SIG-E-400

Serveur VPN – Routeur IP – Serveur RAS - Firewall

_____

NOTICE D'UTILISATION

Document référence : 9022509-01

_____

SOMMAIRE

Le routeur ADSL et cellulaire de type SIG-E-400 est fabriqué 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
FAX : + (33) (0)4-76-04-20-01
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

SOMMAIRE

Déclaration de conformité

Identification : Serveur VPN

Référence : SIG-E-400

Au nom de la société ETIC Telecom, Philippe DUCHESNE agissant en tant que directeur technique, déclare que le produit ci-dessus est conforme à la directive R&TTE Directive (1999/5/EC).

Le produit routeur est en particulier conforme aux normes suivantes :

Compatibilité : EN 55022
EN 50024
EN 300386-2
FCC Part 15

Sécurité : EN 60950
UL (IEC950)

Substance dangereuses : 2002/95/CE (RoHS)

Date : 4 Février 2015

Philippe DUCHESNE
Directeur technique

1 Identification des produits

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

Serveur VPN	
	SIG-E-400
Serveur VPN	64 VPNs
Débit total de données encryptées	50 Mb/s
Types de VPNs	IPSec et OpenVPN
Nombre de serveurs OpenVPN	4
Firewall SPI	•
Routeur IP	•
Serveur RAS 25 utilisateurs	•
NAT	•
Masquerading	•
Redirection de port (port forwarding)	•
SNMP	•
DNS	•
DHCP client ou serveur sur l'interface LAN	•
Configuration HTTPS / HTML / SSH	•
Ethernet 10 / 100 BT	4
USB	1

2 Présentation du produit

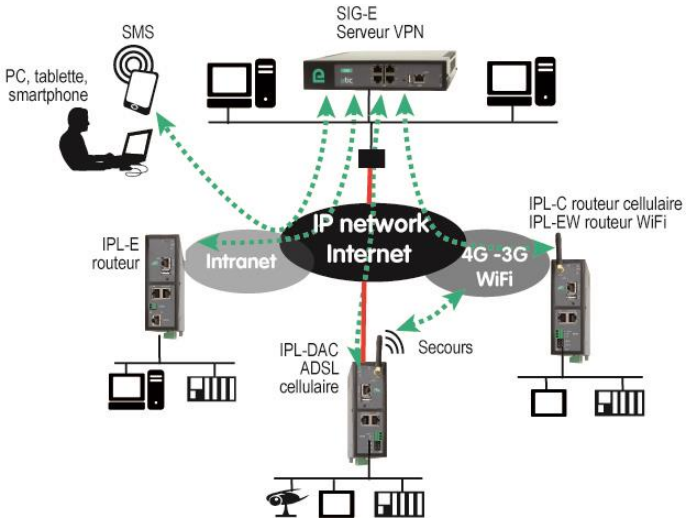
Le routeur SIG-E assure les fonctions de serveur VPN, routeur IP, serveur d'accès distant et firewall pour les systèmes industriels.

Il permet de réaliser des systèmes de télé contrôle entre un réseau de supervision et des équipements distants (systèmes mobiles, automatismes, équipements de mesure...).

Système de télé contrôle de haute sécurité jusqu'à 64 sites
Le routeur SIG-E permet d'interconnecter 64 sites équipés de routeurs IP au moyen de VPNs en offrant un niveau élevé de sécurité.

Haute disponibilité
Le routeur SIG-E prend en compte les chemins de secours ; un site éloigné peut être équipé d'un routeur ADSL avec secours 3G, par exemple ; en cas de défaillance de la ligne ADSL, le VPN sera rétabli par le réseau cellulaire.

De plus, 2 routeurs SIG-E peuvent être placés en redondance l'un de l'autre; en cas de panne de l'un, l'autre prend le relais automatiquement.



Serveur d'accès distant pour la télé-exploitation
Un opérateur autorisé peut se connecter à distance à l'un quelconque des équipements du système au moyen d'un PC, d'une tablette ou d'un smartphone.
Ses droits peuvent être limités en fonction de son identité.

Filtrage des échanges (Firewall)
Le routeur SIG-E placé entre deux réseaux filtre les trames IP et concourt à la sécurité du système.

PRESENTATION

2.1 Fonctions principales

VPNs IPSec et OpenVPN pour la sécurité
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.

Le router SIG-E permet d'établir simultanément des tunnels VPN de type IPSec et OpenVPN.

64 tunnels VPN au total de type OpenVPN et IPSec peuvent être établis.

Bien que le routeur SIG-E soit conçu pour réaliser la fonction de concentrateur de VPNs (on dit aussi serveur VPN), il Il peut aussi bien se comporter en serveur ou en client VPN.

Le routeur SIG-E contient 4 modules serveurs VPN OpenVPN indépendants ; chacun de ces modules OpenVPN peut être réglé différemment pour répondre aux nécessités techniques (période de rafraichissement des clés, type de cryptage …).

Le paramétrage d' IPSec peut être différent pour chaque VPN.

Ces différentes caractéristiques permettent d'accepter des VPNs OpenVPNs ou IPSec provenant de routeurs de constructeurs différents et aussi de prendre en compte des chemins de secours (backup) afin de construire des systèmes de télé contrôle de haute disponibilité.

Serveur RAS pour PC, tablette et smartphone
Le routeur SIG-E 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.

Firewall
Le routeur SIG-E 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 SIG-E peut se déclarer en stand-by en sorte qu'un autre routeur SIG prenne le relais avec un fonctionnement identique.

SNMP
Le routeur SIG-E 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 SIG-E 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 SIG-E peut se comporter en serveur DHCP.

Configuration HTML, TTPS, SSH
Le routeur SIGE se configure au moyen d'un navigateur HTML (ou HTTPS).

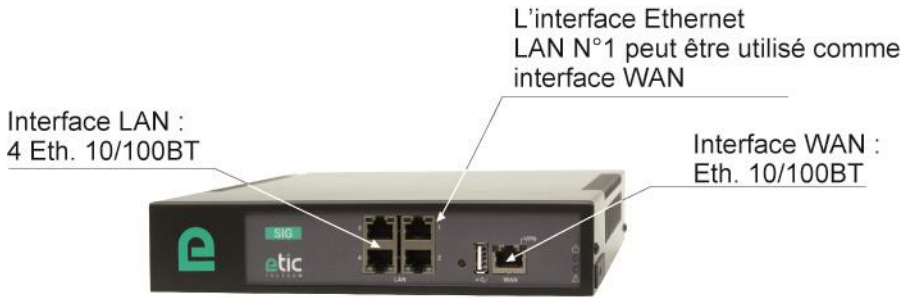
EticFinder
Le logiciel ETICFinder livré avec le routeur ; il permet de détecter simplement tous les produits de marque ETIC connectés à un segment Ethernet pour afficher leur adresse MAC ainsi que l'adresse IP qui leur est attribuée sur le réseau.

2.2 Interfaces du routeur

Le routeur SIG-E présente une interface WAN et une interface LAN.
Les VPN peuvent être établis à partir de l'interface WAN ou éventuellement de l'interface LAN (OpenVPN seulement).

Interface WAN du routeur
L'interface WAN est normalement l'interface Ethernet « WAN » (voir figure ci-dessous).
L'interface Ethernet LAN1 peut également être utilisée comme interface WAN.

Interface LAN du routeur
L'interface LAN est constituée de 4 prises Ethernet switchées.
Les équipements de l'interface LAN constituent le réseau LAN.



Firewall
Le firewall est placé entre les interfaces WAN et VPN d'une part, et l'interface LAN d'autre part.
Le firewall filtre les adresses source et destination et assure la protection contre les attaques.

Serveur d'accès distant
Les utilisateurs distants sont accueillis sur l'interface WAN.

3 Fiche technique

Caractéristiques générales	
Dimensions	Avec pied : 50 X 22 X 22 cm (h, l, p) Sans pied : 44 X 22 X 22 cm (h, l, p)
EMI	EN50082-2
Sécurité électrique	EN 60950- UL 1950
CEM	ESD : EN61000-4-2 : Décharge 6 KV Champ HF : EN61000-4-3 : 10V/m < 2 GHz Transitoires : EN61000-4-4 Choc : EN61000-4-5 : 4KV line / earth
Substances dangereuses	2002/95/CE (RoHS)
Tension d'alimentation	110 à 230 VAC
Puissance absorbée	8 W
T° d'utilisation	-20°C / + 60°C Humidité 5 à 95 %
Ventilation	Naturelle (pas de ventilateur)

Ethernet / routage IP	
Ethernet	10-100 BT Détection de débit 10 ou 100 Mb/s et de câble croisé
Routeur	Connexions distantes - Routes statiques - RIP V2
Translation d'@IP	Translation d'@IP source (NAT) Translation d'@IP destination (DNAT) Translation de port (Port forwarding) Substitution d'@ IP source et destination (version B seulement)
DNS	Gestion du système de nom de domaine
DHCP	Internet : Client ou @IP fixe LAN : DHCP client ou serveur ou @ IP fixe

PRESENTATION

VPN / Firewall	
VPN OpenVPN	4 serveurs VPNs configurables individuellement Client ou serveur cryptage AES256 ou 3DES Authentification OpenVPN : Certificat X509 Authentification IPSec : Clé partagée ou certificat X509
VPN IPSec	Cryptage AES256 ou 3DES Authentification IPSec : Clé partagée ou certificat X509
VPN	64 VPN max Débit total maximum d'encryptage et de décryptage : 50 Mb/s
Firewall	Stateful packet inspection (50 règles) Filtrage d'adresses IP et des N° de port source et destination
Logs	Tableau d'événements horodatés

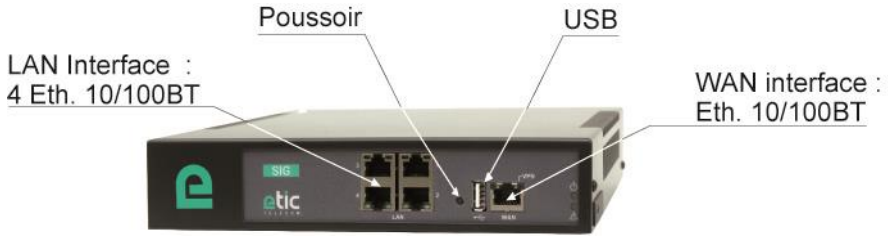
Serveur d'accès distant (RAS)	
Utilisateurs distants	Liste de 25 utilisateurs
Connexion	Sécurisée par VPN PPTP / L2TP-IPSec / Open VPN Contrôle de Login et mot de passe Contrôle de certificat X509
M2Me	Compatible du logiciel client VPN M2Me_Secure Compatible du service de médiation M2Me_Connect

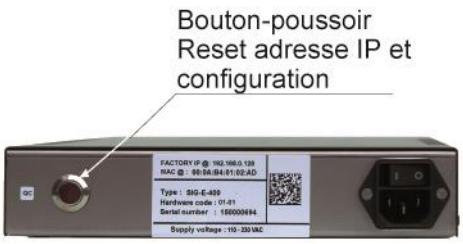
Redondance et secours de liaison	
Redondance en cas de panne du routeur	VRRP et OSPF permettent de placer deux routeurs en backup l'un de l'autre
Gestion des liaisons de secours	le serveur SIG-E gère la reconnexion de VPN OpenVPN en cas de basculement d'un routeur distant d'une liaison principale à une liaison de secours

1 Description

1.1 Dimensions

Boutons-poussoirs, connecteurs, voyants





1.2 Boutons poussoirs

Bouton poussoir de face avant Autoriser temporairement l'accès distant		
Appui Sur BP1	Voyant ⏻	Fonction
5 secondes	3 impulsions en vert	La hotline d'ETIC TELECOM est autorisée à établir une connexion distante OpenVPN vers le routeur. La connexion distante doit intervenir dans un délai de 1 heure.
10 secondes	5 impulsions en vert	Un utilisateur distant est autorisé à établir une connexion distante OpenVPN vers le routeur sans identificateur / mot de passe d'utilisateur distant. La connexion distante doit intervenir dans un délai de 10 mn. L'accès est limité au serveur de configuration du routeur.

Bouton poussoir de face arrière Retour à l'adresse usine ou à la configuration usine		
Appui sur BP de face arrière	Voyant ⏻	Fonction
pendant le fonctionnement	Clignotement rouge	Retour à l'adresse IP usine 192.168.0.128 La configuration courante reste active.
Simultanément avec la mise sous tension	Clignotement rouge	Retour à la configuration Usine La configuration courante est perdue sauf si elle a été sauvegardée dans un fichier.

Connecteurs RJ45 Ethernet		
Broche	Signal	Fonction
1	Tx +	Emission polarité +
2	Tx -	Emission polarité -
3	Rx +	Réception polarité +
4	N.C	-
5	N.C	-
6	Rx -	Réception polarité -
7	N.C.	-
8	N.C.	-

1.3 Voyants

Voyants		
	Désignation	Fonction
Opération	⏻	Allumé fixe vert : En fonction Rouge : Erreur de démarrage grave - erreur chargement firmware Clignotant rouge lent : Démarrage ou Alarme matérielle Clignotant rouge rapide : Chargement du firmware en cours

.

1 Première configuration

La première configuration s'effectue au moyen d'un navigateur HTML et en connectant le PC directement à l'un des connecteurs Ethernet de l'interface LAN du produit.

A la livraison, l'adresse attribuée à l'interface LAN est 192.168.0.128.

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, comme par exemple l'adresse 192.168.0.127.

Etape 2 : Connecter le PC au routeur
Connecter le PC au routeur.

Etape 3 : Lancer le navigateur HTML
Ouvrir le navigateur et saisir 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.

Remarque : une fois la configuration effectuée, Il est conseillé de la sauvegarder dans un fichier

2 Protéger l'accès au serveur d'administration

Pour éviter la modification inopportune du paramétrage du routeur, il est utile de protéger l'accès au serveur d'administration.

- Sélectionner le menu Configuration>Sécurité>Droits d'accès.
- Entrer un login et un mot de passe et sélectionner la case à cocher « Protéger l'accès au serveur d' administration ».

3 Choix de l'outil de configuration

Le routeur peut se configurer par l'un des moyens suivants :

- un navigateur HTML avec le protocole http (par défaut)
- un navigateur HTML avec le protocole de sécurité HTTPS (voir ci-dessous)
- En mode commande, au moyen d'une connexion sécurisée SSH

4 Modification ultérieure de la configuration

Le serveur de configuration se trouve à l'adresse IP attribuée à l'interface LAN du routeur (= adresse IP attribuée au switch Ethernet 4 ports.

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

Pour autoriser l'accès au serveur d'administration par l'interface WAN,
- sélectionner le menu Configuration > Sécurité >Droits d'administration,
- saisir le nom d'utilisateur et le mot de passe,
- cocher la case « utiliser HTTPS pour la configuration »,
- cocher la case « Activer l'accès par le WAN ».

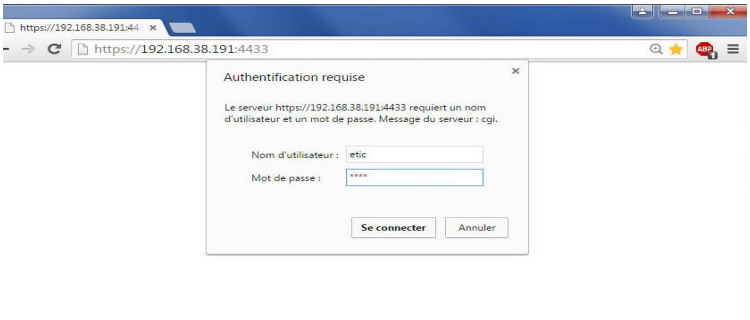
Le serveur d'administration est accessible au moyen d'un navigateur dans le mode HTTPS par l'interface WAN ou l'interface LAN.

6 Opération 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 sur « 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 de configuration s'affiche.

7 Configuration en SSH

La connexion SSH (Secure Shell) est une connexion telnet sécurisée par le protocole TLS.

Le port SSH est 22.

Le nom et le mot de passe permettant une connexion SSH sont ceux qui ont été configurés dans la page web "Droits d'administration".

L'utilisateur peut alors consulter ou modifier les paramètres de configuration en mode « commande CLI ».

8 Restituer l'@IP Usine et l'accès libre à l'administration

En cas de perte du mot de passe du serveur d 'administration ou bien si l'adresse IP du serveur d'administration n'est pas connue, il peut être utile de restituer l'adresse IP usine du routeur et l'accès libre par l'interface LAN.

- Appuyer sur le bouton-poussoir placé sur la face arrière alors que le routeur est en fonctionnement.

la led d'alimentation clignote rapidement en rouge.

Le routeur reprend l'adresse IP usine 192.168.0.128 jusqu'à la prochaine mise sous tension.

Le serveur HTML d'administration est accessible sans mot de passe et en HTTP jusqu'à la prochaine mise sous tension.

La configuration programmée n'est pas modifiée.

Remarque :
Le logiciel ETICFinder permet de détecter tous les produits fabriqués par ETIC TELECOM et connectés à un réseau Ethernet ; le logiciel affiche l'adresse IP attribuée à chacun d'entre eux.

9 Retour à la configuration Usine

Il peut être nécessaire de restaurer la configuration Usine, par exemple, si l'accès au serveur d'administration n'est plus possible à la suite d'une erreur dans la programmation du firewall ou bien pour d'autres raisons.

Il est possible de restituer la configuration Usine au moyen du bouton poussoir de la face arrière, ou bien en utilisant le serveur d'administration.

Pour restituer la configuration Usine au moyen du bouton poussoir de la face arrière du routeur,

- Mettre le routeur hors tension,
- Appuyer sur le poussoir de la face arrière avec une pointe de tournevis par exemple.
- Mettre sous en tension tout en maintenant le poussoir enfoncé 10 secondes.

Le voyant « Operation » passe au rouge ; le routeur s'initialise et la configuration Usine est restituée.

Pour restituer la configuration Usine au moyen du serveur d'administration,

- Sélectionner le menu « Maintenance », puis le menu « Gestion des configurations ».
- Sélectionner la configuration « Factorydefault » puis cliquer le bouton « charger ».

Le voyant « Operation » passe au rouge ; le routeur s'initialise et la configuration par défaut est restituée.

Remarque :
Après avoir restauré la configuration Usine du routeur, la configuration courante est perdue, sauf si elle a été préalablement sauvegardée dans un fichier (voir paragraphe sauvegarde de la configuration).

10 Syntaxe

Format des adresses réseau
Dans la suite du texte on appelle « adresse réseau », l'adresse 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.

11 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 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 *.txt 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.

12 Paramétrage du routeur

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

- Configurer la connexion WAN
- Configurer l'interface LAN
- Configurer les VPN avec d'autres routeurs
- Configurer les fonctions de translation d'adresse et redirection de port si nécessaire
- Configurer le service d'utilisateurs distants : Connexion distante, User list, droits d'accès
- Configurer le firewall

Pour le détail du paramétrage du routeur on se reportera au document intitulé «Notice de paramétrage des routeurs IPL et SIG ».
Après la mise sous tension, le voyant « Opération » s'éclaire en rouge durant 30 secondes environ pendant la phase d'initialisation du routeur
Après ce délai, le voyant passe au vert lorsque le produit est prêt à fonctionner.
Si le voyant reste éclairé rouge après de délai, le routeur est probablement en panne ; contacter la hotline.

1 Diagnostic visuel de défaut de fonctionnement

Après la mise sous tension, le voyant  s'éclaire en rouge durant 30 secondes environ pendant la phase d'initialisation du routeur

Après ce délai, le voyant passe au vert lorsque le produit est prêt à fonctionner.

Si le voyant reste éclairé rouge après de délai, le routeur est probablement en panne ; contacter la hotline.

2 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 du réseau Ethernet WAN
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.

- Sélectionner le menu Diagnostic > Etat réseau > Interfaces

Etat de l'interface Ethernet WAN / Paramètres de base :

Champ « Connecté » : Oui / Non

Champ « Adresse IP » : Adresse IP attribué à l'interface WAN du routeur.

2.2 Outils « Ping »

Cette page permet de commander l'émission d'une trame « ping » vers une machine du réseau raccordé au routeur.

3 Mise à jour du firmware

Elle s'effectue par la prise Ethernet en local 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 ».

ETIC TELECOM
13 chemin du vieux Chêne
38240 Meylan
France
contact@eticTelecom.com