VPN OpenVPN «Normal» déconnecté	VPN OpenVPN «Normal» connecté	Le critère de basculement est la perte du VPN Détection de basculement rapide
3	VPN OpenVPN «Normal» déconnecté	VPN OpenVPN «Normal» connecté	Le critère de basculement est la perte du VPN Variante du scénario 2
4	VPN IPSec «Normal» déconnecté	VPN IPSec «Normal» connecté	Le critère de basculement est la perte du VPN

8.1 Basculement sur détection de perte de la liaison ADSL

8.1.1 Objectif

Proposer une solution universelle pour secourir la liaison ADSL par le réseau cellulaire

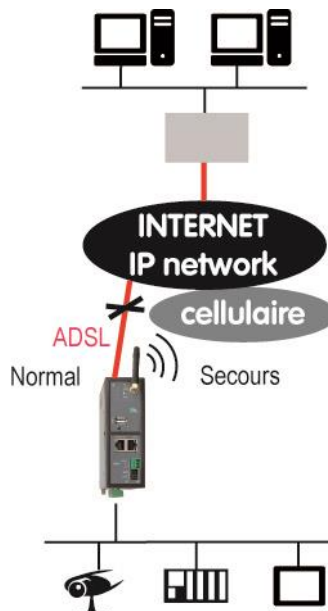
8.1.2 Solution

L'interface ADSL est déclarée avec une priorité haute (valeur 10) et l'interface cellulaire avec une priorité basse (valeur 20).

Lorsque le Routeur détecte la perte de la liaison ADSL, et après confirmation, il désactive la route correspondante ; les données sont automatiquement routées vers le réseau cellulaire.

Dès que l'interface ADSL est à nouveau active, les données sont véhiculées par l'interface ADSL.

Cette solution fonctionne dans toutes les situations sauf si le routeur doit établir un tunnel IPSec



8.1.3 Paramétrage du routeur IPL-DAC

Menu : Configuration >	Observation
>Interface. WAN > WAN ADSL	Affecter au paramètre Priorité une valeur faible : 10 par exemple
>Interface. WAN > Interface WAN	Affecter au paramètre Priorité une valeur plus élevée : 20 par exemple
Si un VPN OpenVPN doit être établi :	
>réseau>OpenVPN>Connexion sortante	Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « Tous »

PARAMETRAGE

8.2 Secours de connexion OpenVPN (Mode standard)

8.2.1 Objectif

Obtenir un basculement ADSL / cellulaire rapide.

Fournir une solution compatible du cas où deux serveurs VPN agissent en redondance.

8.2.2 Solution proposée

Pour se prémunir de la défaillance du serveur VPN, ou de la liaison du serveur VPN à l'internet ou à un réseau d'opérateur, on associe le routeur IPL-DAC et le serveur VPN de référence SIG.

De nombreux routeurs IPL-DAC peuvent être reliés au même serveur VPN.

Deux routeurs SIG agissant en serveurs VPN peuvent être placés en redondance.

Si un routeur SIG unique est utilisé, cette solution procure une bonne rapidité de basculement mais, bien sûr, ne procure pas la sécurité maximale puisque le routeur central n'est pas dupliqué.

Si le routeur SIG est dupliqué, soit au moyen de VRRP, soit qu'un autre routeur central de secours soit placé sur un autre site, la solution proposée procure la rapidité mais aussi une meilleure disponibilité du système puisque la défaillance du routeur central ou même de sa liaison peut être palliée.

Le principe utilisé est d'établir en permanence deux VPNs à partir de chaque routeur IPL-DAC : L'un sur l'ADSL et l'autre sur le réseau cellulaire, par exemple.

Les données sont aiguillées vers le VPN désigné comme le plus prioritaire (le VPN de l'interface ADSL en général).

Différentes variantes de cette solution peuvent donc être mises en œuvre selon la façon dont les serveurs VPN sont reliés à Internet ou au réseau d'opérateur; dans le présent paragraphe, on étudie le cas des schémas 1 ou 2 ci-dessous.

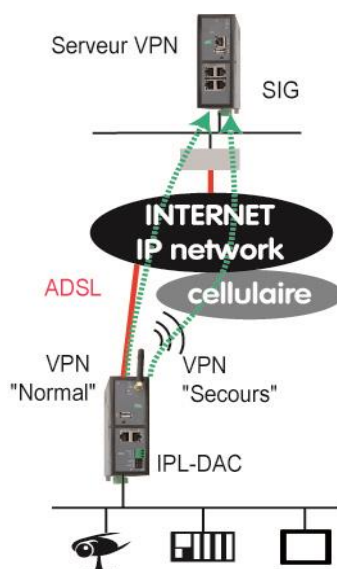


Schéma 1

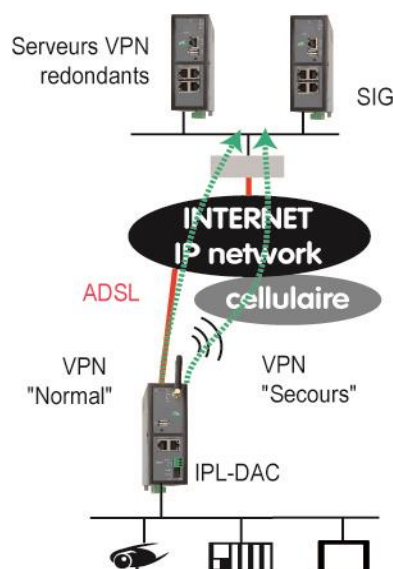


Schéma 2

8.2.3 Principe de fonctionnement du Mode standard

Dans le routeur IP-DAC, on crée deux connexions OpenVPN VPN sortantes établies en permanence :

Le client OpenVPN « Normal » est lié à l'interface ADSL.

Le client OpenVPN « Secours » est lié à l'interface Cellulaire.

Le VPN « Normal » et le VPN « Secours » doivent être transportés dans deux ports différents (UDP 1195 pour l'un et UDP 1196 pour l'autre par exemple) pour pouvoir être différenciés par le serveur VPN.

Dans chaque routeur faisant office de serveur VPN, on crée deux serveurs VPN ; l'un appelé serveur VPN Normal sur le port UDP1195 et avec une priorité haute et l'autre appelé Secours sur le port UDP 1196 avec une priorité basse.

Lorsque les deux VPNs sont connectés, le serveur VPN utilise le VPN « Normal » déclaré plus prioritaire pour véhiculer les données. Les données sont véhiculées par l'interface ADSL du routeur IPL-DAC.

Lorsque le VPN « Normal » se déconnecte, le serveur le VPN utilise le VPN « Secours » de priorité moindre. Les données sont véhiculées par l'interface cellulaire du routeur IPL-DAC.

Remarque : Le VPN « Secours » est établi en permanence sur le réseau cellulaire ; cela signifie qu'une trame de contrôle est transmise périodiquement sur le réseau cellulaire ; la consommation correspondante est de quelques dizaines de MO/mois sur le réseau cellulaire. Elle dépend de la valeur du paramètre «Délai de détection de la perte de connexion » programmé dans le serveur VPN « Secours ».

Typiquement la consommation est de 20 MO/ mois pour un délai de détection de 15 mn de perte du VPN de secours.

8.2.4 Paramétrage du routeur IPL-DAC

Paramétrage du routeur IPL-DAC	
Menu : Configuration >	Observation
>Interface. WAN > WAN ADSL	Affecter au paramètre Priorité une valeur faible : 10 par exemple.
>Interface. WAN > Interface WAN cellulaire	Affecter au paramètre Priorité une valeur plus élevée : 20 par exemple.
>Réseau>OpenVPN>Connexion sortante	- Créer une connexion VPN avec le nom « Normal » : Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN ADSL ». Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). - Créer une connexion VPN avec le nom « Secours » : Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN cellulaire » Sélectionner le port 1196 et le protocole UDP pour le transport du VPN.

PARAMETRAGE

Ecran de paramétrage du client
VPN « Normal »

The screenshot shows the web interface of the IPL-DAC-400 router. The left sidebar contains a navigation menu with options like 'Accueil', 'Configuration', 'Interfaces WAN', 'Interface LAN', 'Accès distant', 'Réseau', 'Connexions VPN', 'OpenVPN', 'IPSec', 'Routage', 'Redondance VRRP', 'Redirection de port', 'NAT avancé', 'DynDNS', 'QoS - DiffServ', 'Sécurité', 'Passerelles série', 'Alarmes', 'Système', 'Diagnostics', 'Maintenance', and 'À propos'. The main content area is titled 'IPL-DAC-400' and shows the path '> Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes'. The 'Actif' checkbox is checked. The form includes fields for 'Nom' (Normal), 'Identifiant' (ETIC TELECOM), 'Mot de passe' (12356), 'Adresse IP du serveur VPN' (10.10.10.1), and 'Adresse IP du serveur VPN de backup'. Below these, there are fields for 'Numéro de port' (1195), 'Protocole' (UDP), 'Chiffrement' (BlowFish), 'Authentification' (MD5), and 'Lier le VPN à une interface spécifique' (WAN ADSL). There are also checkboxes for 'Démarrer sur événement' and 'Envoyer une alarme sur connexion/déconnexion'. The bottom of the form has buttons for 'Enregistrer', 'Annuler', and 'Retour'.

Ecran de paramétrage du client
VPN « Secours »

The screenshot shows the web interface of the IPL-DAC-400 router, similar to the previous one but for a 'Secours' (Backup) VPN client. The left sidebar and main content area are the same. The 'Actif' checkbox is checked. The form includes fields for 'Nom' (Secours), 'Identifiant' (ETIC TELECOM), 'Mot de passe' (123456), 'Adresse IP du serveur VPN' (10.10.10.1), and 'Adresse IP du serveur VPN de backup'. Below these, there are fields for 'Numéro de port' (1196), 'Protocole' (UDP), 'Chiffrement' (BlowFish), 'Authentification' (MD5), and 'Lier le VPN à une interface spécifique' (WAN 3G). There are also checkboxes for 'Démarrer sur événement' and 'Envoyer une alarme sur connexion/déconnexion'. The bottom of the form has buttons for 'Enregistrer', 'Annuler', and 'Retour'.

8.2.5 Paramétrage du serveur VPN

Deux routeurs faisant office de serveur VPN peuvent être placés en redondance l'un de l'autre au moyen de VRRP et de RIP. Leurs serveurs VPN doivent être paramétrés de façon identique.

Deux serveurs VPNs doivent être déclarés dans chaque routeur faisant office de serveur VPN.

Paramétrage du routeur serveur VPN	
Menu : Configuration >	Observation
>Réseau>OpenVPN>Serveur VPN	• Créer un premier serveur VPN avec le nom « Normal » : Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). Régler le paramètre « Délai de détection de perte de connexion à 20 s voir moins si nécessaire. Cette valeur détermine le temps de basculement. Affecter une priorité élevée au serveur VPN (10 par exemple). • Créer un second serveur VPN avec le nom « Secours » : Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). Régler le paramètre « Délai de détection de perte de connexion à 15 mn ou moins si nécessaire. Cette valeur détermine le temps de basculement en retour. Plus elle est faible, plus le trafic d'entretien du VPN sur le réseau cellulaire est important. Affecter une priorité basse au serveur VPN (20 par exemple).

8.2.6 Estimation de performance

Les valeurs ci-dessous sont données à titre indicatif.

Délai de basculement ADSL vers cellulaire = 20 s

Le flux de données est interrompu tant que la perte du VPN n'a pas été détectée.

Ce délai est égal à la valeur du temporisateur de perte de connexion du VPN « Normal » programmé dans le serveur VPN.

Délai de basculement cellulaire vers ADSL= 10s

Dès que l'interface ADSL est à nouveau active et le VPN à nouveau établi, les données sont à nouveau routées par l'interface ADSL.

L'interruption n'est que de quelques secondes.

PARAMETRAGE

8.3 Secours de connexion OpenVPN (Mode Eco)

8.3.1 Objectif

L'objectif est le même que dans le cas du scénario 2, mais on cherche à éviter le trafic périodique d'entretien du VPN sur le réseau cellulaire.

8.3.2 Solution proposée

La solution est identique à la solution du scénario 2, mais le VPN de secours n'est établi que lorsque le VPN normal est déconnecté.

8.3.3 Principe de fonctionnement du Mode Eco

Les VPN « Normal » est établi en permanence sur l'ADSL et le VPN « Secours » est établi sur le réseau cellulaire uniquement lorsque le VPN « Normal » se déconnecte.

8.3.4 Paramétrage du routeur IPL-DAC

Paramétrage du routeur IPL-DAC	
Menu : Configuration >	Observation
>Interface. WAN > WAN ADSL	Affecter au paramètre Priorité une valeur faible : 10 par exemple.
>Interface. WAN > Interface WAN cellulaire	Affecter au paramètre Priorité une valeur plus élevée : 20 par exemple.
>Réseau>OpenVPN>Connexion sortante	• Créer une connexion VPN avec le nom « Normal » : Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN ADSL ». Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). • Créer une connexion VPN avec le nom « Secours » : Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN cellulaire » Sélectionner le port 1196 et le protocole UDP pour le transport du VPN. Cocher la case « Démarrer sur événement » Sélectionner l'événement = « ADSL déconnecté »

Ecran client VPN « Normal »

The screenshot shows the 'IPL-DAC-400' web interface. The left sidebar contains a navigation menu with options like 'Accueil', 'Configuration', 'Interfaces WAN', 'Interface WAN', 'Accès distant', 'Réseau', 'Connexions VPN', 'OpenVPN', 'IPSec', 'Routage', 'Redondance VRRP', 'Redirection de port', 'NAT avancé', 'DynDNS', 'CoS - DiffServ', 'Sécurité', 'Passerelles série', 'Alarmes', 'Système', 'Diagnostics', 'Maintenance', and 'À propos'. The main content area is titled 'IPL-DAC-400' and shows the configuration path: '> Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes'. The configuration is for a 'Normal' VPN client. It includes fields for 'Nom' (Normal), 'Identifiant' (ETIC TELECOM), 'Mot de passe' (12356), 'Adresse IP du serveur VPN' (10.10.10.1), and 'Adresse IP du serveur VPN de backup'. The 'Numéro de port' is 1195, 'Protocole' is UDP, 'Chiffrement' is BlowFish, and 'Authentification' is MD5. The 'Lier le VPN à une interface spécifique' is set to WAN ADSL. There are checkboxes for 'Démarrer sur événement' and 'Envoyer une alarme sur connexion/déconnexion'. Buttons at the bottom are 'Enregistrer', 'Annuler', and 'Retour'.

Ecran client VPN « Secours »

The screenshot shows the 'IPL-DAC-400' web interface with the same navigation menu as the previous screen. The main content area shows the configuration path: '> Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes'. The configuration is for a 'Secours' VPN client. It includes fields for 'Nom' (Secours), 'Identifiant' (ETIC TELECOM), 'Mot de passe' (123456), 'Adresse IP du serveur VPN' (10.10.10.1), and 'Adresse IP du serveur VPN de backup'. The 'Numéro de port' is 1196, 'Protocole' is UDP, 'Chiffrement' is BlowFish, and 'Authentification' is MD5. The 'Lier le VPN à une interface spécifique' is set to WAN 3G. There are checkboxes for 'Démarrer sur événement' and 'Démarrer seulement lorsque WAN ADSL déconnecté'. There is also a checkbox for 'Envoyer une alarme sur connexion/déconnexion'. Buttons at the bottom are 'Enregistrer', 'Annuler', and 'Retour'.

PARAMETRAGE

8.3.5 Paramétrage du serveur VPN

Deux routeurs faisant office de serveur VPN peuvent être placés en redondance l'un de l'autre au moyen de VRRP et de RIP. Leurs serveurs VPN doivent être paramétrés de façon identique.

Deux serveurs VPNs doivent être déclarés dans chaque routeur faisant office de serveur VPN.

Paramétrage du routeur serveur VPN	
Menu : Configuration >	Observation
>Réseau>OpenVPN>Serveur VPN	• Créer un premier serveur VPN avec le nom « Normal » : Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). Régler le paramètre « Délai de détection de perte de connexion à 20 s voir moins si nécessaire. Cette valeur détermine le temps de basculement. Affecter une priorité élevée au serveur VPN (10 par exemple). • Créer un second serveur VPN avec le nom « Secours » : Sélectionner le port 1195 et le protocole UDP pour le transport du VPN (exemple). Régler le paramètre « Délai de détection de perte de connexion à 15 mn ou moins si nécessaire. Cette valeur détermine le temps de basculement en retour. Plus elle est faible, plus le trafic d'entretien du VPN sur le réseau cellulaire est important. Affecter une priorité basse au serveur VPN (20 par exemple).

8.3.6 Estimation de performance

Les valeurs ci-dessous sont données à titre indicatif.

Délai de basculement ADSL vers cellulaire = 1 mn

Le flux de données est interrompu tant que la perte du VPN « Normal » n'a pas été détectée ; il faut ajouter à ce délai le temps d'établissement du VPN « Secours ».

Délai de basculement cellulaire vers ADSL= 10s

Dès que l'interface ADSL est à nouveau active et le VPN « Normal » à nouveau établi, les données sont à nouveau routée par l'interface ADSL.

L'interruption n'est que de quelques secondes.

8.4 Secours de connexion IPSec

8.4.1 Objectif

Obtenir un basculement ADSL / cellulaire rapide.

Fournir une solution compatible des tunnels IPSec et du cas où deux serveurs VPN IPSec agissent en redondance.

8.4.2 Solution proposée

Pour se prémunir de la défaillance du serveur VPN, ou de la liaison du serveur VPN à l'internet ou à un réseau d'opérateur, on associe le routeur IPL-DAC et le serveur VPN de référence SIG.

De nombreux routeurs IPL-DAC peuvent être reliés au même serveur VPN.

Deux routeurs SIG agissant en serveurs VPN peuvent être placés en redondance.

Si un routeur SIG unique est utilisé, cette solution protège contre la défaillance de la liaison ADSL du routeur IPL-DAC mais ne procure pas la sécurité maximale puisque le routeur central n'est pas dupliqué.

Si le routeur SIG est dupliqué, soit au moyen de VRRP, soit qu'un autre routeur central de secours soit placé sur un autre site, la solution proposée procure la rapidité mais aussi une meilleure disponibilité du système puisque la défaillance du routeur central ou même de sa liaison peut être palliée.

Le principe utilisé est d'établir deux VPNs à partir de chaque routeur IPL-DAC : L'un sur l'ADSL et l'autre sur le réseau cellulaire. La connexion VPN « Secours » n'est établie que lorsque la connexion « Normal » se déconnecte ».

Les données sont aiguillées vers le VPN désigné comme le plus prioritaire (le VPN de l'interface ADSL en général).

Différentes variantes de cette solution peuvent donc être mises en œuvre selon la façon dont les serveurs VPN sont reliés à Internet ou au réseau d'opérateur; dans le présent paragraphe, on étudie le cas des schémas 1 ou 2 ci-dessous.

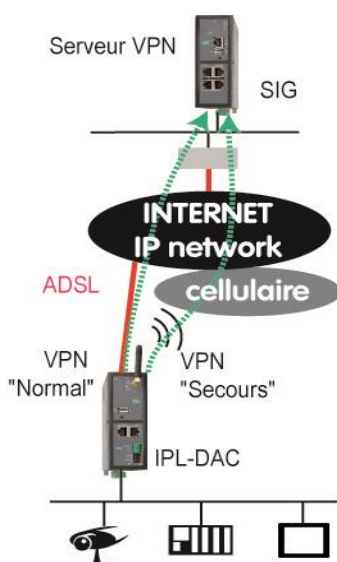


Schéma 1

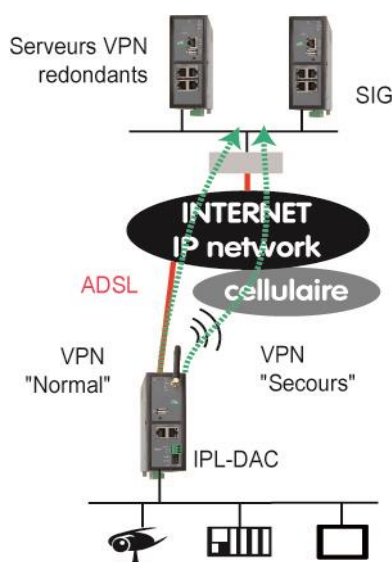


Schéma 2

PARAMETRAGE

8.4.3 Principe de fonctionnement

Dans le routeur IP-DAC, on crée deux connexions IPSec sortantes :

Le client IPSec « Normal » est lié à l'interface ADSL.

Le client IPSec « Secours » est lié à l'interface Cellulaire.

La connexion « Secours » ne s'établit que lorsque la connexion « Normal » est déconnectée.

Dans chaque routeur faisant office de serveur VPN, on crée deux connexions entrantes ; l'une appelée « Normal » avec une priorité haute et l'autre appelée « Secours » avec une priorité basse.

Lorsque le VPN « Normal » se déconnecte, le serveur le VPN utilise le VPN « Secours » de priorité moindre. Les données sont véhiculées par l'interface cellulaire du routeur IPL-DAC.

8.4.4 Paramétrage du routeur IPL-DAC

Paramétrage du routeur IPL-DAC	
Menu : Configuration >	Observation
>Interface. WAN > WAN ADSL	Affecter au paramètre Priorité une valeur faible : 10 par exemple.
>Interface. WAN > Interface WAN cellulaire	Affecter au paramètre Priorité une valeur plus élevée : 20 par exemple.
>Réseau>Connexions VPN>IPSec	• Créer une connexion VPN Initiateur avec le nom « Normal » : Utiliser obligatoirement l'authentification par Certificat et pas par clé partagée. Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN ADSL ». Fixer la période des messages DPD keep-alive à 30 s et le délai de perte de détection à 1 mn. • Créer une connexion VPN avec le nom « Secours » : Utiliser obligatoirement l'authentification par Certificat et pas par clé partagée. Affecter au paramètre « Lier le VPN à une interface spécifique » la valeur « WAN cellulaire ». Fixer la période des messages DPD keep-alive à 1 mn et le délai de perte de détection à 2 mn. <u>Cocher la case « Démarrer sur événement » et sélectionner l'événement « Aucun VPN connecté »</u>

8.4.5 Paramétrage du serveur VPN

Deux routeurs faisant office de serveur VPN peuvent être placés en redondance l'un de l'autre au moyen de VRRP et de RIP. Leurs serveurs VPN doivent être paramétrés de façon identique.

Paramétrage du routeur serveur VPN	
Menu : Configuration >	Observation
>Réseau>OpenVPN>Serveur VPN	• Créer une connexion VPN Répondeur avec le nom «Normal» réglée comme la connexion Initiateur «Normal» du routeur IPL-DAC. • Créer une connexion VPN Répondeur avec le nom «Secours». Cette connexion est réglée comme la connexion Initiateur «Secours» du routeur IPL-DAC mais la case «Démarrer sur événement» ne doit pas être cochée.

8.4.6 Estimation de performance

Les valeurs ci-dessous sont données à titre indicatif.

Délai de basculement ADSL vers cellulaire = 1 mn

Le flux de données est interrompu tant que la perte du VPN « Normal » n'a pas été détectée ; il faut ajouter à ce délai le temps d'établissement du VPN « Secours ».

Délai de basculement cellulaire vers ADSL= 10s

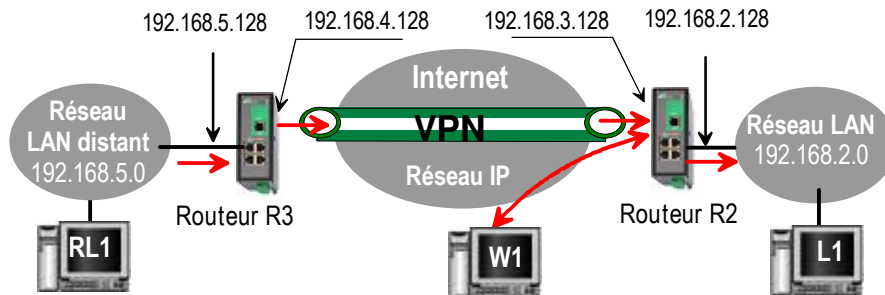
Dès que l'interface ADSL est à nouveau active et le VPN « Normal » à nouveau établi, les données sont à nouveau routées par l'interface ADSL.

L'interruption n'est que de quelques secondes.

9 Routage IP

9.1 Fonctions de base

Le routeur R2 (voir schéma ci-dessous) est prêt à effectuer sa fonction de routeur entre le réseau LAN et l'Internet dès qu'on lui a attribué une adresse IP sur l'interface LAN (ici 192.168.2.128) et une autre sur l'Internet et que l'on a configuré la connexion Internet.



Pour que le routage s'effectue, Il faut cependant enregistrer dans chaque machine du réseau LAN l'adresse LAN du routeur en tant « routeur par défaut ».

Le routeur R2 peut alors router des trames IP entre le réseau «LAN» et le réseau LAN distant au travers du VPN s'il a été défini; par exemple entre la machine RL1 et la machine L1 du schéma ci-dessus. En effet, par défaut, le firewall autorise le transfert entre les deux réseaux si un VPN relie les routeurs.

Par contre, par défaut, les paquets IP émis par la machine W1 depuis l'internet sont bloqués par le firewall.

9.2 Route statique

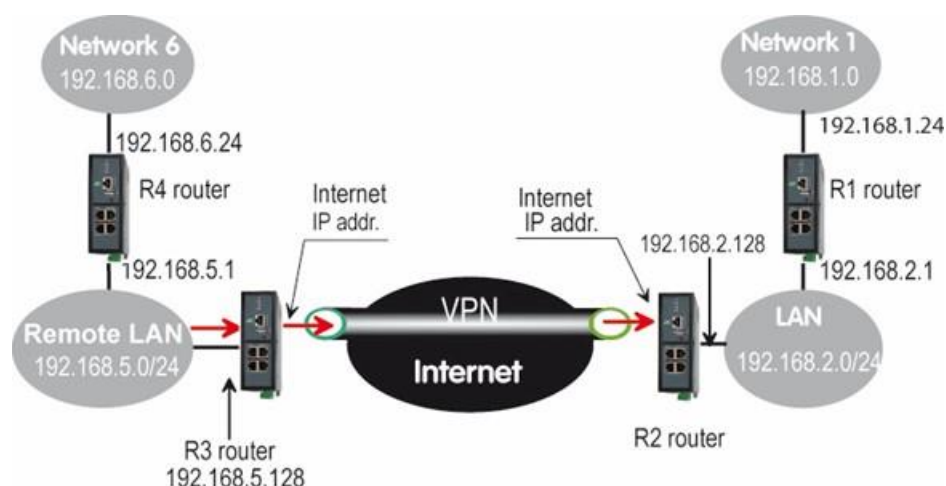
Après avoir configuré ses adresses LAN et WAN et défini la connexion VPN, le routeur R2 (voir schéma ci-dessus) peut router les trames entre le réseau LAN et le WAN et inversement, ainsi qu'entre le LAN et le réseau Remote LAN et inversement au travers du VPN.

Mais il ne peut pas router des trames entre le LAN et un réseau connecté au réseau LAN distant (réseau 6 du schéma ci-dessous).

La raison de cette difficulté est que le réseau 6 n'est pas connu du routeur R2.

La déclaration de routes statiques permet de résoudre ce problème.

Une route statique associe l'adresse d'un routeur voisin à une adresse IP de réseau de destination (adr. Réseau = adr. de base + netmask).



On décrit ci-dessous les routes statiques qui doivent être enregistrées dans le routeur R2 pour que tous les équipements de chacun des réseaux puissent échanger des paquets IP.

Route statique à enregistrer dans le routeur R2						
Active	Nom de la route	Destination	Masque de réseau	Passerelle	Interface	Distance
Oui	Vers Réseau 6	192.168.6.0	255.255.255.0	192.168.5.1		
Oui	Vers Réseau 1	192.168.1.0	255.255.255.0	192.168.2.1		
Oui	Vers Réseau WAN distant	192.168.4.0	255.255.255.0	192.168.5.128		

De la même façon, il faut enregistrer des routes dans les routeurs R1, R3 et R4.

Remarque :

Il n'est pas nécessaire d'enregistrer dans R2 une route vers le réseau WAN ni vers le réseau LAN distant; en effet, R2 les connaît puisque l'adresse et le netmask du réseau WAN ainsi que l'adresse du réseau LAN distant ont été déclarés au cours de la configuration.

Pour programmer une route statique,

- sélectionner le menu « Configuration », puis « Routage » puis « Route statique » puis cliquer « Ajouter une route ».

Paramètre « Nom de la route » :

Entrer un mnémonique pour désigner la route.

Paramètres « Adresse IP de destination » & « netmask » :

Entrer l'adresse IP du réseau de destination et le netmask de ce réseau.

Paramètre « Passerelle » :

Saisir l'adresse IP de la passerelle (routeur) permettant l'accès à ce réseau.

Paramètre « Interface » :

Une route peut être établie en désignant une passerelle (voir ci-dessus) ou bien une interface.

Par exemple : On peut désigner une route passant par l'interface PPOE de la ligne ADSL ou du port Ethernet N°1.

Si une route est établie en désignant l'adresse d'une passerelle, laisser ce champ vide.

PARAMETRAGE

Paramètre «Priorité» :

Le paramètre de priorité s'applique à chaque route statique de la même manière qu'aux liaisons VPNs.

Lorsque deux routes mènent au même réseau de destination, le routeur sélectionne la route la plus prioritaire.

Le degré de priorité est décroissant : Une route de de priorité 10 est plus prioritaire qu'une route de priorité 20.

Remarque :

Ce champ ne doit pas être laissé vide ; en l'absence de nécessité de désigner une priorité, saisir la même valeur, 10 par exemple, pour chacune des routes.

9.3 Protocole RIP

RIP (**R**outing **I**nformation **P**rotocol) est un protocole de routage IP qui permet à chaque routeur d'un réseau de connaître la route menant à un sous réseau quelconque de ce réseau.

Le principe utilisé est le suivant :

Diffusion des tables de routage

Chaque routeur transmet aux routeurs voisins et aux écouteurs RIP voisins, la table qui associe à chaque destination du réseau l'adresse du routeur voisin menant à cette destination ainsi que la métrique de la route pour y parvenir.

Mise à jour des tables de routage

Chaque routeur met à jour sa propre table au moyen des informations reçues des autres.

Le protocole RIP permet d'éviter de déclarer les routes statiques dans chacun des routeurs.

Prenons l'exemple du réseau du paragraphe précédent ; au lieu de déclarer les routes statiques dans les routeurs R1, R2, R3 et R4, il est possible d'activer le protocole RIP dans chacun des routeurs.

Pour activer le protocole RIP,

- Sélectionner le menu Configuration > Routage > RIP.

Cocher les cases « Activer RIP sur l'interface LAN » et la case Activer RIP sur l'interface WAN ».

10 Substitution d'adresses (NAT, Redirection de port, NAT avancé)

Le Routeur offre différentes fonctions de substitution d'adresses IP.

Ces fonctions consistent à remplacer l'adresse IP et le port source ou destination de certaines trames IP traitées par le Routeur.

Les possibilités offertes sont les suivantes :

10.1 Translation d'adresse (NAT)

Cette fonction s'applique aux trames IP issues d'un équipement du réseau LAN et destinées au réseau WAN.

Elle consiste à remplacer l'adresse IP source (celle de l'équipement du LAN) par l'adresse IP WAN du routeur et à effectuer l'opération inverse pour les trames de réponse.

Cette fonction est utile lorsque les équipements du LAN doivent échanger des trames avec l'Internet.

Pour activer la fonction NAT,

- Sélectionner le menu Configuration > Interface WAN
- Cocher la case « Activer la translation d'adresse NAT ».

10.2 Redirection par port

10.2.1 Principe

La redirection de port consiste à transférer vers une machine définie du réseau LAN, un trafic adressé au Routeur sur son interface WAN.

Elle s'applique aux trames adressées au Routeur sur l'interface WAN.

Le critère de « redirection » est le N° du port utilisé ; le mécanisme consiste à utiliser le N° de port de destination comme un complément d'adresse IP :

Une trame IP adressée sur l'interface WAN au Routeur sur le port déterminé P1 (ou un ensemble de ports) peut être redirigée vers un équipement déterminé du réseau LAN.

Le mécanisme de redirection de port décrit ci-dessus permet de résoudre le cas où un équipement appartenant au réseau WAN veut échanger des trames IP avec une ou des équipements du réseau LAN alors que les adresses du réseau LAN ne peuvent être transportées dans le réseau WAN.

La vraie solution à ce problème est d'établir un VPN ; mais lorsque ce n'est pas possible la redirection de port apporte la solution.

Exemple :

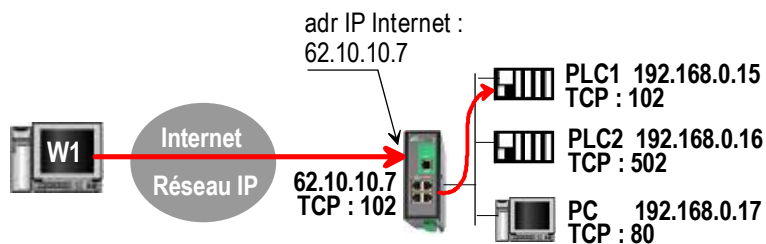
Considérons un réseau 1 et un réseau 2 connectés par un Routeur selon le schéma ci-dessous.
Supposons

1/ que le PC « W1 » du réseau WAN ait à échanger des trames avec l'équipement PLC1 du réseau LAN.

PARAMETRAGE

2/ que les adresses du réseau LAN ne puissent pas circuler sur le réseau WAN, quelle que soit la raison.

La solution la plus performante serait d'établir un VPN qui assurerait à la fois la transparence et la sécurité ; si ce n'est pas possible, on peut procéder comme suit :



Lorsque le PC « W1 » doit adresser une trame à l'équipement « PLC1 » du réseau LAN, il l'adresse à l'adresse IP WAN du routeur IPL-DAC (62.10.10.7 dans notre exemple) et sur le port 102 (par exemple).

Le Routeur analyse la trame, modifie l'adresse IP de destination et éventuellement le N° de port, puis route la trame vers le réseau LAN.

Port (destination)	Redirection	
Service	Device	Service
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

Note :

Les trames IP « redirigées » sont transférées directement à l'équipement choisi sans passer par le filtre principal du firewall.

10.2.2 Configuration

Pour programmer une règle de redirection de port,

- Sélectionner le menu Configuration > Réseau, Routage, et Redirection de port.
- Saisir les caractéristiques des trames qui doivent être redirigées : N° de port (de destination), protocole de transport (TCP, UDP...), adresse IP source (optionnelle).
- Saisir les caractéristiques des trames modifiées : Adresse IP et N° de port de destination, et protocole de transport (TCP, UDP...).

10.3 Substitution généralisée d'adresses IP (NAT avancé)

10.3.1 Principe

La fonction de substitution d'adresses IP consiste à modifier les adresses de source et / ou de destination ainsi que le N° de port des trames IP qui transitent par le routeur.

Elle s'applique à toute trame IP reçue par le routeur aussi bien sur son interface LAN que sur son interface WAN hormis aux trames véhiculées dans une connexion d'utilisateur distant PPTP ou TLS.

Elle s'applique aux trames dont la destination est le Routeur lui-même aussi bien qu'aux trames dont la destination est un équipement du réseau relié directement ou non à l'interface WAN ou à l'interface LAN.

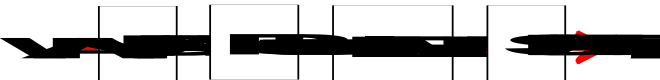
On distingue

la fonction DNAT qui consiste à remplacer l'adresse IP et le port de destination,

la fonction SNAT qui consiste à remplacer l'adresse IP source.

Puisque cette fonction consiste à modifier les adresses de source et / ou de destination des trames IP qui transitent par le Routeur, il est important de préciser si le firewall traite des trames IP dont les adresses ont été déjà substituées ou non.

L'ordre dans lequel s'effectue la substitution modifie en effet la manière de configurer les règles du filtre principal du firewall. Les traitements de substitution s'effectuent comme suit :

Direction	
WAN vers le LAN	
LAN vers le WAN	

La fonction de substitution décrite ci-dessus (on dit aussi translation) est utile dans des cas très particuliers : Pour router des trames par un chemin de secours, par exemple, ou encore pour adapter un réseau ancien à un nouveau plan d'adresses IP (Mapping).

PARAMETRAGE

10.3.2 Configuration

Pour mettre en œuvre la fonction NAT avancée,

- Sélectionner le menu Configuration > Réseau > Routage > NAT avancé.

The screenshot shows the configuration interface of an etic router (IPL-A-400) in French. The breadcrumb trail is: Accueil > Configuration > Réseau > NAT avancé > Règle DNAT. The left sidebar contains a tree menu with categories like Configuration, Accès distant, Réseau, Sécurité, and Diagnostics. The main content area is titled 'Règle DNAT' and includes several sections: 'Champ adresse IP' with instructions on how to enter IP addresses or networks; 'Champs port' with instructions on how to enter port numbers or ranges; 'Champ Nouvelle destination' with instructions on how to enter the destination IP and port; an 'Active' checkbox which is checked; a 'Trame à modifier' section with input fields for 'Adresse IP source', 'Adresse IP destination', and a 'Protocole' dropdown menu set to 'Tous'; and a 'Translation' section with a 'Nouvelle adresse IP destination' input field. At the bottom, there are buttons for 'Enregistrer', 'Annuler', and 'Retour'.

Pour créer une règle de substitution d'adresse de destination (DNAT),

- Cliquer sur le bouton « Ajouter une règle ». La fenêtre de création s'affiche :
- Sélectionner Oui pour rendre la règle active.
- Saisir les critères de substitution :
 - Adr. IP source
 - Adr. IP destination
 - Protocole (TCP, UDP, ...)
 - Port source
 - Port destination
- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP et port de destination.

Pour créer une règle de substitution d'adresse source (SNAT),

- Cliquer sur le bouton « Ajouter ». La fenêtre de création d'une règle SNAT s'affiche :

The screenshot shows the web interface of an etic IPL-A-400 router. The browser address bar shows a URL starting with https://192.168.38.191:4433/. The interface has a green header with the etic logo and 'IPL-A-400' model name. A sidebar on the left contains a menu with categories like Configuration, Accès distant, Réseau, Sécurité, and Diagnostics. The main content area is titled 'Règle SNAT' and includes a breadcrumb trail: '> Accueil > Configuration > Réseau > NAT avancé > Règle SNAT'. There are buttons for 'Enregistrer' and 'Annuler', and a message 'Modifications sur la page non enregistrées'. The configuration fields include:

- Champ adresse IP:** A text input field with instructions: 'Laisser le champ vide pour que la règle s'applique à toutes les adresses IP. Saisir une adresse IP seule (ex 192.168.0.1) ou une adresse réseau (ex: 192.168.0.0/24 ou 192.168.0.0/255.255.0.0)'. There is an 'Active' checkbox checked.
- Champs port:** A text input field with instructions: 'Laisser le champ vide pour que la règle s'applique à tous les ports. Entrer un numéro sous la forme xx pour désigner un port unique (ex 80 pour HTTP). Entrer un numéro sous la forme xx.yy,...zz pour désigner un groupe de port (ex 21;80 pour spécifier FTP et HTTP). Entrer un numéro sous la forme xx-yy pour désigner une plage de port (ex: 80-90 pour désigner tous les ports entre 80 et 90)'.
- Champ Nouvelle source:** A text input field with instructions: 'Saisir une adresses IP seule (ex 192.168.10.1). Laisser le champ vide ou saisir "0.0.0.0" pour ne pas effectuer de translation (Null NAT)'.
- Trame à modifier:** A section with three input fields: 'Adresse IP source', 'Adresse IP destination', and 'Protocole' (with a dropdown menu currently showing 'Tous').
- Translation:** A section with one input field: 'Nouvelle adresse IP source'.

 At the bottom of the form are buttons for 'Enregistrer', 'Annuler', and 'Retour'.

- Sélectionner « Oui » pour rendre la règle active.
- Saisir les critères de substitution :
 - Adr. IP source
 - Adr. IP destination
 - Protocole (TCP, UDP, ...)
 - Port source
 - Port destination
- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP source.

11 Redondance VRRP

11.1 Principe

VRRP est un protocole qui permet à deux ou plusieurs routeurs sur un même réseau IP d'agir en redondance les uns des autres afin d'augmenter la disponibilité de la fonction de routeur.

Le mécanisme est le suivant : Les routeurs placés en redondance les uns des autres possèdent chacun une adresse IP, comme tout équipement d'un réseau IP ; mais ils possèdent aussi une adresse IP commune appelée adresse IP virtuelle.

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

De plus un indice de priorité (compris 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'indice de priorité le plus élevé ; par la suite, il annoncera 255 comme indice de priorité, tandis que les autres routeurs que l'on désignera comme routeur de secours resteront silencieux.

Le routeur maître prend en charge la fonction de routeur ; il répond aux requêtes ARP émises par les équipements du réseau.

De plus, il diffuse régulièrement un message de présence au moyen de l'adresse multicast 224.0.0.18 avec un numéro de protocole IP 112.

A défaut de recevoir le message, un nouveau routeur maître est élu.

Le Routeur gère ce protocole aussi bien sur l'interface LAN.

11.2 Configuration

Paramètres « Activer VRRP sur l'interface LAN » :

Cocher cette case pour activer VRRP sur l'interface LAN.

Paramètres « Identité VRRP (1-255) » :

Affecter un code d'identité au groupe de routeurs entre 1 et 255.

Tous les routeurs du même groupe doivent posséder le même code.

Deux groupes différents ne peuvent posséder le même code.

Paramètres « Adresse IP virtuelle » :

Enregistrer l'adresse IP virtuelle commune à tous les routeurs du groupe

Tous les routeurs agissant en redondance doivent posséder la même adresse IP virtuelle.

Paramètres « Indice de priorité VRRP (1-255) » :

Affecter un indice de priorité au routeur entre 1 et 255.

L'indice le plus élevé désigne le routeur le plus prioritaire.

Paramètres « adresse MAC virtuelle » :

On peut associer une adresse MAC virtuelle à l'adresse IP virtuelle.

De cette manière, lorsqu'un équipement du 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 du groupe VRRP codé en hexadécimal.

12 Publier l'adresse IP du routeur sur l'Internet

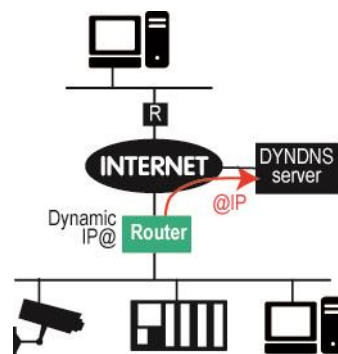
12.1 Principe

Si l'abonnement ADSL ne prévoit pas d'attribuer une adresse IP fixe au produit, mais une adresse IP « dynamique – c'est à dire qui change à chaque connexion ou de façon périodique - il peut être utile de la publier à chaque changement sur un serveur spécialisé tel que DynDNS ou NoIP.

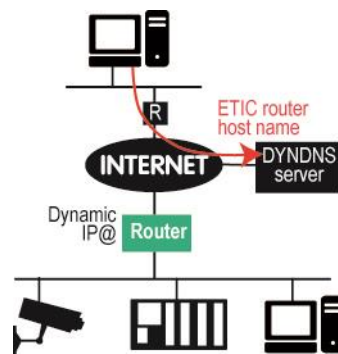
Grâce à ce type de serveur, un utilisateur pourra connecter son PC au produit en utilisant le nom de domaine dynamique attribué au Routeur (mon_routeur_etitelecom.dyndns.org, par exemple) au lieu de l'adresse IP inconnue.

Le procédé est le suivant :

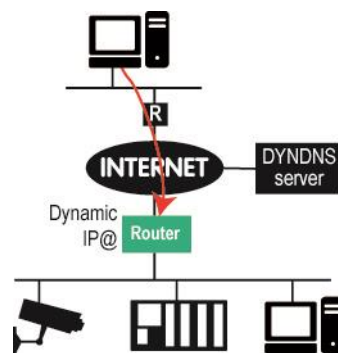
Chaque fois qu'il se connecte à l'Internet, le Routeur inscrit l'adresse IP provisoire qu'il reçoit sur l'Internet auprès du serveur DynDNS ou NoIP à l'emplacement qui lui est réservé (mon_routeur_etitelecom, dans notre exemple).



Chaque fois qu'il souhaite se connecter au produit, le PC ou le routeur distant transmet au serveur DYNDNS une requête visant à obtenir en retour l'adresse IP du Routeur possédant le nom de domaine « mon_routeur_etitelecom ».



Une fois qu'il a acquis l'adresse IP du Routeur, le PC distant peut établir la connexion à travers l'Internet.



12.2 Paramétrage

Etape 1 : Ouvrir un compte auprès de DynDNS ou NoIP.org pour réserver un nom de domaine dynamique.
C'est le nom que l'on attribue au routeur sur l'Internet (mon_routeur_etitelecom.dyndns.org, par exemple).

Etape 2 : Configurer le routeur

- Sélectionner le menu Configuration > Réseau > Routage > Dyndns.
- Cocher la case « Activer »

Paramètre « Fournisseur de service DNS » :

Choisir DynDNS ou NoIP

Paramètres « Identifiant du compte DNS dynamique » et « Mot de passe » :

Saisir l'identifiant et le mot de passe du compte ouvert chez le fournisseur de service de DNS dynamique.

Paramètres « Hostname» :

Saisir le nom de domaine enregistré chez le fournisseur ; par exemple « mon_routeur_etitelecom ».

13 Connexion distante

Pour offrir un service d'accès distant, il faut successivement effectuer les étapes suivantes :

- Etape 1 : Configurer la communication distante. PPTP ou OpenVPN ou L2TP décrite dans le présent paragraphe, ou bien encore une connexion HTTPS décrite au paragraphe suivant.
- Etape 2 : Enregistrer les utilisateurs autorisés dans la « liste d'utilisateurs » (voir paragraphe suivant).
- Etape 3 : Définir les droits d'accès de chaque utilisateur (voir paragraphe suivant).

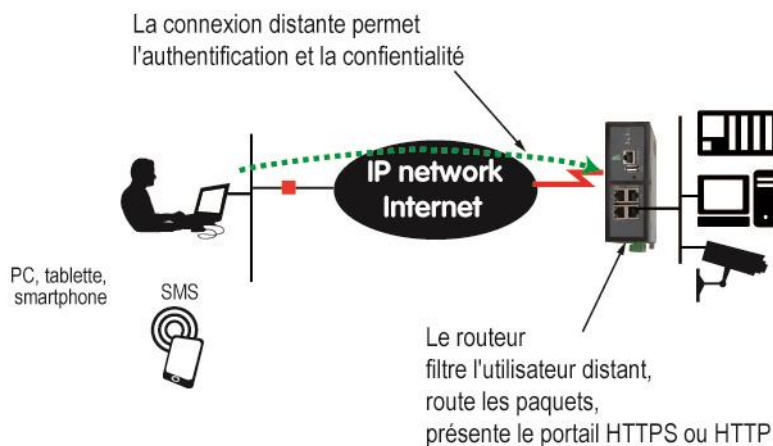
Le Routeur permet aux utilisateurs distants de se connecter à une machine, simplement et avec un niveau de sécurité élevé en établissant une connexion distante pour réaliser les opérations de télé-exploitation ou télémaintenance, par exemple.

Une fois identifié, l'utilisateur distant peut accéder aux différents équipements du réseau comme s'il était sur place.

Les données peuvent être chiffrées pour la confidentialité.

Le Routeur permet d'attribuer à chaque utilisateur des droits d'accès individualisés : Un utilisateur peut accéder à tel « équipement ou groupe d'équipements tandis qu'un autre peut accéder à d'autres équipements.

La fonction « portail » est destinée à la consultation des pages web d'automates ou de HMI ; elle permet à l'utilisateur d'un smartphone (ou d'une tablette, ou d'un PC) de consulter les serveurs web embarqués en procurant un niveau de sécurité adapté aux applications industrielles.



13.1 Avantages de la connexion distante

Une connexion distante établie depuis un PC, une tablette ou un smartphone procure les avantages suivants :

- **Identification des utilisateurs distants**

L'utilisateur distant est identifié au moyen d'un identificateur et d'un mot de passe ou bien encore d'un certificat.

L'utilisateur n'est autorisé que s'il a été enregistré dans la liste d'utilisateurs.

- **Connexion transparente**

S'il y est autorisé par ses droits d'accès, l'utilisateur peut accéder à chaque équipement du réseau distant.

- **Attribution automatique d'une adresse IP du réseau**

Le PC de l'utilisateur distant est téléporté sur le réseau local. Une fois identifié, son PC reçoit automatiquement une adresse IP du réseau local. Aucune intervention n'est nécessaire dans le PC de l'utilisateur distant.

- **Cryptage des échanges**

Les connexions distantes permettent de crypter les échanges pour assurer la confidentialité.

PARAMETRAGE

13.2 Types de connexions distantes

Quatre types de VPN sont proposés : OpenVPN., PPTP et L2TP/IPSec et HTTPS.

Les quatre types de connexion peuvent co-exister.

Pour paramétrer une connexion distante,

- Sélectionner le menu Configuration > Accès distant > moyen d'accès

The screenshot shows the web interface of an etic router (IPL-A-400) at the URL `https://192.168.38.191:4433/cgi?method=get_menu&menu=true&lang=fr`. The left sidebar contains a navigation menu with options like 'Accueil', 'Configuration', 'Interface WAN', 'Interface LAN', 'Accès distant', 'Liste des utilisateurs', 'Droits d'accès', 'Moyens d'accès', 'Réseau', 'Sécurité', 'Passerelles série', 'Alarms', 'Système', 'Diagnostics', 'Maintenance', and 'À propos'. The main content area is titled '> Accueil > Configuration > Accès distant > Moyens d'accès'. It features buttons for 'Enregistrer' and 'Annuler', and a note 'Modifications sur la page non enregistrées'. The configuration is organized into sections: 'Proxy HTTPS' (with 'Activer le proxy HTTPS' checked), 'Propriétés L2TP/IPsec' (with 'Activer L2TP/IPsec' checked, encryption set to 3DES, hashing to MD5, and pre-shared key authentication), 'Propriétés OpenVPN' (with 'Activer OpenVPN (OpenVPN)' checked, port 1194, UDP protocol, and Login/Mot de passe authentication), 'Propriétés OpenVPN (Accès Smartphone)' (with 'Activer OpenVPN (OpenVPN) pour Smartphones' unchecked), 'Propriétés PPTP' (with 'Activer PPTP' checked), and 'Remapping IP' (with 'Traduire les adresses IP du réseau LAN' checked and a field for the target LAN address). Authentication protocols for L2TP/IPsec, OpenVPN, and PPTP are listed with checkboxes: PAP, CHAP, MS-CHAP, and MS-CHAP v2.

13.3 Paramétrage d'une connexion distante de type OpenVPN

Une connexion distante OpenVPN établie entre un PC distant et un réseau Ethernet garantit un niveau élevé de sécurité : Authentification, chiffrement, intégrité des données.

Le logiciel M2Me_Secure s'installe sur le PC distant pour constituer une interface de connexion simple et puissante.

Il est aussi possible de paramétrer dans le PC une connexion de type « client OpenVPN ».

Configuration du Routeur

- Sélectionner la case à cocher OpenVPN

Paramètres « Numéro de port » et « protocoles » :

Choisir le protocole de transport du VPN (UDP ou TCP) ; UDP est préférable à TCP.

Le N° de port peut être quelconque mais la valeur doit être choisie parmi celles qui sont autorisés sur le réseau du client.

Attention : Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour les connexions d'utilisateurs distants TLS.

Paramètres « Authentification des utilisateurs » :

Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « Login / mot de passe et certificat numérique », la sécurité est renforcée. Le PC distant est authentifié au moyen du certificat enregistré dans le PC et l'utilisateur est identifié au moyen du login et du mot de passe.

Note : dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le Routeur, dans la fiche de l'utilisateur.

Paramètres « Algorithme de chiffrement » et « Algorithme de hachage » :

Laisser les valeurs par défaut Blowfish et MD5.

Configuration du logiciel M2Me_Secure du PC

- Cliquer l'icône « Menu » puis « Nouveau site ». La fenêtre de paramétrage du site apparaît.
- Sélectionner l'onglet « Général », saisir le nom du site.
- Sélectionner l'onglet « Connexion » ; cocher la case « Ce site est accessible par Internet ».
- Dans le champ « Nom d'hôte ou adresse IP », saisir l'adresse IP permettant d'atteindre le routeur ETIC.
- Sélectionner l'onglet « Avancé » ; Choisir le protocole (UDP ou TCP), le N° du port et les algorithmes de cryptage et hachage.

Attention : Ces paramètres doivent avoir la même valeur que ceux sélectionnés dans le routeur ETIC.

PARAMETRAGE

13.4 Paramétrage d'une connexion OpenVPN pour smartphone

Il est possible de distinguer l'accès VPN destiné aux PC (voir paragraphe précédent de l'accès destiné aux smartphones.

Cette connexion est de type identique à la connexion OpenVPN du paragraphe précédent mais on la distingue par le N° de port de destination.

- Sélectionner la case à cocher OpenVPN pour smartphone

Paramètres « Numéro de port » et « protocoles » :

Choisir le protocole de transport du VPN (UDP ou TCP) ; UDP est préférable à TCP.

Le N° de port peut être quelconque mais la valeur doit être choisie parmi celles qui sont autorisées sur le réseau du client.

Attention : Le numéro de port utilisé pour l'interconnexion de routeurs par VPN doit être différent du N° de port utilisé pour les connexions d'utilisateurs distants OpenVPN.

Paramètres « Authentification des utilisateurs » :

Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « Login / mot de passe et certificat numérique », la sécurité est renforcée. Le PC distant est authentifié au moyen du certificat enregistré dans le PC et l'utilisateur est identifié au moyen du login et du mot de passe.

Note : dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le routeur ETIC, dans la fiche de l'utilisateur.

Paramètres « Algorithme de chiffrement » et « Algorithme de hachage » :

Laisser les valeurs par défaut Blowfish et MD5.

13.5 Paramétrage d'une connexion distante de type PPTP

Configurer le routeur

- Sélectionner la case à cocher PPTP

Sélectionner le choix PPTP.

Configurer la connexion PPTP dans le PC

Voir procédure en annexe 2.

13.6 Paramétrage d'une connexion distante de type L2TP / IPSec

- Sélectionner la case à cocher L2TP / IPSec

Paramètres « Algorithme de chiffrement » et « Algorithme de hachage » :

Laisser les valeurs par défaut Blowfish et MD5.

Paramètres « Authentification des utilisateurs » :

Si l'on choisit la valeur « Login / mot de passe », l'authentification est réalisée à l'aide de ces deux codes uniquement.

Si l'on choisit la valeur « certificat numérique », le PC distant est authentifié au moyen du certificat enregistré dans le PC distant.

Note : Dans ce cas, le nom du certificat du PC de l'utilisateur devra être enregistré dans le routeur ETIC, dans la fiche de l'utilisateur.

Paramètres « Valeur clé » :

Saisir la valeur de la clé partagée qui authentifie l'utilisateur distant.

14 Portail sécurisé (HTTPS) pour smartphone, tablette ou PC

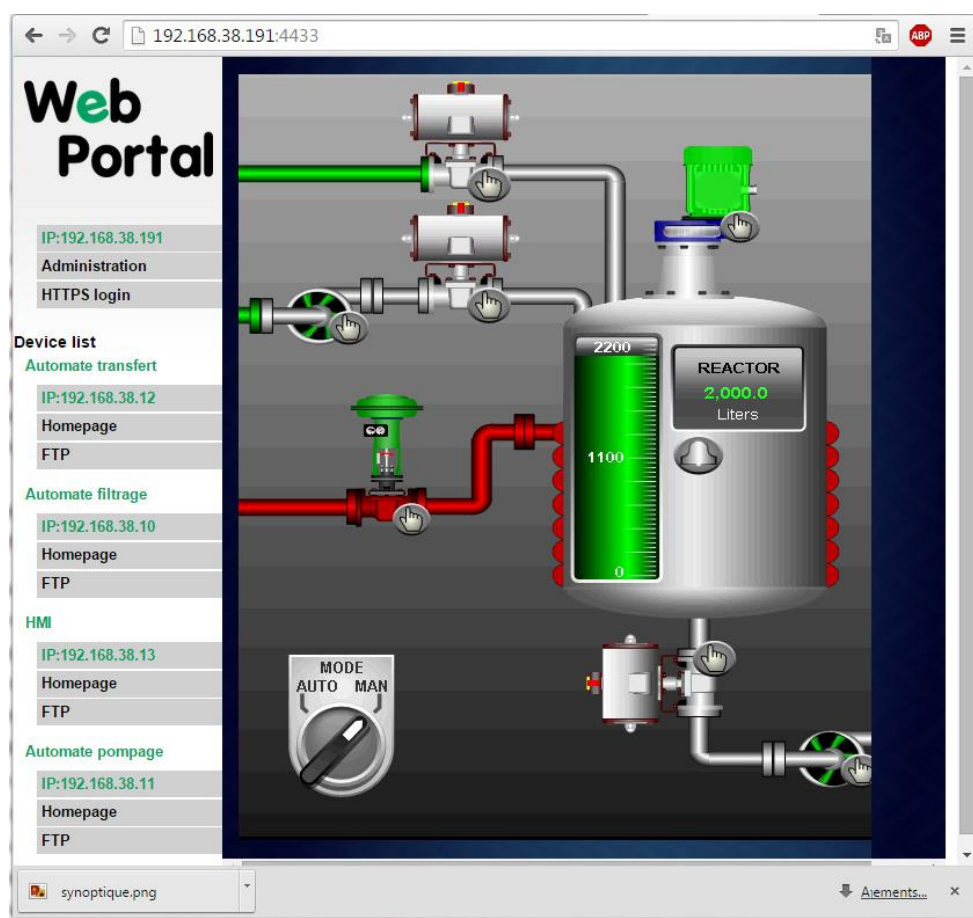
14.1 Présentation

Le portail sécurisé est une page web affichée par le routeur ETIC lorsqu'un utilisateur distant se connecte au routeur au moyen d'un simple navigateur en mode sécurisé HTTPS.

La page « Portail » affiche la liste des équipements accessibles à l'utilisateur selon ses droits d'accès.

Il suffit de cliquer sur l'équipement souhaité et les pages web du serveur web embarquées dans cet équipement s'affichent.

Conjuguée à une alarme SMS ou email, le portail web est particulièrement adapté à la télé-exploitation au moyen de smartphone.



14.2 Configuration

Pour activer la fonction portail web HTTPS et y donner accès par le réseau LAN,

- Sélectionner le menu Configuration > Accès distant > Moyen d'accès
- Cocher la case « Activer le proxy HTTPS ».

Pour y donner en plus accès par l'Internet (WAN),

- Sélectionner le menu Configuration > Sécurité > Droits d'administration
- Cocher la case « Utiliser HTTPS pour la configuration »
- Cocher la case « Activer l'accès par le WAN ».

Note importante :

Lorsque le portail HTTPS est activé, le serveur de configuration du Routeur est remplacé par le portail web ; Cependant, le serveur de configuration reste accessible mais, il faut préciser le N° de port :

Accès	Par l'Internet	Par le LAN
Portail Web HTTPS :	https://adr. IP Internet	https://adr. IP LAN
Serveur de configuration HTTPS du routeur	https://adr. IP Internet : 4433 ou adr. IP Internet :8080 avec login et PWD	https://adr. IP LAN : 4433 ou adr. IP LAN :8080 avec login et PWD

14.3 Accéder au portail HTTPS par l'Internet

Pour accéder au portail web HTTPS par l'Internet,

- Lancer le navigateur
- Entrer l'adresse publique Internet du routeur : [https : //](https://) « [adresse](https://) IP Internet du routeur »
- Saisir le nom et le mot de passe d'un utilisateur enregistré dans la liste d'utilisateurs.

La page d'accueil du portail HTTPS s'affiche ; elle n'affiche que les équipements autorisés à l'utilisateur.

15 M2Me_Connect pour la prise en main de machine à distance

Le service M2Me_Connect est disponible en standard sur les produits RAS et est une option pour les autres Routeurs qu'il faut commander séparément.

Référence de l'option : M2Me_pack_initial

15.1 Présentation

Principe

Il arrive fréquemment que la connexion entre le PC et le routeur sur l'Internet ne soit pas possible parce que ni le PC ni le routeur ne disposent d'adresses IP publiques, ou bien faute de pouvoir régler le routeur d'entreprise ou bien faute d'autorisation.

Le service M2Me_Connect permet de résoudre la difficulté : Grâce à M2Me_Connect, le PC se connecte à la machine, pour une opération de maintenance par exemple, même si, ni le PC ni le routeur ne possèdent d'adresse publique.

Fonctionnement

L'utilisateur du PC enregistre dans son logiciel M2Me_Secure le nom du certificat d'authentification du Routeur.

Lorsque l'utilisateur ouvre son logiciel M2Me_Secure, son PC établit automatiquement une connexion sécurisée vers le service M2Me_Connect. Il s'authentifie sur le service.

De son côté, le Routeur fait de même dès qu'il est sous tension.

Une fois connectés au service, et après authentification réciproque, le PC et le Routeur établissent un VPN de bout en bout.

15.2 Paramétrage d'une connexion au service M2Me_Connect

Pour paramétrer la connexion au service M2Me_Connect, il suffit de paramétrer le VPN établi depuis le Routeur vers le service M2Me_Connect ainsi que le VPN établi depuis le PC vers le service M2Me_Connect.

Chacun de ces VPN peut être supporté soit par le protocole UDP soit par le protocole TCP.

L'utilisation du protocole UDP plutôt que TCP est recommandée.

Etape 1 : Paramétrage du Routeur

- Sélectionner le menu Configuration > Accès distant > M2Me_Connect

Paramètre « Activer » :

Cocher la case pour activer la connexion au service M2Me_Connect.

Paramètres « Port TCP et paramètres « Port UDP » :

Cocher tous les ports UDP ou TCP que le Routeur peut tester afin de tenter d'établir la connexion vers le service M2Me_Connect.

Si un port UDP ou TCP unique a été autorisé, cocher la case correspondante ou bien saisir la valeur de ce N° de port TCP ou UDP.

Note : L'utilisation du protocole UDP est préférable à TCP.

- Si un serveur proxy filtre les connexions sortantes, décocher la case « Accès à Internet (pas de proxy » et saisir les paramètres de ce serveur :

Paramètre « Serveur proxy » :

Type (http ou SOCKS5),

Adresses et N° de port,

Authentification Login et mot de passe à fournir pour s'y présenter (éventuellement).

Attention : « La clé de produit » que l'on trouve dans le menu « A propos » doit être copiée afin d'être reporté dans le logiciel M2Medu PC de télémaintenance. C'est en effet cette clé qui autorise l'accès à la machine.

- Tester la connexion

Pour commander la connexion du routeur au service M2Me_Connect, cliquer le bouton « Connecter maintenant ».

Pour vérifier que la connexion s'effectue normalement, sélectionner le menu « Diagnostic » puis « Etat réseau » puis « M2Me ».

Lorsque la connexion aboutit, le message « Connecté » s'affiche dans le champ « Etat » ainsi que le N° de port et le protocole utilisé.

Etape 2 : Paramétrage du logiciel M2Me_Secure du PC distant

- Ouvrir le logiciel M2Me_Secure et saisir l'identificateur et le mot de passe de l'utilisateur (c'est celui qui sera ensuite contrôlé par le Routeur pour identifier l'utilisateur du PC).

PARAMETRAGE

- Pour créer la connexion avec le site du routeur, cliquer l'icône « Menu » puis « Nouveau site ».
- Sélectionner l'onglet « Général », et saisir le nom du site du Routeur (ce libellé n'a qu'un rôle mnémonique).
- Sélectionner l'onglet « Connexion » ; cocher les cases « Ce site est accessible par Internet » et « Ce site est visible à travers le service M2Me ».
- Saisir le code appelé « Product key » ; on le trouve dans le menu « A propos » du Routeur.
Il s'agit du résumé du certificat d'authentification enregistré dans le Routeur en usine; il permet au PC de s'adresser au Routeur lorsque l'un et l'autre sont connectés au service M2Me_Connect.
Le mot de passe doit être gardé secret par chaque utilisateur ; il n'apparaît jamais en clair.

Paramètre « e-mail » :

Il sera utilisé par le Routeur soit pour transmettre un e-mail d'alarme à la suite du passage en défaut de l'entrée TOR, soit lorsque l'utilisateur souhaite se connecter par l'Internet ; dans ce cas, l'adresse IP publique du Routeur peut lui être transmise par e-mail.

Paramètre « Filtre pare-feu » :

Un filtre est un ensemble de règles de sécurité limitant l'accès aux machines et services raccordées derrière le routeur. Un filtre peut être appliqué pour un ou plusieurs utilisateurs ce qui permet de différencier les droits d'accès aux machines en fonction de qui se connecte. Par défaut, rien n'est filtré.

Paramètre «Certificat » :

Ce paramètre n'apparaît que si l'on a choisi un VPN L2TP/IPSec ou TLS/SSL avec authentification par Certificat numérique. Il décrit les champs du certificat qui doivent être contrôlés par le Routeur.

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 191 (0xbf)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=FR, ST=Isere, L=Meylan, O=ETIC Telecommunications, OU=Security,

CN=ETIC_Telecom_CA/emailAddress=Security@etictelecom.com

Validity

Not Before: Nov 22 14:46:58 2007 GMT

Not After : Nov 14 14:46:58 2037 GMT

Subject: C=FR, ST=Isere, L=Meylan, O=ETIC Telecommunications, OU=Security, CN=b4b4d3c9-b200-4869-8637-

edb3d421d55a/emailAddress=b4b4d3c9-b200-4869-8637-edb3d421d55a@etictelecom.com

Subject Public Key Info:

16 Enregistrer les utilisateurs distants autorisés

16.1 Présentation

La liste d'utilisateurs du Routeur enregistre l'identité de chaque utilisateur distant autorisé à se connecter ainsi que ses paramètres (email...) et ses droits d'accès aux machines du réseau local définis dans le firewall.

Pour accéder à la liste d'utilisateurs,

- Sélectionner le menu « Configuration > Accès distant > Liste d'utilisateurs

The screenshot shows the ETIC router configuration interface in a web browser. The URL is `https://192.168.38.191:4433/cgi?method=get_menu&menu=true&lang=fr`. The page title is "IPL-A-400" and the user is logged in as "site". The breadcrumb trail is "> Accueil > Configuration > Accès distant > Liste des utilisateurs".

On the left is a navigation menu with the following items:

- Accueil
- Configuration
 - Interface WAN
 - Interface LAN
 - Accès distant
 - Liste des utilisateurs
 - Droits d'accès
 - Moyens d'accès
 - Réseau
 - Connexions VPN
 - Routing
 - Redondance VRRP
 - Redirection de port
 - NAT avancé
 - DynDNS
 - QoS - DiffServ
 - Sécurité
 - Pare-feu
 - Droits d'administration
 - Certificats X509
 - Passerelles série
 - Alarmes
 - Système
 - Diagnostics
 - Maintenance
 - À propos

The main content area shows the "Liste des certificats autorisés" section with buttons: Afficher, Modifier, Supprimer, Ajouter..., Copier et modifier, and navigation arrows. Below it is the "Liste des utilisateurs" section with a table:

	Actif	Nom complet	Adresse E-mail	Entreprise	Numéro de téléphone
☒	Oui	renaud	renaudi@etictelecom.com	ETIC TELECOM	+336736870
☒	Oui	Martin	martin@etictelecom.com	ETIC TELECOM	
☒	Oui	simon	simon@etictelecom.com	ETIC TELECOM	067368740
☒	Oui	Jane	jane@etictelecom.com	ETIC TELECOM	

Below the table are buttons: Afficher, Modifier, Supprimer, Ajouter..., Copier et modifier, and navigation arrows.

Note :

A la livraison, pour des raisons de sécurité, aucun utilisateur n'est enregistré.

PARAMETRAGE

16.2 Définir des utilisateurs

- Cliquer sur le bouton « Ajouter » ; la fiche utilisateur est affichée.

The screenshot shows the 'Configuration Utilisateur' page in the ETIC Telecom web interface. The page has a sidebar on the left with navigation links: Accueil, Configuration (Interface WAN, Interface LAN, Accès distant, Liste des utilisateurs, Droits d'accès, Moyens d'accès), Réseau (Connexions VPN, Routage, Redondance VRRP, NAT avancé, DynDNS, CoS - DiffServ), Sécurité (Passerelles série, Alarmes, Système), Diagnostics, Maintenance, and À propos. The main content area shows the 'Liste des utilisateurs' page with a table of users. The 'Actif' checkbox is checked. The 'Mot de passe' field is masked with asterisks. The 'Force du mot de passe' is indicated as 'moyen'. The page also includes a top navigation bar with the ETIC Telecom logo and a 'site' link.

Case à cocher « Actif » :

Elle permet de retirer temporairement un utilisateur de la liste.

Paramètre « Nom complet » :

C'est le libellé qui apparaît dans le premier champ de la liste des utilisateurs autorisés. Il permet en particulier de garder la trace de chaque connexion de l'utilisateur dans le journal.

Paramètres « Email » et « N° de téléphone » :

L'adresse mail permet l'émission d'un email d'alarme.

Remarque : le champ N° de téléphone est réservé pour des usages ultérieurs.

Paramètres « Nom d'utilisateur » et « mot de passe » :

Ce sont deux codes différents attribués à chaque utilisateur. Lorsqu'il se connecte à distance, il doit saisir ces deux codes dans les champs correspondants de la fenêtre de CONNEXION DISTANTE.

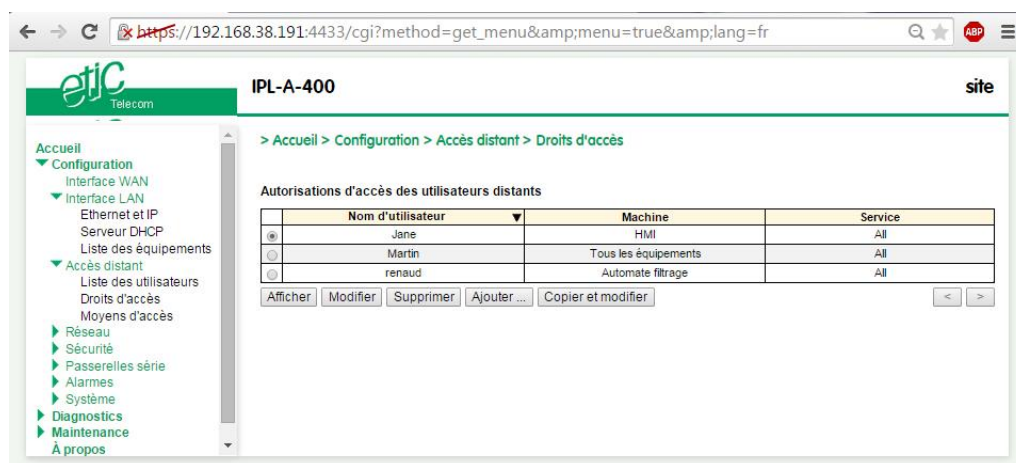
17 Définir les droits d'accès des utilisateurs

Il est possible de définir les équipements auxquels chaque utilisateur peut accéder.

Au préalable, il faut définir la liste des machines du réseau qui sont accessibles à distance (voir menu Interface LAN > Liste des équipements).

Pour définir les droits d'accès d'un utilisateur

- Sélectionner le menu Configuration > Droits d'accès, le tableau des droits s'affiche.



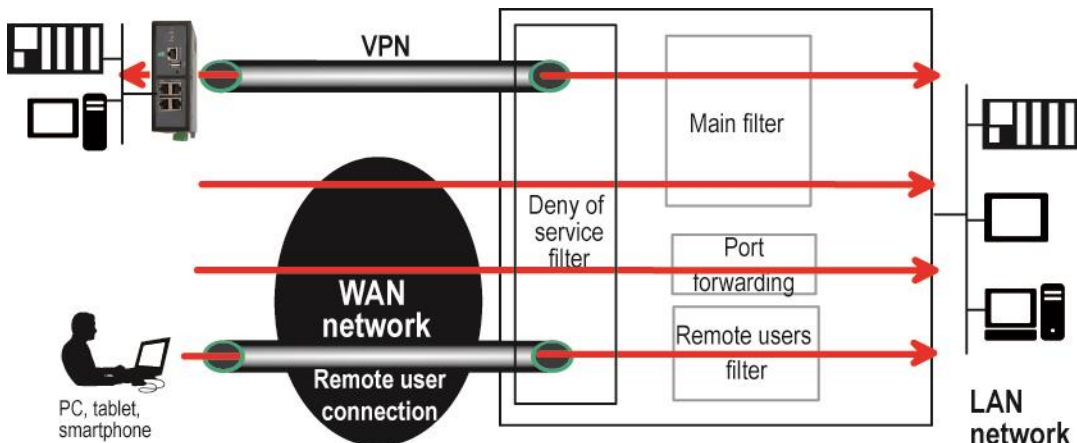
- Cliquer le bouton « Ajouter » ; puis sélectionner un utilisateur dans la liste puis lui attribuer un équipement dans la liste pour autoriser l'accès à cet équipement.

18 Configuration du pare-feu

18.1 Présentation du pare-feu

Le pare-feu a pour but de filtrer les échanges de trames IP entre l'interface WAN et l'interface LAN pour protéger les équipements connectés au réseau LAN.

Sa structure est résumée ci-dessous :



Il comporte trois parties :

- **Le filtre principal (main filter)**

Il filtre les trames IP en fonction de l'adresse IP et du port source et de l'adresse IP et du port destination.

Ce filtrage s'applique aux trames véhiculées dans les VPN ou hors des VPN.

Pour une meilleure organisation, il comporte deux filtres séparés :

Le filtre qui agit sur les trames IP véhiculées dans les VPN

Le filtre qui agit sur les trames IP véhiculées hors des VPN

Le filtre principal agit sur toutes les trames sauf celles qui sont véhiculées dans les connexions d'utilisateurs distants qui sont traitées par le filtre d'utilisateurs distants (voir ci-dessous).

Pour distinguer une connexion d'utilisateur distant de type OpenVPN d'un tunnel OpenVPN établi entre routeurs, le routeur détecte le N° de port : Si le N° de port détecté est le N° déclaré pour une connexion d'utilisateurs distants), le filtre des connexion d'utilisateurs s'appliquera et pas le filtre principal..

Notes :

On veillera donc à choisir un N° de port différent pour les connexions OpenVPN d'Utilisateur distant et les connexions OpenVPN entre routeurs.

La fonction dite de redirection de port qui renvoie le trafic destiné au Routeur sur l'interface WAN (Internet) vers une adresse IP particulière de l'interface LAN sur le critère de N° de port, n'est pas soumise au filtre principal.

- **Le filtre «Utilisateurs distant » (remote users filter)**

Ils permettent d'autoriser ou d'interdire l'accès à chaque équipement connecté à l'interface LAN en fonction de l'identité de l'utilisateur distant (Login et mot de passe et éventuellement certificat) lorsqu'il se connecte au moyen de la connexion distante PPTP OpenVPN ou L2TP/IPSec..

Par exemple, on peut attribuer à l'utilisateur de login « admin » et de mot de passe « admin » un filtre bloquant toutes les trames issues de son PC sauf celle qui sont adressées à un équipement particulier de l'interface LAN.

Note :

La configuration de ce filtre est réalisée dans le menu Configuration > Accès distant > Droits d'accès

- **Le filtre de « déni de Service »**

Le filtre de déni de service (DoS) protège les équipements de l'interface LAN contre les attaques par saturation pouvant provenir de l'interface WAN : Ping de la mort, SYN flood

Ce filtre est prédéfini et n'est pas configurable par l'utilisateur. Il toujours opérationnel sur l'interface WAN.

18.2 Filtre principal

18.2.1 Présentation

- **Organisation**

Le filtre principal comporte deux parties

La première partie est intitulée « **Règles pour le trafic WAN** »

Elle a pour but de définir le filtrage à apporter aux trames IP non transportées dans un VPN.

Elle définit la politique par défaut et le tableau de règles de filtrage.

Chaque ligne du tableau est une règle de filtrage qui autorise ou interdit un type de trames IP.

La seconde partie est intitulée « **Règles pour le trafic VPN** »

Elle a pour but de définir le filtrage à apporter aux trames IP transportées dans un VPN.

Elle a la même forme que la première partie.

- **Politique par défaut :**

C'est l'action qui sera appliquée à une trame qui n'est conforme à aucune règles du tableau.

On considère séparément les deux directions de trafic car on peut souhaiter que la décision prise soit différente selon qu'un paquet provient du LAN ou du WAN.

On peut souhaiter, par exemple que la politique par défaut interdise le routage « WAN vers LAN » mais autorise le routage « LAN vers WAN ».

La politique par défaut prudente consiste à interdire le trafic WAN vers LAN et éventuellement LAN vers WAN ; de cette façon, toute trame qui ne se conforme pas à l'une des règles du filtre est bloquée.

En effet, supposons que la politique par défaut consiste à autoriser le trafic WAN vers LAN ; alors tout flux IP qui ne serait conforme à aucune des règles du filtre principal, serait routée vers le LAN.

- **Tableau de règles de filtrage**

Chaque ligne est une règle de filtrage.

PARAMETRAGE

Chaque règle définit une action (autoriser ou interdire) associée à un flux IP défini par les différents champs de la ligne de règle :

- Direction (« LAN vers WAN » ou « WAN vers LAN »),
- protocole (TCP, UDP...),
- @IP et port source
- @IP et port destination

Voici un exemple de filtre qui autorise deux équipements du réseau WAN (192.168.2.X) à accéder à un équipement particulier du réseau LAN. Tout autre flux du WAN vers le LAN est interdit.

Politique par défaut : LAN -> WAN : Autoriser - WAN -> LAN : interdire						
Direction	Action	Protocole	@ IP source	port source	@IP destination	port dest
WAN->LAN	Autoriser	any	192.168.2.1	any	192.168.1.12	any
WAN->LAN	Autoriser	TCP	192.168.2.2	any	192.168.1.12	502

● Fonctionnement

Lorsque le firewall reçoit une trame IP véhiculée dans le VPN, il applique la politique et les règles du filtre « Trafic VPN ».

Lorsque le firewall reçoit une trame IP véhiculée hors du VPN, il applique la politique et les règles du filtre « Trafic WAN ».

Il vérifie successivement la conformité aux règles de filtrage.

Si la trame n'est pas conforme à la première règle, elle est soumise à la suivante et ainsi de suite.

Dès qu'elle est conforme à une règle du tableau, le firewall lui applique l'action associée (autoriser ou interdire).

Si la trame n'est conforme à aucune règle, la politique par défaut lui est appliquée (autoriser ou interdire).

Note :

A la livraison, le filtre principal est réglé de la façon suivante :

Le trafic véhiculé dans les VPN est autorisé sans restriction.

Le trafic véhiculé hors des VPNs est limité :

- Le trafic à l'initiative d'un équipement du LAN vers le WAN est autorisé.

- Le trafic à l'initiative d'un équipement du WAN vers le LAN est interdit

Fonctions avancées

19 Ajouter un certificat

Pour établir un tunnel VPN, le Routeur peut s'authentifier au moyen de certificat. Cette solution procure un niveau élevé de sécurité.

Le routeur est livré avec un certificat X509 au format PKC#12 délivré par ETIC TELECOM ; cependant, il est possible d'ajouter un ou plusieurs autres certificats qui pourront être sélectionnés à la place du certificat initial.

Ces certificats peuvent être introduits soit en format PKCS#12 avec mot de passe ou en en format PEM.

Un seul certificat peut être actif à la fois.

Attention : les certificats du routeur client VPN et du routeur serveur VPN doivent avoir été délivrés par la même autorité de certification.

Pour ajouter un certificat,

- Sélectionner Configuration > Sécurité > Certificats.
- Cliquer le bouton ajouter.
- Sélectionner le type de certificat (PKC#12 ou PEM).
- Sélectionner le certificat actif parmi la liste des certificats enregistrés.

20 Alarmes

20.1 Transmettre un email ou un SMS

Tous les modèles de Routeurs permettent de transmettre un email sur l'un des événements suivants :

Ouverture de l'entrée tout ou rien.
Fermeture de l'entrée tout ou rien.
Ouverture ou la fermeture de l'entrée tout ou rien.
Connexion / déconnexion VPN.

L'IPL-EC ou RAS-CW permet au choix de transmettre un SMS ou un email.

- Sélectionner le menu Configuration > Alarmes > SMS / Email

Paramètre « Activer l'alarme par email » :

Si cette case est cochée, une alarme par e-mail est émise lorsque l'entrée TOR N° 1 change d'état.

Paramètre « Source de l'alarme » :

Ce paramètre permet de déterminer le ou les changements d'état qui provoquent l'alarme :

Passage à l'état fermé de l'entrée TOR
Passage à l'état ouvert de l'entrée TOR
Passage à l'état fermé ou ouvert de l'entrée TOR
VPN connecté ou déconnecté

Paramètre « Adresse d'expédition de l'alarme » :

Entrer l'adresse mail d'expédition de l'alarme.

Paramètre « Adresse du destinataire de l'alarme » :

Entrer l'adresse mail du destinataire du mail ou bien le N° du téléphone mobile (s'il s'agit d'un SMS).

Paramètre « Objet » :

Entrer l'objet du mail ; par exemple « Alarme site de Grenoble ».

Paramètre « Texte à envoyer » :

Entrer le texte du mail de l'email ou du SMS d'alarme.

Paragraphe Serveur SMTP

Paramètre « Utiliser le service M2Me pour envoyer les emails » :

ETIC TELECOM entretient un serveur SMTP (mails sortants) qui peut être utilisé par les routeurs ETIC.
Ce service permet aux routeurs ETIC d'envoyer des mails sans configuration spécifique.

Cocher cette case pour envoyer des mails sans autre configuration du Routeur ; autrement, saisir le nom du serveur SMTP à utiliser ainsi que le N° de port et le choix du niveau de sécurité.

20.2 Alarmes SNMP

Le Routeur dispose d'un agent SNMP qui supporte la MIB-II standard et l'envoi de TRAP sous certaines conditions.

Pour enregistrer les paramètres de fonctionnement du gestionnaire SNMP vers lequel les traps doivent être transmis,

- Sélectionner Configuration > Système.

Case à cocher « Activer » :

Si cette case est cochée l'agent SNMP est lancé.

Paramètre « Adresse IP du premier gestionnaire SNMP » :

Ce paramètre enregistre l'adresse IP du gestionnaire SNMP vers lequel les TRAP SNMP doivent être envoyés.

Paramètre « Adresse IP du second gestionnaire SNMP » :

Les traps SNMP peuvent être transmis vers un second serveur SNMP.
Ce paramètre enregistre l'adresse IP de ce second serveur.

Paramètre « version du protocole SNMP » :

Choisir dans la liste la version du protocole SNMP à utiliser.

Paramètre « Nom de communauté » :

C'est nom partagé entre chaque agent et le manager SNMP.
L'agent SNMP ne répond qu'aux requêtes d'un manager qui s'identifie par ce nom.

Paramètres « Nom du système » et « Localisation du système » :

Ces deux paramètres permettent au gestionnaire SNMP d'identifier l'origine des traps.
Saisir les chaînes de caractères qui identifieront le routeur ; leur valeur est au choix.

Case à cocher « Surveiller le statut du backup OpenVPN » :

Le serveur VPN peut surveiller via SNMP l'état des VPN principaux et backup de ses clients.
Il utilise ces données pour afficher un tableau récapitulatif dans la page diag/openvpn.

21 Passerelles série IP

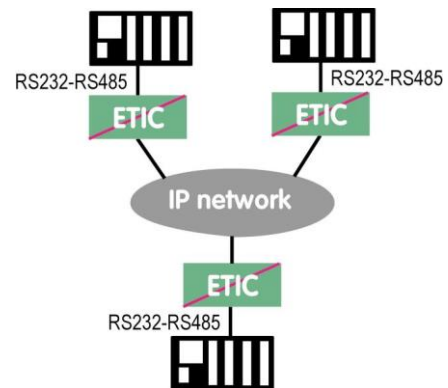
21.1 Présentation des types de passerelles

Certains modèles de Routeur comportent 2 liaisons série : Soit 2 RS232, soit 1 RS232 et 1 RS485, soit 1 RS422 isolée ou 1 RS485 isolée.

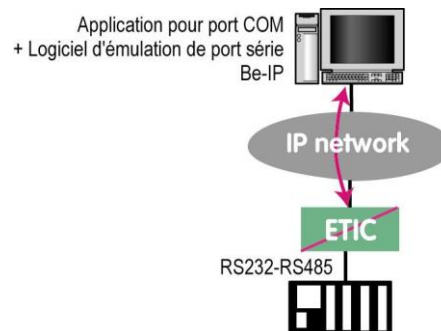
Une passerelle peut être affectée à chaque liaison série.

Chaque passerelle série permet d'utiliser un réseau IP pour faire communiquer des équipements série entre eux ou bien avec des équipements IP.

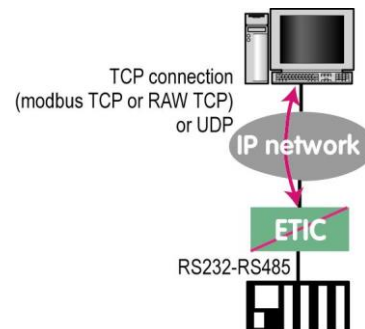
- Communication entre équipements à interface série



- Communication avec une application sur PC en utilisant un logiciel d'émulation de port COM



- Communication avec application sur PC capable d'empaqueter un protocole série dans UDP ou TCP (Modbus TCP par exemple)



Pour réaliser les fonctions décrites ci-dessus et s'adapter aux différentes situations qu'il est possible de rencontrer différents types de passerelles sont proposées.

21.2 Passerelle Modbus

La passerelle Modbus permet de connecter des équipements série RS232-RS485 esclaves ou maître à un ou plusieurs équipements Modbus TCP (clients ou serveurs selon le cas) connectés au réseau IP.

21.2.1 Définitions

Un client TCP Modbus est un équipement connecté au réseau IP et capable de transmettre une requête Modbus (= question ; par ex. demande de lecture ou d'écriture) à un autre équipement du réseau appelé serveur TCP MODBUS qui lui répondra.

Le client est l'équivalent d'un maître Modbus, mais plusieurs clients peuvent poser des questions au même serveur.

Un serveur TCP Modbus est un équipement connecté au réseau IP et capable de répondre à une requête Modbus posée par un autre équipement du réseau appelé client TCP MODBUS.

Le serveur est l'équivalent d'un esclave Modbus ; mais un serveur peut répondre à plusieurs clients.

Un maître Modbus est un équipement connecté à la liaison série RS232 ou RS485 et capable de poser une requête Modbus à un autre équipement du réseau appelé esclave MODBUS.

Un esclave Modbus est un équipement connecté à la liaison série RS232 ou RS485 et capable de poser une question Modbus à un autre équipement du réseau qui est appelé esclave MODBUS.

Adresse Modbus : Elle code entre 0 et 255 le destinataire d'une requête Modbus adressée à un serveur Modbus (réseau IP) ou à un esclave Modbus (liaison série).

Attention : Ne pas confondre adresse Modbus et adresse IP.

Pour plus de concision le mot « adresse » est souvent remplacé par le signe @ dans la suite du texte.

21.2.2 Choix de la passerelle Client ou de la passerelle Serveur

Pour connecter des équipements « série » esclaves Modbus à un ou plusieurs équipements TCP Modbus client, on utilisera la passerelle « Modbus serveur ».

Pour connecter un équipement « série » maître Modbus à un ou plusieurs équipements TCP Modbus serveur, on utilisera la passerelle « Modbus client ».

21.2.3 Affectation d'une passerelle Modbus à un port série

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

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

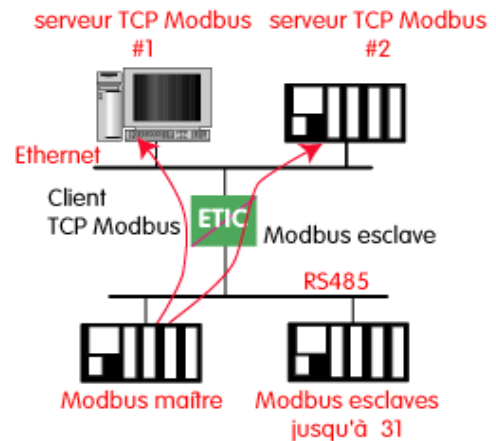
PARAMETRAGE

21.2.4 Passerelle Modbus client

La passerelle Modbus client permet la connexion d'un maître Modbus sur la liaison série du produit.

Plusieurs serveurs TCP Modbus peuvent être adressés sur le réseau IP.

D'autres esclaves peuvent être connectés à la liaison série.

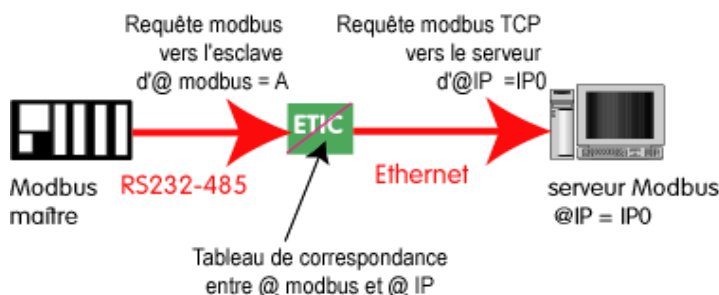


Principe de la passerelle Modbus Client :

Pour adresser un serveur TCP Modbus sur le réseau IP, on configure une table de correspondance entre une adresse Modbus esclave et une adresse IP ; ainsi, lorsque le maître Modbus transmet une requête à destination de l'esclave d'adresse Modbus A, le tableau de correspondance permet de transmettre cette requête à l'adresse IP correspondant à l'adresse A.

De plus, le champ adresse Modbus de la trame Modbus TCP prend la valeur A.

Le tableau de correspondance peut comporter 32 lignes permettant ainsi à un maître Modbus d'adresser 32 serveurs sur le réseau IP.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Modbus > Client Modbus**.
- Cocher la case **Activer le client Modbus**.

Port COM

Choisir la liaison série 1 ou 2 du produit.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Protocole Modbus

Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

Temps inter-caractères

Fixe le temps maximum admissible entre caractères des réponses de l'esclave Modbus.

Timeout d'inactivité sur TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de requêtes Modbus reçues du réseau IP.

Port TCP

Fixe le N° du port TCP à utiliser. Le N° de port Modbus par défaut est 502.

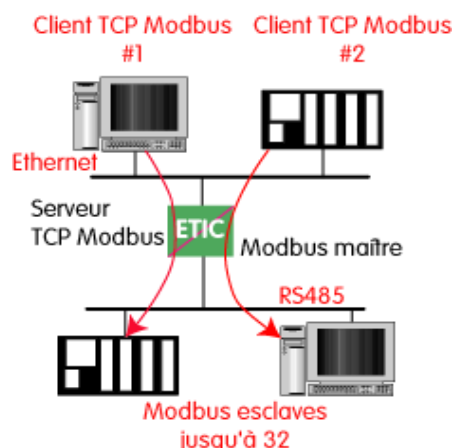
Esclaves Modbus

Le tableau permet de faire correspondre une adresse d'esclave Modbus et une adresse IP.

21.2.5 Passerelle Modbus serveur

La passerelle permet la connexion d'esclaves Modbus sur la liaison série du produit.

32 esclaves, au maximum, peuvent être connectés au port RS485.

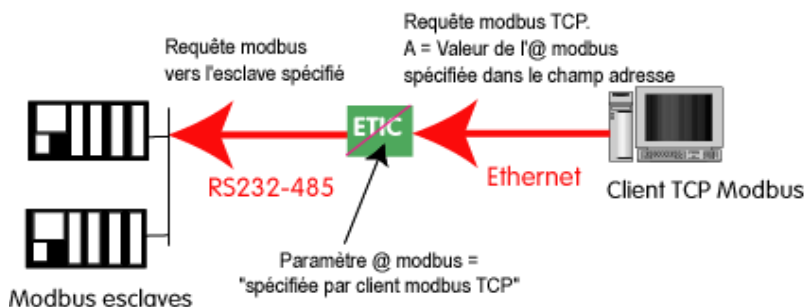
**Principe de la passerelle Modbus serveur :**

Un client TCP Modbus adresse une requête TCP Modbus à la passerelle ;

La passerelle se comporte en maître sur la liaison série.

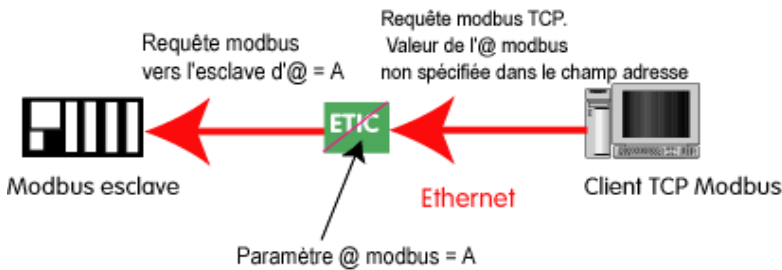
Elle « répète » la requête sur la liaison série ; l'adresse de la requête émise sur la liaison série est,

- soit l'adresse contenue dans le champ d'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.

PARAMETRAGE



Attention : Plusieurs client TCP Modbus peuvent adresser des requêtes aux esclaves de la liaison série. Néanmoins, on prendra garde à ne pas saturer la liaison série puisque son débit est bien inférieur à celui d'Ethernet.

Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Modbus > Serveur Modbus**.
- Cocher la case **Activer le serveur Modbus**.

Port COM

Choisir la liaison série 1 ou 2 du produit.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Protocole Modbus

Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

Activer la fonction proxy/cache

Si cette fonction est active, une requête n'est adressée à un esclave que si la même requête ne lui a pas été adressée depuis le temps fixé par le paramètre « rafraîchissement du cache ».

Rafraîchissement du cache

Fixe le délai minimum entre deux requêtes identiques adressées au même esclave

.

Temps inter-caractères

Fixe le temps maximum admissible entre caractères des réponses de l'esclave Modbus.

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 de la liaison série ; on peut ainsi adresser jusqu'à 32 esclaves de la liaison série.

Si l'on sélectionne une valeur particulière (entre 1 et 255), la passerelle adresse toutes les requêtes au N° d'esclave sélectionné ; on ne peut interroger qu'un seul esclave sur la liaison série.

Time out d'inactivité sur TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de requêtes Modbus reçues du réseau IP.

Temps d'attente réponse esclave

C'est le délai d'attente de réponse à la requête adressée à un esclave.

Port TCP

Fixe le N° du port TCP à utiliser. Le N° de port Modbus par défaut est le port 502.

Nombre de réitérations locales

Fixe le nombre de réitérations d'une requête Modbus par la passerelle en cas de non réponse de l'esclave Modbus.

PARAMETRAGE

21.3 Passerelle Raw TCP

21.3.1 Passerelle « Raw TCP client »

Elle permet de raccorder un équipement se comportant en « maître » sur la liaison RS232 / RS485.

Le serveur peut être une passerelle ETIC ou un PC incluant une application TCP serveur.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Transparent > Raw client COMx**.
- Cocher la case **Activer**.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Taille du buffer

Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Timeout fin de trame RS

Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Timeout d'inactivité TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Port TCP

Fixe le N° du port TCP à utiliser.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port TCP

Adresse IP serveur

Fixe l'adresse IP à laquelle sont transmis les caractères reçus de la RS232 / RS485 (c'est l'adresse du serveur RAW).

21.3.2 Passerelle « Raw serveur »

Elle permet de raccorder des équipements « esclaves » sur la liaison RS232-RS485.

L'équipement de la liaison série peut ainsi communiquer avec un PC Client Raw TCP.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Transparent > Raw serveur COMx**.
- Cocher la case **Activer**.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Taille du buffer de réception

Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Timeout fin de trame RS

Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Timeout d'inactivité TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Port TCP

Fixe le N° du port TCP à utiliser.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port TCP.

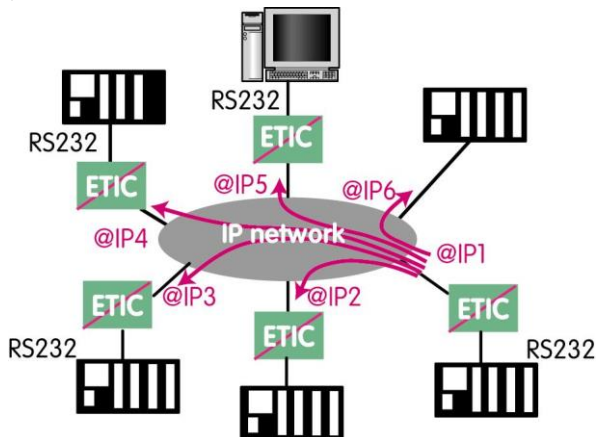
PARAMETRAGE

21.4 Passerelle « Raw UDP »

Cette passerelle permet de relier un ensemble d'équipements série ou IP, au travers d'un réseau IP.

Les destinataires sont désignés dans une liste établie par configuration.

Cette solution est très simple de mise en œuvre : On désigne chaque correspondant par son adresse IP ; les données RS232 sont envoyées sous forme de trames IP adressées individuellement à chaque correspondant enregistré.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Transparent > Raw UDP COMx**.
- Cocher la case **Activer**.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Taille du buffer de réception

Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Timeout fin de trame RS

Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Port UDP

Fixe le N° du port UDP à utiliser permettant de recevoir les données d'un ou plusieurs équipements sur le réseau.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port UDP.

Destinations

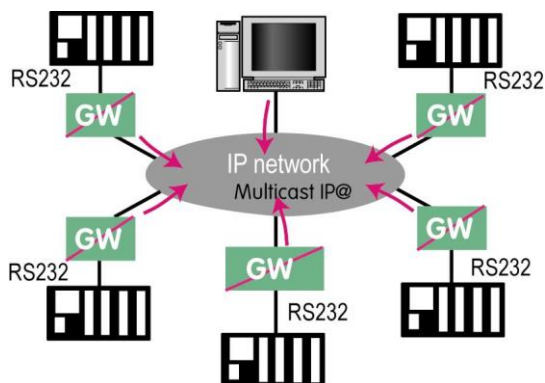
Cette table contient les adresse IP des passerelles vers lesquelles seront envoyés les caractères reçus de la liaison série.

Un port UDP différent peut être défini pour chaque adresse IP de destination.

21.5 Passerelle « Raw Multicast »

Cette passerelle est également destinée à relier un équipement série à un ensemble d'équipements du réseau IP.

Elle utilise le protocole « Multicast » qui permet de délivrer simultanément une trame IP à de nombreux destinataires sans accroître le trafic : Les données RS232 sont transmises dans une trame IP adressée à une adresse IP particulière appelée adresse multicast ; tous les abonnés à cette adresse décodent la trame.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Transparent > Raw Multicast COMx**.
- Cocher la case **Activer**.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Taille du buffer de réception

Fixe la taille maximum, en octets, d'un bloc transmis vers le réseau IP.

Timeout fin de trame RS

Fixe délai de silence maximum après lequel le buffer de caractères reçus de la liaison RS232-RS485 est transmis vers le réseau IP.

Port UDP

Fixe le N° de port UDP à utiliser.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port UDP.

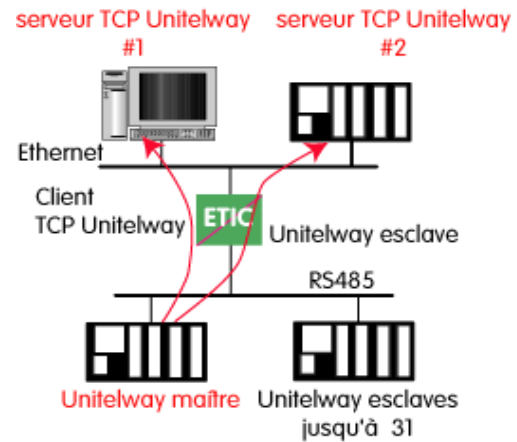
Adresse IP du groupe multicast

Saisir l'adresse IP attribué au groupe de diffusion (multicast) en respectant les règles de l'IANA .

PARAMETRAGE

21.6 Passerelle « Unitelway »

La passerelle Unitelway permet de connecter un automate série maître unitelway à un réseau IP. Elle permet en particulier de réaliser la fonction de télémaintenance d'automates Schneider Electric RS485 via un réseau IP.



Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Unitelway**.
- Cocher la case **Activer**.

Port COM

Choisir la liaison série 1 ou 2 du produit.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Adresse Xway

Adresse de la passerelle dans le réseau Xway.

Timeout d'inactivité TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Esclaves Unitelway

Désigne la correspondance entre l'adresse de chaque esclave Unitelway émulé par la passerelle et l'adresse IP et Xway de la station sur Ethernet.

21.7 Passerelle « Telnet »

Cette passerelle permet à un PC sur le réseau IP et équipé d'un logiciel client Telnet de se connecter à un équipement raccordé à la liaison série du Router.

Le débit et le format de la liaison série peuvent être pilotés selon la recommandation RFC2217.

Pour configurer la passerelle :

- Dans le menu, choisir **Configuration > Passerelle IP-RS > Transparent > Telnet**.
- Cocher la case **Activer**.

Port COM

Choisir la liaison série 1 ou 2 du produit.

Débit binaire, Parité, Données, Bits d'arrêt

Permet de configurer le débit et format de la liaison série.

Timeout d'inactivité TCP

Fixe le temps au bout duquel la liaison TCP est rompue en cas d'absence de caractères reçus du réseau IP ou de la liaison série.

Port TCP

Fixe le N° du port TCP à utiliser.

Attention : Si 2 passerelles du même type sont actives sur les deux ports série, elles ne peuvent pas utiliser le même N° de port TCP.

PARAMETRAGE

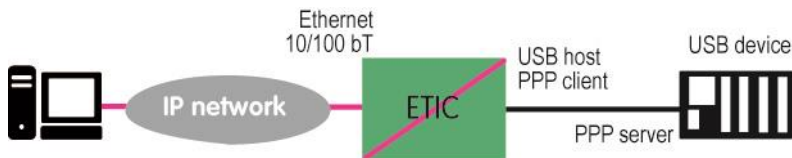
21.8 Passerelle USB

21.8.1 overview

The USB to IP gateway is able to forward IP traffic from devices connected to the Ethernet network to a USB device.

On the USB interface, the Router behaves like a USB host and a PPP client.

The USB device connected to the Router USB interface must behave like a PPP server.



Destination IP address; main case

When a device, connected to the Ethernet network, needs to transmit data to the USB device, the destination address of the IP frames which need to be transmitted to the USB device must be a specific IP address assigned to the USB gateway of the Router (see the configuration below).

Destination IP address; Modbus case

If no specific IP address is assigned to the USB gateway (see below), the Router forwards only modbus TCP traffic to the USB interface.

The destination IP address of the IP frames must be the LAN IP address of the Router.

21.8.2 Set-up

Select the "Setup" menu and then the "USB" menu.

"Activate" checkbox :

Select the "Activate" checkbox.

"Use a specific IP address" checkbox :

If modbus TCP traffic only has to be forwarded to the USB device, that checkbox must not be selected.

If other kinds of traffic have to be forwarded, that checkbox has to be selected.

"Specific IP address" parameter :

If modbus TCP traffic only has to be forwarded to the USB interface, no IP address has to be entered.

If other kinds of traffic have to be forwarded to the USB device, an additional IP address must be assigned to the Router. That address belongs to the network connected to the LAN interface of the Router. It is the IP address of the USB gateway.

It will be used as the destination IP address of the IP frames which must be forwarded to the USB device.

"Accept WAN traffic" checkbox:

It is necessary to select that checkbox if the PC is connected to the network through the Router the WAN interface.

It is not necessary to select that checkbox if the remote PC is connected to the Router through a VPN or through the LAN interface.

DIAGNOSTICS ET MAINTENANCE

1 Diagnostic visual de défaut de fonctionnement

Après la mise sous tension, le voyant  s'éclaire en rouge durant 20 secondes environ pendant la phase d'initialisation du produit.

Après ce délai, le voyant passe au vert et clignote durant 30 secondes puis devient fixe lorsque le produit est prêt à fonctionner.

Si le voyant reste éclairé rouge après de délai, le produit est probablement en panne ; contacter la hotline.

2 Menu Diagnostic

2.1 Journaux

Pour accéder aux différents journaux,

- Sélectionner la page le menu Diagnostic >Journal

Journal principal

Le journal principal enregistre et horodate les principaux événements du routeur et en particulier :

- Connexions et déconnexions ADSL
- Connexions et déconnexions des VPN
- Connexion / déconnexions d'utilisateurs distants
- Initialisation et démarrage du routeur

Journal OpenVPN et journal IPSec

Ces journaux enregistrent en détail et horodatent les principaux événements relatifs aux connexions et déconnexions VPN.

Journal avancé

Ce journal est destiné à notre hotline en cas d'événements particulièrement difficiles à analyser avec les autres outils.

2.2 Etat de l'interface WAN du routeur

Sélectionner le menu Diagnostic > Etat réseau > Interfaces

Etat de l'interface ADSL / Paramètres de base :

Champ « Adresse IP » : Adresse IP attribué à l'interface ADSL du routeur.

Champ Etat du modem :

Connected :	Le modem ADSL est connecté
Showtime tc sync :	Le modem ADSL est connecté
Full init :	Phase de négociation de la connexion
Handshake :	Prise de contact avec l' ATU-C (DSLAM), l'ATU-C a été détecté
Silent :	Pas d'ATU-C détecté
Idle :	Modem prêt, pas d'ATU-C détecté
Exception :	Le modem était connecté, une erreur (câble débranché en général) a causé une déconnexion

Etat de l'interface ADSL / Paramètres avancés :

Débit descendant :	Débit en ligne vers le routeur IPL (Mb/s)
Débit montant :	Débit en ligne depuis le routeur IPL (Mb/s)
Débit descendant atteignable :	Débit descendant maximum atteignable compte tenu de la qualité de la ligne (Mb/s)
Débit montant atteignable :	Débit montant maximum atteignable compte tenu de la qualité de la ligne (Mb/s)
Atténuation signal descendant :	Atténuation du signal reçu par le routeur IPL (dB).
Atténuation signal montant :	Atténuation du signal émis par le routeur et reçu par l'opérateur (dB)
Marge signal descendant :	Excès du rapport signal à bruit observé par rapport au minimum requis
Marge signal montant :	Excès du rapport signal à bruit observé par rapport au minimum requis

2.3 Etat des passerelles série

- Sélectionner le menu Diagnostic > Etat des passerelles

Cette page permet d'afficher l'état courant du paramétrage des passerelles, le nombre d'octets et de trames échangées et le nombre de trames en erreur.

Le menu « Visualisation des données série » permet de visualiser le trafic RX et TX sur la liaison série.

2.4 Outils « Ping »

Cette page permet de commander l'émission d'une trame « ping » vers une machine du réseau raccordé au routeur.

2.5 Outil « Scanner Wi-Fi »

Le scanner Wi-Fi affiche la liste des réseaux Wi-Fi détectés par le routeur.

Pour chacun de réseaux détectés, le scanner affiche les informations suivantes :

- Identificateur du réseau (SSID)
- L'adresse MAC du point d'accès
- N° du canal
- Niveau de réception

Le scanner est utile afin de choisir un N° de canal non utilisé lorsque l'on souhaite configurer le canal en point d'accès.

Réciproquement, il facilite la configuration de l'interface Wi-Fi du routeur lorsque l'interface Wi-Fi doit être utilisée en client.

Remarque : le scanner Wi-Fi ne peut fonctionner que si l'interface W-iFi est déclarée comme client Wi-Fi (et pas comme point d'accès Wi-Fi).

Pour déclarer l'Interface Wi-Fi comme client W-iFi afin d'utiliser le Scanner :

- Dans le menu Configuration > WAN, sélectionner Wi-Fi dans la liste.
- Dans le menu Configuration > LAN > Point d'accès Wi-Fi, décocher la case « Activer le point d'accès Wi-Fi ».

3 Sauvegarde et chargement d'un fichier de paramètres

Une fois un produit configuré, il est possible d'enregistrer la configuration dans la mémoire du routeur, ou de la sauvegarder sous forme d'un fichier éditable.

Réciproquement, il est possible de charger une configuration parmi l'ensemble des configurations enregistrées dans la mémoire du produit ou bien de restaurer un fichier de configuration sauvegardé dans un PC.

- Sélectionner les menus Maintenance > Gestion des configurations.

Le tableau qui enregistre la liste des configurations enregistrées dans la mémoire du routeur s'affiche.

Pour enregistrer la configuration courante dans la mémoire du Routeur,

- Face au champ « Nom de la configuration », attribuer un nom pour la configuration et cliquer le bouton « Save ».

La configuration s'ajoute à la liste dans le tableau des « configurations sauvegardées ».

Pour charger comme configuration courante l'une des configurations de la liste,

- sélectionner la configuration dans la liste et cliquer charger.

Pour sauvegarder la configuration courante dans un fichier .txt,

- commencer par enregistrer la configuration courante dans la mémoire du routeur comme indiqué précédemment,
- puis sélectionner dans la liste la configuration à exporter et cliquer le bouton « Exporter vers le PC ».

Pour restaurer un fichier de paramètres sauvegardé,

- Cliquer le bouton « choisissez un fichier » puis sélectionner le fichier (XXX.txt) à restituer.
- Modifier éventuellement le nom du fichier et cliquer le bouton « Importer ». la configuration correspondante apparaît dans la liste « Configurations sauvegardées ».
- Sélectionner la configuration dans la liste puis cliquer « Charger » ; elle remplace la configuration courante.

Note : Un fichier de configuration ne peut être restauré que s'il a été constitué avec la même version de firmware.

4 Mise à jour du firmware

Elle s'effectue par la prise Ethernet ou bien à distance.

Si la mise à jour échoue, par exemple si elle s'effectue à distance et que la connexion est interrompue pendant le chargement, le routeur redémarre avec la version antérieure du firmware.

Après la mise à jour, le produit utilise le fichier de paramétrage utilisé auparavant.

On vérifiera que la nouvelle version de firmware peut utiliser le fichier de paramétrage antérieur ; la règle est la suivante :

Le paramétrage antérieur peut être utilisé si le chiffre majeur des versions de firmware est le même.

Exemple V2.3 et V2.6.

Pour effectuer la mise à jour du logiciel,

- sélectionner les menus Maintenance > Mise à jour du logiciel ;
- sélectionner le fichier du nouveau firmware ;
- Cliquer le bouton « Mettre à jour maintenant



13, Chemin du Vieux Chêne
38240 Meylan - France

Tel : +33 (0)4 76 04 20 00
contact@etictelcom.com

www.etictelcom.com