



**IPL-M156 IPL-L134 IPL-I1128
IPL-RS232**

Routeur d'accès distant

NOTICE D'UTILISATION
Document référence : 9013509-02

La famille de routeurs d'accès distant est fabriquée par

ETIC TELECOMMUNICATIONS

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

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

TEL : + (33) (0)4-76-04-20-05
FAX : + (33) (0)4-76-04-20-01
E-mail : hotline@eticlecom.com
web : www.eticlecom.com

PRESENTATION

1	IDENTIFICATION DES PRODUITS	7
2	FONCTIONS PRINCIPALES DES PRODUITS	8
2.1	Interconnexion de sites distants	8
2.2	Port RS232-RS485 pour modem externe	9
2.3	Serveur d'accès distant	10
2.4	Routeur d'accès distant par Internet.....	12
2.5	Passerelle asynchrone.....	13
2.6	Filtrage des machines et services accessibles (Fire-wall)	16
2.7	Email ou SMS d'alarme	16
2.8	Visualisation / télécommande de trois E/S	17
2.9	Configuration par navigateur html	17

INSTALLATION

1	DESCRIPTION DU PRODUIT	19
1.1	Voyants	19
1.2	Connecteurs.....	20
1.3	Micro-switches	21
2	VENTILATION.....	21
3	ALIMENTATION	22
4	FUSIBLE	22
5	CONNEXION AU RESEAU LOCAL ETHERNET	22
6	CONNEXION A L'INTERFACE RS232 / RS485	23
7	CONNEXION A LA LIGNE TELEPHONIQUE (IPL-M156).....	23
8	CONNEXION A LA LIGNE RNIS (IPL-I1128).....	24
9	RACCORDEMENT DES ENTREES SORTIES	24
10	ABONNEMENT A L'INTERNET	25
10.1	Avantages de la connexion par Internet	25
10.2	Abonnement à l'Internet du routeur	26

../..

CONFIGURATION

1	INTRODUCTION	29
2	PREMIERE CONFIGURATION PAR L'INTERFACE ETHERNET.....	29
3	MODIFICATIONS ULTERIEURES DE LA CONFIGURATION PAR LE LAN.....	31
4	PREMIERE CONFIGURATION A DISTANCE	32
5	MODIFICATION DE LA CONFIGURATION A DISTANCE.....	34
6	PERTE DU MOT DE PASSE ET / OU D'ADRESSE IP	34
7	PARAMETRAGE DU ROUTEUR	35
7.1	Arborescence du serveur d'administration	36
7.2	Menu « Configuration système »	38
7.2.1	Menu « Protocole IP».....	38
7.2.2	Menu « Liste des machines»	39
7.2.3	Menu « date et heure»	41
7.2.4	Menu « modem »	41
7.2.5	Menu RS232 RS485	42
7.2.6	Menu RIP	43
7.2.7	Menu SNMP	43
7.2.8	Menu « sauvegarder / restaurer ».....	43
7.2.9	Menu « Redémarrer »	43
7.3	Menu « Routage et accès distant »	44
7.3.1	Liste d'utilisateurs.....	44
7.3.2	Menu « Nœuds distants»	47
7.3.3	Menu « Routes statiques »	50
7.4	Menu « Configuration sécurité ».....	51
7.4.1	Menu « droits d'administration »	51
7.4.2	Menu Pare-feu.....	52
7.5	Menu « configuration Internet».....	56
7.5.1	Compte.....	56
7.5.2	Routage Internet.....	57
7.5.3	Menu « VPN »	59
7.6	Menu « Passerelle IP<>RS ».....	62
7.6.1	Menu « Passerelle Unitelway »	63
7.6.2	Menu « Passerelle Modbus »	64
7.6.3	Menu passerelle transparente	65
7.7	Menu « Diagnostic».....	66
7.8	Menu « Alarme e-mail».....	67

../..

UTILISATION

1	ETABLIR UNE CONNEXION « RAS »	69
1.1	Les différentes possibilités de connexion.....	69
1.2	Etablir la connexion	71
1.2.1	Préparation de la connexion	71
1.2.2	Connexion sans contre-appel	72
1.2.3	Connexion avec contre-appel à la demande	73
1.2.4	Connexion avec contre-appel de sécurité	74
1.2.5	Accéder aux machines du réseau local	74
1.2.6	Portail web.....	75
1.3	Libérer une connexion	75
2	CONNEXION SECURISEE PAR INTERNET	76
2.1	1ere étape :Connecter le routeur IPL au réseau Internet.....	77
2.1.1	Contre-appel IP	77
2.1.2	Connexion automatique dès la mise sous tension	77
2.1.3	Connexion automatique par fermeture de l'entrée TOR N°1.....	78
2.1.4	Connexion automatique en cliquant « connecter »	78
2.2	2eme étape : Etablir la connexion sécurisée.....	79
2.2.1	Etablir la connexion sécurisée via un e-mail.....	80
2.2.2	Etablir la connexion sécurisée via un routeur FTP	81

1 Identification des produits

La présente notice décrit la mise en service et l'utilisation des produits suivants :

	IPL-	RS232	M156	L134	I1128
Modem V90 international			•		
Modem liaison permanente 2 fils				•	
RNIS 64 Kb/s (SO EURO-ISDN)					•
Ethernet 10 Mb/s	•	•	•	•	•
1 port RS232 / RS485	•	•	•	•	•
1 Sortie et 3 ETOR	•	•	•	•	•
Fonctions principales					
Routeur d'accès distant multinoeuds » (30 nœuds)	•	•	•	•	•
1 port longue distance (PPP) avec modem interne	•	•	•	•	•
1 port longue distance (PPP) RS232 pour modem externe	•	•	•	•	•
Mode serveur RAS par Internet sécurisée par VPN	•	•	•	•	•
Passerelle Modbus et Unitelway RS232-RS485	•	•	•	•	•
Fire-wall haute sécurité	•	•	•	•	•
Alarme e-mail –SMS sur changement d'état d'1 E-TOR	•	•	•	•	•
Visualisation/télécommande 1 STOR & 3 ETOR	•	•	•	•	•
Configuration HTML (à distance si autorisée)	•	•	•	•	•

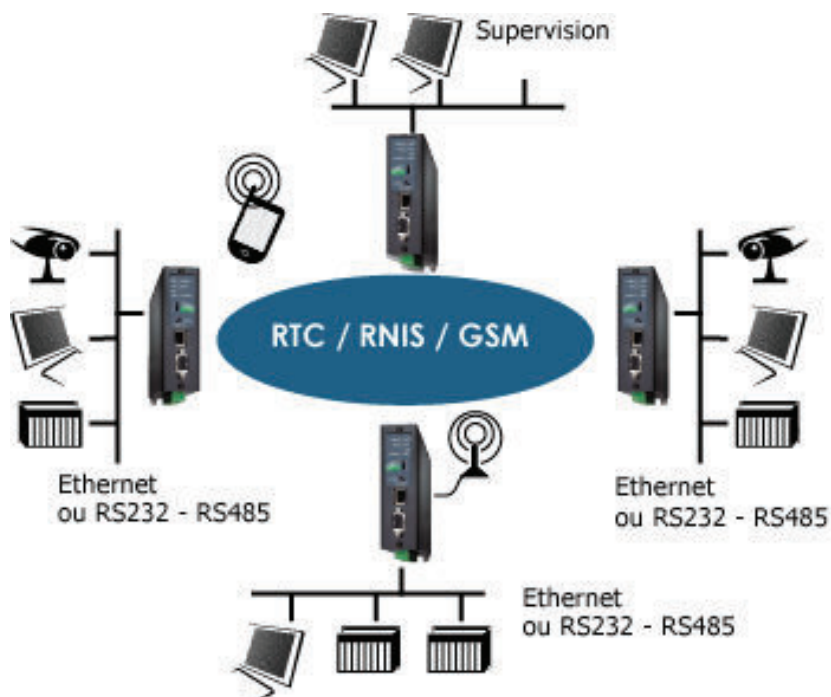
2 Fonctions principales des produits

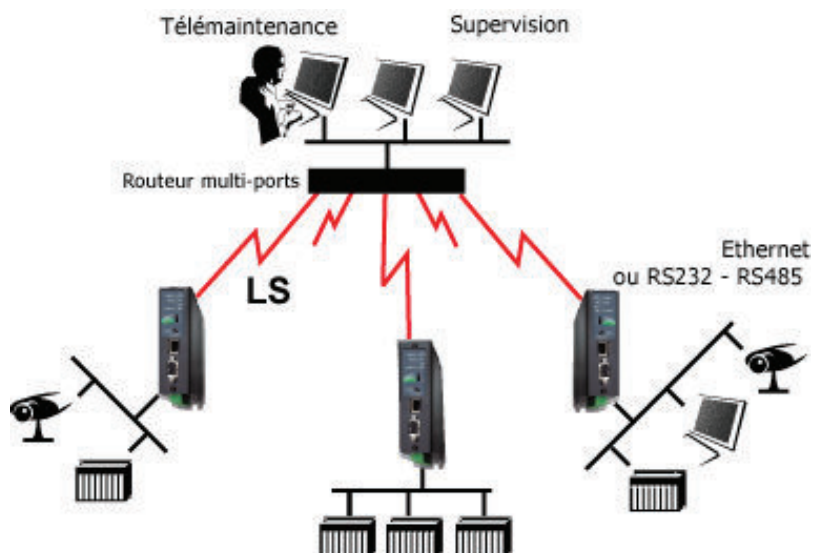
2.1 Interconnexion de sites distants

Selon le modèle, les routeurs d'accès distants IPL intègrent un modem permettant d'interconnecter des réseaux Ethernet d'automatisme par les réseaux suivants :

- réseau téléphonique (modèle IPL-M156)
- liaison permanente analogique (modèle IPL-L134)
- RNIS (modèle IPL-I1128)

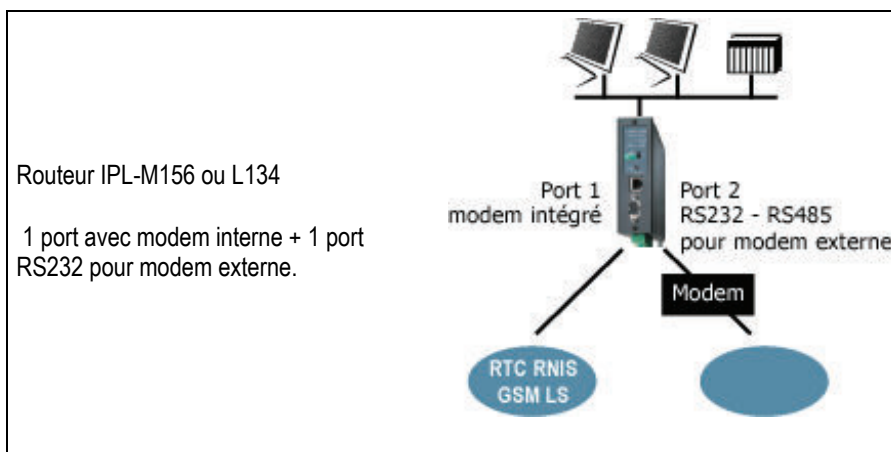
Le modèle IPL-RS232 n'inclut pas de modem ; il est fait pour piloter un modem externe au moyen de commandes « AT ».



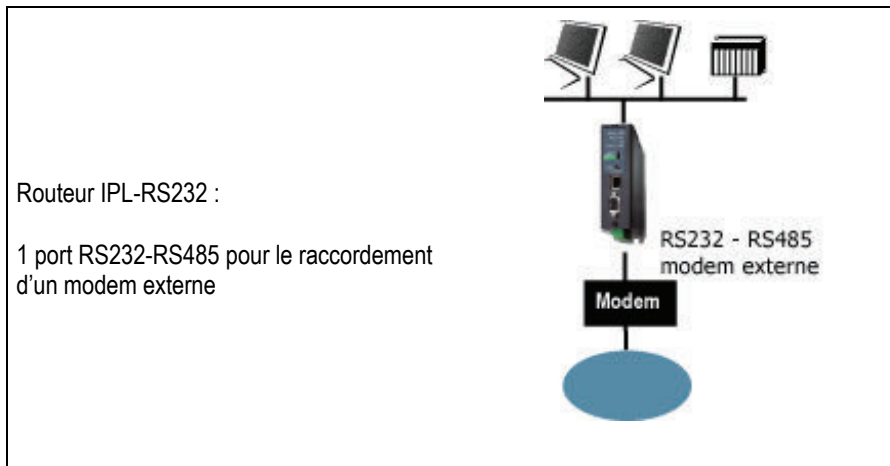


2.2 Port RS232-RS485 pour modem externe

Tous les modèles de routeurs IPL possèdent un port RS232-RS485 permettant de connecter un modem externe.



Dans le cas du modèle IPL-RS232, ce port RS232-RS485 est le port longue distance unique.



2.3 Serveur d'accès distant

Le routeur IPL permet également à des utilisateurs distants autorisés d'accéder aux machines d'un réseau Ethernet ou RS232-RS485 au moyen d'un modem.

Contrôle de l'identité de l'utilisateur

Le routeur gère une liste d'utilisateurs autorisés (25 au maximum); lorsqu'un utilisateur distant se connecte, il doit saisir son nom d'utilisateur et son mot de passe pour accéder au réseau local.

Call-back de sécurité

Si l'on souhaite renforcer la sécurité de l'accès au réseau local, la fonction call-back de sécurité permet de forcer le routeur à rappeler l'utilisateur au numéro de téléphone qui lui est affecté.

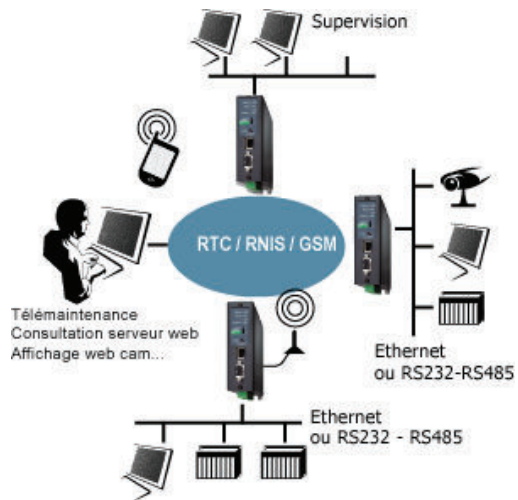
Call-back à la demande

Si l'on souhaite imputer le coût de communication à la ligne du routeur, la fonction call-back à la demande permet à un utilisateur de demander à être rappelé au N° qu'il fournit à distance.

Filtrage des N° d'appel acceptés

Pour renforcer la sécurité, l'appel d'un utilisateur peut n'être accepté que s'il provient d'un N° paramétré.

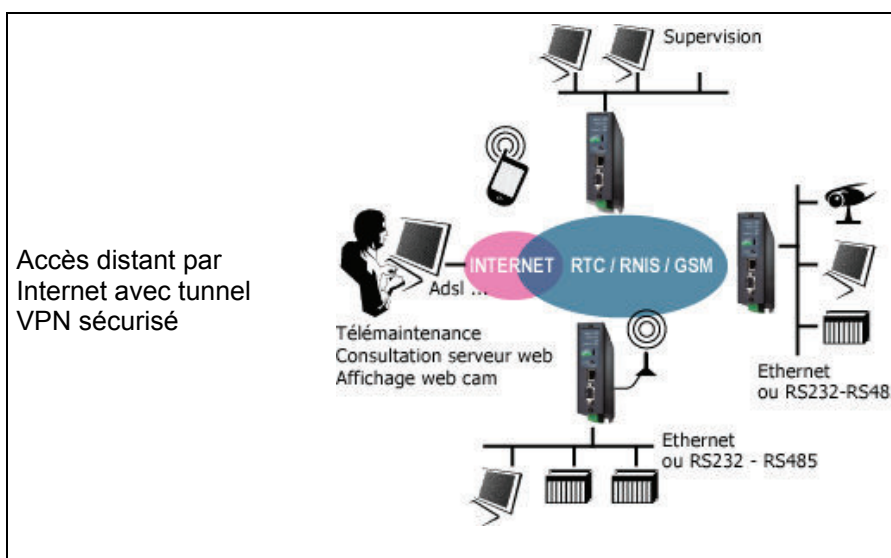
Accès distant par un utilisateur équipé d'un modem.



2.4 Routeur d'accès distant par Internet

Le routeur IPL permet également à des utilisateurs distants autorisés d'accéder aux machines d'un réseau Ethernet ou RS232-RS485 par Internet en établissant un tunnel sécurisé (VPN).

La technologie VPN procure à la fois la sécurité sur l'Internet et la possibilité d'accéder à chacune des machines du réseau local « comme si l'on était sur place » et sous réserve des droits ouverts par le fire-wall.



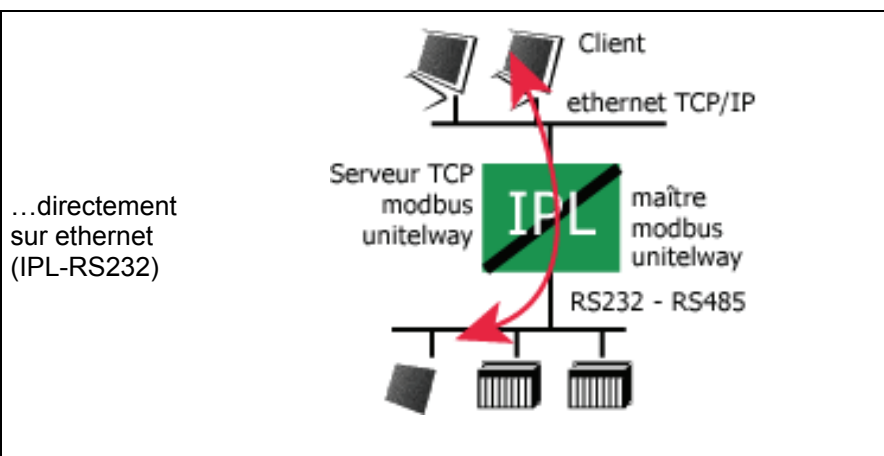
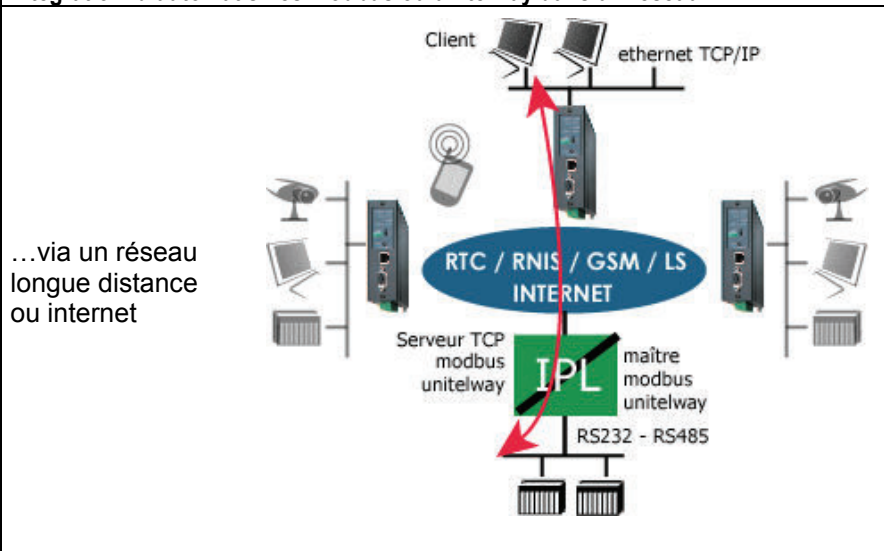
2.5 Passerelle asynchrone

Le routeur comporte une liaison asynchrone RS232-RS485 ; elle peut être utilisée comme 2^{ème} port longue distance comme décrit au paragraphe 2.2.

Le port RS232-RS485 peut aussi être utilisé (de manière exclusive) comme port pour la connexion d'un équipement asynchrone.

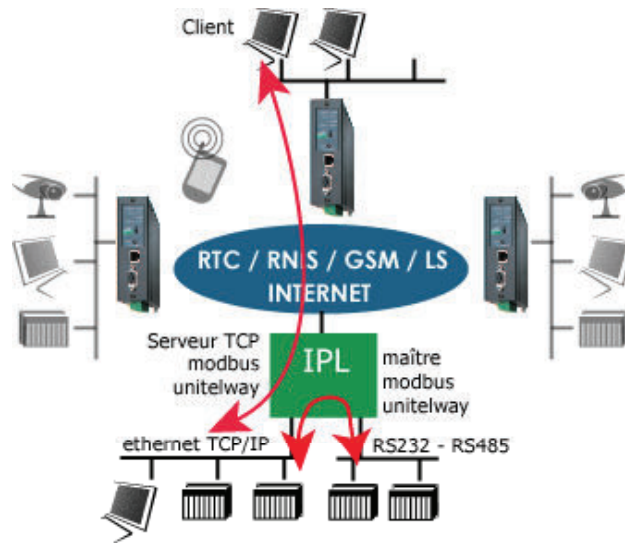
Le routeur IPL peut alors fournir le service « d'intégrateur » d'équipements RS232-RS485 dans un réseau IP réparti ou bien de passerelle TCP-IP.

Intégration d'automatismes modbus ou unitelway dans un réseau IP...



Intégration d'automatismes modbus ou unitelway dans un réseau IP (suite)....

Accès distant à
un réseau
ethernet et
passerelle
ethernet -RS485



2.6 Filtrage des machines et services accessibles (Fire-wall)

Le pare-feu (fire-wall) embarqué dans le routeur IPL permet de limiter le domaine accessible sur le réseau local, en fonction de l'identité du nœud ou de l'utilisateur connecté.

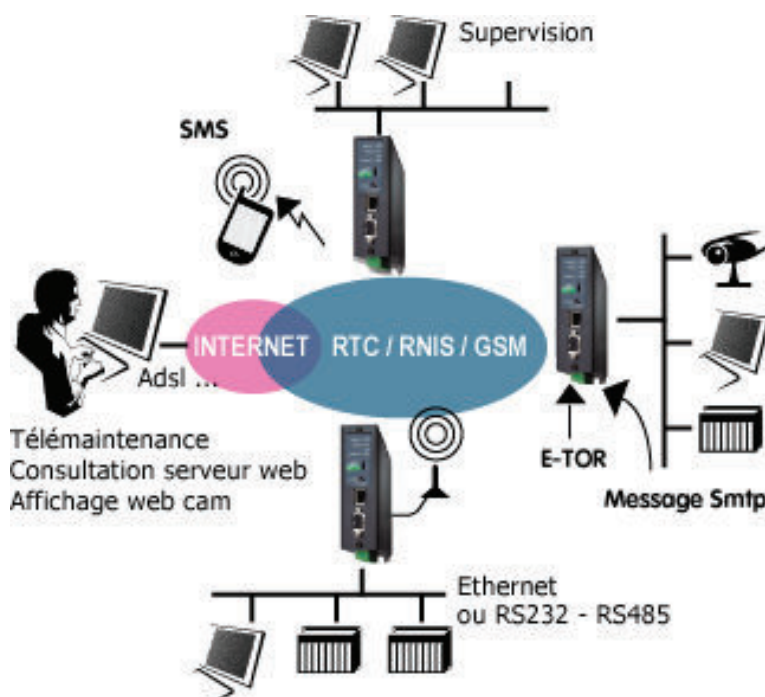
Par domaine accessible, on entend les adresses IP accessibles et les ports de chacune de ces adresses IP.

Le pare-feu est de type « stateful inspection » assurant une très haute résistance aux attaques.

25 filtres peuvent être constitués ; chaque filtre peut être attribué à un nœud ou un utilisateur autorisé.

2.7 Email ou SMS d'alarme

Le routeur IPL possède 1 entrée TOR qui permet d'émettre un email d'alarme lorsqu'elle change d'état.



2.8 Visualisation / télécommande de trois E/S

Le routeur comporte 1 sortie et 3 entrées TOR.

Un utilisateur autorisé peut télécommander à distance la sortie TOR et visualiser l'état des 3 entrées au moyen de son navigateur html.

2.9 Configuration par navigateur html

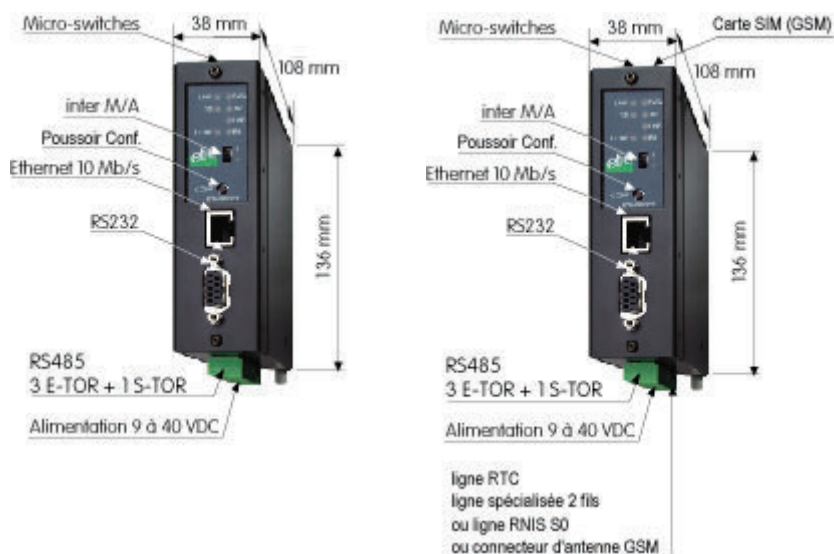
Le routeur se configure au moyen d'un navigateur HTML.

La configuration peut s'effectuer par Ethernet ou à distance.

La configuration à distance peut être limitée ou même interdite si la sécurité du réseau l'impose.

FICHE TECHNIQUE	
Encombrement	130 x 38 x 110 mm (h, l, p)
C.E.M	EN50082-2
Sécurité électrique	EN 60950
Foudre	EN61000-4 et -5 (2kW modes commun et différentiel)
Alimentation	9 à 40 VDC
Consommation	150 mA sous 24 VDC (sauf modèle GSM)
T° de fonct.	0° / + 50°C atmosphère sèche
Réseau téléphonique	Conforme à la norme européenne CTR21
Modem	V90 (56kb/s) ou GSM-GPRS ou EURO-ISDN S0
Ethernet	10 Mb/s
RS232-RS485	1200 à 115200 kb/s avec ou sans parité passerelle Modbus / unitelway / Telnet ou raw
Protocoles	PPP / CHAP Call-back MS CB Affectation d'@ IP au client distant : PROXI-ARP
Contrôle d'accès	Liste d'utilisateurs (25 lignes) Nom d'utilisateur et mot de passe
Contre-appel	Contre-appel de sécurité Contre-appel vers un N° à la demande
Pare-feu	Limitation du domaine IP accessible Limitation des services accessibles
Journal	Journal horodaté des 50 dernières connexions
Configuration	Par navigateur HTML Via le LAN ou le RTC

1 Description du produit





IPL-RS232

IPL-M156 / IPL-L134 / IPL-I1128

1.1 Voyants

6 voyants permettent de visualiser le fonctionnement du routeur.

Voyant	Fonction
LINK	Le routeur est correctement connecté au réseau Ethernet
DATA	Activité sur le réseau Ethernet
RD	Caractères reçus du réseau RTC ou RNIS ou GSM
TD	Caractères transmis vers le réseau RTC ou RNIS ou GSM
EXT. L	Connexion distante établie sur le port RS232-RS485 quand il est utilisé pour une liaison distante avec modem externe
L ou L / 	Eclairé : Connexion distante établie via le modem interne Clignotant : Connexion en cours d'établissement
CONF	La configuration à distance a été autorisée en appuyant sur le poussoir CONF de la face avant.
	Voyant d'alimentation

1.2 Connecteurs

Bornier 2 points : Alimentation		
Broche	Signal	Fonction
1	+	Tension + 9 à 40 V continu
2	-	0 V

Bornier 8 points : Entrées-sorties (Modèles dont la référence se termine par « e » uniquement)		
Broche	Signal	Fonction
1	+	Tension + 3 V DC fournie par le produit.
2	IN1	Entrée TOR N°1
3	IN2	Entrée TOR N°2
4	IN3	Entrée TOR N°3
5	OUT1	Sortie relais
6	OUT2	Sortie relais
7	B +	RS485 polarité B
8	A -	RS485 polarité A

Broche	Circuits			Désignation	Terminal - IPL
1	DP	CD	109	Détection de porteuse	⇐
2	RD	RX	104	Réception de données	⇐
3	ED	TX	103	Emission de données	⇒
4	TDP	DTR	108	Terminal de données prêt Et commande d'appel	⇒
5	TS	SG	102	Terre de signalisation	
6	PDP	DSR	107	Poste de données prêt	⇐
7	DPE	RTS	105	Demande pour émettre	⇒
8	PAE	CTS	106	Prêt à émettre	⇐
9	IA	RI	125	Indicateur d'appel	⇐

1.3 Micro-switches

Micro-switches		
SW 1	SW 2	
OFF	OFF	L'@ IP du serveur d'administration est l'adresse programmée
ON	OFF	L'@ IP du serveur d'administration est l'adresse usine : 192.168.0.128 L'@ IP attribuée à un client distant est l'adresse usine : 192.168.0.129
OFF	ON	l'adresse IP du serveur d'administration est obtenue auprès d'un routeur BOOTP ou DHCP.
ON	ON	Réservé
SW3		
OFF		Le nom d'utilisateur et le mot de passe permettant l'accès au serveur d'administration sont les valeurs programmées
ON		Le serveur d'administration est accessible sans protection par le réseau Ethernet
SW 4 à 8		Inutilisés

2 Ventilation

Le produit est conçu pour être fixé sur un rail DIN 35 mm.
Pour éviter tout échauffement, en particulier lorsque la température ambiante peut s'élever dans l'armoire électrique, on veillera à ménager un espace de 1 cm de chaque côté du produit pour faciliter l'écoulement de la chaleur.

3 Alimentation

La tension d'alimentation doit être régulée et strictement comprise entre 9 et 40 Volt continu.

La consommation est de 170 mA / 24 VDC.

4 Fusible

La carte électronique est équipée d'un fusible rapide 3 A situé à proximité des borniers débrochables.

!!! Un fusible de rechange est disponible sur la carte électronique au-dessus des voyants.

5 Connexion au réseau local Ethernet

L'interface locale du routeur IPL est une interface Ethernet 10 Mb/s.

Connecter le routeur IPL au réseau local via un hub ou un switch Ethernet en utilisant un câble droit.

Connexion directe d'un PC

Pour connecter directement un PC au routeur (par exemple, à la mise en service), utiliser le cordon Ethernet croisé (couleur rouge) fourni avec le routeur ou un câble équivalent.

6 Connexion à l'interface RS232 / RS485

Le routeur dispose d'une interface asynchrone RS232 et RS485 .

Cette interface permet

- soit le raccordement d'un modem externe pour constituer un 2^{ème} lien longue distance (PPP-TCP/IP),
- soit le raccordement d'un équipement asynchrone (automate ...) afin de pouvoir y accéder « en mode TCP/IP » (fonction passerelle IP-RS) depuis le réseau local ou à distance.

Raccordement d'un modem à l'interface RS232

Si l'on veut raccorder un modem à l'interface RS232 pour établir un 2^{ème} port longue distance, on utilisera le câble de référence CAB 605 à commander séparément.

Longueur maximale du câble RS232

L'équipement raccordé à l'interface RS232 ne doit pas être éloigné de plus d'une dizaine de mètres du routeur IPL et le câble de raccordement doit de préférence être blindé.

Liaison RS485

La liaison RS485 est polarisée par des résistances de 1 K Ohm à l'intérieur du produit.

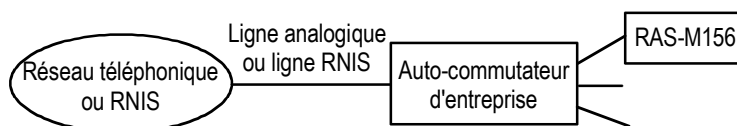
Si l'équipement asynchrone est raccordé à une distance supérieure à 10m, on aura soin de connecter une résistance de terminaison de bus RS485 suivant les règles de l'art.

7 Connexion à la ligne téléphonique (IPL-M156)

Le routeur IPL-M156 se raccorde à une ligne téléphonique de type analogique (identique à celle que l'on utilise pour un fax ou un modem téléphonique).

La ligne peut être directe ou bien être une ligne secondaire analogique (souvent appelée ligne interne) d'un auto-commutateur téléphonique privé.

L'auto-commutateur (ou standard) peut être indifféremment raccordé au réseau téléphonique public analogique ou bien au réseau RNIS ou à un autre type de réseau.



8 Connexion à la ligne RNIS (IPL-I1128)

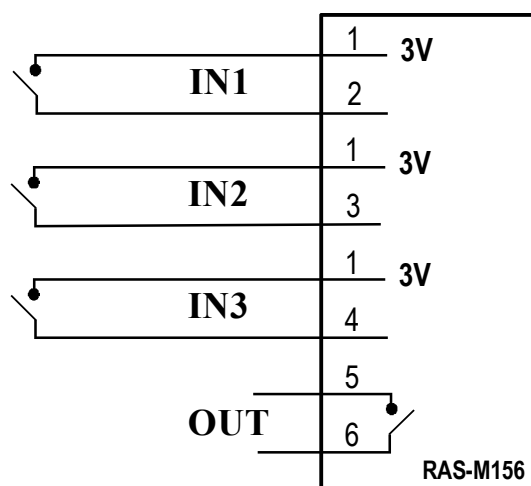
Le routeur d'accès distant IPL-I1128 se raccorde à une interface de base SO du réseau RNIS européen (EURO-ISDN).

La ligne peut être directe ou bien être une ligne secondaire d'un auto-commutateur téléphonique privé.

9 Raccordement des entrées sorties

L'entrée 1 permet d'émettre une alarme par e-mail ou bien de commander la connexion du routeur à l'Internet.

Par ailleurs, le menu du menu « Contrôle des E/S » du routeur d'administration permet de visualiser l'état des 3 entrées et de télécommander la sortie.



Sortie sur relais : Tension maximum 50 VDC
Courant maximum : 500 mA

Entrées : Non isolée
Tension maximum 20 VDC

10 Abonnement à l'Internet

Le routeur IPL est pensé pour l'Internet ; un tunnel crypté (VPN) est mis en œuvre, le firewall protège et différencie l'accès au réseau local, le journal enregistre les tentatives de connexion.

A titre d'exemple, Il est très efficace pour les opérations de télémaintenance, le transport de vidéo provenant de webcams ou les systèmes de télécontrôle.

Cependant, avant de faire le choix de l'Internet, on aura soin d'évaluer les risques encourus par les personnes et le biens, au cas où une personne mal intentionné parviendrait à se connecter. On prendra toutes précautions nécessaires pour pallier cette éventualité.

Une précaution élémentaire consiste, par exemple, à faire en sorte que le routeur ne soit pas connecté en permanence à l'Internet en sorte qu'un attaquant n'est qu'un temps limité pour sa tentative d'effraction.

10.1 Avantages de la connexion par Internet

La connexion par Internet procure trois avantages, en particulier dans le cas des connexions internationales ou transcontinentales, :

- **Communication plus économique**

Le coût des communications internationales par réseau RTC peut être élevé en particulier si les communications doivent durer longtemps. La connexion par Internet résout ce problème.

- **Débit plus élevé**

Lorsque l'on utilise le réseau commuté pour les communications transcontinentales, le débit est souvent faible. La connexion par Internet résout aussi ce problème.

- **Fiabilité de la transmission**

Les protocoles basés sur TCP/IP permettent de s'affranchir des défauts parfois observés dans la transmission entre modems dans le cas des communications transcontinentales.

10.2 Abonnement à l'Internet du routeur

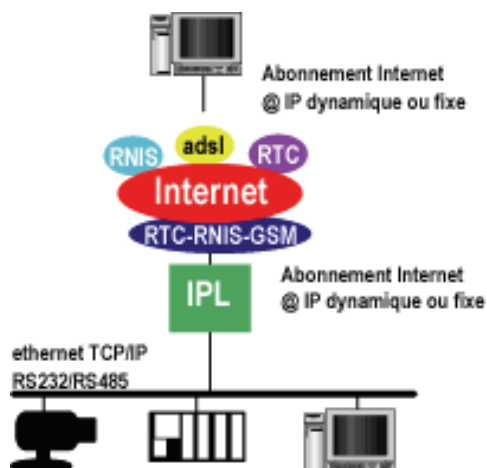
Le routeur IPL est fait pour les fonctions de téléexploitation ou télémaintenance sur les lignes les plus facilement disponibles à travers le monde : Réseau RTC ou réseau GSM ou réseau RNIS.

- L'abonnement à Internet doit donc être pris pour supporter l'un de ces réseaux.
- L'abonnement peut être à adresse IP dynamique (économique voire gratuit). Il peut être aussi à adresse fixe.
- L'abonnement doit être pris **dans le pays** où est installé le routeur
- Si le routeur IPL communique avec un routeur d'une autre marque, il faut configurer le routeur partenaire de la façon suivante de manière à autoriser l'établissement d'un tunnel sécurisé :

Ouvrir le port TCP 1723: Il s'agit du service « VPN avec protocole PPTP » appelé aussi « Point To Point Tunneling Protocol».

Le routeur doit laisser passer le protocole IP 47 : GRE (Generic Routing Encapsulation)..

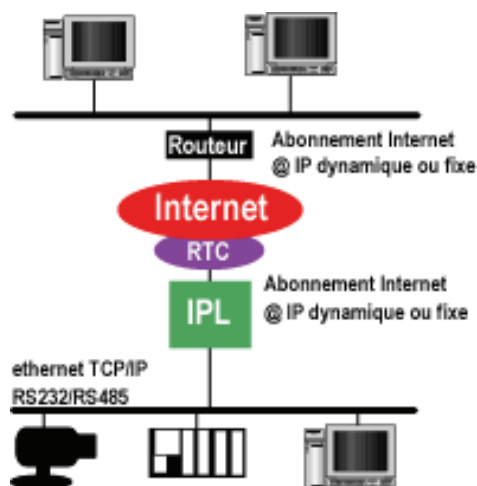
**Connexion Internet depuis un PC
« isolé »**



**Communication avec un
routeur partenaire via
Internet :**

Port TCP 1723 ouvert

Protocole IP47 "GRE" autorisé



1 Introduction

Le routeur se configure au moyen d'un PC équipé d'un navigateur HTML.

La configuration initiale peut être effectuée par l'interface Ethernet ou bien à distance.

Les modifications ultérieures peuvent être en plus effectuées par le réseau local.

Il est préférable de connecter le routeur au réseau Ethernet avant de le mettre sous tension (inter. A/M).

Les caractères accentués ne doivent pas être utilisés.

Attention : 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.

Voir paragraphe 6 : perte de l'adresse IP du serveur d'administration.

Voir aussi paragraphe 7.4.1. : Droits d'administration

2 Première configuration par l'interface ethernet

Etape 1 : Créer ou modifier la connexion TCP/IP du PC (voir annexe 1).

Attribuer à cette connexion une adresse IP différente mais cohérente avec l'adresse IP usine du routeur qui est 192.168.0.128.

On utilisera par exemple l'adresse 192.168.0.127 pour le PC.

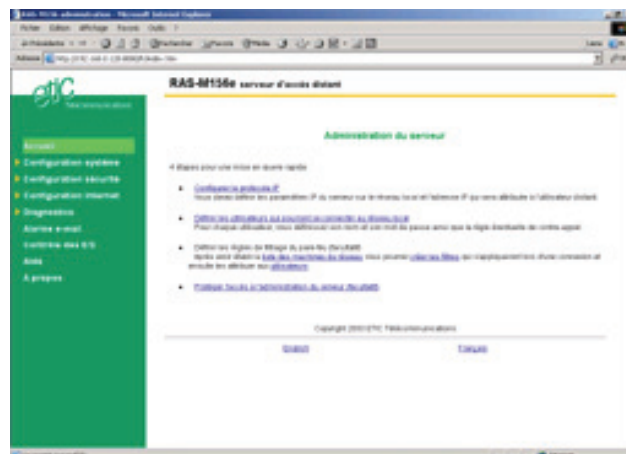
Etape 2 : Connecter directement le PC au routeur

Connecter directement le PC au routeur au moyen du câble croisé fourni (couleur rouge), puis ensuite seulement, mettre le routeur sous tension.

Etape 3 : Lancer le navigateur

Ouvrir le navigateur et désigner l'adresse IP du serveur d'administration programmée en usine : 192.168.0.128 (ne pas faire précéder l'adresse de www).

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 ; voir paragraphe 7.4.1 pour protéger l'accès au serveur d'administration.

3 Modifications ultérieures de la configuration par le LAN

Les modifications peuvent être effectuées depuis le réseau local à l'adresse qui a été attribuée au serveur d'administration (voir paramétrage).

- Ouvrir le navigateur du PC et saisir l'adresse IP du serveur d'administration du routeur.
- Saisir, s'il y a lieu, le nom d'utilisateur et le mot de passe qui ont été programmés pour protéger l'accès au serveur d'administration.

Si la fenêtre de demande d'identification ne s'affiche pas :

- L'accès au serveur d'administration a été limité ; il faut appuyer sur le poussoir CONF. De la face avant du produit.
- Ou bien, l'adresse IP que vous avez saisie est fausse.

Si la fenêtre de demande d'identification s'affiche, mais pas la page web :

- Le nom d'utilisateur ou le mot de passe d'accès au serveur d'administration sont erronés.

Voir paragraphe 6 ou paragraphe 7.4.1.

4 Première configuration à distance

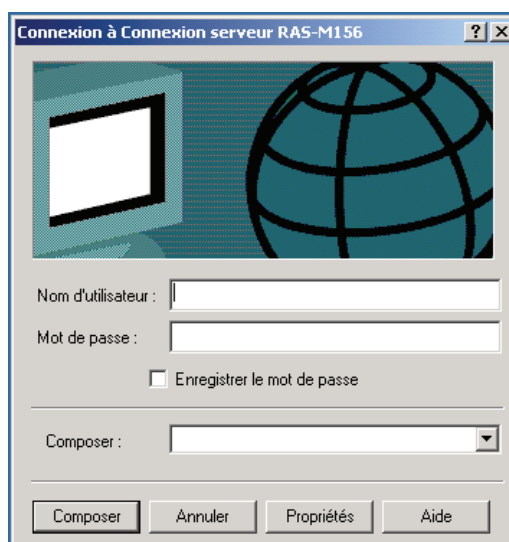
La première configuration peut aussi être effectuée à distance, par exemple au moyen d'un modem et d'une ligne téléphonique de type analogique.

Les opérations à effectuer sont les suivantes :

Etape 1 : Créer une « connexion PPP distante » sur le PC
(voir annexe 2).

Etape 2 : S'identifier et appeler

- Cliquer droit sur la « connexion distante » et sélectionner « connecter ».
- Saisir le **nom d'utilisateur** « admin » et le **mot de passe** « admin » pour être reconnu dans la liste des utilisateurs autorisés.
- Saisir le N° de téléphone à composer et valider.
- Attendre la connexion.

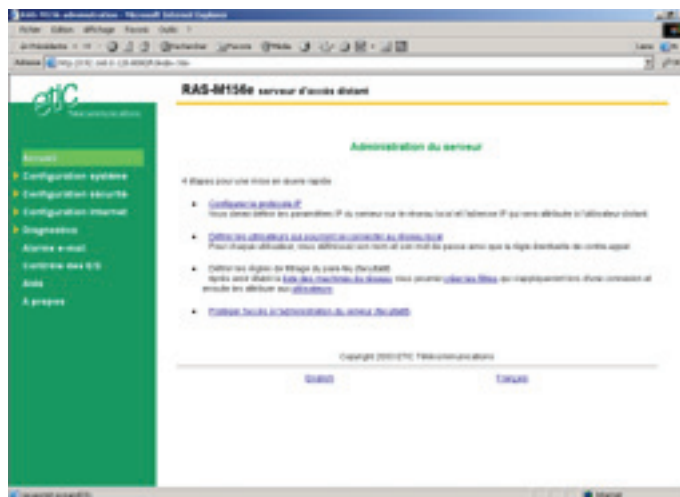


Etape 3 : Lancer le navigateur

Ouvrir le navigateur et saisir l'adresse IP du serveur d'administration du routeur qui a été programmée en usine : 192.168.0.128 (ne pas faire précéder (l'adresse des caractères www).

Note : La valeur de « l'adresse usine » est inscrite sur l'étiquette apposée sur le côté du produit face à la mention « adresse IP du routeur ».

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



Note : A la première configuration, l'accès au serveur web n'est pas protégé ; voir paragraphe 7.4.1 pour protéger l'accès au serveur d'administration.

5 Modification de la configuration à distance

Comme la configuration initiale, la modification de la configuration peut s'effectuer à distance.

Attention, l'accès au serveur d'administration peut être restreint ou interdit.

Après avoir lancé le navigateur, si vous ne parvenez pas à vous connecter à distance au serveur d'administration, il se peut que ce soit pour l'une des raisons suivantes :

Si la fenêtre de demande d'identification ne s'affiche pas :

- L'accès au serveur d'administration par le réseau téléphonique a été interdit ou limité (il faut appuyer sur le poussoir CONF. De la face avant du produit).
- Ou bien, l'adresse IP saisie est fausse.

Si la fenêtre de demande d'identification s'affiche, mais pas la page web :

- Le nom d'utilisateur ou le mot de passe d'accès au serveur d'administration sont erronés.

Voir paragraphe 6 ci-dessous.

6 Perte du mot de passe et / ou d'adresse IP

Perte de l'adresse IP du serveur d'administration

En cas de perte de l'adresse IP du serveur d'administration, il devient impossible d'y accéder.

On peut pallier cette difficulté en plaçant le switch SW01 sur la position ON.

L'adresse IP « Usine » 192.168.0.128 est restituée tant que le switch SW01 est sur ON.

Perte du nom d'utilisateur et du mot de passe autorisant l'accès au serveur d'administration

En cas de perte du nom d'utilisateur et du mot de passe autorisant l'accès au serveur d'administration, il devient impossible d'y accéder.

On peut pallier cette difficulté en plaçant le switch SW03 sur la position ON.

Le serveur d'administration devient accessible **depuis le réseau local** sans aucun mot de passe tant que le switch SW03 est sur ON

7 Paramétrage du routeur

Certains paramètres ne sont pris en compte par le routeur IPL qu'après redémarrage complet du produit.

Lorsque l'on effectue la configuration à distance, ceci a en plus pour effet de libérer la ligne (couper la liaison).

Il est donc conseillé d'opérer comme suit :

- **Après chaque modification, cliquer le bouton « enregistrer » placé en bas de chaque page de paramétrage.**
- **Lorsque le paramétrage est terminé, pour que les modifications soient prises en compte, cliquer le bouton « redémarrer » de couleur rouge qui apparaît en bas de la barre verte de menu.**
Le routeur coupe la liaison RTC ou RNIS ou GSM si elle était établie et redémarre (la durée du redémarrage est de 10 sec. Environ).
- **Fermer le navigateur html**, puis l'ouvrir à nouveau pour contrôler que le paramétrage a correctement été pris en compte.
Le bouton « redémarrer » doit avoir disparu.
- Si nécessaire, sauvegarder le fichier de configuration sur le disque dur du PC au moyen du menu Configuration Système puis Sauvegarde / Restauration.

Attention : Le bouton « redémarrer » est situé sous le dernier menu de la barre de couleur verte; il peut ne pas apparaître à l'écran si tous les menus sont ouverts ; contrôler en utilisant la barre de navigation.

7.1 Arborescence du serveur d'administration

Configuration Système

Protocole IP	Enregistrer l'@ IP attribuée au routeur IPL. Enregistrer l'@IP attribuée à l'utilisateur distant.
Liste des machines	Enregistrer les machines IP auxquelles s'appliquera le fire-wall et constituer le « portail » d'accueil.
Date et heure	Mettre à jour la date et l'heure.
Modem	Activer le modem externe, choisir le type et modifier la séquence d'init. du modem (si nécessaire).
RS232/RS485	Fixer le débit / format / contrôle de flux de la liaison RS.
RIP	Activer l'échange de tables de routage entre routeurs sur le réseau local.
SNMP	Activer l'agent SNMP du routeur IPL (Simple Network Management Protocol).
Mise à jour	Charger un nouveau logiciel dans le produit.
Sauvegarde / restauration	Sauvegarder la configuration du produit dans un fichier du PC, ou au contraire, la charger dans le produit.
Redémarrer	Initialiser le routeur IPL lorsque les modifications du paramétrage rendent cette opération nécessaire.

Routage & Accés distant

Utilisateurs	Enregistrer la liste d'utilisateurs autorisés et leur attribuer des droits (voir pare-feu).
Nœuds distants	Définir les caractéristiques des routeurs(=nœuds) susceptibles de s'interconnecter avec le routeur IPL.
Routes statiques	Pour les routeurs non accessibles directement, définir la passerelle permettant d'y accéder.

Configuration sécurité

Droits d'administration	Protéger et limiter l'accès au serveur d'administration.
Pare-feu	Constituer les filtres qui limitent l'accès aux machines et applications (ports) du réseau local.

Configuration Internet

Compte	Enregistrer les paramètres de l'abonnement Internet du routeur IPL.
Routage	Sélectionner et paramétrer le routage vers Internet.
VPN	Paramétrer le fonctionnement de la communication distante par Internet.

Passerelle IP <- > RS

Unitelway	Configuration de la passerelle unitelway.
Modbus	Configuration de la passerelle modbus.
Transparent	Configuration des passerelles Telnet et RAW TCP.

Diagnostic

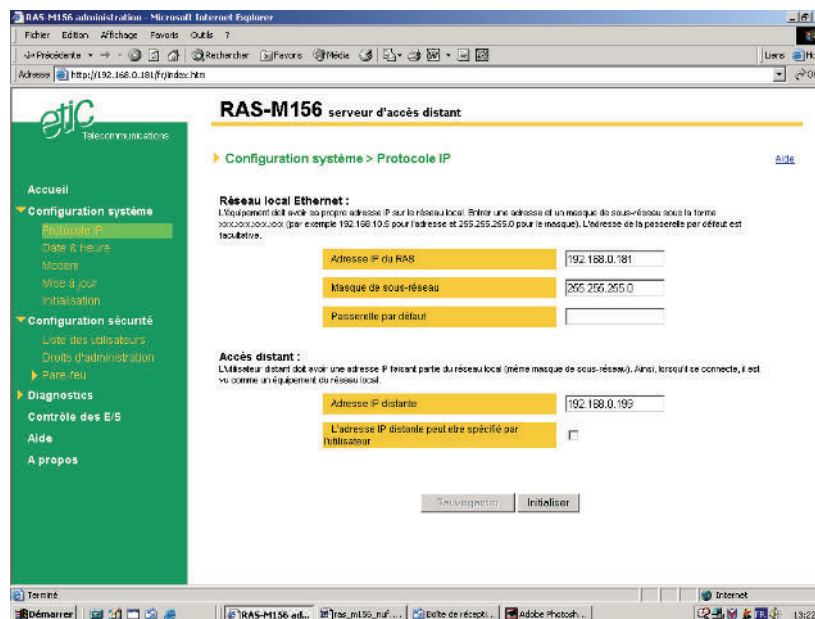
Journal	Visualiser la liste horodatée des utilisateurs qui se sont connectés à distance au réseau local.
Etat du réseau	Afficher l'état actuel du produit : @ MAC, @IP, utilisateur actuellement connecté à distance
Etat des interrupteurs	Afficher l'état actuel des DIP switches.
Table de routage	Afficher la table de routage du routeur IPL.
Ping	Tester le fonctionnement du système.
Syslog	Activer l'exportation du journal système vers un serveur SYSLOG du réseau local.
Contrôle des E/S	Visualiser l'état des 3 ETOR, commander la STOR.
Récapitulatif	Visualiser le tableau récapitulatif de tous les paramètres.

Alarme e-mail	Paramétrer l'envoi d'alarmes par e-mail.
----------------------	--

A propos	Afficher les informations d'identification du produit.
-----------------	--

7.2 Menu « Configuration système »

7.2.1 Menu « Protocole IP »



Adresse IP du produit

C'est l'adresse IP du routeur IPL sur le réseau local. Elle permet aussi d'accéder au serveur d'administration (à distance ou par Ethernet).

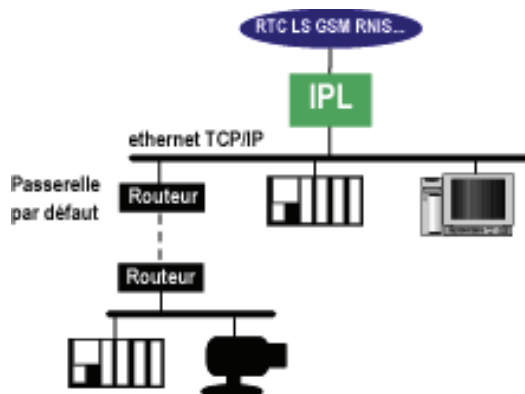
Masque de sous-réseau (netmask)

Saisir le masque de réseau, qui définit la structure des adresses IP de toutes les stations d'un segment de réseau local.

La valeur de ce masque doit être fournie par le responsable du réseau ; cependant, on notera que dans les réseaux de 256 stations, le masque de sous-réseau est 255.255.255.0.

Passerelle par défaut :

Saisir l'adresse IP de la passerelle (routeur) par défaut du réseau local. Il est nécessaire de saisir cette adresse lorsque le réseau local comporte un autre routeur et que certaines stations doivent être jointes à travers ce routeur.



Début du pool d'adresse IP utilisateurs

Il s'agit de la première adresse de l'ensemble des adresses IP qui seront automatiquement attribuées à un **utilisateur distant** lorsqu'il se connectera. Cette adresse doit être cohérente avec le masque de sous réseau, et non attribuée par ailleurs à une machine du réseau local.

7.2.2 Menu « Liste des machines »

Ce menu permet de désigner les machines du réseau local et de fixer certains paramètres associés.

La liste des machines permet ensuite de construire le firewall et de constituer le « portail » qui peut être affiché comme page d'accueil de l'utilisateur distant.

Paramètre Nom du site :

Le nom du site est le libellé qui s'affiche en haut à droite de toutes les pages du serveur d'administration et du portail.

Paramètre Nom de domaine du site :

Le nom de domaine est le suffixe DNS que l'on peut saisir pour accéder à une machine.

Par exemple, si l'on désigne une machine par le libellé « **assemblage** » et que l'on a saisi « **grenoble** » pour nom de domaine du site, on peut accéder aux services web de cette machine en tapant « **assemblage.grenoble** » dans le masque de saisie d'adresse du navigateur html.

Option « Afficher le portail web »

L'option « Afficher le portail web » force, lorsqu'elle est cochée, l'affichage de la page « portail » comme page d'accueil html à la connexion d'un utilisateur distant. (voir chapitre Utilisation).

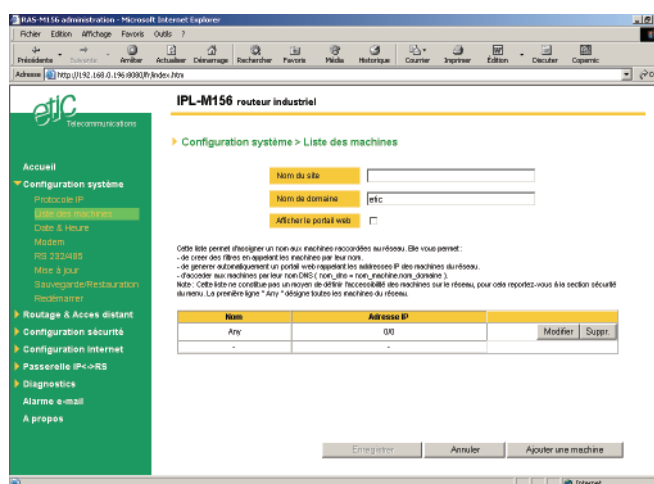
Tableau de liste des machines

Pour ajouter une machine à la liste,

- Cliquer le bouton « Ajouter une machine » en bas de l'écran.
- Enregistrer un libellé (le nom que vous souhaitez donner à la machine) et son adresse IP.
- Valider. La machine qui vient d'être créée apparaît maintenant dans la liste des machines. Elle sera affichée dans la page « portail ».

Pour supprimer une machine de la liste,

- Assurez-vous au préalable que la machine à supprimer n'intervient pas dans une règle de firewall ; si la machine intervient dans une règle de firewall, et que le filtre a en plus été affecté à un ou plusieurs utilisateurs, retirer d'abord ce filtre aux utilisateurs en accédant à la fiche de chacun d'entre eux, puis ensuite supprimer ou modifier le filtre ; alors seulement, il devient possible de supprimer une machine.
- Cliquer le bouton « Suppr. »
- Valider ; la machine ne fait plus partie de la liste des machines.



7.2.3 Menu « date et heure »

Il permet de remettre à l'heure et à la bonne date le routeur IPL.
Il est important que le routeur IPL soit à l'heure et la date juste si l'on veut pouvoir exploiter les informations enregistrées dans le journal.

7.2.4 Menu « modem »

Ce menu permet de paramétrer le fonctionnement du modem interne du routeur (sauf cas du routeur IPL-RS232 qui n'inclut pas de modem interne) et du modem externe éventuellement raccordé à la liaison RS232.

MODEM INTERNE

Paramètre « préfixe de numérotation »

Saisir le préfixe qui doit être composé par le modem avant le N° d'appel du nœud distant.

Note : Dans le cas du routeur IPL-L134 fait pour la communication sur liaison spécialisée aucun préfixe ne doit être saisi.

Paramètre « Utiliser la séquence d'initialisation par défaut » et « Spécifier une chaîne d'initialisation »

Le modem (RTC ou LS ou RNIS ou GSM) est intégré dans le routeur IPL qui en assure le contrôle.

La séquence par défaut que le routeur transmet au modem intégré ne doit être modifiée qu'en cas de difficulté de communication et après avoir pris l'avis de notre service après-vente.

- Pour modifier la séquence d'initialisation, cocher le bouton radio « Spécifier une chaîne d'initialisation », puis saisir la nouvelle séquence.

Paramètre « Liaison permanente (LS) » (ref. IPL-L134 seulement)

Dans le cas de l'utilisation du routeur IPL-L134 pour la communication sur liaison spécialisée, ce paramètre doit être coché.

Paramètre « Reporter l'état de la connexion sur la sortie TOR »

Si cette case est cochée, la sortie TOR est fermée lorsque le routeur est connecté à un autre routeur via la liaison modem ; elle est ouverte autrement.

Note : Si cette case est cochée, la sortie TOR ne peut plus être télécommandée via le serveur web (menu diagnostic puis Contrôle des E/S).

Paramètre « Pays d'installation du routeur »

Sélectionner le pays dans lequel doit être installé le routeur ; pour l'Europe, et la France en particulier, sélectionner la valeur « International ».

MODEM EXTERNE

Les paramètres qui suivent permettent de régler le fonctionnement du routeur lorsqu'on utilise un modem raccordé à la liaison RS232 ou RS485.

Paramètre « activer »

Si un modem est raccordé à la liaison RS232-RS485 pour établir un lien IP longue distance (liaison PPP), cocher la case « activer ».

Note : Dans ce cas, la liaison RS232-RS485 n'est plus utilisable pour le raccordement d'un équipement d'automatisme ou autre (fonction passerelle IP/RS).

Paramètre « préfixe de numérotation »

Saisir le préfixe qui doit être composé par le modem externe avant le N° d'appel du nœud distant.

Paramètre « Liaison permanente (LS) »

Si le modem externe est un modem pour la communication sur liaison spécialisée, ce paramètre doit être coché.

Paramètre « Spécifier une chaîne d'initialisation »

Saisir la séquence d'initialisation qui doit être transmise au modem via la liaison RS232.

Paramètre « Reporter l'état de la connexion sur la sortie TOR »

Si cette case est cochée, la sortie TOR est fermée lorsque le routeur est connecté à un autre routeur via la liaison RS232 et le modem externe; elle est ouverte autrement.

Note : Si cette case est cochée, la sortie TOR ne peut plus être télécommandée via le serveur web (menu diagnostic puis Contrôle des E/S).

7.2.5 Menu RS232 RS485

Ce menu permet de fixer les paramètres de fonctionnement de la liaison RS232 / RS485, soit qu'elle soit utilisée pour connecter un modem externe ou bien pour réaliser la fonction de passerelle IP / RS.

7.2.6 Menu RIP

Ce menu permet d'activer l'agent RIP du routeur IPL. Le protocole RIP (Routing Information Protocol) permet l'échange de tables de routage entre routeurs. Ce protocole agit uniquement sur le réseau local Ethernet.

Note : Certains systèmes tel que Windows 2000 possèdent un « écouteur RIP » leur permettant de connaître les différents réseaux accessibles à travers les routeurs du réseau local.

7.2.7 Menu SNMP

Ce menu permet d'activer l'agent SNMP inclus dans le routeur IPL. SNMP (Simple Network Management Protocol) est un protocole de supervision de réseaux, une console SNMP pourra donc interroger le routeur IPL pour connaître son état.

7.2.8 Menu « sauvegarder / restaurer »

Ce menu permet de sauvegarder sur le disque d'un PC l'ensemble des paramètres de la configuration du routeur IPL ou au contraire de charger vers le routeur IPL un fichier de configuration préalablement sauvegardé.

7.2.9 Menu « Redémarrer »

Ce menu permet d'initialiser le routeur IPL.

7.3 Menu « Routage et accès distant »

Ce menu permet de désigner en détail les **nœuds distants** et les **utilisateurs autorisés**.

Les nœuds distants sont les routeurs distants qui constituent le réseau étendu.

Les utilisateurs distants sont les utilisateurs autorisés à accéder au réseau local au moyen d'un PC et d'un modem; certaines particularités de fonctionnement leur sont appliquées telles que le « call-back », l'attribution automatique d'une adresse IP ou encore l'affichage du portail web.

7.3.1 Liste d'utilisateurs

Afficher la liste des utilisateurs

- Cliquer sur « Routage & Accès distant » puis sur « liste d'utilisateurs ».

La liste des utilisateurs autorisés s'affiche :

Chaque ligne de la liste comporte 2 champs : Le nom de l'utilisateur et le filtre de pare-feu qui lui est affecté.

A la livraison, elle comporte l'utilisateur « default user » dont les caractéristiques sont les suivantes :

Nom d'utilisateur : admin

Mot de passe : admin

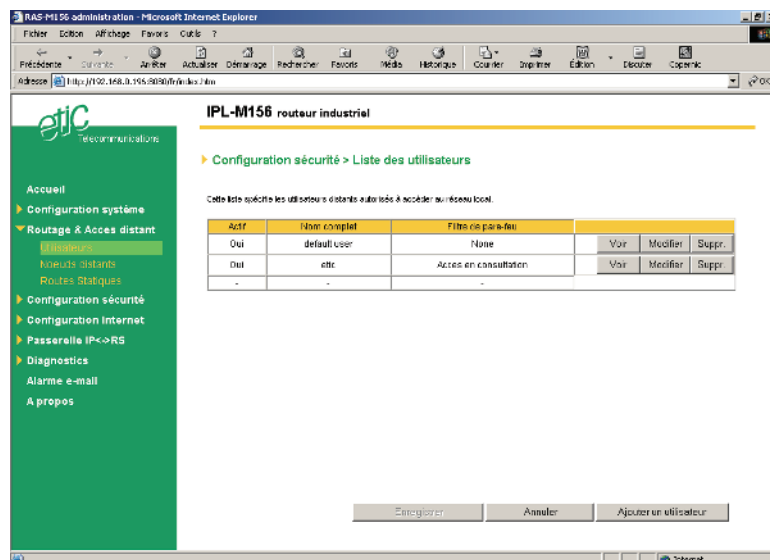
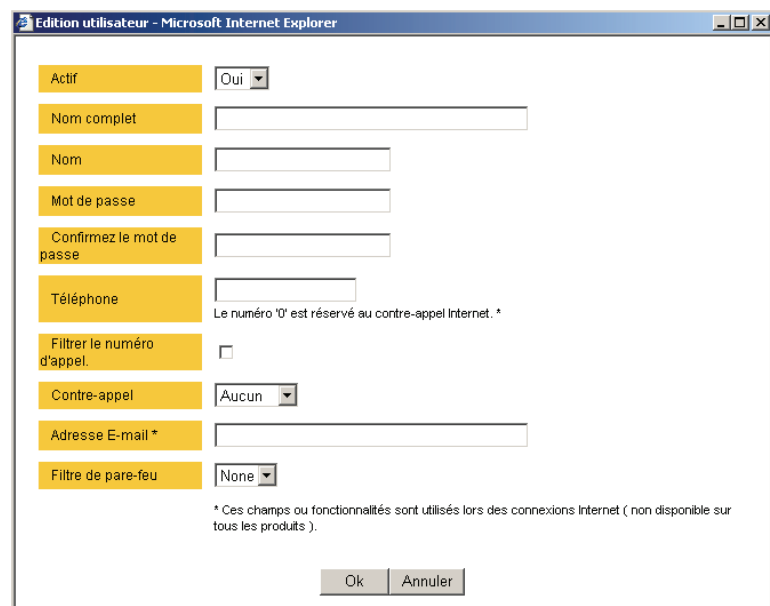
Visualiser ou modifier la fiche d'un utilisateur

- cliquer sur le bouton « Voir » ou bien sur « Modifier »

Ajouter un utilisateur

- Cliquer sur le bouton « ajouter un utilisateur ».

Saisir les paramètres et valider.

The screenshot shows the 'Edition utilisateur' form. It contains several input fields and dropdown menus for user configuration. The fields are: 'Actif' (dropdown with 'Oui'), 'Nom complet' (text input), 'Nom' (text input), 'Mot de passe' (text input), 'Confirmez le mot de passe' (text input), 'Téléphone' (text input), 'Filtrer le numéro d'appel' (checkbox), 'Contre-appel' (dropdown with 'Aucun'), 'Adresse E-mail *' (text input), and 'Filtre de pare-feu' (dropdown with 'None'). A note at the bottom states: '* Ces champs ou fonctionnalités sont utilisés lors des connexions Internet (non disponible sur tous les produits).' Buttons for 'Ok' and 'Annuler' are at the bottom.

Le paramètre « Actif » (valeur OUI ou NON) permet de désactiver temporairement un utilisateur de la liste.

Le paramètre « Nom complet » est le libellé qui apparaît dans le premier champ de la liste des utilisateurs autorisés.

Les paramètres « Nom d'utilisateur » et « mot de passe » 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.

Le nom d'utilisateur n'a pas à être tenu secret ; il apparaît donc toujours en clair ; il permet en particulier de garder la trace de chaque connexion de l'utilisateur dans le journal.

Le mot de passe doit être gardé secret par chaque utilisateur ; il n'apparaît jamais en clair. Ces paramètres doivent contenir au moins deux caractères.

Le paramètre « Téléphone » contient le N° de la ligne de l'utilisateur. Ce N° est utilisé par le routeur soit pour le filtrage d'appel, soit pour le call-back (voir ci-dessous).

Le paramètre « Filtrer le N° d'appel » permet de n'accepter les appels d'un utilisateur qu'en provenance du N° de téléphone enregistré (paramètre « Téléphone »). Ainsi, par exemple, l'appel de l'utilisateur ETIC peut n'être accepté que s'il appelle depuis la ligne 04 76 04 20 00.

Le paramètre « call-back » permet de déterminer comment la connexion téléphonique doit être établie une fois qu'un utilisateur s'est correctement identifié.

Call-back = Aucun : Après s'être correctement identifié, l'utilisateur accède directement au réseau local.

Call back = Autorisé : Une fois qu'il s'est correctement identifié, l'utilisateur peut accéder directement au réseau local ou spécifier un N° auquel il demande à être rappelé pour imputer le coût de la communication à la ligne du routeur IPL.

Call-back = Forcé : Une fois qu'il s'est correctement identifié, le routeur IPL coupe la communication et rappelle au N° enregistré (paramètre Téléphone)

Le paramètre e-mail

Cette adresse mail peut être utilisée par le routeur IPL dans deux cas :

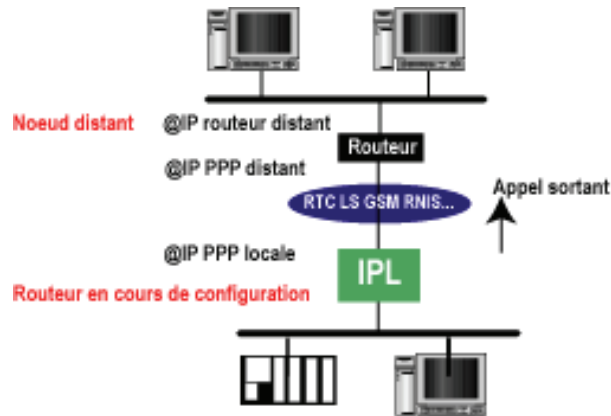
- soit pour transmettre un e-mail d'alarme à la suite du passage en défaut de l'entrée TOR,
 - soit lorsque l'utilisateur souhaite se connecter par l'Internet ; dans ce cas, l'adresse IP du routeur peut lui être transmise par e-mail.
- (voir chapitre UTILISATION)

Paramètre « Filtre pare-feu »

Sélectionner le filtre à affecter à cette liaison. Le filtre doit avoir été défini par ailleurs (cf 7.4 Menu « Configuration sécurité »).

7.3.2 Menu « Nœuds distants »

Ce menu permet de désigner en détails les routeurs (nœuds distants) avec lesquels devra communiquer le routeur dont la configuration est en cours.



Pour ajouter un nœud distant au réseau étendu, cliquer le bouton « ajouter un nœud » ; la fiche du nouveau nœud apparaît.

Paramètre « actif »

Sélectionner Oui pour faire en sorte que le nœud distant soit ajouté au réseau.

Sélectionner Non, pour retirer le nœud du réseau tout en conservant ses paramètres en mémoire.

Paramètre « Nom »

C'est un libellé qui désigne le nœud ; éviter les caractères accentués.

Paramètre « Direction d'appel »

- Choisir « Sortante » si la connexion doit être établie uniquement à l'initiative du routeur en cours de configuration vers le nœud distant (le routeur appelle le nœud distant ; pas d'appel entrant).
- Choisir « Entrante » si la connexion doit être établie uniquement à l'initiative du nœud distant (appel entrant uniquement).
- Choisir « Entrante et sortante » si la connexion peut être établie à l'initiative de l'un ou de l'autre.

@IP du routeur distant et Masque réseau distant

Saisir l'adresse IP du routeur du nœud distant ainsi que le masque du réseau distant.

Paramètre « Modem »

Indiquer si la connexion avec ce nœud distant doit utiliser le modem interne ou le modem externe ou indifféremment l'un ou l'autre.

Note : le choix n'est offert que si la liaison RS232 a au préalable été affectée à la connexion d'un modem externe.

Paramètre « Numéro d'appel »

Saisir le N° d'appel que doit composer le routeur pour atteindre le nœud distant.

Paramètre « Mon identifiant » et « Mon mot de passe »

Saisir l'identifiant et le mot de passe que **le routeur utilisera pour s'authentifier auprès du routeur distant** lors d'une connexion sortante.

Paramètre « Identifiant du nœud » et « Mot de passe du nœud »

Saisir l'identifiant et le mot de passe que **le routeur distant devra fournir pour être accepté** lors d'une connexion entrante. Ces paramètres sont obligatoires.

Paramètre « Time-out inactivité »

Si aucun paquet IP n'est reçu ou transmis sur la liaison PPP pendant ce temps, le routeur libère la ligne.

Paramètre « Time-out premier paquet »

Dès qu'il est connecté, le routeur se met en attente de paquets IP à transmettre ou recevoir. Si aucun paquet n'a été reçu ou transmis à l'échéance de ce délai, la ligne est libérée.

Paramètre « Vérifier le N° d'appelant »

Si le choix « Oui » est sélectionné, lors d'un appel entrant, le routeur établit la connexion et enregistre l'identifiant et le mot de passe reçus du nœud distant ; si ces codes ne sont pas en accord avec le N° d'appel, le routeur libère la ligne.

Paramètre « Filtre pare-feu »

Sélectionner le filtre à affecter à cette liaison. Le filtre doit avoir été défini par ailleurs (cf 7.4 Menu « Configuration sécurité »).

Paramètre « NAT »

Si le choix « Oui » est sélectionné, le routeur présente toute station du réseau local avec une adresse unique (sa propre adresse).

Paramètre « @IP PPP locale »

Saisir, si nécessaire, l'adresse IP du routeur sur la liaison PPP.

Paramètre « @IP PPP distante »

Saisir, si nécessaire, l'adresse IP du routeur du nœud distant sur la liaison PPP.

7.3.3 Menu « Routes statiques »

Lorsque le réseau destinataire ne peut être atteint directement, il est nécessaire d'indiquer au routeur quelle est la route permettant d'y accéder.

Sélectionner le menu « Route statique » puis cliquer « Ajouter une route ».

Paramètre « actif »

Cliquer « oui » pour rendre la route active.

Cliquer « Non » pour désactiver temporairement la route sans effacer ses paramètres.

Paramètre « Nom de la route »

Désigner la route par un libellé; les caractères accentués ne sont pas acceptés.

Paramètre « @IP réseau »

C'est l'adresse IP générique du réseau à atteindre ; elle est obtenue en remplaçant par 0 les chiffres variables des stations de ce réseau.

Paramètre « masque réseau »

C'est le masque du réseau à atteindre.

Paramètre « @IP passerelle »

C'est l'adresse du routeur par lequel il faut faire transiter les trames IP pour atteindre le destinataire.

7.4 Menu « Configuration sécurité »

Ce menu permet de déterminer les règles d'accès aux machines et applications du réseau local (firewall), ainsi qu'au serveur de configuration du routeur.

7.4.1 Menu « droits d'administration »

Le menu « Droits d'administration » permet de limiter ou interdire l'accès à distance au serveur d'administration du routeur et de programmer le nom d'utilisateur et le mot de passe qui en protègent l'accès.

Administration par le réseau Ethernet

Elle est toujours possible cependant, elle peut être limitée en obligeant l'opérateur à appuyer sur le poussoir de la face avant du produit.

- Sélectionner « toujours autorisé » pour autoriser l'accès à l'administration avec uniquement un nom d'utilisateur et un mot de passe.
- Sélectionner « après appui sur le poussoir CONF. » pour n'autoriser l'accès à l'administration que lorsqu'un opérateur a appuyé sur le poussoir CONF de la face avant du routeur.

Administration à distance

Elle peut être interdite ou bien autorisée temporairement ou bien autorisée sans restriction.

- Sélectionner « Interdit » pour interdire l'accès à l'administration par le réseau téléphonique.
- Sélectionner « Autorisé après appui sur le poussoir CONF » pour autoriser l'accès à l'administration à distance uniquement si un opérateur a appuyé au préalable sur le poussoir CONF.
Ce choix permet à un opérateur situé sur site de n'autoriser l'accès à la configuration que lorsqu'il l'estime nécessaire.
Le nom d'utilisateur et le mot de passe restent nécessaires pour accéder au serveur.
- Sélectionner « toujours autorisé » pour autoriser l'accès à l'administration par le réseau téléphonique avec uniquement un nom d'utilisateur et un mot de passe.

Nom d'utilisateur et mot de passe

- Saisir le nom d'utilisateur et le mot de passe d'accès au serveur d'administration et confirmer. Si un couple nom d'utilisateur / mot de passe vide est saisi, la protection d'accès est désactivée.

Attention : En cas de perte du nom d'utilisateur et du mot de passe d'accès au serveur d'administration, on peut restituer un accès libre au serveur **d'administration via l'interface Ethernet uniquement** en plaçant le micro-switch N°3 sur la position ON. Pour accéder aux micro-switches, mettre le routeur hors tension, puis retirer la trappe de la face supérieure du boîtier.

7.4.2 Menu Pare-feu

Ce menu permet de définir une liste de filtres qui constituent le pare-feu (25 filtres au maximum).

Fonction des filtres du pare-feu (firewall)

Un filtre définit un ensemble de machines du réseau et de services de chacune de ces machines qui sont rendus accessibles ou au contraire interdits.

Une fois que tous les filtres sont composés, on les attribue individuellement à chaque nœud ou à chaque utilisateur.

Structure d'un filtre

Un filtre est un tableau dont chaque ligne est appelé « règle ».

Une règle définit une autorisation ou une interdiction d'accès à une machine (définie par son adresse IP) et à un service de cette machine (N° de port et protocole sous-jacent).

Exemple de filtre

Nom du filtre : Accès aux serveurs web de deux machines

Politique	Interdire l'accès à toute machine sauf celles qui sont autorisées ci-dessous.
Règle 1	Autoriser l'accès à la machine d'adresse IP 200.200.200.71 et, à cette adresse, au service html.
Règle 2	Autoriser l'accès à la machine d'adresse IP 200.200.200.80 et, à cette adresse, au service html.

Composer un filtre « Tout est interdit sauf ... »

Ainsi, pour composer un filtre on peut d'abord interdire toutes les adresses IP et services du réseau local, puis autoriser l'accès à certaines machines et certains services explicitement désignés par les règles successives du tableau; c'est la manière la plus prudente de rédiger un filtre.

Pour cela, il faut cliquer « On désigne ce que l'on autorise et tout le reste est interdit ».

Composer un filtre « Tout est autorisé sauf ... »

Pour composer un filtre, on peut aussi autoriser toutes les adresses IP et services du réseau local, puis interdire spécifiquement l'accès à certaines machines et certains services explicitement désignés par les règles successives du tableau; pour cela il faut cliquer « On désigne ce que l'on interdit et tout le reste est autorisé ».

On ne procédera ainsi que dans les cas simples, car on notera que si une nouvelle machine est connectée sur le réseau local, elle devient immédiatement et automatiquement accessible.

Pour définir la liste des filtres on procède par étapes :

Etape 1 :

On complète éventuellement la liste des machines accessibles
Se reporter au chapitre 7.2.2 Menu « Liste des machines ».

Etape 2 :

On complète éventuellement la liste des services accessibles

Etape 3 :

On compose les filtres l'un après l'autre (menu Liste des filtres)

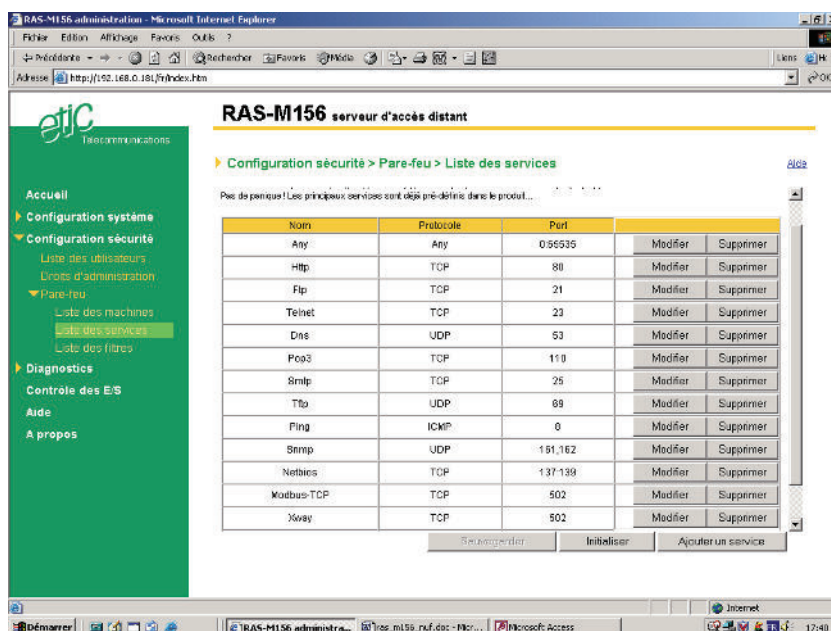
Etape 4 :

En retournant à la liste d'utilisateurs autorisés, on affecte un filtre à chaque utilisateur pour limiter les machines et services auxquels il pourra accéder.

Etape 2 : Ajouter des services à la liste des services

Note importante : de nombreux services sont créés en usine, tel que html, ftp etc..., si bien que dans la plupart des cas, cette étape peut être passée.

- Sélectionner le menu « configuration de la sécurité » puis « pare-feu » puis « Liste des services » ; la liste des services déjà enregistrés s'affiche.
- Ajouter un nouveau service en cliquant le bouton « Ajouter un service » en bas de l'écran.
- Enregistrer un libellé (le nom que vous souhaitez donner au service), sélectionner un protocole dans la liste proposée (udp, tcp, icmp) et désigner le N° de port attribué à ce service.
- Valider. Le service qui vient d'être créé apparaît maintenant dans la liste des services.



RAS-M156 serveur d'accès distant

Configuration sécurité > Pare-feu > Liste des services

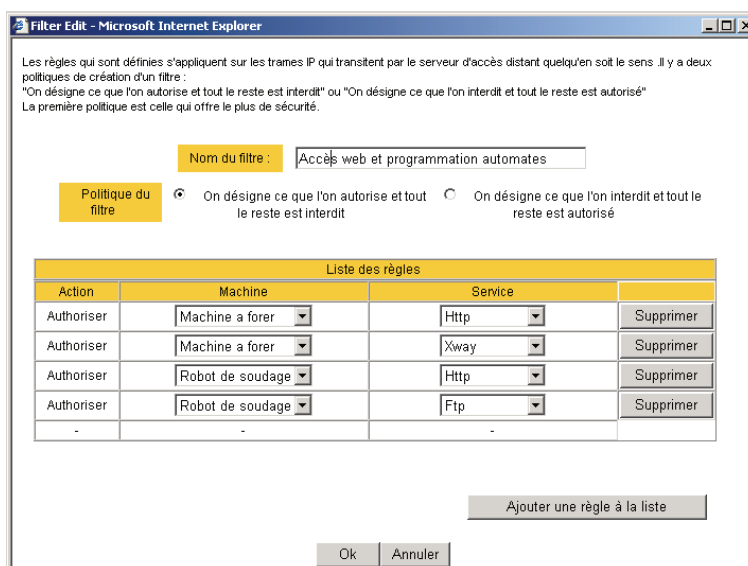
Pas de panique ! Les principaux services sont déjà pré-définis dans le produit...

Nom	Protocole	Port	Modifier	Supprimer
Any	Any	0-65535	Modifier	Supprimer
Http	TCP	80	Modifier	Supprimer
Ftp	TCP	21	Modifier	Supprimer
Telnet	TCP	23	Modifier	Supprimer
Dns	UDP	53	Modifier	Supprimer
Pcp3	TCP	119	Modifier	Supprimer
Smtp	TCP	25	Modifier	Supprimer
Tftp	UDP	69	Modifier	Supprimer
Ping	ICMP	0	Modifier	Supprimer
Sntp	UDP	151,162	Modifier	Supprimer
Netbios	TCP	137-139	Modifier	Supprimer
Modbus-TCP	TCP	502	Modifier	Supprimer
Xway	TCP	502	Modifier	Supprimer

Sauvegarder Initialiser Ajouter un service

Etape 3 : Composer un filtre

- Sélectionner le menu « sécurité » puis « pare-feu » puis « Liste des filtres » ; la liste des filtres déjà enregistrés s'affiche.
- Créer un nouveau filtre en cliquant le bouton « Nouveau filtre ».
- Saisir un libellé (le nom que vous souhaitez donner au filtre) ; exemple de libellé : Accès au serveur web de l'automate N°1
- Cliquer sur le bouton radio « On désigne ce que l'on autorise et tout le reste est interdit » si vous souhaitez que chaque règle désigne ensuite une machine explicitement autorisée ; c'est la solution prudente.
- Cliquer sur le bouton radio « On désigne ce que l'on interdit et tout le reste est autorisé » si vous souhaitez que chaque règle désigne ensuite une machine interdite.
- Cliquer sur le bouton « ajouter une règle » ; une ligne s'ajoute dans le tableau du filtre.
- Sélectionner une machine (autorisée ou interdite selon le cas) puis un service.
- Ajouter autant de règles que nécessaire en cliquant sur « ajouter une règle ».
- Lorsque le filtre est complet, valider en cliquant le bouton OK puis sauvegarder.
- La liste actualisée des filtres s'affiche.



Les règles qui sont définies s'appliquent sur les trames IP qui transitent par le serveur d'accès distant quelqu'en soit le sens. Il y a deux politiques de création d'un filtre :
 "On désigne ce que l'on autorise et tout le reste est interdit" ou "On désigne ce que l'on interdit et tout le reste est autorisé"
 La première politique est celle qui offre le plus de sécurité.

Nom du filtre :

Politique du filtre : ☒ On désigne ce que l'on autorise et tout le reste est interdit ☐ On désigne ce que l'on interdit et tout le reste est autorisé

Liste des règles			
Action	Machine	Service	
Authoriser	Machine a forer	Http	Supprimer
Authoriser	Machine a forer	Xway	Supprimer
Authoriser	Robot de soudage	Http	Supprimer
Authoriser	Robot de soudage	Ftp	Supprimer
-	-	-	

Ajouter une règle à la liste

Ok Annuler

Etape 4 : Affecter les filtres aux nœuds distants ou aux utilisateurs

Une fois la liste de filtres composée, il faut les rendre actifs en les affectant aux nœuds distants ou aux utilisateurs.

- Sélectionner le menu « Routage & accès distant » puis « Nœuds distants » ou bien « Utilisateurs » selon le cas.
- Sélectionner le nœud distant ou bien l'utilisateur de la liste auquel vous souhaitez affecter un filtre, en cliquant le bouton « Modifier » ; la fiche du nœud ou de l'utilisateur apparaît.
- Lui affecter un filtre en sélectionnant l'un des filtres proposés et valider par « OK ».
- Sauvegarder la liste d'utilisateurs modifiée en cliquant « sauvegarder la liste ».

7.5 Menu « configuration Internet»**7.5.1 Compte**

Il faut saisir dans cette page les paramètres de la connexion Internet du routeur; **Ces informations sont indiquées par votre fournisseur d'accès Internet.**

Paramètre « Activer la connexion Internet »

Si cette case n'est pas cochée, le routeur ne se connecte jamais à l'Internet.

Si cette case est cochée, le routeur peut se connecter à l'Internet

- soit lorsqu'un utilisateur en fait la demande pour la fonction d'accès distant avec tunnel VPN,
- soit pour envoyer un email d'alarme à la suite de la fermeture ou de l'ouverture de l'ETOR.

Note : le routeur ne routera des données vers l'Internet que si le paramètre « Router le trafic du LAN vers Internet » du menu « Routage » est activé.

Numéro de téléphone :

C'est le N° de téléphone que doit composer le routeur IPL pour se connecter au fournisseur de service Internet.

Nom d'utilisateur et mot de passe :

Ce sont les codes que doit fournir le routeur IPL lorsqu'il se connecte au fournisseur Internet.

Serveur de courriers sortants (SMTP) :

C'est le l'adresse du serveur SMTP pour les courriers à émettre; par exemple « smtp.free.fr ».

Adresse e-mail du compte :

C'est l'adresse e-mail associée au compte ; elle est utilisée par le fournisseur de services Internet pour identifier l'émetteur du courrier électronique.

7.5.2 Routage Internet

Paramètre « Router le trafic du LAN vers Internet » :

Le routeur IPL peut router vers Internet les trames IP provenant de son interface Ethernet et répondant aux conditions suivantes :

- L'adresse IP de destination ne correspond pas au masque de sous réseau de son interface Ethernet ;
- Elle ne correspond pas non plus à l'un des réseaux définis comme nœuds distants ;
- Elle ne correspond pas non plus à l'une des réseaux accessibles par l'une des routes statiques déclarées.

Pour sélectionner cette fonction, la case « Router le trafic du LAN vers Internet » doit être cochée.

Paramètre « Temps d'inactivité avant déconnexion » :

Lorsque le routeur se connecte à Internet parce qu'il doit router des données provenant d'une machine du réseau local, il reste connecté tant que le trafic IP ne s'interrompt pas durant cette temporisation programmable.

Note :

Cette temporisation ne s'applique que si la connexion à Internet a été initialisée par routage.

Si le routeur IPL s'est connecté à l'Internet à la suite de l'alarme de l'entrée 1, il se déconnecte dès que l'e-mail a été envoyé.

Si le routeur IPL s'est connecté à l'Internet à la demande de l'opérateur pour établir une connexion distante « VPN », cette temporisation ne s'applique pas non plus.

Paramètre « Temps d'attente premier paquet » :

Dès qu'il est connecté, le routeur se met en attente de paquets IP à transmettre ou recevoir. Si aucun paquet n'a été reçu ou transmis à l'échéance de ce délai, la ligne est libérée.

Paramètre « Utiliser le modem » :

Indiquer si la connexion Internet doit utiliser le modem interne ou le modem externe ou indifféremment l'un ou l'autre.

Note : le choix n'est offert que si la liaison RS232 a au préalable été affectée à la connexion d'un modem externe.

7.5.3 Menu « VPN »

Ce menu permet de déterminer les conditions de l'établissement d'une connexion sécurisée par Internet entre un utilisateur distant isolé (équipé d'un modem ou d'un abonnement adsl par exemple) et le routeur.

Cette connexion sécurisée, appelée aussi « tunnel VPN » permet à l'utilisateur d'accéder à chacune des machines du réseau comme s'il était sur place et dans la limite de ses droits.

Lors de l'utilisation, il faut tout d'abord connecter le routeur IPL à l'Internet puis établir une connexion sécurisée.

- **Connexion du routeur IPL à l'Internet**

4 possibilités sont offertes pour commander ou télécommander la connexion du routeur IPL à l'Internet en vue d'établir une liaison VPN avec un utilisateur distant. Le mode opératoire détaillé est donné au chapitre « Utilisation ».

Paramètre «Autoriser le contre-appel vers Internet » :

Si cette case est cochée, le routeur IPL se connecte à Internet chaque fois qu'un utilisateur distant lui en donne l'ordre en se connectant directement par le réseau commuté ou le RNIS ou le GSM.

Note : Un utilisateur ordonne à l'IPL de se connecter à Internet en entrant 0 (zéro) comme numéro de contre-appel.

Paramètre « Se connecter à Internet suite à un appel venant du »

Si un numéro de téléphone est spécifié, le routeur se connecte à Internet dès que le réseau (RTC, RNIS, GSM) présente un appel entrant en provenance de ce numéro. Le routeur ne prend pas l'appel, puis il se connecte automatiquement à l'Internet.

Paramètre « Se connecter à Internet à la mise sous tension »

Si cette case est cochée, le routeur IPL se connecte à Internet à chaque mise sous tension (commutateur 0/1 de face avant).

Paramètre «Se connecter à Internet à la fermeture de l'entrée 1»

Si cette case est cochée, le routeur IPL se connecte à Internet chaque fois que l'entrée TOR N°1 est fermée par un opérateur (au moyen d'un commutateur par exemple).

Bouton «Se connecter à Internet maintenant»

Si l'utilisateur clique le bouton « connecter », le routeur IPL se connecte immédiatement à Internet.

Quelle que soit la méthode retenue, et pour des raisons de sécurité, **le délai d'attente de la connexion de l'utilisateur sur l'Internet peut être limité au moyen du paramètre «Temps d'attente de la connexion VPN».**

Une fois que le routeur IPL est connecté à l'Internet, si l'abonnement est du type « à adresse IP dynamique », le routeur IPL obtient du fournisseur de service une adresse IP dont l'utilisateur distant doit avoir connaissance pour établir une connexion sécurisée.

Le routeur IPL peut transmettre cette adresse IP à l'utilisateur par deux moyens différents au choix : Soit par e-mail directement vers l'utilisateur, soit par le dépôt d'une page HTML sur serveur FTP identifié et protégé, que l'utilisateur vient consulter.

- **Transmission par e-mail de l' @ IP obtenue sur l'Internet**

Paramètres «Transmettre l'adresse IP par e-mail»

Si cette case est cochée, le routeur IPL transmet par e-mail, à l'utilisateur distant, l'adresse IP que lui a attribué le fournisseur d'accès Internet.

Paramètre «Email HTML avec lanceur VPN»

Si cette case est cochée, le routeur IPL ajoute à l'e-mail contenant l'adresse IP qui lui a été attribuée sur Internet, un « lanceur VPN » qui automatise la procédure VPN.

Note : Pour pouvoir utiliser le « lanceur VPN », une « connexion à un réseau privé via Internet » nommée « VPN » devra avoir été créée sur le PC client. Cette fonctionnalité est de plus réservée aux utilisateurs de Windows 2000, XP et ultérieurs.

Paramètre «Destinataire de l'email»

Ce paramètre permet de choisir le destinataire de l'e-mail contenant l'adresse IP attribuée au routeur IPL.

Lorsque le routeur IPL se connecte à Internet (à la mise sous tension, ou à la fermeture de l'entrée 1 ou lorsqu'un opérateur clique le bouton « Connecter »), il envoie à ce destinataire un email contenant l'adresse IP qui lui a été attribuée.

Note :

Si la connexion VPN est télécommandée grâce au « contre-appel Internet », l'email est envoyé automatiquement vers l'utilisateur distant qui s'est identifié lors du contre-appel.

- **Transmission vers un serveur FTP de l'adresse IP obtenue sur l'Internet**

Paramètre « Transmettre l'adresse IP vers un serveur FTP »

Si cette case est cochée, le routeur IPL transmet l'adresse IP qu'il a obtenue sur l'Internet vers un serveur FTP et sous forme d'une page HTML que l'utilisateur peut venir consulter.

Paramètres « Adresse du Serveur FTP » « Nom d'utilisateur », « mot de passe », « chemin du fichier à déposer » .

Ces paramètres identifient le serveur FTP dans lequel la page html sera chargée.

Note : Le chemin du fichier à déposer spécifiera le chemin proprement dit ainsi que le nom du fichier **sans extension** (l'extension .htm sera automatiquement ajoutée).

7.6 Menu « Passerelle IP<>RS »

Ce menu permet de sélectionner et de mettre en œuvre l'une des passerelles proposées : Modbus, unitelway, Telnet et RawTCP.

Une passerelle permet soit de connecter une station du réseau Ethernet avec un équipement RS232 / RS485, soit de réaliser cette fonction à partir d'un PC distant. Une passerelle peut aussi être simultanément active depuis le réseau local et à distance.

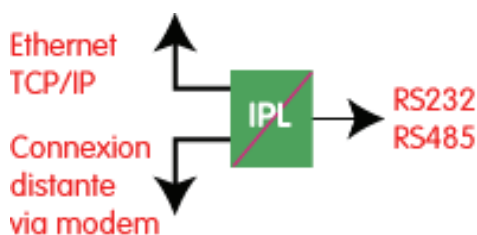
- **Passerelle entre le réseau IP et la liaison RS232-RS485 :**



- **Passerelle entre le réseau distant et la liaison RS232-RS485 :**



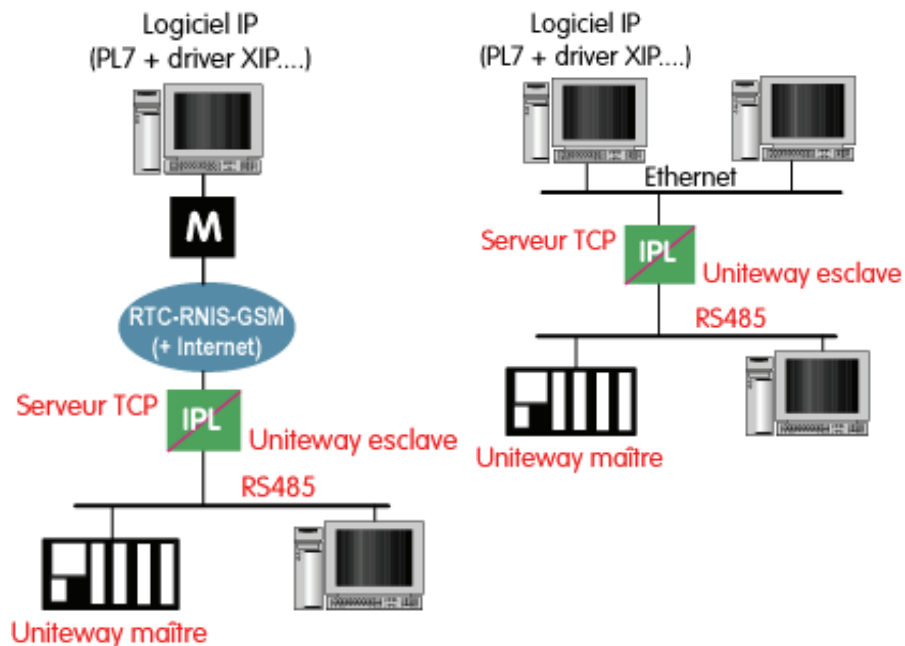
- **Passerelle simultanée :**



Note importante : la fonction passerelle ne peut être utilisée que si le port RS232-RS485 n'a pas été affecté à un modem pour réaliser un 2^{ème} port longue distance.

7.6.1 Menu « Passerelle Unitelway »

Le routeur IPL est serveur TCP sur Ethernet et sur la liaison RTC (ou RNIS ou GSM), et d'autre part esclave Unitelway sur la liaison RS232-485.



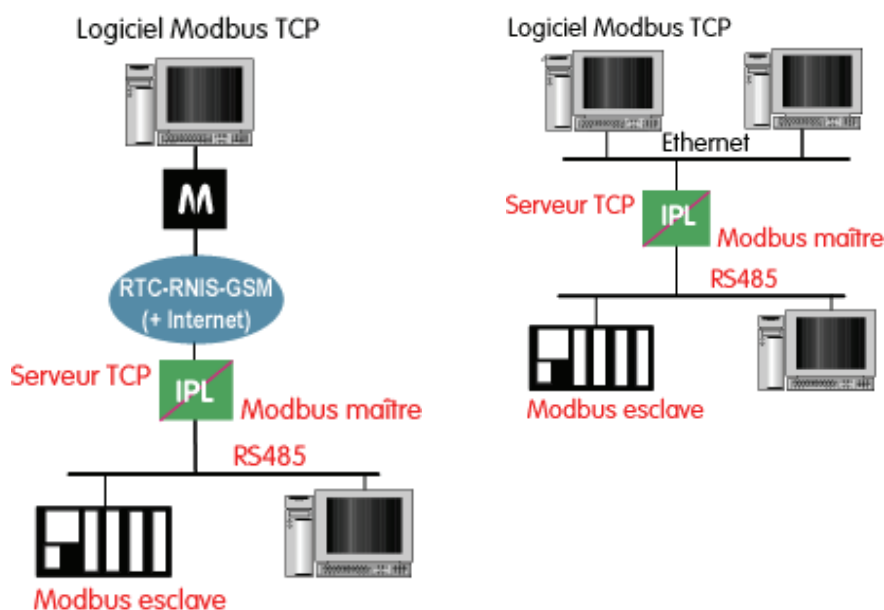
La passerelle Unitelway permet, d'intégrer des automates Unitelway dans un réseau IP.

On peut ainsi, par exemple, réaliser la fonction de télémaintenance d'automates Schneider Electric dans des conditions de sécurité maximum que ce soit par RTC, RNIS ou même par le réseau GSM et l'Internet.

- **Cliquer le menu Unitelway**
- **Cocher « activer la passerelle ».**
- **Désigner l'adresse Xway de l'automate maître et celle des automates esclaves éventuellement raccordés à l'interface RS485.**

7.6.2 Menu « Passerelle Modbus »

Le routeur IPL est serveur modbus TCP sur Ethernet et sur la liaison RTC, et d'autre part maître modbus sur la liaison RS232-485.



- Cliquer le menu modbus.
- Cocher « activer la passerelle ».
- Fixer le délai d'attente maximum de réponse de l'esclave modbus (time-out attente réponse).
- Fixer le temps maximum admissible entre caractères des réponses de l'esclave modbus (Temps inter-caractères).
- Fixer le nombre de réitération d'une question modbus par le routeur IPL en cas de non réponse de l'esclave modbus.

7.6.3 Menu passerelle transparente

Ce menu propose une passerelle transparente réalisée soit en mettant en œuvre l'application Telnet soit en utilisant le protocole « raw ».

- Si le mode Telnet est sélectionné, le routeur IPL est serveur Telnet sur Ethernet et sur la liaison RTC.
Le débit et le format de la liaison série peuvent être pilotés selon la recommandation RFC2217.
- Si le mode Raw TCP est sélectionné, on spécifie le « numéro de port TCP » à utiliser, la « Taille du buffer de réception RS232/485 » ainsi que le « Timeout fin de trame RS232/485 ».

Dans les 2 cas, le débit et le format de la liaison RS232/485 doit être sélectionné dans le menu « paramètres système » puis « RS232 ».

7.7 Menu « Diagnostic »

Il propose sous-menus suivants :

Voir le journal :

Le journal permet de visualiser l'enregistrement horodaté des connexions à distance et des connexions au serveur d'administration.
Il peut être imprimé.

Etat du réseau :

Cette page résume les caractéristiques que présente actuellement l'interface Ethernet, l'interface vers le réseau longue distance et la connexion sécurisée sur Internet.

Etat des interrupteurs :

Cette page affiche l'état présent des micro-switches situés sur la face supérieure du routeur IPL.

Table de routage :

Cette page affiche la table détaillée et de l'ensemble des routes actuellement enregistrées par le routeur.

Ping :

Pour émettre une trame « ping » vers une machine du réseau.

Syslog :

Cette page permet d'activer l'exportation du journal vers un serveur du réseau local (serveur SYSLOG).

Contrôle des E/S :

Cette page permet de visualiser l'état des 3 entrées TOR du routeur et de télécommander la sortie TOR au moyen des boutons de commande.

Récapitulatif :

Cette page se présente sous forme d'un tableau (imprimable) détaillant l'ensemble des paramètres enregistrés par le routeur.

7.8 Menu « Alarme e-mail »

Lorsque l'entrée TOR N°1 du routeur IPL (située sur le bornier à vis) change d'état, une alarme peut être envoyée, sous forme d'un e-mail (et donc d'un SMS).

Ce menu permet de paramétrer les conditions d'émission de l'alarme.

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 ON (fermé), ou à l'état OFF ou bien les deux.

Paramètre « Temps de maintien de l'état avant alarme » :

Ce paramètre permet de fixer la durée minimale durant laquelle l'état d'alarme doit être maintenu pour provoquer l'envoi de l'e-mail d'alarme (1 à 60 secondes).

Paramètre « Destinataire de l'alarme » :

Ce paramètre permet de choisir le destinataire de l'alarme parmi la liste des utilisateurs autorisés (User list).

Note :

on peut souhaiter recevoir l'alarme sous forme d' **un message SMS** sur un téléphone portable. Ceci est possible en adressant l'e-mail d'alarme vers une adresse mail ouverte chez l'opérateur GSM qui le route ensuite vers le portable associé. Les opérateurs GSM offrent cette fonction. On consultera notre service hotline pour la mise en œuvre.

1 Etablir une connexion « RAS »

On désigne par « connexion RAS », la connexion d'un utilisateur au moyen d'un modem.

1.1 Les différentes possibilités de connexion

Pour établir une connexion depuis un PC isolé (fonction RAS), les différentes solutions ci-dessous sont possibles.

Note :

Le cas de la connexion par Internet est traité séparément.

• Cas d'un routeur IPL équipé d'un modem réseau téléphonique

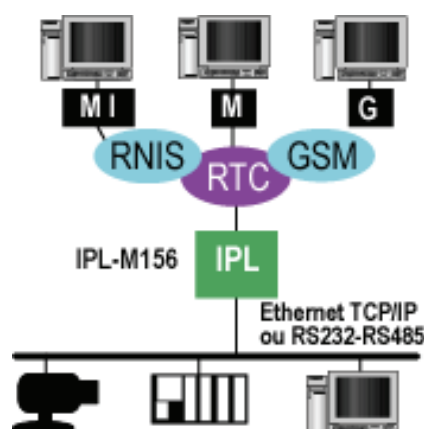
Lorsque le routeur IPL est équipé d'un modem téléphonique, il est possible de se connecter à distance indifféremment avec ...

... un PC + un modem téléphonique connecté à une ligne téléphonique analogique

... un PC + un modem RNIS connecté au réseau RNIS

Un modem RNIS (noté MI sur le schéma ci-dessous) est un boîtier mixte intégrant la fonction modem téléphonique (avis V34 ou V90 par exemple) mais conçu pour être connecté à une ligne RNIS (numérique).

... un PC + un modem GSM



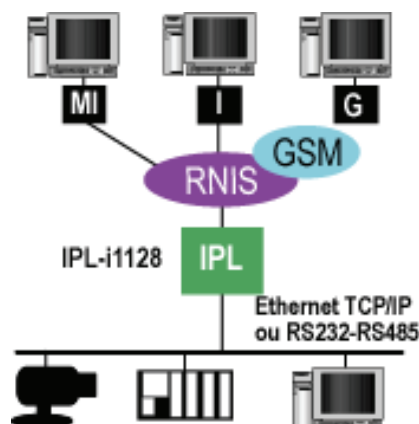
- **Cas d'un routeur IPL équipé d'un adaptateur RNIS**

Lorsque le routeur IPL est équipé d'un adaptateur RNIS, il est possible de se connecter à distance indifféremment avec ...

... un PC + un adaptateur RNIS (noté I) connecté au réseau RNIS

... un PC + un modem RNIS (noté MI) connecté au réseau RNIS

... un PC + un modem GSM (noté G)



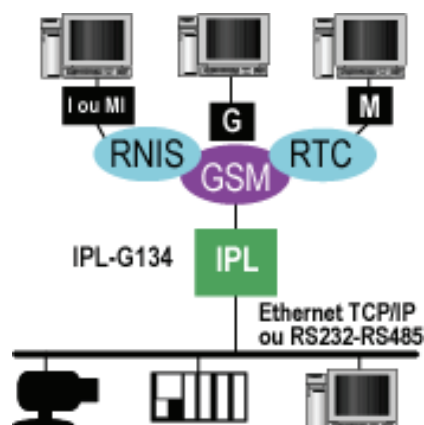
- **Cas d'un routeur IPL équipé d'un modem GSM**

Lorsque le routeur IPL est équipé d'un modem GSM, il est possible de se connecter à distance indifféremment avec ...

... un PC + un modem téléphonique (noté M) connecté à une ligne téléphonique analogique

... un PC + un modem GSM (noté G)

... un PC + un modem RNIS (noté MI) connecté au réseau RNIS.
Un modem RNIS est un boîtier mixte intégrant la fonction modem téléphonique (avis V34 ou V90 par exemple) mais fait pour être connecté à une ligne RNIS (numérique).



... un PC + un adaptateur RNIS
V110 (noté I) connecté au réseau
RNIS

1.2 Etablir la connexion

3 possibilités sont offertes :

- **Etablir une connexion sans contre-appel**
- **Etablir une connexion avec contre appel à la demande :**
L'utilisateur distant demande à être rappelé à un N° qu'il spécifie pour imputer le coût de la communication à la ligne du routeur IPL.
- **Etablir une connexion avec contre-appel de sécurité :**
L'utilisateur distant se connecte, puis est rappelé automatiquement au N° qui est associé à son identité.

1.2.1 Préparation de la connexion

Avant la première connexion, et une fois pour toute, il est nécessaire de créer un objet « connexion distante » **dans le PC** de l'utilisateur. La procédure de création de cet objet dépend du système d'exploitation installé sur le PC.

Le cas de windows 2000 est décrit en annexe 2.

1.2.2 Connexion sans contre-appel

Pour établir la connexion avec le réseau distant,

- Cliquer droit sur l'icône de la connexion distante
- Sélectionner « connecter » ; la fenêtre de connexion s'affiche.
- Saisir le nom d'utilisateur et le mot de passe sous lequel vous avez été enregistré dans la liste d'utilisateurs autorisés du routeur («admin» et «admin» par défaut).
- Saisir le N° d'appel.



- Cliquer « composer » ; le modem numérote et se connecte au routeur. La fenêtre indique que le PC est connecté.
- Si la fenêtre de contre-appel s'affiche, cliquer sur « Annuler ».
- L'icône de la connexion indique que la connexion est établie.

Le PC est maintenant connecté au réseau local avec l'adresse qui lui a été attribuée par le routeur.

Les conditions de la connexion peuvent être contrôlées dans le menu « Diagnostic » puis « Etat réseau » du routeur d'administration du routeur.

1.2.3 Connexion avec contre-appel à la demande

Il est possible d'établir une connexion en faisant en sorte que le routeur rappelle l'utilisateur à un N° qu'il précise à distance.

Cette fonction permet d'imputer le coût de la communication à la ligne du routeur; ce n'est pas une fonction de sécurité.

Pour être utilisable, cette fonction doit au préalable avoir été autorisée individuellement dans la fiche de l'utilisateur concerné (Menu « Configuration sécurité » puis « Liste des utilisateurs » puis « Contre appel autorisé » dans la fiche de l'utilisateur choisi).

Pour établir la connexion avec le réseau distant en utilisant le contre-appel à la demande,

- Cliquer droit sur l'icône de la connexion distante
- Sélectionner « connecter » ; la fenêtre de connexion s'affiche.
- Saisir le nom d'utilisateur et le mot de passe (« admin » et « admin » par défaut).
- Saisir le N° d'appel du routeur.
- Lorsque la fenêtre de contre-appel s'affiche, saisir le N° auquel vous souhaitez être rappelé puis cliquer sur « OK ».
- Le routeur libère la ligne et rappelle après quelques secondes.

L'icône de la connexion indique que la connexion est établie

1.2.4 Connexion avec contre-appel de sécurité

Il est possible d'établir une connexion en faisant en sorte que le routeur rappelle l'utilisateur à un N° fixe, associé à son identité.

Cette fonction garantit un haut niveau de sécurité.

En effet, si un intrus a dérobé l'identificateur et le mot de passe d'un utilisateur habilité, et s'il essaie de se connecter, le routeur libère la ligne et rappelle au N° associé à l'utilisateur habilité.

Pour être utilisable, cette fonction doit au préalable avoir été affectée individuellement à l'utilisateur (Menu «Routage & accès distant» puis «Utilisateurs» puis «Contre appel forcé» dans la fiche de l'utilisateur choisi).

Pour établir la connexion avec le réseau distant en utilisant le contre-appel de sécurité,

- Cliquer droit sur l'icône de la connexion distante.
- Sélectionner « connecter » ; la fenêtre de connexion s'affiche.
- Saisir le nom d'utilisateur et le mot de passe (« admin » et « admin » par défaut).
- Saisir le N° d'appel du routeur et cliquer « connecter ».
- Lorsqu'il a contrôlé l'identité de l'utilisateur, le routeur libère la ligne puis rappelle au N° associé.

L'icône de la connexion indique que la connexion est établie.

Une fois connecté, l'utilisateur peut utiliser toute application comme s'il était connecté au réseau local.

1.2.5 Accéder aux machines du réseau local

Une fois connecté, l'utilisateur distant peut utiliser ses applications comme s'il était connecté directement au réseau local.

Il peut être aidé par la page portail web que transmet le routeur lorsque l'utilisateur désigne son adresse IP avec son navigateur html; elle joue le rôle de carnet d'adresse et peut servir de lien vers les machines du réseau local (voir détails paragraphe suivant).

L'utilisateur peut accéder au serveur de configuration du routeur soit en tapant son adresse dans le masque de saisie du navigateur html ou bien en cliquant sur le lien « serveur d'administration » situé en bas de la page portail web.

1.2.6 Portail web

Une fois connecté, lorsque l'utilisateur distant désigne l'adresse attribuée au routeur au moyen du navigateur html, **la page portail web** s'affiche à condition que l'option ait été sélectionnée au préalable (« configuration système » puis « liste des machines » puis « afficher le portail web »). Elle joue le rôle de « carnet d'adresse » et de lien vers les machines.

Elle affiche la liste des machines déclarées; chacune d'entre elles est désignée par son libellé, son adresse IP et comporte 3 liens associés :

Le lien « html » permet d'aiguiller simplement l'utilisateur distant vers le serveur web de la machine cible.

Le lien « explore » permet d'afficher sur le PC distant l'explorateur de fichiers de la machine cible. Cette fonction n'est opérationnelle que dans l'environnement Windows.

Le lien « ftp » permet d'afficher sur le PC distant l'explorateur de fichiers de la machine cible. Cette fonction n'est pas liée à l'environnement windows.

1.3 Libérer une connexion

- Cliquer l'icône de la connexion distante.

La fenêtre de connexion apparaît.

- Cliquer « déconnecter ».

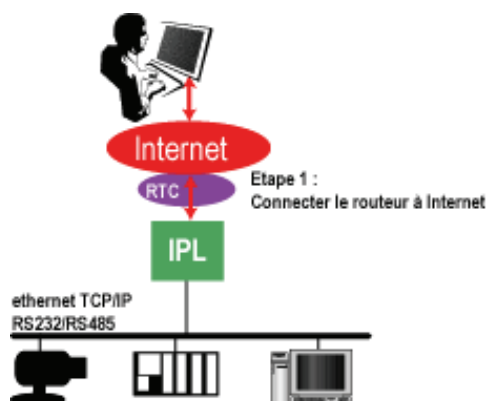
2 Connexion sécurisée par Internet

Il est possible d'établir une connexion sécurisée (VPN) par Internet entre un PC distant et le réseau local protégé par le routeur.

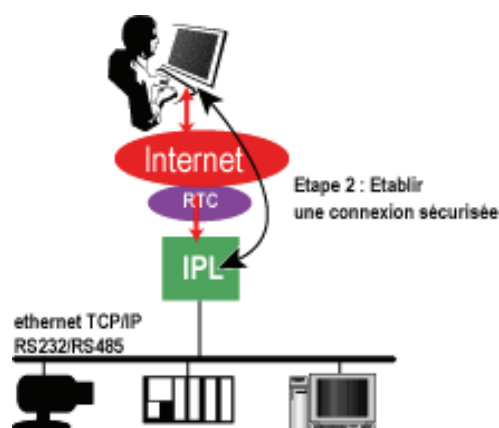
Avant d'utiliser le produit sur l'Internet, on se référera au chapitre Installation afin de contrôler que les abonnements Internet (côté PC et côté IPL) et la configuration du routeur d'entreprise, s'il existe, autorisent le fonctionnement sur l'Internet.

Lorsque l'abonnement Internet attribué au routeur IPL est du type « à adresse IP dynamique », l'établissement de la connexion s'effectue en 2 étapes :

1ere étape :
Connecter le routeur
au réseau Internet



2eme étape :
Etablir une connexion sécurisée
(VPN) entre le PC distant et le routeur
IPL.



2.1 1ere étape :Connecter le routeur IPL au réseau Internet

Selon ce qui a été paramétré dans le menu Configuration Internet puis VPN du serveur d'administration, 4 méthodes différentes et non exclusives sont proposées pour commander la connexion du routeur à Internet :

- **Le contre-appel IP**
- **La connexion par fermeture de l'entrée TOR N°1**
- **La connexion dès la mise sous tension**
- **La connexion en cliquant le bouton « Connecter » du serveur d'administration**

2.1.1 Contre-appel IP

Cette solution est intéressante, car aucune action locale sur le routeur n'est nécessaire.

L'option « contre-appel autorisé » doit avoir été affectée à l'utilisateur. La case « Autoriser le contre-appel vers Internet » du menu « Configuration Internet » puis « VPN » doit être cochée.

- Se connecter au routeur IPL par le réseau commuté (RTC, RNIS, GSM) **sans utiliser l'internet.**
- Lorsque la fenêtre de « contre appel à la demande » s'affiche, taper le chiffre 0 pour demander au routeur de se connecter à l'internet.

Le routeur IPL libère la ligne et se connecte à l'Internet.

2.1.2 Connexion automatique dès la mise sous tension

Un opérateur doit être présent sur le site du routeur pour mettre le routeur IPL sous tension.

La case « Se connecter à Internet à la mise sous tension » du menu « Configuration Internet » puis « VPN » doit être cochée.

- Placer le commutateur 0/1 du routeur à l'état fermé.

Le routeur se connecte à l'Internet après quelques secondes.

2.1.3 Connexion automatique par fermeture de l'entrée TOR N°1

Un opérateur doit être présent sur le site du routeur pour fermer l'entrée TOR n°1.

La case « Se connecter à Internet à la fermeture de l'entrée 1 » du menu « Configuration Internet » puis « VPN » doit être cochée.

- Placer l'entrée TOR n°1 du routeur IPL à l'état fermé.

Le routeur se connecte à l'Internet.

2.1.4 Connexion automatique en cliquant « connecter »

Un opérateur doit être présent sur le site du routeur.

- Au moyen d'un PC sur le réseau Ethernet et d'un navigateur html, accéder au serveur d'administration du routeur.

- Accéder au menu « Configuration Internet » puis « VPN »
- Cliquer le bouton connecter.

Le routeur se connecte à l'Internet.

2.2 2eme étape : Etablir la connexion sécurisée

Une fois que le routeur est connecté à l'Internet, un tunnel sécurisé (VPN) doit être établi entre le PC de l'utilisateur et le routeur.

Si l'abonnement Internet du routeur est du type dynamique, le fournisseur d'accès attribue au routeur IPL une adresse IP différente à chaque connexion.

Cette adresse doit être transmise à l'utilisateur du PC pour qu'il établisse le tunnel sécurisé.

Pour établir le tunnel sécurisé, 3 méthodes sont possibles :

- Un première méthode consiste à lire cette adresse dans le routeur en accédant au menu « Diagnostic », puis « Etat du réseau » au paragraphe « Etat Internet » ; elle est appelée « adresse IP locale ». On peut ensuite la transmettre par téléphone oralement à l'utilisateur du PC.
- L'adresse IP peut aussi être transmise automatiquement à l'utilisateur du PC par email.
- Elle peut également être rendue disponible pour l'utilisateur du PC sur un routeur FTP.

2.2.1 Etablir la connexion sécurisée via un e-mail

Comment paramétrer le routeur IPL ?

La case « **Transmettre l'adresse IP par email** » du menu « **Configuration Internet** » puis « **VPN** » doit être cochée.

Dans ce cas, le routeur transmet l'adresse IP qui lui a été affectée au moyen d'un email adressé soit au destinataire désigné dans la page du menu « VPN », soit à l'utilisateur qui a demandé le contre-appel IP.

- Ouvrir l'email provenant du routeur IPL ; il contient l'adresse IP demandée :

Hello admin, i am connected to internet.

IP: 62.147.75.153

MAC: 00:0A:B4:00:01:5F

SITE: FORD BRESIL

DATE: Mon Nov 17 09:06:14 2003

- Ouvrir la connexion VPN, puis cliquer Propriétés.
Voir annexe 3 pour la création de la connexion VPN.
- Copier l'adresse Internet dans le champ « Adresse IP de destination » de la connexion VPN, puis cliquer Connecter.

Note : il est également possible d'automatiser complètement le processus en cochant **en plus** la case « Email HTML avec lanceur VPN » de la page VPN (menu « **Configuration Internet** » puis « **VPN** »).

2.2.2 Etablir la connexion sécurisée via un routeur FTP

Comment paramétrer le routeur ?

- Accéder au menu « Configuration Internet » puis « VPN » du routeur,
- Cocher la case « Transmettre l'adresse IP vers un routeur FTP » et les caractéristiques du routeur FTP doivent être renseignées dans les masques de saisies qui suivent.

Exemple :

Transmission vers un routeur FTP de l'adresse IP obtenue sur l'Internet

Adresse du Routeur FTP	ftppero.free.fr
Nom d'utilisateur	etic1
Mot de passe	dwbbbfz
Chemin du fichier à déposer	test

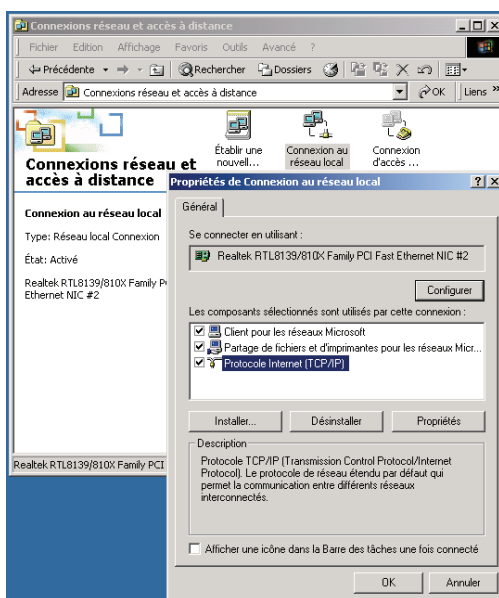
Comment opérer ?

- Ouvrir le navigateur Internet
- Saisir l'adresse du routeur ftp dans la barre d'adresse du navigateur.
par exemple, <http://etic1.free.fr/test.htm>.
La page du routeur ftp s'affiche.
- Cliquer le bouton LAUNCH VPN.

La connexion sécurisée s'établit automatiquement ; une fenêtre à fond noir renseigne sur la progression de la connexion, puis La fenêtre Connexion VPN indique l'état « Connecté ».

Modifier une connexion Ethernet Sous Windows 2000 en vue de connecter directement le PC au routeur

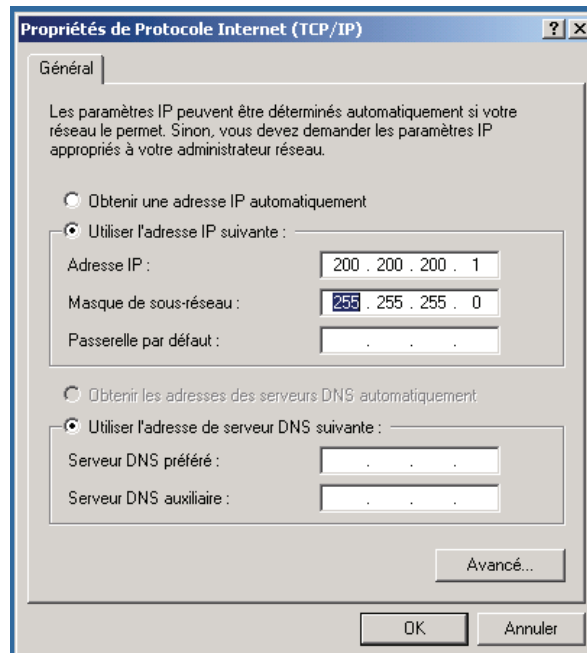
- Ouvrir le panneau de configuration
- Ouvrir le dossier connexion réseau et accès à distance
- Cliquer droit sur la connexion au réseau local existante puis « propriétés »
- Sélectionner Protocole Internet (TCP/IP)
- Cliquer sur Propriétés



- Cliquer sur « utiliser l'adresse IP suivante » .

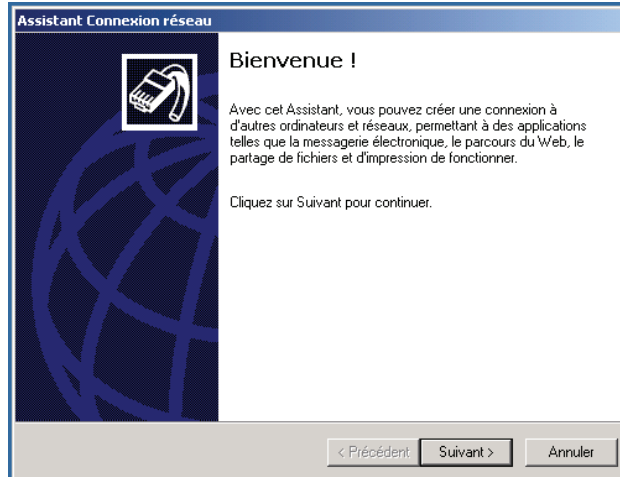
Attribuer au PC une adresse IP et un masque de réseau compatible de l'adresse IP affectée au routeur d'administration du routeur.

Note : L'adresse « Usine » du routeur est 192.168.0.128 ; pour la première configuration, on pourra affecter au PC l'adresse IP 192.168.0.127.



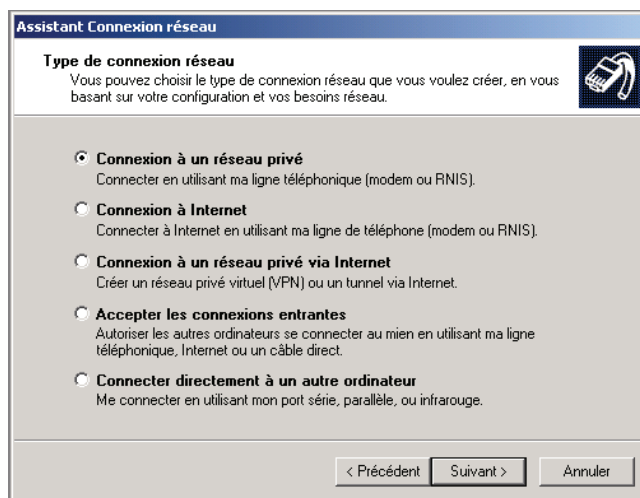
**Création d'une connexion distante Sous Windows 2000
en vue de connecter par le réseau téléphonique au réseau distant**

- Sélectionner Démarrer / paramètres / panneau de configuration / Connexion réseau et accès à distance.
- Double-cliquer l'icône « Nouvelle connexion » ; l'assistant de connexion s'affiche.

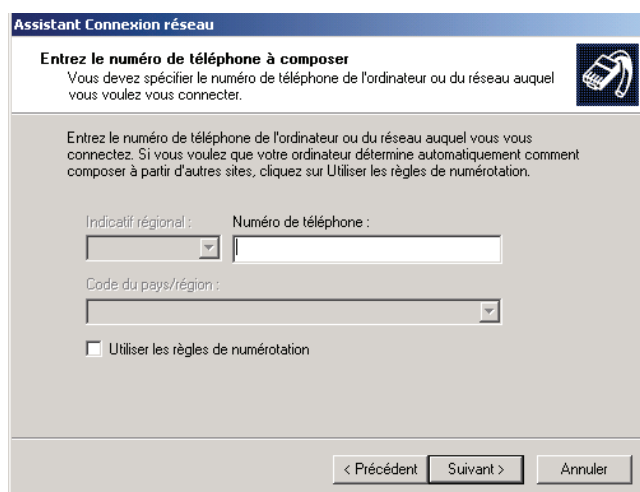


- Cliquer le bouton « Suivant ».

- Cliquer le bouton radio « Connexion à un réseau privé. Connecter en utilisant ma ligne téléphonique (modem ou RNIS) ».



- Cliquer le bouton « suivant » ; la fenêtre invite à saisir un n° de téléphone ; cliquer suivant sans saisir un n° d'appel, on le fera ultérieurement au moment de se connecter.



- Cliquer le bouton « suivant » et laisser l'option par défaut « pour tous les utilisateurs » cochée.
- Cliquer le bouton « suivant » ; donner un nom à la connexion ; par exemple « Routeur-M156 » ou bien tout autre nom qui indique l'usage de cette connexion.
- Sélectionner l'option « ajouter un raccourci sur mon bureau » pour que l'icône de cette connexion distante soit disponible sur le bureau de l'ordinateur.
- Cliquer le bouton « terminer ».

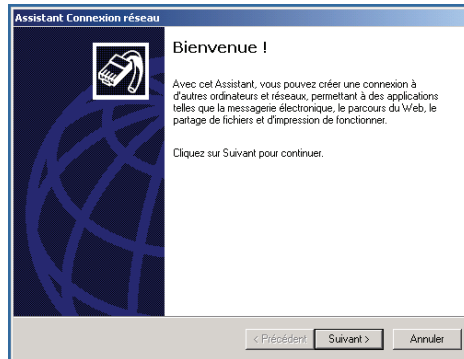
La fenêtre d'identification s'affiche ; saisir le nom d'utilisateur et le mot de passe qui vous ont été attribués pour accéder au réseau distant. Sélectionner l'option « Enregistrer le mot de passe » si vous le souhaitez.



- Vérifier que la connexion distante apparaît bien sur le bureau de votre ordinateur.

**Création d'une connexion sécurisée sous Windows 2000
en vue de connecter le PC au routeur via l'Internet**

- Sélectionner Démarrer / paramètres / panneau de configuration / Connexion réseau et accès à distance.
- Double-cliquer l'icône « Nouvelle connexion » ; l'assistant de connexion s'affiche.



- Cliquer le bouton « Suivant ».
- Cliquer le bouton radio « Connexion à un réseau privé via l'Internet. Créer un réseau privé virtuel (VPN) ou un tunnel via l'Internet ».
- Cliquer le bouton « suivant » .
- La fenêtre suivante s'affiche ; cliquer « ne pas composer automatiquement la connexion initiale ».
- Cliquer le bouton « suivant » 3 fois de suite sans modifier le paramétrage proposé .
- Lorsque la fenêtre « FIN DE L'ASSISTANT DE CONNEXION RESEAU » s'affiche, **donner impérativement le nom « VPN »** (majuscules) à cette connexion, puis cliquer le bouton Terminer.





13, Chemin du Vieux Chêne

38240 Meylan France

Tél : 04 76 04 20 00

Fax : 04 76 04 20 01

E-mail : info@eticlecom.com

Web : www.eticlecom.com