

# CT-633 C

## IAD VoIP sans fil

# Manuel de l'utilisateur

Version A1.0, 27 août 2004

---



## **Attention**

- Débranchez toujours les lignes d'alimentation et téléphoniques avant d'entretenir ou de démonter cet appareil.
- Utilisez une alimentation électrique appropriée et un cordon de téléphone agréé UL. Les spécifications de l'alimentation électrique sont clairement indiquées dans l'annexe A – Spécifications.

## **Préface**

Le présent manuel de l'utilisateur fournit des informations générales sur les caractéristiques, les fonctions et le mode d'emploi de l'IAD VoIP sans fil CT-633 C.

Le lecteur est supposé avoir des connaissances de bases en télécommunications. Pour les actualisation du produit, la publication de nouveaux produits, les révisions du manuel, la mise à jour du logiciel, le support technique etc., consultez Comtrend Corporation à l'adresse suivante <http://www.comtrend.com>

Ce document peut être modifié sans préavis.

## **Copyright**

Copyright© 2004 Comtrend Corporation. Tous droits réservés. Les informations et les messages contenus dans le présent document sont la propriété exclusive de Comtrend Corporation. Aucune partie de ce document ne peut être traduite, transcrite, reproduite sous quelque forme que ce soit sans l'autorisation écrite préalable de Comtrend Corporation.

## **Assistance technique**

Si le produit est en panne ou s'il ne fonctionne pas correctement, contactez un technicien de l'assistance technique pour réparation immédiate, ou envoyez un e-mail à [INT-support@comtrend.com](mailto:INT-support@comtrend.com)

# Table des matières

<b>CHAPTER 1</b>	<b>PRESENTATION</b>	<b>6</b>
1.1	VUE D'ENSEMBLE DU PRODUIT	6
1.2	APPLICATION	8
1.3	CARACTERISTIQUES	9
1.4	VOYANTS DEL DU PANNEAU FRONTAL	10
<b>CHAPTER 2</b>	<b>INSTALLATION DU MATERIEL</b>	<b>11</b>
2.1	INSTALLATION DU MATERIEL	11
2.2	INSTALLATION DU PILOTE USB	13
2.3	DESINSTALLATION DU PILOTE USB	15
<b>CHAPTER 3</b>	<b>CONNEXION VIA LE NAVIGATEUR WEB</b>	<b>17</b>
3.1	ADRESSE IP	17
3.2	PROCEDURE DE CONNEXION	19
<b>CHAPTER 4</b>	<b>MGCP</b>	<b>21</b>
<b>CHAPTER 5</b>	<b>CONFIGURATION DE BASE</b>	<b>24</b>
5.1	INFORMATIONS RELATIVES A LA VERSION	24
5.2	ETAT INTERNET&VOIP	24
5.3	CHANGEMENT DE MOT DE PASSE	25
5.4	ETAT DE LA LIAISON ADSL	26
5.5	CONFIGURATION DU WAN	28
5.5.1	<i>RFC 1483 Bridged</i>	29
5.5.2	<i>RFC 1483 Routed</i>	30
5.5.3	<i>PPPoE</i>	31
5.5.4	<i>PPPoA</i>	34
5.5.5	<i>MER</i>	35
5.6	CONFIGURATION DU LAN	38
5.7	CONFIGURATION DU WLAN	39
5.7.1	<i>Paramètres WLAN de base</i>	39
5.7.2	<i>Fonction WLAN avancées</i>	40
5.7.3	<i>Paramètres WEP WLAN</i>	41

5.8	ROUTAGE.....	43
5.8.1	<i>Activation RIP.....</i>	44
5.8.2	<i>Configuration de route statique.....</i>	45
5.9	ENREGISTREMENT .....	46
5.10	REDEMARRER.....	46
5.11	RECUPERATION DES PARAMETRES PAR DEFAUT.....	47
<b>CHAPTER 6 CONFIGURATION AVANCEE .....</b>		<b>48</b>
6.1	MODE ADSL.....	48
6.1.1	<i>DHCP.....</i>	49
6.1.2	<i>Serveur DHCP.....</i>	49
6.1.3	<i>Relais DHCP.....</i>	52
6.1.4	<i>Client DHCP.....</i>	53
6.2	PARE-FEU .....	54
6.2.1	<i>Politiques.....</i>	54
6.2.2	<i>Attaques.....</i>	56
6.2.3	<i>NAT politique.....</i>	60
6.2.4	<i>Interfaces NAT.....</i>	62
6.2.5	<i>Adresse NAT publique.....</i>	64
6.3	CONFIGURATION.....	65
6.3.1	<i>Interfaces.....</i>	66
6.3.2	<i>VCC.....</i>	70
6.3.3	<i>PPPoE.....</i>	74
6.3.4	<i>PPPoA.....</i>	75
6.4	PROXY IGMP .....	75
6.5	PONTAGE.....	77
6.5.1	<i>Pont.....</i>	77
6.5.2	<i>Spanning tree.....</i>	79
6.5.3	<i>Filtres.....</i>	81
6.5.4	<i>Filtre Layer2.....</i>	83
6.6	IPQOS .....	85
6.6.1	<i>Configuration.....</i>	85

6.6.2	<i>Poids WFQ</i> .....	91
6.6.3	<i>Condition du trafic</i> .....	92
6.7	STATISTIQUES DU SYSTEME .....	93
6.7.1	<i>Statistiques de l'interface</i> .....	93
6.7.2	<i>TCP-IP</i> .....	95
6.7.3	<i>DHCP-Lease</i> .....	96
6.8	STATISTIQUES ATM .....	97
6.8.1	<i>AAL5</i> .....	97
6.8.2	<i>Encapsulation</i> .....	97
6.9	STATISTIQUES WFQ.....	98
6.10	DIAGNOSTICS .....	99
6.10.1	<i>OAM Loopback</i> .....	99
6.10.2	<i>Ping</i> .....	100
<b>CHAPTER 7</b>	<b>MISE A JOUR DU LOGICIEL VIA FTP</b> .....	<b>102</b>
<b>CHAPTER 8</b>	<b>ANNEXE A : SPECIFICATIONS</b> .....	<b>104</b>
<b>CHAPTER 9</b>	<b>ANNEXE B : BROCHAGES</b> .....	<b>107</b>
<b>CHAPTER 10</b>	<b>ANNEXE C : DEPANNAGE</b> .....	<b>108</b>
<b>CHAPTER 11</b>	<b>ANNEXE D : GLOSSAIRE</b> .....	<b>109</b>

## Chapter 1 Présentation

La voix transmise par IP (VoIP) utilise le protocole Internet (IP) pour transmettre la voix par paquets sur un réseau IP. Par conséquent, une VoIP peut être réalisée sur tout réseau de données utilisant l'IP : Internet, intranets et réseaux locaux (LAN). En VoIP, les signaux vocaux sont numérisés, compressés et convertis en paquets IP. Les paquets compressés sont transmis par le réseau IP. Des protocoles de signalisation sont utilisés pour définir et fractionner les appels, transporter les informations nécessaires pour localiser les utilisateurs et négocier les capacités. La VoIP est basée sur l'IP, et l'IP est normalement utilisé pour la circulation de données.

Les problèmes de temps réel sont plus préoccupants lorsque la voix et les données sont transmises sur le même réseau. Ces problèmes concernent la qualité vocale, interopérabilité, l'évolutivité etc. Initialement, l'ITU est sorti avec des normes VoIP comme ITU-T H.323. Ensuite, plusieurs normes VoIP importantes ont été proposées, comme MGCP, H.248 Megaco, SIP, etc.

Ce chapitre présente l'IAD VoIP CT-633 C. Il comprend une vue d'ensemble du produit, la description de ses caractéristiques et applications, et explique les fonctions des voyants DEL du panneau frontal.

### 1.1 Vue d'ensemble du produit

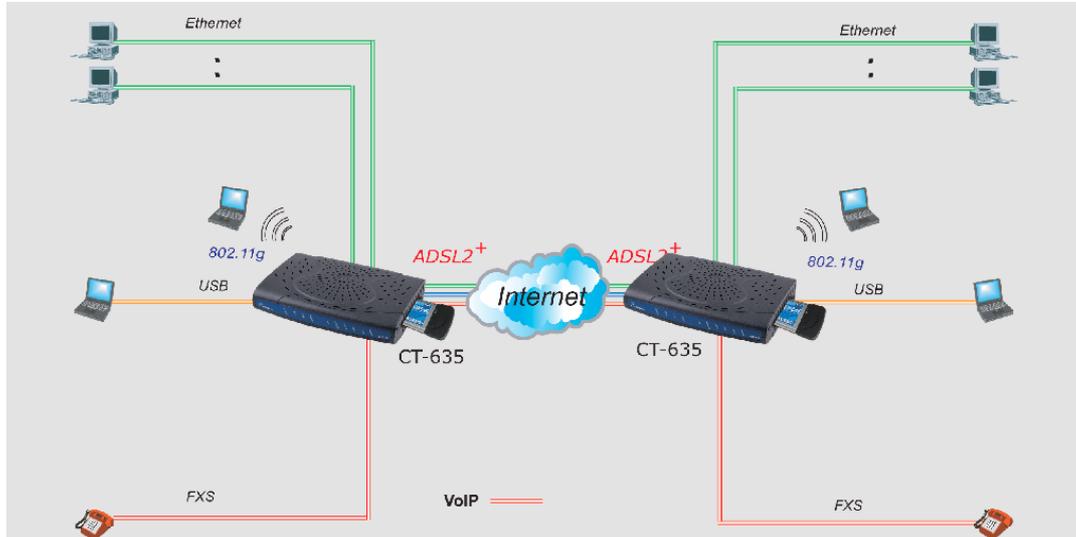
Le modèle CT-633 C de Comtrend est un IAD (Integrated Access Device) sans fil VoIP puissant qui offre un signal vocal de qualité similaire à celle des réseaux payants, fiable et en temps réel par Internet. Le CT-633 C est destiné à l'ADSL2/2+ par réseau téléphonique ordinaire (Annexe A). Le CT-633 C est destiné aux utilisateurs privés et professionnels souhaitant intégrer les technologies ADSL2/2+, WLAN et VoIP. Avec la technologie à large bande ADSL2/2+, le CT-633 C offre aux utilisateurs un accès facile à Internet via WLAN ou Ethernet, et le support VoIP à très hautes vitesses.

Un téléphone ordinaire est raccordé au port RJ-11 (prise de téléphone) au dos du CT-633 C, permettant d'acheminer les appels vers n'importe quelle destination dans le monde – ce qui réduit considérablement ou élimine la facturation d'appels longue distance. Il est inutile d'allumer vos PC pour appeler. Le CT-633 C supporte la qualité de service politique sur la couche 3, qui offre un service vocal de haute qualité. Le CT-633 C répond à l'ensemble de vos besoins en termes de réseau et

de téléphonie avec une seule unité intégrée qui réduit l'espace nécessaire et le coût du matériel et du câblage. Le CT-633 C représente ainsi la solution la plus économique pour votre application.

## 1.2 Application

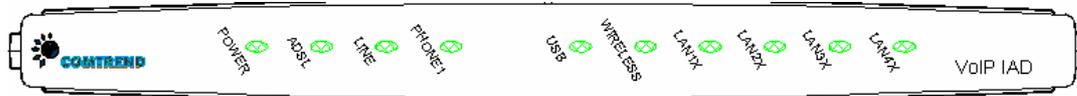
Les figures ci-après indiquent le diagramme d'application du CT-633 C.



## 1.3 Caractéristiques

- Routeur ADSL2/2+ intégré**
- Supporte la voix sur IP (VoIP)**
- AP 802.11g intégré**
- Compatibilité rétroactive avec 802.11b**
- Supporte l'identification de l'appelant**
- Supporte la suppression de silence**
- Utilise un téléphone ordinaire pour appeler par Internet à faible coût**
- Utilise une seule adresse IP pour accéder à Internet sur l'ensemble de votre réseau**
- Configurable par l'intermédiaire du navigateur web de votre PC en réseau**
- Bloque des accès Internet spécifiques externes et internes grâce au filtrage des paquets**
- Supporte PPTP, L2TP et IpSec indirect**
- Supporte la Life Line pour les urgences**

## 1.4 Voyants DEL du panneau frontal



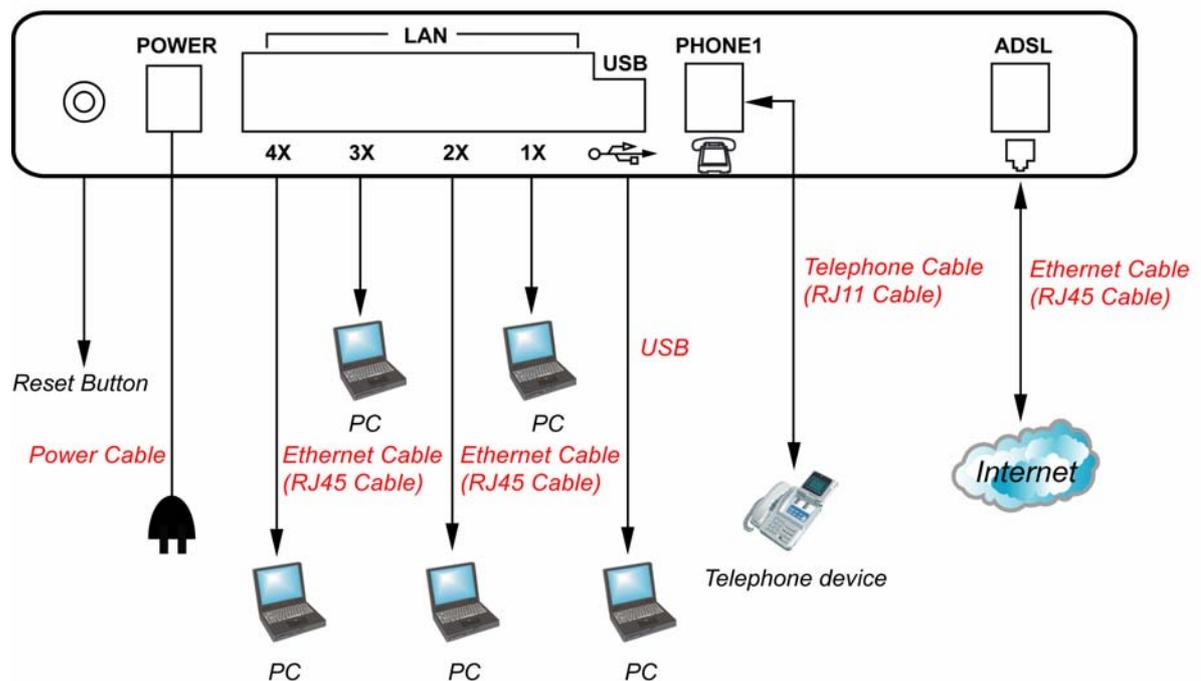
CT-635 FRONT PANEL

Voyant DEL	Couleur	Mode	Fonction
Alimentation	Vert	Allumé	L'appareil est alimenté.
		Eteint	L'appareil n'est pas alimenté.
ADSL	Vert	Allumé	La liaison ADSL est établie.
		Clignotant	La liaison ADSL est en vérification ou un trafic ADSL est en cours.
		Eteint	La liaison ADSL n'est pas établie.
LINE	Vert	Allumé	La ligne PSTN externe dessert le téléphone.
		Eteint	La VoIP dessert le téléphone.
PHONE1	Vert	Allumé	Le téléphone est décroché.
		Eteint	Le téléphone est raccroché.
		Clignotant	La VoIP ne peut pas desservir ce téléphone.
USB	Vert	Allumé	Une liaison USB est établie.
		Eteint	La liaison USB n'est pas établie.
		Clignotant	Activité sur la liaison USB
WIRELESS	Vert	Clignotant	Trafic en cours par l'intermédiaire du WLAN.
LAN 1x~4x	Vert	Allumé	Connexion Ethernet établie.
		Clignotant	Transmission ou réception de données en cours
		Eteint	La connexion Ethernet n'est pas établie.

## Chapter 2 Installation du matériel

### 2.1 Installation du matériel

La figure ci-dessous illustre les connexions possibles au panneau arrière du CT-633 C.



**Prudence** : Débranchez toujours les lignes téléphoniques de la prise murale avant de réparer ou de démonter cet appareil.

- Branchez l'adaptateur d'alimentation à la **prise d'alimentation** de l'appareil, puis branchez l'adaptateur dans la prise murale.
- Raccordez le **port USB** à un PC avec un câble USB standard.
- Raccordez le **port LAN** à un PC ou à un hub avec un câble RJ45.
- Raccordez le **port LINE** à la prise murale, à un téléphone ordinaire ou à un filtre micro avec un câble à connecteur RJ11.
- Branchez le téléphone au **port RJ11 PHONE1** pour le service VoIP.

- Allumez le commutateur d'alimentation du panneau arrière.

**Remarque 1:** Si l'appareil ne s'allume pas, ou s'il ne fonctionne pas normalement, vérifiez en premier lieu que l'alimentation électrique est correctement branchée et essayez de l'allumer. (Si la DEL ALARM clignote en rouge, une alarme s'est produite.)

**Remarque 2:** Restaurez les paramètres par défaut du routeur en maintenant le bouton Reset de l'appareil enfoncé jusqu'à ce que la DEL **PHONE1** commence à clignoter simultanément (environ 5 secondes). Une fois l'appareil réinitialisé, et si la connexion est établie, les DEL LAN, ADSL ou USB sont allumées en vert, en fonction du type de connexion.

**Remarque 3:** Vous pouvez aussi réinitialiser le routeur en exécutant le logiciel de l'appareil et en sélectionnant la commande **ERASE** du menu **Erase and Reboot**.

## 2.2 Installation du pilote USB

Vérifiez que le routeur est débranché avant d'installer le logiciel !

Observez les étapes suivantes pour installer le pilote USB :

**ETAPE 1 :** Insérez le disque CD-ROM du routeur ADSL USB.

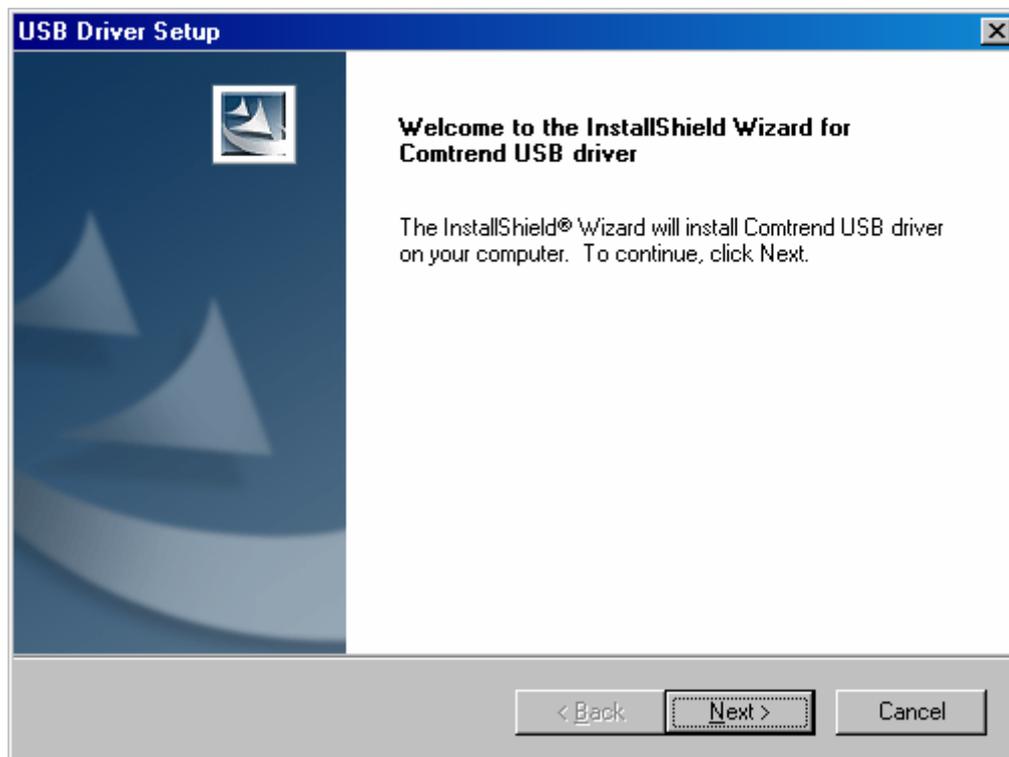
**ETAPE 2 :** Naviguez dans le CD-ROM et ouvrez le dossier **USB Driver**

 (E:)  USB Driver puis cliquez deux fois sur **SETUP.EXE** :

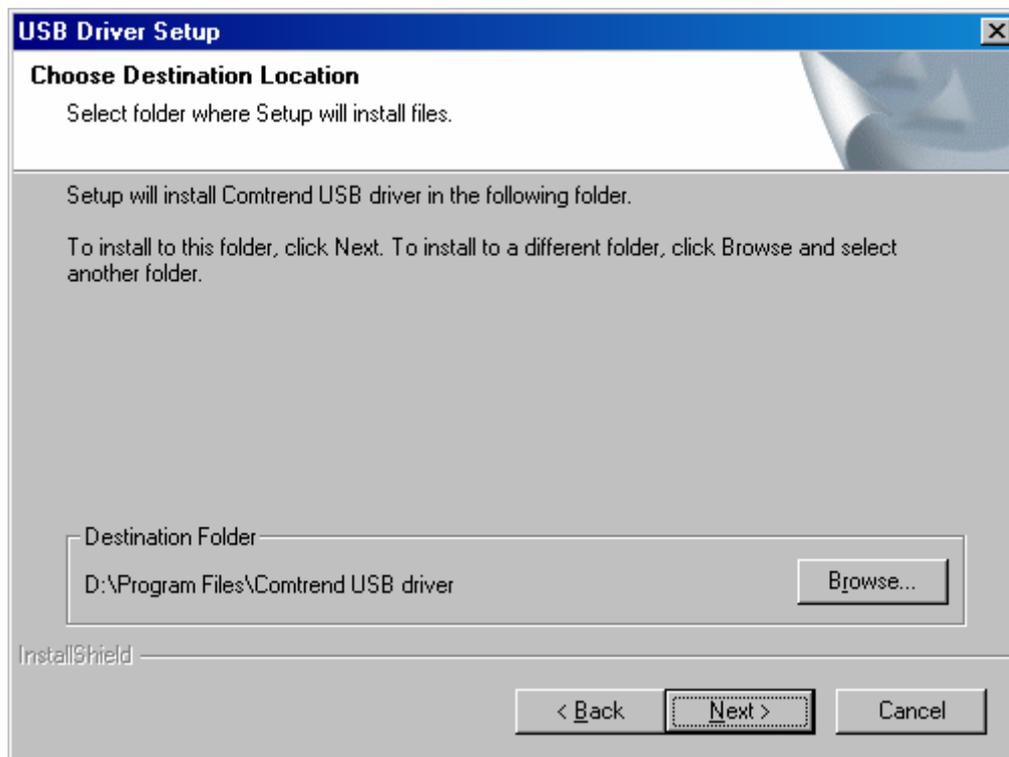


Setup.exe

**ETAPE 3 :** Cliquez sur le bouton **Next** pour que votre système d'exploitation Windows procède à l'installation du pilote.



**ETAPE 4 :** Un message confirmant la réussite de l'installation s'affiche lorsque l'installation est terminée.



**ETAPE 5 :** Raccordez votre routeur au port USB du PC

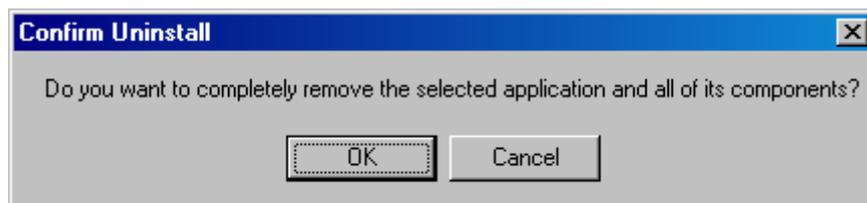
## 2.3 Désinstallation du pilote USB

Observez les étapes suivantes pour désinstaller le pilote USB :

**ETAPE 1 :** Cliquez sur le bouton **Démarrer** de Windows et choisissez Programmes>Pilotes Comtrend CT-6xx. Cliquez sur **Désinstaller**.



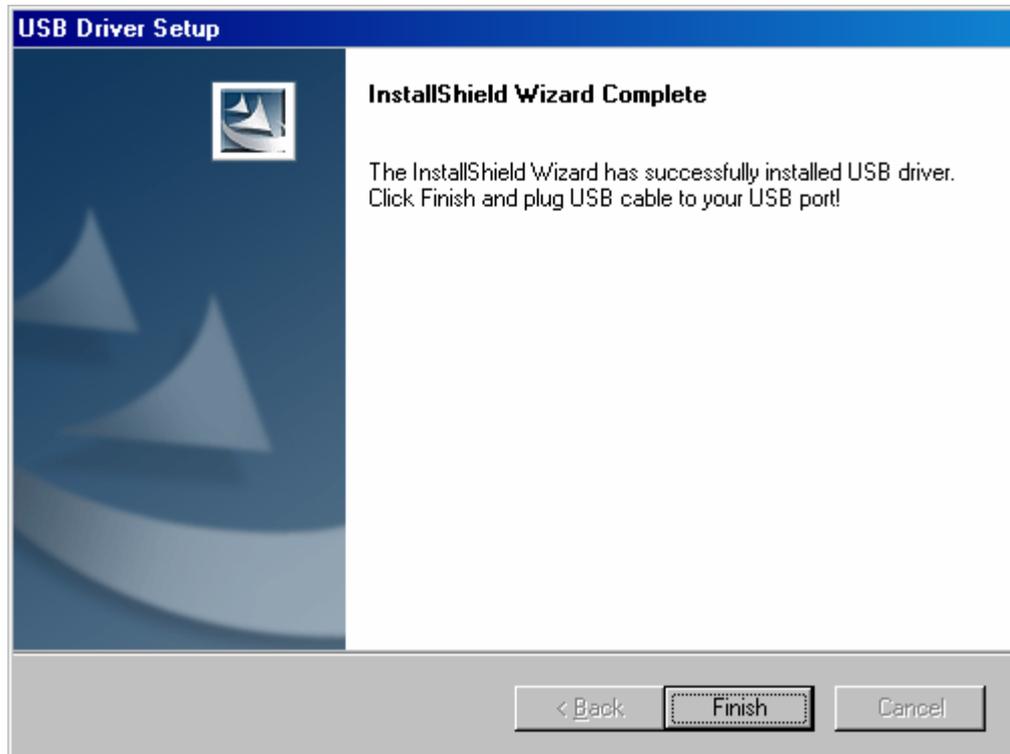
**ETAPE 2 :** Cliquez sur OK lorsque vous êtes invité à confirmer la désinstallation.



**ETAPE 3 :** A l'invite du message ci-dessous, débranchez le câble USB de votre PC et cliquez sur le bouton **OK**.



**ETAPE 4 :** Une fois le pilote supprimé, un message de fin d'opération s'affiche. Cliquez sur Finish (Terminé) pour fermer la fenêtre.



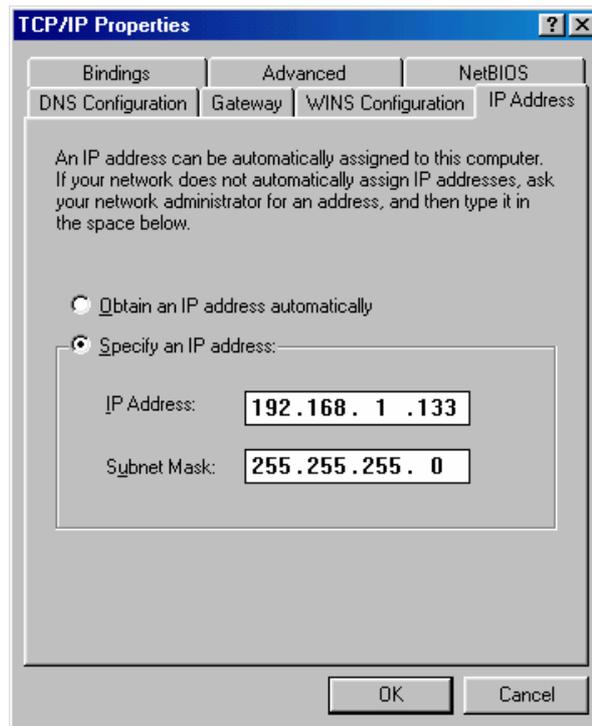
## Chapter 3 Connexion via le navigateur web

Cette section indique comment gérer l'IAD par l'intermédiaire d'un navigateur web à partir des extrémités locale et distante. Vous pouvez utiliser un navigateur web comme Microsoft Internet Explorer ou Netscape Navigator. Pour configurer le système, il est conseillé d'utiliser des versions récentes des navigateurs, capables de supporter intégralement JavaScript. Il est préférable de régler la résolution de votre écran sur 1024 x 768. Pour changer la résolution, vous pouvez utiliser le panneau de configuration de Microsoft Windows, cliquer sur l'icône **Affichage** et modifier les paramètres d'affichage. Un compte utilisateur unique par défaut est attribué, dont le nom d'utilisateur est **root** et le mot de passe **1234**. Les utilisateurs peuvent changer le mot de passe par défaut lorsqu'ils sont connectés à l'appareil.

### 3.1 Adresse IP

Pour vous connecter à l'appareil à l'aide d'un navigateur web, votre poste de travail et l'appareil doivent se trouver sur le même segment. L'adresse IP par défaut est 192.168.1.1. Vous pouvez modifier l'adresse IP de votre PC en changeant son TCP/IP. Observez les étapes ci-après :

**ETAPE 1** : Accédez à l'écran TCP/IP et changez l'adresse IP pour le domaine 192.168.1.x/24.



**ETAPE 2 :** Cliquez sur **OK** pour envoyer les paramètres. Redémarrez l'ordinateur comme vous y êtes invité.

**ETAPE 3 :** Démarrez votre navigateur Internet avec l'adresse IP par défaut 192.168.1.1.

### 3.2 Procédure de connexion

Pour vous connecter au système depuis le navigateur web, observez les étapes suivantes :

**ETAPE 1: \_\_\_\_\_** Démarrez votre navigateur Internet.

**ETAPE 2 :** Tapez l'adresse IP de l'IAD dans le champ d'adresse web. Par exemple, si l'adresse IP est 192.168.1.1, tapez <http://192.168.1.1>

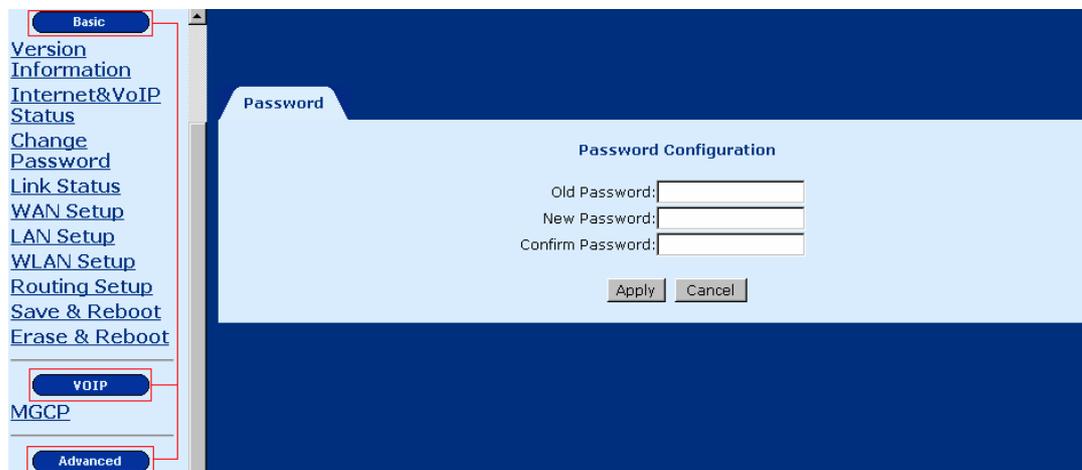


**ETAPE 3 :** A l'invite, tapez votre nom d'utilisateur et votre mot de passe ; le nom d'utilisateur par défaut est **root**, et le mot de passe **1234**. Les deux sont sensibles à la casse.

**Remarque :** Le nom d'utilisateur et le mot de passe peuvent être différents selon les fournisseurs d'accès ; contactez votre fournisseur d'accès pour plus de détails.

**ETAPE 4 :** Une fois la connexion réussie, vous accédez au menu principal. Cette fenêtre encadrée présente un menu d'hyperliens sur la gauche. Tous ces liens sont classés en trois groupes :

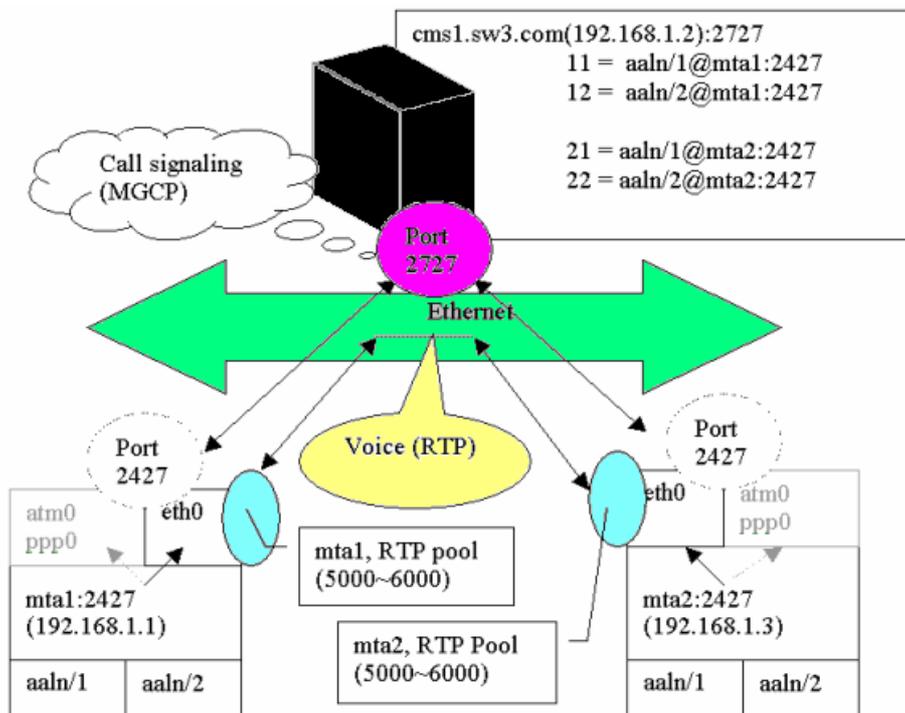
1. **Basic**
2. **VoIP**
3. **Advanced**



## Chapter 4 MGCP

L'option MGCP sert à vérifier l'application MGCP que vous avez configurée.

Nous utiliserons le scénario illustré par le diagramme ci-dessous pour expliquer la configuration du web :



**ETAPE 1 :** Choisissez **MGCP** dans le menu **VoIP** ; la configuration courante de la passerelle média est affichée.

**ETAPE 2 :** Sélectionnez les terminaux à modifier et cliquez sur **Update** ; "aaln/1" est le nom de terminal **FXS**.

The screenshot shows the MGCP Configuration web interface. The left sidebar contains navigation links: Status, Change Password, Link Status, WAN Setup, LAN Setup, WLAN Setup, Routing Setup, Save & Reboot, Erase & Reboot, VOIP, MGCP, Advanced, and ADSL Mode. The main content area displays the MGCP Configuration page with the following tables:

**Gateway & RTP**

Domain Name	Gateway		RTP	
	Port	Interface	Port Maximum	Port Minimum
[ppp0-IP]	2427	(ppp0) not ready	6000	5000

**Endpoints**

Select	Endpoint	CallAgent Address	Codecs	Status
C	aaln/1	192.168.10.254:2427	G729:PCMA:PCMA:PCMU:PCMU	Up

Buttons: Update, VoiceOption

**ETAPE 3 :** Entrez les informations de passerelle MGCP et de gestionnaire d'appel correspondant à votre fournisseur d'accès. Les champs sont expliqués ci-dessous.

MGCP Configuration				
<b>Gateway &amp; RTP</b>				
Gateway			RTP	
Domain Name	Port	Interface	Port Maximum	Port Minimum
[ppp0-IP]	2427	(ppp0) not ready	6000	5000
<b>Endpoints</b>				
Select	Endpoint	CallAgent Address	Codecs	Status
<input type="radio"/>	aaln/1	192.168.10.254:2427	G729:PCMA:PCMA:PCMU:PCMU	Up
			<input type="button" value="Update"/>	<input type="button" value="VoiceOption"/>

- **Gateway**

**Domain Name :** nom de domaine de la passerelle, par exemple "mta1".

**Port Number :** Numéro de port de la passerelle pour le contrôle de signal d'appel MGCP, par exemple "2427".

**Interface Name :** Interface de liaison de la passerelle pour le contrôle de signal d'appel MGCP, par exemple "ppp0" pour PPPoE ou PPPoA, "atm0" pour RFC1483 routé et "mer0" pour encapsulation MER.

Exemple :

```

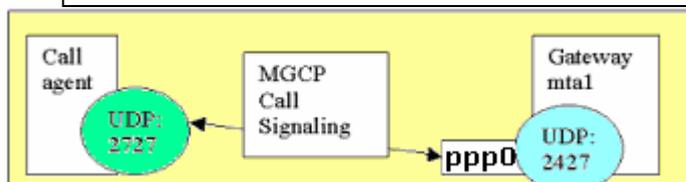
RQNT 1201 aaln/1@mta1 MGCP 1.0

N: ca@ca1.whatever.net:5678

X: 0123456789AC

R: l/hd(N)

```



- **RTP**

**Numéro de port (Min)** : Plage inférieure du pool RTP

**Numéro de port (Max)** : Plage supérieure du pool RTP

- **CallAgent**

**Nom de domaine/Numéro de port** : Type de nom de domaine et numéro de port du gestionnaire d'appel

**Adresse IP/Numéro de port** : Type d'adresse IP et numéro de port du gestionnaire d'appel

**Remarque 1:** Vous pouvez attribuer le gestionnaire d'appel comme adresse IP ou type de nom de domaine. Si vous choisissez le type d'adresse IP, à chaque redémarrage de la machine, la passerelle envoie un RSIP à cette adresse IP. Si vous choisissez le type de nom de domaine, à chaque redémarrage de la machine, la passerelle recherche un DNS jusqu'à ce qu'elle reçoive une translation d'adresse IP valable du serveur DNS, puis envoie un RSIP à cette adresse IP.

**Remarque 2:** Si vous avez choisi le type de nom de domaine, le champ d'adresse IP affiche automatiquement le résultat de recherche du DNS.

- **Terminal**

**Nom de terminal** : Nom de terminal du port de téléphone dans la configuration, par exemple "aaln/1" pour le port **PHONE1**.

**Status:** Paramètre d'état du terminal.

**UP** : Si vous choisissez « UP », la passerelle envoie un RSIP \*@[nom de passerelle] avec la méthode « Redémarrage » au gestionnaire d'appel pour ce terminal.

**DOWN** : Si vous choisissez « DOWN », la passerelle envoie un RSIP \*@[nom de passerelle] avec la méthode « Normale » au gestionnaire d'appel pour ce terminal.

**Types de charge** : Liste de Codec associée au terminal

**ETAPE 4 :** Cliquez sur le bouton **Apply** pour actualiser la configuration.

## Chapter 5 Configuration de base

Depuis le menu **Basic**, vous pouvez paramétrer une liste d'utilisateurs, configurer les interfaces WAN/LAN, définir le routage, enregistrer les paramètres, redémarrer l'appareil et récupérer les paramètres d'usine par défaut.

### 5.1 Informations relatives à la version

Pour vérifier la version du logiciel de votre routeur, depuis la barre de menu **Basic**, cliquez sur **Version Information**. Les informations sont affichées comme dans la copie d'écran ci-dessous.



### 5.2 Etat Internet&VoIP

Pour afficher l'état Internet et VoIP, cliquez sur le bouton **Internet&VoIPStatus**.

Basic

- Version Information
- Internet&VoIP Status**
- Change Password
- Link Status
- WAN Setup
- LAN Setup
- WLAN Setup
- Routing Setup
- Save & Reboot
- Erase & Reboot

VOIP

MGCP

Advanced

- ADSL Mode
- DHCP
- Firewall
- Configure
- IGMP Proxy

### Internet&VoIP Status

ADSL Status	UNTRAINED
ADSL Rate Status	DOWN: 0Kbps UP:0Kbps
Internet Check Type	Interface(ppp0) Status
Internet Check Status	DOWN PPP status:
VoIP Action Type	MGCP CA Lost
VoIP Action Status	Checking
USB Status	NO CABLE

### Internet&VoIP Configuration

ADSL Mode	ANSI1.413
Internet Connection Type	8/35/LLC PPPoE
Internet Connection Account	user
USB Information	Device IP:192.168.2.1 DHCP Server Start
VoIP EndPoint Name	[ppp0-IP]

## 5.3 Changement de mot de passe

Basic

- Version Information
- Internet&VoIP Status
- Change Password**
- Link Status
- WAN Setup
- LAN Setup
- WLAN Setup
- Routing Setup
- Save & Reboot
- Erase & Reboot

Advanced

- ADSL Mode
- DHCP
- Firewall
- Configure
- IGMP Proxy

### Password Configuration

Old Password:

New Password:

Confirm Password:

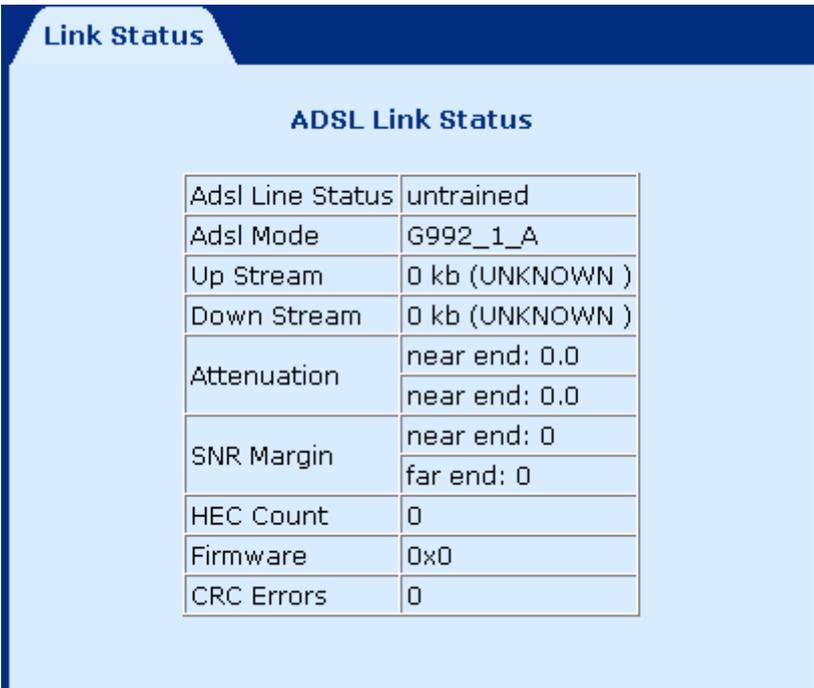
Apply Cancel

Pour modifier le mot de passe, cliquez sur **Change Password** dans la barre de menu. Tapez l'ancien mot de passe, puis le nouveau à deux reprises. Cliquez sur **Apply** pour envoyer les paramètres.

Si vous changez le mot de passe, ne manquez pas de le conserver en lieu sûr, car il sera nécessaire pour la prochaine connexion.

## 5.4 Etat de la liaison ADSL

Pour afficher l'état de la liaison ADSL, cliquez sur **Link Status** dans la barre d'outils. La page comporte les informations suivantes :



The screenshot shows a window titled 'Link Status' with a sub-header 'ADSL Link Status'. Below the header is a table with the following data:

Adsl Line Status	untrained
Adsl Mode	G992_1_A
Up Stream	0 kb (UNKNOWN )
Down Stream	0 kb (UNKNOWN )
Attenuation	near end: 0.0
	near end: 0.0
SNR Margin	near end: 0
	far end: 0
HEC Count	0
Firmware	0x0
CRC Errors	0

ADSL Line Status	Affiche l'état actuel de la ligne ADSL
Mode ADSL	Affiche la norme ADSL actuellement configurée. Les normes sont les suivantes : MULTI, G992_1_A, G992_1_B, G992_1_C, G992_2_C, G992_3_A, G992_3_B, G992_3_I, G992_3_J, G992_3_L, G992_5_A
Up Stream	Débit de données en amont négocié par la liaison DSL (Ko/s)
Down Stream	Débit de données en aval négocié par la liaison DSL (Ko/s)
Attenuation	Atténuation actuelle (dB) de l'extrémité proche et lointaine.
SNR Margin	Marge SNR actuelle (dB)
HEC Count	Nombre de cellules ATM reçues avec des erreurs depuis le début de la liaison.
Firmware	Numéro de version du microprogramme
CRC Errors	Nombre d'erreurs par seconde depuis vérification

## 5.5 Configuration du WAN

Cliquez sur WAN Setup dans la barre d'outils et configurez l'interface WAN pour ces services : RFC1483 Bridged, RFC1483 Routed, PPPoE, PPPoA et MER. Les paramètres habituels de ces services sont indiqués ci-après.

- VPI et VCI : Entrez une valeur pour les paramètres VPI et VCI. La plage VPI se situe entre 0 et 255, et entre 33 et 65535 pour le VCI.
- Encapsulation LLC : Avec l'encapsulation LLC, un en-tête de contrôle de liaison est ajouté au paquet Ethernet qui identifie le type de protocole (Ethernet). Ainsi, plusieurs protocoles peuvent être transmis par le circuit virtuel ATM.
- Multiplexage VC : Avec le multiplexage VC, aucun en-tête de contrôle de liaison n'est nécessaire, car le circuit virtuel ATM est considéré comme porteur d'un protocole unique.
- Activation NAPT : La NAPT (Translation d'adresse réseau), permet la translation d'adresses privées et publiques. Cette fonction est disponible pour les services RFC1483 Bridged, RFC1483 Routed, PPPoE, PPPoA et MER. Elle est automatiquement activée pour les services PPPoE et PPPoA.

WAN Setup

WAN Setup

VPI :  VCI :   LLC/SNAP  Vc Multiplexing  Enable NAPT

**RFC1483 Bridged**

**RFC1483 Routed** WAN IP Address:  WAN Subnet Mask:

**PPPoE** User Name:  Password:   
 Mode :  Idle Timeout( min ) :   
 Authentication:  Enable DHCP Server:

**PPPoA (NAT Enabled)** User Name:  Password:   
 Authentication:

**MER** Enable DHCP Client:   
 IP Address:  Subnet Mask:

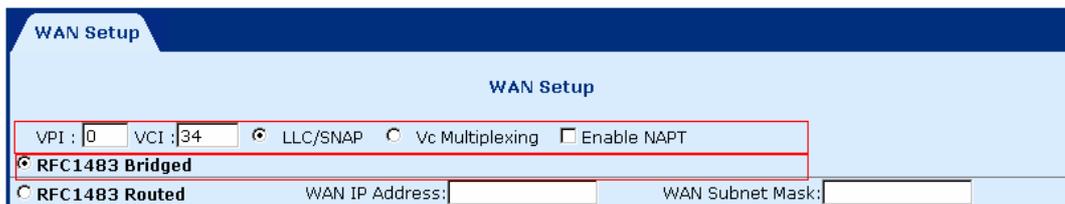
Manual Mode:  Manual Mode Trigger:

Current ATM PVC List													
Select	Mode	VPI	VCI	Encap	NAPT	IP Address	Subnet Mask	User Name	Authentication	Protocol	Idle Timeout	PPP Mode	Status
<input checked="" type="radio"/>	PPPoE	8	35	LLC	on	none	none	user	CHAP		30	direct	inactive

### 5.5.1 RFC 1483 Bridged

Avec la méthode de pontage RFC 1483, les cadres Ethernet sont "pontés" sur les circuits virtuels ATM. Les cadres Ethernet sont encapsulés soit par encapsulation LLC, soit par multiplexage VC. Avec l'encapsulation LLC, un en-tête de contrôle de liaison est ajouté au paquet Ethernet qui identifie le type de protocole (Ethernet). Ainsi, plusieurs protocoles peuvent être transmis par le circuit virtuel ATM. Avec le multiplexage VC, aucun en-tête de contrôle de liaison n'est nécessaire, car le circuit virtuel ATM est considéré comme porteur d'un protocole unique. Les paquets Ethernet étant pontés, la seule responsabilité de l'IAD consiste à transmettre les paquets Ethernet entre le fournisseur d'accès Internet et le réseau local. Les adresses IP du réseau local sont attribuées par l'ISP, de façon statique ou dynamique.

Pour paramétrer le service RFC 1483 Bridged, configurez les champs communs en haut de la page et cliquez sur le bouton Add pour ajouter la saisie.



Dans l'exemple ci-dessus, nous avons ajouté une nouvelle PVC, VPI:0/VCI: 34, pour le mode RFC1483 Bridged.

#### MODIFICATION D'UNE ENTREE

Observez les étapes suivantes pour modifier une entrée :

**ETAPE 1** : Sélectionnez la valeur dans la liste **Current ATM PVC**, en bas de la page de configuration WAN. Les valeurs actuelles de l'entrée sélectionnée sont affichées dans la partie supérieure de la page.

**ETAPE 2** : Changez les paramètres

**ETAPE 3** : Cliquez sur **Modify**.

#### SUPPRESSION D'UNE ENTREE

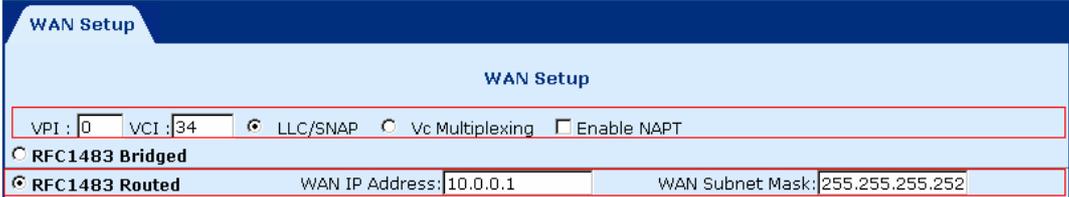
Pour supprimer une entrée, sélectionnez-la dans la liste **Current ATM PVC**, en

bas de la page de configuration WAN, et cliquez sur le bouton **Delete**.

## 5.5.2 RFC 1483 Routed

### AJOUT D'UNE ENTREE

Pour paramétrer le service RFC 1483 Routed, configurez les paramètres communs en haut de la page, cliquez sur RFC 1483 Routed et configurez les paramètres spécifiques (adresse IP du WAN et masque de sous-réseau WAN). Cliquez sur le bouton Add pour ajouter l'entrée.



The screenshot shows the 'WAN Setup' configuration page. At the top, there are fields for 'VPI : 0' and 'VCI : 34'. Below these are radio buttons for 'LLC/SNAP' (selected), 'Vc Multiplexing', and 'Enable NAPT'. A list of modes is shown: 'RFC1483 Bridged' and 'RFC1483 Routed' (selected). Below the selected mode, there are fields for 'WAN IP Address: 10.0.0.1' and 'WAN Subnet Mask: 255.255.255.252'.

Dans l'exemple ci-dessus, nous avons ajouté une nouvelle PVC, VPI:0/VCI:34, pour le mode RFC1483 Routed.

### MODIFICATION D'UNE ENTREE

Observez les étapes suivantes pour modifier une entrée :

**ETAPE 1** : Sélectionnez la valeur dans la liste **Current ATM PVC**, en bas de la page de configuration WAN. Les valeurs actuelles de l'entrée sélectionnée sont affichées dans la partie supérieure de la page.

**ETAPE 2** : Changez les paramètres

**ETAPE 3** : Cliquez sur **Modify**.

### SUPPRESSION D'UNE ENTREE

Pour supprimer une entrée, sélectionnez-la dans la liste **Current ATM PVC**, en bas de la page de configuration WAN, et cliquez sur le bouton **Delete**.

### 5.5.3 PPPoE

Le service PPPoE offre l'authentification de session en utilisant un protocole d'authentification par mot de passe (PAP) ou un protocole d'authentification par défi-réponse CHAP (Challenge Handshake Authentication Protocol). Le comptage de session est possible et la bande passante peut être conservée en fermant les sessions inutilisées. En utilisant le service PPP – les paramètres de liaison et de réseau sont facilement négociés entre l'IAD/Routeur et l'ISP.

Lorsqu'un service PPPoE est utilisé, une adresse IP est attribuée au système par le fournisseur d'accès Internet dans le processus d'établissement de la connexion réseau. Le système peut être configuré comme serveur DHCP pour LAN et le NAT peut servir à la translation d'adresses privées en adresses publiques. De cette façon, les ordinateurs du LAN n'ont pas besoin d'adresses IP publiques individuelles.

The screenshot shows the 'WAN Setup' configuration page. At the top, there are fields for 'VPI : 0' and 'VCI : 34', and checkboxes for 'LLC/SNAP', 'Vc Multiplexing', and 'Enable NAPT'. Below this, there are three radio button options: 'RFC1483 Bridged', 'RFC1483 Routed', and 'PPPoE'. The 'PPPoE' option is selected. Under 'PPPoE', there are fields for 'User Name: adstest', 'Password: \*\*\*\*', 'Mode: direct', 'Idle Timeout( min ) : 0', 'Authentication: both', and 'Enable DHCP Server: [checked]'. A red box highlights the VPI/VCI fields and the PPPoE configuration section.

Dans l'exemple ci-dessus, nous avons ajouté une nouvelle PVC, VPI:0/VCI: 34, pour le mode PPPoE.

## AJOUT D'UNE ENTREE

Pour paramétrer le service PPPoE, cliquez sur PPPoE, configurez les champs communs en haut de la page ainsi que les champs ci-après. En bas de l'écran, cliquez sur le bouton **Add** pour ajouter l'entrée. En outre, si le mode PPPoE est réglé sur **auto**, cliquer sur le bouton **Enable** du MODE MANUEL désactive en effet le mode auto et exige que l'utilisateur reconnecte une session PPPoE terminée en cliquant sur le bouton **Trigger** du MODE MANUEL. Par la suite, pour revenir en mode Auto, cliquez sur le bouton **Disable** du MODE MANUEL, qui est affiché à la place du bouton **Enable** du mode manuel.

- **User name/Password:** utilisé pour la connexion des clients distants pendant la numérotation.
- **Mode** Direct et Auto. Si le mode est réglé sur AUTO, la négociation PPPoE commence automatiquement lorsque le système identifie du trafic à transférer sur la liaison. Le réglage par défaut est DIRECT.
- **Idle Timeout:** détermine la période d'attente (en minutes) à l'issue de laquelle la liaison PPPoE est interrompue. Elle est valable pour le mode Auto.
- **Authentication:** Définit le code d'authentification : PAP, CHAP ou BOTH. Si le code d'authentification est réglé sur BOTH, le routeur suit les paramètres d'authentification (PAP, CHAP) du DSLAM distant.
- **Enable DHCP Server:** active le serveur DHCP. Ce champ est automatiquement coché lorsque le mode PPPoE est sélectionné. Désactivez le champ pour désactiver le serveur DHCP. Le serveur DHCP attribue dynamiquement les adresses réseau et transmet les paramètres de configuration aux hôtes.

## MODIFICATION D'UNE ENTREE

Observez les étapes suivantes pour modifier une entrée :

**ETAPE 1 :** Sélectionnez la valeur dans la liste **Current ATM PVC**, en bas de la page de configuration WAN. Les valeurs actuelles de l'entrée sélectionnée sont affichées dans la partie supérieure de la page.

**ETAPE 2** : Changez les paramètres

**ETAPE 3** : Cliquez sur **Modify**.

### **SUPPRESSION D'UNE ENTREE**

Pour supprimer une entrée, sélectionnez-la dans la liste **Current ATM PVC**, en bas de la page de configuration WAN, et cliquez sur le bouton **Delete**.

## 5.5.4 PPPoA

Pour paramétrer le mode PPPoA, cliquez sur **PPPoA**; configurez les champs communs ainsi que les champs ci-après. Cliquez sur le bouton Add pour ajouter l'entrée.

- **User name** et **Password**: utilisé pour la connexion des clients distants lors de la numérotation. Le mode PPPoA est activé manuellement en entrant des commandes de démarrage depuis la page : Advanced>Configure PPPoA.
- **Authentication**: Définit le code d'authentification : PAP, CHAP ou BOTH. Si le code d'authentification est réglé sur BOTH, le routeur suit les paramètres d'authentification (PAP, CHAP) du B-RAS distant.

The screenshot shows the 'WAN Setup' configuration page. At the top, there are fields for VPI (0) and VCI (34), and radio buttons for LLC/SNAP (selected), Vc Multiplexing, and Enable NAPT. Below this, there are three main configuration sections: RFC1483 Bridged, RFC1483 Routed, and PPPoE. The PPPoE section is expanded, showing fields for User Name, Password, Mode (direct), Idle Timeout (min), Authentication (both), and Enable DHCP Server. The PPPoA (NAT Enabled) section is also expanded, showing fields for User Name (adsltest), Password (\*\*\*\*), and Authentication (both). A red box highlights the VPI/VCI fields and the PPPoA (NAT Enabled) section.

Dans l'exemple ci-dessus, nous avons ajouté une nouvelle PVC, VPI:0/VCI:34, pour le mode PPPoA.

### AJOUT D'UNE ENTREE

Pour paramétrer le mode PPPoA, cliquez sur PPPoA; configurez les champs communs ainsi que les champs ci-après. Cliquez sur le bouton Add pour ajouter l'entrée.

- **User name** et **Password**: utilisé pour la connexion des clients distants lors de la numérotation. Le mode PPPoA est activé manuellement en entrant des commandes de démarrage depuis la page : Advanced>Configure PPPoA.

**Authentication**: Définit le code d'authentification : PAP, CHAP ou BOTH. Si le code d'authentification est réglé sur BOTH, le routeur suit les paramètres d'authentification (PAP, CHAP) du DSLAM distant. MER

Le mode MAC Encapsulation Routing (MER) permet à l'IAD d'acheminer des adresses IP sur la liaison RFC1483 bridged. La fonction NAPT est supportée pour permettre à plusieurs adresses IP privées sur le LAN de partager une adresse IP publique.

### 5.5.5 MER

Le mode MAC Encapsulation Routing (MER) permet à l'IAD d'acheminer des adresses IP sur la liaison RFC1483 bridged. La fonction NAPT est supportée pour permettre à plusieurs adresses IP privées sur le LAN de partager une adresse IP publique.

The screenshot shows the 'WAN Setup' configuration page. At the top, there are input fields for 'VPI : 0' and 'VCI : 34', and radio buttons for 'LLC/SNAP' (selected), 'Vc Multiplexing', and 'Enable NAPT'. Below this, several radio buttons are listed: 'RFC1483 Bridged', 'RFC1483 Routed', 'PPPoE', 'PPPoA (NAT Enabled)', and 'MER' (selected). The 'MER' section is highlighted with a red border and contains the following fields: 'Enable DHCP Client:' with a checked checkbox, 'IP Address:', and 'Subnet Mask:'.

Dans l'exemple ci-dessus, nous avons ajouté une nouvelle PVC, VPI:0/VCI: 34, pour le mode MER. L'adresse IP est attribuée par l'intermédiaire du protocole DHCP.

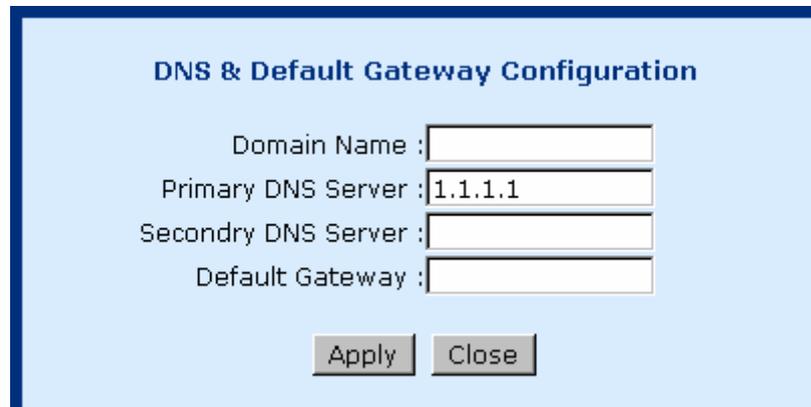
**Pour paramétrer le service MER**, configurez les champs communs puis entrez l'adresse IP et le masque de sous-réseau dans la section MER de l'écran. Cliquez sur le bouton Add pour ajouter l'entrée.

Une fois l'entrée MER paramétrée, configurez la passerelle par défaut en cliquant sur le bouton Routing Setup dans le menu Basic. L'adresse IP de la passerelle par défaut (Next Hop IP) doit être communiquée par votre fournisseur d'accès. Des détails supplémentaires sont fournis ci-après :

**ETAPE 1** : Cliquez sur **Configure** dans la barre de menu Advanced.

**ETAPE 2** : Cliquez sur **DNS and Default G/W** en bas de la page de configuration.

**ETAPE 3** : Complétez les champs expliqués ci-dessous.



**DNS & Default Gateway Configuration**

Domain Name :

Primary DNS Server :

Secondary DNS Server :

Default Gateway :

- **Domain Name** : Défini par l'utilisateur
- **Primary DNS server** : Entrez l'adresse IP du serveur principal.
- **Secondary DNS server** : Entrez l'adresse IP du serveur secondaire utilisé en cas d'indisponibilité ou de défaillance de l'adresse IP du serveur principal
- **Default Gateway** : Adresse IP de la passerelle pour le réseau IP

**ETAPE 4** : Cliquez sur **Apply** pour envoyer les paramètres.

Observez les étapes suivantes pour **modifier une entrée** :

**ETAPE 1** : Sélectionnez la valeur dans la liste **Current ATM PVC**, en bas de la page de configuration WAN. Les valeurs actuelles de l'entrée sélectionnée sont affichées dans la partie supérieure de la page.

**ETAPE 2** : Changez les paramètres

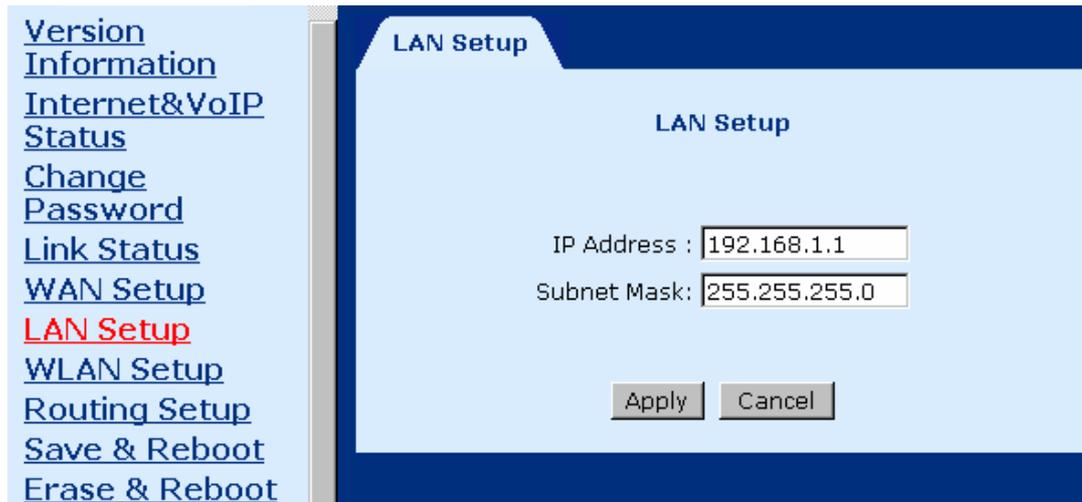
**ETAPE 3** : Cliquez sur **Modify**.

**Pour supprimer une entrée**, sélectionnez-la dans la liste **Current ATM PVC**, en bas de la page de configuration WAN, et cliquez sur le bouton **Delete**.



## 5.6 Configuration du LAN

L'adresse IP par défaut du LAN est 192.168.1.1. Cliquez sur **LAN Setup** dans la barre de menu pour configurer l'adresse IP du LAN. Tapez **l'adresse IP du LAN** et le **masque de sous-réseau**. Cliquez sur **Apply** pour envoyer les paramètres. Lors de l'application de la nouvelle adresse IP, la configuration web est interrompue. Utilisez la nouvelle adresse IP pour vous connecter.



The screenshot shows a web interface for LAN configuration. On the left is a vertical menu with the following items: [Version Information](#), [Internet&VoIP Status](#), [Change Password](#), [Link Status](#), [WAN Setup](#), [LAN Setup](#) (highlighted in red), [WLAN Setup](#), [Routing Setup](#), [Save & Reboot](#), and [Erase & Reboot](#). The main content area is titled 'LAN Setup' and contains two input fields: 'IP Address : 192.168.1.1' and 'Subnet Mask: 255.255.255.0'. Below these fields are two buttons: 'Apply' and 'Cancel'.

## 5.7 Configuration du WLAN

Les paramètres spécifiques des fonctions sans fil de votre routeur sont accessibles depuis l'option **WLAN Setup** de la barre de menu Basic. Le menu est divisé en plusieurs sous-menus : WLAN Basic, WLAN Advanced, WLAN WEP, WLAN Filter et WLAN Radio. Chacun de ces menus est examiné plus loin.

### 5.7.1 Paramètres WLAN de base

Pour accéder aux paramètres WLAN de base, cliquez sur l'onglet **WLAN Basic** dans l'écran **WLAN Settings**. Le menu des paramètres de WLAN de base contient les paramètres indiqués ci-dessous. Après chaque modification de paramètre, cliquez sur le bouton **Apply** pour actualiser les paramètres ou sur le bouton **Restore** pour conserver les paramètres d'origine.

IP Address	Entrez l' <b>adresse IP</b> de l'interface WLAN
Subnet Mask	Entrez un <b>masque de sous-réseau</b> pour l'interface WLAN
SSID	La SSID doit correspondre à vos adaptateurs client. La SSID (Service Set ID) permet l'identification exclusive de votre point d'accès dans l'environnement radio.
Channel	Le canal doit correspondre à vos adaptateurs client. Le numéro de canal Direct Sequence Spread Spectrum (DSSS) est un identifiant pour la fréquence sur laquelle votre connectivité WLAN est activée sur le réseau WLAN. Bien que la plage configurable de numéro de canal DSSS se situe entre 1 et 14, des restrictions s'appliquent en fonction du pays où le routeur ADSL sans fil est utilisé - <b>FCC</b> : canaux 1 à 11; <b>ETSI</b> : canaux 1 à 13; <b>ETSI</b> :

### 5.7.2 Fonction WLAN avancées

Pour accéder aux paramètres WLAN avancés, cliquez sur l'onglet **WLAN Advance** dans l'écran **WLAN Settings**. Le menu des paramètres WLAN avancés contient les paramètres indiqués ci-dessous. Après chaque modification de paramètre, cliquez sur le bouton **Apply** pour actualiser les paramètres ou sur le bouton **Restore** pour conserver les paramètres d'origine.

Beacon Interval	Indiquez la valeur d'intervalle de balise. Entrez une valeur entre 1 et 1000. La valeur représente le délai d'envoi en nanosecondes des paquets balisés par un point d'accès pour synchroniser un réseau sans fil.
RTS Threshold	Cette valeur doit normalement conserver son réglage par défaut de 2,432. En cas de débit de données irrégulier, seules des modifications mineures sont recommandées. La valeur doit correspondre à vos adaptateurs client.
Fragmentation	Ce champ sert à indiquer le seuil de fragmentation. Entrez une valeur entre 256 et 2346. En cas de taux élevé d'erreur de paquet, essayez d'augmenter légèrement le seuil de fragmentation. La valeur doit normalement conserver son réglage par défaut de 2,346. Elle doit correspondre aux adaptateurs client.
Preamble Type	<b>long, short</b> . Doit correspondre aux adaptateurs client. Short permet un débit plus élevé, mais n'est utilisable que lorsque tous les éléments du réseau sont conformes à la norme IEEE 802.11b.
Preamble Type	<b>Open System</b> [sans sécurité pendant le processus d'authentification], <b>Shared Key</b> [utilise l'encryptage WEP pendant le processus d'authentification].
Tx Rates	Le taux de transfert du routeur doit être égal ou supérieur à celui des clients ; les options sont : 1-2-5-11 (Mbps).

AP Visible	Lorsque cette option est sur <b>ON</b> l'AP peut être détecté par les clients sans fil, ce qui n'est pas possible lorsqu'elle est sur <b>Off</b> .
------------	--

**Wireless LAN Advance Setup**

Beacon Interval : 100

RTS Threshold : 2347

Fragmentation : 2346

Preamble Type : Long

Auth. Type : Open System

Tx Rate : Auto

AP Visible  ON  OFF

Apply Cancel

### 5.7.3 Paramètres WEP WLAN

Pour accéder aux paramètres WEP WLAN, cliquez sur l'onglet **WLAN WEP** dans l'écran **WLAN Settings**. Cet écran sert à paramétrer la sécurité WEP. La sécurité WEP utilise un mot clé d'encryptage sur toutes les données transmises et reçues. Les paramètres sont décrits ci-dessous. Après chaque modification de paramètre, cliquez sur le bouton **Apply** pour actualiser les paramètres ou sur le bouton **Restore** pour conserver les paramètres d'origine.

**Wireless LAN WEP Setup**

EncrypType : WEP

Key Select : KEY 1

KEY 1 : 12345abc678

KEY 2 :

KEY 3 :

KEY 4 :

Apply Cancel

Encryp Type	Sélectionnez la méthode de vérification de sécurité WLAN.
Key Select	Si vous utilisez la génération manuelle de clé, choisissez un numéro de clé entre 0~4, et tapez le mot de passe d'accès dans le champ choisi.
Key 0~4	Le mot de passe d'accès peut être un code chaîne hexadécimal ou ASCII, qui dépend du format de clé choisi ci-dessus. Vous pouvez configurer les mots de passe des quatre clés (0-4), mais seule la clé choisie prend effet. Le mot de passe est nécessaire sur tous les clients sans fil que vous souhaitez connecter à votre point d'accès.

## 5.8 Routage

Cliquez sur **Routing Setup** dans la barre de menu pour configurer les fonctions de routage. Ces fonctions comprennent le RIP et le routage statique. Vous pouvez afficher les informations RIP en cliquant sur le bouton **RIP information**. Pour changer les routes de base configurées, vous devez commencer par sélectionner l'entrée concernée pour modifier/supprimer la configuration courante.

The screenshot shows a web interface for configuring routing. On the left is a sidebar with a 'Basic' tab selected, containing links for Version Information, Internet&VoIP Status, Change Password, Link Status, WAN Setup, LAN Setup, WLAN Setup, **Routing Setup**, Save & Reboot, and Erase & Reboot. Below this are 'VOIP' and 'Advanced' tabs with links for MGCP, ADSL Mode, DHCP, Firewall, Configure, IGMP Proxy, and Bridging.

The main content area has a 'Routing' tab selected. It contains the following sections:

- Routing Setup:** Fields for Destination Network Address, Destination Subnet Mask, Next Hop IP (radio button), and Next Interface (dropdown menu set to 'atm0'). Buttons for Add, Modify, and Delete are below.
- List of Static Routes:** A table with columns: Select, Network Address, Subnet Mask, Next Hop IP, and Flag.
- Rip Information:** Fields for Rip Status (dropdown set to 'off'), Version (dropdown set to 'version 1'), and Silent (dropdown set to 'disable'). An Apply button is below.

Select	Network Address	Subnet Mask	Next Hop IP	Flag
<input type="radio"/>	10.0.0.0	255.255.255.252	10.0.0.1	C
<input type="radio"/>	192.168.1.0	255.255.255.0	192.168.1.1	C
<input type="radio"/>	192.168.2.0	255.255.255.0	192.168.2.1	C
<input type="radio"/>	192.168.101.0	255.255.255.0	192.168.101.1	C

## 5.8.1 Activation RIP

Observez les étapes suivantes pour activer le RIP :

**ETAPE 1 :** Cliquez sur **Routing Setup** dans la barre de menu.

**Rip Information**

Rip Status :  Version :  Silent:

**ETAPE 2 :** Configurez les champs suivants :

- **Rip Status:** Pour activer le Rip, sélectionnez **on** ; et **off** pour le désactiver.
- **Version:** Version 1, Version 2
- **Silent:** Pour utiliser le Rip silencieux, sélectionnez **Enable** ; et **Disable** pour le désactiver.

**ETAPE 3 :** Cliquez sur **Apply** pour envoyer les paramètres.

**ETAPE 5 :** Une fois les nouveaux paramètres Rip envoyés, la liste des routes statiques est actualisée en conséquence. Un écran similaire à celui-ci est affiché :

**List of Static Routes**

Select	Network Address	Subnet Mask	Next Hop IP	Flag
<input type="radio"/>	10.0.0.0	255.255.255.252	10.0.0.1	C
<input type="radio"/>	172.16.11.0	255.255.255.0	172.16.11.111	C
<input type="radio"/>	192.168.2.0	255.255.255.0	192.168.2.1	C
<input type="radio"/>	192.168.101.0	255.255.255.0	192.168.101.1	C

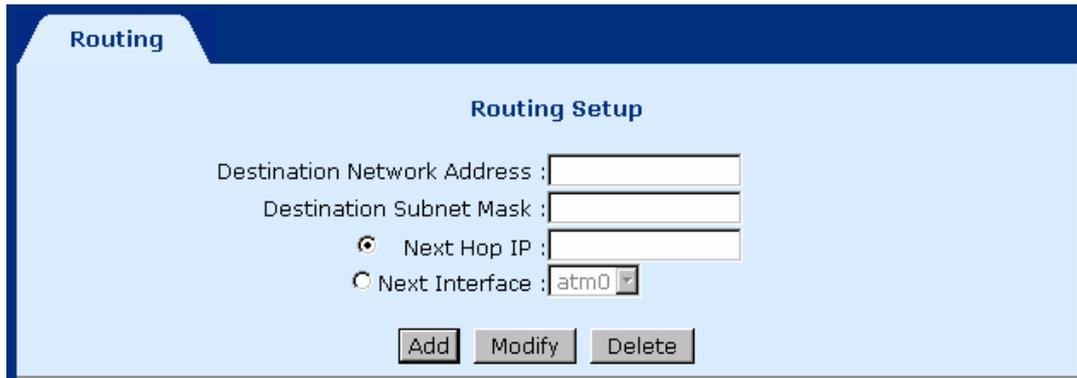
**Rip Information**

Rip Status :  Version :  Silent:

Flag: R = Route RIP, S = Route statique, C = Route de connexion

## 5.8.2 Configuration de route statique

Le champ Routes Configuration permet d'ajouter, de modifier et de supprimer une route statique. Complétez les champs Destination Network Address (ID du réseau de destination), Destination Subnet Mask et Next hop IP puis cliquez sur un bouton en dessous pour exécuter la fonction demandée. Il est possible d'ajouter un maximum de 20 routes statiques.



The screenshot shows a web interface for configuring static routes. At the top, there is a blue header with the word "Routing". Below it, the main content area is titled "Routing Setup". There are four input fields: "Destination Network Address", "Destination Subnet Mask", "Next Hop IP" (with a radio button selected), and "Next Interface" (with a dropdown menu showing "atm0"). Below the fields are three buttons: "Add", "Modify", and "Delete".

### Ajouter :

Observez les étapes suivantes pour ajouter une route statique :

**ETAPE 1 :** Cliquez sur Routing Setup dans la barre de menu.

**ETAPE 2 :** Entrez les paramètres des champs Destination Network ID, Subnet Mask, Next Hop IP et Next Interface (notez que vous devez choisir entre Next Hop IP et Next interface).

**ETAPE 3 :** Cliquez sur le bouton ADD.

### Modifier :

Observez les étapes suivantes pour modifier une route statique :

**ETAPE 1 :** Sélectionnez l'entrée à modifier dans la liste des routes statiques.

**ETAPE 2 :** Changez les paramètres

**ETAPE 3 :** Cliquez sur le bouton **Modifier**.

### Supprimer :

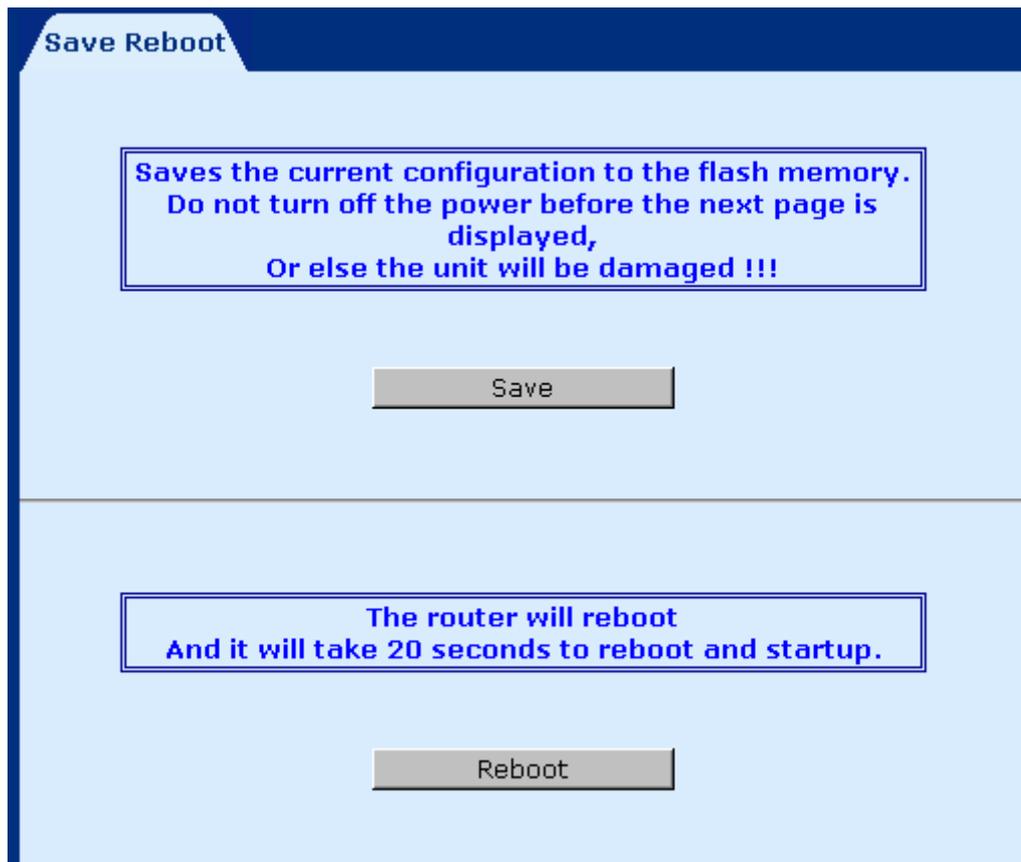
**ETAPE 1 :** Sélectionnez l'entrée à **supprimer** dans la liste des routes statiques.

**ETAPE 2 :** Changez les paramètres

**ETAPE 3** : Cliquez sur le bouton **Delete**.

## 5.9 Enregistrement

Pour enregistrer les paramètres sur Flash, cliquez sur **Save & Reboot** dans la barre de menu. Cliquez sur **Save** dans le volet principal.

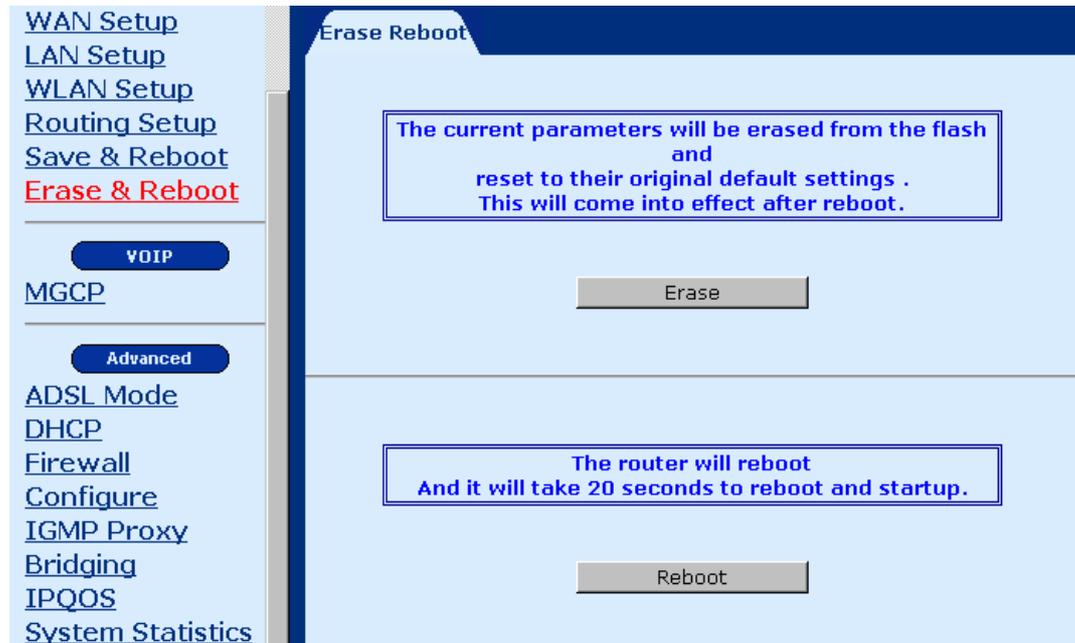


## 5.10 Redémarrer

Pour redémarrer le routeur, cliquez sur **Save & Reboot** dans la barre de menu. Cliquez sur **Reboot** dans le volet principal.

## 5.11 Récupération des paramètres par défaut

Pour récupérer les paramètres par défaut, cliquez sur **Erase & Reboot** dans la barre de menu. Cliquez sur **Erase** dans le volet principal. Cliquez ensuite sur **Reboot**.



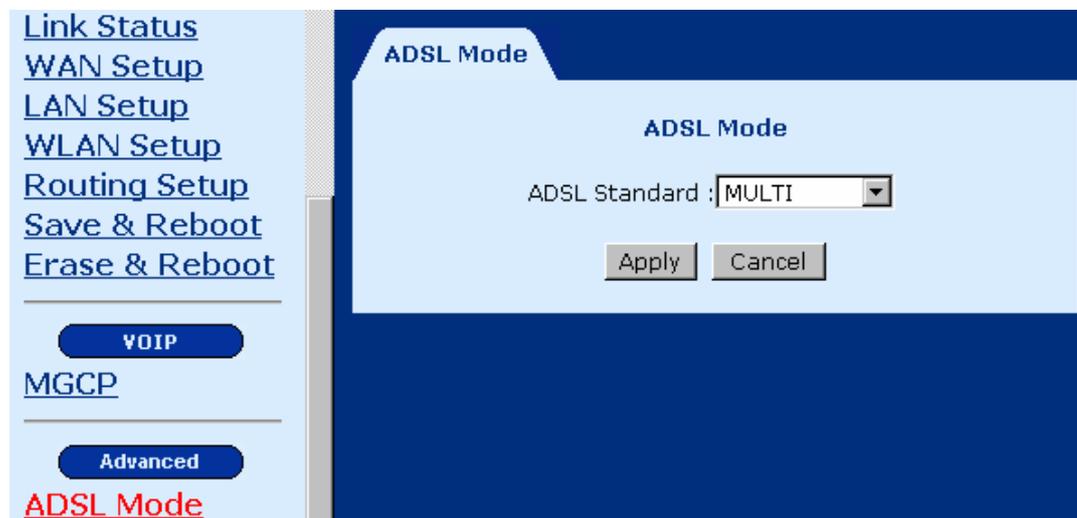
## Chapter 6 Configuration avancée

### 6.1 Mode ADSL

Cliquez sur le bouton **ADSL Mode** dans la barre de menu Advanced.

- Il existe onze normes ADSL, soit : MULTI, G992\_1\_A, G992\_1\_B, G992\_1\_C, G992\_2\_C, G992\_3\_A, G992\_3\_B, G992\_3\_I, G992\_3\_J, G992\_3\_L, G992\_5\_A. La norme par défaut est MULTI.

Une fois la norme ADSL sélectionnée, cliquez sur le bouton **Apply** pour envoyer les paramètres.



### 6.1.1 DHCP

Le protocole Dynamic Host Configuration Protocol (DHCP) offre une approche centralisée de l'attribution d'adresses IP. Il permet l'attribution dynamique des adresses IP selon les besoins, à partir d'un pool d'adresses.

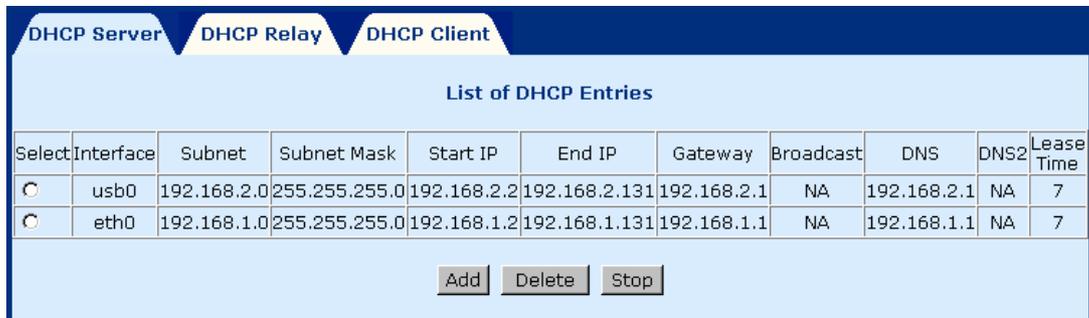
### 6.1.2 Serveur DHCP

Il existe deux entrées DHCP par défaut, constituées des paramètres ci-après :

Select	Interface	Subnet	Subnet Mask	Start IP	End IP	Gateway	Broadcast	DNS	DNS2	Lease Time
<input type="radio"/>	usb0	192.168.2.0	255.255.255.0	192.168.2.2	192.168.2.131	192.168.2.1	NA	192.168.2.1	NA	7
<input type="radio"/>	eth0	192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.131	192.168.1.1	NA	192.168.1.1	NA	7

### Activation du serveur DHCP

**ETAPE 1 :** Cliquez sur **DHCP** dans la barre de menu. Deux entrées DHCP par défaut sont présentes à l'écran. Les paramètres par défaut sont les suivants.



The screenshot shows a web interface for DHCP configuration. At the top, there are three tabs: "DHCP Server" (selected), "DHCP Relay", and "DHCP Client". Below the tabs is a section titled "List of DHCP Entries" containing a table with the same data as shown in the previous table. Below the table are three buttons: "Add", "Delete", and "Start".

**ETAPE 2 :** Pour activer l'entrée DHCP, choisissez-la et cliquez sur le bouton Start. Un bouton est affiché à l'écran comme suit.



## Ajouter un DHCP Server

Pour ajouter une entrée, cliquez sur le bouton Add et complétez les paramètres suivants. Cliquez sur **Apply** pour envoyer les paramètres.

The screenshot shows the 'DHCP Server Configuration' window. It features three tabs: 'DHCP Server', 'DHCP Relay', and 'DHCP Client'. The 'DHCP Server' tab is active. The configuration fields are as follows:

- Interface: eth0 (dropdown menu)
- Starting IP Address: (empty text box)
- End IP Address: (empty text box)
- Gateway: 172.16.11.111 (text box)
- Netmask: 255.255.255.0 (text box)
- DNS: (empty text box)
- DNS2: (empty text box)
- Lease Time (in Days): 7 (text box)

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Back'.

- **Interface: eth0/wlan0.** Ceci configure l'interface qui fournit la fonction DHCP. Par défaut en usine, l'entrée pour l'interface **eth0** est définie avec l'adresse de passerelle 192.168.1.1 et un masque de sous-réseau 255.255.255.0. Par défaut en usine, l'entrée pour l'interface **eth0** est définie avec l'adresse de passerelle 192.168.1.1 et le masque de sous-réseau 255.255.255.0.
- **Starting IP Address:** Première adresse IP du pool d'adresses dans le serveur DHCP. Notez que l'adresse IP doit se trouver dans le même sous-réseau que l'adresse IP LAN du routeur.
- **End IP Address:** Dernière adresse IP du pool d'adresses dans le serveur DHCP. Notez que l'adresse IP doit se trouver dans le même sous-réseau que l'adresse IP LAN du routeur.
- **Gateway:** Adresse IP de la passerelle
- **Netmask:** Masque de sous-réseau du réseau IP
- **DNS :** Adresse IP du serveur de nom de domaine
- **DNS2:** Deuxième adresse IP du serveur de nom de domaine
- **Lease Time (in Days):** Lors de la connexion, le poste de travail distant obtient une adresse IP. Ce champ détermine la durée pendant laquelle le

poste de travail peut utiliser cette adresse IP pour accéder à Internet.

### **Désactiver un serveur DHCP :**

Observez les étapes suivantes pour **arrêter** un serveur DHCP :

**ETAPE 1 :** Cliquez sur **DHCP** dans la barre de menu.

**ETAPE 2 :** Choisissez une entrée de DHCP et cliquez sur **Stop**.

### **Supprimer un serveur DHCP**

Observez les étapes suivantes pour **supprimer** un serveur DHCP :

**ETAPE 1 :** Cliquez sur **DHCP** dans la barre de menu.

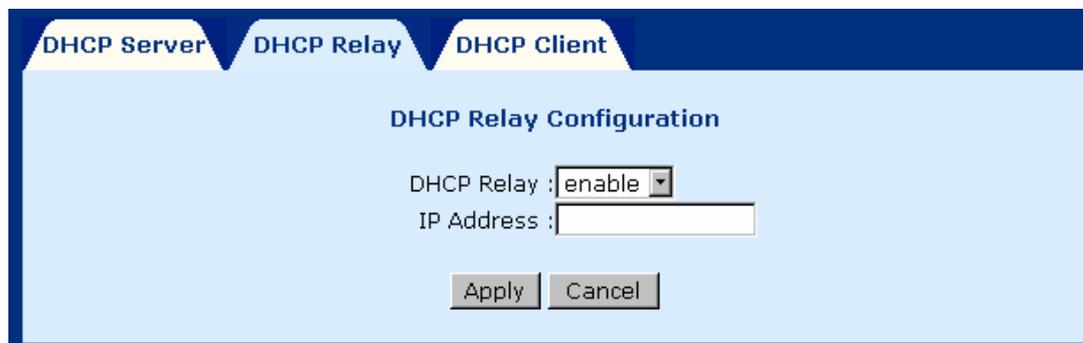
**ETAPE 2 :** Choisissez une entrée de DHCP et cliquez sur **Delete**.

### 6.1.3 Relais DHCP

Le format de paquet DHCP est basé sur un paquet BootP. Par conséquent, le DHCP utilise l'agent relais BootP pour transmettre les paquets DHCP. Cette organisation permet l'interopérabilité entre les clients BootP existants et les serveurs DHCP. L'agent relais BootP utilise les mêmes critères et méthodes pour transmettre les paquets DHCP et BootP. Le relais DHCP est désactivé par défaut.

Observez les étapes suivantes pour activer le relais BOOTP/DHCP :

**ETAPE 1 :** Accédez à l'écran du relais BOOTP/DHCP en cliquant sur **DHCP** dans le menu Advanced, puis sur l'onglet **DHCP Relay**.



The image shows a software configuration window titled "DHCP Relay Configuration". At the top, there are three tabs: "DHCP Server", "DHCP Relay" (which is the active tab), and "DHCP Client". The main area of the window contains two configuration fields: "DHCP Relay" with a dropdown menu currently showing "enable", and "IP Address" with an empty text input box. Below these fields are two buttons: "Apply" and "Cancel".

**ETAPE 2 :** Dans le champ DHCP Relay, choisissez **Enable** et entrez l'adresse IP à laquelle vous souhaitez recevoir les paquets BOOT REQUEST ou DHCP des clients.

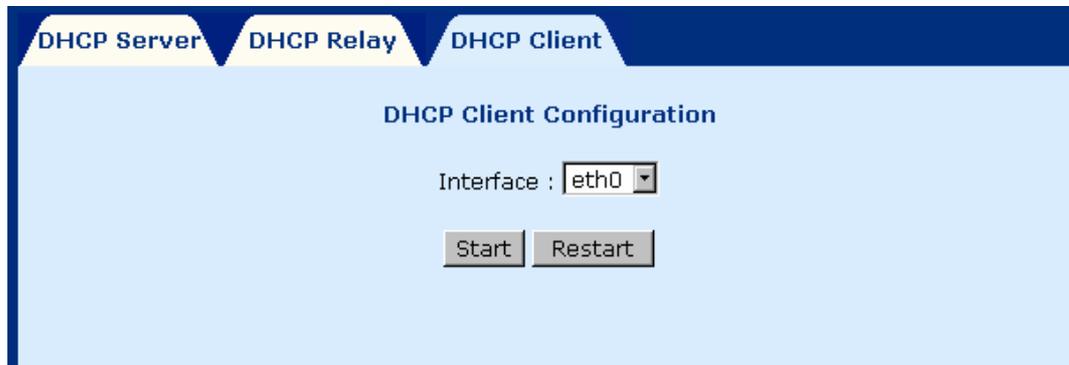
**ETAPE 3 :** Cliquez sur le bouton **Apply**.

## 6.1.4 Client DHCP

**Remarque :** Avant de lancer la fonction Client DHCP, l'utilisateur doit vérifier que le serveur DHCP est accessible ; si le routeur ADSL ne parvient pas à obtenir l'adresse IP du serveur DHCP, il doit être redémarré.

Le routeur peut aussi être configuré comme client DHCP. Dans ce cas, le routeur peut émettre une requête d'attribution d'une adresse IP, de masques de sous-réseau et de nom de domaine vers l'hôte DHCP. Pour configurer le routeur en mode client DHCP, sélectionnez l'**interface** à connecter à l'hôte DHCP et cliquez sur le bouton **Start**.

Le bouton Stop sert à arrêter le fonctionnement du routeur en mode DHCP et le bouton Restart à obtenir que le routeur renvoie une requête à l'hôte DHCP pour l'attribution d'une adresse IP, d'un masque de sous-réseau et d'un nom de domaine.



The image shows a web-based configuration interface for a DHCP Client. At the top, there are three tabs: "DHCP Server", "DHCP Relay", and "DHCP Client", with "DHCP Client" being the active tab. Below the tabs, the title "DHCP Client Configuration" is centered. Underneath the title, there is a label "Interface :" followed by a dropdown menu showing "eth0". Below the dropdown menu, there are two buttons: "Start" and "Restart".

## 6.2 Pare-feu

Pour vérifier que toutes les communications au sein du réseau sont légitimes, un filtrage par connexion est effectué par le module de pare-feu complet. Toute tentative de connexion entrant ou sortant du réseau est contrôlée et n'est autorisée que si elle correspond aux normes de l'entreprise.

### 6.2.1 Politiques

L'onglet Politiques configure les politiques du pare-feu avec les paramètres indiqués et les insère dans la table des politiques. Une politique est rattachée à une paire d'interfaces (Rx\_Interface, Tx\_Interface), et signifie qu'elle est applicable aux paquets reçus sur Rx\_Interface et transmis sur Tx\_Interface.

Les politiques sont classées par ordre de priorité relative. La priorité relative n'est autre que l'indication d'une position d'insertion à l'aide des politiques existantes. En supposant qu'il existe dix politiques pour une paire d'interfaces spécifique, et qu'elles sont classées par priorités relatives pour la confort de l'utilisateur (1, 3, 5, ... et 19. Tous les nombres sont impairs.). Dans ce cas '1' reçoit la plus haute priorité et '19' la plus basse priorité. Il est aisé d'insérer une nouvelle politique avec une priorité 0 (avant 1) ou 20 (après 19), ou 2, 4, 6, ... , 18 (dans les intervalles de 1 à 19) ou bien un nombre pair en mots.

Select	Sequence	Source Ip Address	Source Port	Destination Ip Address	Destination Port	Protocol	Firewall Action	To Action Id
		From	From	From	From			
		To	To	To	To			
No Policies Configured								

Pour ajouter une politique, choisissez l'interface de réception et de transmission et cliquez sur Add pour compléter les paramètres de la politique ci-après. Cliquez sur Apply pour envoyer les paramètres. Les paramètres sont les suivants :

**Receive Interface:** Sélectionnée dans l'écran Firewall Politiques précédent.

**Transmit Interface:** Sélectionnée dans l'écran Firewall Politiques précédent.

**Source IP From- To:** Plage de l'adresse IP source. Lorsqu'une adresse IP source seulement est nécessaire, tapez-la dans le champ Source IP From.

**Destination IP From - To:** Plage de l'adresse IP de destination. Lorsqu'une adresse IP de destination seulement est nécessaire, tapez-la dans le champ Destination IP From.

**Source Port From - To:** Plage de ports source du paquet (pour le protocole TCP/UDP seulement). Lorsqu'un port source seulement est nécessaire, tapez le numéro de port dans le champ Source Port From.

**Destination Port From - To:** Plage de ports de destination du paquet (pour le protocole TCP/UDP seulement). Lorsqu'un port de destination seulement est nécessaire, tapez le numéro de port dans le champ Destination Port From.

**Protocol:** Choisissez le protocole parmi les suivants : Any, TCP, UDP, ICMP, GRE, AH, ESP

**Firewall Action:** Choisissez **Allow** pour permettre aux paquets de passer par le routeur ou **Deny** pour abandonner les paquets correspondants.

**NAT Action ID:** L'ID d'action NAT est créée à partir de l'onglet Policy Based NAT.

**TC Action ID:** ID du contrôle de trafic.

**Policy Configuration**

Receive Interface :  Transmit Interface :

Sequence :

Source IP From :  To :

Destination IP From :  To :

Source Port From :  To :

Destination Port From :  To :

Protocol :  Firewall Action :

NAT Action Id :  Tc Action Id :

## 6.2.2 Attaques

L'onglet Attacks configure l'attaque avec les valeurs optionnelles de seuil et de temporisation. Les attaques sont désactivées par défaut. Cochez l'élément et cliquez sur Modify pour changer les paramètres.

**Attacks**

**Attack List**

Select	Attack Type	Threshold	Timeout	Status
<input checked="" type="radio"/>	tcpportscan	15	50	enabled
<input type="radio"/>	tcpnullscan	10	50	disabled
<input type="radio"/>	tcpfinscan	10	50	disabled
<input type="radio"/>	tcpsynscan	10	50	enabled
<input type="radio"/>	udpflood	25	50	disabled
<input type="radio"/>	smurfscan	90	30	disabled
<input type="radio"/>	xmasscan	10	50	disabled
<input type="radio"/>	pingflood	70	60	disabled
<input type="radio"/>	ssrr	N/A	N/A	disabled
<input type="radio"/>	lsrr	N/A	N/A	disabled
<input type="radio"/>	timestamp	N/A	N/A	disabled
<input type="radio"/>	rr	N/A	N/A	disabled
<input type="radio"/>	security	N/A	N/A	disabled
<input type="radio"/>	satid	N/A	N/A	disabled
<input type="radio"/>	tcpflags	N/A	N/A	disabled

Modify

**Interface Configuration**

Interface Name :   Trusted  Untrusted

Set List

La protection contre les attaques suivantes est mise en œuvre.

- Drapeaux TCP:

Les paquets dotés des combinaisons suivantes de drapeaux TCP sont

abandonnés.

Paquet d'en-tête TCP fragmenté

Drapeaux NO

Drapeaux ALL

Paquets TCP avec drapeaux sans sens.

Drapeau SYN, ACK et FIN/RST.

Drapeaux SYN et FIN.

SYN sans ACK mais avec d'autres drapeaux.

FIN sans ACK.

- Balayage de port TCP :

Le balayage de port est l'une des techniques les plus courantes employées par les pirates pour découvrir les services qu'ils peuvent forcer. L'ordinateur victime potentielle exécute de nombreux 'services' qui écoutent des 'ports' connus. Le balayage de port le plus simple essaie simplement chacun des 65536 ports disponibles de la victime pour vérifier lesquels sont ouverts. Le pirate découvre les faiblesses potentiellement exploitables en balayant les ports disponibles de la victime. Le balayage de port signifie généralement balayage des ports TCP. Un balayage TCP classique tente d'ouvrir des connexions. Une autre technique envoie des paquets erronés à un port dans l'espoir que les ports "ouverts" à l'écoute envoient des messages d'erreur différents de ceux des ports « fermés ».

- Balayage TCP FIN :

Le balayage FIN tente de fermer une connexion qui n'est pas ouverte. S'il n'y a pas de service à l'écoute au port cible, le système d'exploitation génère un message d'erreur. Dans le cas contraire, le système d'exploitation abandonne silencieusement le paquet entrant. Par conséquent, l'absence de réponse indique un service à l'écoute au port. En revanche, des paquets pouvant être abandonnés silencieusement sur la ligne ou par les pare-feu, ce type de balayage n'est pas très efficace.

- Balayage TCP XMAS :

Avec ce type de balayage, tous les drapeaux du paquet ou bien certaines des combinaisons de drapeaux TCP invalides sont activés.

- Balayage TCP NULL :

NULL balaye où aucun des bits (drapeaux) n'est activé. Les différents systèmes

d'exploitation répondent toutefois différemment à ces balayages.

- Saturation UDP :

Les attaques par saturation UDP exploitent les services UDP, qui sont saturés au niveau de l'appareil ou d'un système individuel, ce qui empêche le traitement des flux réels. Elles peuvent se solder par une défaillance de l'appareil.

- Saturation ICMP :

Les attaques par saturation ICMP impliquent le bombardement de paquets ICMP vers le pare-feu ou un système individuel, ce qui empêche le traitement des flux réels. Elles peuvent se solder par une défaillance de l'appareil.

- Smurf UDP :

Les attaques de saturation UDP exploitent les services UDP, qui répondent aux paquets. Un pirate est armé d'une liste d'adresses de diffusion à laquelle il envoie des paquets UDP falsifiés. Les paquets sont généralement dirigés par le port 7 des machines ciblées, c'est-à-dire le port d'écho. Le port chargen est parfois ciblé. Un pirate est parfois en mesure d'établir une boucle entre les ports d'écho et chargen. Le résultat de cette attaque, comme indiqué plus haut, est une énorme quantité de trafic sur le réseau. Des réseaux complets peuvent ralentir et s'arrêter et des systèmes individuels peuvent perdre leur connectivité à Internet et/ou, dans certains cas, tomber en panne.

- Smurf ICMP :

Le smurf commence lorsqu'un pirate envoie un gros volume de trafic d'écho ICMP à une adresse de sous-réseau de diffusion. Le trafic est doté d'une adresse de retour falsifiée. L'adresse falsifiée est celle de la victime visée par l'attaque. Lorsque des machines individuelles du réseau reçoivent les requêtes d'écho ICMP, elles répondent par une réponse d'écho. Ces réponses arrivent toutes à l'adresse falsifiée dans les requêtes d'écho ICMP d'origine. Sur les réseaux qui comptent un grand nombre de systèmes, le trafic généré peut être réellement volumineux. Le système victime de l'attaque (indiqué par l'adresse IP falsifiée) est rapidement dépassé par le trafic entrant et perd à coup sûr la connectivité avec l'Internet.

- Options IP :

Une option IP est une technique où l'expéditeur d'un paquet peut spécifier la route qu'il doit emprunter à travers le réseau. Un attaquant peut envoyer des paquets avec les options vers les systèmes individuels. Si les systèmes individuels ne supportent pas le traitement d'option, ceci peut entraîner une défaillance de systèmes.

LSRR (option Loose Source Record Route).

SSRR (option Strict Source Record Route).

RR (option Record Route).

Option Timestamp.

Option Security.

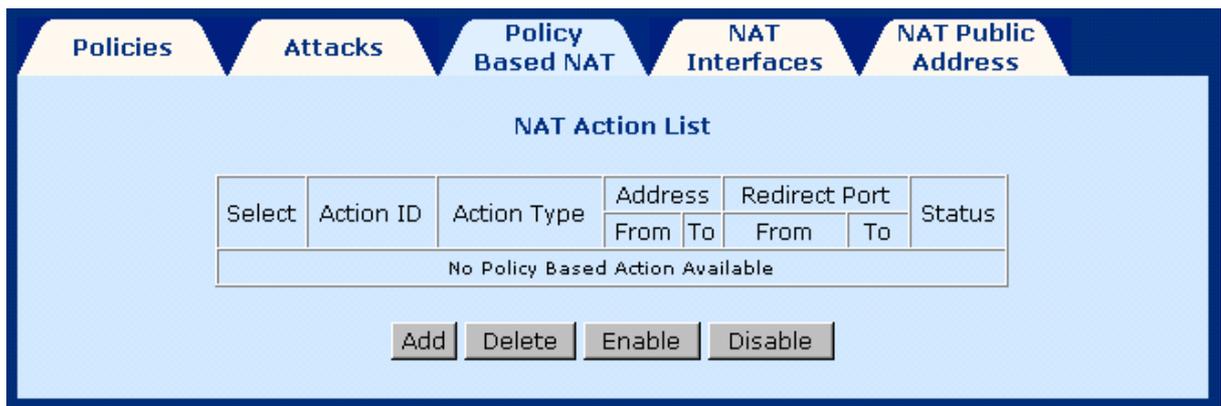
### 6.2.3 NAT politique

La NAT politique permet aux utilisateurs de spécifier des mappages de NAT statique, d'adresse de redirection et de port de redirection à l'aide de politiques et d'actions NAT associées. Le mappage de NAT statique sert à mapper un ensemble d'adresses locales sur un ensemble d'adresses publiques pour garantir l'accès au monde extérieur. Le mappage d'adresse ou de port de redirection sert à permettre l'accès entrant aux hôtes externes en dirigeant le trafic destiné à l'adresse ou au port configuré vers un nœud spécifique du réseau privé. La politique indique les critères correspondants et l'action NAT spécifie l'adresse cible et/ou le port de remplacement.

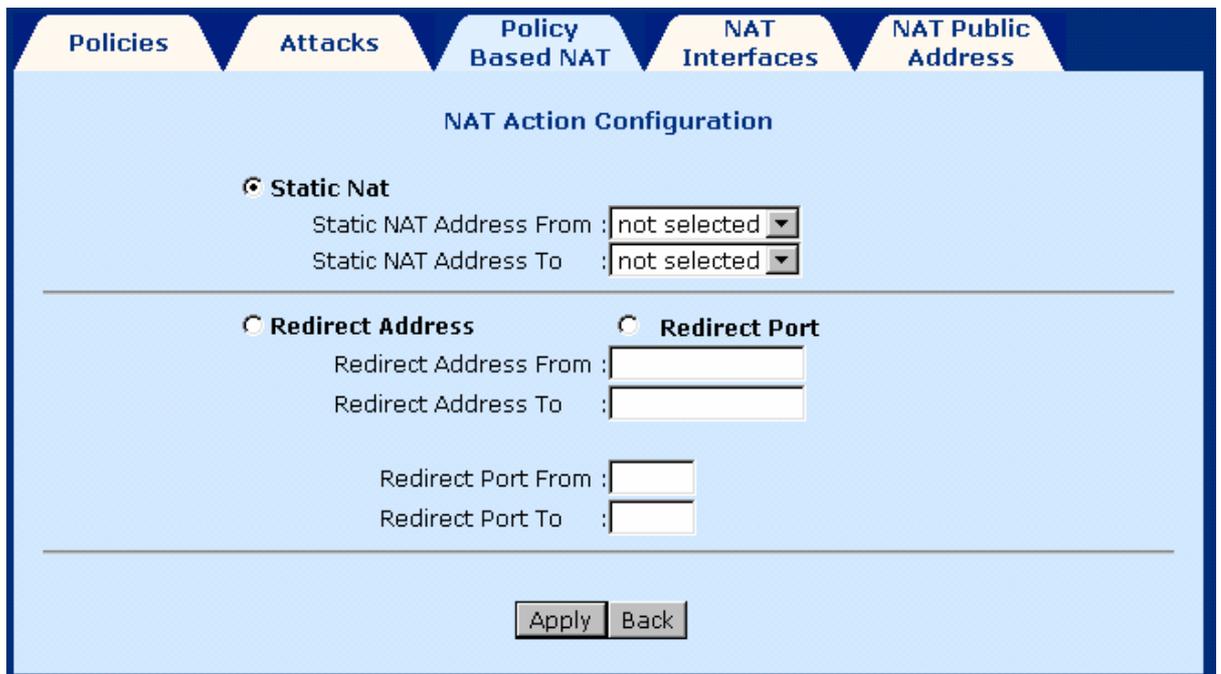
En configurant un mappage NAT statique, la politique contient l'adresse ou les adresses source correspondante(s) et l'action NAT contient l'adresse ou les adresses IP publique(s) de remplacement. L'adresse source des paquets sortants qui correspondent à la politique est remplacée par l'adresse IP publique indiquée dans l'action NAT.

En configurant un mappage d'adresse de redirection, la politique contient l'adresse ou les adresses de destination correspondante(s) et l'action NAT contient l'adresse ou les adresses IP locale(s) de remplacement. L'adresse de destination des paquets sortants qui correspondent à la politique est remplacée par l'adresse locale indiquée dans l'action NAT.

En configurant un mappage de port de redirection, la politique contient l'adresse ou les adresses et le(s) port(s) de destination correspondant(s) et l'action NAT contient l'adresse ou les adresses IP locale(s) et le(s) port(s) de remplacement. L'adresse de destination et le port du trafic entrant qui correspond à la politique sont remplacés par l'adresse locale et le port indiqués dans l'action NAT.



Pour ajouter une liste d'actions NAT, cliquez sur le bouton **Add** pour afficher l'écran ci-après. L'écran contient les paramètres de mappage NAT statique et ou d'adresse/port de redirection. Lorsqu'une entrée est créée, une ID d'action est ajoutée, qui est nécessaire pour définir l'entrée de politique dans l'onglet Policies.



### NAT statique

Le champ Static NAT configure le mappage de la NAT statique. Vous pouvez choisir une seule adresse IP ou une plage d'adresses. L'adresse IP est créée à partir de l'onglet NAT Public Address. Par exemple, cinq adresses IP publiques sont nécessaires, 10.0.0.2 – 10.0.0.6. Ajoutez ces adresses IP une par une dans l'onglet NAT Public Address. Puis, dans cet écran, sélectionnez la première adresse IP (10.0.0.2) dans le champ **Static NAT Address From** puis 10.0.0.6

dans le champ **Static NAT Address To**.

The screenshot shows a configuration window with two main sections. The first section, 'Static Nat', has a radio button selected. It contains two fields: 'Static NAT Address From' with a dropdown menu set to 'not selected', and 'Static NAT Address To' with a dropdown menu open. The open menu lists the following IP addresses: 10.0.0.2, 10.0.0.3, 10.0.0.4, 10.0.0.6, and 10.0.0.5. The second section, 'Redirect Address', has a radio button unselected and contains two empty fields: 'Redirect Address From' and 'Redirect Address To'.

### Redirection d'adresse/redirection de port

Lorsque l'option Redirect Address est choisie, complétez l'adresse de redirection. Lorsque l'option Redirect Port est choisie, complétez l'adresse de redirection ou la plage d'adresses, puis le port de redirection ou la plage de ports.

## 6.2.4 Interfaces NAT

La NAT offre la sécurité minimale pour masquer la configuration interne du réseau local au monde extérieur. Elle permet aux hôtes du réseau privé d'accéder de façon transparente au réseau extérieur et autorise l'accès à des hôtes locaux sélectionnés de l'extérieur. La NAT contribue également à surmonter les limitations d'adressage IP comme l'attribution restreinte d'adresses IP et les structures d'adressage interne non enregistrées.

L'onglet NAT Interfaces indique l'état de l'interface NAT (activée ou désactivée) de chaque interface. La NAT peut être activée simultanément sur plusieurs interfaces. Pour activer la NAT d'une interface WAN, vérifiez qu'une PVC lui a déjà été attribuée. Par exemple, si l'interface mer0 n'est pas paramétrée pour une PVC, vous ne pouvez pas activer la NAT pour mer0 dans cet écran. Vous devez créer une entrée MER depuis l'écran WAN Setup.

## List of NAT Interface Entries

Select	Interface	Nat Status
<input type="radio"/>	eth0	disabled
<input type="radio"/>	mer0	disabled
<input type="radio"/>	ph0	disabled
<input type="radio"/>	wlan0	disabled
<input type="radio"/>	usb0	disabled
<input type="radio"/>	atm0	disabled
<input type="radio"/>	atm1	disabled
<input type="radio"/>	atm2	disabled
<input type="radio"/>	atm3	disabled
<input type="radio"/>	atm4	disabled
<input type="radio"/>	atm5	disabled
<input type="radio"/>	atm6	disabled
<input type="radio"/>	atm7	disabled
<input type="radio"/>	ppp0	disabled
<input type="radio"/>	ppp1	disabled
<input type="radio"/>	ppp2	disabled
<input type="radio"/>	ppp3	disabled
<input type="radio"/>	ppp4	disabled
<input type="radio"/>	ppp5	disabled
<input type="radio"/>	ppp6	disabled
<input type="radio"/>	ppp7	disabled

Enable

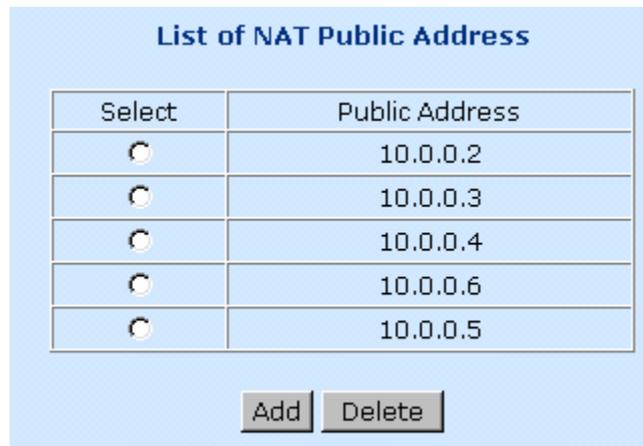
Disable

## 6.2.5 Adresse NAT publique

L'adresse NAT publique ajoute ou supprime une adresse IP publique de l'interface WAN. Plusieurs adresses IP peuvent être définies. L'adresse IP à définir doit se trouver dans le même sous-réseau que l'interface WAN.



Par exemple, une PVC est définie pour RFC1483 routé avec l'adresse IP WAN 10.0.0.1, et le masque de sous-réseau 255.255.255.0. Les cinq adresses IP publiques sont nécessaires, 10.0.0.2 – 10.0.0.6. Ajoutez ces adresses IP une par une dans l'onglet NAT Public Address.



**Remarque :** Si l'adresse IP publique à définir ne se trouve pas dans le même sous-réseau que l'interface WAN, le message d'erreur suivant est affiché.

**Error : IP address does not belong to WAN interface's subnet**  
[Back](#)

## 6.3 Configuration

Depuis la page **Configure** du menu Advanced, vous pouvez configurer les interfaces LAN et WAN, VCC, PPPoE, PPPoA, passerelle DNS & Default, et NAT.

Select	Interface	IP Address	Subnet Mask	MAC Address	Status
<input type="radio"/>	eth0	172.16.11.111	255.255.255.0	00:30:da:45:56:67	up
<input type="radio"/>	mer0	none	none	NA	down
<input type="radio"/>	ph0	none	none	NA	down
<input type="radio"/>	wlan0	192.168.101.1	255.255.255.0	NA	up
<input type="radio"/>	usb0	192.168.2.1	255.255.255.0	NA	up
<input type="radio"/>	lo0	127.0.0.1	255.0.0.0	NA	up
<input type="radio"/>	atm0	10.0.0.1	255.255.255.252	NA	up
<input type="radio"/>	atm1	none	none	NA	down
<input type="radio"/>	atm2	none	none	NA	down
<input type="radio"/>	atm3	none	none	NA	down
<input type="radio"/>	atm4	none	none	NA	down
<input type="radio"/>	atm5	none	none	NA	down
<input type="radio"/>	atm6	none	none	NA	down
<input type="radio"/>	atm7	none	none	NA	down
<input type="radio"/>	ppp0	none	none	NA	down
<input type="radio"/>	ppp1	none	none	NA	down
<input type="radio"/>	ppp2	none	none	NA	down
<input type="radio"/>	ppp3	none	none	NA	down
<input type="radio"/>	ppp4	none	none	NA	down
<input type="radio"/>	ppp5	none	none	NA	down
<input type="radio"/>	ppp6	none	none	NA	down
<input type="radio"/>	ppp7	none	none	NA	down

Configure Interface    DNS & Default G/W    NAT

**Attention :** Ne configurez pas ces paramètres dans le sous-menu web Configurer si vous n'êtes pas technicien.

## 6.3.1 Interfaces

Pour configurer une interface, choisissez-la en cliquant dans le cercle à gauche de l'écran. Cliquez ensuite sur le bouton **Configure Interface** en bas de l'écran.

Notez les remarques suivantes :

### Interfaces

- **eth0** affiche l'état du port LAN.
- **mer0** affiche l'interface configurée pour MER.
- **wlan0** affiche l'interface LAN sans fil.
- **usb0** affiche l'interface USB
- **lo0** est l'interface loopback. Lorsque OAM loopback est exécuté, le champ d'état affiche UP.
- **atm0 to atm7** affiche les interfaces configurées pour le mode RFC1483 Bridged ou RFC 1483 Routed.
- **ppp0 to ppp7** affiche les interfaces configurées pour PPPoE ou PPPoA.

### Paramètres :

- **Interface Name** : affiche le type d'interface.
- **IP Address** : Adresse IP de l'interface.
- **Subnet Mask** : Masque de sous-réseau de l'interface sélectionnée.
- **MAC Address** : Adresse MAC de l'interface. Normalement, seule l'interface LAN est dotée de l'adresse MAC. Les autres affichent N/A.
- **Status**: UP et Down. Lorsqu'une interface est réglée sur **Down**, le système ne tente pas de transmettre de messages par cette interface. Lorsqu'elle est sur **UP**, les messages peuvent être transmis par l'interface.

## Configuration de l'interface

L'illustration ci-dessous est une copie de l'écran d'interface LAN (eth0) après avoir choisi eth0 et cliqué sur le bouton Configure Interface.

**Interfaces**   **VCC**   **PPPoE**   **PPPoA**

### Ethernet Interface Configuration

Dynamic IP Address from DHCP Server  
 Static IP Address

Interface : eth0      IP Address : 192.168.1.1  
Subnet Mask : 255.255.255.0      MTU : 1500  
Status : down

Apply   Cancel

L'écran suivant est celui de l'interface ATM.

**Interfaces**   **VCC**   **PPPoE**   **PPPoA**

### ATM Interface Configuration

Interface : atm0      IP Address : 10.0.0.1  
Subnet Mask : 255.255.255.252      Status : up  
MTU : 1500

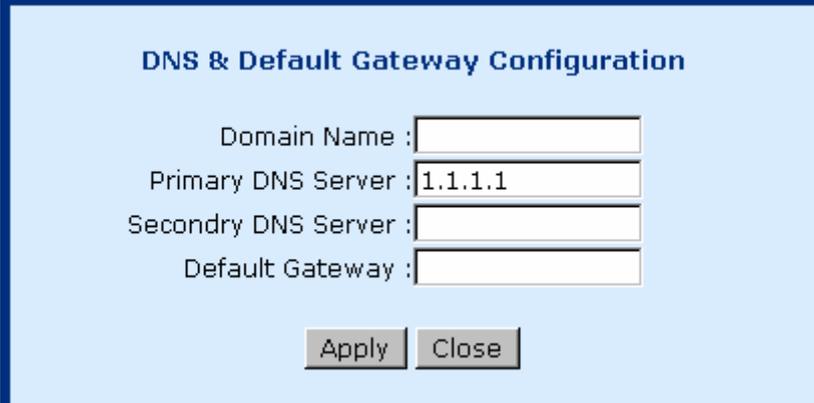
Apply   Back

## Passerelle DNS & Default

Observez les étapes suivantes pour configurer la passerelle DNS & Default :

**ETAPE 1** : Cliquez sur **Interface Configure** dans la barre de menu.

**ETAPE 2** : Cliquez sur le bouton **DNS and Default gateway** en bas de la page de configuration.



The image shows a dialog box titled "DNS & Default Gateway Configuration" with a light blue background and a dark blue border. It contains four input fields for configuration: "Domain Name", "Primary DNS Server" (with the value "1.1.1.1" entered), "Secondary DNS Server", and "Default Gateway". At the bottom of the dialog are two buttons: "Apply" and "Close".

**ETAPE 3** : Complétez les champs ci-dessous :

- **Domain Name** : Défini par l'utilisateur
- **Primary DNS server** : Entrez l'adresse IP du serveur principal.
- **Secondary DNS server** : Entrez l'adresse IP du serveur secondaire utilisé en cas d'indisponibilité ou de défaillance de l'adresse IP du serveur principal
- **Default Gateway** : Adresse IP de la passerelle pour le réseau IP

**ETAPE 4** : Cliquez sur **Apply** pour envoyer les paramètres.

## NAT

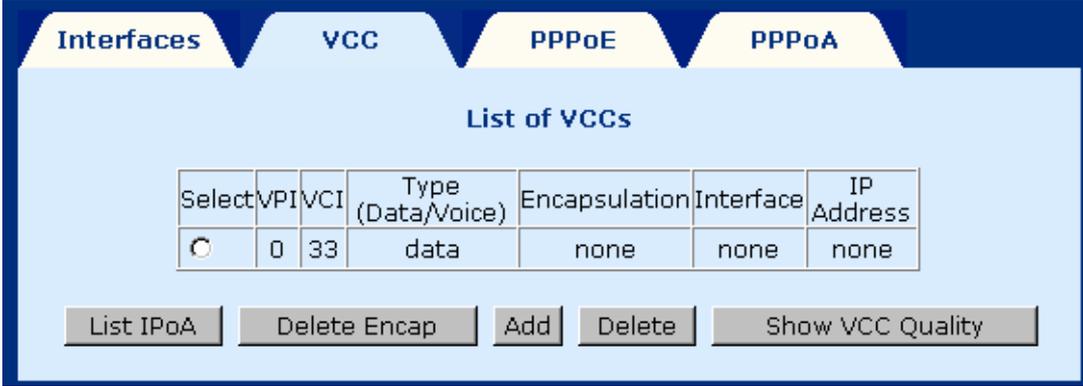
Pour activer la NAT sur une interface, cochez l'élément et cliquez sur Enable, et sur Disable pour la désactiver.

**List of NAT Interface Entries**

Select	Interface	Nat Status
<input type="radio"/>	eth0	disabled
<input type="radio"/>	mer0	disabled
<input type="radio"/>	ph0	disabled
<input type="radio"/>	wlan0	disabled
<input type="radio"/>	usb0	disabled
<input type="radio"/>	atm0	disabled
<input type="radio"/>	atm1	disabled
<input type="radio"/>	atm2	disabled
<input type="radio"/>	atm3	disabled
<input type="radio"/>	atm4	disabled
<input type="radio"/>	atm5	disabled
<input type="radio"/>	atm6	disabled
<input type="radio"/>	atm7	disabled
<input type="radio"/>	ppp0	disabled
<input type="radio"/>	ppp1	disabled
<input type="radio"/>	ppp2	disabled
<input type="radio"/>	ppp3	disabled
<input type="radio"/>	ppp4	disabled
<input type="radio"/>	ppp5	disabled
<input type="radio"/>	ppp6	disabled
<input type="radio"/>	ppp7	disabled

### 6.3.2 VCC

Cet écran indique toutes les entrées VCC courantes au milieu de l'écran. Depuis cet écran, vous pouvez aussi : lister les IPoA, supprimer l'encapsulation, ajouter un VCC, supprimer un VCC, et afficher la qualité VCC.



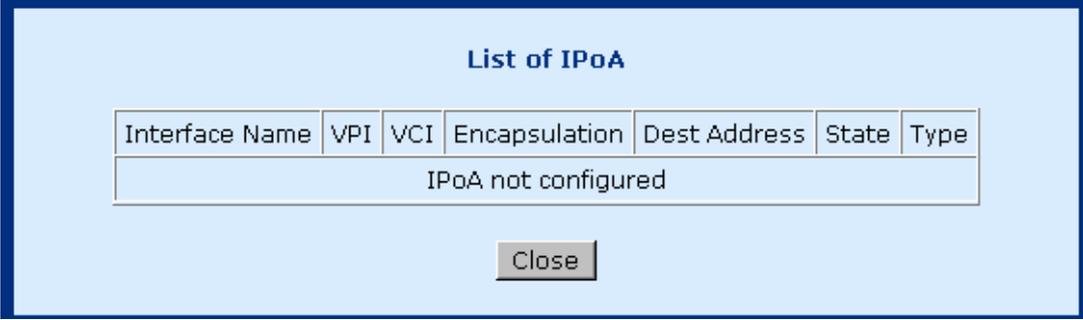
The screenshot shows a web interface with a navigation bar at the top containing four tabs: "Interfaces", "VCC", "PPPoE", and "PPPoA". The "VCC" tab is selected. Below the navigation bar, the title "List of VCCs" is centered. A table displays the following data:

Select	VPI	VCI	Type (Data/Voice)	Encapsulation	Interface	IP Address
<input type="radio"/>	0	33	data	none	none	none

Below the table, there are five buttons: "List IPoA", "Delete Encap", "Add", "Delete", and "Show VCC Quality".

#### Liste IPoA

Pour lister les informations IP sur ATM cliquez sur le bouton **IPoA** dans le coin inférieur gauche de l'écran.



The screenshot shows a web interface with the title "List of IPoA" centered. A table displays the following headers:

Interface Name	VPI	VCI	Encapsulation	Dest Address	State	Type
IPoA not configured						

Below the table, there is a "Close" button.



VPI :	Identifiant de chemin virtuel (VPI) qui identifie cette connexion ATM. Le VPI est un nombre entier situé entre 0 et 4095.
VCI :	Identifiant de canal virtuel (VCI) qui identifie cette connexion ATM. Le VCI est un nombre entier situé entre 0 et 65 535.
Peak Cell rate (cells/sec):	Détermine le débit le plus rapide auquel l'utilisateur peut envoyer des cellules au réseau. Il est exprimé en unités de cellule par seconde.
Average Cell rate (cells/sec):	Détermine le débit maximum durable/moyen auquel l'utilisateur peut envoyer des cellules au réseau. Il est exprimé en cellules par seconde. Ceci détermine l'utilisation de la bande passante. Cette valeur doit toujours être inférieure ou égale au débit Peak Cell Rate.
Burst size (cells):	Nombre maximal de cellules que l'utilisateur peut envoyer au débit le plus rapide en une fois, à une vitesse durable.
CDVT (cells):	Contraint le nombre maximal de cellules que l'utilisateur peut envoyer au réseau à la vitesse de ligne maximale.
Type:	Choisissez data ou voice
<b>Service Type:</b>  <b>cbr</b> Constant Bit Rate:  <b>rtvbr</b> Real Time Variable Bit Rate:  <b>Nrtvbr</b> Real Time Variable Bit Rate:  <b>Ubr</b> Unspecified Bit Rate:	<p>Supporte les applications en temps réel exigeant une quantité fixe de bande passante. Les applications produisent des données à intervalles réguliers, comme un flux vidéo. L'utilisateur peut indiquer combien de bande passante réserver.</p> <p>Supporte les applications sensibles à la durée, comme les applications vocales. Le débit d'arrivée des cellules varie dans ces applications.</p> <p>Supporte les applications qui ne présentent pas de contrainte de délai et de variation de délai, mais qui comportent des caractéristiques de débit variable et de pointe de trafic.</p> <p>Service selon disponibilité qui n'exige pas de délai étroit ni de variation de délai. UBR offre n'offre pas de qualité de service définie ni de débit garanti.</p>

Interfaces
VCC
PPPoE
PPPoA

### VCC Configuration

VPI : <input style="width: 80%;" type="text"/>	VCI : <input style="width: 80%;" type="text"/>
Peak Cell Rate (cells/sec): <input style="width: 80%;" type="text" value="3000"/>	Avg. Cell Rate (cells/sec): <input style="width: 80%;" type="text" value="3000"/>
Burst Size (cells): <input style="width: 80%;" type="text" value="45"/>	CDVT (cells): <input style="width: 80%;" type="text" value="500000"/>
Type : <input style="width: 80%;" type="text" value="data"/>	Service Type : <input style="width: 80%;" type="text" value="ubr"/>

---

For data flow:

Routed  
Interface :

---

IPoA  
Interface :   
Default PVC :   
Next Hop IP Address :

---

PPPoA  
Profile ID :   
User Name :   
Authentication Type :   
Encapsulation Type :   
NAT :

Password :   
Interface :   
Trace :

---

PPPoE  
Profile ID :   
User Name :   
Authentication Type :   
Mode :   
Encapsulation Type :   
NAT :

Password :   
Interface :   
Idle Timeout (min) :   
Trace :

---

### Suppression d'un VCC

Pour supprimer une entrée de VCC, sélectionnez-la dans la liste des VCC et cliquez sur le bouton **Delete**.

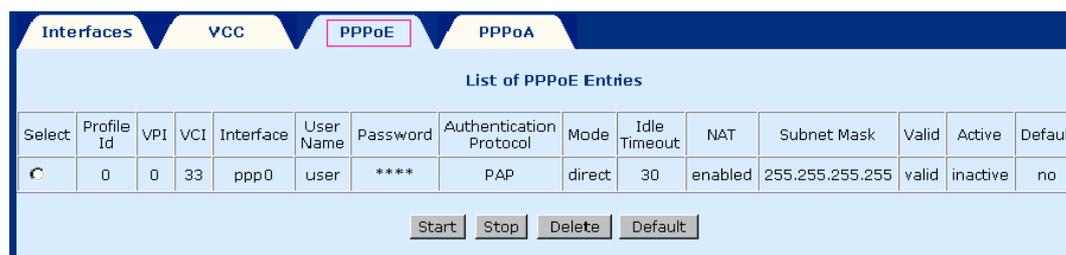
### Affichage de la qualité VCC

Pour afficher les informations relatives à la qualité VCC, cliquez sur le bouton **Show VCC Quality**.

### 6.3.3 PPPoE

Cette section explique comment démarrer, arrêter, supprimer et paramétrer une entrée PPPoE par défaut.

Cliquez sur **Configure** dans la barre de menu Advanced pour accéder à la page PPPoE. Pour démarrer, arrêter, supprimer ou paramétrer une entrée comme PPPoE par défaut, sélectionnez-la dans List of PPPoE Entries et cliquez sur le bouton approprié en bas de la page.



The screenshot shows a web interface for configuring PPPoE. At the top, there are four tabs: 'Interfaces', 'VCC', 'PPPoE', and 'PPPoA'. The 'PPPoE' tab is selected and highlighted with a pink border. Below the tabs, the title 'List of PPPoE Entries' is centered. A table with 14 columns and 2 rows is displayed. The columns are: Select, Profile Id, VPI, VCI, Interface, User Name, Password, Authentication Protocol, Mode, Idle Timeout, NAT, Subnet Mask, Valid, Active, and Default. The first row contains the following values: a refresh icon, 0, 0, 33, ppp0, user, \*\*\*\*, PAP, direct, 30, enabled, 255.255.255.255, valid, inactive, and no. Below the table, there are four buttons: Start, Stop, Delete, and Default.

Select	Profile Id	VPI	VCI	Interface	User Name	Password	Authentication Protocol	Mode	Idle Timeout	NAT	Subnet Mask	Valid	Active	Default
	0	0	33	ppp0	user	****	PAP	direct	30	enabled	255.255.255.255	valid	inactive	no

Start Stop Delete Default

### 6.3.4 PPPoA

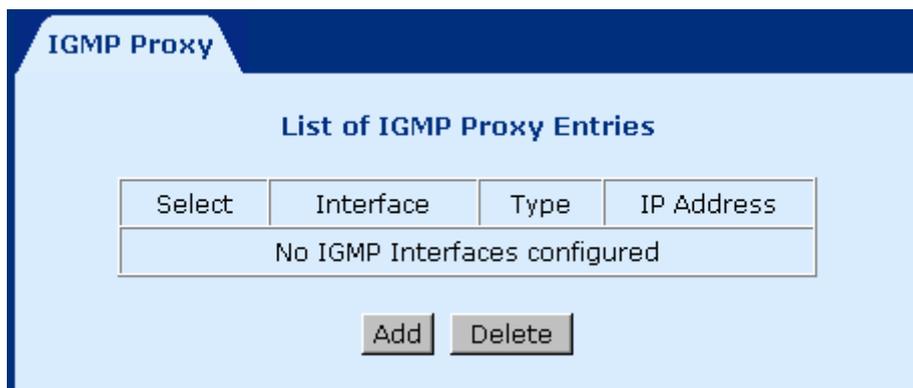
Cette section explique comment démarrer, arrêter, supprimer et paramétrer une entrée PPPoA par défaut.

Cliquez sur **Configure** dans la barre de menu Advanced pour accéder à la page PPPoA. Pour démarrer, arrêter, supprimer ou paramétrer une entrée comme PPPoA par défaut, sélectionnez-la dans List of PPPoA Entries et cliquez sur le bouton approprié en bas de la page.



### 6.4 Proxy IGMP

IGMP (Internet Group Membership Protocol) est un protocole utilisé par les hôtes IP pour signaler leurs adhésions de groupe multicast aux routeurs multicast immédiatement voisins.



### Ajout d'une entrée IGMP

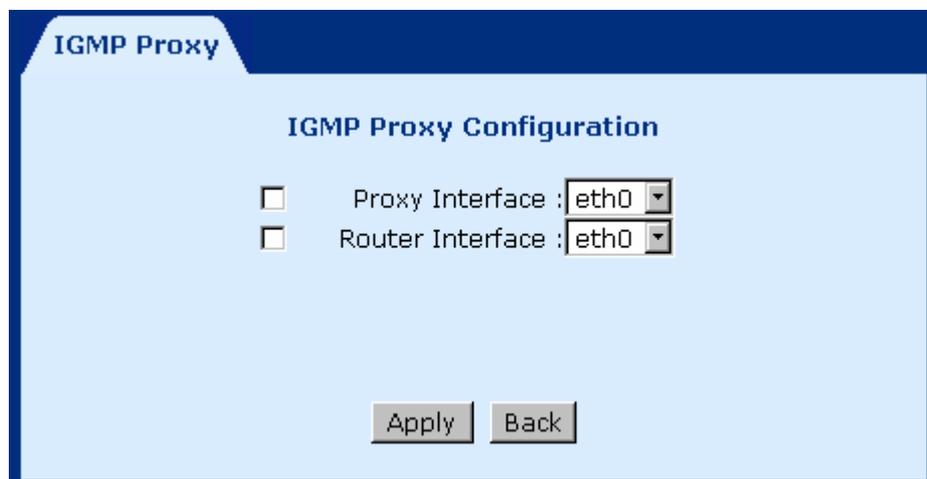
Observez les étapes suivantes pour ajouter un proxy IGMP :

**ETAPE 1** : Choisissez **IGMP Proxy** dans la barre de menu.

**ETAPE 2** : Cliquez sur **Add** en bas de l'écran.

**ETAPE 3** : Choisissez Proxy interface, Router interface ou les deux en cochant la case à côté de l'interface, puis utilisez le menu déroulant de gauche pour sélectionner l'interface eth0 (Ethernet), usb0, mer0, atm0-7, ou ppp0-7.

**ETAPE 4** : Cliquez sur **Apply** pour activer les paramètres.



The screenshot shows a configuration window titled "IGMP Proxy" with a sub-header "IGMP Proxy Configuration". It contains two rows of configuration options, each with a checkbox and a dropdown menu. The first row is "Proxy Interface : eth0" and the second row is "Router Interface : eth0". At the bottom of the window, there are two buttons: "Apply" and "Back".

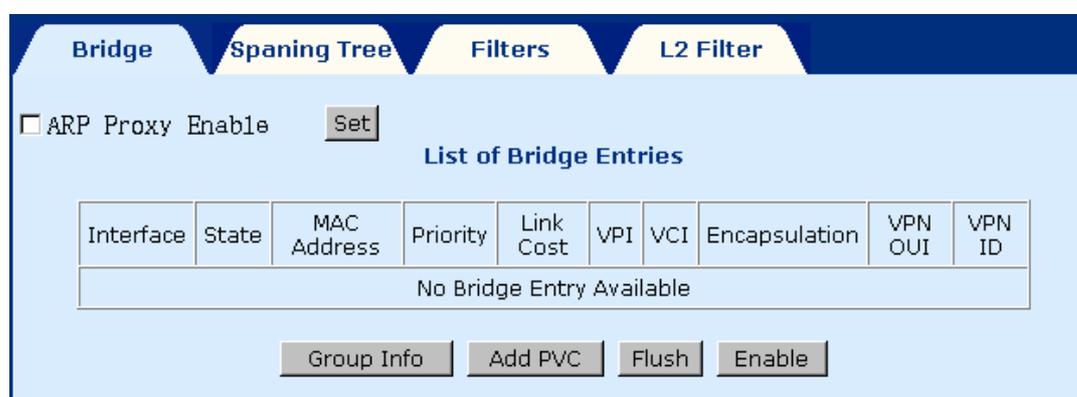
### Suppression d'une entrée IGMP

Pour supprimer une entrée, sélectionnez-la dans la liste et cliquez sur **Delete**.

## 6.5 Pontage

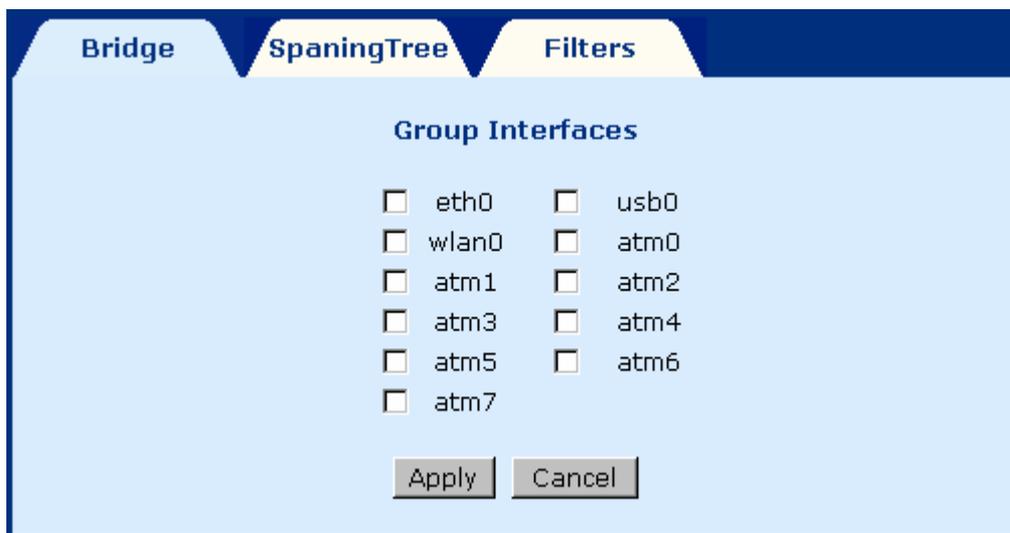
### 6.5.1 Pont

La fenêtre Bridge affiche les entrées de pontage PVC configurées des interfaces. Quatre boutons sont présents en bas du volet principal : Group Info, Add PVC, Flush et Disable.



**ARP Proxy** : Vous pouvez activer la fonction ARP Proxy en cochant la case et en cliquant sur le bouton **Set**. Le proxy d'ARP permet au routeur de répondre à une requête ARP locale pour une destination distante. L'ARP (Address Resolution Protocol) (ARP) permet au routeur de déterminer l'adresse physique d'un hôte réseau en liant une adresse IP 32 bits à une adresse MAC 48 bits.

**GroupInfo** : Cette option configure les paquets LAN qui passent par l'interface LAN vers les interfaces WAN sélectionnées. Si vous souhaitez changer les interfaces configurées, vous devez d'abord cliquer sur le bouton **Flush** (pour supprimer la configuration actuelle) puis cliquer sur le bouton **Group Info**, sélectionner les interfaces du groupe et cliquer sur le bouton **Apply**. Vous devez sélectionner eth0, car eth1 n'est pas disponible dans cette version du produit.

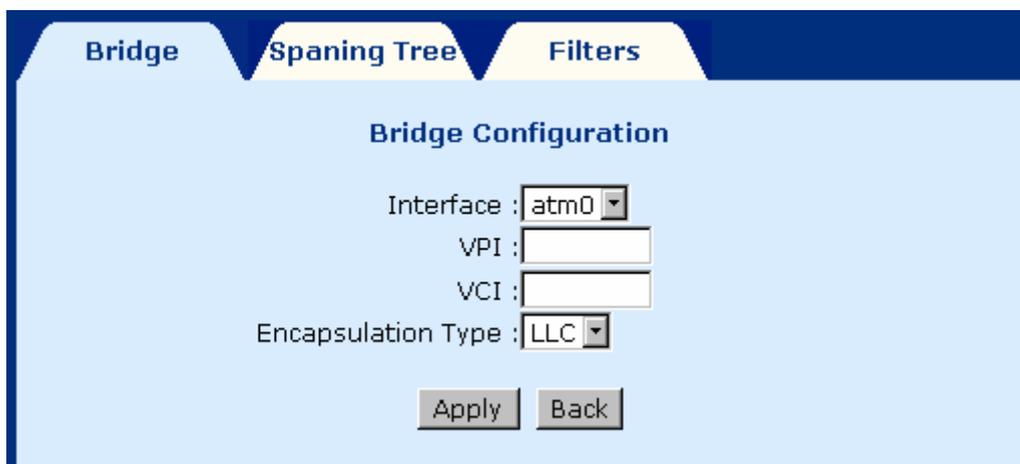


The screenshot shows a configuration window with three tabs: 'Bridge', 'SpaningTree', and 'Filters'. The 'Filters' tab is active. The title is 'Group Interfaces'. Below the title, there is a list of interface names with checkboxes next to them:

<input type="checkbox"/> eth0	<input type="checkbox"/> usb0
<input type="checkbox"/> wlan0	<input type="checkbox"/> atm0
<input type="checkbox"/> atm1	<input type="checkbox"/> atm2
<input type="checkbox"/> atm3	<input type="checkbox"/> atm4
<input type="checkbox"/> atm5	<input type="checkbox"/> atm6
<input type="checkbox"/> atm7	

At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

**AddPVC** : Vous pouvez ajouter une PVC à l'interface ATM. Cliquez d'abord sur le bouton Add PVC. Puis, à partir de l'écran **Bridging**, sélectionnez un type d'interface ATM, de Vpi, Vci et Encapsulation et cliquez sur **Apply**.



The screenshot shows a configuration window with three tabs: 'Bridge', 'Spaning Tree', and 'Filters'. The 'Spaning Tree' tab is active. The title is 'Bridge Configuration'. Below the title, there are several input fields:

Interface : atm0 (dropdown menu)

VPI : (text input field)

VCI : (text input field)

Encapsulation Type : LLC (dropdown menu)

At the bottom of the window, there are two buttons: 'Apply' and 'Back'.

**Flush** : Le choix de cette commande dans l'écran **Bridging** élimine toutes les entrées PVC.

**Disable** : Le choix de cette commande dans l'écran **Bridging** désactive toutes les PVC mais conserve les paramètres pour les réactiver ultérieurement.

## 6.5.2 Spanning tree

Pour accéder au menu, cliquez sur l'onglet **Spanning Tree**, situé en haut de l'écran **Bridging**.

Select	Port	State	Port Id	Link Cost	Tx CBpdu	Rx CBpdu	TX TBpdu	RX TBpdu
<input type="radio"/>	1	disabled	32769	100	0	0	0	0

### Affichage des paramètres STP

Pour afficher les paramètres STP, cliquez sur l'onglet **STP parameters**, situé en bas de l'écran Spanning Tree.

**List of Spaning Tree Parameters**

STP	disabled
Active Ports	1
Bridge Id	00:00:00:00:80:00
Root Id	00:00:00:00:00:00
Hello Time	2
Max Age	20
Forwarded Delay	15
Root Port	0
Root Path Lost	0
Hold Time	1

Pour configurer les paramètres STP

**ETAPE 1 :** Cliquez sur l'onglet **Spanning Tree**, situé en haut de l'écran **Bridging**.

**ETAPE 2 :** Cliquez sur le bouton **Configure Port**.

**ETAPE 3 :** Configurez les paramètres

**ETAPE 4 :** Cliquez sur le bouton Apply.

**Port Configuration**

Port Parameters

Interface Name :  Port Priority :

Link Cost :

---

Bridge Parameters

Bridge Priority :   Hello Time :

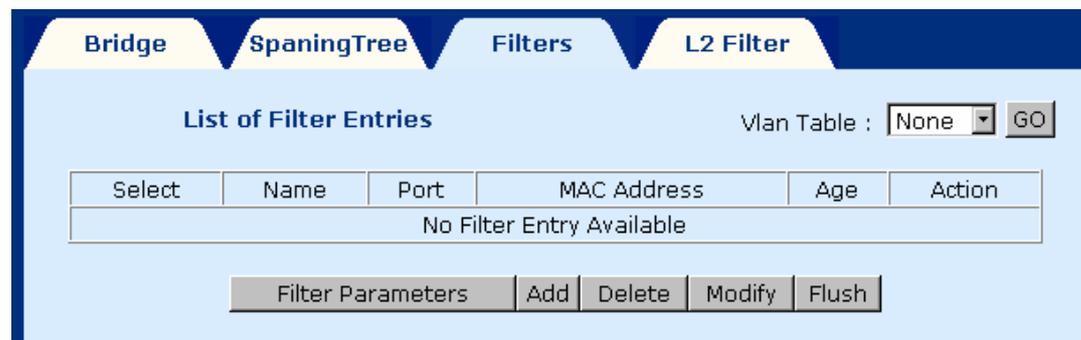
Max Age Time :   Forward Delay Priority :

## Activer/Désactiver le STP

Pour activer/désactiver une entrée STP, sélectionnez-la et cliquez sur le bouton **Enable** ou **Disable**, situé en bas et à droite de l'écran Spanning Tree. Notez que si une entrée est déjà activée, le bouton Disable est présent. Inversement, si une entrée est déjà désactivée, le bouton Enable est présent.

## 6.5.3 Filtres

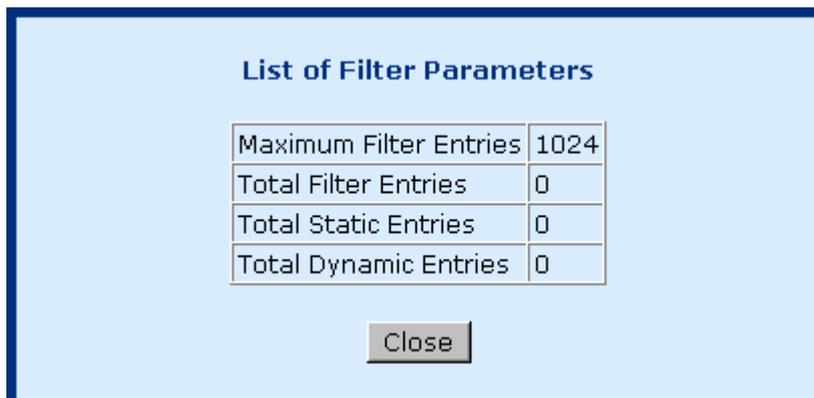
Le filtrage est un type de pare-feu utile pour augmenter la sécurité du réseau ou pour limiter le trafic indésirable. Les filtres de cet appareil sont basés sur les adresses MAC. La page s'ouvre sur une liste des entrées de filtre actuellement configurées. Depuis cette page, vous pouvez aussi afficher les paramètres du filtre, ajouter, supprimer, modifier un filtre ou éliminer les paramètres de filtre. Ces fonctions sont décrites ci-dessous.



### List of filter entries

Pour afficher la liste des paramètres du filtre, cliquez sur le bouton **Filter parameters** en bas de la page Filters. Les paramètres suivants sont affichés :

Maximum filter entries	Nombre d'entrées de filtre potentiellement paramétrables
Total filter entries	Nombre d'entrées de filtre actuellement paramétrées
Total static entries	Nombre d'entrées statiques actuellement paramétrées
Total dynamic entries	Nombre d'entrées dynamiques actuellement paramétrées



### Ajout d'une entrée de filtre

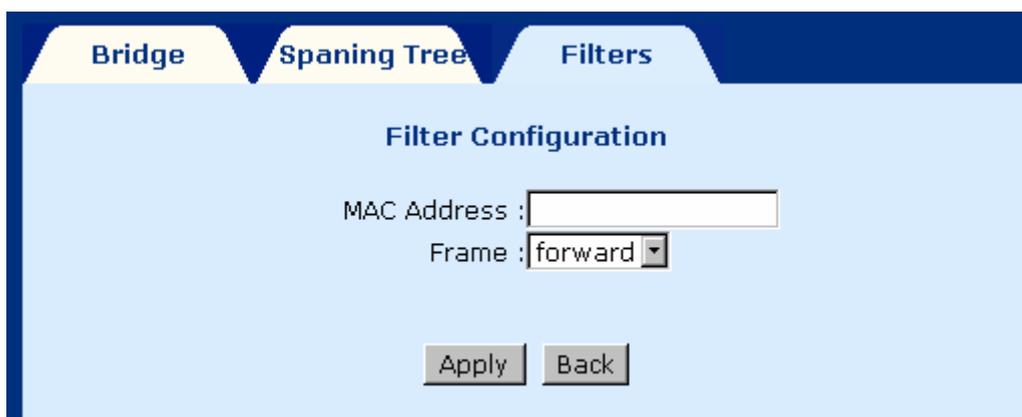
Observez les étapes suivantes pour ajouter une entrée de filtrage :

**ETAPE 1** : Cliquez sur le bouton **Add** en bas de la page Filters.

**ETAPE 2** : Entrez l'adresse MAC

**ETAPE 3** : Réglez l'option Frame sur **forward** pour envoyer des paquets correspondant à l'adresse MAC, ou sur **Drop** pour abandonner les paquets correspondants.

**ETAPE 4** : Cliquez sur **Apply**.



## Suppression d'une entrée de filtre

Pour supprimer une entrée de filtrage, sélectionnez-la et cliquez sur le bouton **Delete** en bas de la page Filters.

Modification d'une entrée de filtre

Pour modifier une entrée de filtrage, sélectionnez-la et cliquez sur le bouton **Modify** en bas de la page Filters.

Elimination des entrées de filtre

Pour éliminer toutes les entrées de filtrage, cliquez sur le bouton **Flush** en bas de la page Filters.

## 6.5.4 Filtre Layer2

Les filtres L2 de cet appareil sont basés sur les adresses MAC. La page s'ouvre sur une liste des entrées de filtre de pont L2 actuellement configurées. Les paquets sont abandonnés ou acceptés en fonction des conditions paramétrées dans chaque entrée. Depuis cette page, vous pouvez aussi afficher les paramètres du filtre, ajouter, supprimer, modifier un filtre. Ces fonctions sont décrites ci-dessous.

**Bridge L2 Filter**

L2 Filter :  Enable  Disable

Priority :

Destination MAC :

Source MAC :

Ethernet Type :

Interface :

Action :

**List of Layer 2 Bridge Filter Entry**

Select	Priority	Destination MAC	Source MAC	Ether Type	Interface	Action
--------	----------	-----------------	------------	------------	-----------	--------

## Activer/Désactiver le filtrage L2

Pour activer/désactiver le filtrage de pont L2, cliquez sur **Enable** ou **Disable** puis sur le bouton **Set**. Ce réglage s'applique à la liste d'entrées de filtrage de pont L2.

## Ajout d'une entrée de filtre de pont L2

Observez les étapes suivantes pour ajouter une entrée de filtrage L2 :

**ETAPE 1** : Complétez les paramètres à l'écran :

**Priority**: Entrez une valeur de priorité entre 0 et 19. Plus la valeur numérique est basse, plus la priorité de l'entrée est haute. Par exemple, 3 a une plus haute priorité que 5. Ces valeurs de priorité déterminent l'ordre de priorité de traitement des paquets.

**Destination MAC** : Il s'agit de l'adresse MAC de destination du paquet. Entrez l'adresse ou cliquez sur le bouton **Set Multicast** pour paramétrer l'adresse MAC Multicaste. Si l'adresse est paramétrée sur 00:00:00:00 ou qu'elle est laissée vide, ce champ est ignoré lorsque la vérification de transmission ou d'abandon du paquet est effectuée.

**Source MAC**: Il s'agit de l'adresse MAC source du paquet. Si l'adresse est paramétrée sur 00:00:00:00 ou qu'elle est laissée vide, ce champ est ignoré lorsque la vérification de transmission ou d'abandon du paquet est effectuée.

**Ethernet Type**: Entrez le type Ethernet au format hexadécimal. Par exemple, entrez 0800 pour l'adresse IP ou 0806 pour l'ARP.

**Interface** : Choisissez l'interface du paquet dans la liste déroulante Interface. Les options d'interface disponibles sont eth0, wlan0 et atm0.

**Action** : Choisissez Allow ou Deny pour autoriser ou interdire le passage du paquet.

**ETAPE 2** : Cliquez sur le bouton **Add** en bas de la page L2 Filter pour appliquer les paramètres.

## Suppression d'une entrée de filtre L2

Pour supprimer une entrée de filtrage L2, sélectionnez-la et cliquez sur le bouton

Delete en bas de la page L2 Filters.

## 6.6 IPQOS

QoS représente la capacité de performance du réseau pour offrir des applications utilisateur telles que voix, vidéo et données. La technologie QoS est essentielle pour garantir les performances optimales du réseau, particulièrement alors que les organisations intègrent rapidement des applications Internet essentielles pour communiquer pleinement avec leurs partenaires commerciaux, clients et personnel distant.

La qualité du service IP (IPQoS) se rapporte à la performance du flux de paquets IP à travers les réseaux. Son objectif est d'offrir une qualité de service totale au trafic utilisateur. Elle se caractérise par un petit ensemble de mesures, notamment la disponibilité du service, le délai des paquets, la gigue, la perte de paquets et le débit.

The screenshot shows a network configuration page for WFQ Traffic Conditioning. On the left is a navigation menu with links like 'Change Password', 'Link Status', 'WAN Setup', 'LAN Setup', 'WLAN Setup', 'Routing Setup', 'Save & Reboot', 'Erase & Reboot', 'VOIP', 'MGCP', 'Advanced', 'ADSL Mode', 'DHCP', 'Firewall', 'Configure', 'IGMP Proxy', 'Bridging', and 'IPQOS'. The main content area is titled 'WFQ Traffic Conditioning' and contains two sections:

**List of WFQ Traffic Parameters**

Traffic Type	Weights
Default	5
Low	5
Medium	5
High	5
Critical	5
Real Time	65
Premium	5
Urgent	5

Below the table is a 'Modify' button.

**List of WFQ Interfaces**

Select	If Name	Link Speed	Admission	Borrow	Ack	Priority	Default	Low	Medium	High	Critical	Real Time	Premium	Urgent
No WFQ Configured														

Below the table are 'Attach' and 'Remove' buttons.

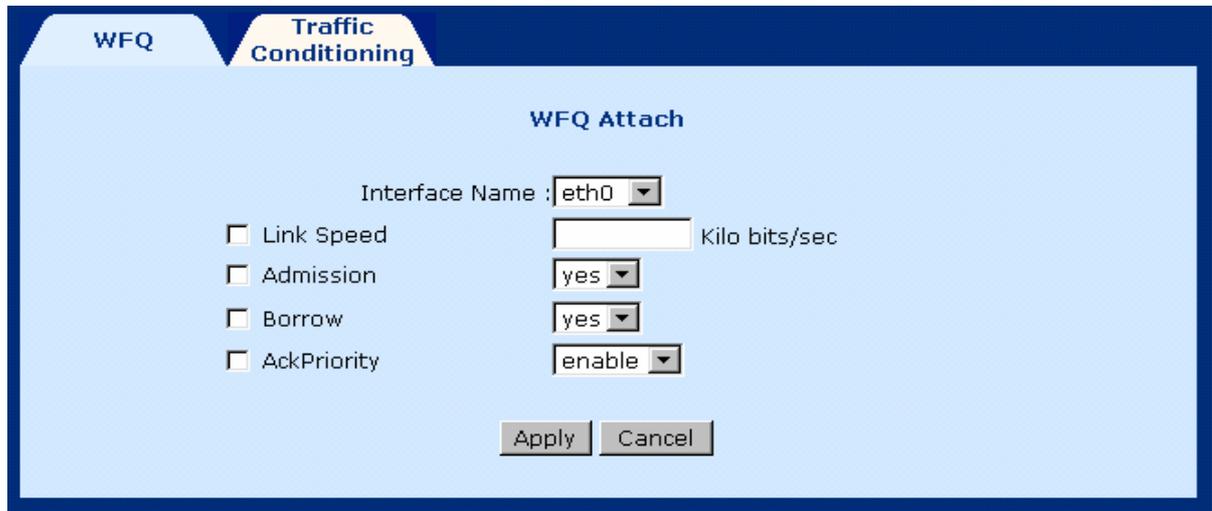
### 6.6.1 Configuration

La configuration de la QoS Ip se décompose en trois parties :

- Rattachement de l'interface de sortie (adsl0/mer0/eth0...)
- Création des différentes conditions de trafic
- Création d'une politique en attribuant une ID à l'action TC. Vous devez spécifier quel paquet utilise quel TC.

## ETAPE 1 : Rattachement de l'interface de sortie

L'interface de sortie signifie l'interface WAN. Pour configurer l'interface de sortie, cliquez sur IPQOS dans la barre de menu Attached. Sélectionnez le bouton **Attach**.



The screenshot shows a configuration window titled "WFQ Attach" with two tabs: "WFQ" and "Traffic Conditioning". The "WFQ Attach" tab is active. The configuration includes the following elements:

- Interface Name:** A dropdown menu currently set to "eth0".
- Link Speed:** A checkbox followed by an empty text input field and the label "Kilo bits/sec".
- Admission:** A checkbox followed by a dropdown menu set to "yes".
- Borrow:** A checkbox followed by a dropdown menu set to "yes".
- AckPriority:** A checkbox followed by a dropdown menu set to "enable".

At the bottom of the window are two buttons: "Apply" and "Cancel".

- **Interface Name :** L'interface de transmission est celle sur laquelle les données doivent être transmises. Trois options sont disponibles - eth0, usb0 et adsl0. L'option eth0 est l'interface Ethernet. Pour toutes les interfaces "atm" et "ppp", l'interface de transmission est fournie sous la forme "adsl0".
- **Link Speed:** L'option vitesse de liaison indique la bande passante totale en Ko par seconde. Il s'agit d'un paramètre facultatif et, si vous ne fournissez pas de valeur lors de la configuration, la valeur par défaut adoptée est le "débit en bauds de l'interface".
- **Admission :** La configuration de la bande passante peut être réalisée selon deux méthodes :

En choisissant l'option « no », la bande passante est configurée par l'intermédiaire des poids WFQ, soit le pourcentage de la bande passante totale pour les différentes classes de trafic, à la disposition de l'ordonnanceur.

**List of WFQ Traffic Parameters**

Traffic Type	Weights
Default	5
Low	5
Medium	5
High	5
Critical	5
Real Time	65
Premium	5
Urgent	5

En choisissant l'option « yes », la bande passante est configurée par l'intermédiaire du TC (Traffic Conditioning) pour différentes priorités de classes.

- **Borrow:** L'ordonnanceur de trafic travaille sur la base du « concept du déficit évalué sur une base prioritaire ». Drapeau Borrow utilisé pour permettre l'action de l'ordonnanceur de trafic si la bande passante inutilisée par une classe de trafic peut être employée par une autre classe lorsque la première ne l'utilise pas totalement. Pour obtenir les meilleurs résultats, la valeur recommandée pour ce paramètre est "yes"
- **AckPriority:** Ce paramètre est utile en cas de liaisons asymétriques, avec un flux montant et descendant différent. Par exemple, dans le cas où l'IPQOS de l'interface ADSL est nécessaire au niveau de l'interface montante mais pas de l'interface descendante, car l'entrée a moins de bande passante que la sortie (absence de congestion). Même lorsqu'une connexion TCP est utilisée pour envoyer des données uniquement dans une direction (comme le téléchargement de fichiers depuis par FTP). Les accusés de réception TCP (ACK) doivent être envoyés dans la direction opposée faute de quoi son pair considère que ses paquets sont perdus et les retransmet. Pour maintenir l'envoi de données du pair au débit maximum, il importe de renvoyer rapidement les ACK lorsque la liaison montante est saturée par d'autres connexions (un téléchargement par exemple), tous les paquets sortants sont retardés de façon homogène par défaut. Par conséquent, un téléchargement simultané saturant la liaison montante retarde la sortie des ACK, ce qui a pour effet de provoquer la baisse de débit du téléchargement entrant.

Les ACK sortants liés au téléchargement entrant sont modestes, car ils ne contiennent aucune charge de données. Ainsi, l'idée consiste à attribuer une priorité aux ACK TCP sans charge de données.

Dans le cas du TCP, la valeur recommandée pour ce paramètre est "yes"

## **ETAPE 2 : Création des conditions de trafic**

Cette étape définit la priorité de file d'attente du trafic. Sélectionnez l'onglet Traffic Conditioning dans l'écran IPQOS. Ajoutez une liste de conditionnement du trafic en cliquant sur le bouton **Add** et configurez les paramètres suivants.

**Marking (dfmark/dfnomark)** : Les paquets doivent être marqués au TC pour différents traitements de priorité et de bande passante. Le TC doit être créé avec des marquages comme dfmark pour fournir un traitement de bande passante et de priorité différent et en cas de marquage dfnomark tous les paquets passent par la classe par défaut et aucun traitement de bande passante ni de priorité n'est appliqué.

**Priority** : Identique à la classe de trafic, qui varie entre 0 et 7.

**Assured Bandwidth** : Il s'agit de la bande passante garantie ; une fois configurée, le trafic inférieur à la bande passante assurée n'est pas abandonné.

**Maximum Bandwidth** : Il s'agit de la bande passante maximale. Le trafic excédant la bande passante maximale est abandonné au TC et ne rejoint pas la file d'attente de l'ordonnanceur.

WFQ Traffic Conditioning

### Traffic Conditioning List

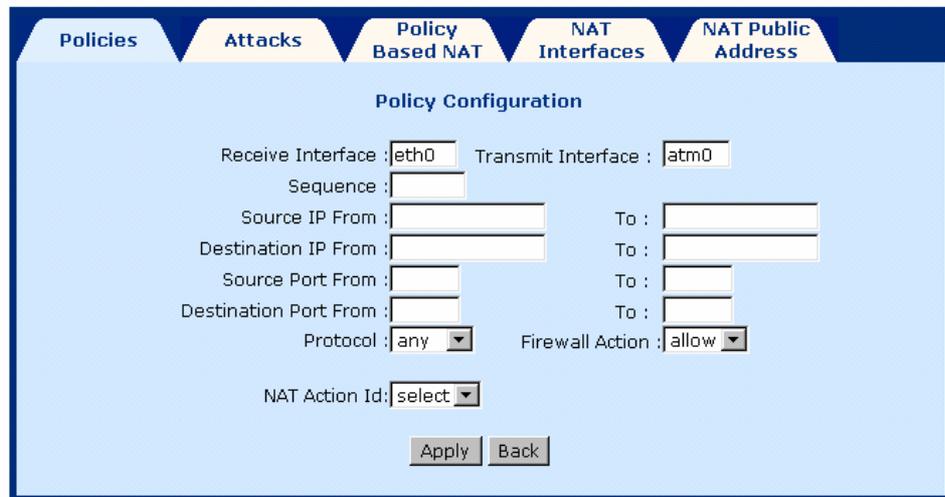
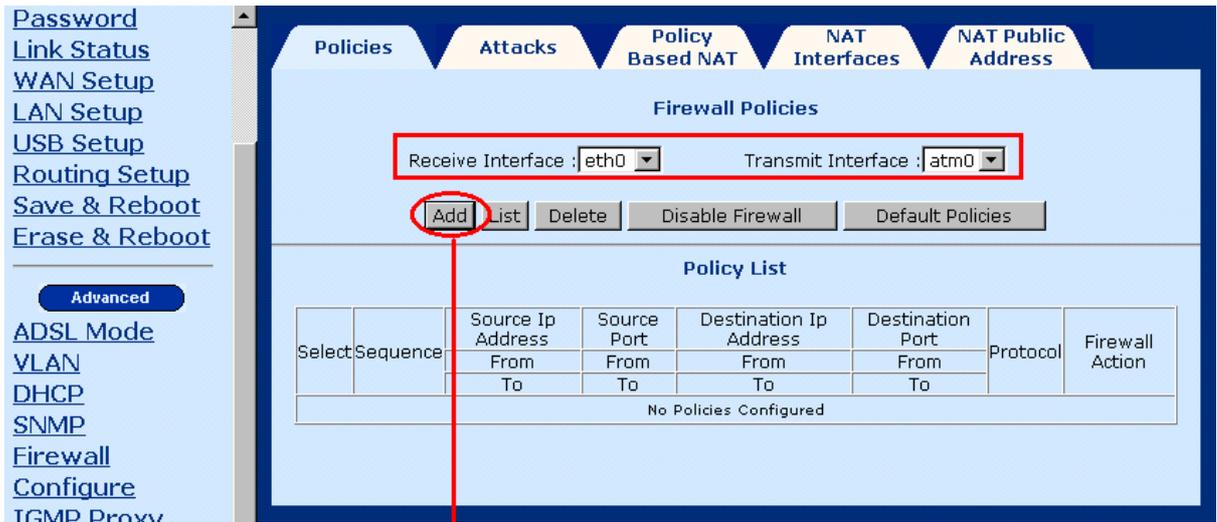
Select	Action Id	DF-Marking	Priority	Assured BW(kbps)	Maximum BW(kbps)
No Traffic Condition Configured					

WFQ Traffic Conditioning

### Traffic Conditioning

DF-Marking : dfmark   
Assured BW(Kbps) :  Priority : Low   
Maximum BW(Kbps) :

**ETAPE 3 :** Créez une entrée de politique. Cliquez sur Firewall dans la barre de menu Advanced. Choisissez l'interface de réception (any, eth0, usb0, mer0, atm0-atm7 et ppp0-ppp7) et l'interface de transmission. Cliquez sur Add pour configurer l'entrée. Entrez le numéro de séquence, l'adresse IP source/destination ou la plage IP, le port source ou la plage de ports, le protocole, l'action du pare-feu et l'ID d'action NAT.

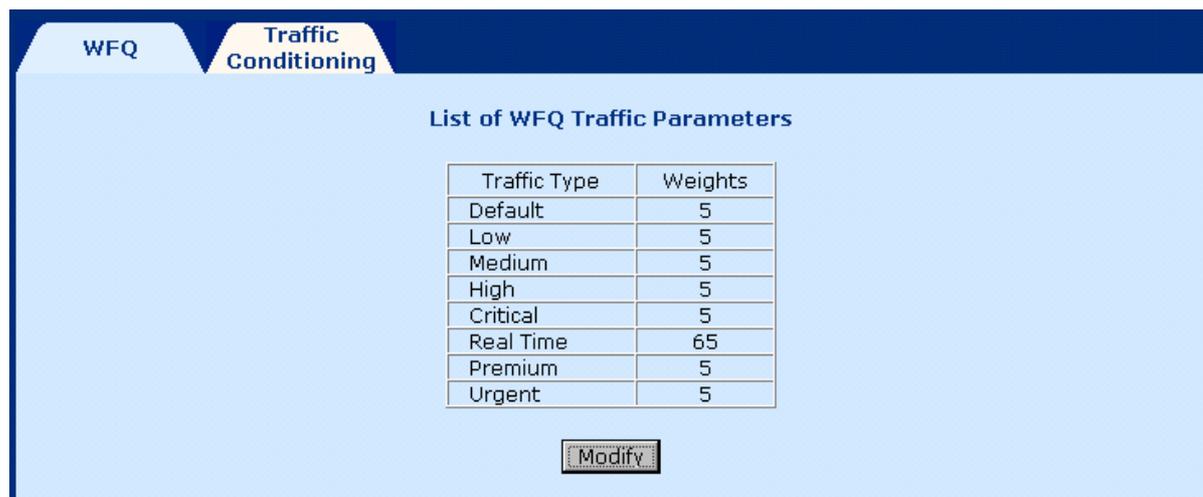


**ETAPE 4 :** Cliquez sur **Apply** pour configurer.

## 6.6.2 Poids WFQ

Les poids WFQ servent à fournir les informations de bande passante à l'ordonnanceur du trafic en cas d'admission "no". Le total des poids doit être 100 et les priorités se situent entre 0 et 7. Un pourcentage supérieur signifie davantage de bande passante.

L'écran suivant affiche la configuration des poids WFQ par défaut.



The screenshot shows a configuration interface with two tabs: 'WFQ' and 'Traffic Conditioning'. The 'Traffic Conditioning' tab is active. Below the tabs, the title 'List of WFQ Traffic Parameters' is displayed. A table lists various traffic types and their corresponding weights. Below the table is a 'Modify' button.

Traffic Type	Weights
Default	5
Low	5
Medium	5
High	5
Critical	5
Real Time	65
Premium	5
Urgent	5

Modify

Pour une meilleure qualité vocale, le trafic en temps réel a reçu le plus fort pourcentage de bande passante, qui peut être ajusté si données et voix coexistent.

### 6.6.3 Condition du trafic

Le conditionnement du trafic peut être déployé pour assurer la conformité au contrat de niveau de service (SLA) afin de fournir aux utilisateurs ultimes la qualité de service négociée. Le conditionnement du trafic est réalisé en le mesurant, par marquage Diff-Serv et contrôle de débit par rapport à la bande passante garantie et maximale.



#### Configuration des paramètres

**Marking (dfmark/dfnomark) :** Les paquets doivent être marqués au TC pour différents

traitements de priorité et de bande passante. Le TC doit être créé avec des marquages comme dfmark pour fournir un traitement de bande passante et de priorité différent et en cas de marquage dfnomark tous les paquets passent par la classe par défaut et aucun traitement de bande passante ni de priorité n'est appliqué.

**Priority :** Identique à la classe de trafic, qui varie entre 0 et 7.

**Assured Bandwidth :** Il s'agit de la bande passante garantie ; une fois configurée, le trafic inférieur à la bande passante assurée n'est pas abandonné. Pour le trafic excédant la bande passante assurée, le traitement bande passante/priorité par défaut est appliqué et l'ordonnanceur peut abandonner ou non ce paquet en fonction de la disponibilité de la bande passante du moment.

**Maximum Bandwidth :** Il s'agit de la bande passante maximale. Le trafic excédant la bande passante maximale est abandonné au TC et ne rejoint pas la file d'attente de l'ordonnanceur.

## 6.7 Statistiques du système

Pour afficher les statistiques du système, cliquez sur le bouton **System Statistics**, proche de la partie inférieure de la barre de menu. Les statistiques relatives aux Interfaces, TCP-IP, et DHCP-Lease sont enregistrées.

### 6.7.1 Statistiques de l'interface

Pour afficher les statistiques de l'interface, cliquez sur l'onglet **Interface**, situé en haut et à gauche de l'écran Statistics. La page Interface Statistics affiche les statistiques de toutes les interfaces. Les informations suivantes sont affichées :

Interface Name	Nom de l'interface.
Admin Status	Indique si l'interface est active ou inactive
Octets In	Nombre d'octets (bytes) reçus
Unicast PktsIn	Nombre de paquets unicast reçus
Broadcast PktsIn	Nombre de paquets de diffusion reçus
Discards In	Nombre de paquets reçus et supprimés
Errors In	Nombre d'erreurs entrantes
Octets Out	Nombre d'octets (bytes) transmis
Unicast PktsOut	Nombre de paquets unicast transmis
Broadcast PktsOut	Nombre de paquets de diffusion transmis
Discards Out	Nombre de paquets transmis et supprimés
Errors Out	Nombre d'erreurs sortantes

Interfaces		TCP-IP		DHCP-Lease		Interface Statistics					
Interface	Admin Status	Octets In	Unicast PktsIn	Broadcast PktsIn	Discards In	Errors In	Octets Out	Unicast PktsOut	Broadcast PktsOut	Discards Out	Errors Out
eth0	up	3145	41	0	0	0	2012	7	0	0	0
mer0	down	0	0	0	0	0	0	0	0	0	0
ph0	down	0	0	0	0	0	0	0	0	0	0
usb0	up	0	0	0	0	0	42	1	0	0	0
lo0	up	0	0	0	0	0	0	0	0	0	0
atm0	up	0	0	0	0	0	0	0	0	0	0
atm1	down	0	0	0	0	0	0	0	0	0	0
atm2	down	0	0	0	0	0	0	0	0	0	0
atm3	down	0	0	0	0	0	0	0	0	0	0
atm4	down	0	0	0	0	0	0	0	0	0	0
atm5	down	0	0	0	0	0	0	0	0	0	0
atm6	down	0	0	0	0	0	0	0	0	0	0
atm7	down	0	0	0	0	0	0	0	0	0	0
ppp0	down	0	0	0	0	0	0	0	0	0	0
ppp1	down	0	0	0	0	0	0	0	0	0	0
ppp2	down	0	0	0	0	0	0	0	0	0	0
ppp3	down	0	0	0	0	0	0	0	0	0	0
ppp4	down	0	0	0	0	0	0	0	0	0	0
ppp5	down	0	0	0	0	0	0	0	0	0	0
ppp6	down	0	0	0	0	0	0	0	0	0	0
ppp7	down	0	0	0	0	0	0	0	0	0	0

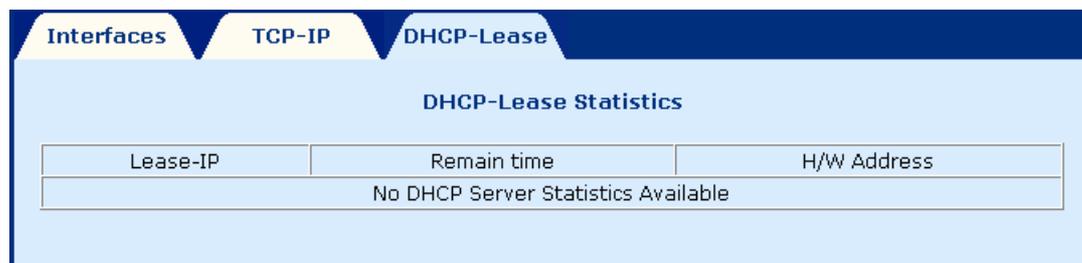
## 6.7.2 TCP-IP

Pour afficher les statistiques TCP-IP, cliquez sur l'onglet **TCP-IP**, situé en haut de la page System Statistics. La page TCP-IP affiche les statistiques IP, UDP, TCP et ICMP.

Interfaces		TCP-IP		DHCP-Lease	
<b>TCP-IP Statistics</b>					
<b>IP Statistics</b>					
In receives	32	In Errors	7	In Unknown Protos	0
Out Requests	32	Out Discards	0	Out No Routes	7
				Forwarded Datagrams	0
<b>Udp Statistics</b>					
Data grams In	0	Datagrams Out	0	Errors In	0
<b>Tcp Statistics</b>					
Active Opens	0	Passive Opens	4	Attempt Fails	0
Segments In	32	Segments Out	34	Segments retransmitted	0
				Current Establishments	1
				Errors In	0
<b>Icmp Statistics</b>					
<b>IN</b>					
Messages	1	Errors	0	Destination Unreaches	0
Source Quenches	0	Redirects	0	Echos	0
				Time Exceeds	0
				Echo Replys	0
<b>OUT</b>					
Messages	0	Errors	0	Destination Unreaches	0
Source Quenches	0	Redirects	0	Echos	0
				Time Exceeds	0
				Echo Replys	0

### 6.7.3 DHCP-Lease

Pour afficher les statistiques DHCP-Lease, cliquez sur l'onglet **DHCP-Lease**, situé en haut de la page System Statistics. La page DHCP-Lease indique les PC qui ont obtenu une adresse IP depuis le pool DHCP.



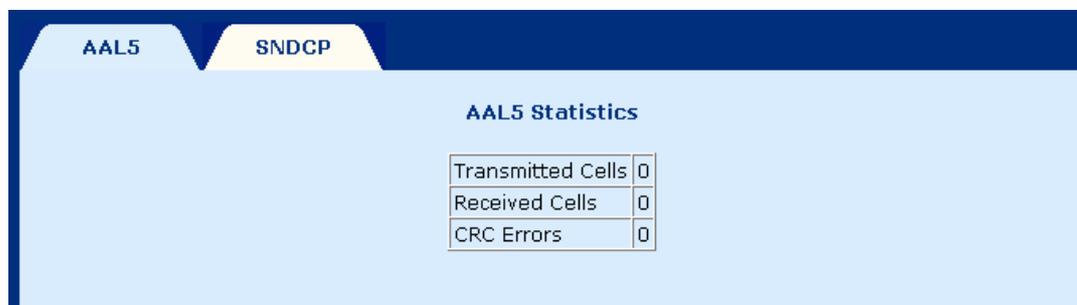
Lease-IP	Remain time	H/W Address
No DHCP Server Statistics Available		

## 6.8 Statistiques ATM

Cliquez sur **ATM Statistics** dans la barre de menu pour afficher les statistiques ATM. La page ATM Statistics contrôle les informations relatives à l'AAL5 et à l'encapsulation.

### 6.8.1 AAL5

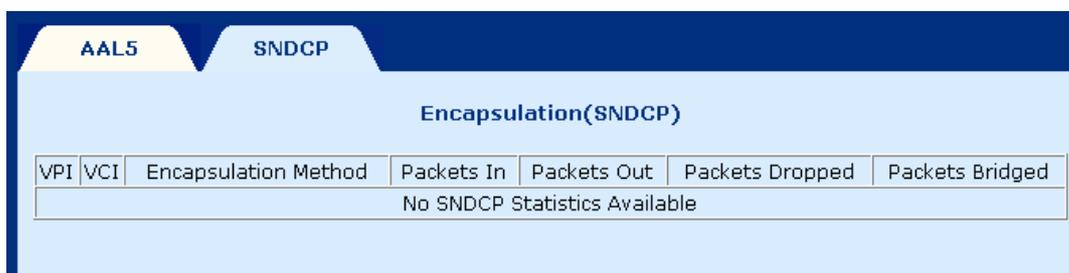
La page AAL5 affiche les statistiques AAL5.



AAL5 Statistics	
Transmitted Cells	0
Received Cells	0
CRC Errors	0

### 6.8.2 Encapsulation

Cliquez sur l'onglet **SNDCP** pour afficher les statistiques d'encapsulation. Cette page affiche les VC en cours d'exécution. (SNDCP signifie protocole de convergence des dépendances du sous-réseau).



VPI	VCI	Encapsulation Method	Packets In	Packets Out	Packets Dropped	Packets Bridged
No SNDCP Statistics Available						

## 6.9 Statistiques WFQ

Cliquez sur IPQOS pour afficher les statistiques WFQ.

The screenshot shows a network configuration interface. On the left is a sidebar with various configuration options. The main content area is titled 'WfqStats' and 'WFQ Statistics'. It contains a table with the following headers: Q.Name, Priority, Pkt-Sent, Pkt-Dropped, Byte-Sent, and Byte-Dropped. Below the table, a message states 'No Wfq Interface Available'.

[Change Password](#)  
[Link Status](#)  
[WAN Setup](#)  
[LAN Setup](#)  
[WLAN Setup](#)  
[Routing Setup](#)  
[Save & Reboot](#)  
[Erase & Reboot](#)

**VOIP**

[MGCP](#)

**Advanced**

[ADSL Mode](#)  
[DHCP](#)  
[Firewall](#)  
[Configure](#)  
[IGMP Proxy](#)  
[Bridging](#)  
[IPQOS](#)  
[System Statistics](#)  
[ATM Statistics](#)  
[IPQOS Statistics](#)

WfqStats

WFQ Statistics

Q.Name	Priority	Pkt-Sent	Pkt-Dropped	Byte-Sent	Byte-Dropped
No Wfq Interface Available					

## 6.10 Diagnostics

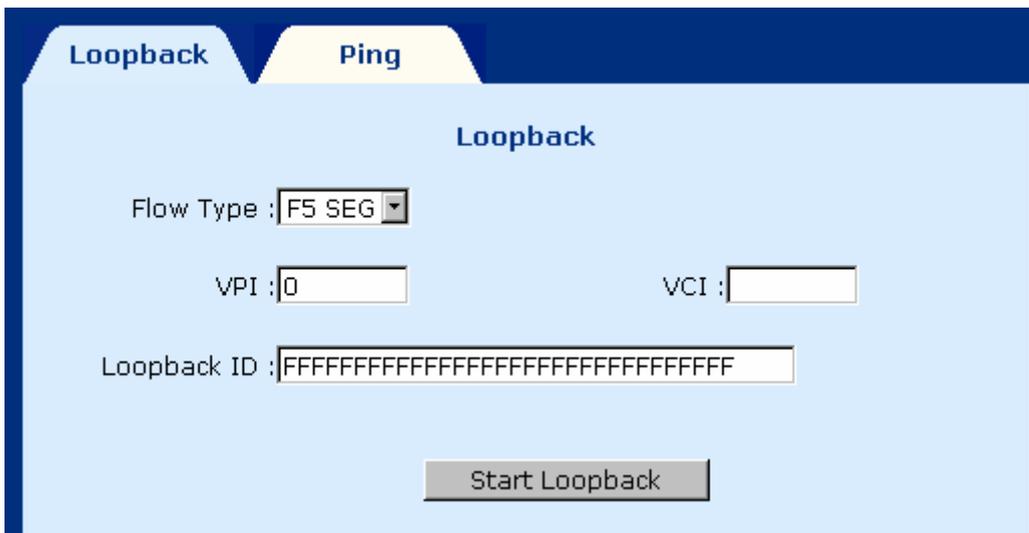
Pour accéder à l'écran de diagnostics, cliquez sur le bouton **Diagnostics** situé dans la barre de menu. L'écran Diagnostics compte deux fonctions de test : Test OAM Loopback et Ping.

### 6.10.1 OAM Loopback

**ETAPE 1** : Cliquez sur le bouton **Diagnostics** dans la barre de menu.

**ETAPE 2** : Cliquez sur l'onglet **Loopback** dans l'écran Diagnostics.

**ETAPE 3** : Entrez les informations suivantes pour exécuter le test OAM loopback :



- **Flow type:** F5 SEG (Segment à Segment) et F5 ETE (bout-en-bout). Le loopback **SEG** va de ATUR à DSLAM. Le loopback **ETE** va de ATUR à ISP RAS.
- **VPI et VCI** : Spécifiez le canal virtuel qui exécutera le test OAM loopback.
- **Loopback ID:** Tapez le modèle de loopback

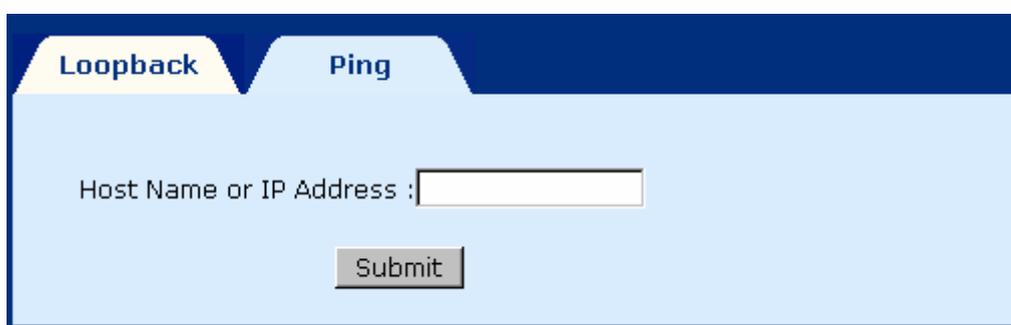
**ETAPE 4** : Cliquez sur le bouton **Start Loopback** en bas de l'écran.

## 6.10.2 Ping

Un test Ping est utilisé pour vérifier l'état d'une connexion réseau après activation de la fonction RIP ou route statique. Le Ping envoie un message de requête à l'hôte et attend un message en retour. Cette fonction de diagnostic peut vérifier si l'hôte distant est accessible. Le Ping peut aussi mesurer la durée de l'aller-retour vers l'hôte distant.

Pour accéder à l'écran de test Ping, cliquez sur l'onglet **Ping** dans l'écran diagnostic.

Complétez le champ **Host Name or IP address** du terminal distant et cliquez sur **Submit** pour démarrer le ping et afficher les résultats.



L'exemple qui suit est le résultat d'un test ping. Les informations sont les suivantes :

Packets transmitted:	Nombre de paquets transmis
Packets received:	Nombre de paquets reçus
Packets Loss (%)	Pourcentage de paquets perdus (transmis-reçus)
Minimum round trip time:	Durée minimum de l'aller-retour
Maximum round trip time:	Aller-retour le plus lent

Loopback

Ping

Host is alive

Ping Statistics	
Packets Transmitted	4
Packets Received	4
Packet Loss (%)	0
Minimum Round Trip Time (ms)	0
Maximum Round Trip Time (ms)	999

Back

## Chapter 7 Mise à jour du logiciel via FTP

Observez les étapes ci-après pour mettre à jour la version du microprogramme du CT-633 C via FTP. Les procédures ci-après utilisent l'adresse IP de port LAN 192.168.1.1 comme illustration.

**ETAPE 1 :** Connectez l' IAD à un PC à l'aide du câble LAN. Paramétrez le PC sur le même sous-réseau que l'IAD (192.168.1.1).

**ETAPE 2 :** Restaurez les paramètres par défaut du routeur sans fil en maintenant le bouton **Reset** de l'appareil enfoncé jusqu'à ce que la DEL **WLAN** commence à clignoter (environ 5 secondes). Une fois l'appareil réinitialisé, et si la connexion ADSL est établie, la DEL **WLAN** cesse de clignoter et la DEL ADSL s'allume en vert. En cas d'erreur, la DEL **ALARM** commence à clignoter en rouge.

**Remarque :** Vous pouvez aussi réinitialiser le routeur sans fil en exécutant le logiciel de l'appareil et en sélectionnant la commande **ERASE** du menu **Erase and Reboot**.

**ETAPE 3 :** Démarrez le DOS et accédez au menu où le microprogramme est installé :

Exemple : C:\Upgrade

**ETAPE 4 :** Entrez la commande : ftp 192.168.1.1 (adresse IP de l'IAD)

```
C:\>ftp 192.168.1.1
```

**ETAPE 5 :** A l'invite USER, tapez **root** (bas de casse)

```
Connected to 192.168.1.1.
220 Welcome to the update FTP server v1.0.
User (192.168.1.1:(none)): root
```

```
7.1.1.1.1.1.1.1.1
```

**ETAPE 6 :** A l'invite Password, tapez **1234**

```
331 Password required for root.
Password:
```

**ETAPE 7 :** Une fois le message **User Logged in** affiché, tapez : **Bin**



## Chapter 8 Annexe A : Spécifications

### Interface WAN

Norme ADSL ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ITU-T G.992.2,  
ANSI T1.413 Issue 2

G.992.3(ADSL2) Descendante : Jusqu'à 12 Mbps Montante : 1,3 Mbps

G.992,5(ADSL2) Descendante : Jusqu'à 24 Mbps Montante : 1,3 Mbps

### Interface LAN

Ethernet x 4, USB x 1

### Sans fil

Norme Compatibilité rétroactive avec 802.11b

Encryptage 64, 128 bits Encryptage de données Wired Equivalent Privacy  
(WEP)

Canaux 11 canaux (US, Canada)/ 13 canaux (Europe)/ 14 canaux  
(Japon)

Débit des données : Jusqu'à 54Mbps

Filtrage d'adresse MAC, WPA, IEEE 802.1x

Canal de bande passante 10, 25, 50, 100mW @ 22MHz, niveau de puissance de  
sortie sélectionné en fonction de l'environnement

### Interface analogique

FXS x 2, FXO x 1

### Attributs ATM

Pont RFC 2364, RFC 2684 (RFC 1483) ; route RFC 2684 (RFC 1483) ; RFC  
2516; RFC 1577

VC 8

Type de flux : AAL5

Classe de service ATM UBR/CBR/VBR

support ATM UNI UNI3.1/4.0

OAM F4/F5 Oui

### Gestion

SNMP, SNTP, ILMI 4.0, Telnet, gestion web, sauvegarde et restauration de  
configuration

Mise à jour du logiciel via client TFTP ou serveur FTP

### **Fonctions de pontage**

Pontage et apprentissage transparents	IEEE 802.1d
Algorithme de Spanning Tree	Oui
Proxy IGMP	Oui

### **Fonctions de routage**

Route statique, RIP et RIP v1,v2, NAT/PAT, DHCP Client/Serveur/Relais, DNS, ARP

### **Fonctions de sécurité**

Protocoles d'authentification PAP, CHAP,  
Caractéristiques VPN PPTP/L2TP/IpSec pass-through  
Stateful Packet Inspection, Packet filtering, Denial Of Service protection,  
Traffic Conditioning, WFQ-based Bandwidth  
Management, HTTP proxy

### **QoS**

QoS L3 politique, IP QoS, ToS

### **Fonctions Vocales**

SIP	RFC 3261
MGCP	RFC 3435
H.323	H.323 v3
Codec	G.711, G.723.1, G.729ab
RTP	RFC 1889
SDP	RFC 2327
ID appelant accroché/décroché	base ETSI
Ligne de vie	Oui
Annulation d'écho	G.168
Suppression de silence	Oui

### **Alimentation**

Adaptateur d'alimentation externe 110 Vac ou 220 Vac

### **Conditions environnementales**

Température d'exploitation	0 ~ 50 degrés Celsius
Humidité relative	5 ~ 90% (sans condensation)

**Dimensions**

205 mm (L) x 47 mm (H) x 145 mm (P)

## Chapter 9 Annexe B : Brochages

Port ligne (RJ11) :

Numéro de Broche	Définition	Numéro de Broche	Définition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

**Brochage du port RJ11**

Port LAN (RJ45)

Numéro de Broche	Définition	Numéro de Broche	Définition
1	Transmission de données +	5	NC
2	Transmission de données -	6	Réception de données -
3	Réception de données +	7	NC
4	NC	8	NC

**Brochage du port LAN**

## Chapter 10 Annexe C : Dépannage

Événement	Procédure de contrôle ou cause possible
Impossible d'accéder à la gestion web	Vérifiez la connexion LAN. Vérifiez le paramétrage TCP/IP de votre PC
Rejet du nom d'utilisateur	Vérifiez votre mot de passe. Le nom d'utilisateur par défaut est <b>root</b> ; le nom d'utilisateur n'est pas paramétré. Le nom d'utilisateur et le mot de passe sont sensibles à la casse.
La DEL POWER n'est pas allumée	Contrôlez l'adaptateur d'alimentation et vérifiez qu'il correspond aux exigences indiquées dans l'annexe A, Spécifications.
	Les branchements de l'alimentation sont desserrés ou mal connectés
	La source d'alimentation est éteinte.
Le port USB ne parvient pas à accéder à Internet	Vérifiez que le port LAN n'est pas connecté. Lorsque les ports LAN et USB sont connectés simultanément, seul le port LAN fonctionne.
	Vérifiez la connexion USB.
Impossible d'utiliser le logiciel de mise à jour automatique	Par défaut, l'IAD ne nécessite pas de mot de passe pour s'y connecter. En revanche, de la fonction de mise à jour automatique exige qu'un mot de passe soit défini.

## Chapter 11 Annexe D : GLOSSAIRE

**100BaseT** : Norme Ethernet 100 Mbps qui utilise un câblage en paire torsadée.

**10BaseT** : Norme Ethernet 10 Mbps qui utilise un câblage en paire torsadée

**adresse** : Symbole (généralement numérique) qui identifie une interface rattachée à un réseau.

**ADSL** : Forme asynchrone de DSL dans laquelle la bande passante disponible pour les connexions descendantes est beaucoup plus large que pour les connexions montantes.

**boucle analogique** : Un test dans lequel le signal vocal d'un modem est k à son récepteur.

**signal analogique** : Signal continuellement variable (comparé av numérique).

**Annexe A** : Partie de la norme G.992.1 se rapportant à l'ADSL sur POTS (ad par les USA).

**Annexe B** : Partie de la norme G.992.1 se rapportant à l'ADSL sur ISDN (ad par les USA).

**Annexe C** : Partie de la norme G.992.1 se rapportant à l'ADSL sur ISDN (ad par le Japon).

**ANSI** : American National Standards Institute.

**ASCII** : American Standard Code for Information Interchange.

**atténuation** : Perte de puissance d'un signal transmis pendant son parcours sur un câble.

**auto-summary** : Commande RIP pour restaurer le comportement par défaut de résumé auto des routes de sous-réseau dans les routes du niveau réseau.

**dorsale** : Circuit principal qui transporte les données avant d'être séparé en circuits étendus jusqu'à leur destination finale. Terme souvent utilisé en référence à la partie du réseau qui rejoint des LAN.

**bande passante** : Gamme de fréquences d'un canal de transmission. Plus la plage est large, plus haut est le débit auquel les données peuvent être envoyées. Par conséquent, le terme bande passante est également considéré comme l'expression du débit.

**Baud** : Un baud est un symbole (transition d'état ou transition de niveau) par seconde.

**BERT** : Bit Error Rate Test. Test qui compare un modèle reçu avec un modèle connu transmis pour en déterminer la qualité.

**Bit** : Chiffre binaire dont la valeur est -0 ou -1.

**démarrage** : Démarrer un appareil.

**Bps** : Bits par seconde. Vitesse à laquelle les bits sont transmis par une connexion de données.

**pont** : Dispositif qui relie des réseaux distants ou locaux et transmet des paquets sur la base d'une adresse MAC (comparé au routeur).

**large bande** : Canaux de communication fonctionnant à des débits supérieurs à 64 Kbps.

**diffusion** : Transmission simultanée vers plusieurs appareils de communication.

**BT** : Tolérance aux pointes. Paramètre de limite du GCRA (Generic Cell Rate Algorithm).

**tampon** : Stockage temporaire utilisé pour compenser une différence de débit des données.

**bus** : Ensemble de conducteurs qui transporte les signaux des appareils sur un chemin et qui fait office de connexion commune pour un groupe d'appareils liés.

**occupé** : Etat opérationnel d'un appareil, lorsqu'il est occupé par le traitement d'un appel.

**Octet** : Huit bits organisés en séquence

**canal** : Voie de communication bidirectionnelle entre un serveur hôte et un client.

**CHAP** : Challenge-Handshake Authentication Protocol. Protocole PPP pour garantir l'authentification de la connexion entre deux appareils.

**circuit** : Connexion logique entre deux appareils.

**CO** : Bureau central, centre d'échange téléphonique local, également appelé PSTN.

**Port COM** : Port de communication série d'un ordinateur.

**CPE** : Customer Premises Equipment. Equipement employé par l'utilisateur final.

**communication croisée** : Couplage indésirable du signal d'un circuit ou d'un canal avec un autre.

**débit des données** : Vitesse mesurée en bits par secondes à laquelle les données sont transférées sur la ligne du transporteur.

**Défaut** : Valeur d'origine prédéfinie.

**démodulation** : Récupération d'un signal depuis un transporteur modulé.

**Serveur DHCP** : Serveur qui attribue dynamiquement les adresses réseau et transmet les paramètres de configuration aux hôtes.

**DHCP** : Dynamic Host Configuration Protocol. Protocole TCP/IP qui permet à un réseau connecté à Internet d'attribuer automatiquement une adresse IP temporaire à un hôte lorsque celui-ci se connecte au réseau.

**signal numérique** : Signal discret ou discontinué où les états sont à intervalles discrets, tels que +10 volts et -10 volts. Ces états sont ensuite

représentés par les chiffres binaires 0 et 1.

**numérique : test loopback** : Test qui reconnecte la sortie du récepteur de l'appareil à l'entrée de l'émetteur. Ce test interrompt la transmission des données principales.

**DLL** : Dynamic Link Library. Les DLL sont des fichiers automatiquement chargés en mémoire en cas de besoin.

**DMT** : Discrete MultiTone. Système de modulation de la norme T1.413 pour la technologie DSL (Digital Subscriber Line).

**DNS** : Domain Name Server. Serveur qui conserve les adresses et les informations de routage des utilisateurs TCP/IP PAT.

**téléchargement descendant** : Réception d'un fichier par un réseau (voir téléchargement montant).

**pilote** : Module logiciel qui fournit une interface entre une carte d'interface réseau et le logiciel du protocole de couche supérieure exécuté sur un ordinateur.

**DSL** : Digital Subscriber Line. Famille de services à large bande fournis par l'intermédiaire d'une ligne téléphonique standard telle que ADSL, SHDSL et VDSL.

**DSP** : Digital Signal Processor. Microprocesseur qui traite la signalisation de ligne d'un modem.

**DTE** : Data Terminal Equipment. Equipement qui transmet ou réceptionne des données sous forme de signaux numériques.

**détection dynamique** : Processus de détection automatique d'un nouveau périphérique ajouté ou supprimé d'un PC.

**EOC** : Embedded Operations Channel. Canal de bande entre les dispositifs DSL qui fonctionne comme couche physique pour les données d'administration et de maintenance.

**contrôle d'erreur** : Algorithme utilisé pour détecter et corriger les erreurs de transmission de données.

**seconde erronée** : Élément du rapport de mesure de performances, concernant une période d'une seconde avec un ou plusieurs blocs erronés.

**adresse Ethernet** : Autre nom pour adresse MAC.

**Ethernet** : Protocole normalisé (IEEE 802.3) pour un bus de réseau local 10-Mo/bande de base (PAT) qui supporte les communications à haute vitesse entre les systèmes. Il fonctionne au niveau de la couche physique du modèle OSI.

**ETSI** : European Telecommunications Standards Institute.

**FCC** : Federal Communications Commission of the United States.

**filtre** : Configuration qui interrompt le flux de certains types de cadres de données.

**microprogramme** : Logiciel chargé temporairement ou de façon permanente dans la ROM.

**mémoire flash** : Type de RAM qui conserve ses informations, même après

coupure de l'alimentation.

**contrôle de débit** : Processus qui utilise des tampons pour arrêter et démarrer le débit des données dans un réseau pour éviter d'en perdre et qui permet à des appareils dotés de systèmes de transmission différents de communiquer entre eux.

**FTP** : File Transfer Protocol. Protocole TCP/IP normalisé de transfert de fichiers.

**full-duplex** : transmission simultanée dans deux directions.

**G.991.2** : Spécification ITU-T pour DSL à haute vitesse appelée G.SHDSL.

**G.DMT** : Autre nom de la spécification G.99200.1 ITU.

**G.lite** : Autre nom de la spécification G.9920.2 ITU.

**passerelle** : Dispositif de communications qui relie deux réseaux différents.

**en-tête** : Début d'un cadre ou d'une cellule contenant les informations de gestion et d'adressage.

**hop** : L'une des transmissions point à point d'une série, nécessaire pour transmettre un message entre deux hôtes d'un réseau.

**hôte** : Ordinateur adressable connecté à un réseau.

**hub** : Dispositif qui sert d'emplacement central pour brancher les câbles des postes de travail.

**ICMP** : Internet Control Management Protocol. Protocole Internet qui permet le générer des messages d'erreur, des paquets test et des messages d'informations liés à l'IP.

**IDSL** : Forme de DSL ISDN utilisant le code ligne 2B1Q.

**IEEE** : Institute of Electrical and Electronics Engineers.

**IEEE** : Institute of Electrical and Electronics Engineers.

**ILMI** : Interim Local Management Interface. Permet la gestion de la couche ATM entre un commutateur et un appareil client.

**adresse IP** : Adresse de protocole Internet. Adresse décimale-numérique de longueur fixe attribuée à un hôte Internet.

**IP multicaste** : Technique qui permet la transmission simultanée des paquets sur l'Internet vers plusieurs destinations.

**IPOA** : IP sur ATM.

**IRQ** : Requête d'interruption, une interruption matérielle sur un PC.

**ISO** : International Standards Organization.

**ISP** : Fournisseur de service Internet (FAI). Entreprise qui fournit l'accès à l'Internet.

**ITU** : International Standards Organization. Agence de télécommunications des Nations Unies.

**kbps** : Signifie littéralement Kilobits par seconde, mais signifie généralement 1,024 bits par seconde.

**LAN** : Local Area Network. Un LAN est un système de communication de données situé dans une zone limitée dans l'espace, avec un groupe d'utilisateur et une topologie spécifiques.

**latence** : Temps nécessaire à la transmission d'un signal entre sa source et sa destination.

**DEL** : Diode d'émission lumineuse. Voyant lumineux ou indicateur d'état.

**LOC** : Loss of Cell delineation. Situation dans laquelle l'équipement de réception est incapable d'identifier les limites d'une cellule.

**loopback local analogique** : Un test dans lequel le signal VF du modem est bouclé à son récepteur.

**boucle locale** : Ligne téléphonique ordinaire.

**test loopback local** : Un loopback analogique est un test qui re-boucle la sortie du récepteur de l'appareil à l'entrée de l'émetteur.

**loopback** : Procédure de diagnostic dans laquelle un message test est envoyé à son point d'origine, dans le but d'isoler un problème d'équipement ou de ligne de données.

**LOS** : Loss of Signal. Etat d'une ligne numérique sans impulsion.

**adresse MAC** : Adresse Media Access Control. Adresse fixe unique d'un appareil, généralement définie en usine et utilisée dans les protocoles PAT.

**MAC** : Medium Access Control, protocole qui permet de déterminer quel appareil peut accéder au réseau à tout moment.

**Mbps** : Mégabits par seconde. Un mégabit compte 1 048 576 (10242) bits.

**MCU** : Multi-Commercial Unit. Bâtiment commercial ou complexe avec plusieurs locataires.

**MDU** : Multi-Dwelling Unit. Bâtiment résidentiel avec plusieurs locataires.

**MIB II** : MIB Version 2. Mise à jour de la norme MIB définie par RFC 1213.

**MIB** : Management Information Base. Base de données d'objets gérés utilisés par les protocoles de gestion de réseau pour permettre la gestion des informations de réseau et le contrôle des dispositifs.

**modem** : Modulateur Démodulateur. Appareil utilisé pour convertir un signal numérique et signal analogique et vice-versa et permettre la transmission de données par l'intermédiaire d'une ligne téléphonique.

**modulation** : Processus de variation d'amplitude, de fréquence ou de phase d'une onde de transport pour former les transmissions de données.

**multicasting** : Capacité d'un nœud de réseau à envoyer les mêmes données à plusieurs terminaux.

**multiframe** : Séquence de cadres ordonnée et fonctionnelle sur un circuit numérique multiplexé.

**NAT** : Network Address Translation est une fonction de routage transparente qui translate une adresse IP privée sur un PAT en une adresse publique utilisable sur un réseau public.

**adresse réseau** : Partie réseau d'une adresse IP.

**protocole réseau** : Les protocoles réseau encapsulent et transmettent des paquets de données entre deux interfaces.

**NIC** : Une carte interface réseau est une carte installée dans un appareil pour permettre les communications à partir et vers cet appareil.

**nœud** : Point de connexion ou de commutation dans un réseau, également appelé hôte.

**bruit** : Interférence indésirable de source extérieure avec un signal transmis.

**PAP** : Password Authentication Protocol. Protocole PPP qui assure l'authentification de la connexion entre deux appareils.

**PAT** : Port Address Translation. Forme de NAT qui mappe plusieurs adresses IP privées sur une seule adresse IP.

**ping** : Signal Internet utilitaire envoyé pour vérifier l'accessibilité d'un appareil.

**Plug-and-Play** : Capacité d'un PC à configurer automatiquement des cartes d'extension et d'autres périphériques sans que l'utilisateur soit contraint d'arrêter le système pendant l'installation.

**connexion point à point** : Toute connexion dotée uniquement de deux terminaux. Liaison de données qui connecte uniquement deux postes.

**poison reverse** : Commande de protocole de routage qui indique aux passerelles voisines que l'une d'entre elles n'est plus connectée.

**POP** : Point Of Presence. Point de présence.

**Port** : Point d'accès où les données peuvent entrer ou sortir.

**POTS** : Plain Old Telephone Service. Service téléphonique ordinaire.

**PPP sur ATM** : Protocole point-à-point sur mode de transfert asynchrone.

**PPP** : Protocole point-à-point. Protocole (RFC 1661) de transmission de paquets sur des liaisons série entre des appareils provenant d'un même constructeur ou de constructeurs différents.

**PPPoE** : Protocole point-à-point sur Ethernet. Méthode d'établissement de sessions et d'encapsulation de paquets PPP sur un Ethernet, spécifiée par RFC 2516.

**PPTP** : Point-to-Point Tunneling Protocol Extension de protocole point-à-point utilisée pour créer des réseaux virtuels entre des PC.

**protocole** : Ensemble de règles qui gouvernent la transmission de données entre des appareils interconnectés pour maintenir ou améliorer la communication.

**serveur proxy** : Fournit la liste des éléments disponibles sur d'autres serveurs pour augmenter la disponibilité et la vitesse de récupération de ces informations.

**PSTN** : Public Switched Telephone Network. Réseau téléphonique normal.

**PVC** : Permanent Virtual Circuit. Circuit virtuel établi de façon permanente.

**QoS** : Qualité du service. Perte de données ou latence attendue.

**accès distant** : Communication depuis un emplacement ou une installation distant par l'intermédiaire d'une liaison de données.

**test loopback numérique distant** : Ce test re-boucle la sortie du récepteur numérique à l'entrée de l'émetteur.

**hôte distant** : Ordinateur qui reçoit les commandes du réseau.

**RFC** : Request for Comments. Documents publiés par Internet Engineering Task Force en relation avec les protocoles et les politiques Internet.

**RIP** : Routing Information Protocol. Protocole qui régit l'échange d'informations de routage.

**RJ11** : Prise à 6 broches utilisée avec les réseaux et les combinés téléphoniques à numérotation.

**RJ45** : Prise à 8 broches utilisée avec les réseaux à numérotation programmable.

**routeur** : Périphérique assujéti à protocole qui connecte des sous-réseaux entre eux. Les routeurs fonctionnent au niveau de la couche réseau (couche 3) de l'interconnexion du modèle de référence ISO (Open Systems Interconnection).

**table de routage** : Table qui indique les chemins de routage pour permettre à un nœud d'acheminer le trafic vers un autre nœud du réseau.

**RS-232** : interface DCE/DTE basse vitesse 25 broches.

**serveur** : matériel ou logiciel qui offre un service spécifique, gestion de base de données par exemple, à un client.

**SHDSL** : Symmetric High Bit Rate Digital Subscriber Loop. Technologie DSL qui permet des transmissions symétriques sur longues distances. Définie par la norme G991.2 ITU.

**SLA** : Service Level Agreement. Contrat entre un prestataire de service et un client, qui garantit un niveau minimal ou une qualité de service au client.

**SMTP** : Simple Mail Transport Protocol. Protocole utilisé pour transférer les messages électroniques entre ou parmi les serveurs.

**agent SNMP** : Programme d'application qui permet la communication entre un système de gestion et un périphérique.

**piège SNMP** : Message envoyé à un gestionnaire SNMP pour communiquer des informations relatives aux changements sur le réseau, la réinitialisation d'un périphérique par exemple.

**SNMP** : Simple Network Management Protocol. Protocole de gestion en réseau ouvert.

**route statique** : Route permanente par opposition à une route attribuée dynamiquement par un autre routeur.

**STP** : Shielded Twisted Pair. Câble téléphonique protégé par une gaine pour éliminer les interférences externes.

**adresse de sous-réseau** : Partie sous-réseau d'une adresse IP.

**masque de sous-réseau** : Numéro qui identifie la partie sous-réseau

d'une adresse réseau, de sorte que les adresses IP puissent être partagées sur un réseau local.

**sous-réseau** : Segment de réseau indépendant, c'est-à-dire dont l'adresse réseau est identique mais l'adresse de sous-réseau est différente.

**commutateur** : Un commutateur de données connecte des périphériques informatiques aux ordinateurs hôtes et permet à plusieurs périphériques de partager un nombre de ports limité. Un commutateur électrique est un dispositif qui permet d'établir, d'interrompre ou de changer les connexions d'un circuit électrique.

**transmission synchrone** : Transmission avec l'émetteur et le récepteur synchronisés afin que les données soient transmises avec un débit fixe.

**synchrone** : Toute opération contrôlée par une horloge ou un mécanisme de temporisation. (*Par comparaison avec asynchrone*).

**TCP/IP** : Transmission control protocol/Internet protocol, un ensemble de protocoles qui régissent les fonctions de connectivité paire-à-paire pour les réseaux locaux et étendus.

**TCP** : Transmission Control Protocol.

**Telnet** : Protocole virtuel TCP/IP qui permet à l'utilisateur d'un site d'accéder à un système distant sur un autre site.

**débit** : Nombre de bits, de caractères ou de blocs qui peuvent passer par un système de communication de données.

**apprentissage** : Processus où deux modems tentent de déterminer les protocoles et les vitesses de transmission correctes pour établir une session de communication.

**modulation par codage en treillis** : Technique de codage avancée de correction d'erreur pour transmettre une correction d'erreur à un système de modulation en ajoutant un bit supplémentaire à chaque baud.

**UDP** : User Datagram Protocol. Protocole sans connexion qui convertit les messages de données générés par une application en paquets à envoyer par IP.

**UNIX** : Système d'exploitation développé par les laboratoires AT&T Bell.

**téléchargement montant** : Pour recevoir un fichier transmis sur un réseau.

**URL** : Uniform Resource Locator. Protocole d'adressage Internet standard pour décrire l'emplacement d'une ressource sur Internet et la méthode pour y accéder.

**USB** : Universal Serial Bus. Interface série bidirectionnelle, isochrone pour ajouter des périphériques raccordés dynamiquement sans redémarrage.

**UTP** : La paire torsadée non blindée est le type de câblage téléphonique en cuivre le plus courant.

**VC** : Virtual Circuit. Connexion logique ou mécanisme de commutation de paquets établi entre deux périphériques au début d'une transmission.

**VCI** : Virtual Channel Identifier. Champ de 16 bits dans un en-tête de cellule ATM qui spécifie le canal virtuel sur lequel la cellule doit être transmise.

**VDSL** : Very-high-speed DSL. Protocole DSL exécuté jusqu'à 52 Mbps, limité à de courtes distances.

**circuit virtuel** : Circuit logique établi entre deux périphériques au début d'une transmission.

**VOD** : Video On Demand. Service vidéo à la demande pour les abonnés.

**VPI** : Virtual Path Identifier

**VPI** : Virtual Path Identifier. Champ de 8 bits dans l'en-tête d'une cellule ATM qui spécifie le chemin de routage d'une cellule.

**VPN** : Virtual Private Network. Réseau mis en œuvre sur un réseau public, rendu « privé » par cryptage.

**VT100** : Terminal utilisé pour des communications asynchrones.

**WAN** : Wide area network. Réseau de communications qui connecte des zones géographiquement séparées (par comparaison au LAN).

**xDSL** : Terme générique pour tous les types de DSL.

**XOFF** : Caractère qui notifie à un périphérique de stopper l'émission de données.

**XON** : Caractère qui notifie à un périphérique de commencer l'émission de données.