



# **XSLAN / XSLAN+ / XSMIL**

## **SHDSL Switch**

---

### **GUIDE DE CONFIGURATION**

---

Les familles de produits XSLAN, XSLAN+ et XSMIL sont fabriquées par

**ETIC TELECOM**  
405 rue Lavoisier  
38330 MONTBONNOT SAINT MARTIN  
FRANCE

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

TEL : + (33) (0)4-76-04-20-05  
E-mail : [hotline@etictelecom.com](mailto:hotline@etictelecom.com)  
web : [www.etictelecom.com](http://www.etictelecom.com)

#### HISTORIQUE DES MODIFICATIONS

REVISION	DATE	MODIFICATIONS	Rédigé par	Vérifié par
E	10/07/2023	Mise en conformité pour le nouveau XSLAN : Ajout chapitres NAT avancé, Pare-Feu, MACSec	P. Duchesne	P. Duchesne
F	10/12/2024	Ajout du serveur d'état Modbus TCP Correction du tableau d'OID des interfaces réseau	D.Jeannin	P.Duchesne

<b>PRESENTATION.....</b>	<b>7</b>
1 But du document.....	7
2 Principales caractéristiques de la famille XS.....	7
<b>PREPARER LE PARAMETRAGE.....</b>	<b>9</b>
1 Connexion du PC en vue de la configuration .....	9
1.1 Introduction.....	9
1.2 Première configuration.....	10
1.3 Modification ultérieure de la configuration .....	10
2 Retour temporaire à la configuration usine.....	10
3 Restitution de la configuration usine.....	11
4 Protection de l'accès au serveur d'administration.....	11
5 Etapes de configuration .....	12
<b>PARAMETRAGE.....</b>	<b>13</b>
1 Attribution des adresses IP.....	13
2 Principe de fonctionnement et de paramétrage d'une connexion SHDSL.....	15
2.1 Fonctionnement d'une connexion SHDSL.....	15
2.2 Profils de connexion .....	16
3 Mise en service d'une liaison au moyen d'une paire torsadée.....	17
3.1 Etapes du paramétrage .....	18
3.2 Etape 1 : Régler la liaison SHDSL.....	18
3.3 Etape 2 : Vérification du bon fonctionnement .....	20
4 Mise en service d'une liaison au moyen de 2, 3 ou 4 paires torsadées.....	22
5 Paramétrage avancé d'une liaison SHDSL.....	23
6 RSTP .....	28
6.1 Présentation.....	28
6.2 Configuration .....	29
7 Anneau redondant .....	32
8 VPN de bouclage .....	34
9 Réseau virtuel VLAN .....	36
9.1 Vue d'ensemble.....	36
9.2 Paramétrage .....	37
9.3 Serveur d'administration et passerelles série.....	41
10 MACSec.....	42
10.1 Présentation.....	42
10.2 Configuration de MACSec.....	42
10.3 Mode dérivé d'un mot de passe.....	43
10.4 Etat MACSec .....	44
10.5 Gestion des clés et effacement sécurisé.....	44
10.6 Considérations sur le MTU.....	45
11 IGMP snooping.....	46
11.1 Présentation.....	46
11.2 Configuration de la fonction IGMP snooping.....	46
12 SNMP.....	47
12.1 Présentation.....	47
12.2 Configuration de la fonction SNMP .....	47
12.3 Configuration des traps SNMP .....	49

## TABLE DES MATIERES

13	NTP	50
13.1	Présentation	50
13.2	Configuration de la fonction client NTP	50
13.3	Configuration de la fonction serveur NTP	50
14	Qualité de service DiffServ	51
14.1	Principe	51
14.2	Configuration basique	52
14.3	Configuration avancée	53
15	Routage IP	56
15.1	Principe	56
15.2	Routes statiques	56
15.3	Protocole RIP	57
15.4	Protocole OSPF	57
16	NAT avancé	58
16.1	Principe	58
16.2	Configuration	58
17	Pare-feu	60
17.1	Présentation	60
17.2	Configuration	60
18	Alarmes	61
18.1	Alarmes SNMP	61
18.2	Digital output	61
19	Passerelles série IP	62
19.1	Présentation des types de passerelles	62
19.2	Passerelle Modbus	63
19.3	Passerelle Raw TCP	68
19.4	Passerelle « Raw UDP »	70
19.5	Passerelle « Raw Multicast »	71
19.6	Passerelle « Unitelway »	72
19.7	Passerelle « Telnet »	73
20	Serveur d'état Modbus TCP	75
<b>DIAGNOSTICS ET MAINTENANCE</b>		<b>76</b>
21	Diagnostic visual de défaut de fonctionnement	76
22	Journal	76
23	Mesure de la qualité de liaison	77
24	Statistiques SHDSL	79
25	Etat des passerelles	80
26	Outil PING	81
27	Sauvegarde et chargement d'un fichier de paramètres	82
28	Mise à jour du logiciel	84
<b>ANNEXE 1 : SNMP MIB</b>		<b>85</b>
1	Purpose of the document	85
2	Accessible OIDs and MIBs	85
2.1	Supported MIBs	85
2.2	Network interface indexes	86
2.3	Querying the MIB	86
3	Description of the supported OIDs	87
3.1	Sysdesc, Syslocation, SysName	87

## TABLE DES MATIERES

3.2	Network interfaces table (IF-MIB::ifTable) .....	87
3.3	SHDSL MIB (HDSL2-SHDSL-LINE-MIB) .....	88
3.4	MIB : BRIDGE-MIB::dot1dBridge.....	89
ANNEXE 2 : Portée de la liaison SHDSL .....		91
ANNEXE 3 : Compatibilité entre un ancien switch XSLAN et le switch XSLAN+ .....		92
ANNEXE 4 : Registres du serveur d'état Modbus TCP .....		93



# PRESENTATION

## 1 But du document

Le présent document décrit comment configurer les familles de switches SHDSL XSLAN, XLAN+ and XSMIL fabriqués par ETIC TELECOM.

Il est applicable à partir de la version 2.4.0 du logiciel.

Dans ce document, le nom "XS" concerne aussi bien les produits XSLAN, XSLAN+ que XSMIL.

## 2 Principales caractéristiques de la famille XS

La famille XS de switches SHDSL permet de prolonger un réseau Ethernet distant au moyen de une, deux ou quatre paires de cuivre torsadées (selon le modèle).

Principales caractéristiques :

- 5,7 Mb/s sur 3,7 Km (1 paire diam. 0,9 mm)
- 15 Mb/s sur 700 m
- Concentrateur avec 4 ports SHDSL
- VLAN & SNMP, DiffServ QoS
- Redondance de réseau (RSTP protocole propriétaire)
- 2 ou 4 ports Ethernet 10/100 BT
- 2 ports série (option)
- T° : -20°C / +70°C
- Fonction Bypass (option)
- Configuration & diagnostic via un serveur html



# PREPARER LE PARAMETRAGE

## 1 Connexion du PC en vue de la configuration

### 1.1 Introduction

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

**Aide en ligne :**

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

**Adresse du serveur d'administration :**

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

**Configuration :**

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

Les modifications ultérieures peuvent être en plus effectuées à distance.

**Restitution de l'adresse IP usine :**

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

**Protection d'accès au serveur d'administration :**

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

**Format des adresses réseau :**

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

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

**Caractères autorisés :**

Les caractères accentués ne peuvent être saisis.

# PREPARER LE PARAMETRAGE

## 1.2 Première configuration

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

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

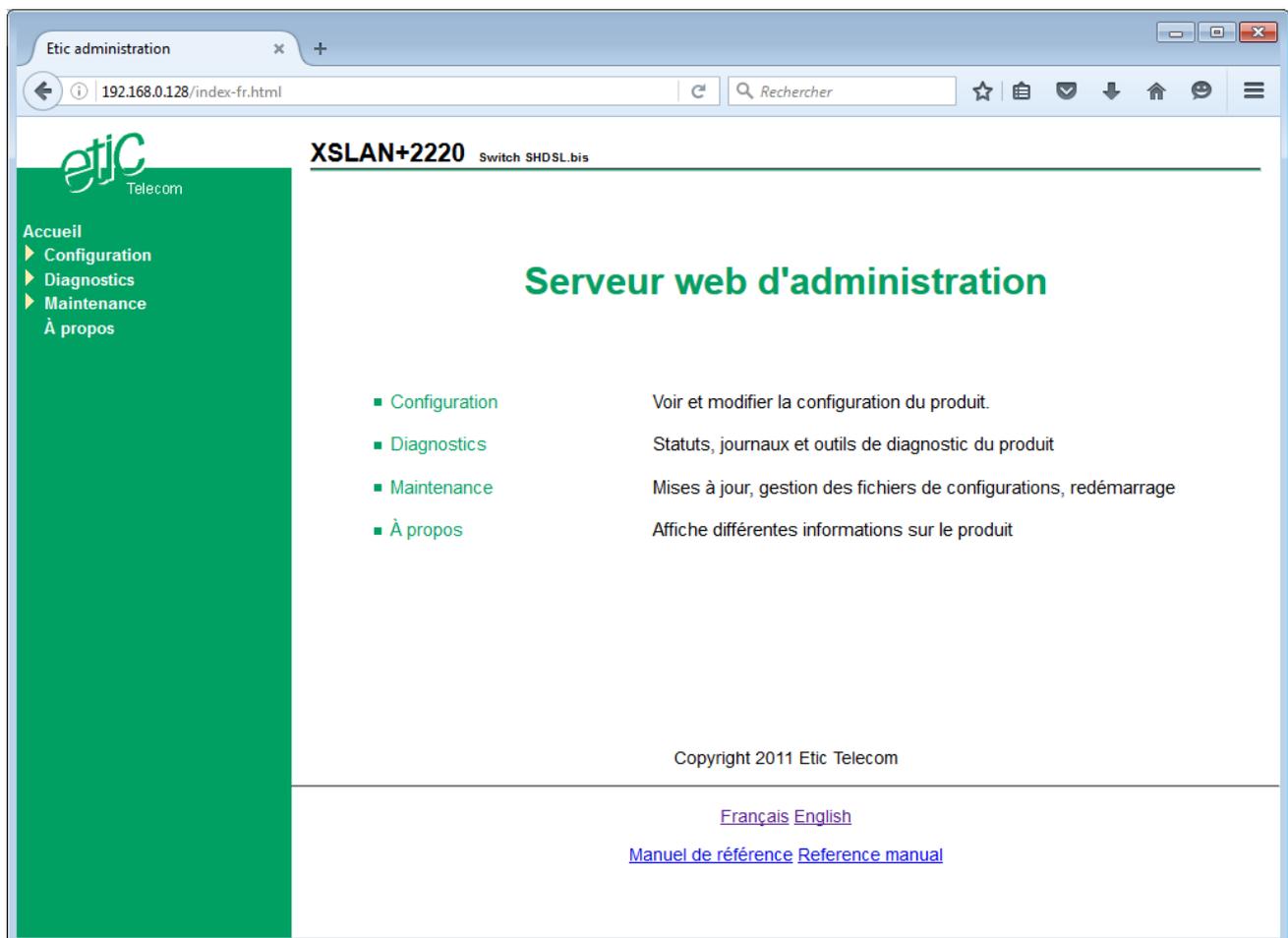
### Etape 2 : Connecter le PC au switch XS

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

### Etape 3 : Lancer le navigateur

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

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



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

## 1.3 Modification ultérieure de la configuration

Par la suite, le serveur d'administration du switch XS est accessible depuis l'interface Ethernet ou à distance à travers la ligne SHDSL au moyen du navigateur, à l'adresse IP attribuée au produit.

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

## 2 Retour temporaire à la configuration usine

Au cas où l'adresse IP du XS ne pourrait être identifiée, ou bien en cas d'impossibilité d'accéder au serveur d'administration à la suite d'une erreur de configuration des VLAN, par exemple, il est possible de restituer la configuration Usine sans pour autant perdre la configuration courante.

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

Note :

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

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

### 3 Restitution de la configuration usine

**Pour restituer la configuration Usine au moyen du bouton poussoir,**

- Mettre le XS hors tension,
- Appuyer sur le bouton poussoir avec une pointe de tournevis par exemple,
- Mettre sous tension tout en maintenant le bouton poussoir enfoncé.

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

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

### 4 Protection de l'accès au serveur d'administration

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

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

# PREPARER LE PARAMETRAGE

## 5 Etapes de configuration

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

- [Configurer l'interface LAN](#)
- [Configurer l'interface SHDSL](#)
- [Configurer la redondance](#)
- [Configurer la fonction VLAN](#)
- [Configurer SNMP](#)
- [Configurer la qualité de service](#)
- [Configurer les fonctions de routage](#)
- [Configurer les passerelles série](#)

# PARAMETRAGE

## 1 Attribution des adresses IP

- Dans le menu, sélectionner **Configuration > Protocole IP et routage > Protocole IP**

Etic administration

192.168.0.128/index-fr.html

etIC Telecom

XSLAN+2220 Switch SHDSL.bis

> Accueil > Configuration > Protocole IP et routage > Protocole IP

Réseau Ports LAN

Adresse IP administration	192.168.0.128
Masque de sous réseau	255.255.255.0
Passerelle par défaut	
Utiliser une adresse différente pour les passerelles série	<input type="checkbox"/>
Activer IPv6	<input type="checkbox"/>

Routage entre SHDSL et LAN

Mode routeur	<input checked="" type="checkbox"/>
--------------	-------------------------------------

Réseau Ports SHDSL

Adresse IP	10.10.10.2
Masque de sous réseau	255.0.0.0
Activer IPv6 sur les ports SHDSL	<input type="checkbox"/>

Enregistrer Annuler

- Configurer les paramètres **Réseau Ports LAN** :

### Adresse IP administration

C'est l'adresse IP attribuée à l'interface Ethernet du XS sur le réseau local.

C'est l'adresse IP du serveur d'administration et des passerelles série.

Valeur par défaut : 192.168.0.128

### Masque de sous-réseau

Le masque de sous-réseau définit la structure des adresses IP de toutes les stations d'un segment Ethernet de réseau local.

Valeur par défaut : 255.255.255.0

### Passerelle par défaut

C'est l'adresse IP du routeur par défaut sur le réseau local.

## PARAMETRAGE

### Utiliser une adresse IP différente pour les passerelles série

Par défaut, l'adresse IP des passerelles série est l'adresse IP d'administration du XS.

Il peut être nécessaire de loger les passerelles série à une autre adresse IP en particulier lorsque la fonction VLAN est activée ; si c'est le cas, cette case doit être cochée et une adresse IP et un masque de sous-réseau doivent être saisis.

Valeur par défaut : Non cochée

### Activer IPV6

Les adresses IP attribuées au XS doivent être saisies au format IPV4.

Cependant le switch supporte aussi l'adressage IPV6. Si cette case est cochée, des adresses IP doivent aussi être saisies au format IPV6.

Valeur par défaut : Non cochée

- Configurer les paramètres **Routage entre SHDSL et LAN** :

### Mode routeur

Par défaut, le XS se comporte comme un switch administré.

Cependant, si cette case est cochée, le XS offre des fonctions de base de routeur IP entre deux interfaces :

Les ports LAN Ethernet 10/100BT d'une part,  
et les ports SHDSL d'autre part.

Les ports LAN Ethernet sont considérés comme une interface unique ; les ports SHDSL (1 à 4 selon les modèles) également. Le XS doit alors avoir deux adresses IP. Celle précédemment définie s'applique uniquement aux ports LAN Ethernet et une nouvelle doit être définie pour les ports SHDSL.

Le but principal est d'éviter que les trames de broadcast ou d'autres trames ne viennent saturer les lignes SHDSL.

Valeur par défaut : Non cochée

Les paramètres ci-dessous sont affichés seulement lorsque le mode routeur IP est sélectionné.

### Adresse IP

C'est l'adresse IP unique attribuée à l'interface ou aux interfaces SHDSL du XS.

Valeur par défaut : aucune

### Masque de sous-réseau

Masque du sous réseau constitué par tous les équipements IP raccordés aux ports SHDSL

Valeur par défaut : 255.255.255.0

### Activer IPV6 sur les ports SHDSL

Voir ci-dessus.

Valeur par défaut : Non cochée

## 2 Principe de fonctionnement et de paramétrage d'une connexion SHDSL

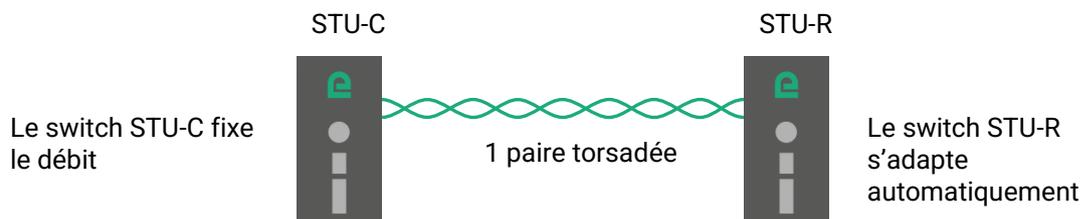
### 2.1 Fonctionnement d'une connexion SHDSL

Lorsque deux switches XS sont connectés par une paire torsadée, l'un des deux switches prend l'initiative de la connexion tandis que l'autre répond et s'adapte automatiquement en débit.

Le switch qui prend l'initiative de la connexion est appelé STU-C.

Le switch qui répond et s'adapte est appelé STU-R.

Ainsi une ligne est toujours connectée d'un côté à un switch agissant comme STU-C et de l'autre à un switch agissant comme STU-R.



**Un des switches est normalement configuré en STU-C et l'autre en STU-R. Cependant, pour rendre la configuration plus simple, le switch configuré en STU-C est capable de basculer automatiquement en mode STU-R s'il détecte la présence en face d'un autre STU-C. Ainsi deux XS configurés tous les deux en STU-C trouveront le moyen de se connecter. L'un des deux basculera en STU-R.**

Le STU-C a l'initiative de la connexion et mesure le niveau du signal reçu et le niveau du bruit et calcule le rapport signal à bruit de la connexion.

Plus la ligne est longue et plus l'environnement électromagnétique est perturbé, plus le rapport signal à bruit diminue.

Pour assurer le fonctionnement, un rapport signal à bruit minimum est nécessaire.

On appelle « marge de signal à bruit » la différence entre le rapport signal à bruit mesuré et le minimum requis. C'est, en quelque sorte, la marge de sécurité de fonctionnement.

Pour configurer une connexion, l'utilisateur doit indiquer la marge de signal qu'il exige. Plus il exige une marge importante, plus le débit s'établit à une valeur faible et plus la connexion est endurante aux perturbations.

# PARAMETRAGE

## 2.2 Profils de connexion

Un profil de connexion regroupe l'ensemble des paramètres techniques d'une connexion SHDSL. Pour rendre le paramétrage particulièrement simple, cinq profils de connexion préprogrammés sont proposés. Pour paramétrer une liaison SHDSL, Il faut donc simplement attribuer un de ces profils à chaque port SHDSL.

### STU-R, Auto

le profil qu'il faut attribuer à un port SHDSL qui attend la connexion (voir schéma ci-dessus).

### STU-C, Standard

Le port SHDSL auquel est attribué ce profil prend l'initiative de la connexion mais est capable de basculer en mode STU-R s'il détecte la présence d'un STU-C à l'autre extrémité.

Il établit la connexion en utilisant un débit conforme à la norme EFM jusqu'à 5,6 Mb/s.

La marge de sécurité est moyenne ; le débit s'établit donc à une valeur moyenne et le risque de déconnexion est raisonnable en cas de perturbation.

Le temps d'établissement de la connexion est rapide, typiquement de 45 secondes et peut aller jusqu'à 1 minute 30.

Ce profil est adapté pour une majorité de situations, c'est-à-dire sur des lignes faiblement à moyennement bruitées et en utilisant des câbles de transmission courants à paires torsadées.

### STU-C, Endurance

Le port SHDSL auquel est attribué ce profil prend l'initiative de la connexion mais est capable de basculer en mode STU-R s'il détecte la présence d'un STU-C à l'autre extrémité.

Il établit la connexion en utilisant un débit conforme à la norme EFM jusqu'à 5,6 Mb/s.

La marge de sécurité est élevée ; le débit s'établit donc à une valeur basse et le risque de déconnexion est faible en cas de perturbation.

Le temps d'établissement de la connexion est plus long, typiquement de 3 minutes et peut aller jusqu'à 5 minutes.

Ce profil est adapté pour des lignes moyennement à fortement bruitées ou sur des câbles non dédiés à la transmission tel que des câbles à fort diamètre ou des câbles électriques.

### STU-C, Performance

Le port SHDSL auquel est attribué ce profil prend l'initiative de la connexion mais est capable de basculer en mode STU-R s'il détecte la présence d'un STU-C à l'autre extrémité.

Il établit la connexion en utilisant un débit conforme à la norme EFM jusqu'à 15,2 Mb/s.

La marge de sécurité est plus faible ; le débit s'établit donc à une valeur plus élevée et le risque de déconnexion est plus grand en cas de perturbation.

Le temps d'établissement de la connexion est plus long, typiquement de 3 minutes et peut aller jusqu'à 5 minutes.

Ce profil est adapté pour des lignes faiblement bruitées. Les débits les plus élevés sont obtenus sur de courtes distances.

### STU-C, Fixed datarate

Le port SHDSL auquel est attribué ce profil prend l'initiative de la connexion.

Ce profil n'est pas utilisable directement ; Il faut l'éditer pour choisir le débit désiré (fonction « Copier et modifier ») Voir le chapitre [Paramétrage avancé d'une liaison SHDSL](#).

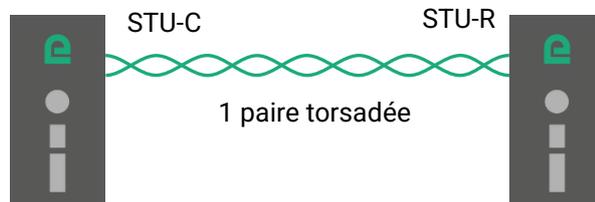
Ce profil permet le temps d'établissement de la connexion le plus rapide, typiquement de 30 secondes.

Cependant il oblige l'utilisateur à effectuer des essais en modifiant la valeur du débit jusqu'à obtenir une connexion avec une marge de rapport signal sur bruit conforme aux attentes.

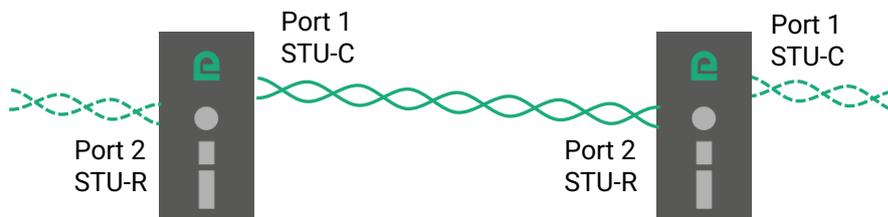
### 3 Mise en service d'une liaison au moyen d'une paire torsadée

Le présent paragraphe décrit la mise en œuvre d'une liaison point à point sur une paire torsadée.

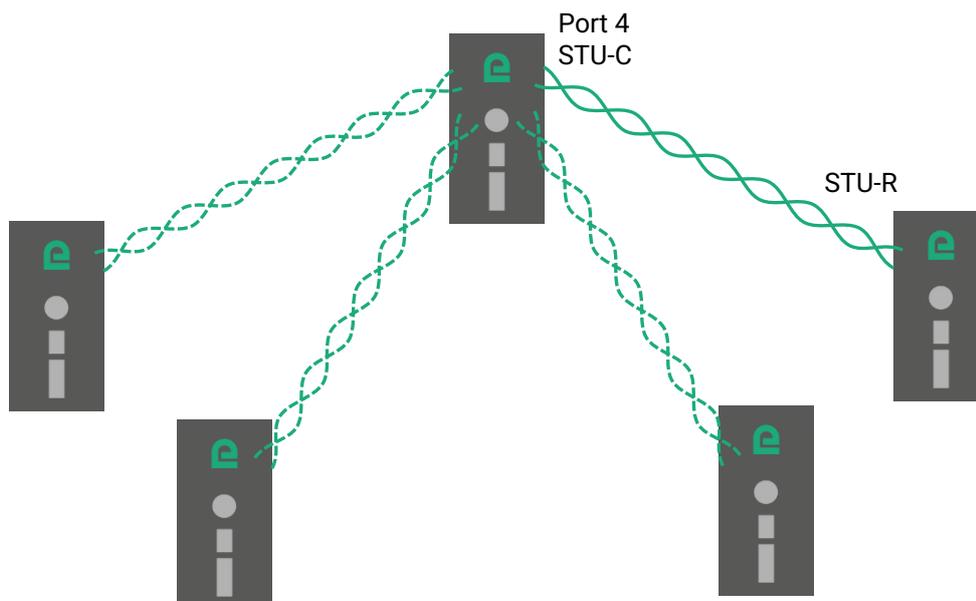
Que ce soit quand on relie deux XS comme dans le schéma ci-dessous.



Ou bien quand on relie deux XS dans le cas d'un réseau chaîné ou en anneau comme dans le schéma ci-dessous.



Ou bien encore quand on relie un XS 4 ports utilisé en concentrateur avec des XS 1 port comme dans le schéma ci-dessous.



# PARAMETRAGE

## 3.1 Etapes du paramétrage

### Etape 1 : Configurer la liaison SHDSL

Attribuer le profil **STU-R, Auto** au port SHDSL du premier XS

Attribuer le profil de connexion à l'autre XS (**STU-C, Standard** ou **STU-C, Endurance** ou **STU-C, Performance**).

### Etape 2 : Vérifier le fonctionnement de la liaison

## 3.2 Etape 1 : Régler la liaison SHDSL

### Paramétrage du premier XS :

- Dans le menu, choisir **Configuration > Ethernet & commutation > Ports SHDSL**.
- Cocher la case **Activer la ligne SHDSL** (port 1 ou 2 ou 3 ou 4 selon le cas).
- Attribuer le profil **STU-R, Auto**.
- Cliquer **Enregistrer**.

The screenshot shows a web browser window titled "Etic administration" with the address bar displaying "192.168.0.128/index-fr.html". The page content is for "XSLAN+2220 Switch SHDSL.bis" and is titled "Ports SHDSL". A green sidebar on the left contains a navigation menu with categories like "Accueil", "Configuration", "Ethernet et commutation", "Protocole IP et routage", "Alarmes", "Passerelles IP-RS", "Sécurité", "Système", "Diagnostics", "Maintenance", and "À propos". The main content area shows configuration options for "Port SHDSL1" and "Port SHDSL2". For "Port SHDSL1", the "Activer le port SHDSL1" checkbox is checked, and the "Profil de connexion SHDSL1" dropdown is set to "STU-R, Auto". For "Port SHDSL2", the "Activer le port SHDSL2" checkbox is unchecked. Below these, the "Agrégration EFM" section has "Mode d'agrégation des lignes" set to "Pas d'agrégation". The "Paramètres avancés" section has "Montrer les paramètres avancés" unchecked. At the bottom, there are "Enregistrer" and "Annuler" buttons.

**Paramétrage de l'autre XS :**

- Dans le menu, choisir **Configuration > Ethernet & commutation > Ports SHDSL**.
- Cocher la case **Activer la ligne SHDSL** (port 1 ou 2 ou 3 ou 4 selon le cas).
- Sélectionner le profil **STU-C, Standard** ou **STU-C Performance** ou **STU-C Endurance**.  
On se reportera au paragraphe précédent pour le choix entre ces trois profils.
- Cliquer **Enregistrer**.

The screenshot shows a web browser window titled "Etic administration" with the URL "192.168.0.128/index-fr.html". The page displays the configuration for "XSLAN+2220 Switch SHDSL.bis" under the path "Accueil > Configuration > Ethernet et commutation > Ports SHDSL".

The left sidebar contains a navigation menu with the following items:

- Accueil
- Configuration
  - Ethernet et commutation
    - Ports SHDSL
    - Ports LAN
    - RSTP - Anneau redondant
    - VLAN
    - Filtrage d'adresses MAC
  - Protocole IP et routage
  - Alarmes
  - Passerelles IP-RS
  - Sécurité
  - Système
- Diagnostics
- Maintenance
- À propos

The main content area shows the configuration for "Port SHDSL1" and "Port SHDSL2":

- Port SHDSL1**: "Activer le port SHDSL1" (checkbox, unchecked).
- Port SHDSL2**: "Activer le port SHDSL2" (checkbox, checked), "Profil de connexion SHDSL2" (dropdown menu).

The dropdown menu for "Profil de connexion SHDSL2" is open, showing the following options:

- STU-C, Standard (selected)
- STU-R, Auto
- STU-C, Standard
- STU-C, Performance
- STU-C, Endurance
- STU-C, Fixed datarate

Below these settings, there is a section for "Agrégation EFM" with "Mode d'agrégation des lignes" and a "Paramètres avancés" section with "Montrer les paramètres avancés" (checkbox, unchecked). At the bottom, there are "Enregistrer" and "Annuler" buttons.

# PARAMETRAGE

## 3.3 Etape 2 : Vérification du bon fonctionnement

- Raccorder les XS aux paires torsadées. Les deux fils d'une même paire torsadée peuvent être intervertis.
- Mettre les XS sous tension.
- La connexion s'établit en environ 45 s avec le profil standard et peut être plus long avec d'autres profils
- Le voyant SHDSLx de chaque port indique l'état d'avancement de la connexion comme décrit dans le tableau suivant :

Etat de la connexion	Voyant SHDSL
L'autre XSLAN n'a pas été détecté (par exemple quand la ligne n'est pas raccordée)	Clignotant 0,1 s ON / 2 s OFF
Négociation du débit	Clignotant 0,3 s ON / 0,3 s OFF
Connecté	Allumé fixe
Connecté & transmission de données	Allumé clignotements brefs

- Une fois les lignes connectées, dans le menu, choisir **Diagnostics > Etat du réseau > Interfaces** pour vérifier la qualité des liaisons SHDSL.

**XSLAN+2220** Switch SHDSL.bis

> Accueil > Diagnostics > Etat du réseau > Interfaces

Adresse MAC: 00:0a:b4:00:4e:f7

État des ports LAN: État du port LAN1 Up 100Mb/s Full Duplex, État du port LAN2 Down

État des ports SHDSL

	Nom du port	État du lien SHDSL	Débit binaire	Marge de rapport signal à bruit	Atténuation de la ligne	Secondes erronées dans la dernière heure	Pertes de connexion dans les dernières 24 heures
<input checked="" type="radio"/>	SHDSL1	Connecté	5696 kbits/sec	18 dB (4/4)	1 dB	0	0
<input type="radio"/>	SHDSL2	Connecté	5696 kbits/sec	19 dB (4/4)	1 dB	1	0

Afficher

Redémarrer les connexions SHDSL

Rafraîchir

- Contrôler la qualité de chaque port SHDSL.

La marge de rapport signal à bruit doit être au moins de 2/4.

Le nombre de secondes erronées dans la dernière heure doit être proche de zéro.

Le nombre de pertes de connexion dans les dernières 24 heures doit être nul ou très faible.

- Si la marge de signal à bruit est de 1/4, avec le profil **STU-C standard**, attribuer le profil **STU-C Endurance** et contrôler à nouveau la connexion.
- Vérifier le bon fonctionnement en transmettant un PING périodique depuis le PC vers le XS distant ou vers un autre équipement au travers de la liaison SHDSL.

Note : On peut aussi utiliser la fonction PING intégrée au XS (menu **Diagnostics > Outils > PING**).

- Si, malgré ces modifications, la qualité reste insuffisante, ou si des déconnexions se produisent, ou si la connexion ne s'établit pas, vérifier la ligne :
  - Vérifier que chaque fil de la paire torsadée est enfoncé en butée dans la borne à vis du switch.
  - Vérifier que les raccordements intermédiaires des paires torsadées sont correctement serrés.
  - Retirer les parasurtenseurs de ligne qui peuvent éventuellement être défaillants.
  - Vérifier que le blindage, s'il existe est correctement connecté à la terre.

## PARAMETRAGE

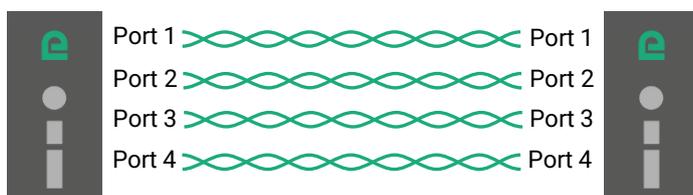
### 4 Mise en service d'une liaison au moyen de 2, 3 ou 4 paires torsadées

Le présent paragraphe décrit la mise en oeuvre d'une liaison point à point multiplexée.

Une liaison multiplexée est une liaison entre deux XS qui utilise deux ou trois ou quatre paires torsadées pour multiplier le débit total. Le débit obtenu est approximativement la somme des débits obtenus sur chaque paire torsadée.

Un XS avec deux ports SHDSL permet l'établissement d'une liaison multiplexée avec deux lignes ; le débit est approximativement doublé soit jusqu'à 11 Mb/s ou même 20 Mb/s jusqu'à 1 Km environ.

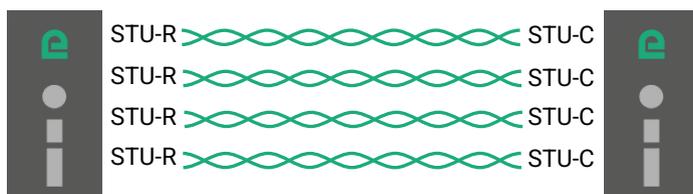
Un XS avec quatre ports SHDSL permet l'établissement d'une liaison multiplexée jusqu'à quatre lignes ou bien de deux liaisons de deux lignes chacune ; le débit est approximativement quadruplé soit jusqu'à 22 Mb/s ou même 40 Mb/s jusqu'à 1 Km environ.



#### Paramétrage :

Le paramétrage s'effectue de la même manière que pour la Mise en service d'une liaison au moyen d'une paire torsadée

- Attribuer le profil **STU-R, Auto** à tous les ports SHDSL du premier XS.
- Attribuer un profil de connexion à chacun des ports SHDSL de l'autre XS (**STU-C Standard** ou **STU-C Endurance** ou **STU-C Performance**).
- Agréger les lignes



#### Mode d'agrégation des lignes

Valeurs possibles :

- Pas d'agrégation
- 1 groupe de 2 lignes (XS avec 2 ports SHDSL)
- 2 groupes de 2 lignes (1-3) et (2-4) (XS avec 4 ports SHDSL)
- 1 groupe de 4 lignes (XS avec 4 ports SHDSL)

## 5 Paramétrage avancé d'une liaison SHDSL

Dans des cas particuliers, il peut être utile de modifier l'un des profils de connexion préprogrammé pour modifier la marge de rapport signal à bruit ou bien forcer une modulation, par exemple.

Le profil modifié s'ajoute aux cinq profils

**Pour ajouter un profil de connexion,**

- Dans le menu, choisir **Configuration > Ethernet & commutation > Ports SHDSL**,
- Cocher la case **Montrer les paramètres avancés**,

The screenshot shows the 'Ports SHDSL' configuration page. The breadcrumb trail is: Accueil > Configuration > Ethernet et commutation > Ports SHDSL. The page title is 'XSLAN+2220 Switch SHDSL.bis'. The left sidebar contains a navigation menu with 'Configuration' expanded to 'Ethernet et commutation' and 'Ports SHDSL' selected. The main content area shows settings for 'Port SHDSL1' and 'Port SHDSL2'. For 'Port SHDSL1', 'Activer le port SHDSL1' is checked and 'Profil de connexion SHDSL1' is set to 'STU-R, Auto'. For 'Port SHDSL2', 'Activer le port SHDSL2' is checked and 'Profil de connexion SHDSL2' is set to 'STU-C, Standard'. Under 'Agrégration EFM', 'Mode d'agrégation des lignes' is set to 'Pas d'agrégation'. The 'Paramètres avancés' section has 'Montrer les paramètres avancés' checked. Below this is a table of 'Profils SHDSL' with the following data:

	Nom du profil	Mode de connexion	Commentaire
<input checked="" type="radio"/>	STU-R, Auto	Mode STU-R	
<input type="radio"/>	STU-C, Standard	Mode STU-C	
<input type="radio"/>	STU-C, Performance	Mode STU-C	
<input type="radio"/>	STU-C, Endurance	Mode STU-C	
<input type="radio"/>	STU-C, Fixed datarate	Mode STU-C	

Buttons at the bottom include 'Afficher', 'Modifier', 'Supprimer', 'Ajouter ...', 'Copier et modifier', 'Enregistrer', and 'Annuler'.

- Sélectionner l'un des profils enregistrés.
- Cliquer **Copier et modifier**.

La fenêtre du profil correspondant s'affiche ; elle permet de régler les paramètres suivants.

- Cliquer **Enregistrer** ; le profil créé apparaît dans la liste des profils et peut être sélectionné.

The screenshot shows a web browser window with the URL 192.168.0.128/index-fr.html. The page title is 'XSMIL-BP4200 Switch SHDSL.bis'. The breadcrumb navigation is '> Accueil > Configuration > Ethernet et commutation > Ports SHDSL > Profils SHDSL'. A warning message 'Valeurs non valides sur la page' is displayed. The 'Réglages généraux' section contains the following fields:

- Nom du profil: STU-C, Performance
- Commentaire: (empty)
- Sélectionner automatiquement STU-R/C:

The 'Adaptation du débit à la ligne' section contains the following fields:

- Système d'adaptation du débit: Recherche par dichotomie (Meilleure adaptation du débit à la ligne)
- Nombre de tentatives de bisection: 6 (de 3 à 6, multiple de 1)
- Marge minimale: 5 (de -10 à 21, multiple de 1)
- Marge maximale: 6 (de -10 à 21, multiple de 1)
- Débit binaire minimal: 0 (de 0 à 15232, multiple de 64)
- Activer les débits supérieurs à 5696 kbps:
- Temps minimal de connexion avant d'autoriser une reconnexion rapide: 0 (de 0 à 86400, multiple de 1)
- Timeout de la tentative de reconnexion rapide: 0 (de 0 à 120, multiple de 1)

The 'Réglages avancés' section contains the following fields:

- Annexe: Annexe A
- Liste de capacités: Nouveau mode
- Mode Power Back-Off: Normal
- Utiliser EPL pour calculer le Power Back-Off:
- Activer la renégociation automatique:

Buttons at the bottom: Enregistrer, Annuler, Retour.

## Réglages généraux :

### Sélectionner automatiquement STU-R/C

Si la case est cochée, le XS tente alternativement de se connecter en mode STU-C et STU-R. Ainsi la connexion peut être établie sans se soucier du mode choisi pour le XS distant.

### Mode de connexion

Valeurs possibles : STU-C : le XS a l'initiative de la connexion et en négocie les conditions.  
STU-R : Le XS attend la connexion.

## Adaptation du débit à la ligne :

### Système d'adaptation du débit

Valeurs possibles : Examen de ligne (Rapide, mais adaptation approximative)  
Recherche par dichotomie (Meilleure adaptation du débit à la ligne, mais plus long)  
Débit fixe (Connexion plus rapide, mais pas d'adaptation à la ligne)

### Mode « Examen de la ligne » :

Une mesure succincte pour estimer l'atténuation de la ligne est effectuée au préalable. La connexion est ensuite établie au débit qui permet d'obtenir la marge de rapport signal sur bruit ciblée.

## Débit binaire minimum

C'est la valeur de débit minimum autorisé pour cette connexion.

Valeurs possibles : 192 à 5696 kb/s par pas de 64 Kb/s

## Débit binaire maximum

C'est la valeur de débit maximum autorisé pour cette connexion.

Valeurs possibles : 192 à 5696 kb/s par pas de 64 Kb/s

## Marges utilisées

La détermination de la marge de rapport signal sur bruit peut être déterminée soit selon les conditions courantes (CC) ou selon des conditions prédéfinies considérées comme les pires (WC).

Valeurs possibles : Marge CC, Marge WC, Marge CC et WC, aucune

Valeur par défaut : Marge CC

## Marge de SNR CC

C'est la marge de sécurité qui est souhaitée au-dessus du seuil minimum de fonctionnement.

Lorsque le XS établit la connexion, il mesure le rapport signal à bruit et retranche la marge de rapport signal à bruit.

Si le résultat est supérieur au minimum requis, la liaison est établie.

Valeurs possibles : -10 à 21 dB

## Marge de SNR CC alternative

Visible lorsque le paramètre « Système d'adaptation du débit » est réglé sur « Examen de ligne ».

Si la connexion avec la valeur de marge de rapport signal sur bruit ne peut s'établir, alors le XS tente de se connecter avec cette marge de SNR alternative. La valeur doit être plus élevée que la précédente, ce qui aura pour conséquence une connexion à un débit plus faible.

Valeurs possibles : -10 à 21 dB

## Mode « Recherche par dichotomie » :

Le XS effectue successivement plusieurs connexions à différents débits jusqu'à obtenir une connexion qui satisfasse les critères demandés de débit et de marge de rapport signal sur bruit.

## Nombre de tentatives de bisection

Plus ce nombre est élevé et plus le résultat sera précis mais le temps d'établissement de la connexion sera plus long.

Valeurs possibles : 3 à 6

## Marge minimale

C'est la marge minimale de rapport signal sur bruit acceptable pour cette connexion.

Valeurs possibles : -10 à 21 dB

## Marge maximale

C'est la marge maximale de rapport signal sur bruit acceptable pour cette connexion. Plus la plage de marge entre minimale et maximale est grande et plus le résultat sera rapide mais imprécis.

Valeurs possibles : -10 à 21 dB

## Débit binaire minimal

En définissant un débit binaire minimal, on interdit la connexion à un débit jugé trop faible. Ceci est utile dans une topologie avec liaisons redondantes où il vaut mieux emprunter la liaison de secours plutôt que la liaison principale lorsque les conditions de la ligne sont devenues mauvaises.

Valeurs possibles : 0 à 15232 kb/s par pas de 64 Kb/s (0 si inutilisé)

## PARAMETRAGE

### Activer les débits supérieurs à 5696 kbps

Laisser cette case décochée si on sait que la distance de la ligne ne permet pas de se connecter à des débits supérieurs. Ainsi la plage de valeurs de débits essayées sera plus étroite et le résultat sera plus précis ou plus rapide.

### Temps minimal de connexion avant d'autoriser une reconnexion rapide

Si la connexion est stable depuis un certain temps et si une déconnexion survient par exemple à cause d'une brève perturbation, il est probable que les conditions de la ligne n'ont pas changé. Aussi le XS peut tenter la reconnexion directe au même débit que précédemment ce qui permet de réduire considérablement la durée d'indisponibilité de la liaison.

Valeurs possibles : 0 à 86400 s (0 si inutilisé)

### Timeout de la tentative de reconnexion rapide

Lorsqu'une déconnexion survient et que le XS détecte à nouveau l'équipement à l'autre extrémité avant ce Timeout alors il peut tenter la reconnexion directe au même débit que précédemment ce qui permet de réduire considérablement la durée d'indisponibilité de la liaison.

Valeurs possibles : 0 à 120 s (0 si inutilisé)

### Réglages avancés :

#### Annexe

Valeurs possibles : Annexe A ou Annexe B

Valeur par défaut : Annexe A

#### Constellation PAM

La constellation PAM désigne la technique de modulation utilisées.

Valeurs possibles : Automatique, PAM16, PAM32

Valeur par défaut : Automatique

#### Liste des capacités

La liste des capacités échangées entre les switches peut s'effectuer selon un ancien mode pour inter-opérer avec des switches d'ancienne génération (XSLAN-).

Valeurs possibles : Automatique, Ancien mode, nouveau mode

Valeur par défaut : Automatique

#### Mode power-back off

Permet de réduire la puissance d'émission lorsque les lignes sont courtes afin de moins perturber les lignes environnantes par diaphonie.

Valeurs possibles : Normal, forcé

Valeur par défaut : normal

#### Utiliser EPL pour calculer le power back-off

TBD

#### Activer les débits étendus

Cocher cette case pour activer les débits étendus qui permettent de transmettre jusqu'à 15 Mb/s lorsque la ligne mesure moins de 1 Km.

#### Constellation PAM étendue

La constellation PAM désigne la technique de modulation utilisées.

Valeurs possibles : Automatique, PAM 4, PAM8, PAM16, PAM32, PAM64, PAM128

Valeur par défaut : Automatique

#### Activer la renégociation automatique

La liaison SHDSL est établie en fonction des conditions de la ligne au moment de la connexion. Par exemple un bruit peut exister sur le câble à cet instant et disparaître par la suite. Par défaut le switch ne renégocie

pas de nouveau sa liaison, la marge de rapport signal sur bruit sera plus importante que prévue. Si cette case est cochée le switch renégociera sa liaison qui pourra s'établir à un débit supérieur.

### **Marge minimale pour renégociation (dB)**

La renégociation entraîne une déconnexion et donc une perte de service, le temps du rétablissement. C'est pourquoi la renégociation ne doit être tentée que si la marge s'est accrue de manière très significative, ce qui permettra une augmentation importante du débit.

### **Durée minimale avant renégociation (heures)**

La renégociation entraîne une déconnexion et donc une perte de service, le temps du rétablissement. C'est pourquoi la renégociation ne doit être tentée que si la marge s'est accrue de manière très durable.

### 6.1 Présentation

L'objectif du protocole est

d'établir à chaque instant un réseau offrant un chemin unique entre deux devices en bloquant les liens qui forment des boucles et provoquent des dysfonctionnement d'Ethernet. Le réseau prend alors la forme d'un arbre dépourvu de boucles.

d'établir dynamiquement un autre réseau arborescent en cas de défaillance d'un lien ou d'un bridge en utilisant certains des liens bloqués en temps normal.

Le protocole RSTP est décrit par la norme IEEE 802-1D 2004. Un équipement qui gère

Un bridge du réseau est élu automatiquement « racine de l'arbre de recouvrement ».

Il a en particulier pour fonction d'émettre sur ses différents ports une trame appelée BPDU qui est propagée par les bridges.

La trame BPDU comporte un champ que l'on peut appeler compteur d'âge ; le compteur d'âge est incrémenté à chaque passage dans un bridge ; le compteur d'âge est donc l'image du nombre de sauts franchis par la trame BPDU depuis la racine.

La trame BPDU comporte également un champ de coût de route ; le coût de route est incrémenté de la valeur du coût de port à chaque passage dans un bridge ; en comparant le coût de route contenu dans les trames BPDU reçues sur deux ports différents, chaque bridge détermine la meilleure route depuis la racine.

Lorsqu'un bridge reçoit la trame BPDU sur deux de ses ports ou davantage, il ne conserve à l'état actif (Etat Forwarding) qu'un seul port : Celui par lequel il a reçu la trame BPDU avec le coût de route minimum.

Les autres ports sont des chemins redondants d'une distance plus longue ; ils sont bloqués par le bridge.

Le trafic reçu par un bridge sur un port bloqué n'est pas retransmis ; et aucun trafic n'est émis par un bridge vers un port bloqué.

Lorsque le bridge ne reçoit plus la trame BPDU et après le délai fixé par le hello time, le port est bloqué et le port bloqué présentant le coût de route minimum est rendu actif.

Une trame d'avertissement est émise par le bridge qui modifie l'état de ses ports.

Les autres bridges tiennent compte de cette modification et après une période dite de convergence, le nouvel état de l'arbre est pris en compte par l'ensemble des bridges.

Classification des ports :

Un port P2P est un port reliant directement deux équipements RSTP ; c'est à dire, en particulier, sans l'intermédiaire d'un switch « non RSTP ». Par exemple, les ports SHDSL d'un XS doivent être déclarés comme ports P2P.

Un port Edge est un port situé à la frontière du réseau ; il relie un switch RSTP à un équipement n'agissant pas comme bridge ; par exemple un port Ethernet qui relie le XS à un PC ou un automate est un port Edge

## 6.2 Configuration

- Dans le menu, choisir **Configuration > Ethernet & commutation > RSTP – Anneau redondant**.
- Sélectionner le mode **RTSP**.

The screenshot shows the Etic administration web interface. The browser address bar shows '192.168.0.128/index-fr.html'. The page title is 'XSLAN+2220 Switch SHDSL.bis'. The navigation menu on the left includes 'Configuration', 'Ethernet et commutation', 'Ports SHDSL', 'Ports LAN', 'RSTP - Anneau redondant', 'VLAN', 'Filtrage d'adresses MAC', 'Protocole IP et routage', 'Alarmes', 'Passerelles IP-RS', 'Sécurité', 'Système', 'Diagnostics', 'Maintenance', and 'À propos'. The main content area shows the configuration for 'RSTP - Anneau redondant'. The configuration includes a table for general RSTP settings and a table for port-specific RSTP settings.

Mode	Priorité du bridge	Hello time (s)	Forward delay (s)	Maximum age (s)	Age increment
RSTP	8192 (de 0 à 61440, multiple de 4096)	2 (de 1 à 10, multiple de 1)	15 (de 4 à 30, multiple de 1)	20 (de 6 à 40, multiple de 1)	Valeur normalisée

Réglages RSTP par port

Identifiant du port	Désactiver RSTP sur ce port	Priorité du port	Coût du port	Edge port	P2P port
SHDSL1	Non	64	20000000	Non	Oui
SHDSL2	Non	64	20000000	Non	Oui
SHDSL3	Non	64	20000000	Non	Oui
SHDSL4	Non	64	20000000	Non	Oui
LAN1	Non	64	20000000	Non	Auto
LAN2	Non	64	20000000	Non	Auto
LAN3	Non	64	20000000	Non	Auto
LAN4	Non	64	20000000	Non	Auto

La page est divisée en deux parties :

- Les paramètres généraux
- Les paramètres des ports SHDSL et Ethernet 10/100

### Paramètres généraux :

#### Priorité du bridge

Ce paramètre s'associe à l'adresse MAC pour former l'identité du bridge (bridge ID).

Il est utilisé par le réseau pour déterminer quel bridge doit être élu racine de l'arbre (root spanning tree).

Le bridge racine est celui qui a le plus faible bridge ID.

#### Hello time

Ce paramètre fixe la période d'émission des messages BPDU propagés par le XS.

Il doit être le même pour tous les bridges du réseau.

Un port actif (Forwarding) est rendu bloqué lorsque la trame BPDU n'a pas été reçue à l'issue de deux hello.

#### Forward delay

Le paramètre « Forward delay » n'est pris en compte ni sur les ports P2P, ni sur les ports Edge.

Quand la topologie du réseau change suite à la défaillance d'une liaison par exemple, le port bloqué le plus

## PARAMETRAGE

favorable (celui qui a le coût de route le plus faible) passe dans l'état « Listening / learning » :

Le port vérifie qu'il reçoit les trames BPDU et fait l'apprentissage des adresses MAC des trames reçues sur ce port.

Il reste dans cet état durant le délai fixé par le paramètre « Forward delay » de façon à éviter la création de boucles transitoires qui pourraient être créées pendant la convergence.

Il est conseillé d'attribuer la valeur 15 secondes pour un réseau de diamètre 7 ; un réseau de diamètre 7 est un réseau dont le chemin le plus long entre deux devices comporte le passage par sept switches.

### Maximum age

Si le compteur d'âge de la trame BPDU a atteint la valeur attribuée au paramètre « Maximum age », la trame BPDU n'est pas propagée par le bridge.

La valeur attribuée au paramètre « Maximum age » doit être assez grande pour que n'importe quel bridge du réseau, même très éloigné de la racine, puisse recevoir la trame BPDU.

La valeur « Maximum age » doit être inférieure à deux fois la valeur attribuée au paramètre « Forward delay » - 2.

Par exemple, si dans la totalité du réseau, le chemin le plus long pour aller d'un device à un autre fait passer par 10 bridges, alors la valeur minimale à attribuer au paramètre « maximum age » sera 10 plus une marge de sécurité égale trois fois la valeur attribuée au hello time.

Exemple :

Diamètre du réseau : 10

Hello time : 2

Forward delay : 15

Maximum age préconisé :  $10 + 3 * 2 = 16$

Valeur du « maximum age » à ne pas dépasser :  $FD * 2 - 2 = 28$

### Age increment

Valeur de l'incrément du compteur d'âge au passage dans le bridge.

## Paramètres associés à chaque port Ethernet & SHDSL :

- Sélectionner le port à paramétrer dans le tableau.

### Identifiant du port

Sélectionner le N° de port (Ethernet 1 à 4 or SHDSL 1 ou 2).

### Désactiver RTSP sur ce port

Cocher cette case lorsque le port ne participe pas au protocole RSTP.

Remarque : Il est recommandé de laisser cette case non cochée en sorte que tous les ports participent au protocole RSTP.

### Priorité du port

Ce paramètre permet de privilégier un chemin plutôt qu'un autre.

Plus la valeur est basse plus le chemin est prioritaire.

### Coût du port

Ce paramètre traduit le débit du port.

Il est utilisé dans les calculs du chemin actif pour rendre plus prioritaire un chemin à haut débit.

Un bas coût est attribué à un chemin à haut débit.

Les valeurs suivantes sont recommandées :

Port SHDSL : 200 000 000

Port Ethernet 100 Mb/s : 200 000

### Edge port »

Un port « Edge » est un port situé à la frontière du réseau ; il ne se comporte pas en bridge.

Les trames BPDU ne peuvent être retransmises vers un port Edge. De plus ce type de port ne peut être bloqué par le bridge.

Un port connecté à un automate, par exemple doit être désigné comme un port Edge.

Remarque : Un port Edge passe dans le mode « P2P » lorsqu'il reçoit une trame BPDU ; ainsi, si un bridge supplémentaire est branché sur un port initialement configuré en Edge, le nouveau bridge est automatiquement intégré au réseau RSTP.

### P2P port

Définit si un port est connecté directement à un autre port participant au protocole RSTP.

Cette information permet de passer directement de l'état « bloqué » à l'état « Forwarding » sans passer par l'état « learning » ce qui permet au protocole RSTP de converger plus rapidement et de détecter plus rapidement les modifications de topologie du réseau dues aux défaillances.

Les ports SHDSL doivent être déclarés comme port P2P.

## 7 Anneau redondant

Basé sur le protocole RSTP, cet algorithme propriétaire est adapté à la gestion d'une topologie en anneau comptant jusqu'à 16 switches SHDSL.

L'un des switches de l'anneau est désigné comme le switch « maître » ; il a comme fonction d'émettre des trames BPDU sur une liaison SHDSL et de les recevoir et de les bloquer sur l'autre liaison SHDSL afin de détecter la défaillance d'un lien ou d'un switch.

Lorsque la défaillance d'un lien se produit, le « Ring master » active son second port SHDSL afin de rétablir le fonctionnement normal.

Les avantages de cette solution sont la simplicité de configuration et la rapidité de cicatrisation (1 seconde pour un anneau comptant 5 XS).

Remarque : Dans ce mode, les ports Ethernet 10/100 BT ne participent pas au protocole.

### Configuration du Ring master :

- Dans le menu, choisir **Configuration > Ethernet & commutation > RSTP – Anneau redondant**.

The screenshot shows a web browser window titled "Etic administration" with the address bar displaying "192.168.0.128/index-fr.html". The page content is for the configuration of "XSLAN+2220 Switch SHDSL.bis". The breadcrumb navigation is "> Accueil > Configuration > Ethernet et commutation > RSTP - Anneau redondant".

On the left, there is a green sidebar menu with the following items: Accueil, Configuration (expanded), Ethernet et commutation (expanded), Ports SHDSL, Ports LAN, RSTP - Anneau redondant (selected), VLAN, Filtrage d'adresses MAC, Protocole IP et routage, Alarmes, Passerelles IP-RS, Sécurité, Système, Diagnostics, Maintenance, and À propos.

The main configuration area has the following settings:

- Mode: Anneau Redondant (dropdown menu)
- Ring Master:
- Port bloqué par défaut: Port SHDSL 1 bloqué (dropdown menu)

Buttons for "Enregistrer" and "Annuler" are present above and below the configuration fields. A red message states "Modifications sur la page non enregistrées".

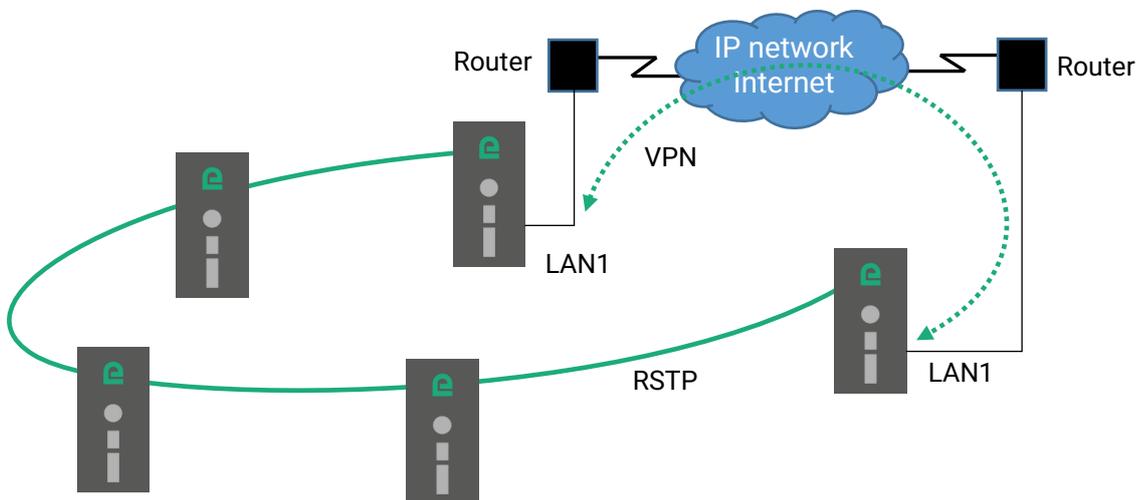
- Sélectionner le mode **Anneau redondant**.
- Cocher la case **Ring master**.
- Sélectionner le port SHDSL bloqué en situation normal (1 ou 2).
- Cliquer **Enregistrer**.

### **Configuration des autres switches SHDSL de l'anneau**

- Dans le menu, choisir **Configuration > Ethernet & commutation > RSTP – Anneau redondant**.
- Sélectionner le mode **Anneau redondant**.
- Laisser la case **Ring master** non sélectionnée.
- Cliquer **Enregistrer**.

## 8 VPN de bouclage

Quand le réseau est de type multipoints (c'est à dire une chaîne de switches SHDSL), et quand cependant il n'est pas possible de former un anneau sécurisé, la fonction « VPN de bouclage » permet de réaliser la redondance du réseau si un accès réseau WAN public (Internet) ou privé (MPLS) est disponible à chaque extrémité de la branche.



Les 2 XS d'extrémité établissent un VPN à travers le réseau WAN. Ce VPN assure une connectivité au niveau Ethernet. Ainsi en activant le protocole RSTP la redondance peut être assurée par ce VPN.

Un XS doit être configuré en mode serveur VPN et doit pouvoir être accessible par une adresse IP fixe à travers le réseau WAN. L'autre XS doit être configuré en mode client VPN.

Le VPN est établi à travers le port LAN Ethernet 1 du XS qui devient un port « WAN » avec une adresse IP propre. Ce port Ethernet doit être raccordé au routeur d'accès au réseau WAN et de ce fait, ne peut plus être utilisé pour raccorder un autre équipement accessible à travers la liaison SHDSL.

### Configuration du VPN

- Dans le menu, choisir **Configuration > Protocole IP et routage > VPN de bouclage**.
- Cocher la case **Activer le VPN**.

Etic administration

192.168.0.128/index-fr.html

etec Telecom

XSLAN+2220 Switch SHDSL.bis

> Accueil > Configuration > Protocole IP et routage > VPN de bouclage

Enregistrer Annuler Modifications sur la page non enregistrées

Activer le VPN

Adresse IP WAN locale 10.10.2.56

Masque de sous réseau 255.255.255.0

Mode Serveur

Adresse IP du serveur VPN 194.240.12.17

Port 1195 (de 1 à 65000, multiple de 1)

Protocole UDP

Clé pré-partagée ..... Passwords match

Enregistrer Annuler

### Adresse IP WAN locale

C'est l'adresse IP attribuée au port LAN1 du XS dans le réseau IP du routeur d'accès WAN. Ce réseau est différent de celui utilisé sur les autres ports LAN.

### Masque de sous-réseau

Masque du sous réseau.

### Mode serveur

Cocher cette case à cocher sur le XS utilisé comme serveur VPN. Laisser la case décochée sur celui utilisé comme client VPN.

### Adresse IP du serveur VPN

Lorsque le XS est le client VPN, c'est l'adresse IP pour joindre le XS serveur VPN. Cette adresse IP n'est pas nécessairement celle attribuée au XS serveur VPN dans le champ « Adresse IP WAN locale » si le VPN traverse des routeurs avec translation d'adresse (NAT).

### Port

Numéro de port TCP ou UDP utilisé pour le VPN.

### Protocole

Protocole TCP ou UDP utilisé pour le VPN.

### Clé pré-partagée

C'est une chaîne de caractères secrète qui sert pour le cryptage et l'authentification du trafic VPN. Elle doit être la même dans les 2 XS du VPN.

## 9 Réseau virtuel VLAN

### 9.1 Vue d'ensemble

#### Fonction des VLAN

La technique des réseaux privés virtuels conforme à la norme IEEE 802.1Q permet de faire coexister jusqu'à 4096 réseaux virtuels sur le même réseau Ethernet.

Les équipements appartenant à un même VLAN peuvent communiquer entre eux mais ne peuvent communiquer avec ceux d'un autre VLAN hormis par l'intermédiaire d'un routeur IP ou un switch de niveau 3.

#### Ports Ethernet

Quand on parle des ports Ethernet du XS, cela inclut les port LAN Ethernet 10/100 BT, mais aussi les ports SHDSL. Tous les ports SHDSL sont considérés comme un seul port.

#### Principes de fonctionnement

Toutes les trames Ethernet appartenant à un même VLAN sont marquées par une étiquette de Numéro de VLAN appelée Tag ou VLAN ID. Cette étiquette est un champ particulier de la trame Ethernet.

Lorsqu'un N° de VLAN est inscrit dans ce champ, on dit que la trame Ethernet est tagguée.

A l'entrée, sur chaque port Ethernet, les trames non tagguées prennent le N° de VLAN affecté au port.

A la sortie, un port Ethernet ne peut transmettre vers l'extérieur que les trames Ethernet du (ou des) VLAN auquel le port appartient. La trame peut être transmise avec ou sans son tag.

#### Serveur d'administration et passerelles série

Le serveur d'administration et les passerelles série peuvent également être affectées à un VLAN particulier.

Si la passerelle série n'appartient pas au même VLAN que l'administration, alors une adresse IP spécifique doit être attribuée aux passerelles série.

## 9.2 Paramétrage

Attention :

Avant d'enregistrer la configuration VLAN, assurez-vous que vous pourrez accéder au serveur d'administration par un port LAN Ethernet ou à distance par la ligne. Au moins un des ports Ethernet doit faire partie du même VLAN que le serveur d'administration du XS.

- Dans le menu, choisir **Configuration > Ethernet & Commutation > VLAN**.
- Cocher la case **Activer les VLANs**.

**etec** Telecom

**XSLAN+2220** Switch SHDSL.bis

> Accueil > Configuration > Ethernet et commutation > VLAN

Enregistrer Annuler Modifications sur la page non enregistrées

Attention : vérifiez vos réglages avant de sauvegarder, vous pourriez perdre l'accès au serveur web d'administration.

Activer les VLANs

VLAN ID pour l'administration  (de 0 à 4095, multiple de 1)

VLAN ID pour les passerelles série  (de 0 à 4095, multiple de 1)

**VLANs : Politique de sortie**

Cette table définit la politique de sortie des trames lorsque la gestion par VLAN est activée.

	Nom du VLAN	ID du VLAN	politique de sortie LAN1	politique de sortie LAN2	politique de sortie LAN3	politique de sortie LAN4	politique de sortie SHDSL
<input checked="" type="radio"/>	VLAN4	4	Les trames sortent taggées	Le port n'appartient pas au VLAN	Le port n'appartient pas au VLAN	Le port n'appartient pas au VLAN	Les trames sortent taggées
<input type="radio"/>	VLAN5	5	Les trames sortent taggées	Le port n'appartient pas au VLAN	Le port n'appartient pas au VLAN	Le port n'appartient pas au VLAN	Les trames sortent taggées
<input type="radio"/>	VLAN12	12	Le port n'appartient pas au VLAN	Les trames sortent non taggées	Le port n'appartient pas au VLAN	Le port n'appartient pas au VLAN	Les trames sortent taggées

Afficher Modifier Supprimer Ajouter ... Copier et modifier ▲ ▼ < >

**VLANs : Politique d'entrée**

Ces paramètres définissent la politique d'entrée des trames lorsque la gestion par VLAN est activée.

Politique d'entrée LAN1 Refuser les trames n'appartenant pas à un des VLANs associés au port ▼

VLAN ID d'entrée LAN1  (de 0 à 4095, multiple de 1)

Politique d'entrée LAN2 Refuser les trames n'appartenant pas à un des VLANs associés au port ▼

VLAN ID d'entrée LAN2  (de 0 à 4095, multiple de 1)

Politique d'entrée LAN3 Refuser les trames n'appartenant pas à un des VLANs associés au port ▼

VLAN ID d'entrée LAN3  (de 0 à 4095, multiple de 1)

Politique d'entrée LAN4 Refuser les trames n'appartenant pas à un des VLANs associés au port ▼

VLAN ID d'entrée LAN4  (de 0 à 4095, multiple de 1)

Politique d'entrée SHDSL Refuser les trames n'appartenant pas à un des VLAN configurés ▼

VLAN ID d'entrée SHDSL  (de 0 à 4095, multiple de 1)

Enregistrer Annuler

La page permet de définir la politique de sortie, la politique d'entrée et les N° de VLAN du serveur d'administration et des passerelles série.

## PARAMETRAGE

### 9.2.1 Politique de sortie

La politique de sortie consiste à enregistrer les VLAN et définir l'appartenance ou non des ports Ethernet à chaque VLAN et le traitement à appliquer le cas échéant.

Le traitement qui peut être appliqué à une trame sortante est :

- Les trames sortent tagguées
- Les trames sortent non tagguées
- Les trames sortent non modifiées
- Le port n'appartient pas au VLAN

Exemple simplifié ;

On définit trois VLAN : le 4, le 5 et le 12.

Le port LAN1 est abonné aux VLAN 4 et 5. Les trames appartenant à ces VLAN sortent par le port LAN1 tagguées.

Le port LAN2 est abonné au VLAN 12. Les trames appartenant à ce VLAN sortent par le port LAN2 non tagguées.

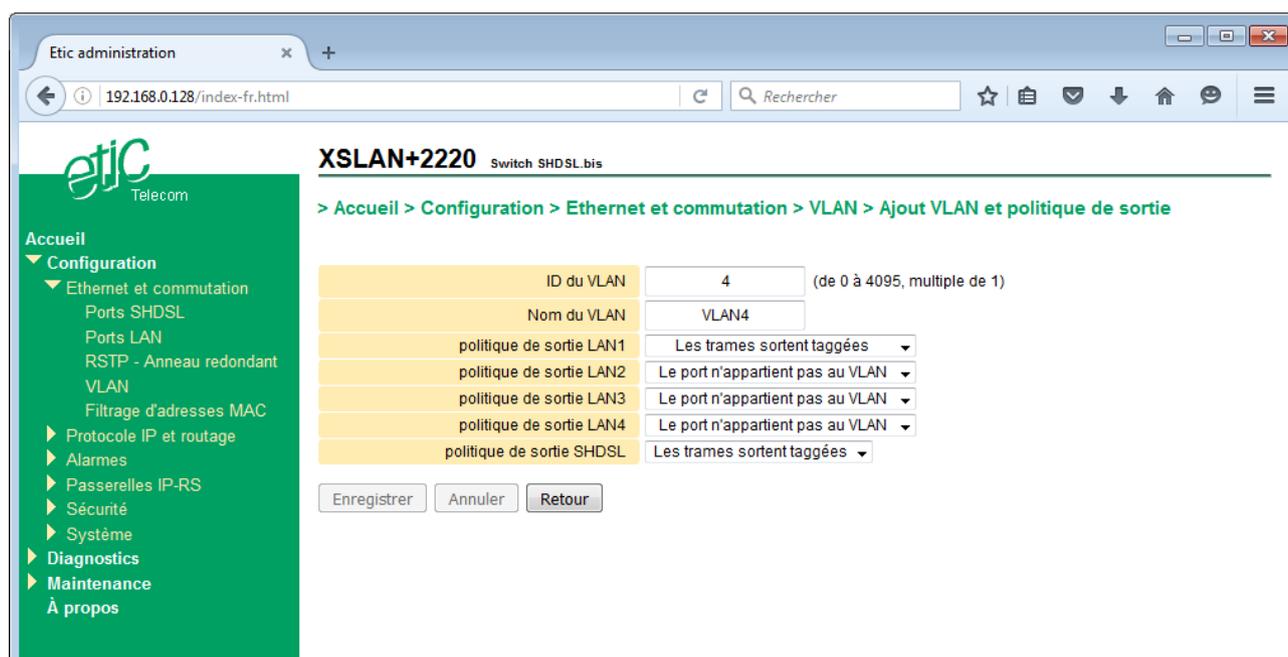
Les ports LAN3 et LAN4 ne sont abonnés à aucun VLAN (non utilisés).

Les port SHDSL sont abonnés à tous les VLAN. Toutes les trames sont transmises vers le réseau SHDSL tagguées.

Politique de sortie	LAN1	LAN2	LAN3	LAN4	SHDSL
VLAN 4	Oui – tagguée	Non	Non	Non	Oui – tagguée
VLAN 5	Oui – tagguée	Non	Non	Non	Oui – tagguée
VLAN 12	Non	Oui – non tagguée	Non	Non	Oui – tagguée

**Pour paramétrer la politique de sortie,**

- Dans le menu, choisir **Configuration > Ethernet & Commutation > VLAN**.
- Cliquer **Ajouter**.
- Saisir le N° de VLAN à enregistrer et lui donner un nom.
- Abonner chaque port Ethernet en indiquant si une trame du VLAN peut sortir sur ce port, et le traitement à appliquer à la trame.



### ID du VLAN

Saisir le N° de VLAN à enregistrer.

### Nom du VLAN

Attribuer un nom à ce VLAN.

### Politique de sortie LAN1 (ou 2, ou 3, ou 4)

#### Les trames sortent tagguées

Les trames Ethernet appartenant à ce VLAN peuvent sortir sur le port LAN1 (ou 2 ou 3 ou 4).  
Les trames sortent tagguées.

#### Les trames sortent non tagguées

Les trames Ethernet appartenant à ce VLAN peuvent sortir sur le port LAN1 (ou 2 ou 3 ou 4).  
Les trames sortent non tagguées.

#### Les trames sortent non modifiées

Les trames Ethernet appartenant à ce VLAN peuvent sortir sur le port LAN1 (ou 2 ou 3 ou 4).  
Les trames sortent sans modification (tagguées ou non tagguées selon le cas).

#### Le port n'appartient pas au VLAN

Les trames Ethernet appartenant à ce VLAN ne peuvent pas sortir sur le port LAN1 (ou 2 ou 3 ou 4).

### Politique de sortie SHDSL

#### Les trames sortent tagguées

Les trames Ethernet appartenant à ce VLAN sont transmises vers le ou les ports SHDSL.  
Les trames sortent tagguées.

Note : Dans les cas simples, les ports SHDSL doivent être abonnés à tous les VLAN afin que les trames Ethernet provenant de tous les équipements connectés localement au XS soient transmises vers la ligne SHDSL.

## PARAMETRAGE

### 9.2.2 Politique d'entrée

La politique d'entrée consiste à définir le traitement appliqué aux trames Ethernet quand elles entrent dans le switch.

On définit

**quelles trames déjà tagguées à l'extérieur du switch sont acceptées ou refusées à l'entrée du switch.**

**quel N° de VLAN doit être appliqué aux trames non tagguées à l'entrée du switch.**

Exemple :

Poursuivons l'exemple du paragraphe précédent ; la politique de sortie enregistrée est résumée par le tableau ci-dessous.

Politique de sortie	LAN1	LAN2	LAN3	LAN4	SHDSL
VLAN 4	Oui – tagguée	Non	Non	Non	Oui – tagguée
VLAN 5	Oui – tagguée	Non	Non	Non	Oui – tagguée
VLAN 12	Non	Oui – non tagguée	Non	Non	Oui – tagguée

Le tableau ci-dessous définit la politique d'entrée :

	LAN1	LAN2	LAN3	LAN4	SHDSL
N° de VLAN	4	12	0	0	12
Ne rien refuser					
Refuser les trames n'appartenant pas à l'un des VLAN du réseau					X
Refuser les trames n'appartenant pas à l'un des VLAN du port	X	X	X	X	

#### LAN1

Seules les trames tagguées avec le VLAN ID 4 ou 5 peuvent entrer par ce port.

Les trames non tagguées sont affectées au VLAN 4 et peuvent entrer par ce port.

#### LAN2

Seules les trames tagguées avec le VLAN ID 12 peuvent entrer par ce port.

Les trames non tagguées sont affectées au VLAN 12 et peuvent entrer par ce port.

#### LAN3 et LAN4

Aucune trame ne peut entrer par ces ports.

#### SHDSL

Seules les trames tagguées avec le VLAN ID 4 ou 5 ou 12 peuvent entrer par ce port.

Les trames non tagguées sont affectées au VLAN 12 et peuvent entrer par ce port.

## Pour paramétrer la politique d'entrée,

- Dans le menu, choisir **Configuration > Ethernet & Commutation > VLAN**.
- Successivement pour chaque port Ethernet, choisir la politique d'entrée et le VLAN ID affecté aux trames non tagguées.

### Politique d'entrée LAN1 (ou 2 ou 3 ou 4 ou SHDSL)

#### Ne rien refuser

Toutes les trames qui entrent sur les ports Ethernet sont acceptées qu'elles soient non tagguées ou déjà tagguées.

Si elles ne sont pas déjà tagguées, elles prennent le N° de VLAN du port.

Si elles sont déjà tagguées, le N° de VLAN n'est pas modifié.

#### Refuser les trames n'appartenant pas à un des VLAN configurés

Les trames qui ne sont pas déjà tagguées, prennent le N° de VLAN du port.

Les trames déjà tagguées qui entrent sur le port Ethernet sont acceptées seulement si leur N° de VLAN est l'un de ceux qui a été préalablement enregistré (voir politique de sortie).

Les trames tagguées avec un N° de port autre sont refusées.

#### Refuser les trames n'appartenant pas au VLAN associé au port

Les trames qui ne sont pas déjà tagguées, prennent le N° de VLAN du port.

Les trames déjà tagguées qui entrent sur le port Ethernet sont acceptées seulement si leur N° de VLAN est l'un de ceux auquel ce port Ethernet est abonné (voir politique de sortie).

Les trames tagguées avec un N° de port autre sont refusées.

### VLAN ID d'entrée LAN1 (ou 2 ou 3 ou 4 ou SHDSL)

C'est le n° de VLAN affecté à une trame qui arrive non tagguée.

## 9.3 Serveur d'administration et passerelles série

Quand les VLAN sont activés, Le serveur d'administration et les passerelles série doivent appartenir à un VLAN.

### VLAN ID pour l'administration

N° de VLAN auquel appartient le serveur d'administration.

### VLAN ID pour les passerelles série

N° de VLAN auquel appartiennent les passerelles série.

#### Remarque :

Si les passerelles série n'appartiennent pas au même VLAN que le serveur d'administration, alors une adresse particulière doit être affectée aux passerelles série.

- Dans le menu, choisir **Configuration > Protocole IP et routage > Protocole IP**.
- Cocher la case **Utiliser une adresse différente pour les passerelles séries**.
- Saisir l'adresse IP et le masque de sous-réseau pour les passerelles série

## 10 MACSec

### 10.1 Présentation

MACSec (Media Access Control Security) est défini par le standard IEEE 802.1AE et assure la sécurité des liens SHDSL point à point.

MACSec agit au niveau de la couche liaison de données (MAC) et assure, sans établir de connexion, la confidentialité et l'intégrité des données transmises par les couches de protocole supérieures.

MACSec permet de chiffrer et de signer les trames sortantes sur une interface SHDSL. Les trames entrant sur une interface SHDSL sont déchiffrées et authentifiées.

Le système se compose de deux parties :

- Le « DataPath Virtual interface » qui chiffre, déchiffre, signe et authentifie les trames,

- Le « MACSec Key Agreement » (MKA) qui est responsable de l'installation des clés sur l'interface virtuelle.

#### 10.1.1 L'interface virtuelle

L'interface virtuelle utilise une seule clé de 256 bit pour le chiffrement et l'authentification (SAK).

L'interface virtuelle utilise l'AES-256 en mode GCM.

L'interface virtuelle utilise un EtherType dédié pour les trames MACSec (elle traite les trames entrantes qui ont cet EtherType et génère les trames sortantes avec cet EtherType).

#### 10.1.2 MKA

MKA génère, distribue et installe la SAK dans l'interface virtuelle.

Cela requiert deux variables :

- La CKN qui identifie un groupe d'équipements qui doivent établir une SAK commune,

- La CAK qui est une PSK.

Le fonctionnement général est le suivant :

1. Le participant qui a la plus petite adresse MAC est élu le serveur de clé,
2. Le serveur de clé choisit aléatoirement une SAK en utilisant CSPRNG et diverses sources d'entropie.
3. Le serveur de clé chiffre la SAK avec la CAK en utilisant AES-keywrap and et la signe avec la CAK,
4. Le serveur de clé distribue la SAK chiffrée aux autres participants.
5. Les participants vérifient, déchiffrent et installent la SAK dans l'interface virtuelle.
6. The participants verify, decrypt and install the SAK in the virtual interface.

Chaque fois qu'un participant est ajouté ou retiré, le processus redémarre.

MKA utilise les BPDU 802.1X pour échanger les données (MKPDUs).

L'adresse de destination est 01:80:C2:00:00:03. Cette adresse est utilisée sur un lien local et ces trames ne sont pas transférées par les switches.

### 10.2 Configuration de MACSec

- Dans le menu, choisir **Configuration > Ethernet & Commutation > MACSec**.
- Activer MACSec sur les ports SHDSL
- Saisir la CKN (32 caractères hexadecimal) et la CAK (64 caractères hexadecimal)

etic TELECOM XSLAN-BP4200

Documentation | EN | FR

> Accueil > Configuration > Ethernet et commutation > MACSec

Enregistrer Annuler Modifications sur la page non enregistrées Valeurs non valides sur la page

Méthode de saisie de la clé	Clés AES hexadécimales
Activer MACSec sur SH1	<input checked="" type="checkbox"/>
CKN	
CAK	
Activer MACSec sur SH2	<input checked="" type="checkbox"/>
CKN	
CAK	
Activer MACSec sur SH3	<input checked="" type="checkbox"/>
CKN	
CAK	
Activer MACSec sur SH4	<input checked="" type="checkbox"/>
CKN	
CAK	

Enregistrer Annuler

### 10.3 Mode dérivé d'un mot de passe

Un mode « Dérivé d'un mot de passe » est ajouté dans le XS et ne fait pas partie du standard. Le fonctionnement est le suivant :

Un nom de réseau et un mot de passe sont saisis par l'utilisateur.

La CKN est calculée de la façon suivante :

$$\text{CKN} = \text{sha256}(\text{nom\_réseau})$$

La CAK est calculée de la façon suivante :

$$\text{CAK} = \text{pbkdf2\_sha512}(\text{mot de passe} = \text{mot de passe}, \text{salt} = \text{nom\_réseau}, \text{iterations} = 30000, \text{len} = 32\text{bytes})$$

etic TELECOM XSLAN-BP4200

Documentation | EN | FR

> Accueil > Configuration > Ethernet et commutation > MACSec

Enregistrer Annuler Modifications sur la page non enregistrées

Méthode de saisie de la clé	Dérivées d'un mot de passe
Activer MACSec sur SH1	<input checked="" type="checkbox"/>
Nom du réseau	etic
Mot de passe	
Activer MACSec sur SH2	<input checked="" type="checkbox"/>
Nom du réseau	etic
Mot de passe	
Activer MACSec sur SH3	<input type="checkbox"/>
Activer MACSec sur SH4	<input type="checkbox"/>

Enregistrer Annuler

# PARAMETRAGE

## 10.4 Etat MACSec

Pour verifier l'état de MACSec :

- Dans le menu, choisir **Diagnostics > Etat du réseau > Interfaces**.

### État MAC Sec

État MACSec SHDSL1	Non sécurisé
État MACSec SHDSL2	Non sécurisé
État MACSec SHDSL3	Désactivé
État MACSec SHDSL4	Désactivé

Rafraîchir

## 10.5 Gestion des clés et effacement sécurisé

Les clés MACSec sont stockés dans une zone séparée de la zone de stockage de la configuration. Il est possible d'exécuter un effacement sécurisé de ces clés.

Ce processus efface la copie des clés MACSec de la RAM, efface la zone de stockage séparée et coupe l'alimentation de la CPU/RAM un bref instant pour que la RAM-DDR3 puisse perdre son contenu.

Pour effectuer un effacement sécurisé :

- Dans menu, choisir **Maintenance > Effacement sécurisé**
- Cliquer **Effacer**.

The screenshot shows the etic TELECOM web interface. The top left features the etic TELECOM logo. The top right displays the model number XSLAN-BP4200. Below the logo, there is a navigation menu with 'Accueil', 'Configuration', 'Diagnostics', and 'Maintenance' (which is expanded to show 'Gestion des configurations', 'Mises à jour du logiciel', 'Effacement sécurisé', 'Bloc notes', and 'Redémarrage'). The main content area shows the breadcrumb path '> Accueil > Maintenance > Effacement sécurisé' and a button labeled 'Déclencher un effacement sécurisé maintenant' with an 'Effacer' button next to it. A large, faint padlock icon is visible in the background of the main content area.

## 10.6 Considérations sur le MTU

Le MTU de l'interface L2 pour l'adresse IP du serveur d'administration est le suivant :

1500 avec MACSec désactivé

1468 si MACSec est activé

1464 si les VLANs et MACSec sont activés.

Cela permet d'avoir accès aux pages web dans tous les cas avec un TCP MSS correct.

Le MTU d'un lien SHDSL avec MACSec est 1468 octets, 32 octets sont pris par l'entête MACSec .

Le MTU d'un lien SHDSL avec MACSec et VLANs est 1464 octets, 4 octets additionnels sont pris par l'entête VLAN .

## 11 IGMP snooping

### 11.1 Présentation

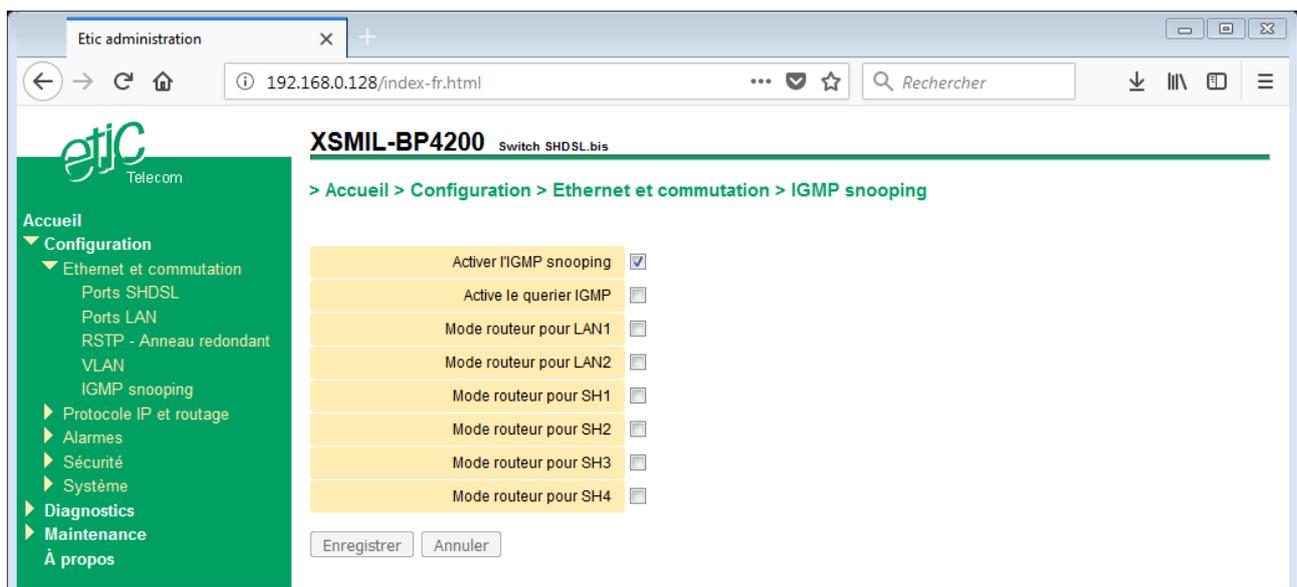
Par défaut, un switch retransmet les trames multicast sur tous ces ports. Dans un scénario où le trafic est chargé, cela peut entraîner la saturation des liens et tout particulièrement des liens SHDSL à faible débit. Pour éviter cela, un switch peut inspecter le trafic IGMP échangés par des équipements faisant du multicast.

Typiquement dans un réseau avec du trafic multicast, il y a un routeur multicast. Celui-ci interroge périodiquement en IGMP les autres équipements pour savoir lesquels veulent recevoir tel trafic multicast. En transmettant les trames, le switch contrôle s'il doit transmettre ou bloquer un trafic multicast donné sur un port donné.

Quand il n'y a pas de router multicast pour interroger le réseau, un des switches ayant l'IGMP snooping activé peut assurer l'interrogation. Celui avec la plus petite adresse IP est élu comme le querier du réseau.

### 11.2 Configuration de la fonction IGMP snooping

- Dans le menu, choisir **Configuration > Ethernet et commutation > IGMP snooping**.
- Cocher la case **Activer l'IGMP snooping**.



#### Activer l'IGMP snooping

Active le filtrage/transfert des paquets IP multicast basé sur le trafic IGMP.

#### Activer le querier IGMP

Autorise le XS à pouvoir être élu comme querier s'il n'y a pas de routeur dans le réseau.

#### Mode routeur pour LAN1

#### Mode routeur pour LAN2

#### Mode routeur pour SH1

#### Mode routeur pour SH2

#### Mode routeur pour SH3

#### Mode routeur pour SH4

Accepte tout le trafic multicast arrivant sur ce port.

## 12 SNMP

### 12.1 Présentation

Le XS supporte les protocoles SNMP V2 et V3.

Le XS supporte les MIB suivantes :

- RFC1213-MIB (MIB-2)
- HDLSL2-SHDSL-LINE-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- BRIDGE-MIB
- RSTP-MIB

On trouvera en annexe leur description détaillée.

Le manager SNMP peut en particulier acquérir les informations suivantes :

Etat des ports Ethernet 10/100 BT (Up / down)  
Etat des ports SHDSL (connectés ou non)  
Débit de la liaison SHDSL  
SNR ratio margin  
SHDSL links Number of erroneous seconds during the last quarter of hour  
SHDSL links Number of erroneous seconds during the last 24 hours  
Etat RSTP de chaque port (bloque / learning / forwarding)  
Paramètres RSTP du bridge (bridge ID, priorité, MAC, root)  
Base de données d'adresses MAC apprises

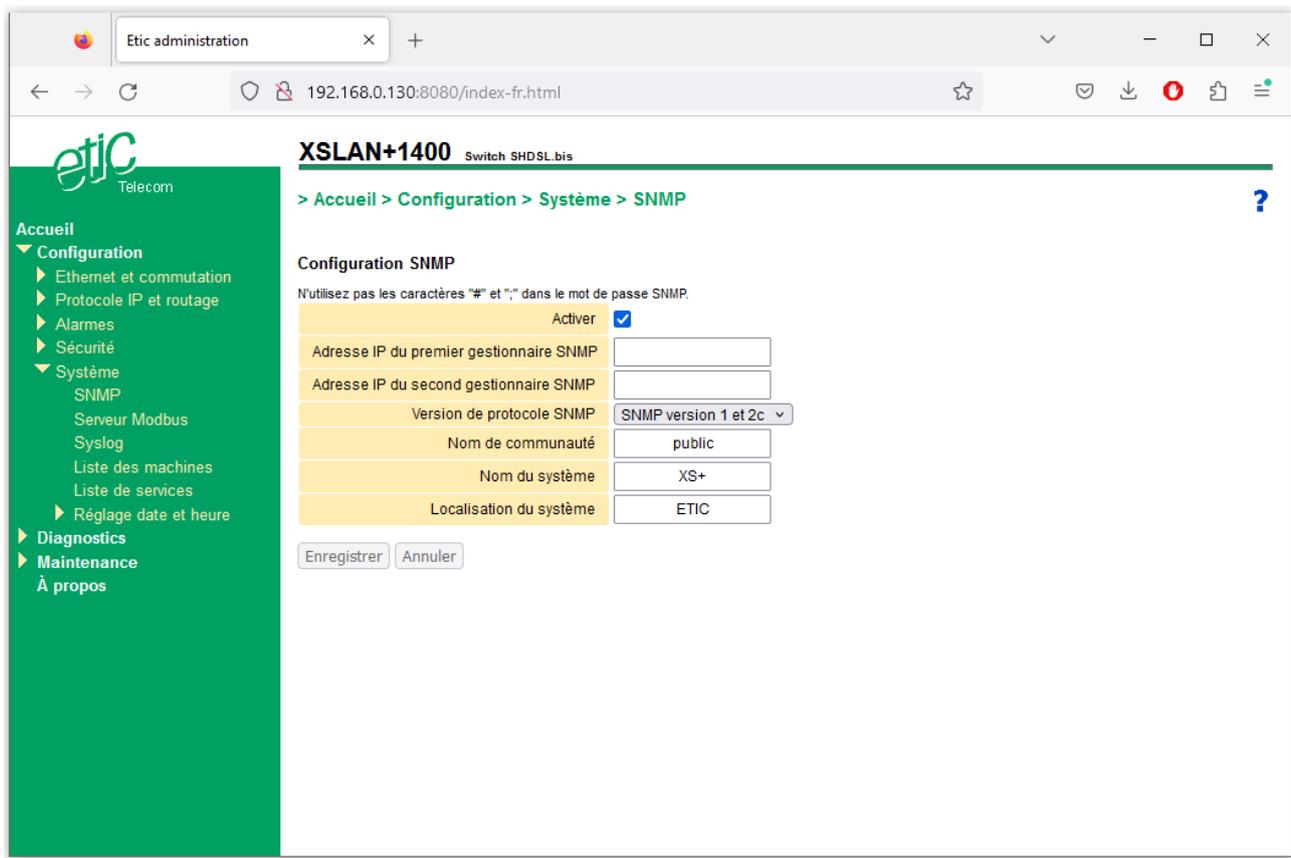
Le XS est également capable de transmettre les traps SNMP suivants :

Connexion des ports Ethernet 10/100 BT  
Déconnexion des ports Ethernet 10/100 BT  
Connexion des liaisons SHDSL  
Déconnexion des liaisons SHDSL  
Anneau établi  
Anneau rompu  
Redémarrage du produit

### 12.2 Configuration de la fonction SNMP

- Dans le menu, choisir **Configuration > Système > SNMP**.
- Cocher la case **Activer**.

# PARAMETRAGE



## Adresse IP du premier gestionnaire SNMP

Saisir l'adresse IP du manager SNMP vers qui seront envoyés les traps SNMP.

## Adresse IP du second gestionnaire SNMP

Saisir l'adresse IP du second manager SNMP le cas échéant.

## Nom de communauté

Saisir le nom de la communauté à laquelle le produit appartient.

## Nom du Système

C'est le nom attribué au produit (XSLAN+2400 par exemple).

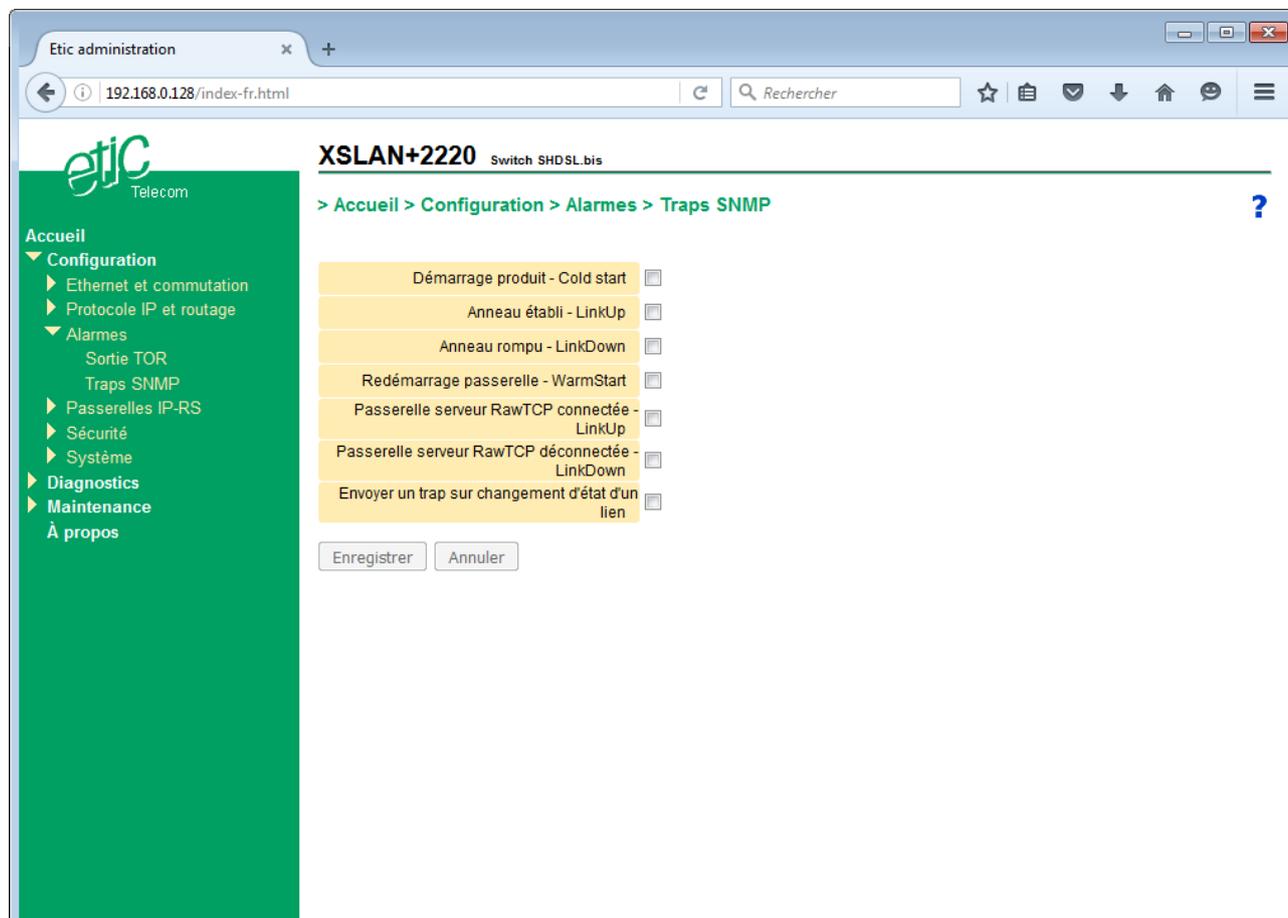
## Localisation du système

C'est la localisation physique du produit.

Saisir un libellé qui permette de situer géographiquement le produit.

## 12.3 Configuration des traps SNMP

- Dans le menu, choisir **Configuration > Alarmes > Traps SNMP**.
- Sélectionner les traps qui doivent être transmis dans la liste proposée.



**Démarrage produit – Cold start**

**Anneau établi – LinkUp**

**Anneau rompu – LinkDown**

**Redémarrage passerelle – WarmStart**

**Passerelle serveur RawTCP connectée – LinkUp**

**Passerelle serveur RawTCP déconnectée – LinkDown**

**Changement d'état d'un lien**

## 13 NTP

### 13.1 Présentation

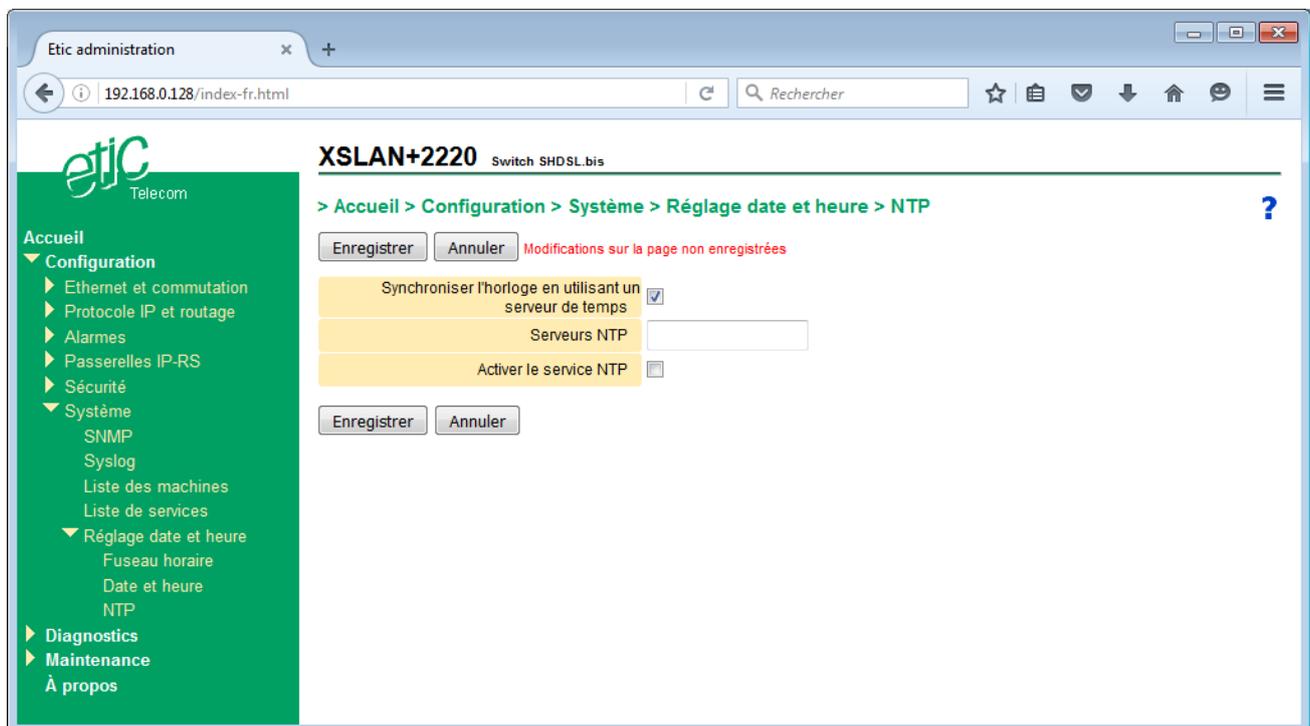
Le protocole NTP permet de synchroniser l'heure d'un équipement sur un serveur de référence.

Le XS supporte ce protocole et peut récupérer l'heure sur un ou plusieurs serveurs de temps.

Le XS peut aussi se comporter comme un serveur de temps et délivrer l'heure à des équipements secondaires. Cette solution est intéressante dans le cas d'une liaison SHDSL à faible débit. Seul le XS interroge un serveur de temps situé à l'autre bout de la liaison. Les équipements raccordés sur les ports LAN se synchronisent sur le XS local. Ceci permet de ne pas encombrer la liaison SHDSL à faible débit par de multiples requêtes NTP.

### 13.2 Configuration de la fonction client NTP

- Dans le menu, choisir **Configuration > Système > Réglage date et heure > NTP**.
- Cocher la case **Synchroniser l'horloge en utilisant un serveur de temps**.



#### Serveurs NTP

Saisir l'adresse IP du serveur de temps NTP. S'il y a plusieurs serveurs, saisir les différentes adresses IP en les séparant par des virgules « , » .

### 13.3 Configuration de la fonction serveur NTP

- Dans le menu, choisir **Configuration > Système > Réglage date et heure > NTP**.
- Cocher la case **Activer le service NTP**.

## 14 Qualité de service DiffServ

### 14.1 Principe

Le protocole IP permet de multiplexer différents services sur le même support (de la vidéo, du contrôle commande, du html ...). Les avantages sont bien connus ; néanmoins, si un service transmet un trafic IP trop important, le réseau est encombré et le temps de traversée excessivement long.

Par défaut, chaque port SHDSL a un tampon d'émission FIFO pouvant accueillir 10 paquets (cette valeur est modifiable). Lorsque l'on active la « Qualité de service » (QoS), le tampon FIFO est remplacé par un tampon SFQ (Stochastic Fairness Queuing). Le SFQ classe automatiquement les trames entrantes en fonction de leurs adresses et ports sources et destination en flux. Chaque flux ainsi déterminé envoie tour à tour une trame. Cette méthode permet de limiter la latence et de réserver de la bande passante pour chaque trafic. Cette méthode est suffisante dans la plupart des cas et ne nécessite aucun autre paramétrage.

Si le résultat n'est pas satisfaisant, il est alors possible de classer et prioriser manuellement les différents trafics en utilisant l'algorithme Diffserv qui va marquer chaque trame IP en utilisant le champ DSCP.

Le principe est le suivant :

On désigne par trafic le couple constitué par une adresse IP et un service (ftp, html, modbus etc...).

Par ailleurs, on partage la bande passante disponible en 5 parties appelées « classes » .

On affecte chaque trafic à l'une des 4 premières classes : Platine, Or, Argent, Bronze.

Le trafic non répertorié est affecté à la classe « Default ».

La classe « Platine » possède la priorité la plus haute ; Ce trafic est acheminé en premier quel que soit le trafic dans les autres classes.

Les classes « Or, Argent, Bronze » se partagent la bande passante disponible :

Exemple	Bande passante minimum	Bande passante maximum
	En % de la bande totale	En % de la bande totale
Or	50 %	80 %
Argent	30 %	80 %
Bronze	15 %	80 %
Default	5 %	Non limité
Total	60 %	

Une fois que le trafic d'une de ces 4 classes occupe la bande minimum allouée, le trafic supplémentaire peut être acheminé sous réserve que de la bande non utilisée par les autres classes soit disponible. La règle d'attribution de cette bande inutilisée est fonction du niveau de priorité de la classe : Le trafic supplémentaire de la classe Or est le plus prioritaire et celui de la classe Default est le moins prioritaire.

On prendra garde à ne pas affecter à la classe « Platine » un trafic trop important. En effet, le trafic de cette classe est acheminé en priorité ; s'il est trop important il empêche le trafic des autres classes de s'écouler.

On réservera le trafic « Platine » au trafic de contrôle-commande, par exemple.

La classification DiffServ est effective dans le domaine des liens SHDSL. Au sein de ce domaine les trames IP gardent leur marque de classification DSCP. Par contre, les trames IP qui ressortent sur les port LAN Ethernet perdent leur classification (champ DSCP à 0). Il est parfois utile d'étendre le domaine DiffServ au réseau LAN Ethernet par exemple pour communiquer avec un autre XS présent sur le LAN Ethernet. Dans ce cas les trames IP qui ressortent sur les port LAN Ethernet gardent leur classification, le champ DSCP n'est pas remis à 0.

# PARAMETRAGE

Valeur DSCP correspondante à chaque classe :

Classes olympiques	Classes DiffServ assignées par le XS	Valeur DSCP	Classes DiffServ Supportées par le XS
Platine	EF	46	EF
Or	AF11	10	CS1, AF11, AF12, AF13
Argent	AF21	18	CS2, AF21, AF22, AF23
Bronze	AF31	26	CS3, AF31, AF32, AF33
Default	BE	0	BE

## 14.2 Configuration basique

- Dans le menu, choisir **Configuration > Protocole IP et routage > QoS – DiffServ**.
- Cocher la case **Activer la QoS**.

The screenshot shows the Etic administration web interface for switch XSLAN+2220. The breadcrumb trail is: > Accueil > Configuration > Protocole IP et routage > QoS - DiffServ. The configuration options are:

- Activer la QoS:
- Activer l'extension du domaine:

The 'Classes' section shows the following bandwidth settings:

Classe	Bande minimum réservée	Bande maximum autorisée
Gold	50	100
Silver	30	100
Bronze	15	100

The 'Classification du trafic' section shows a table with columns: Machine, Service, Classe. Below the table are buttons: Afficher, Modifier, Supprimer, Ajouter ..., Copier et modifier, ^, v, <, >. At the bottom are buttons: Enregistrer, Annuler.

### 14.3 Configuration avancée

#### Etape 1 : Définir les machines du réseau

- Dans le menu, choisir **Configuration > Système > Liste des machines**.
- Cliquer « **Ajouter ...** ».
- Donner un nom à la nouvelle machine ou au nouveau groupe de machines.
- Associer une adresse IP ou un ensemble d'adresses IP à cette machine ou à ce groupe de machines.
- Cliquer **Enregistrer**.

The screenshot shows the Etic administration web interface. The browser address bar displays '192.168.0.128/index-fr.html'. The page title is 'XSLAN+2220 Switch SHDSL.bis'. The breadcrumb navigation is '> Accueil > Configuration > Système > Liste des machines'. On the left, there is a green navigation menu with options like 'Accueil', 'Configuration', 'Système', 'SNMP', 'Syslog', 'Liste des machines', 'Liste de services', 'Réglage date et heure', 'Diagnostics', 'Maintenance', and 'À propos'. The main content area has three input fields: 'Nom du site', 'Nom de domaine', and 'Afficher le portail web'. Below these is the 'Liste de machines' section, which includes a description: 'Cette liste assigne un nom aux machines raccordées au réseau. Elle vous permettra de définir des règles de QoS.' and a table with the following data:

	Nom	Adresse IP
<input checked="" type="radio"/>	Any	0.0.0.0
<input type="radio"/>	PLC	192.168.0.10
<input type="radio"/>	Screen	192.168.0.11

Below the table are buttons for 'Afficher', 'Modifier', 'Supprimer', 'Ajouter ...', 'Copier et modifier', and navigation arrows. At the bottom, there are 'Enregistrer' and 'Annuler' buttons.

#### Etape 2 : Eventuellement définir d'autres services

- Dans le menu, choisir **Configuration > Système > Liste de services**.
- Cliquer « **Ajouter ...** ».
- Donner un nom au nouveau service.
- Associer un protocole et un port à ce service.
- Cliquer **Enregistrer**.

The screenshot shows the 'Liste de services' page in the Etic administration interface. The breadcrumb trail is: Accueil > Configuration > Système > Liste de services. Below the title, there is a description: 'Les services désignent les applications de communications entre les machines (par exemple la navigation web ou le transfert de fichiers). Un service est défini par le couple (port, protocole), par exemple pour le service web/http : (80, tcp)'. A table lists various services with their names, protocols, and ports. The 'Any' service is selected with a radio button.

	Nom	Protocole	Port
<input checked="" type="radio"/>	Any	Tous	0:65535
<input type="radio"/>	Http	TCP	80
<input type="radio"/>	Ftp	TCP	21
<input type="radio"/>	Telnet	TCP	23
<input type="radio"/>	Dns	UDP	53
<input type="radio"/>	Pop3	TCP	110
<input type="radio"/>	Smtpt	TCP	25
<input type="radio"/>	Tftp	UDP	69
<input type="radio"/>	Ping	ICMP	8
<input type="radio"/>	Snmpt	UDP	161,162
<input type="radio"/>	Netbios	TCP	137:139
<input type="radio"/>	SMB MS-ds	TCP	445
<input type="radio"/>	Modbus TCP	TCP	502
<input type="radio"/>	Schneider UNI-TE	TCP	502
<input type="radio"/>	Rockwell EtherNet/IP-CIP	TCP	44818
<input type="radio"/>	Omron FINS	UDP	9600
<input type="radio"/>	Siemens S7 ISO on TCP	TCP	102

At the bottom of the table, there are buttons: Afficher, Modifier, Supprimer, Ajouter ..., Copier et modifier, and navigation arrows.

### Etape 3 : Configurer les classes de trafic

- Dans le menu, choisir **Configuration > Protocole IP et routage > QoS – DiffServ**.
- Cocher la case **Activer la QoS**.
- Attribuer à chaque classe de trafic (Or, Argent, Bronze), une bande passante minimum et maximum.
- Cliquer **Enregistrer**.

### Etape 4 : Assigner une classe à chaque trafic

- Sous la table de classification du trafic, Cliquer **Ajouter ...**.
- Sélectionner le service et la machine ou le groupe de machines pour définir un trafic ;
- Attribuer une classe de trafic (Platine, Or, Argent, Bronze) à ce trafic.
- Cliquer **Enregistrer**.

Etic administration

192.168.0.128/index-fr.html

Rechercher

**etic** Telecom

**XSLAN+2220** Switch SHDSL.bis

> Accueil > Configuration > Protocole IP et routage > QoS - DiffServ

Accueil

- Configuration
  - Ethernet et commutation
  - Protocole IP et routage
    - Protocole IP
    - RIP
    - Routes statiques
    - VPN de bouclage
    - QoS - DiffServ
    - Routage avancé
  - Alarmes
  - Passerelles IP-RS
  - Sécurité
  - Système
- Diagnostics
- Maintenance
- À propos

Activer la QoS

Activer l'extension du domaine

**Classes**

Bande minimum réservée pour la classe Gold	<input type="text" value="50"/>	(de 0 à 95, multiple de 5)
Bande maximum autorisée pour la classe Gold	<input type="text" value="100"/>	(de 0 à 100, multiple de 5)
Bande minimum réservée pour la classe Silver	<input type="text" value="30"/>	(de 0 à 95, multiple de 5)
Bande maximum autorisée pour la classe Silver	<input type="text" value="100"/>	(de 0 à 100, multiple de 5)
Bande minimum réservée pour la classe Bronze	<input type="text" value="15"/>	(de 0 à 95, multiple de 5)
Bande maximum autorisée pour la classe Bronze	<input type="text" value="100"/>	(de 0 à 100, multiple de 5)

**Classification du trafic**

	Machine	Service	Classe
<input checked="" type="radio"/>	PLC	Modbus TCP	Platine
<input type="radio"/>	PLC	Telnet	Argent
<input type="radio"/>	Screen	Http	Or

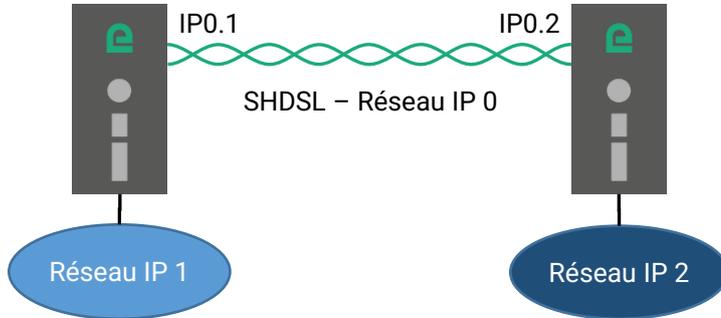
Afficher Modifier Supprimer Ajouter ... Copier et modifier ^ v < >

Enregistrer Annuler

## 15 Routage IP

### 15.1 Principe

Le XS peut effectuer des fonctions de base d'un routeur de trames IP entre son interface locale constitué de 2 à 4 ports Ethernet et son interface SHDSL considérée comme une interface unique même si le produit dispose de plusieurs ports SHDSL.



Voir le chapitre « Attribution des Adresses IP »

Pour accéder à des équipements situés dans un réseau IP différent, le XS adresse généralement les trames IP à sa passerelle par défaut. Cependant pour des cas plus complexes, il est possible de définir des routes statiques ou bien d'utiliser un protocole de routage.

### 15.2 Routes statiques

Pour créer des routes statiques,

- Dans le menu, choisir **Configuration > Protocole IP et routage > Routes statiques**.
- Cliquer **Ajouter...**
- Saisir l'adresse du réseau de destination, son masque, l'adresse de la passerelle qui permet d'y accéder et le coût de la route.

The screenshot shows a web browser window titled 'Etic administration' with the URL '192.168.0.128/index-en.html'. The page content is for 'XSLAN+2220 SHDSL.bis switch' and is titled '> Home > Setup > IP protocol and routing > Static routes'. A 'Static routes table' is displayed with the following data:

	Active	Route name	IP address	Netmask	Gateway IP address	Interface	Metric (0-32000)
<input checked="" type="radio"/>	Yes	Scada	192.168.38.2	255.255.255.0	192.168.0.1		10

Below the table are buttons for 'Show', 'Edit', 'Delete', 'Add ...', 'Copy and edit', and navigation arrows.

### 15.3 Protocole RIP

RIP (**Routing Information Protocol**) est un protocole de routage IP qui permet à chaque routeur ou équipement d'un réseau de connaître la route menant à un autre réseau.

Le principe utilisé est le suivant :

#### Diffusion des tables de routage

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

#### Mise à jour des tables de routage

Chaque routeur met à jour sa propre table au moyen des informations reçues des autres. Le protocole RIP permet d'éviter de déclarer les routes statiques dans chacun des routeurs.

#### Pour activer le protocole RIP,

- Dans le menu, choisir **Configuration > Protocole IP et Routage > RIP**.
- Cocher la case **Activer RIP**.

Lorsqu'il est activé, le protocole RIP tourne sur tous les ports Ethernet, LAN ou SHDSL que le mode routeur soit activé ou non.

### 15.4 Protocole OSPF

Le protocole OSPF assure la même fonction que le protocole RIP mais est utilisé dans le cas de configuration de réseaux plus complexes.

Le XS supporte le protocole OSPF mais la configuration s'effectue en ligne de commande SSH. Il s'agit d'un mode fonctionnement avancé qui permet au XS de se comporter comme un routeur très souple et sophistiqué. Par exemple il est possible de bridger n'importe quel port Ethernet avec n'importe quel port SHDSL et d'attribuer des adresses IP différentes pour chaque port.

#### Pour activer le protocole OSPF,

- Dans le menu, choisir **Configuration > Protocole IP et Routage > Routage avancé**.
- Cocher la case **Activer le mode routage avancé (CLI SSH)**.
- Dans la partie **Configuration des bridges** Cliquer **Ajouter...**
- Saisir la liste des interfaces comprises dans chaque bridge.

Pour chacun de ces bridges une adresse IP et un masque de sous-réseau pourront être attribués par la suite.

La suite de la configuration s'effectue en mode SSH sur le port 22.

Pour plus d'information on se référera au manuel de référence de Quagga.

## 16 NAT avancé

### 16.1 Principe

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

Elle s'applique à toute trame IP reçue par le XS aussi bien sur son interface LAN que sur son interface SHDSL.

On distingue

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

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

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

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

Direction	
SHDSL vers LAN	SHDSL -> DNAT -> Pare-Feu -> SNAT -> LAN
LAN vers SHDSL	LAN -> DNAT -> Pare-Feu -> SNAT -> SHDSL

### 16.2 Configuration

Pour mettre en œuvre la fonction NAT avancée,

- Dans le menu, choisir **Configuration > Protocole IP et Routage > NAT avancé**.

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

- Cliquer **Ajouter** dans le tableau des règles DNAT
- La fenêtre de création s'affiche
- Cliquer **Active** pour rendre la règle active.
- Saisir les critères de substitution :  
Adr. IP source  
Adr. IP destination  
Protocole (TCP, UDP, ...)  
Port source  
Port destination
- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP et port de destination.

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

- Cliquer **Ajouter** dans le tableau des règles SNAT
- La fenêtre de création s'affiche
- Cliquer **Active** pour rendre la règle active.
- Saisir les critères de substitution :  
Adr. IP source  
Adr. IP destination  
Protocole (TCP, UDP, ...)  
Port source  
Port destination
- Saisir la nouvelle destination des trames répondant aux critères décrits ci-dessus : Adr. IP source.

## 17 Pare-feu

### 17.1 Présentation

Le pare-feu filtre les échanges de trames IP entre l'interface SHDSL et l'interface LAN pour protéger les équipements connectés au réseau LAN.

Il se compose d'un ensemble de règles de filtrage qui autorise ou interdit un type de trames IP.

Le pare-feu est de type SPI (Stateful Packet inspection). C'est-à-dire que les règles de filtrage porte uniquement sur les requêtes. Les réponses n'ont pas à être spécifiées, elles sont automatiquement acceptées si elles concernent des requêtes acceptées.

### 17.2 Configuration

Pour activer le pare-feu,

- Dans le menu, choisir **Configuration > Sécurité > Pare-feu**.
- Cliquer **Activer le Pare-feu**.

etic TELECOM XSLAN-BP4200

Documentation | EN | FR

Accueil > Pare-feu

Configuration

- Configuration
- Ethernet et commutation
- Protocole IP et routage
- Alarmes
- Sécurité
  - Droits d'administration
  - Certificats X509
  - Pare-feu
- Système
- Diagnostics
- Maintenance
- A propos

Règles pour le trafic SHDSL-LAN:

Activer le Pare-feu

Politique par défaut LAN->SHDSL Autoriser

Politique par défaut SHDSL->LAN Autoriser

ATTENTION: Si tous les trafics "Interne" sont interdits, Vous ne serez plus capable d'ouvrir cette interface web d'administration.

Politique par défaut LAN->Interne Autoriser

Politique par défaut SHDSL->Interne Autoriser

Direction	Action	Protocole	Adresse IP source	Port source	Adresse IP destination	Port destination
-----------	--------	-----------	-------------------	-------------	------------------------	------------------

Afficher Modifier Supprimer Ajouter ... Copier et modifier [table icon]

Enregistrer Annuler

- **Politique par défaut**

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

On distingue le trafic qui traverse le XS (LAN-SHDSL), du trafic à destination du XS pour, entre autres, l'administration web (LAN/SHDSLvers interne).

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

On peut souhaiter, par exemple que la politique par défaut interdise le trafic « SHDSL vers LAN » mais autorise le trafic « LAN vers SHDSL ». On fera de même pour le trafic interne « SHDSL vers interne » et « LAN vers interne ».

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

- **Tableau de règles de filtrage**

Chaque ligne est une règle de filtrage.

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

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

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

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

- **Fonctionnement**

Lorsque le pare-feu reçoit une trame IP, il vérifie successivement la conformité aux règles de filtrage.

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

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

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

## 18 Alarmes

### 18.1 Alarmes SNMP

Voir le chapitre SNMP.

### 18.2 Digital output

La sortie TOR peut être ouverte lorsque l'un des défauts suivants survient :

**Port SHDSL 1 déconnecté**

**Port SHDSL 2 déconnecté \***

**Port SHDSL 1 ou 2 déconnecté \***

**Anneau redondant rompu \***

\*Disponible uniquement sur les XS avec plus d'un port SHDSL

## 19 Passerelles série IP

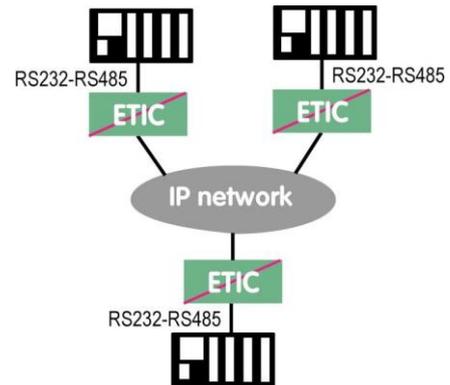
### 19.1 Présentation des types de passerelles

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

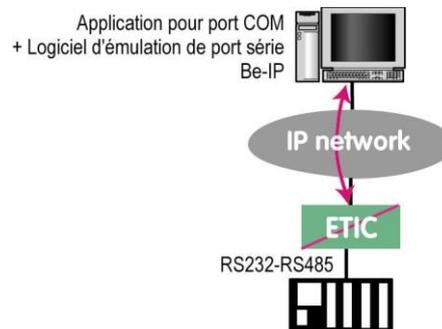
Une passerelle peut être affectée à chaque liaison série.

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

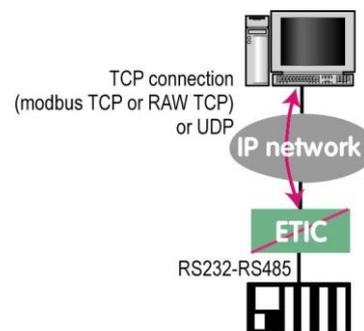
- Communication entre équipements à interface série



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



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



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

## 19.2 Passerelle Modbus

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

### 19.2.1 Définitions

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

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

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

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

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

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

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

Attention : Ne pas confondre adresse Modbus et adresse IP.

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

### 19.2.2 Choix de la passerelle Client ou de la passerelle Serveur

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

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

### 19.2.3 Affectation d'une passerelle Modbus à un port série

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

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

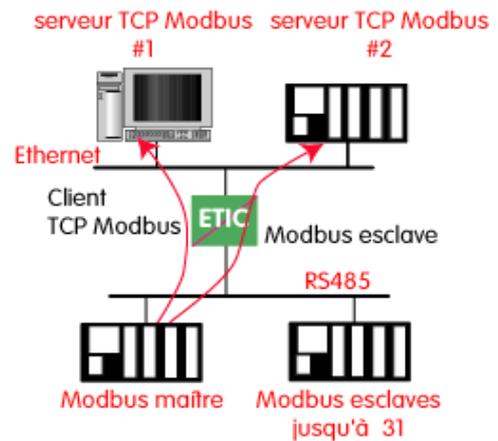
## PARAMETRAGE

### 19.2.4 Passerelle Modbus client

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

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

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

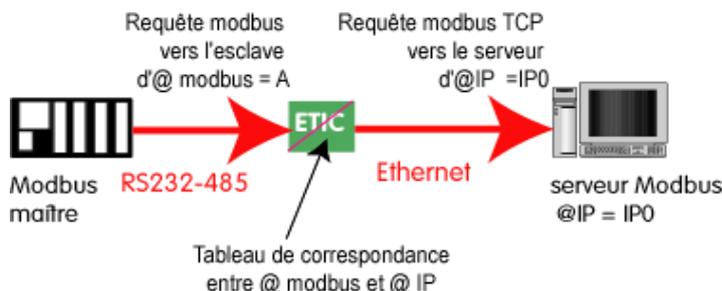


#### Principe de la passerelle Modbus Client :

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

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

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



#### Pour configurer la passerelle :

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

#### Port COM\_

Choisir la liaison série 1 ou 2 du produit.

#### Débit binaire, Parité, Données, Bits d'arrêt

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

#### Protocole Modbus

Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

#### Temps inter-caractères

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

### **Timeout d'inactivité sur TCP**

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

### **Port TCP**

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

### **Esclaves Modbus**

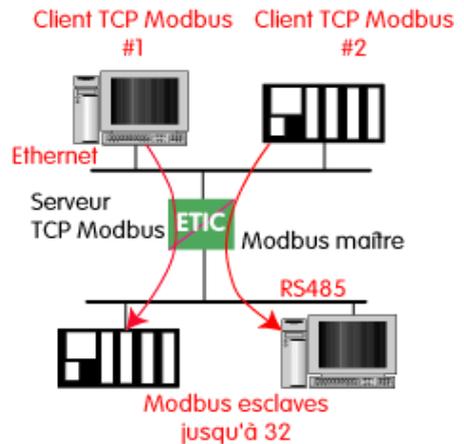
Le tableau permet de faire correspondre une adresse d'esclave Modbus et une adresse IP.

# PARAMETRAGE

## 19.2.5 Passerelle Modbus serveur

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

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



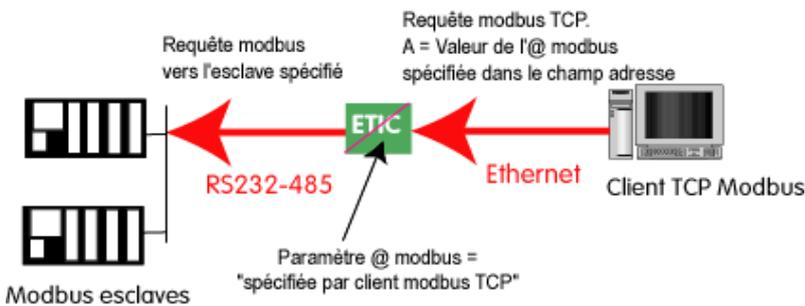
### Principe de la passerelle Modbus serveur :

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

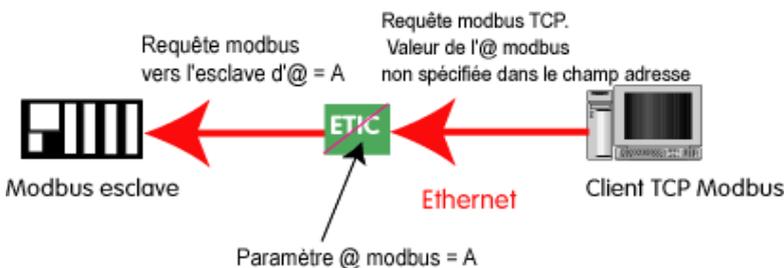
La passerelle se comporte en maître sur la liaison série.

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

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



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



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

### Pour configurer la passerelle :

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

## Port COM

Choisir la liaison série 1 ou 2 du produit.

## Débit binaire, Parité, Données, Bits d'arrêt

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

## Protocole Modbus

Sélectionner RTU (hexadécimal) ou ASCII selon le besoin.

## Activer la fonction proxy/cache

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

## Rafraîchissement du cache

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

.

## Temps inter-caractères

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

## Adresse esclave Modbus

Si la valeur « 0 » est sélectionnée, la passerelle utilise l'adresse Modbus spécifiée par le client Modbus TCP pour adresser l'esclave Modbus de la liaison série ; on peut ainsi adresser jusqu'à 32 esclaves de la liaison série.

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

## Time out d'inactivité sur TCP

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

## Temps d'attente réponse esclave

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

## Port TCP

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

## Nombre de réitérations locales

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

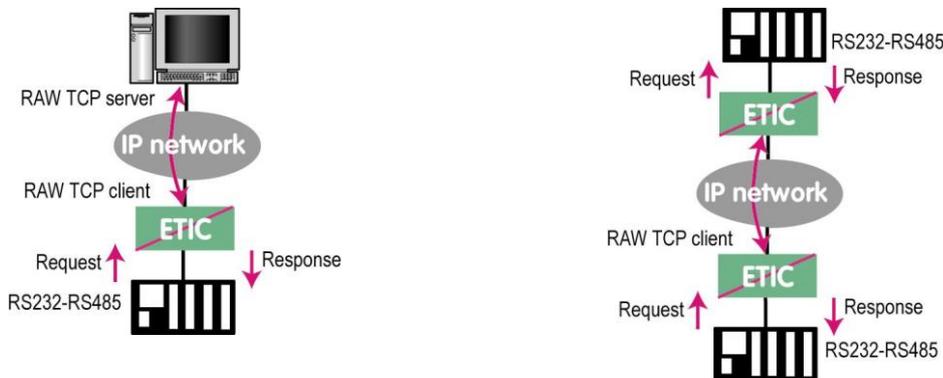
## PARAMETRAGE

### 19.3 Passerelle Raw TCP

#### 19.3.1 Passerelle « Raw TCP client »

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

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



**Pour configurer la passerelle :**

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

#### Débit binaire, Parité, Données, Bits d'arrêt

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

#### Taille du buffer

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

#### Timeout fin de trame RS

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

#### Timeout d'inactivité TCP

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

#### Port TCP

Fixe le N° du port TCP à utiliser.

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

#### Adresse IP serveur

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

### 19.3.2 Passerelle « Raw serveur »

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

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



**Pour configurer la passerelle :**

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

#### Débit binaire, Parité, Données, Bits d'arrêt

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

#### Taille du buffer de réception

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

#### Timeout fin de trame RS

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

#### Timeout d'inactivité TCP

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

#### Port TCP

Fixe le N° du port TCP à utiliser.

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

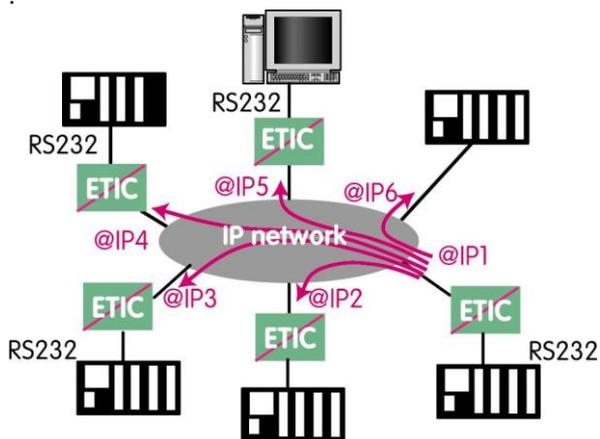
## PARAMETRAGE

### 19.4 Passerelle « Raw UDP »

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

Les destinataires sont désignés dans une liste établie par configuration.

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



**Pour configurer la passerelle :**

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

#### Débit binaire, Parité, Données, Bits d'arrêt

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

#### Taille du buffer de réception

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

#### Timeout fin de trame RS

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

#### Port UDP

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

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

#### Destinations

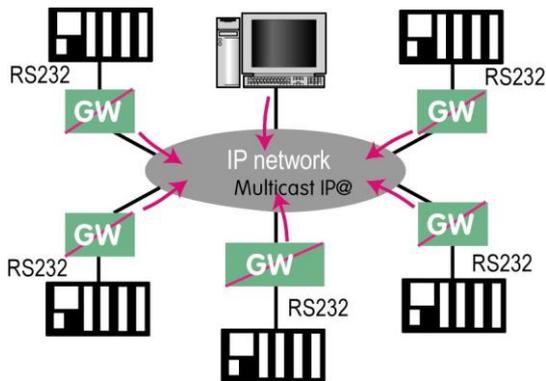
Cette table contient les adresse IP des passerelles vers lesquelles seront envoyés les caractères reçus de la liaison série.

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

## 19.5 Passerelle « Raw Multicast »

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

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



**Pour configurer la passerelle :**

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

### Débit binaire, Parité, Données, Bits d'arrêt

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

### Taille du buffer de réception

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

### Timeout fin de trame RS

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

### Port UDP

Fixe le N° de port UDP à utiliser.

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

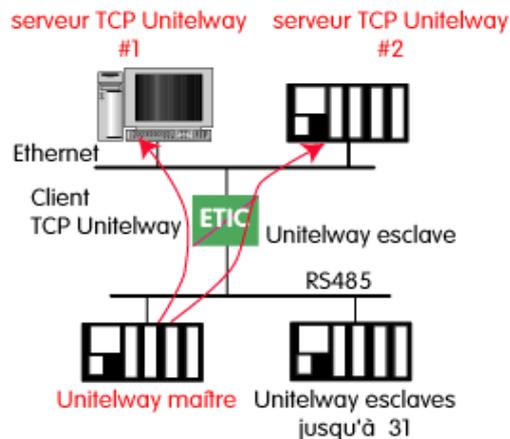
### Adresse IP du groupe multicast

Saisir l'adresse IP attribué au groupe de diffusion (multicast) en respectant les règles de l'IANA .

# PARAMETRAGE

## 19.6 Passerelle « Unitelway »

La passerelle Unitelway permet de connecter un automate série maître unitelway à un réseau IP. Elle permet en particulier de réaliser la fonction de télémaintenance d'automates Schneider Electric RS485 via un réseau IP.



### Pour configurer la passerelle :

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

### Port COM

Choisir la liaison série 1 ou 2 du produit.

### Débit binaire, Parité, Données, Bits d'arrêt

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

### Adresse Xway

Adresse de la passerelle dans le réseau Xway.

### Timeout d'inactivité TCP

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

### Esclaves Unitelway

Désigne la correspondance entre l'adresse de chaque esclave Unitelway émulé par la passerelle et l'adresse IP et Xway de la station sur Ethernet.

## 19.7 Passerelle « Telnet »

Cette passerelle permet à un PC sur le réseau IP et équipé d'un logiciel client Telnet de se connecter à un équipement raccordé à la liaison série du XS.

Le débit et le format de la liaison série peuvent être pilotés selon la recommandation RFC2217.

### Pour configurer la passerelle :

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

### Port COM

Choisir la liaison série 1 ou 2 du produit.

### Débit binaire, Parité, Données, Bits d'arrêt

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

### Timeout d'inactivité TCP

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

### Port TCP

Fixe le N° du port TCP à utiliser.

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



## 20 Serveur d'état Modbus TCP

Le serveur d'état modbus TCP est un serveur permettant à un équipement client Modbus de récupérer des informations d'état du switch XSLAN.

Les valeurs des registres sont documentées en annexe 4.

### **Pour configurer le serveur Modbus:**

- Dans le menu, choisir **Configuration > Système > Serveur Modbus**
- Cocher la case **Activer**

### **Port**

Port utilisé par le serveur Modbus. Par défaut le port 502 est utilisé

## DIAGNOSTICS ET MAINTENANCE

### 21 Diagnostic visual de défaut de fonctionnement

Après la mise sous tension, le voyant  s'éclaire en rouge durant 20 secondes environ pendant la phase d'initialisation du produit.

Après ce délai, le voyant passe au vert et clignote durant 30 secondes puis devient fixe lorsque le produit est prêt à fonctionner.

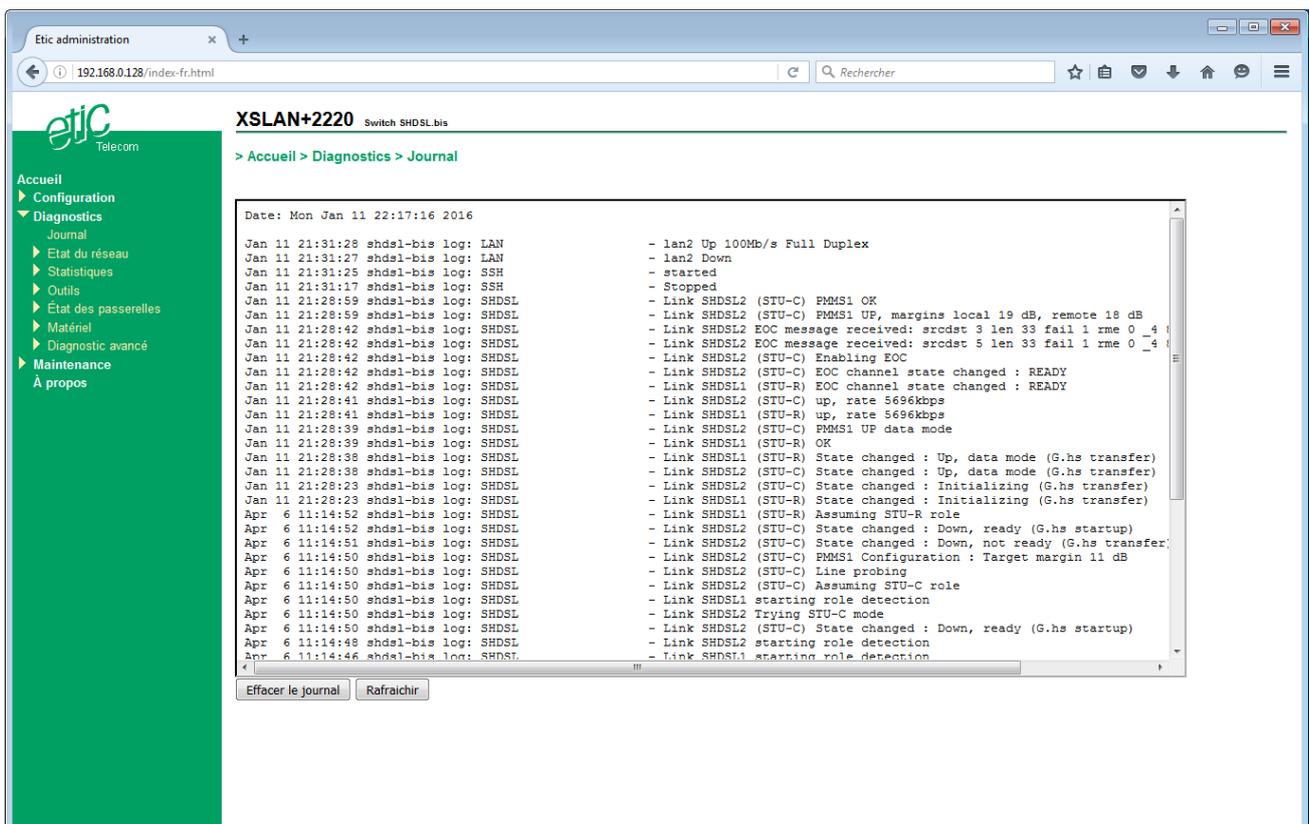
Si le voyant reste éclairé rouge après de délai, le produit est probablement en panne ; contacter la hotline.

### 22 Journal

Le Journal est horodaté ; il enregistre les trois cents derniers événements y compris les connexions et déconnexions de lignes SHDSL.

Pour accéder au journal :

- Dans le menu, choisir **Diagnostics > Journal**.



## 23 Mesure de la qualité de liaison

On évalue la qualité de la connexion au moyen des critères suivants :

### Critère 1 : La marge de rapport signal à bruit

C'est la différence entre le rapport signal à bruit mesuré et le rapport signal à bruit minimum nécessaire pour le débit établi.

Plus la valeur est faible, plus il y a un risque qu'une perturbation provoque des erreurs ou bien une déconnexion.

### Critère 2 : Le nombre de pertes de lien

Le nombre de déconnexions de la liaison est un bon indicateur du fonctionnement de la liaison.

Lorsqu'une liaison fonctionne normalement, les déconnexions doivent être très rares.

Elles peuvent survenir au moment d'un orage ou lors d'une perturbation électromagnétique.

### Critère 3 : Le taux d'erreurs de la ligne

Il se mesure au moyen du nombre de secondes erronées.

Lorsqu'une liaison fonctionne bien, le nombre de secondes erronées doit être très faible.

Des secondes erronées peuvent se produire de temps à autres, par exemple au moment d'un orage ou lors d'une perturbation électromagnétique.

### Pour vérifier la qualité de la liaison,

- Dans le menu, choisir **Diagnostics > Etat du réseau > Interfaces**.

The screenshot shows the 'Etic administration' web interface for a device named 'XSLAN+2220'. The breadcrumb trail is 'Accueil > Diagnostics > Etat du réseau > Interfaces'. The interface displays the following information:

- Adresse MAC:** 00:0a:b4:00:4e:f7
- État des ports LAN:**
  - État du port LAN1: Down
  - État du port LAN2: Up 100Mb/s Full Duplex
- État des ports SHDSL:** A table with 8 columns: Nom du port, État du lien SHDSL, Débit binaire, Marge de rapport signal à bruit, Atténuation de la ligne, Secondes erronées dans la dernière heure, and Pertes de connexion dans les dernières 24 heures.

	Nom du port	État du lien SHDSL	Débit binaire	Marge de rapport signal à bruit	Atténuation de la ligne	Secondes erronées dans la dernière heure	Pertes de connexion dans les dernières 24 heures
<input checked="" type="radio"/>	SHDSL1	Connecté	5696 kbits/sec	18 dB (4/4)	1 dB	0	0
<input type="radio"/>	SHDSL2	Connecté	5696 kbits/sec	19 dB (4/4)	1 dB	1	0

Below the table are buttons for 'Afficher', 'Redémarrer les connexions SHDSL', and 'Rafraîchir'.

## DIAGNOSTICS ET MAINTENANCE

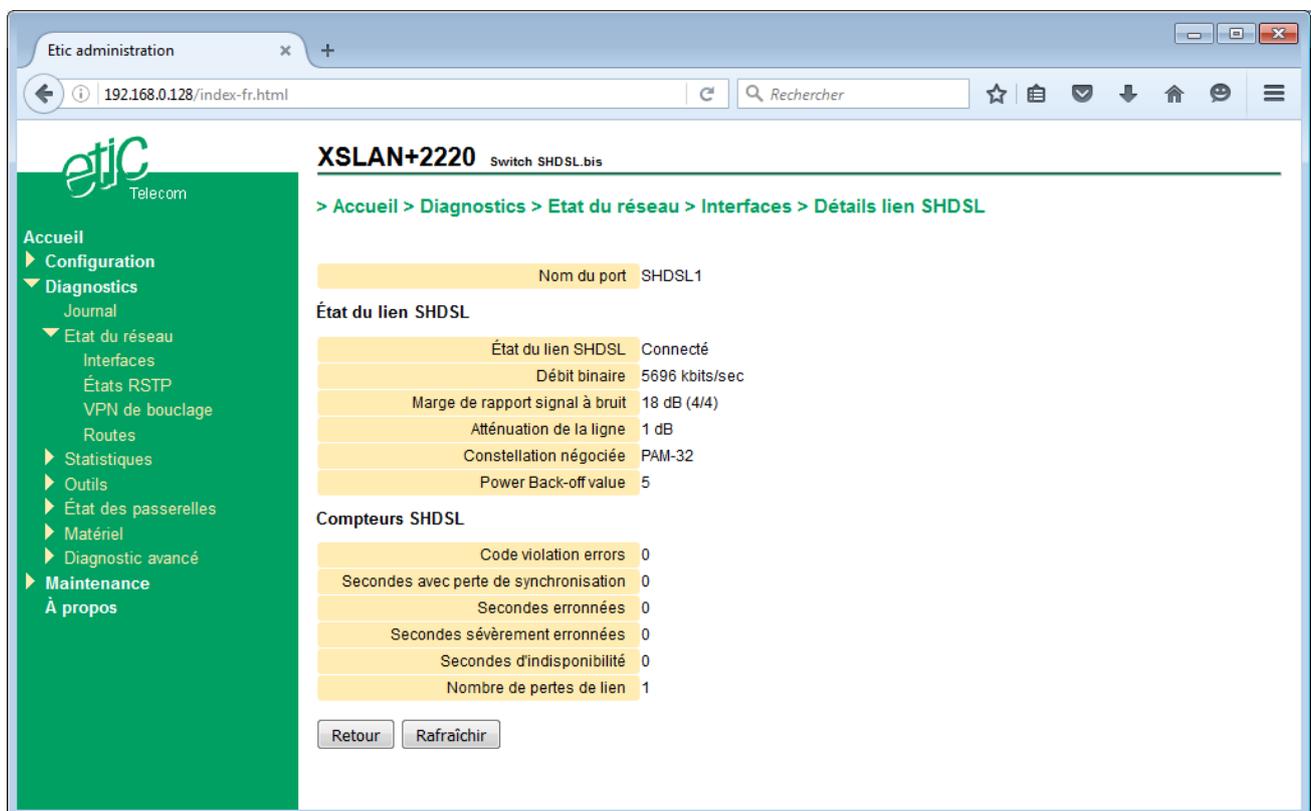
Le tableau de synthèse indique pour chaque ligne SHDSL :

- Si elle est connectée ou non
- le débit
- L'atténuation de la ligne
- la marge de rapport signal à bruit
- le nombre de secondes erronées
- Le nombre de déconnexions

**Pour diagnostiquer le défaut de fonctionnement d'une ligne SHDSL,**

- Sélectionner la ligne SHDSL
- Cliquer **Afficher**.

Le tableau détaillé de la connexion s'affiche.



The screenshot shows a web browser window titled "Etic administration" with the URL "192.168.0.128/index-fr.html". The page displays the configuration for a switch named "XSLAN+2220" (Switch SHDSL.bis). The breadcrumb navigation is: > Accueil > Diagnostics > Etat du réseau > Interfaces > Détails lien SHDSL.

The interface includes a green sidebar menu with the following items: Accueil, Configuration, Diagnostics (expanded), Journal, Etat du réseau (expanded), Interfaces, États RSTP, VPN de bouclage, Routes, Statistiques, Outils, État des passerelles, Matériel, Diagnostic avancé, Maintenance, and À propos.

The main content area shows the following details for the SHDSL line:

- Nom du port: SHDSL1
- État du lien SHDSL: Connecté
- Débit binaire: 5696 kbits/sec
- Marge de rapport signal à bruit: 18 dB (4/4)
- Atténuation de la ligne: 1 dB
- Constellation négociée: PAM-32
- Power Back-off value: 5

Below this, the "Compteurs SHDSL" section shows the following values:

- Code violation errors: 0
- Secondes avec perte de synchronisation: 0
- Secondes erronées: 0
- Secondes sévèrement erronées: 0
- Secondes d'indisponibilité: 0
- Nombre de pertes de lien: 1

At the bottom of the page, there are two buttons: "Retour" and "Rafraîchir".

## 24 Statistiques SHDSL

Les statistiques SHDSL permettent d'avoir une vision globale de la qualité de la liaison en prenant en compte une période longue de fonctionnement.

Il s'agit d'un ensemble de compteurs indiquant la qualité de la liaison pour chaque seconde passée de manière similaire au standard G821. De plus un historique de ces compteurs heure par heure permet de corréliser des éventuels défauts de transmission avec d'autres événements, par exemple le démarrage d'un moteur et ceci sur une profondeur de 15 jours.

### Pour accéder aux statistiques SHDSL,

- Dans le menu, choisir **Diagnosics > Statistiques > Compteurs SHDSL**.

The screenshot shows the Etic administration interface for switch XSLAN+2220. The breadcrumb navigation is: Accueil > Diagnostics > Statistiques > Compteurs SHDSL. The main content area is titled 'Compteurs SHDSL' and contains a table with the following data:

	Nom du port	Secondes sans erreur	Secondes erronées	Secondes sévèrement erronées	Secondes d'indisponibilité	Secondes non connectées
<input checked="" type="radio"/>	SHDSL1	15575	1	1	3	172
<input type="radio"/>	SHDSL2	15578	2	2	3	168

Below the table is a button: 'Remettre à zéro les compteurs SHDSL G.821'. The 'Historique des compteurs SHDSL' section shows a log for 'Line 1' with the following columns: Datetime, EFS, ES, SES, US, NCS. The log data is as follows:

```

Date: Mon Jan 4 23:29:22 2016

EFS : Error free seconds
ES : Erroneous seconds
SES : Severely erroneous seconds
US : Unavailable seconds
NCS : Not connected seconds

Line ID : 1

Datetime      EFS  ES   SES  US   NCS
2016-01-04 23:00:01 3604 0    0    0    0
2016-01-04 22:00:00 3600 0    0    0    0
2016-01-04 21:00:00 3600 0    0    0    0
2016-01-04 20:00:00 3061 1    1    3    172
2016-01-04 19:00:03 0     0    0    0    112
2016-01-04 18:00:02 0     0    0    0    3600
2016-01-04 17:00:02 0     0    0    0    3600
2016-01-04 16:00:02 0     0    0    0    3600
2016-01-04 15:00:02 0     0    0    0    3600
2016-01-04 14:00:02 0     0    0    0    3600
2016-01-04 13:00:02 0     0    0    0    3600
2016-01-04 12:00:02 0     0    0    0    3600
2016-01-04 11:00:02 0     0    0    0    3600
2016-01-04 10:00:02 0     0    0    0    3600
2016-01-04 09:00:02 0     0    0    0    3600
2016-01-04 08:00:02 0     0    0    0    3600
2016-01-04 07:00:02 0     0    0    0    3600
2016-01-04 06:00:02 0     0    0    0    3600
2016-01-04 05:00:02 0     0    0    0    3600
2016-01-04 04:00:02 0     0    0    0    3600
  
```

At the bottom of the history window is a 'Rafraichir' button.

## 25 Etat des passerelles

Pour accéder à l'Etat des passerelles,

- Dans le menu, choisir **Diagnostics > Etat des passerelles**.

Cette page permet d'afficher l'état courant du paramétrage des passerelles, le nombre d'octets et de trames échangées et le nombre de trames en erreur.

The screenshot shows a web browser window with the URL 192.168.0.128/index-fr.html. The page title is 'XSLAN+2220 Switch SHDSL\_bis'. The breadcrumb navigation is '> Accueil > Diagnostics > État des passerelles'. A sub-menu item 'Visualisation des données série' is selected. The main content area is divided into two sections: 'Passerelle COM 1' and 'Passerelle COM 2'. Each section contains a table of configuration and statistics.

Passerelle COM 1	
Passerelle activée	Modbus Server
Configuration port série	9600-8-N-1
Caractères envoyés sur le port série	0
Caractères reçus sur le port série	0
Trames envoyées sur le réseau	0
Trames reçues du réseau	0
Réceptions avec erreur CRC/LRC	N/A
Émissions sans réponse	0
Connexions TCP actives	0

Passerelle COM 2	
Passerelle activée	
Configuration port série	
Caractères envoyés sur le port série	N/A
Caractères reçus sur le port série	N/A
Trames envoyées sur le réseau	N/A
Trames reçues du réseau	N/A
Réceptions avec erreur CRC/LRC	N/A
Émissions sans réponse	N/A
Connexions TCP actives	N/A

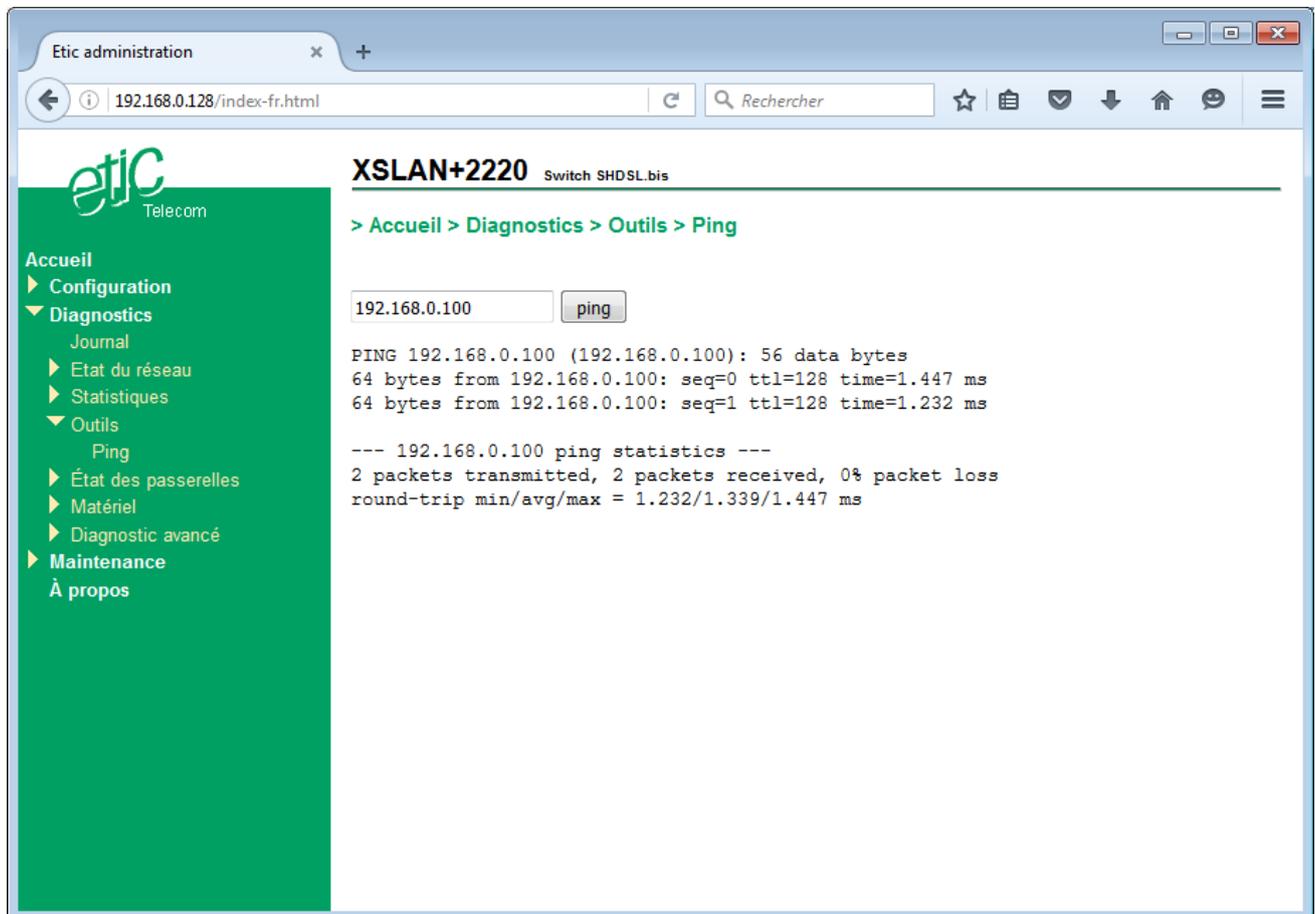
A 'Rafraîchir' button is located at the bottom of the page.

Pour analyser le trafic RX et TX traffic sur le lien série,

- Cliquer **Visualisation des données série**.

**26 Outil PING**

Cette page permet de commander l'émission d'une trame « PING » depuis le produit vers un équipement raccordé au réseau.



The screenshot shows a web browser window titled "Etic administration" with the URL "192.168.0.128/index-fr.html". The page content includes the Etic Telecom logo and a navigation menu on the left. The main content area displays the "XSLAN+2220 Switch SHDSL.bis" configuration page, specifically the "Ping" tool. A text input field contains "192.168.0.100" and a "ping" button. Below the button, the output of the ping command is shown:

```
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: seq=0 ttl=128 time=1.447 ms
64 bytes from 192.168.0.100: seq=1 ttl=128 time=1.232 ms

--- 192.168.0.100 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.232/1.339/1.447 ms
```

## 27 Sauvegarde et chargement d'un fichier de paramètres

Dans chaque page de configuration, il faut cliquer le bouton « Enregistrer » pour que la modification des paramètres soit prise en compte. Elle est sauvegardée en mémoire et appliquée immédiatement. Si le produit redémarre, la configuration n'est pas perdue ; c'est la configuration courante.

Il est possible d'enregistrer la configuration courante dans un fichier situé dans le produit, ou de l'exporter vers un PC sous forme d'un fichier éditable.

Réciproquement, il est possible de charger une configuration parmi l'ensemble des configurations enregistrées dans le produit ou bien d'importer un fichier de configuration sauvegardé dans un PC.

- Dans le menu, sélectionner **Maintenance > Gestion des configurations**.

The screenshot shows a web browser window titled "Etic administration" with the URL "192.168.0.128/index-fr.html". The page displays the "XSLAN+2220 Switch SHDSL.bis" configuration management interface. A green sidebar on the left contains the navigation menu with "Maintenance" selected. The main content area shows a table of saved configurations and options to register or import configurations.

	Nom	Date de création	Type
<input type="radio"/>	Factory_default	Wed Apr 6 11:14:16 2016	Reference configuration
<input type="radio"/>	Factory_default_with_advanced_SHDSL	Wed Apr 6 11:14:16 2016	Reference configuration
<input type="radio"/>	TEST	Mon Jan 11 22:31:18 2016	User configuration

Buttons: Supprimer, Exporter vers le PC, Charger cette configuration

Enregistrer la configuration courante

Nom de la configuration: Saved\_config

Enregistrer

Importer une configuration depuis le PC

Nom de la configuration: Imported\_config

Fichier à importer: Parcourir... Aucun fichier sélectionné.

Importer depuis le PC

**Pour enregistrer la configuration courante dans un fichier dans le produit,**

- Face au champ **Nom de la configuration**, attribuer un nom pour la configuration.
- Cliquer **Enregistrer**.

La configuration s'ajoute à la liste dans le tableau des **Configurations sauvegardées**.

**Pour charger comme configuration courante l'une des configurations de la liste,**

- Sélectionner la configuration dans la liste et cliquer **Charger cette configuration**.

**Pour exporter la configuration courante dans un fichier (.txt) sur un PC,**

- Commencer par enregistrer la configuration courante dans un fichier du produit comme indiqué précédemment,
- Puis sélectionner dans la liste la configuration à exporter et cliquer **Exporter vers le PC**.

**Pour importer un fichier de paramètres sauvegardé,**

- Cliquer **Parcourir...** puis sélectionner le fichier (XXX.txt) à restituer.
- Modifier éventuellement le nom de la configuration et cliquer **Importer depuis le PC**. La configuration correspondante apparaît dans la liste **Configurations sauvegardées**.
- Sélectionner la configuration dans la liste puis cliquer **Charger cette configuration** ; elle remplace la configuration courante.

Note : Un fichier de configuration ne peut être restauré que s'il a été constitué avec la même version de firmware.

## 28 Mise à jour du logiciel

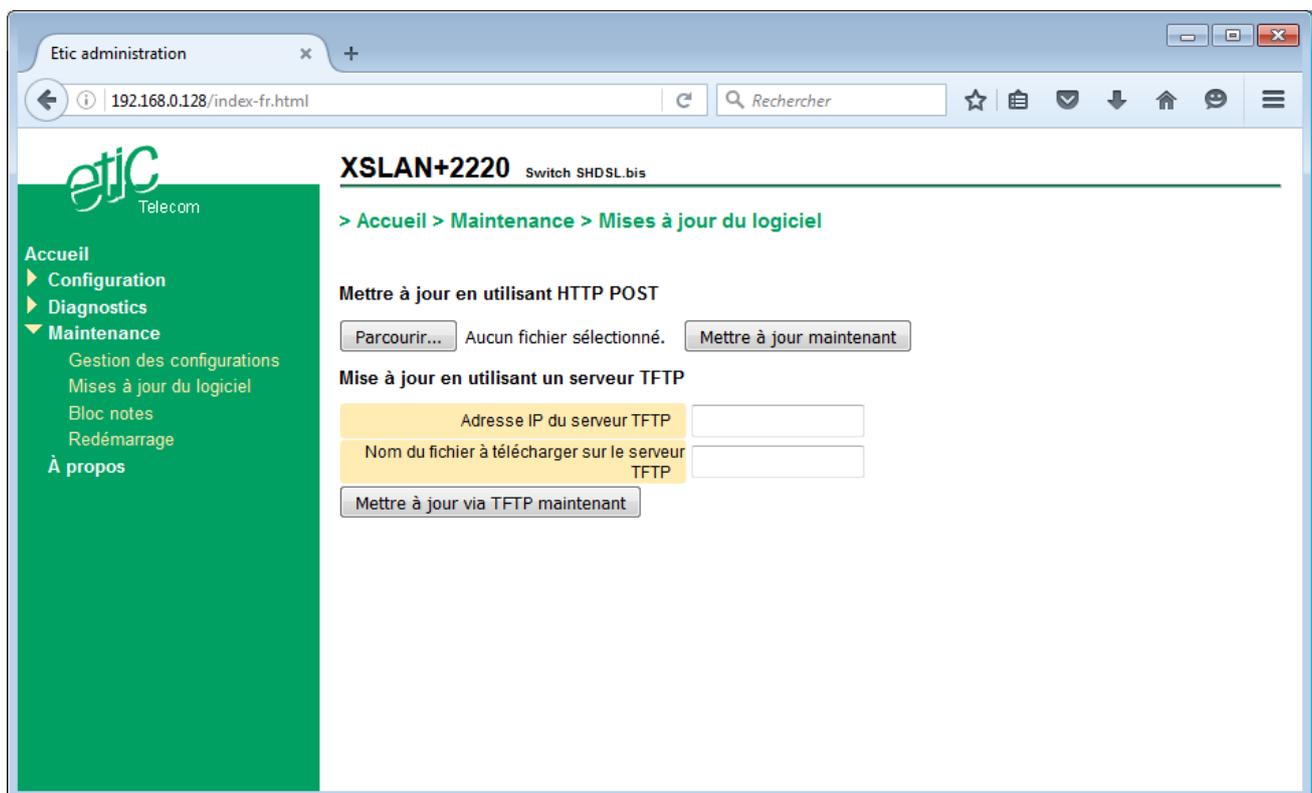
Elle s'effectue par la prise Ethernet de préférence ou bien à distance, via la ligne SHDSL par exemple. La mise à jour ne modifie pas le paramétrage du produit.

Si la mise à jour est effectuée à distance, on vérifiera que la nouvelle version du logiciel est compatible avec le paramétrage en cours, pour que la connexion SHDSL soit rétablie automatiquement après la mise à jour.

La mise à jour peut s'effectuer de deux façons :

Si le fichier de mise à jour est accessible depuis le PC de l'opérateur, elle peut s'effectuer directement par le navigateur en utilisant HTTP POST.

La mise à jour du logiciel peut aussi s'effectuer via un serveur TFTP sur lequel sera chargé au préalable le fichier de mise à jour.



**Pour effectuer la mise à jour du logiciel en utilisant HTTP POST,**

- Dans le menu, choisir **Maintenance > Mise à jour du logiciel**.
- Sélectionner le fichier du nouveau logiciel.
- Cliquer **Mettre à jour maintenant**.

Après quelques secondes, le voyant  clignote en rouge.

Attendre environ 5 minutes puis vérifier que la mise à jour s'est bien effectuée (menu **A propos**).

# ANNEXE 1 : SNMP MIB

## 1 Purpose of the document

This document describes the MIBs and the OIDs supported by the XS devices manufactured by ETIC Telecom.

## 2 Accessible OIDs and MIBs

### 2.1 Supported MIBs

The OIDs used are standard and located under iso.org.dod.internet.mgmt.mib-2.

It is only possible to read information, not to write it. The SET command is not supported.

The SNMP agent functionality in the XS device is provided by the Net-SNMP software package (<http://www.net-snmp.org>). A lot of common MIBs are implemented by this package. In addition to these MIBs, a few more specific MIBs are supported.

The common MIBs supported include the following :

- RFC1213-MIB (MIB-2)
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB

These will not be documented here unless there is something specific in the implementation in the XSLAN+ devices.

The specific MIBs are :

- HDLSL2-SHDSL-LINE-MIB
- BRIDGE-MIB
- RSTP-MIB

These will be described in detail because they are not implemented by default in Net-SNMP.

## ANNEXE 4

### 2.2 Network interface indexes

All the SNMP tables that deal with network interfaces are indexed with the network interface index. Indexes could change after a version upgrade. To be sure that the supervision works over the time the supervision should be linked to the internal interface name.

In the XS software versions the interface names are :

Interface name	Internal name
LAN1	lan1
LAN2	lan2
LAN3	lan3
LAN4	lan4
SHDSL1	sh1
SHDSL2	sh2
SHDSL3	sh3
SHDSL4	sh4

The interface names will not change over the time.

### 2.3 Querying the MIB

To query the MIB of the device and see what OID can be useful, the tools from the Net-SNMP project can be used. They can be installed on an Unix like operating system such as Linux or a BSD variant. They can also be installed on Windows using Cygwin.

To use them, start a shell in a terminal window and test these commands :

# This command will return all OIDs supported by the device.

```
mc@ubuntu:~$ snmpwalk -v1 -c public 192.168.0.128
SNMPv2-MIB::sysDescr.0 = STRING: ETIC Telecom XSLAN+4400 SHDSL switch, firmware
version v2.1.0-b2
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (26205510) 3 days, 0:47:35.10
SNMPv2-MIB::sysContact.0 = STRING: www.etictelecom.com
SNMPv2-MIB::sysName.0 = STRING: XS+
...
```

# This command queries one OID.

```
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 IF-MIB::ifName.8
IF-MIB::ifName.8 = STRING: lan4
```

# This command translates the name of an OID to its numeric representation.

# Note that the MIB file must be installed somewhere where Net-SNMP can find it.

```
mc@ubuntu:~$ snmptranslate IF-MIB::ifName.8 -On
.1.3.6.1.2.1.31.1.1.1.1.8
```

# Table display : SNMP tables can be displayed with this command :

```
mc@ubuntu:~$ snmptable -v1 -c public 192.168.0.201 IF-MIB::ifTable
SNMP table: IF-MIB::ifTable
...
```

## 3 Description of the supported OIDs

### 3.1 Sysdesc, Syslocation, SysName

- OID SNMPv2-MIB::sysDescr.0 : Type of product and firmware version
- OID SNMPv2-MIB::sysLocation.0 : Parameter "syslocation" in the web page
- OID SNMPv2-MIB::sysName.0 : Parameter "sysname" in the web page

#### 3.1.1 Example

```
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 SNMPv2-MIB::sysName.0
SNMPv2-MIB::sysName.0 = STRING: XS+
mc@ubuntu:~$ snmpget -v1 -c public 192.168.0.201 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: ETIC Telecom XSLAN+4400 SHDSL switch, firmware
version v2.1.0-b2
```

### 3.2 Network interfaces table (IF-MIB::ifTable)

List of the network interfaces of the device.

The XS can have up to 8 Ethernet interfaces :

- 4 10/100BASE-T Ethernet ports,
- 4 SHDSL 2BASE-TL ports.

The interfaces are named :

- lan1, lan2, lan3, lan4 for the 10/100BASE-T interfaces (from 1 to 4)
- sh1, sh2, sh3, sh4 for the SHDSL interfaces (from 1 to 4).
- The br\_lan and br\_sh interfaces are Linux bridge interfaces. They allow Ethernet bridging between the ports of the device.

In this table there are a few particularities :

- OID IF-MIB::ifAdminStatus : Display the administrative state of the interface.
- Warning : For the SHDSL ports, the value ifAdminStatus is « up » when the connection is established, and « down » otherwise.
- OID IF-MIB::ifOperStatus : Is « up » when a connection is established, or « down » when there is no connection. This is true for the SHDSL and LAN ports.
- OID ifIndex : Index of the interface, used in many tables of the product.
- OID ifSpeed : Data rate of the interface. Note: for the SHDSL ports, this value is always 100Mb/s.

#### 3.2.1 Example

```
mc@ubuntu:~$ snmptable -v1 -c public 192.168.0.201 IF-MIB::ifTable
SNMP table: IF-MIB::ifTable
```

...

## ANNEXE 4

### 3.3 SHDSL MIB (HDSL2-SHDSL-LINE-MIB)

This MIB contains information relative to the SHDSL connections. It is published by the IETF in RFC4319.

#### 3.3.1 Table HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrTable :

This table contains information about how the line is working.  
At least the Attenuation and SNR margin should be monitored.

The attenuation gives an indication about the length of the line and the insertion losses of the connectors.  
The SNR margin tells how much noise the receiving modem can bear without causing transmission errors or disconnects.

The number of erroneous seconds should also be monitored. It indicates the availability of the line. A number near zero indicates a noise free operation. A high number indicates noise or signal distortion somewhere on the line. Usual causes include crosstalk, inadequate surge protectors and EMI disturbances caused by other equipment.

- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn: Line attenuation
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrSnrMgn: SNR margin
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointrrActivationState: Line status, connected or not (Warning, the other fields are invalid when this parameter value is not « data »)
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCRCAnomalies: CRC errors on the line
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointLOSWS: Seconds with one or more synchronization loss
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointES: Erroneous seconds. A second is « erroneous » if there are one or several CRC errors or synchronization loss
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointSES: Severely erroneous seconds . A second is « severely erroneous » if there are at least 50 CRC errors or one or several synchronization loss.
- OID HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointUAS: Unavailable seconds. A second is « unavailable » after 10 consecutive severely erroneous seconds. It is necessary to have 10 seconds with no « severely erroneous » seconds to leave this state.

For more information, refer to ITU-T standard G.991.2 (G.SHDSL.bis).

The other fields are not supported.

#### Example

```
mc@ubuntu:~$ snmpwalk -v1 -c public 192.168.0.201 HDSL2-SHDSL-LINE-
MIB::hds12ShdslEndPointCurrTable
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.12.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.13.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.14.0.networkSide.wirePair1 =
INTEGER: 0 dB
HDSL2-SHDSL-LINE-MIB::hds12ShdslEndPointCurrAtn.15.0.networkSide.wirePair1 =
INTEGER: 0 dB
...
```

## Numeric OIDs

Replace “ifindex” with the SHDSL interface index in the table below.

hdsl2ShdslEndpointCurrAtn	.1.3.6.1.2.1.10.48.1.5.1.1.ifindex.0.1.1
hdsl2ShdslEndpointCurrSnrMgn	.1.3.6.1.2.1.10.48.1.5.1.2.ifindex.0.1.1
hdsl2ShdslEndpointCurrStatus	.1.3.6.1.2.1.10.48.1.5.1.3.ifindex.0.1.1
hdsl2ShdslEndpointES	.1.3.6.1.2.1.10.48.1.5.1.4.ifindex.0.1.1
hdsl2ShdslEndpointSES	.1.3.6.1.2.1.10.48.1.5.1.5.ifindex.0.1.1
hdsl2ShdslEndpointCRCAnomalies	.1.3.6.1.2.1.10.48.1.5.1.6.ifindex.0.1.1
hdsl2ShdslEndpointLOSWS	.1.3.6.1.2.1.10.48.1.5.1.7.ifindex.0.1.1
hdsl2ShdslEndpointUAS	.1.3.6.1.2.1.10.48.1.5.1.8.ifindex.0.1.1

### 3.3.2 Table HDSL2-SHDSL-LINE-MIB::SpanStatusTable

- OID hdsl2ShdslStatusActualLineRate (.1.3.6.1.2.1.10.48.1.2.1.3.ifindex) : data rate of the SHDSL line. It is recommended to monitor this OID, if the chosen profile for the line is not a fixed datarate profile.

The other fields are not supported and are set to 0.

### 3.3.3 Table HDSL2-SHDSL-LINE-MIB::SpanConfProfileTable

This table gives the list of the profiles defined for the SHDSL links configuration. These informations are the same as the ones in the web page « SHDSL ports »

### 3.3.4 Table HDSL2-SHDSL-LINE-MIB::SpanConfTable

This table gives the SHDSL profile associated with each SHDSL port.

## 3.4 MIB : BRIDGE-MIB::dot1dBridge

Information about the Ethernet bridge are gathered under this OID. This MIB is published by the IETF under RFC4188.

### 3.4.1 OID BRIDGE-MIB::dot1dBase

The following information is displayed :

- OID BRIDGE-MIB::dot1dBaseBridgeAddress : Bridge MAC address
- OID BRIDGE-MIB::dot1dBaseNumPorts : Number of ports in the bridge
- OID BRIDGE-MIB::dot1dBaseType : Type of bridge (Tranparent-only)

## ANNEXE 4

### 3.4.2 Table BRIDGE-MIB::dot1dBasePortTable :

This table provides details of the bridge ports. Throughout the BRIDGE-MIB, ports are referenced by number. This table associates a bridge port number with ifIndex (network interface number).

- OID dot1dBasePort : Port number
- OID dot1dBasePortIfIndex : Port index in the ifTable table
- OID dot1dBasePortCircuit : Always 0
- OID dot1dBasePortDelayExceededDiscards : Not supported
- OID dot1dBasePortMtuExceededDiscards : Not supported

### 3.4.3 OID BRIDGE-MIB::dot1dTp

This oid gathers information on transparent bridges (= Ethernet switches).

### 3.4.4 Table BRIDGE-MIB::dot1dTpFdbTable

This table contains the MAC address table learned by the product.

- OID dot1dFdbAddress : MAC address learned by the switch
- OID dot1dFdbPort : Which port to send a frame with the destination MAC address above.
- OID dot1dFdbStatus : the state of the entry in the table: learned or fixed.

This table allows you to draw a "map" of the network and equipment connected to it.

### 3.4.5 RSTP and STP

The RSTP and STP system can be polled with the standard MIBs BRIDGE-MIB and RSTP-MIB. The RSTP-MIB is published by the IETF in RFC4318.

## ANNEXE 2 : Portée de la liaison SHDSL

Le tableau ci-dessous donne le débit qu'il est possible d'obtenir sur une liaison SHDSL en fonction du diamètre du fil et de la distance.

Ces valeurs sont données à titre indicatif et en l'absence de perturbation.

<b>Débit</b>	192Kb/s	1,2Mb/s	2,3Mb/s	5,7 Mb/s	6.7 Mb/s	10 Mb/s	12 Mb/s	15 Mb/s
<b>Distance (Ø 0.9 mm) *</b>	13 km	8 km	6 km	3.7 km	2.5 km	1.5 km	1 km	0.7 km
<b>Distance (Ø 0.4 mm) *</b>	7 km	4 km	3 km	2 km	1.3 km	0.9 km	0.6 km	0.4 km

## ANNEXE 3 : Compatibilité entre un ancien switch XSLAN et le switch XSLAN+

Cette annexe concerne les XSLAN de première génération (2005-2012). Ces produits étaient conformes au standard Shdsl à 2,3 Mb/s, tandis que les familles suivantes sont conformes au standard Shdsl.bis à 5,7 Mb/s.

Un switch SHDSL XSLAN de première génération et un switch SHDSL XSLAN+ peuvent être connectés l'un à l'autre au travers d'une paire torsadée.

La version du logiciel du switch XSLAN+ doit être supérieure à V1.3.2.

### 1/ Cas d'un switch XSLAN configuré comme STU-R (NTU)

La compatibilité entre un switch XSLAN et un switch XSLAN+ est assurée sans condition.

Le switch XSLAN+ doit être configuré avec le profil « STU-C, standard » ou avec un profil à débit fixe. Dans ce cas le débit doit être inférieur ou égal à 2304 Kb/s.

### 2/ Cas d'un switch XSLAN configuré comme STU-C (LTU)

La compatibilité entre un switch XSLAN et un switch XSLAN+ est assurée uniquement si la version du logiciel du switch XSLAN est supérieure ou égale à 2.20.

Le débit ne peut pas être établi à 128 kb/s ; il doit être établi à une valeur supérieure.

Le switch XSLAN+ doit être configuré avec le profil « STU-R, auto ».

## ANNEXE 4 : Registres du serveur d'état Modbus TCP

Modbus TCP server:

Base Register Address: 40011

NodeID: 255

All statuses can be read in one request Read Holding Register (FC=03)

Register MAP:

**Register 0:** interfaces state: TYPE WORD

- bit 0..1 - status of the Ethernet LAN1
  - 00 disabled
  - 10 enabled / disconnected
  - 11 enabled / connected
- bit 2..3 - status of the Ethernet LAN2
- bit 4..5 - status of the Ethernet LAN3
- bit 6..7 - status of the Ethernet LAN4
- bit 8..9 - status of the SHDSL1
  - 00 disabled
  - 10 enabled / disconnected
  - 11 enabled / connected
- bit 10..11 - status of the SHDSL2
- bit 12..13 - status of the SHDSL3
- bit 14..15 - status of the SHDSL4

**Register 1:** Fail safe ring: TYPE WORD

- Bit 0: (0: disabled; 1: disabled)
- Bit 1: (0: ring OK; 1: ring failure)

**Register 2:** RSTP status: TYPE WORD

- bit 0..1 - status of the Ethernet LAN1
  - 00 disabled
  - 01 blocked
  - 10 learning
  - 11 forwarding
- bit 2..3 - status of the Ethernet LAN2
- bit 4..5 - status of the Ethernet LAN3
- bit 6..7 - status of the Ethernet LAN4
- bit 8..9 - status of the SHDSL1
  - 00 disabled
  - 01 blocked
  - 10 learning
  - 11 forwarding
- bit 10..11 - status of the SHDSL2
- bit 12..13 - status of the SHDSL3
- bit 14..15 - status of the SHDSL4

**Note:** If Vpnlloop is enabled, tap0 RSTP status replace RSTP status of LAN1.

## ANNEXE 4

**Register 3:** Bit rate port 1: TYPE UINT (0 ... 65535) - kbit/s

**Register 4:** Bit rate port 2: TYPE UINT (0 ... 65535) - kbit/s

**Register 5:** Bit rate port 3: TYPE UINT (0 ... 65535) - kbit/s

**Register 6:** Bit rate port 4: TYPE UINT (0 ... 65535) - kbit/s

**Register 7:** SNR ratio margin port 1: TYPE UINT (0 ... 65535) – dB

**Register 8:** SNR ratio margin port 2: TYPE UINT (0 ... 65535) – dB

**Register 9:** SNR ratio margin port 3: TYPE UINT (0 ... 65535) – dB

**Register 10:** SNR ratio margin port 4: TYPE UINT (0 ... 65535) – dB

**Register 11:** Number of erroneous seconds during the last 15mn port 1: TYPE UINT (0 ... 65535)

**Register 12:** Number of erroneous seconds during the last 15mn port 2: TYPE UINT (0 ... 65535)

**Register 13:** Number of erroneous seconds during the last 15mn port 3: TYPE UINT (0 ... 65535)

**Register 14:** Number of erroneous seconds during the last 15mn port 4: TYPE UINT (0 ... 65535)

**Register 15-16:** Number of erroneous seconds during the last 24 hours port 1: TYPE UDINT (0 ... 4294967295)

**Register 17-18:** Number of erroneous seconds during the last 24 hours port 2: TYPE UDINT (0 ... 4294967295)

**Register 19-20:** Number of erroneous seconds during the last 24 hours port 3: TYPE UDINT (0 ... 4294967295)

**Register 21-22:** Number of erroneous seconds during the last 24 hours port 4: TYPE UDINT (0 ... 4294967295)

**Register 23:** Vpnloop state: TYPE WORD

- Bit 0: (0: disconnected; 1: connected)



405 rue Lavoisier  
38330 Montbonnot Saint Martin  
France

Tel : +33 (0)4 76 04 20 00  
contact@etictelecom.com

[www.etictelecom.com](http://www.etictelecom.com)