DrayTek

Guide d'utilisation des routeurs de sécurité à deux ports WAN Vigor2910

Version : 2.1

Date : 15/08/2006

Table des matières

1 Préambule

Le routeur série Vigor2910 a deux ports WAN pour fiabiliser la connexion internet. Le LAN sans fil prend en charge un plus grand nombre de fonctionnalités de sécurisation et la vitesse de transmission peut atteindre 108 Mbit/s (SuperG™). Le pare-feu à objets est souple et sécurise votre réseau. De plus, avec la fonction VoIP, vous pouvez réduire vos coûts de communication longue distance.

1.1 Boutons du configurateur web

Les principaux boutons qui apparaissent sur les pages web sont les suivants :

OK	Enregistre et valide les paramètres actuels.
Annuler	Annule les paramètres actuels et rétablit ceux enregistrés précédemment.
Éffacer	Efface les paramètres actuels pour permettre à l'utilisateur de les redéfinir.
Ajouter	Ajoute de nouveaux paramètres pour l'élément spécifié.
Éditer	Modifie les paramètres pour l'élément sélectionné.
Supprimer	Supprime l'élément sélectionné avec les paramètres correspondants.

Nota : pour ce qui est des autres boutons apparaissant sur les pages web, reportez-vous au Chapitre 4.

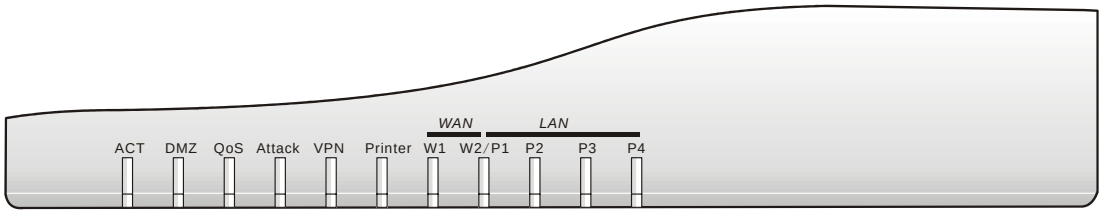
1.2 Voyants lumineux, prises et interfaces

Avant d'utiliser le routeur Vigor, faites connaissance avec les voyants lumineux, les prises et les interfaces.

Il y a de légères différences selon les routeurs.

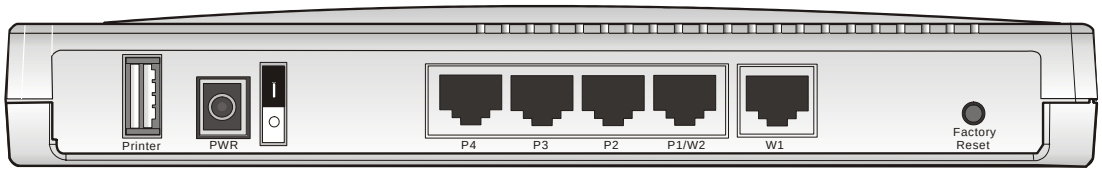
1.2.1 Vigor2910

Explication des voyants



Voyant	État	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint
DMZ	Allumé	Un hôte DMZ est spécifié sur certains sites.
QoS	Allumé	La fonction QoS est active.
	Éteint	La fonction QoS est inactive.
Attack	Allumé	La fonction de protection anti-DoS est active.
	Clignotant	Une attaque est détectée.
VPN	Allumé	Le tunnel de VPN est ouvert.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

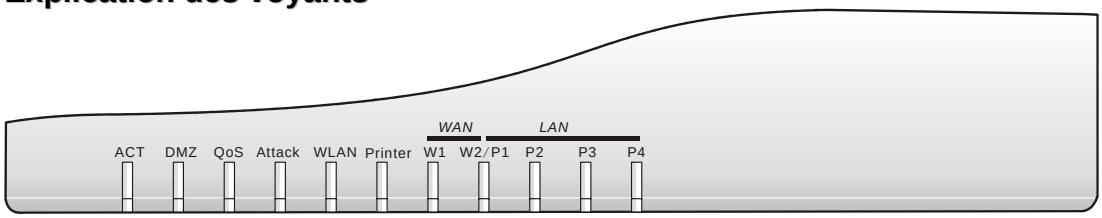
Explication des branchements



Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
I/O	Interrupteur marche-arrêt.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

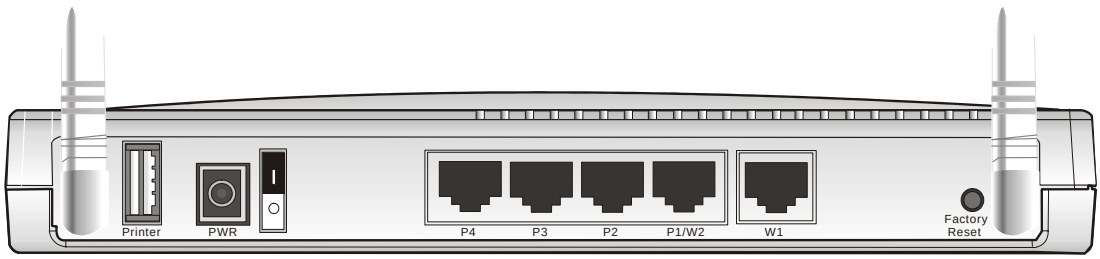
1.2.2 Vigor2910G

Explication des voyants



Voyant	État	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint.
DMZ	Allumé	Un hôte DMZ est spécifié sur certains sites.
QoS	Allumé	La fonction QoS est active.
	Éteint	La fonction QoS est inactive.
Attack	Allumé	La fonction de protection anti-DoS est active.
	Clignotant	Une attaque est détectée.
WLAN	Allumé	Le point d'accès sans fil est prêt.
	Clignotant	Transit de trafic radio.
	Éteint	Le point d'accès sans fil est éteint.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission.
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

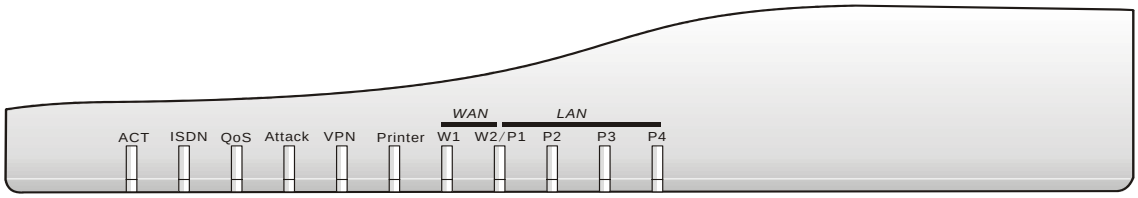
Explication des branchements



Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
I/O	Interrupteur marche-arrêt.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

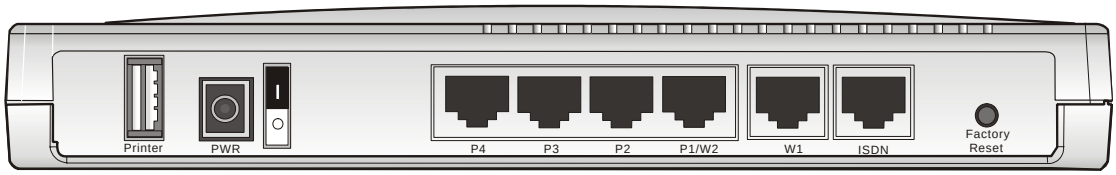
1.2.3 Vigor2910i

Explication des voyants



Voyant	État	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint
ISDN	Allumé	Le réseau RNIS est configuré correctement.
	Clignotant	Connexion réussie sur le canal B1/B2 de l'interface au débit de base (BRI) RNIS.
QoS	Allumé	La fonction QoS est active.
	Éteint	La fonction QoS est inactive.
Attack	Allumé	La fonction de protection anti-DoS est active.
	Clignotant	Une attaque est détectée.
VPN	Allumé	Le tunnel de VPN est ouvert.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

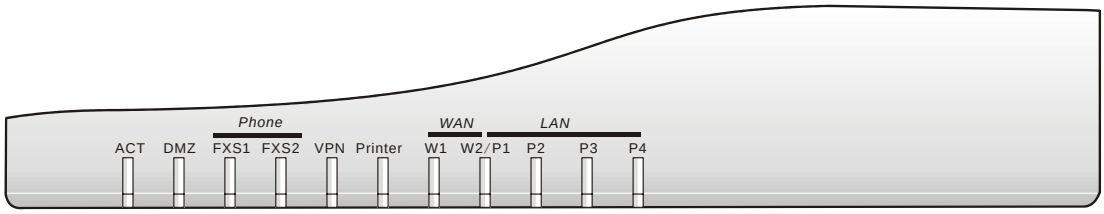
Explication des branchements



Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
I/O	Interrupteur marche-arrêt.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
ISDN	Branchement du boîtier NT1 (ou NT1+) fourni par le fournisseur de service RNIS.
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

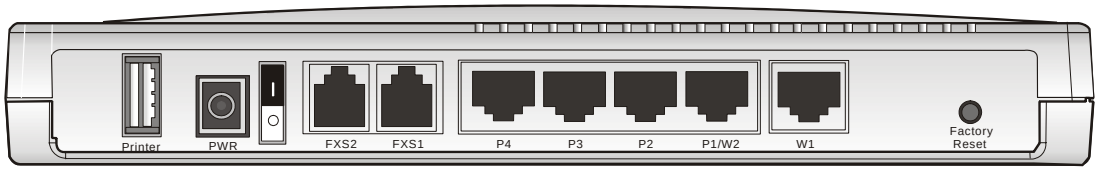
1.2.4 Vigor2910V

Explication des voyants



Voyant	Éteint	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint.
DMZ	Allumé	Un hôte DMZ est spécifié sur certains sites.
FXS1/FXS2	Allumé	Le téléphone est décroché.
	Clignotant	Arrivée d'un appel téléphonique ou en ligne.
VPN	Allumé	Le tunnel de VPN est ouvert.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

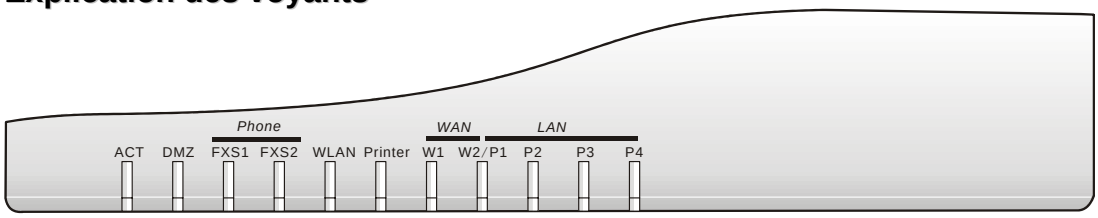
Explication des branchements



Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
I/O	Interrupteur marche-arrêt.
FXS2 & FXS1	Branchement de téléphones analogiques pour les communications VoIP.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

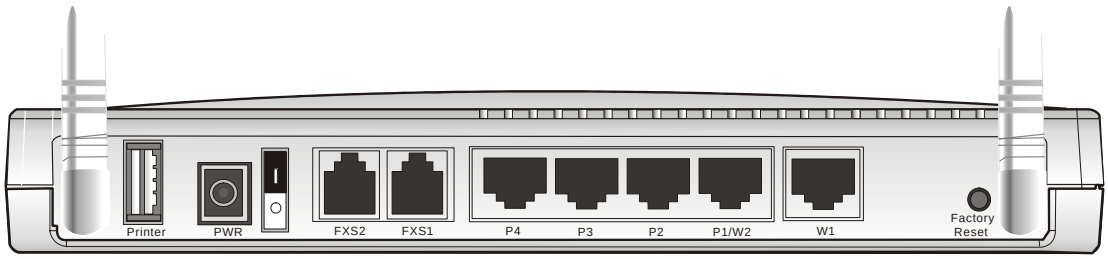
1.2.5 Vigor2910VG

Explication des voyants



Voyant	Éteint	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint.
DMZ	Allumé	Un hôte DMZ est spécifié sur certains sites.
FXS1/FXS2	Allumé	Le téléphone est décroché.
	Clignotant	Arrivée d'un appel téléphonique ou en ligne.
WLAN	Allumé	Le point d'accès sans fil est prêt.
	Clignotant	Transit de trafic radio.
	Éteint	Le point d'accès sans fil est éteint.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

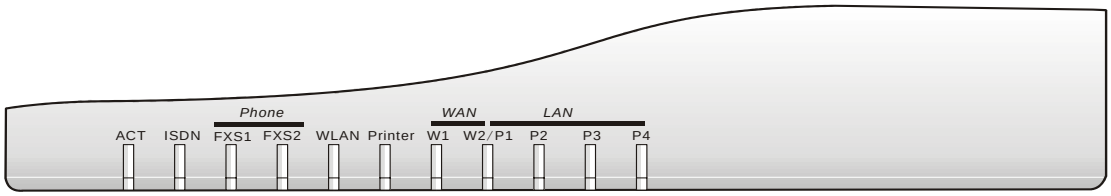
Explication des branchements



Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
ON/OFF	Interrupteur marche-arrêt.
FXS2 & FXS1	Branchement de téléphones analogiques pour les communications VoIP.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

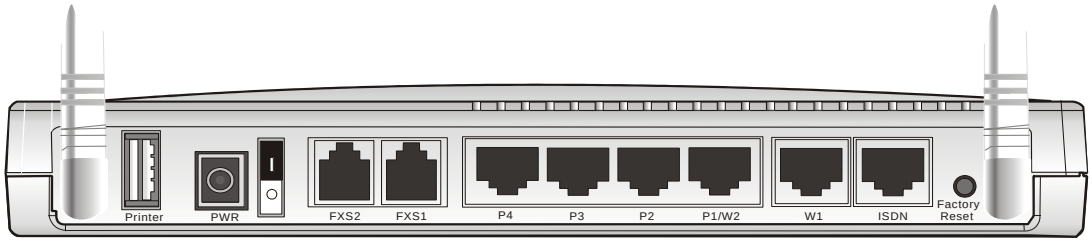
1.2.6 Vigor2910VGi

Explication des voyants



Voyant	Éteint	Explication
ACT (activité)	Clignotant	Le routeur est allumé et fonctionne correctement.
	Éteint	Le routeur est éteint.
ISDN	Allumé	Le réseau RNIS est configuré correctement.
	Clignotant	Connexion réussie sur le canal B1/B2 de l'interface au débit de base (BRI) RNIS.
FXS1/FXS2	Allumé	Le téléphone est décroché.
	Clignotant	Arrivée d'un appel téléphonique ou en ligne.
WLAN	Allumé	Le point d'accès sans fil est prêt.
	Clignotant	Transit de trafic radio.
	Éteint	Le point d'accès sans fil est éteint.
Printer	Allumé	L'imprimante reliée à l'interface USB est prête.
WAN(W1-W2)	Orange	Une liaison WAN 10 Mbit/s normale est prête.
	Vert	Une liaison WAN 100 Mbit/s normale est prête.
	Clignotant	Des paquets Ethernet sont en cours de transmission
LAN (P1, P2, P3, P4)	Orange	Une connexion normale 10 Mbit/s est établie sur le port correspondant.
	Vert	Une connexion normale 100 Mbit/s est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

Explication des branchements



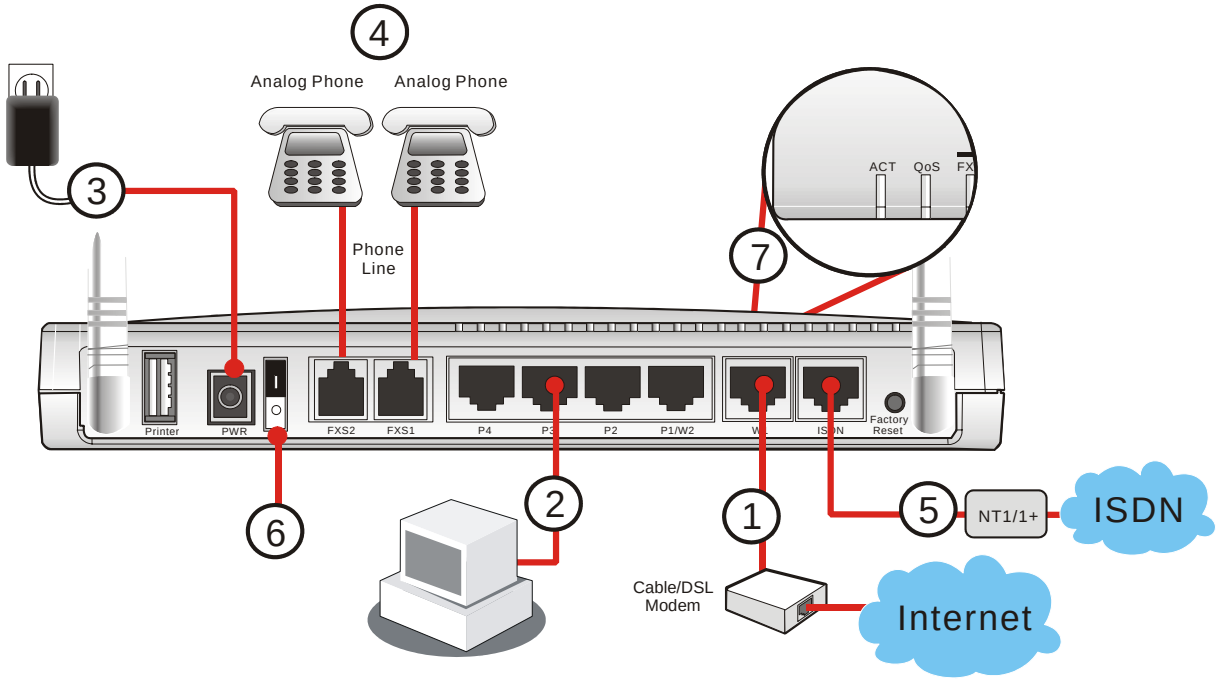
Interface	Description
Printer	Prise pour une imprimante USB.
PWR	Prise pour un adaptateur secteur 12 à 15 V DC.
ON/OFF	Interrupteur marche-arrêt.
FXS2 & FXS1	Branchement de téléphones analogiques pour les communications VoIP.
LAN P4 – P1	Branchement des équipements du réseau local.
W2/W1	Branchement de la ligne ADSL, ADSL2/2+
ISDN	Branchement du boîtier NT1 (ou NT1+) fourni par le fournisseur de service RNIS.
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.

1.3 Installation du matériel

Avant de commencer à configurer le routeur, vous devez raccorder correctement les différents équipements.

1. Reliez ce routeur à un routeur/modem avec un câble Ethernet.
2. Reliez l'un des ports du commutateur 4 ports à votre ordinateur avec un câble RJ-45. Vous pouvez relier directement 4 PC à ce routeur.
3. Enfoncez la fiche du câble d'alimentation dans la prise PWR du routeur et branchez l'autre extrémité sur la prise de courant secteur.
4. Branchez les téléphones analogiques avec des câbles téléphoniques (pour pouvoir utiliser la fonction VoIP). Si votre modem n'a pas de ports VoIP, sautez cette étape.
5. Branchez le boîtier RNIS NT1/1+ avec un câble RNIS. Europe seulement.
6. Allumez le routeur.
7. Vérifiez l'état des voyants **ACT** LED.

(Pour une explication détaillée des indications fournies par les voyants lumineux, reportez-vous à la section 1.1.)



Analogue Phone	*Téléphone analogique*
Phone Line	*Câble téléphonique*
Cable/DSL Modem	*Modem câble ADSL*
Internet	*internet*
ISDN	*RNIS*

Attention : chacun des ports FXS ne peut être utilisé que pour le raccordement d'un seul téléphone analogique. Ne reliez pas les ports FXS à la prise téléphonique murale. Cela risque d'endommager votre routeur.

2 Configuration de base

Pour pouvoir utiliser correctement le routeur, vous devez modifier le mot de passe d'accès au configurateur web et définir les paramètres de base.

Ce chapitre explique comment configurer un mot de passe d'administrateur et comment définir les paramètres de base pour pouvoir accéder à l'internet avec succès. Seul l'administrateur peut modifier la configuration du routeur.

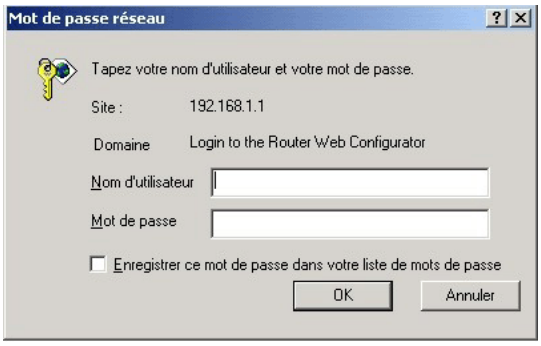
2.1 Changement de mot de passe

Pour changer le mot de passe d'accès au configurateur web du routeur, vous devez d'abord accéder à celui-ci avec le mot de passe par défaut.

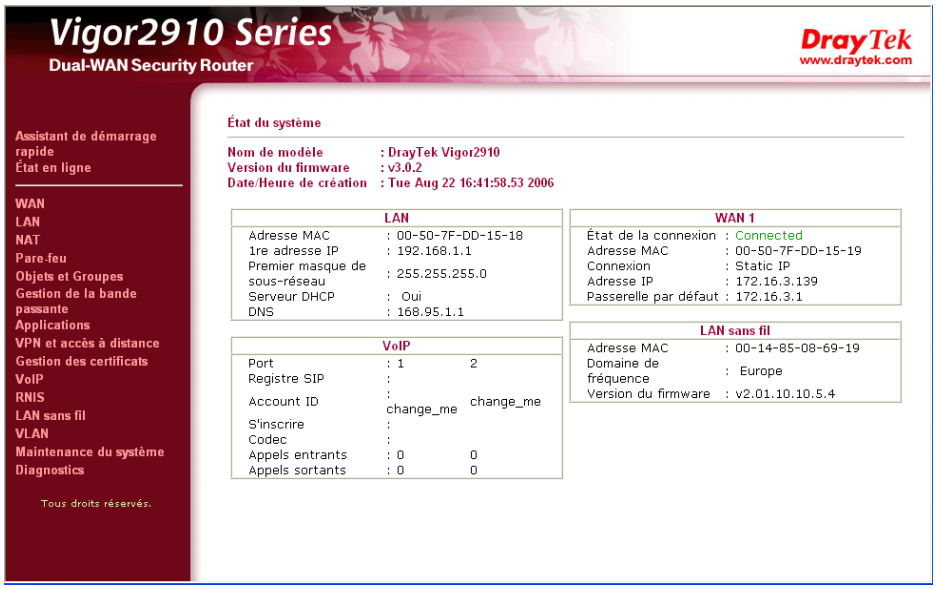
1. Vérifiez que votre PC se connecte correctement au routeur.

> Nota : vous pouvez soit configurer votre ordinateur pour qu'il obtienne dynamiquement une adresse IP du routeur, soit faire en sorte que l'adresse IP de l'ordinateur corresponde au même sous-réseau que **l'adresse IP par défaut du routeur Vigor 192.168.1.1**. Pour plus de détails, reportez-vous au chapitre Dépannage.

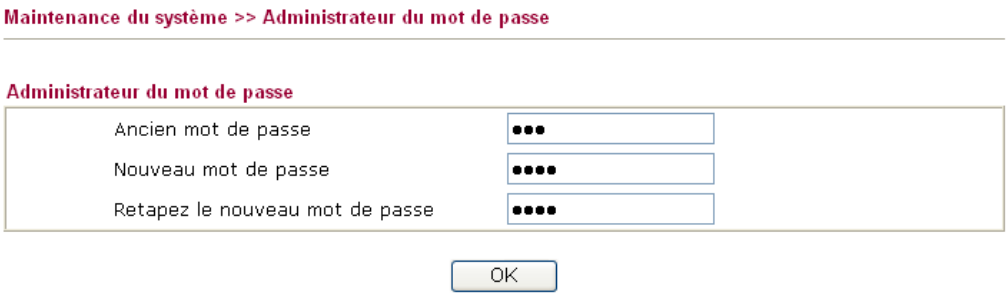
2. Ouvrez un navigateur web sur votre PC et tapez **http://192.168.1.1.** Une fenêtre s'ouvre pour vous demander votre nom d'utilisateur et votre mot de passe. Laissez les champs Nom d'utilisateur et Mot de passe vides et cliquez sur **OK**.



3. L'**écran principal** apparaît. À noter que l'écran principal diffère selon le modèle de routeur. Voici un exemple.

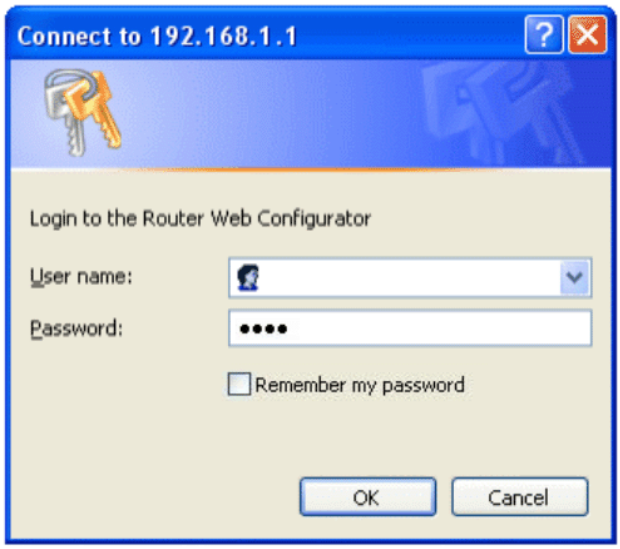


4. Sélectionnez **Maintenance du système,** puis **Mot de passe administrateur**.



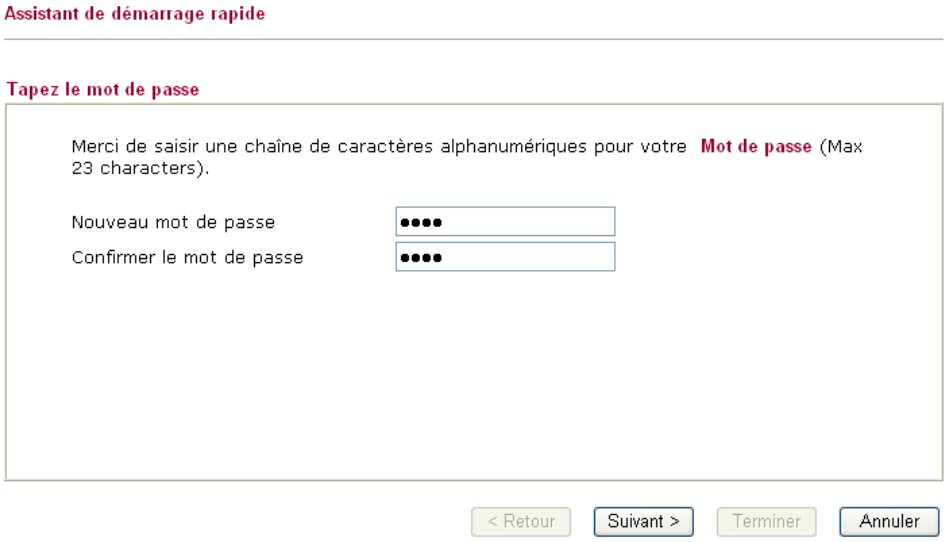
5. Entrez le mot de passe de connexion (rien par défaut) dans le champ **Ancien mot de passe**. Tapez un nouveau mot de passe dans le champ **Nouveau mot de passe** et retapez-le dans le champ **Confirmer le nouveau mot de passe** . Puis cliquez sur **Suivant** pour continuer.

6. La prochaine fois, utilisez le nouveau mot de passe pour accéder au configurateur web pour ce routeur.



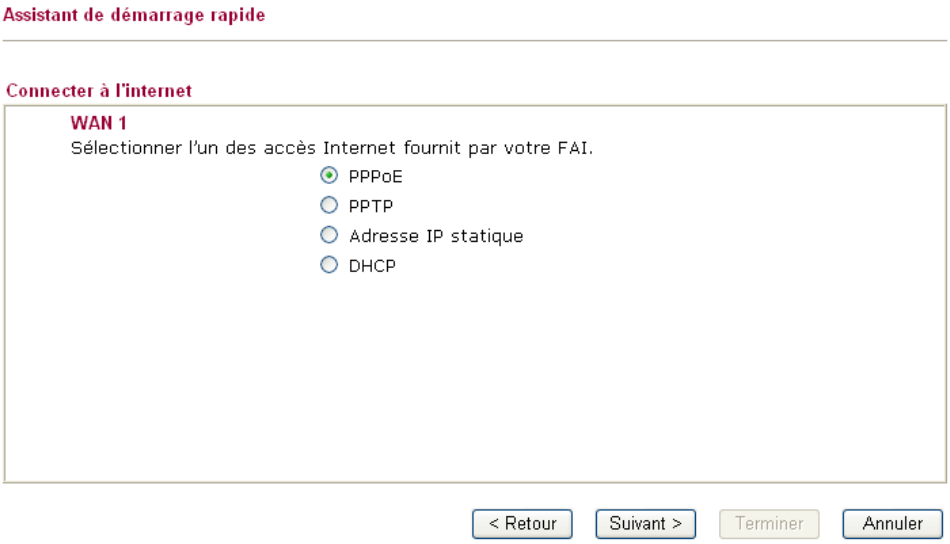
2.2 Assistant de démarrage rapide

Si votre routeur peut fonctionner dans un environnement avec NAT rapide, la configuration décrite ici peut vous aider à mettre rapidement le routeur en service. Le premier écran de **l'assistant de démarrage rapide** vous invite à entrer le mot de passe de connexion. Après avoir tapé le mot de passe, cliquez sur **Suivant**.



Dans l'écran suivant, sélectionnez l'interface WAN que vous utilisez. Choisissez **Auto-négociation** comme type physique pour votre routeur. Puis cliquez sur **Suivant** pour continuer.

Dans l'écran qui apparaît, sélectionnez le type d'accès internet approprié selon les informations fournies par votre FAI. Par exemple, vous devez sélectionner le mode PPPoE si votre FAI vous fournit une interface PPPoE. Puis , cliquez sur **Suivant** pour continuer.



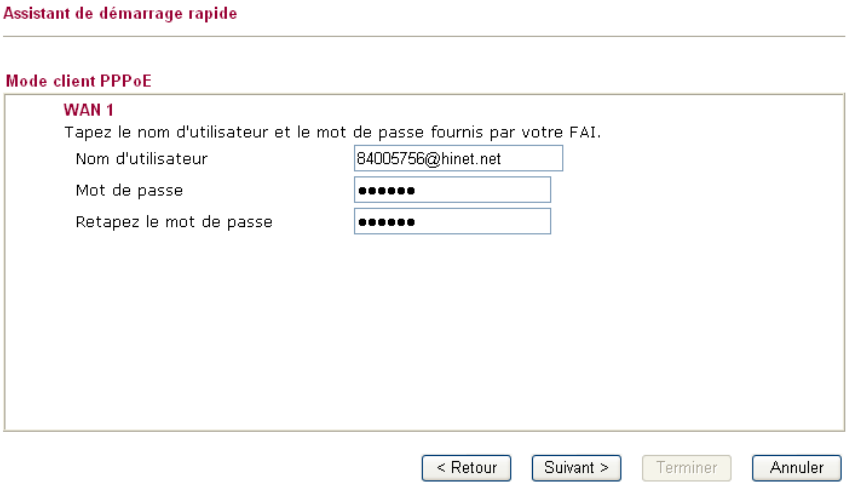
Dans **l'assistant de démarrage rapide**, vous pouvez configurer le routeur pour accéder à l'internet avec différents protocoles et en différents modes, comme **PPPoE**, **PPTP**, **IP statique** ou **DHCP**. Le routeur prend en charge l'interface WAN DSL pour l'accès à l'internet.

2.2.1 PPPoE

PPPoE est l'abréviation de **Point-to-Point Protocol over Ethernet** (protocole point-à-point sur Ethernet). Ce protocole est basé sur deux normes très répandues : PPP et Ethernet. Il connecte des utilisateurs à l'internet par l'intermédiaire d'un réseau Ethernet en utilisant un support à haut débit commun, tel qu'une ligne DSL, une interface sans fil ou un modem câble. Tous les utilisateurs du réseau Ethernet peuvent partager une connexion commune.

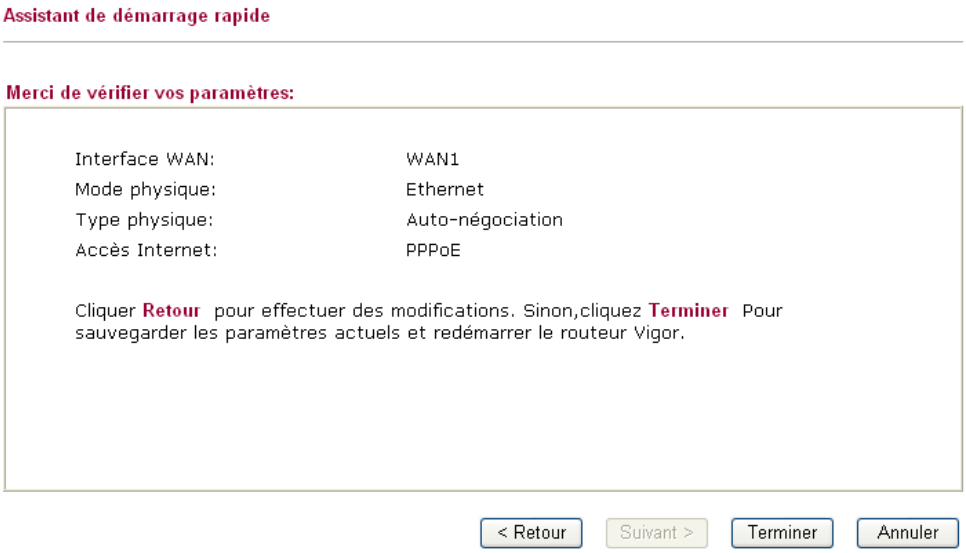
Le protocole PPPoE est utilisé pour la plupart des utilisateurs de modems DSL. Tous les utilisateurs locaux peuvent partager une connexion PPPoE pour accéder à l'internet. Votre FAI vous fournira un nom d'utilisateur (ou identifiant), un mot de passe et un mode d'authentification.

Si votre FAI vous fournit la connexion **PPPoE**, choisissez **PPPoE** pour ce routeur. La page suivante apparaît :



Nom d'utilisateur	Tapez un nom d'utilisateur (identifiant) valable fourni par votre FAI.
Mot de passe	Tapez un mot de passe valable fourni par votre FAI.
Confirmer le mot de passe	Retapez le mot de passe.

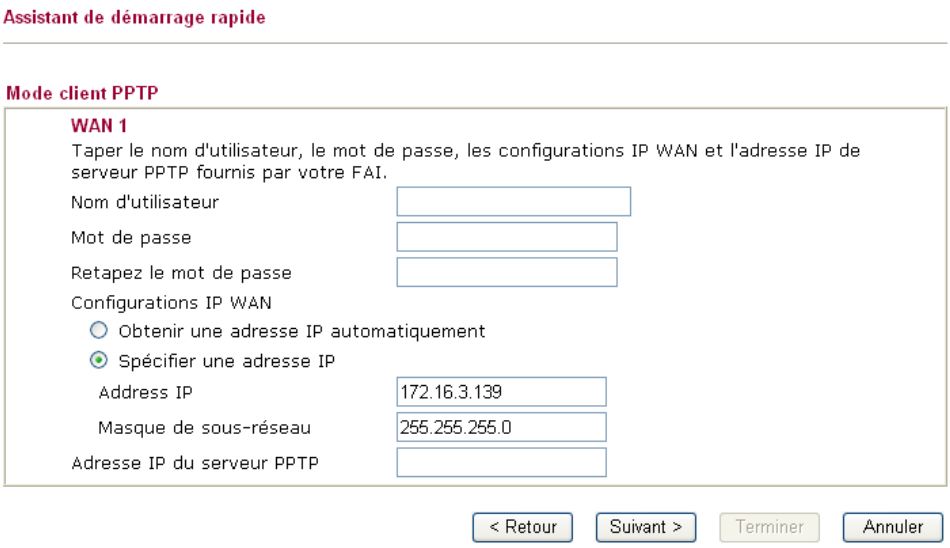
Cliquez sur **Suivant**. La page suivante apparaît.



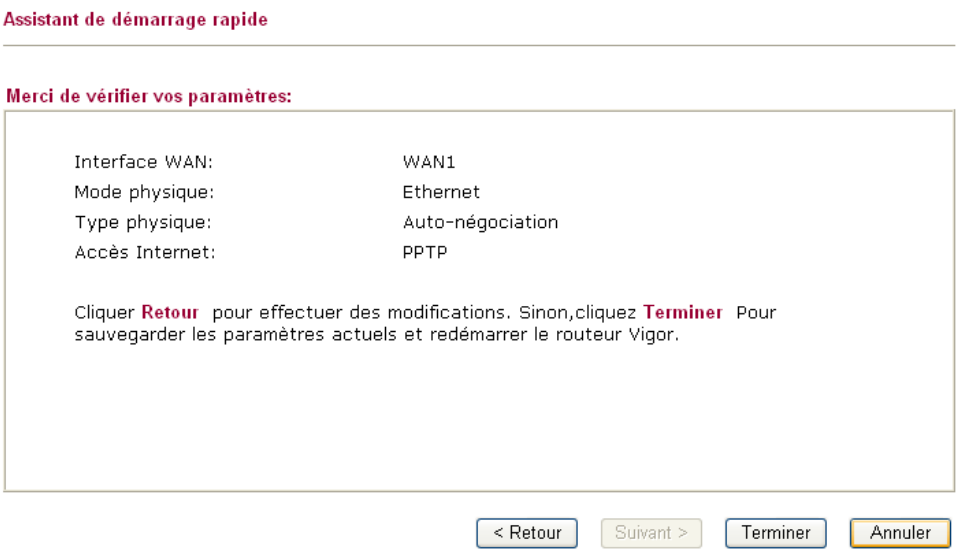
Cliquez sur **Terminer. Quick Start Wizard Setup OK!!!** s'affiche, suivi de l'état du système pour ce protocole.

2.2.2 PPTP

Choisissez **PPTP** comme protocole. Tapez toutes les informations que votre FAI vous a fournies pour ce protocole.



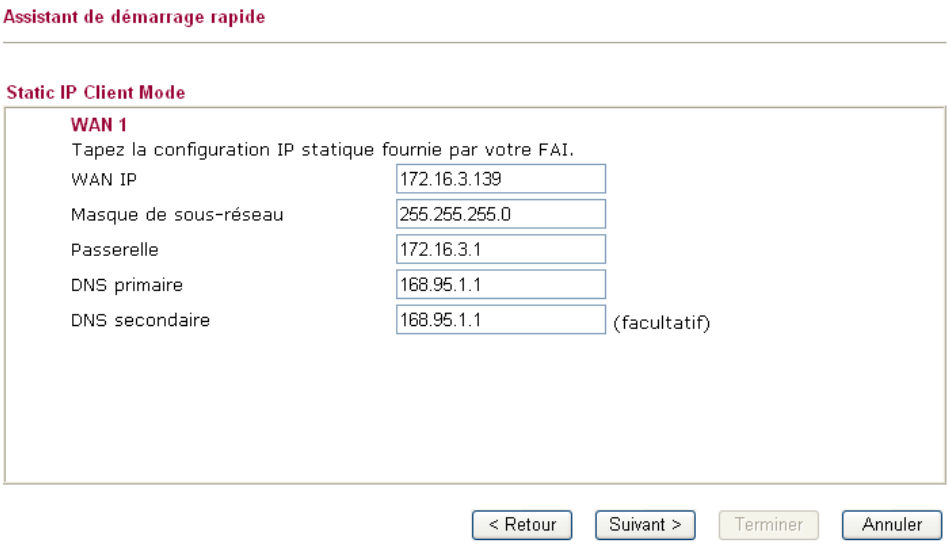
Cliquez sur **Suivant** pour voir la page suivante qui vous invite à confirmer vos paramètres.



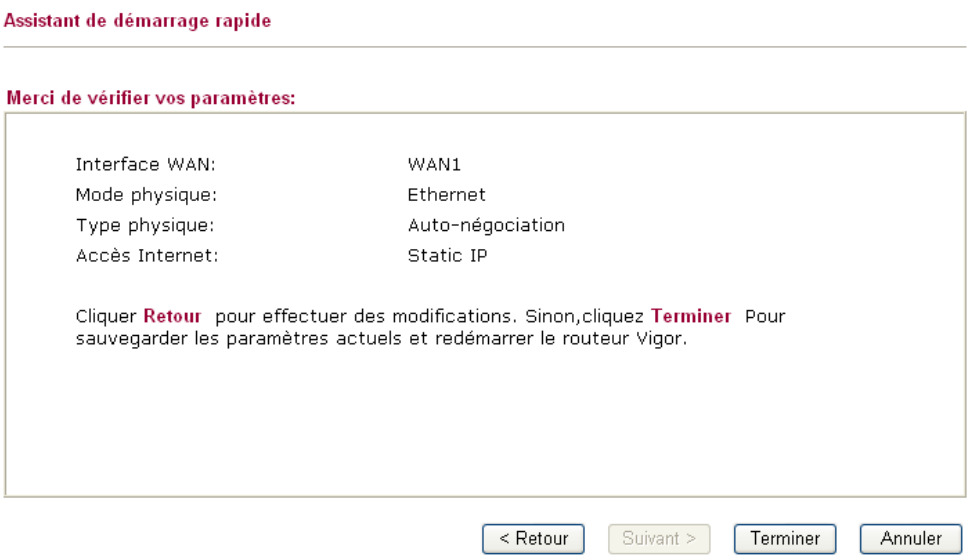
Cliquez sur **Terminer. Quick Start Wizard Setup OK!!!** s'affiche, suivi de l'état du système pour ce protocole.

2.2.3 IP statique

Choisissez **IP statique** comme protocole. Tapez toutes les informations que votre FAI vous a fournies pour ce protocole.



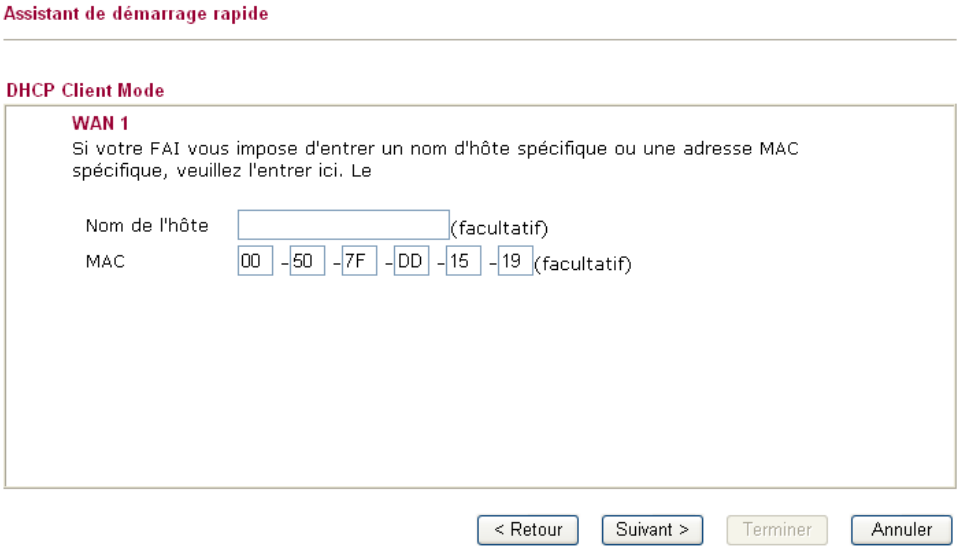
Quand vous avez fini, cliquez sur **Suivant** pour voir la page suivante.



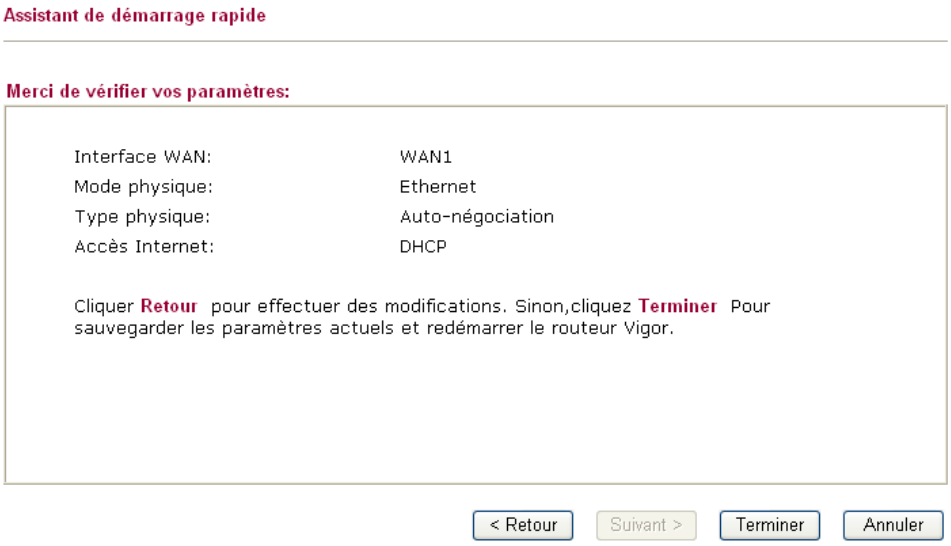
Cliquez sur **Terminer. Quick Start Wizard Setup OK!!!** s'affiche, suivi de l'état du système pour ce protocole.

2.2.4 DHCP

Choisissez **DHCP** comme protocole. Tapez toutes les informations que votre FAI vous a fournies pour ce protocole.



Quand vous avez fini, cliquez sur **Suivant** pour voir la page suivante.

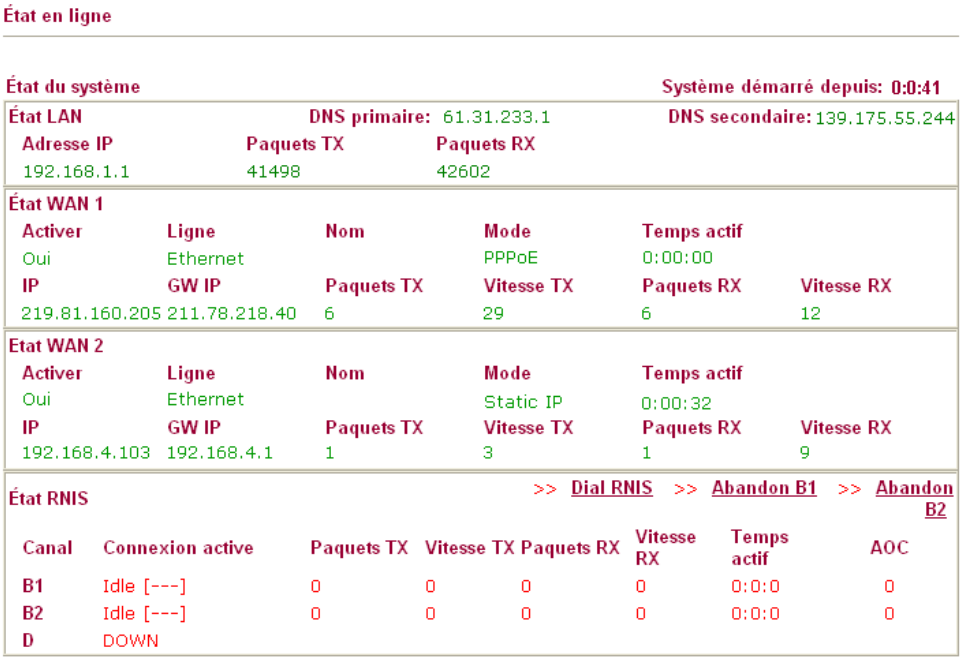


Cliquez sur **Terminer. Quick Start Wizard Setup OK!!!** s'affiche, suivi de l'état du système pour ce protocole.

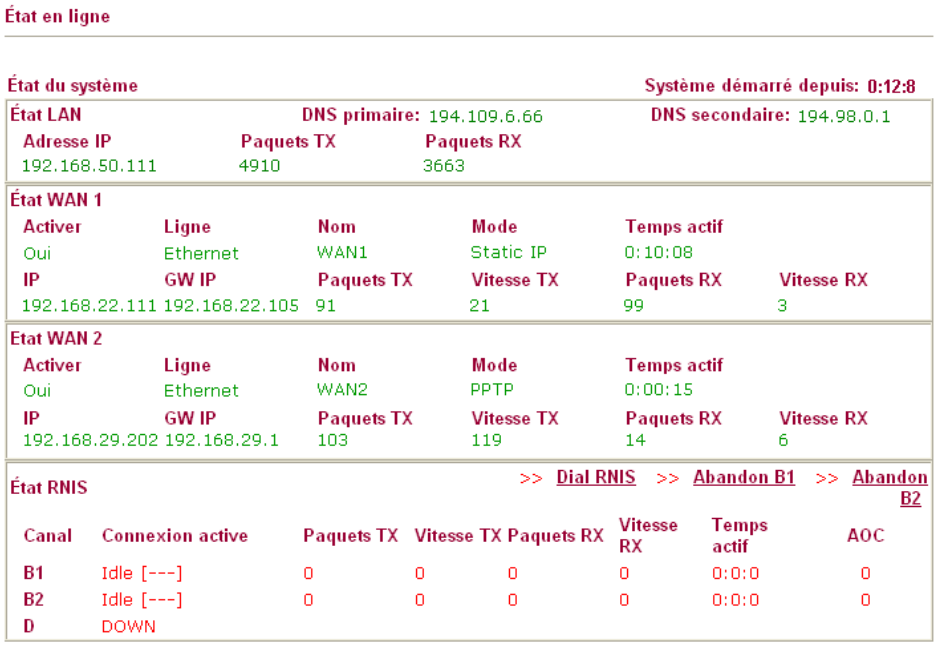
2.3 État en ligne

L'état en ligne affiche l'état du système, l'état du WAN, les informations ADSL et d'autres informations d'état relatives à ce routeur. Si vous choisissez **PPPoE** comme protocole, vous trouverez un bouton **Appel PPPoE** ou **Abandon PPPoE** dans la page web État en ligne.

État en ligne pour PPPoE



État en ligne pour PPTP (pour WAN2)



État en ligne

État du système — Système démarré depuis: 0:12:8

État LAN — DNS primaire: 194.109.6.66 — DNS secondaire: 194.98.0.1

Adresse IP	Paquets TX	Paquets RX
192.168.50.111	4910	3663

État WAN 1

Activer	Ligne	Nom	Mode	Temps actif	
Oui	Ethernet	WAN1	Static IP	0:10:08	
IP	**GW IP**	**Paquets TX**	**Vitesse TX**	**Paquets RX**	**Vitesse RX**
192.168.22.111	192.168.22.105	91	21	99	3

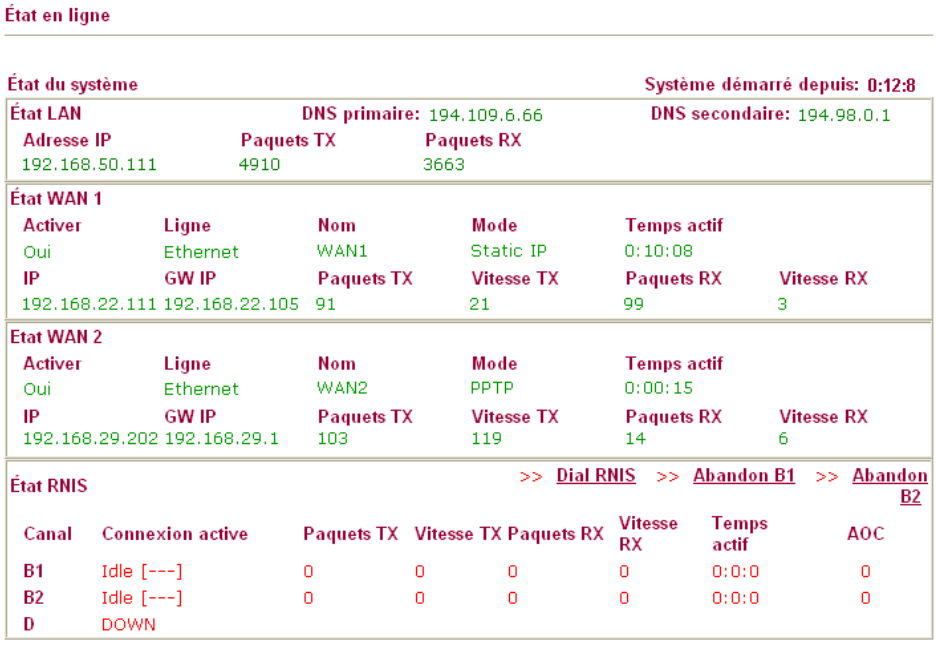
Etat WAN 2

Activer	Ligne	Nom	Mode	Temps actif	
Oui	Ethernet	WAN2	PPTP	0:00:15	
IP	**GW IP**	**Paquets TX**	**Vitesse TX**	**Paquets RX**	**Vitesse RX**
192.168.29.202	192.168.29.1	103	119	14	6

État RNIS — >> Dial RNIS >> Abandon B1 >> Abandon B2

Canal	Connexion active	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Temps actif	AOC
B1	Idle [---]	0	0	0	0	0:0:0	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	DOWN						

État en ligne pour IP statique (pour WAN1)



État en ligne

État du système — Système démarré depuis: 0:12:8

État LAN — DNS primaire: 194.109.6.66 — DNS secondaire: 194.98.0.1

Adresse IP	Paquets TX	Paquets RX
192.168.50.111	4910	3663

État WAN 1

Activer	Ligne	Nom	Mode	Temps actif	
Oui	Ethernet	WAN1	Static IP	0:10:08	
IP	**GW IP**	**Paquets TX**	**Vitesse TX**	**Paquets RX**	**Vitesse RX**
192.168.22.111	192.168.22.105	91	21	99	3

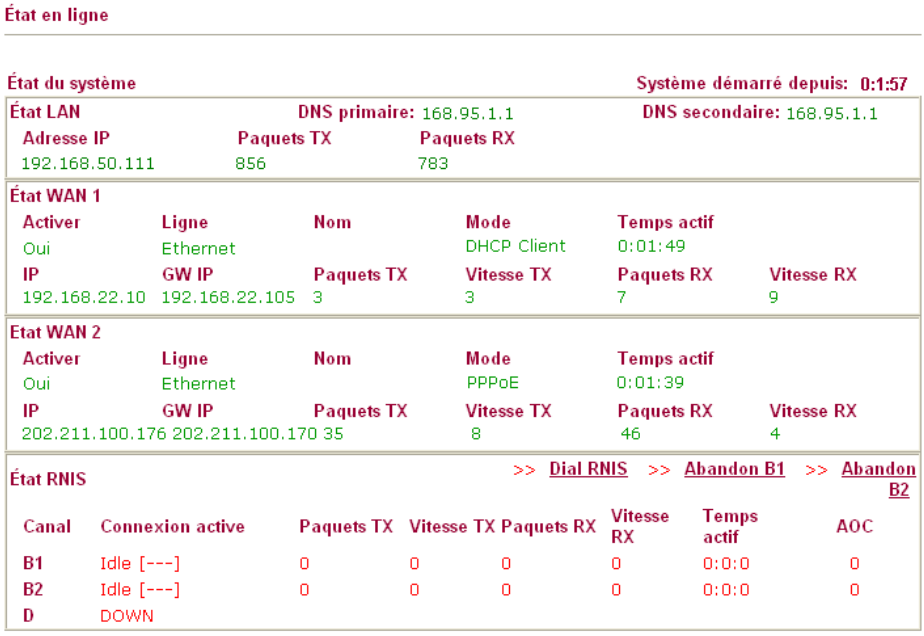
Etat WAN 2

Activer	Ligne	Nom	Mode	Temps actif	
Oui	Ethernet	WAN2	PPTP	0:00:15	
IP	**GW IP**	**Paquets TX**	**Vitesse TX**	**Paquets RX**	**Vitesse RX**
192.168.29.202	192.168.29.1	103	119	14	6

État RNIS — >> Dial RNIS >> Abandon B1 >> Abandon B2

Canal	Connexion active	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Temps actif	AOC
B1	Idle [---]	0	0	0	0	0:0:0	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	DOWN						

État en ligne pour DHCP



Explication détaillée:

DNS primaire Affiche l'adresse IP du DNS primaire.

DNS secondaire Affiche l'adresse IP du DNS secondaire.

État LAN

Adresse IP Affiche l'adresse IP de l'interface LAN.

Paquets TX Affiche le nombre total de paquets émis au niveau de l'interface LAN.

Paquets RX Affiche le nombre total de paquets reçus au niveau de l'interface LAN.

État WAN1/2

Ligne Affiche la connexion physique (Ethernet) de cette interface.

Nom Affiche le nom défini dans la page web WAN1/WAN2.

Mode Affiche le type de connexion WAN (par exemple, PPPoE).

Temps actif Affiche le temps total de connexion de l'interface.

IP Affiche l'adresse IP de l'interface WAN.

IP passerelle Affiche l'adresse IP de la passerelle par défaut.

Paquets TX Affiche le nombre total de paquets émis au niveau de l'interface WAN.

Vitesse TX Affiche la vitesse d'émission des paquets au niveau de l'interface WAN.

Paquets RX Affiche le nombre total de paquets reçus au niveau de l'interface WAN.

Vitesse RX Affiche la vitesse de réception des paquets au niveau de WAN interface.

Nota : si les libellés sont en vert, c'est que la connexion WAN de cette interface (WAN1/WAN2) est prête pour l'accès à l'internet ; s'ils sont en rouge, c'est que la connexion WAN de cette interface (WAN1/WAN2) n'est pas prête pour l'accès à l'internet.

2.4 Enregistrement de la configuration

Chaque fois que vous cliquez sur **OK** dans une page web pour enregistrer la configuration, le système peut afficher des messages à votre attention.

Prêt indique que le système est prêt et que vous pouvez définir vos paramètres.

Paramètres enregistrés indique que vos paramètres seront enregistrés quand vous aurez cliqué sur le bouton **Terminer** ou **OK**.

3 Configuration web avancée

Quand vous en avez fini avec la configuration de base du routeur, vous pouvez accéder facilement à l'internet. Si vous voulez effectuer un paramétrage plus poussé, lisez ce chapitre. Pour des exemples d'applications, reportez-vous au Chapitre 4.

3.1 WAN

L'assistant de démarrage rapide vous offre une méthode facile pour configurer rapidement le mode de connexion du routeur. Si vous voulez définir d'autres paramètres pour différents modes WAN, cliquez sur l'option **Accès à l'internet** du menu **WAN**.

3.1.1 Principes de base d'un réseau à protocole internet (IP)

IP signifie protocole internet. Toutes les machines d'un réseau basé sur le protocole internet (ou réseau IP), notamment les routeurs, le serveur d'impression et certains PC ont besoin d'une adresse IP. Pour éviter les conflits d'adresses, les adresses IP sont enregistrées publiquement auprès d'un organisme appelé Network Information Centre (NIC). Avoir une adresse IP unique est impératif pour les machines qui ont accès au réseau public mais non pour celles des réseaux locaux (LAN) TCP/IP privés, telles que les PC gérés par un routeur, car ils ne sont pas censés être accessibles au public. Le NIC a réservé certaines adresses qui ne seront jamais enregistrées publiquement. Ces adresses dites adresses IP privées appartiennent aux plages suivantes :

de 10.0.0.0 à 10.255.255.255
de 172.16.0.0 à 172.31.255.255
de 192.168.0.0 à 192.168.255.255

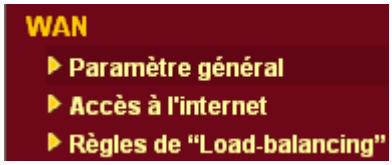
Adresse IP publique et adresse IP privée

Comme le routeur a pour rôle de gérer et de protéger son LAN, il relie entre eux des groupes de PC hôtes qui ont chacun une adresse IP privée attribuée par le serveur DHCP intégré au routeur Vigor. Le routeur lui-même utilise également l'adresse IP par défaut 192.168.1.1 pour communiquer avec les hôtes locaux. Le routeur Vigor communique avec d'autres équipements de réseau à l'aide d'une adresse IP publique. À l'arrivée de données, la fonction de traduction d'adresse réseau (NAT) du routeur traduit les adresses IP publiques en adresses IP privées et les paquets sont acheminés jusqu'aux PC hôtes appropriés du réseau local. Ainsi, tous les PC hôtes peuvent partager une connexion internet commune.

Comment obtenir une adresse IP publique de votre FAI

En ADSL, une authentification et une autorisation par protocole point à point (PPP) sont nécessaires pour mettre en relation les équipements d'installation d'usager (CPE). Le protocole point à point sur Ethernet (PPPoE) connecte un réseau de machines hôtes par l'intermédiaire d'un équipement d'accès à distance ou à un concentrateur d'agrégation. Cette implémentation donne à l'utilisateur une grande facilité d'utilisation. En même temps, elle permet le contrôle d'accès, la facturation et la définition d'un type de service par utilisateur.

Lorsque un routeur se connecte à votre FAI, un processus de découverte se déroule afin de demander une connexion, puis une session est créée. Votre nom d'utilisateur et votre mot de passe sont authentifiés par **PAP** ou **CHAP** à l'aide du système d'authentification **RADIUS**. Votre adresse IP, votre serveur DNS et autres informations sont généralement fournies par votre FAI.



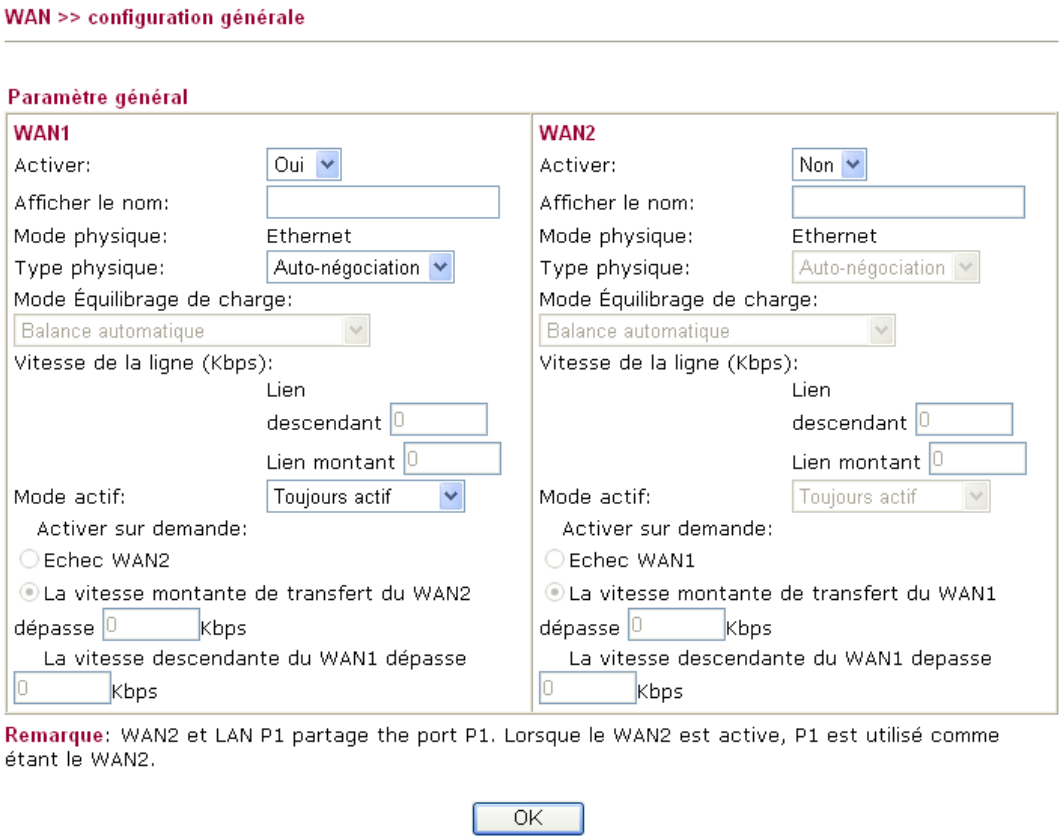
3.1.2 Configuration générale

Cette section présente quelques paramètres généraux de l'accès à l'internet et explique les modes de connexion des ports WAN1 et WAN2.

Ce routeur vous permet de combiner les bandes passantes respectives de deux ports WAN pour accélérer la transmission sur le réseau. Chaque port WAN (WAN1, via le port WAN/WAN2, via le port LAN1) peut se connecter à un FAI différent, même si les FAI utilisent des technologies différentes (DSL, modem câble, etc.). En cas de problème avec l'une des connexions d'accès à l'internet, tout le trafic est aiguillé vers le port de communication normal. Paramétrez les interfaces WAN1 et WAN2.

Cette page web vous permet d'effectuer la configuration générale des interfaces WAN1 et WAN2.

> **Nota :** par défaut, l'interface WAN1 est activée. L'interface WAN2 est facultative.



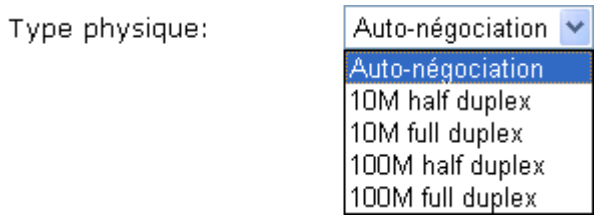
Activer — Choisissez Oui pour activer cette interface WAN. Choisissez Non pour désactiver cette interface WAN.

Nom affiché — Tapez la désignation de l'interface WAN1/WAN2.

Mode physique — Dans le cas de l'interface WAN1, la connexion physique est établie via le port ADSL; tandis que, dans le cas de l'interface WAN2, elle est établie via un port Ethernet (P1). Vous ne pouvez pas changer cela.

Type physique

Vous pouvez changer le type de connexion physique pour l'interface WAN2 ou choisir **Auto-négociation** pour que se soit le système qui le détermine.



Mode d'équilibrage de charge

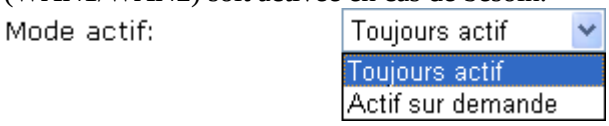
Si vous connaissez la bande passante pratique de votre interface WAN, choisissez **Selon le débit en ligne**. Sinon, choisissez **Pondération automatique** pour laisser au routeur le soin de trouver le meilleur équilibre.

Débit en ligne

Si vous choisissez **Selon le débit en ligne** comme **Mode d'équilibrage de charge**, tapez le débit descendant et le débit montant de l'interface WAN1/WAN2. L'unité est le kbit/s.

Mode d'activation

Choisissez **Connexion permanente** pour que la connexion WAN (WAN1/WAN2) soit toujours active ou bien **Activation à la demande** pour que la connexion WAN (WAN1/WAN2) soit activée en cas de besoin.



Si vous choisissez Activation à la demande, vous pourrez spécifier un délai d'inactivité pour les modes d'accès PPPoE et PPTP WAN>>Accès à l'internet. De plus, vous avez trois options.

Panne WAN2 – La connexion WAN1 sera activée en cas de panne de WAN2.

Débit montant WAN2 > XX kbit/s – La connexion WAN1 sera activée lorsque le débit montant WAN2 dépasse la valeur spécifiée pendant 15 secondes.

Débit descendant WAN2 > XX kbit/s – La connexion WAN1 sera activée lorsque le débit descendant WAN2 dépasse la valeur spécifiée pendant 15 secondes.

Panne WAN1 – La connexion WAN2 sera activée en cas de panne de WAN1.

Débit montant WAN1 > XX kbit/s – La connexion WAN2 sera activée lorsque le débit montant WAN1 dépasse la valeur spécifiée pendant 15 secondes.

Débit descendant WAN1 > XX kbit/s – La connexion WAN2 sera activée lorsque le débit descendant WAN1 dépasse la valeur spécifiée pendant 15 secondes.

3.1.3 Accès à l'internet

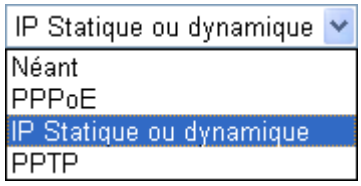
Comme le routeur a deux interfaces WAN, vous pouvez définir des paramètres d'accès à l'internet différents pour WAN1/WAN2. Le mode physique n'étant pas le même pour WAN1 et WAN2, le mode d'accès pour ces deux connexions diffère légèrement.

Index — Indique les modes WAN pris en charge par ce routeur. WAN1 est l'interface WAN d'accès à l'internet par défaut. WAN2 est l'interface WAN facultative utilisée pour accéder à l'internet lorsque l'interface WAN1 est inactive pour une raison ou pour une autre.

Nom affiché — Indique le nom donné à l'interface WAN1/WAN2 dans la page de configuration générale.

Mode physique — Indique le port physique de l'interface WAN1/WAN2.

Mode d'accès — Choisissez un mode d'accès approprié dans la liste déroulante. La page de détails de ce mode apparaît. Sinon, cliquez sur Page détails.

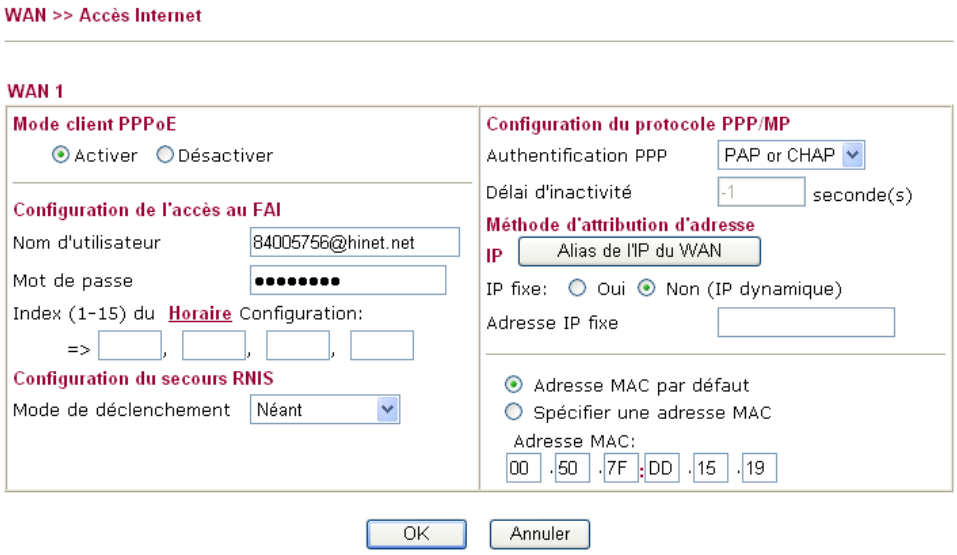


Il y a trois modes d'accès : PPPoE, IP statique ou dynamique et PPTP.

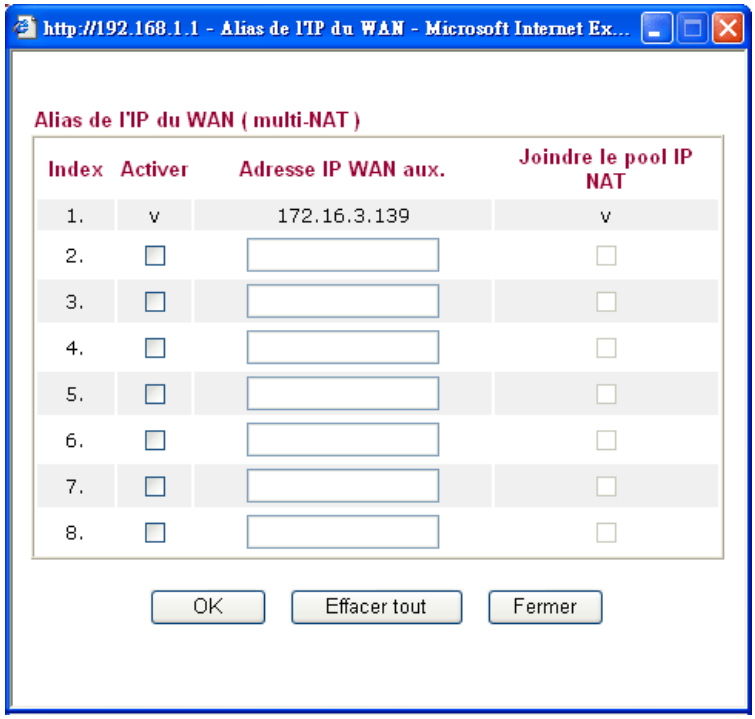
Page détails — Ce bouton ouvre la page web correspondant au mode d'accès que vous avez choisi pour WAN1 ou WAN2.

Page de détails pour PPPoE

Pour utiliser **PPPoE** comme protocole d'accès à l'internet, choisissez l'option **Accès à l'internet** du menu **WAN**, puis sélectionnez le mode **PPPoE** pour WAN2. La page web suivante apparaît.



Mode client PPPoE	Cliquez sur **Activer** pour activer cette fonction. Si vous cliquez sur **Désactiver**, vous perdrez tous les paramètres que vous avez définis dans cette page.
Configuration de l'accès au FAI	Entrez le nom d'utilisateur, le mot de passe et les paramètres d'authentification qui vous ont été fournis par votre FAI. Si vous voulez rester connecté à l'internet en permanence, vous pouvez cocher **Connexion permanente** **Nom d'utilisateur** – Tapez l'identifiant que vous a fourni le FAI. **Mot de passe** – Tapez le mot de passe que vous a fourni le FAI. **Plages horaires (1-15) -** Vous pouvez spécifier quatre plages horaire définies précédemment dans la page web **Applications – Plages horaire** en tapant les numéros d'index correspondants.
Configuration du secours RNIS	Ce paramètre n'est disponible que pour les routeurs prenant en charge la fonction RNIS. Pour pouvoir utiliser le secours RNIS, vous devez avoir créé au préalable un profil de secours. Cliquez sur **Configuration de l'accès à l'internet** > **Connexion à un seul FAI**. Ce paramètre n'est disponible que pour le modèle *i*. Certains modèles n'ont pas d'interface RNIS et ne disposent donc pas du secours RNIS. Les options de configuration du secours RNIS sont les suivantes. **Néant** – Le secours RNIS est désactivé. **Déclenchement par paquet –** Le secours RNIS est activé à la réception par le routeur d'un paquet provenant d'un hôte local. **Connexion permanente –** Si la connexion à haut débit n'est plus disponible, le secours RNIS est activé automatiquement et reste activé jusqu'à ce que la connexion à haut débit soit rétablie. Nous vous recommandons de choisir cette option si vous hébergez un serveur web accessible à vos clients.
Configuration PPP/MP	**Authentification PPP** – Choisissez **PAP seulement, PAP ou CHAP**. **Délai d'inactivité** – Spécifiez le délai au bout duquel la connexion internet sera coupée en l'absence d'activité. Ce paramètre n'est actif que lorsque l'option **Activation à la demande** a été choisie comme mode d'activation dans la page **WAN>> Configuration générale**.
Méthode d'attribution des adresses IP (IPCP)	D'une manière générale, le FAI vous attribue dynamiquement une adresse IP chaque fois que vous vous connectez et que vous demandez une adresse IP. Dans certains cas, votre FAI vous attribue la même adresse IP chaque fois que vous en demandez une. Dans ce cas, vous pouvez taper cette adresse IP dans le champ Adresse IP fixe. Contactez votre FAI avant d'utiliser cette fonction. **Alias IP WAN -** Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction **Alias de I'IP du WAN**. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement. À noter que ce paramètre n'est disponible que pour l'interface WAN1.



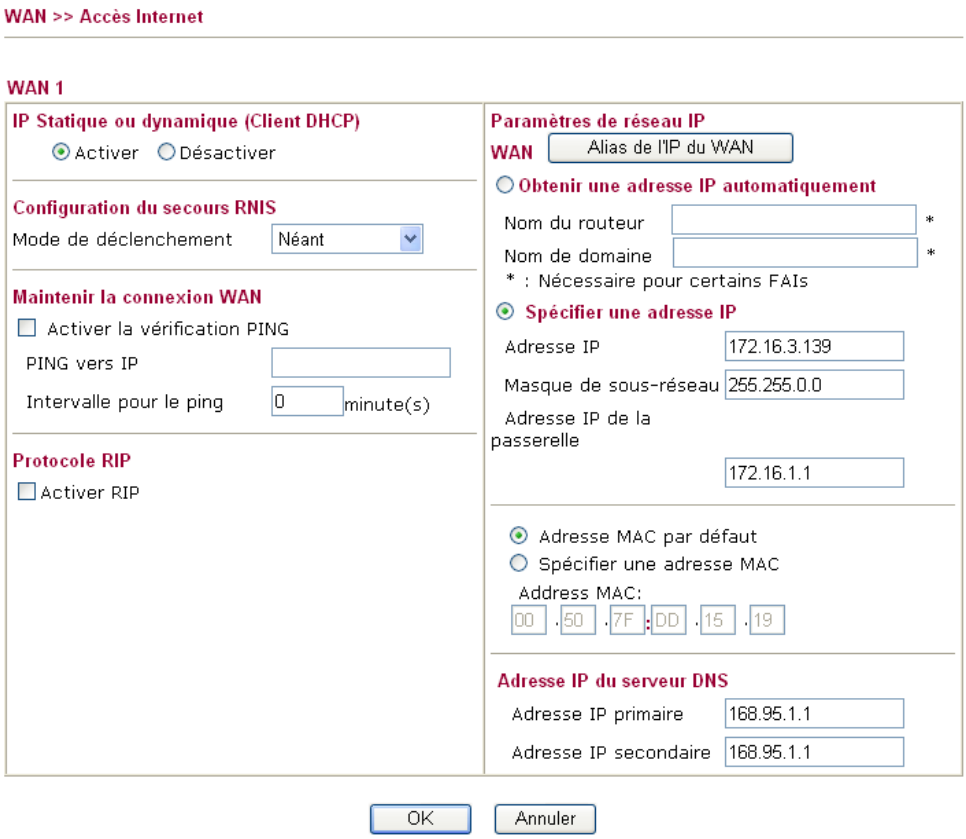
IP fixe – Cliquez sur **Oui** pour utiliser cette fonction et tapez une adresse IP fixe dans le champ **Adresse IP fixe**.
Adresse MAC par défaut – Vous pouvez utiliser l'adresse MAC par défaut ou spécifiez une autre adresse MAC dans les zones prévues à cet effet.
Spécifier une adresse MAC – Tapez l'adresse MAC du routeur.

Quand vous avez fini de définir tous les paramètres de cette page, cliquez sur **OK** pour les activer.

Page de détails pour IP statique ou dynamique

Dans le cas du mode IP statique, vous recevez généralement de votre fournisseur d'accès DSL ou câble une adresse IP publique fixe ou un masque de sous-réseau public, c'est-à-dire plusieurs adresses IP publiques. Dans la plupart des cas, un fournisseur d'accès câble offre une adresse IP publique fixe, tandis qu'un fournisseur d'accès DSL offre un masque de sous-réseau public. Si vous avez un masque de sous-réseau public, vous pouvez attribuer à l'interface WAN une ou plusieurs adresses IP.

Pour utiliser le protocole **IP statique ou dynamique,** cliquez sur l'option **Accès à l'internet** du menu **WAN**. Puis, sélectionnez le mode **IP statique ou dynamique** pour WAN2. La page web suivante apparaît.



IP statique ou dynamique (client DHCP)

Cliquez sur **Activer** pour activer cette fonction. Si vous cliquez sur **Désactiver**, vous perdrez tous les paramètres que vous avez définis dans cette page.

Configuration du secours RNIS

Ce paramètre n'est disponible que pour les routeurs prenant en charge la fonction RNIS. Pour pouvoir utiliser le secours RNIS, vous devez avoir créé au préalable un profil de secours. Cliquez sur **Configuration de l'accès à l'internet** > **Connexion à un seul FAI**.

Certains modèles n'ont pas d'interface RNIS et ne disposent donc pas du secours RNIS. Les options de configuration du secours RNIS sont les suivantes.
Néant – Le secours RNIS est désactivé.
Déclenchement par paquet – Le secours RNIS est activé à la réception par le routeur d'un paquet provenant d'un hôte local.
Connexion permanente – Si la connexion à haut débit n'est plus disponible, le secours RNIS est activé automatiquement et reste activé jusqu'à ce que la connexion à haut débit soit rétablie. Nous vous recommandons de choisir cette option si vous hébergez un serveur web accessible à vos clients.

Maintenir la connexion WAN

Normalement, cette fonction est utilisée dans un environnement IP dynamique car certains FAI coupent les connexions en l'absence de trafic pendant un certain temps. Cochez **Activer la vérification par PING p**our activer cette fonction.
PING vers IP – Si vous activez la fonction PING, spécifiez l'adresse IP à « PINGer ».
Intervalle entre PING – Entrez la fréquence de l'opération PING.

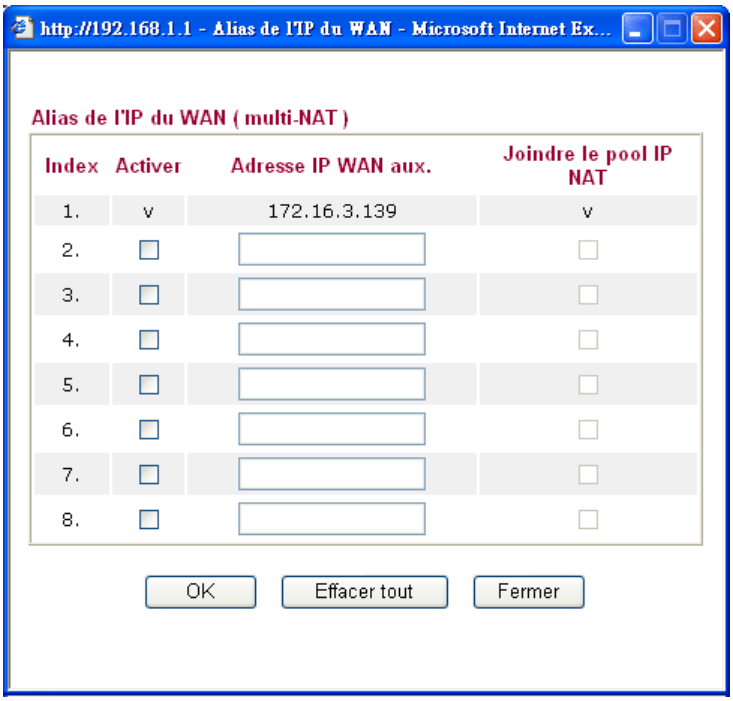
Protocole RIP

Le protocole d'information de routage ou RIP (RFC1058) définit comment les routeurs échangent les informations des tables de routage. Cliquez sur **Activer RIP** pour activer cette fonction.

Paramètres de réseau IP WAN

Ce groupe vous permet d'obtenir une adresse IP automatiquement ou d'en spécifier une.

Alias IP WAN - Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction **Alias IP WAN**. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement. À noter que ce paramètre n'est disponible que pour l'interface WAN1.



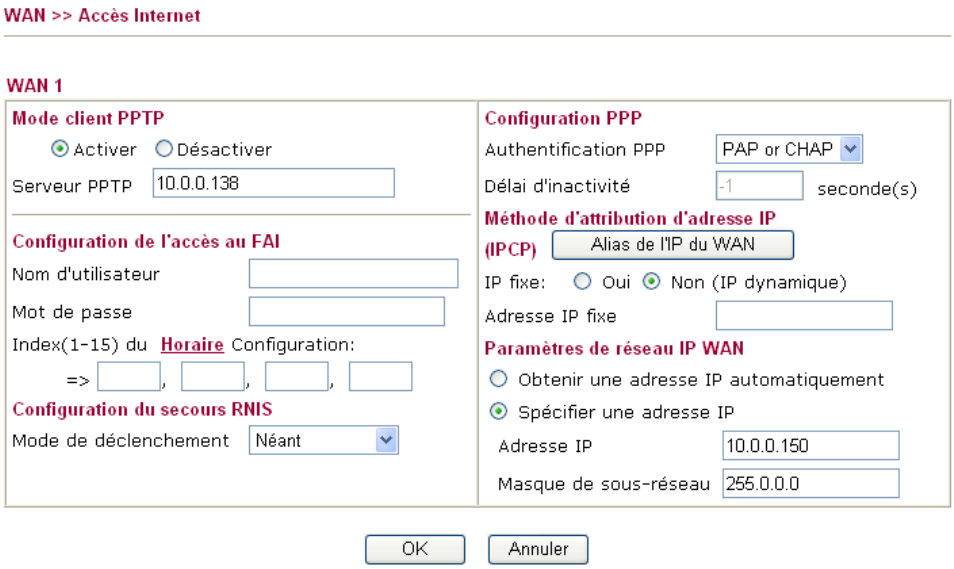
Obtenir une adresse IP automatiquement – Cliquez sur ce bouton pour obtenir l'adresse IP automatiquement si vous voulez utiliser le mode **IP dynamique**.
Nom de routeur : Tapez le nom de routeur fourni par le FAI.
Nom de domaine : Tapez le nom de domaine qui vous a été attribué.
Spécifier une adresse IP – Cliquez sur ce bouton pour spécifier une adresse IP si vous voulez utiliser le mode **IP statique**.
Adresse IP : Tapez l'adresse IP privée.
Masque de sous-réseau : Tapez le masque de sous-réseau.
Adresse IP de la passerelle : Tapez l'adresse IP de la passerelle.
Adresse MAC par défaut : Cliquez sur ce bouton d'option pour utiliser l'adresse MAC par défaut.
Spécifier une adresse MAC : Certains fournisseurs d'accès câble utilisent une adresse MAC spécifique pour l'authentification de l'accès. Dans ce cas, vous devez cocher la case **Spécifier une adresse MAC** et entrer l'adresse MAC dans les champs Adresse MAC.

Adresse IP du serveur DNS

Tapez l'adresse IP primaire du routeur si vous voulez utiliser le mode **IP statique**. Au besoin, tapez une adresse IP secondaire qui pourra être nécessaire ultérieurement.

Page de détails pour PPTP

Pour utiliser **PPTP** comme protocole d'accès à l'internet, cliquez sur l'option **Accès à l'internet** du menu **WAN**, puis sélectionnez le mode **PPTP** pour WAN2. La page web suivante apparaît.



Configuration PPTP

Liaison PPTP - Cochez **Activer** pour permettre à un client PPTP d'établir un tunnel vers un modem DSL sur l'interface WAN.
Serveur PPTP - Spécifiez l'adresse IP du serveur PPTP.

Configuration de l'accès au FAI

Nom d'utilisateur – Tapez l'identifiant que vous a fourni le FAI.
Mot de passe – Tapez le mot de passe que vous a fourni le FAI.
Plages horaires (1-15) - Vous pouvez spécifier quatre plages horaire définies précédemment dans la page web **Applications – Plages horaire** en tapant les numéros d'index correspondants.

Configuration du secours RNIS

Ce paramètre n'est disponible que pour les routeurs prenant en charge la fonction RNIS. Pour pouvoir utiliser le secours RNIS, vous devez avoir créé au préalable un profil de secours. Cliquez sur **Configuration de l'accès à l'internet** > **Connexion à un seul FAI**.

Certains modèles n'ont pas d'interface RNIS et ne disposent donc pas du secours RNIS. Les options de configuration du secours RNIS sont les suivantes.
Néant – Le secours RNIS est désactivé.
Déclenchement par paquet – Le secours RNIS est activé à la réception par le routeur d'un paquet provenant d'un hôte local.
Connexion permanente – Si la connexion à haut débit n'est plus disponible, le secours RNIS est activé automatiquement et reste activé jusqu'à ce que la connexion à haut débit soit rétablie. Nous vous recommandons de choisir cette option si vous hébergez un serveur web accessible à vos clients.

Paramètre PPP

Authentification PPP – Sélectionnez **PAP seulement, PAP ou CHAP**.
Délai d'inactivité – Spécifiez le délai au bout duquel la connexion internet sera coupée en l'absence d'activité. Ce paramètre n'est

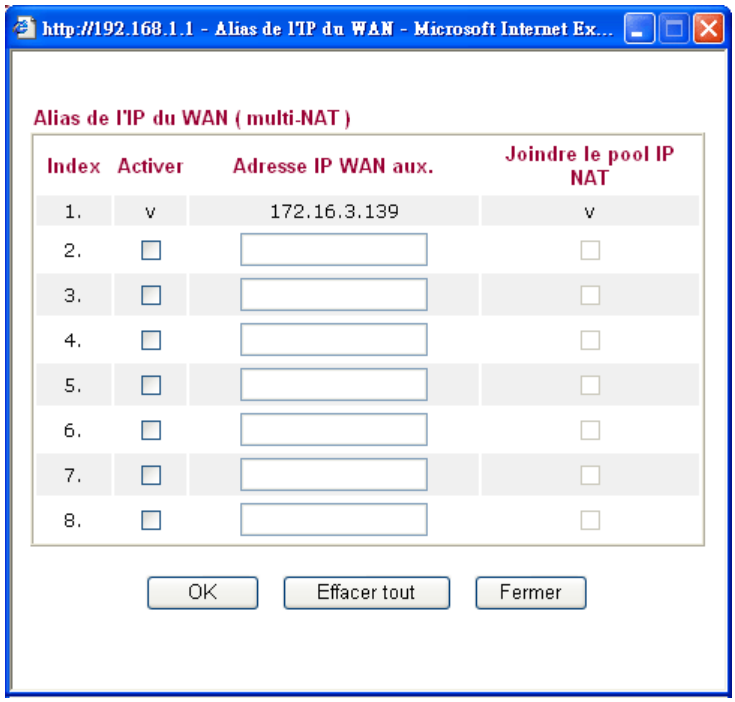
actif que lorsque l'option **Activation à la demande** a été choisie comme mode d'activation dans la page **WAN>> Configuration générale**.

Méthode d'attribution des adresses IP (IPCP)

IP fixe - D'une manière générale, le FAI vous attribue dynamiquement une adresse IP chaque fois que vous vous connectez et que vous demandez une adresse IP. Dans certains cas, votre FAI vous attribue la même adresse IP chaque fois que vous en demandez une. Dans ce cas, vous pouvez taper cette adresse IP dans le champ Adresse IP fixe. Contactez votre FAI avant d'utiliser cette fonction. Cliquez sur **Oui** pour utiliser cette fonction et tapez une adresse IP fixe dans le champ Adresse IP fixe.

Adresse IP fixe – Tapez une adresse IP fixe.

Alias IP WAN - Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction **Alias IP WAN**. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement. À noter que ce paramètre n'est disponible que pour l'interface WAN1.



Adresse MAC par défaut – Cliquez sur ce bouton d'option pour utiliser l'adresse MAC par défaut.
Spécifier une adresse MAC – Certains fournisseurs d'accès câble utilisent une adresse MAC spécifique pour l'authentification de l'accès. Dans ce cas, vous devez cocher la case **Spécifier une adresse MAC** et entrer l'adresse MAC dans les champs Adresse MAC.

Paramètres de réseau IP WAN

Obtenir une adresse IP automatiquement – Cliquez sur ce bouton pour obtenir l'adresse IP automatiquement.

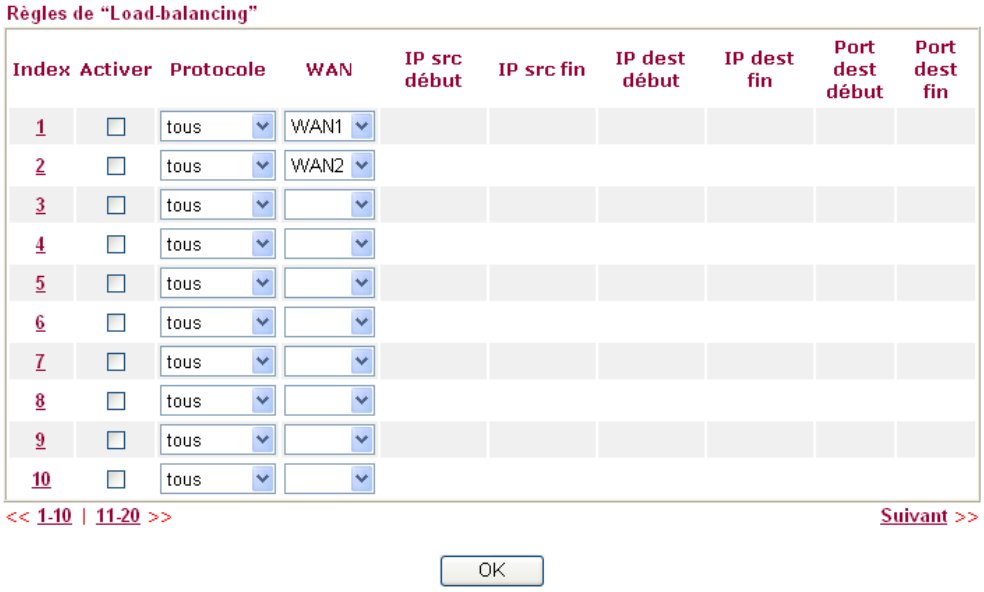
Spécifier une adresse IP – Cliquez sur ce bouton pour spécifier une adresse IP.

Adresse IP– Tapez l'adresse IP privée.
Masque de sous-réseau – Tapez le masque de sous-réseau.

3.1.4 Règles de "Load-balancing"

Ce routeur assure l'équilibrage de charge. Il peut affecter le trafic à l'interface WAN1 ou WAN2 selon le type de protocole, l'adresse IP d'un hôte spécifique, un sous-ensemble d'hôtes et une plage de ports. L'utilisateur peut affecter une catégorie de trafic à une interface réseau particulière selon le paramétrage de la page web suivante. Vous pouvez définir vingt règles d'équilibrage de charge.

Nota : l'équilibrage de charge ne fonctionne que lorsque les deux interfaces WAN1 et WAN2 sont activées.



Index Cliquez sur le numéro pour accéder à la page web de configuration de la règle d'équilibrage de charge.

Activer Cochez cette case pour activer cette règle.

Protocole Utilisez le menu déroulant pour changer le protocole de l'interface WAN.

WAN Utilisez le menu déroulant pour changer l'interface WAN.

IP src Début Affiche l'adresse IP initiale de source.

IP src Fin Affiche l'adresse IP finale de source.

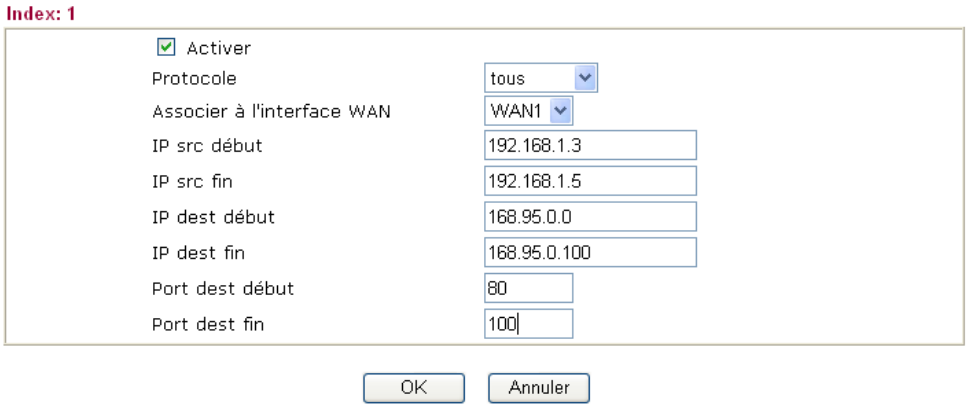
IP dest Début Affiche l'adresse IP initiale de destination.

IP dest Fin Affiche l'adresse IP finale de destination.

Port dest Début Affiche l'adresse IP initiale du port de destination.

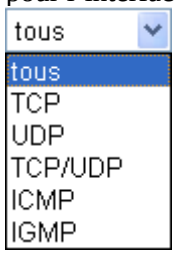
Port dest Fin Affiche l'adresse IP finale du port de destination.

Cliquez sur **Index 1** pour afficher la page de configuration de la règle d'équilibrage de charge.



Activer Cochez cette case pour activer cette règle.

Protocole Utilisez le menu déroulant pour choisir un protocole approprié pour l'interface WAN.



Interface WAN d'affectation Choisissez l'interface WAN d'affectation (WAN1 ou WAN2).

IP src début Tapez l'adresse IP initiale de source pour l'interface WAN spécifiée.

IP src fin Tapez l'adresse IP finale de source pour l'interface WAN spécifiée. Si ce champ est vide, toutes les adresses IP initiales du LAN emprunteront l'interface WAN.

IP dest début Tapez l'adresse IP initiale de destination pour l'interface WAN spécifiée.

IP dest fin Tapez l'adresse IP finale de destination pour l'interface WAN spécifiée. Si ce champ est vide, toutes les adresses IP de destination emprunteront l'interface WAN.

Port dest début Tapez l'adresse IP initiale du port de destination.

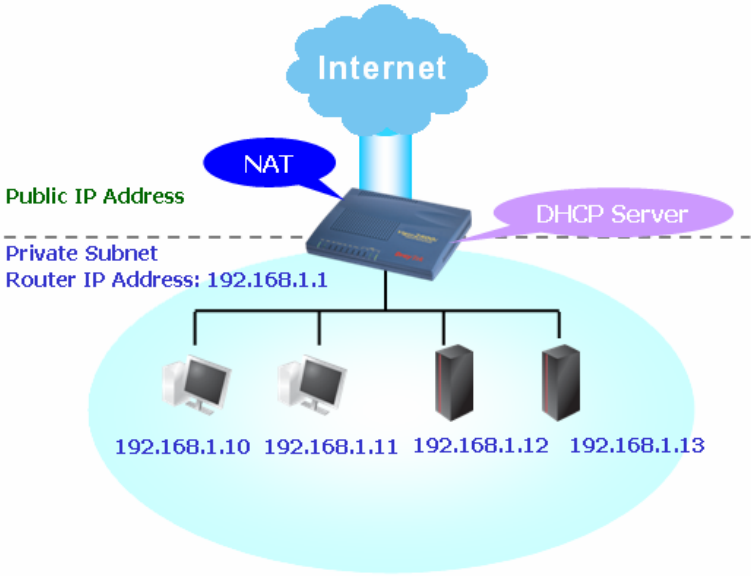
Port dest fin Tapez l'adresse IP finale du port de destination. Si ce champ est vide, tous les ports de destination emprunteront l'interface WAN.

3.2 Réseau local (LAN)

Un réseau local (LAN) est un groupe de sous-réseaux gérés par le routeur. La structure du réseau dépend du type d'adresse IP publiques que votre FAI propose.

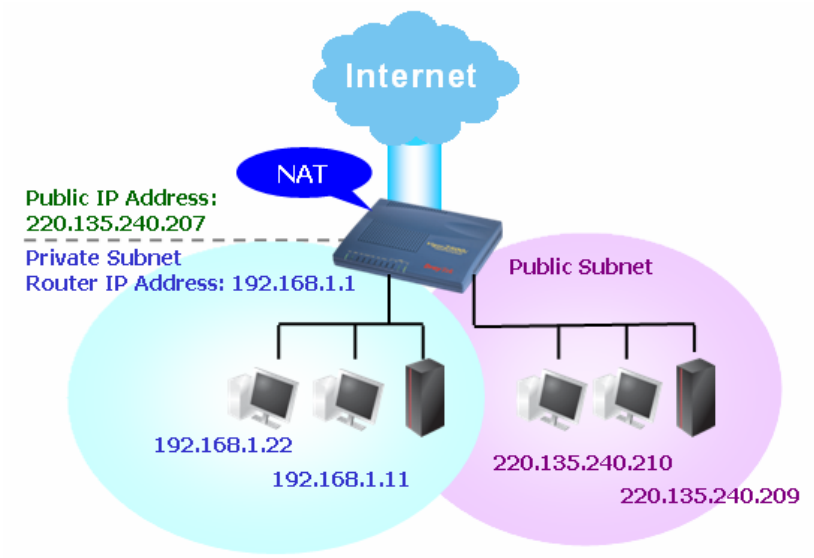
3.2.1 Principes du réseau local

La fonction la plus générique du routeur Vigor est la fonction NAT. Elle crée un sous-réseau privé qui vous est propre. Comme indiqué précédemment, le routeur communique avec les autres hôtes publics sur l'internet à l'aide d'une adresse IP publique et avec les hôtes locaux à l'aide de leur adresse IP privée. Le traducteur d'adresse réseau (NAT) traduit une adresse IP publique en une adresse IP privée afin que les paquets soient acheminés jusqu'à l'hôte à qui ils sont destinés, et vice-versa. En outre, le routeur Vigor comporte un serveur DHCP intégré qui attribue une adresse IP privée à chaque hôte local. Le schéma suivant illustre cela.



DHCP Server	*Serveur DHCP*
Public IP Address	*Adresse IP publique*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*

Dans certains cas, votre FAI peut vous avoir attribué un sous-réseau IP public, par exemple, 220.135.240.0/24. Vous pouvez alors configurer un sous-réseau public, ou 2^{e} sous-réseau, dont chaque hôte possède une adresse IP publique. Dans le cadre du sous-réseau public, le routeur Vigor assure le routage IP afin d'aider les hôtes du sous-réseau public à communiquer avec d'autres hôtes ou serveurs publics extérieurs. Dans ce cas, le routeur doit être configuré en passerelle pour les hôtes publics.



Public IP Address	*Adresse IP publique*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*
Public subnet	*Sous-réseau publique*

Protocole d’information de routage (RIP)

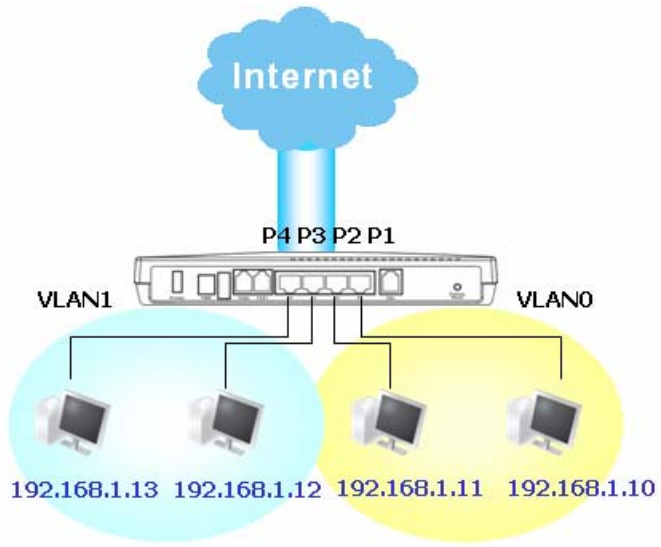
Pour échanger des informations de routage avec les routeurs voisins, le routeur Vigor utilise le protocole d'information de routage (RIP). Cela permet aux utilisateurs de modifier à leur gré les informations du routeur, par exemple, l'adresse IP et les routeurs s'informant mutuellement et automatiquement des modifications faites.

Routes statiques

Lorsque vous avez plusieurs sous-réseaux dans votre LAN, il est quelquefois plus efficace et plus rapide d’utiliser la fonction **Routes statiques**. Avec cette fonction, il vous suffit de définir des règles de transfert des données d'un sous-réseau spécifié à un autre sous-réseau spécifié sans utiliser le RIP.

LAN virtuels et contrôle de débit

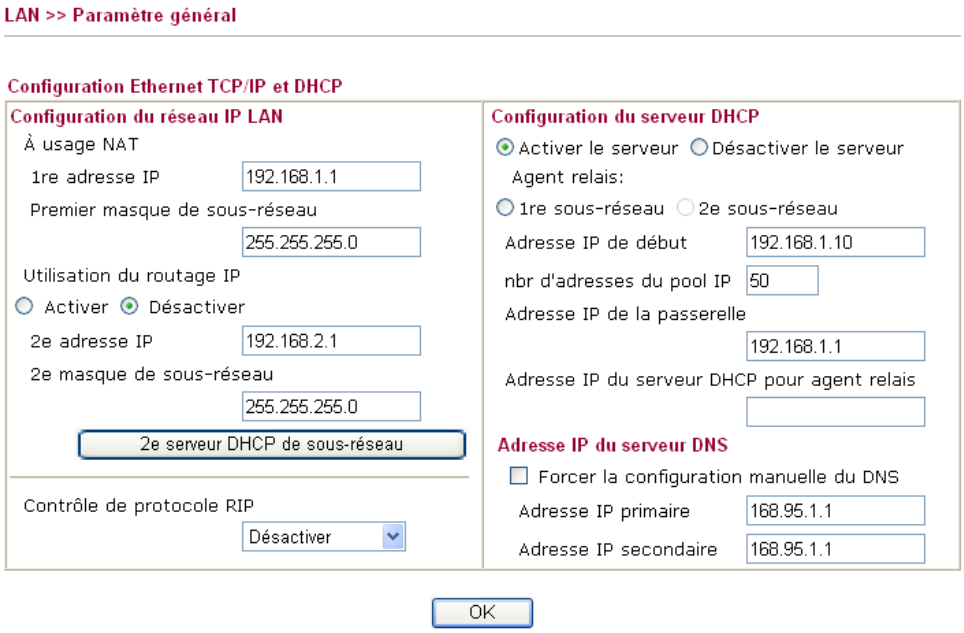
Vous pouvez grouper les hôtes locaux par port physique et créer jusqu'à 4 LAN virtuels. Pour gérer les communications entre les différents groupes, vous pouvez définir des règles dans la fonction LAN virtuel (VLAN) et un débit pour chaque.



3.2.2 Paramètre général

Cette page comporte les paramètres généraux du LAN.

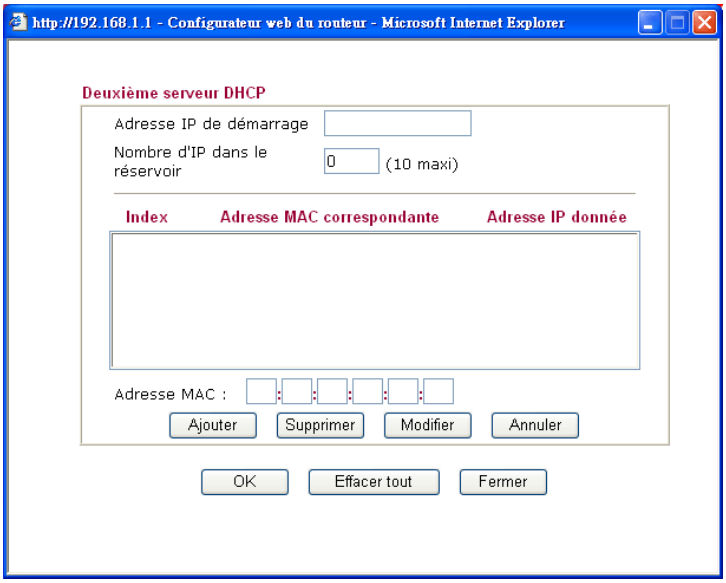
Cliquez sur **LAN** pour ouvrir la page de configuration du LAN et choisissez **Paramètre général**.



1re adresse IP	Adresse IP privée permettant de se connecter à un réseau local (valeur par défaut : 192.168.1.1).
1er masque de sous-réseau	Code d'adresse qui détermine la taille du réseau (valeur par défaut : 255.255.255.0/ 24)
Pour routage IP	Cliquer sur **Activer** pour activer cette fonction. Par défaut, cette fonction est **désactivée**.
2e adresse IP	Adresse IP secondaire permettant de se connecter à un sous-réseau (valeur par défaut : 192.168.2.1/ 24)
2e masque de sous-réseau	Code d'adresse qui détermine la taille du réseau. (valeur par défaut : 255.255.255.0/ 24)

2e serveur DHCP

Vous pouvez configurer le routeur pour qu'il serve de serveur DHCP pour le deuxième sous-réseau.



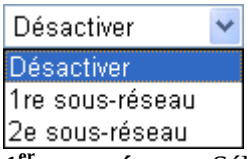
Adresse IP de début : Tapez une valeur du pool d'adresses IP pour définir le début de la plage d'adresses IP qu'attribuera le serveur DHCP. Si la 2e adresse IP de votre routeur est 220.135.240.1, l'adresse IP de début doit être égale ou supérieure à 220.135.240.2 mais inférieure à 220.135.240.254.

Nbr d'adresses du pool IP : Tapez le nombre d'adresses IP du pool (10 maximum). Par exemple, si vous tapez 3 et que la 2e adresse IP de votre routeur est 220.135.240.1, la plage d'adresses IP fournie par le serveur DHCP ira de 220.135.240.2 à 220.135.240.11.

Adresse MAC : Tapez l'adresse MAC des hôtes et cliquez sur **Ajouter** pour créer une liste d'hôtes auxquels sont attribués des adresses IP du pool. La création d'une telle liste pour le 2e serveur DHCP aidera le routeur à attribuer l'adresse IP correcte du sous-réseau correct à l'hôte correct. Ainsi, les hôtes du 2e sous-réseau n'obtiendront pas une adresse IP appartenant au 1er sous-réseau.

Contrôle de protocole RIP

Désactiver le protocole RIP. Cela a pour effet d'arrêter l'échange d'informations de routage entre les routeurs. (Par défaut, le protocole RIP est désactivé).



1er sous-réseau - Sélection du routeur pour modifier les informations RIP du 1er sous-réseau avec information des routeurs voisins.

2e sous-réseau - Sélection du routeur pour modifier les informations RIP du 2e sous-réseau avec information des routeurs voisins.

Configuration du

Le sigle DHCP signifie Dynamic Host Configuration Protocol

serveur DHCP

(protocole de configuration dynamique de machine hôte). Par défaut, le routeur joue le rôle de serveur DHCP pour votre réseau. Il transmet automatiquement les paramètres IP à tout utilisateur local configuré en client DHCP. Il est vivement recommandé de laisser le routeur configuré en serveur DHCP en l'absence de serveur DHCP dans votre réseau.

Si vous voulez utiliser un autre serveur DHCP du réseau au lieu de celui du routeur Vigor, vous pouvez laisser l'agent relais vous aider à rediriger la requête DHCP.

Activer le serveur - Le routeur attribue automatiquement une adresse IP à tous les hôtes du réseau local.
Désactiver le serveur – Vous attribuez manuellement une adresse IP à tous les hôtes du réseau local.
Agent relais – (1er sous-réseau/2e sous-réseau) Spécifiez le sous-réseau où se trouve le serveur DHCP vers lequel l'agent relais doit rediriger la requête DHCP.
Adresse IP de début - Tapez une valeur du pool d'adresses IP pour définir le début de la plage d'adresses IP qu'attribuera le serveur DHCP. Si la 1e adresse de votre routeur est 192.168.1.1, l'adresse IP de début doit être égale ou supérieure à 192.168.1.2 mais inférieure à 192.168.1.254.
Nombre d'adresses du pool IP - Tapez le nombre maximum de PC auquel le serveur DHCP doit attribuer une adresse IP. La valeur par défaut est 50 et la valeur maximale est 253.
Adresse IP de la passerelle - Tapez l'adresse IP de passerelle pour le serveur DHCP. Cette adresse est généralement la même que la 1re adresse IP du routeur, ce qui veut dire que le routeur est la passerelle par défaut.
Adresse IP du serveur DHCP pour l'agent relais - Spécifiez l'adresse IP du serveur DHCP que vous allez utiliser pour que l'agent relais aide à transmettre la requête DHCP au serveur DHCP.

Configuration du serveur DNS

Le sigle DNS signifie Domain Name System (système d'adressage par domaines). Sur l'internet, chaque machine hôte doit avoir une adresse IP unique et peut aussi avoir un nom reconnaissable et facile à mémoriser, comme www.yahoo.com. Le serveur DNS convertit ce nom en l'adresse IP correspondante

Adresse IP primaire - Vous devez spécifier ici une adresse IP de serveur DNS car votre FAI vous en fournira généralement plusieurs. Si votre FAI n'en fournit pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66.
Adresse IP secondaire - Vous pouvez spécifier ici une adresse IP de serveur secondaire car votre FAI vous en fournira plusieurs. Si votre FAI ne vous en fournit pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.

Vous pouvez utilisez la fonction Aide en ligne pour connaître l'adresse IP de serveur DNS par défaut :

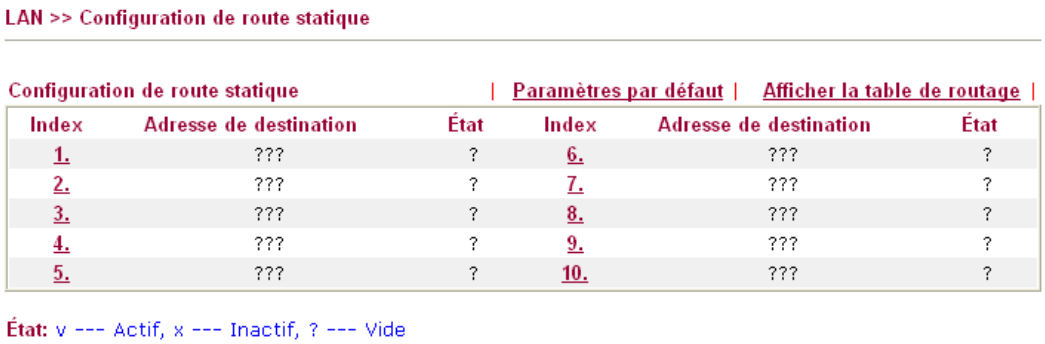
Si les deux champs d'adresse IP primaire et secondaire sont laissés vides, le routeur attribue sa propre adresse IP aux utilisateur locaux en tant que serveur proxy DNS et gère un cache DNS.

Si l'adresse IP d'un nom de domaine se trouve déjà dans le cache DNS, le routeur « résout » immédiatement le nom de domaine. Autrement, le routeur transmet le paquet d'interrogation DNS au serveur DNS externe en établissant une connexion WAN (DSL ou câble).

Des exemples de configurations de LAN sont donnés au Chapitre 4.

3.2.3 Route statique

Cliquez sur **LAN** pour ouvrir la page de configuration et choisissez **Configuration de route statique**.

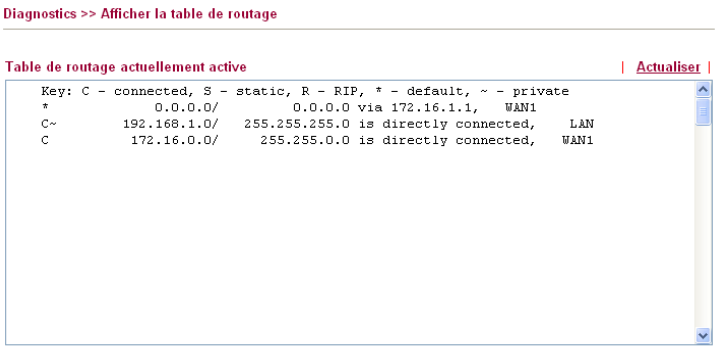


Index Le numéro d'index (1 à 10) vous permet de configurer une route statique.

Adresse de destination Adresse de destination de la route statique.

État État de la route statique.

Afficher la table de routage Affiche la table de routage.



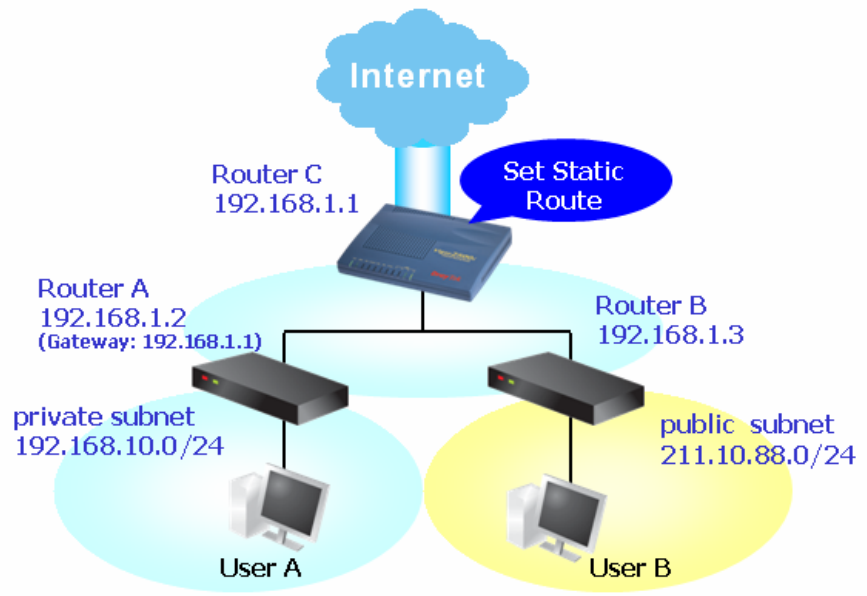
Ajout de routeurs statiques à des réseaux privés et publics

Voici un exemple de configuration d'une route statique dans le routeur principal afin que les utilisateurs A et B se trouvant dans des sous-réseaux différents puissent communiquer par l'intermédiaire du routeur. On suppose que l'accès à l'internet a été configuré et que le routeur fonctionne correctement :

- utilisez le routeur principal pour naviguer sur l'internet.
- créez un sous-réseau privé 192.168.10.0 à l'aide d'un routeur interne A (192.168.1.2)

- créez un sous-réseau public 211.100.88.0 à l'aide d'un routeur interne B (192.168.1.3).
- vous avez configuré le routeur principal 192.168.1.1 comme passerelle par défaut pour le routeur A 192.168.1.2.

Tant qu'une route statique n'a pas été configurée, l'utilisateur A ne peut pas communiquer avec l'utilisateur B car le routeur A ne peut transmettre des paquets reconnus qu'à sa passerelle par défaut, à savoir le routeur principal.

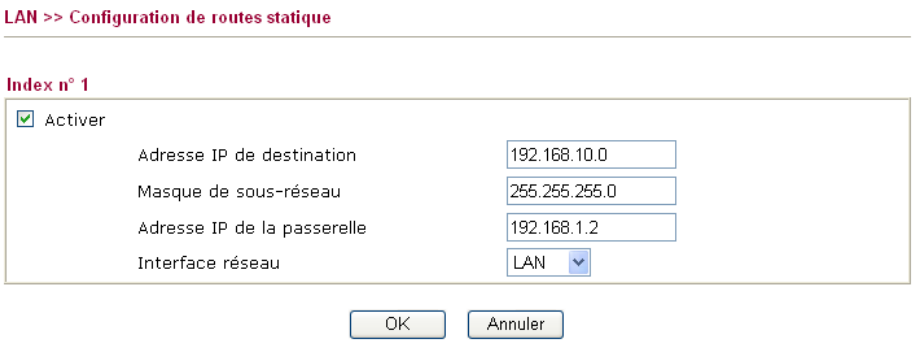


Router A	*Routeur A*
Router B	*Routeur B*
Router C	*Routeur C*
Set static Route	*Configurer une route statique*
private subnet	*sous-réseau privé*
public subnet	*sous-réseau public*
User A	*Utilisateur A*
User B	*Utilisateur B*

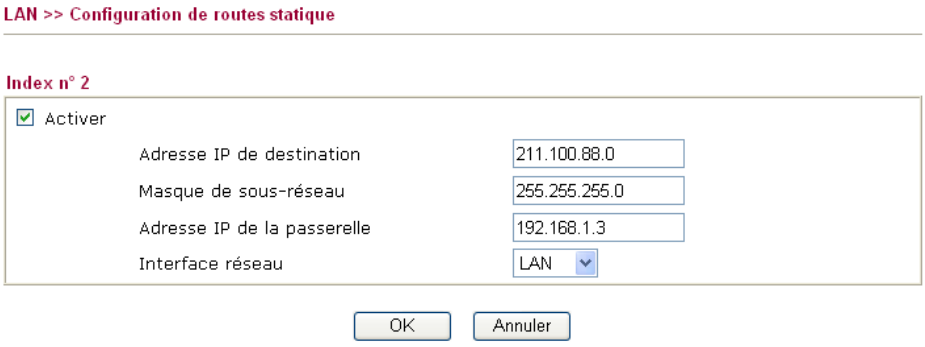
1. Cliquez sur **LAN**, puis sur **Configuration générale**, sélectionnez **Contrôle de protocole RIP** pour le 1er sous-réseau et cliquez sur le bouton **OK**.

   Nota : Nous appliquons le contrôle de protocole RIP au 1er sous-réseau pour deux raisons. La première est que l'interface LAN peut échanger des paquets RIP avec les routeurs voisins via le 1er sous-réseau (192.168.1.0/24). La deuxième est que les hôtes des sous-réseaux privés internes (par exemple, 192.168.10.0/24) peuvent accéder à l'internet via le routeur et échanger en permanence des informations de routage IP avec différents sous-réseaux.

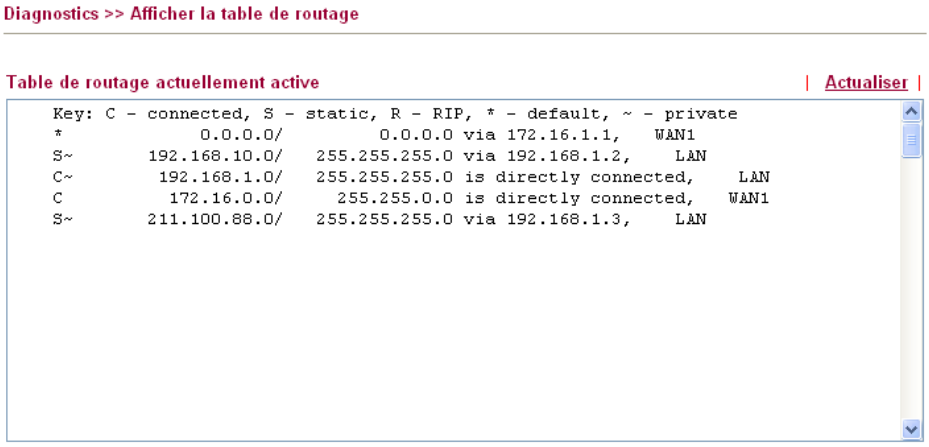
2. Sélectionnez l'option **Configuration de route statique** du menu **LAN** et cliquez sur le numéro d'index 1. Ajoutez une route statique comme indiqué ci-dessous : tous les paquets destinés à 192.168.10.0 seront transmis à 192.168.1.2. Cliquez sur **OK**.



3. Retournez à la page de **Configuration de route statique**. Cliquez sur un autre **Index n°** pour ajouter une autre route statique comme indiqué ci-dessous ; tous les paquets destinés à 211.100.88.0 seront transmis à 192.168.1.3.



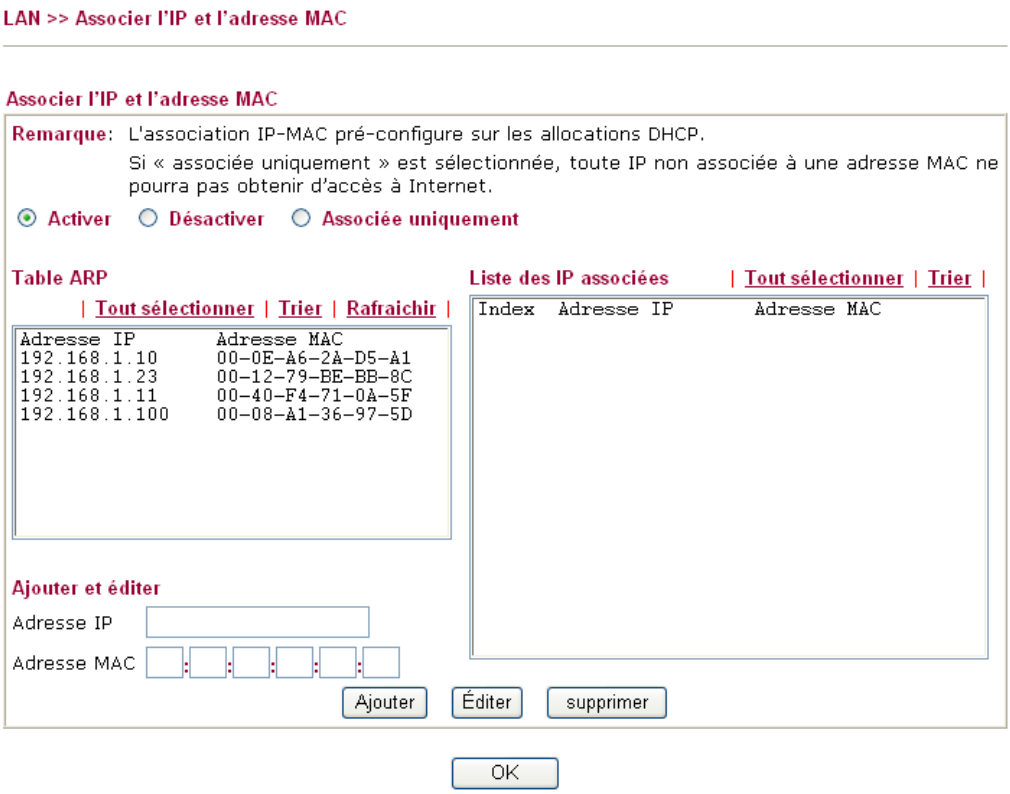
4. Cliquez sur **Diagnostics** puis sur **Table de routage** pour vérifier la table de routage actuelle.



3.2.4 Lien IP-MAC

Cette fonction sert à lier les adresses IP-MAC au sein du LAN pour contrôler plus étroitement le réseau. Lorsque cette fonction est activée, il est impossible de modifier les adresses IP et MAC liées. Si vous modifiez l'adresse IP ou l'adresse MAC, vous risquez de ne plus pouvoir accéder à l'internet.

Cliquez sur **LAN,** puis sur **Lien IP-MAC** pour ouvrir la page de configuration.



Activer	Cliquez sur ce bouton d'option pour activer la fonction. Les adresses IP/MAC qui ne figurent pas dans la liste des liens IP-MAC pourront, elles aussi, se connecter à l'internet.
Désactiver	Cliquez sur ce bouton d'option pour désactiver la fonction. Tous les paramètres de cette page sont alors ignorés.
Lien strict	Cliquez sur ce bouton d'option pour interdire la connexion des adresses IP/MAC qui ne figurent pas dans la liste des liens IP-MAC.
Table ARP	C'est la table ARP du routeur. Elle contient les adresses IP et MAC. Chaque couple d'adresses IP et MAC de la table ARP peut être sélectionnée et ajoutée à la liste des liens IP-MAC en cliquant sur **Ajouter**.
Ajouter et modifier	**Adresse IP** – Tapez l'adresse IP à lier à l'adresse Mac spécifiée. **Adresse Mac** – Tapez l'adresse MAC à lier à l'adresse IP spécifiée.
Actualiser	Actualise la table ARP. Lorsqu' un nouveau PC est ajouté au LAN, vous pouvez cliquer sur ce lien pour obtenir la table ARP actualisée.
Liste des liens IP-MAC	Affiche une liste des adresses IP et MAC liées.
Ajouter	Ce bouton vous permet d' ajouter la couple d' adresses choisie dans la table ARP où les adresses IP/MAC entrées dans la zone **Ajouter et modifier** à la **Liste des liens IP-MAC**.
Modifier	Ce bouton vous permet de modifier les adresses IP et MAC sélectionnées.

Supprimer	Vous pouvez supprimer n'importe quel élément de la **liste des liens IP-MAC**. Cliquez sur la ligne à supprimer, puis sur **Supprimer**.

Nota : avant de sélectionner **Lien strict**, il faut avoir créer un lien IP-MAC pour un PC. Sinon, aucun des PC ne pourra accéder à l'internet et le configurateur web du routeur risque d'être inaccessible.

3.3 NAT

Généralement, le routeur se comporte comme un routeur traducteur d'adresse réseau (NAT). Le traducteur d'adresse réseau (NAT) convertit une ou plusieurs adresses IP en une seule adresse IP publique. L'adresse IP publique est généralement attribuée par votre FAI qui peut vous la facturer. Les adresses IP privées ne sont reconnues que par les hôtes internes.

Lorsque des paquets sortants à destination d'un serveur public sur l'internet parviennent au routeur NAT, celui-ci traduit l'adresse d'origine en l'adresse IP publique qui lui a été attribuée, sélectionne le port public disponible, puis transmet les paquets. En même temps, le routeur consigne la correspondance adresse-port dans une table. Lorsque le serveur public répond, c'est à l'adresse publique du routeur qu'arrive le trafic entrant et le routeur effectue la traduction inverse. Ainsi, l'hôte interne peut communiquer avec l'hôte externe d'une manière transparente.

La traduction d'adresse réseau présente plusieurs avantages, dont les suivants :

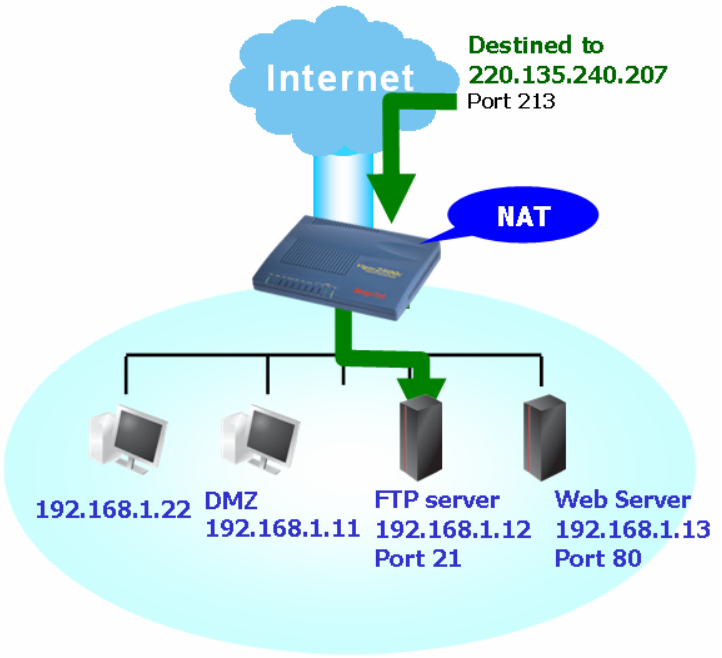
- **Un avantage économique par l'utilisation efficace de l'adresse IP.** Le NAT permet de traduire les adresses IP internes des hôtes locaux en une seule adresse IP publique. Il suffit donc d'avoir une seule adresse IP publique pour tous les hôtes internes.
- **Elle renforce la sécurité du réseau interne en cachant les adresses IP privées.** De nombreuses attaques utilisent l'adresse IP. Comme l'attaquant ne peut connaître aucune des adresses IP privées, la fonction NAT peut protéger le réseau interne.

Dans la page NAT est affichée l'adresse IP privée définie par le RFC 1918. Nous utilisons généralement le sous-réseau 192.168.1.0/24 pour le routeur. Comme il a été dit plus haut, la fonctionnalité NAT peut transposer une ou plusieurs adresses IP, un ou plusieurs ports de service en différents services. En d'autres termes, la fonctionnalité NAT peut être mise en œuvre en utilisant le mappage de ports.

Les options du menu NAT sont les suivantes.

3.3.1 Redirection de ports

La redirection de ports sert généralement pour la mise en œuvre de services au sein du réseau local (LAN) : serveurs web, serveurs FTP, serveurs de messagerie, etc. Dans la plupart des cas, il vous faut une adresse IP publique pour chaque serveur et la combinaison adresse IP publique/nom de domaine est reconnue par tous les utilisateurs. Comme le serveur est situé à l'intérieur du LAN et que le réseau est bien protégé par le NAT du routeur identifié par son adresse/port IP privés, la fonction de redirection de ports transmet toutes les demandes d'accès provenant d'utilisateurs externes au mécanisme de mappage de ports du serveur.



Destined to	*Trafic à destination de*
FTP Server	*Serveur FTP*
Web Server	*Serveur web*

La redirection de ports ne s'applique qu'au trafic entrant.

Pour utiliser cette fonction, affichez la page **NAT** et sélectionnez **Redirection de ports**. La **table de redirection de ports** permet de définir 10 redirections pour les machines hôte internes.

Mode Deux options s'offrent à vous : sélectionnez Plage pour définir une plage de ports à rediriger.

Nom du service Tapez la désignation du service de réseau.

Protocole Sélectionnez le protocole de transport (TCP ou UDP).

Port public Spécifiez quel port doit être redirigé vers **l'adresse IP privée et le port privé** spécifiés. Si vous choisissez **Plage** comme mode de redirection de ports, deux zones de saisie apparaissent. Tapez le numéro voulu dans la première zone. La deuxième zone sera remplie automatiquement par la suite.

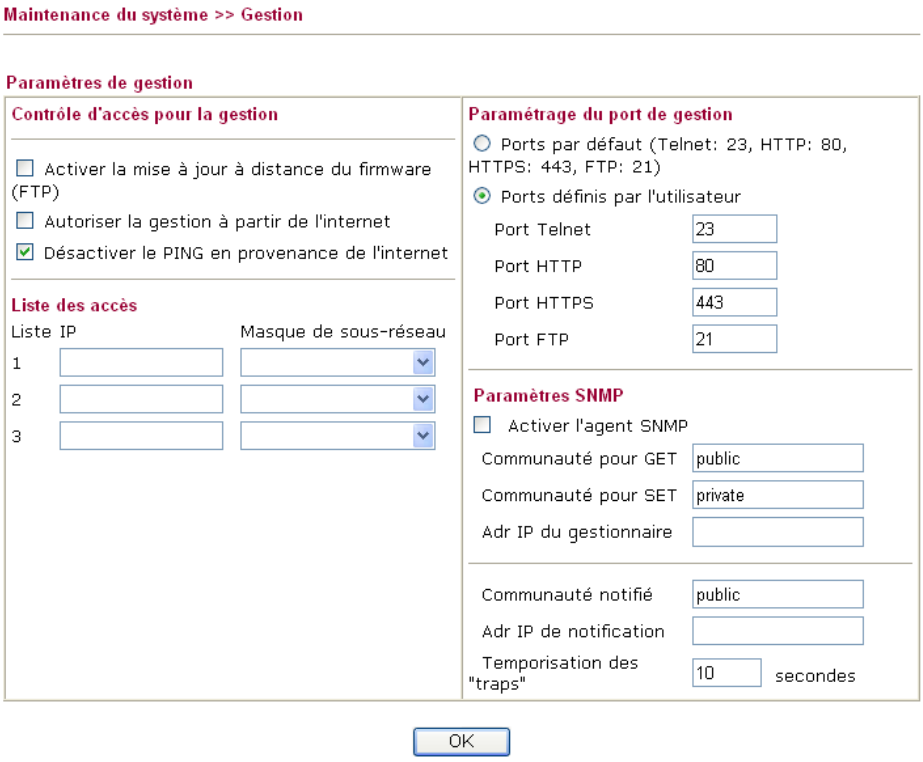
Adresse IP privée Spécifiez l'adresse IP privée de la machine hôte interne offrant le service. Si vous choisissez **Plage** comme mode de redirection de ports, deux zones apparaissent. Tapez une adresse IP complète dans la première zone (adresse de début) et les quatre chiffres dans la deuxième zone (adresse de fin).

Port privé Spécifiez le numéro de port privé du service offert par la machine hôte interne.

Actif Cochez cette case pour activer la redirection.

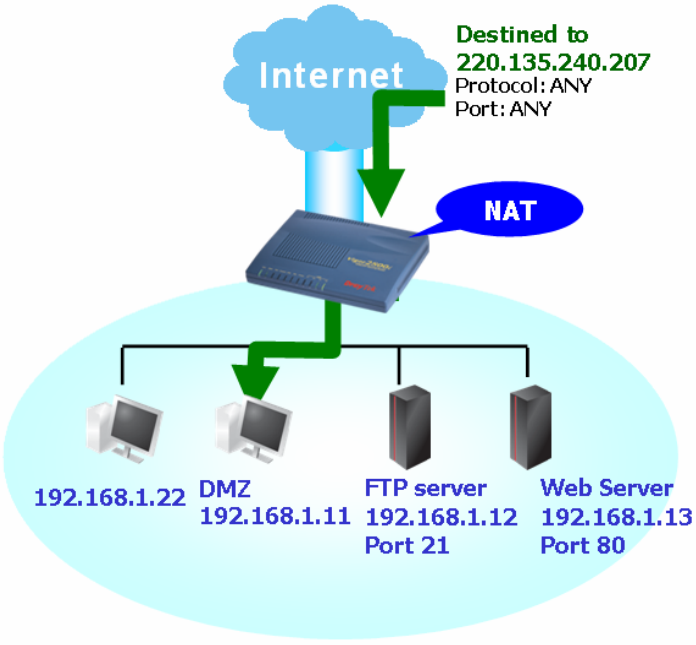
À noter que le routeur a ses propres services intégrés (serveurs), comme Telnet, HTTP, FTP, etc. Comme ces services (serveurs) ont le même numéro de port, il peut être nécessaire de réinitialiser le compteur afin d'éviter les conflits.

Par exemple, le configurateur web du routeur a comme port par défaut le port 80, il peut y avoir conflit avec le serveur web du réseau local, http://92.168.1.13:80. Par conséquent, il vous faut **définir comme port http du routeur un port autre que le port par défaut 80** pour éviter un conflit. À partir du menu **Maintenance du système >>Paramètres de gestion**, accédez à l'écran d'administration en faisant suivre l'adresse IP de 8080, par exemple : http://192.168.1.1:8080.



3.3.2 Configuration de l’hôte DMZ

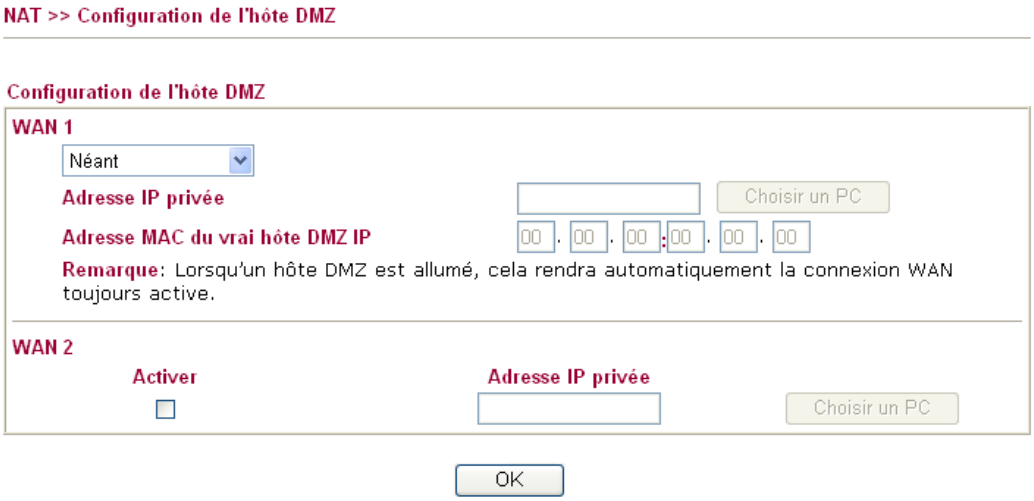
Comme indiqué plus haut, la **redirection de ports** peut rediriger les paquets TCP/UDP entrants ou autre trafic arrivant sur des ports particuliers vers l'adresse IP privée et le port privé d'un hôte du LAN. Toutefois, d'autres protocoles IP, comme les protocoles 50 (ESP) et 51 (AH) n'ont pas un port fixe. Le routeur Vigor a une fonction « **hôte DMZ** » qui vous permet de faire en sorte que TOUTES les données non sollicitées soient transmises, quel que soit le protocole, vers un hôte déterminé du LAN. La navigation normale sur l’internet et autres activités de ce genre des autres clients peuvent se poursuivre sans interruption intempestive. **L'hôte DMZ** permet d'exposer un utilisateur interne déterminé sur l'internet afin d'utiliser certaines applications spéciales, comme Netmeeting, des jeux internet, etc.



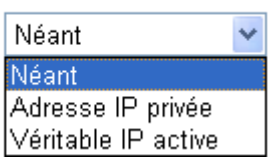
Destined to	*Trafic à destination de*
FTP Server	*Serveur FTP*
Web Server	*Serveur web*

Si vous configurer un hôte DMZ, vous compromettez dans une certaine mesure les propriétés de sécurité inhérentes au NAT. Vous pouvez envisager d'ajouter des règles de filtrage supplémentaires ou un pare-feu secondaire.

Cliquez sur **Hôte DMZ** pour ouvrir la page suivante :



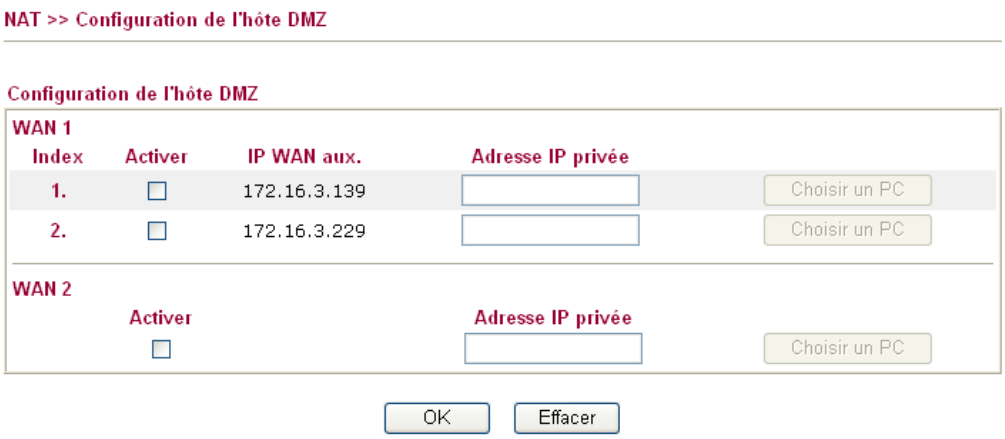
WAN1 Cette page vous permet de choisir entre une adresse IP privée ou une adresse IP vraie active pour l'hôte DMZ.



Adresse IP privée Si vous avez choisi Adresse IP privée, tapez l'adresse IP privée ou sélectionnez-en une en cliquant sur le bouton Choisir un PC.

Adresse MAC de l'hôte DMZ à « adresse IP vraie » Si vous avez choisi Adresse IP vraie active, tapez l'adresse MAC dans ces champs.

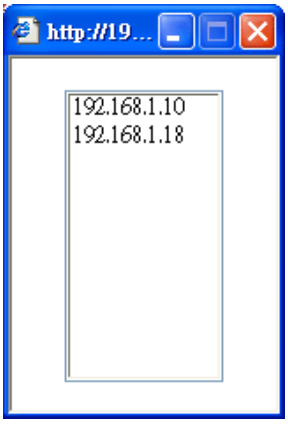
Si vous avez défini précédemment une série **d'alias WAN** dans **Accès à l'internet >>PPPoE/PPPoA** ou **Accès à l'internet >>MPoA,** vous les trouverez dans la **liste IP WAN aux**.



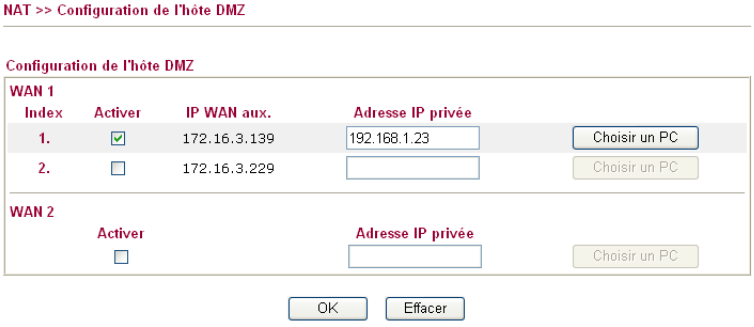
Activer Cochez cette case pour activer la fonction hôte DMZ.

Adresse IP privée Entrez l'adresse IP privée de l'hôte DMZ ou cliquez sur Choisir un PC pour sélectionner une adresse IP privée.

Choisir un PC Cliquez sur ce bouton pour faire apparaître une fenêtre affichant une liste des adresses IP privées de tous les hôtes de votre réseau local. Sélectionnez-en une comme adresse de l'hôte DMZ.



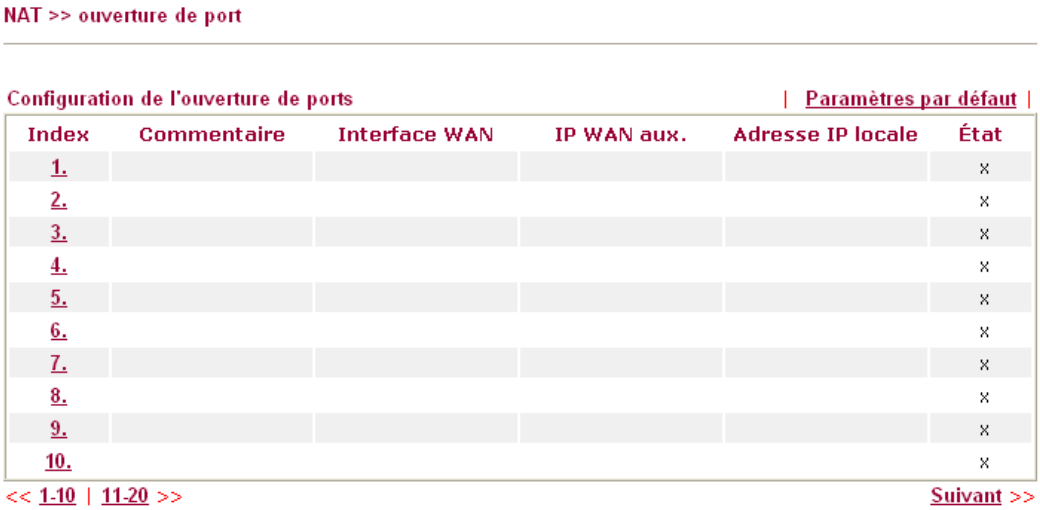
Une fois que vous avez sélectionné une adresse IP privée dans la boîte de dialogue ci-dessus, cette adresse IP est affichée dans l'écran suivant. Cliquez sur OK pour enregistrer les paramètres.



3.3.3 Ouverture de ports

La fonction d'**ouverture de ports** vous permet d'ouvrir une plage de ports pour des applications spéciales dont les plus courantes sont les applications de partage de fichiers entre homologues dites P2P (BT, KaZaA, Gnutella, WinMX, eMule et autres), les caméras internet, etc. Veillez à tenir à jour les applications pour éviter d'être victime de l'exploitation éventuelle de failles de sécurité.

Cliquez sur **Ouverture de Ports** pour ouvrir la page suivante :


NAT >> ouverture de port

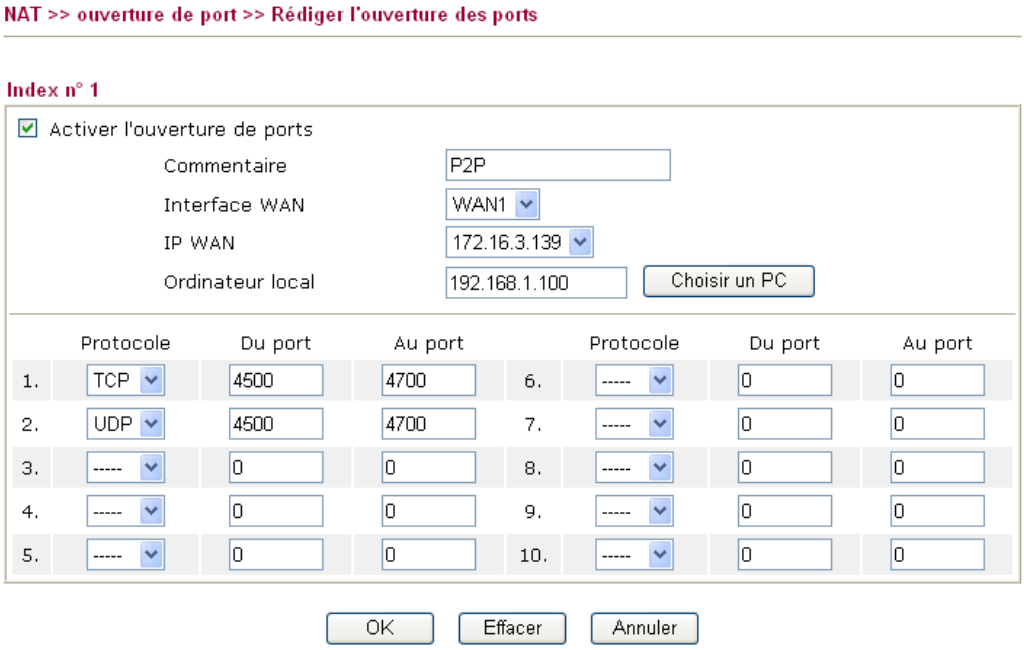
Configuration de l'ouverture de ports | Paramètres par défaut |

Index	Commentaire	Interface WAN	IP WAN aux.	Adresse IP locale	État
1.					x
2.					x
3.					x
4.					x
5.					x
6.					x
7.					x
8.					x
9.					x
10.					x

<< 1-10 | 11-20 >> Suivant >>

Index	Numéro d'ordre de la redirection de port à définir. Cliquez sur le numéro approprié pour modifier ou effacer la redirection correspondante.
Commentaire	Spécifiez le nom du service réseau.
Interface WAN	Affiche l'interface WAN concernée.
Adresse IP locale	Adresse IP privée de l'hôte local pour un service.
État	État de la redirection correspondante. X = redirection inactive, V = redirection active.

Pour ajouter des ports ou modifier le paramétrage de ports, cliquez sur un numéro d'index. La page de paramétrage correspondante apparaît. Pour chaque index, vous pouvez spécifier **10** plages de ports pour divers services.



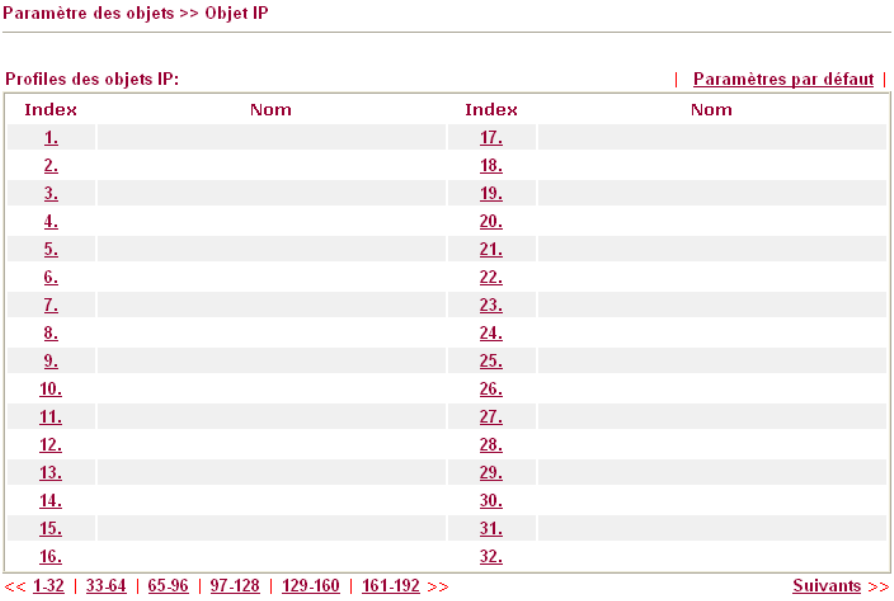
Activer l'ouverture de ports	Cochez cette case pour activer cet index
Commentaire	Tapez la désignation de l'application ou du service de réseau.
Interface WAN	Spécifiez l'interface WAN concernée.
IP WAN	Choisissez l'une des adresses IP WAN dans la liste déroulante. Ce choix n'est possible et visible que si vous avez défini précédemment un alias IP WAN.
Ordinateur local	Tapez l'adresse IP privée de l'hôte local ou cliquez sur Choisir un PC pour en sélectionner une.
Choisir un PC	Cliquez sur ce bouton pour faire apparaître une fenêtre affichant la liste des adresses IP privées des hôtes locaux. Sélectionnez une adresse IP appropriée dans la liste.
Protocole	Spécifiez le protocole de couche transport : TCP, UDP ou ----- (NÉANT).
Du Port	Spécifiez le numéro du premier port de la plage de ports.
Au Port	Spécifiez le numéro du dernier port de la plage de ports.

3.4 Objets et groupes

On a la possibilité de créer des ***objets*** définissant des plages d'adresses IP et de les lier à des ***groupes***. Par la suite, on peut sélectionner un objet ou un groupe particulier à appliquer globalement. Par exemple, toutes les adresses IP d'un même service peuvent être définies avec un objet IP (plage d'adresses IP).

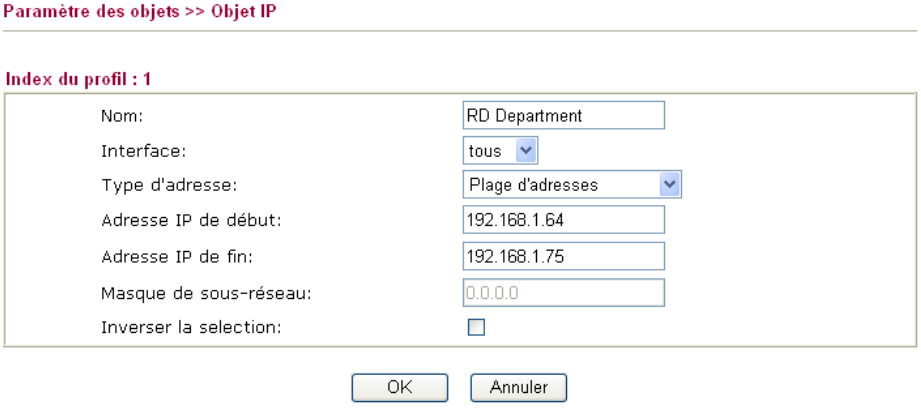
3.4.1 Objet IP

Vous pouvez paramétrer jusqu'à 192 profils d'objet IP avec des conditions différentes.



Paramètres par défaut Effacer tous les profils.

Cliquez sur le numéro qui se trouve dans la colonne Index pour paramétrer un profil.



Nom Tapez un nom pour le profil (15 caractères maximum).

Interface	Choisissez une interface appropriée (WAN, LAN ou bien Any, c'est-à-dire n'importe laquelle). Interface: tous (tous, LAN, WAN) Par exemple, le paramètre **Sens** de la page **Modifier la règle de filtrage** impose de spécifier une adresse IP ou une plage d'adresses IP pour l'interface WAN ou LAN ou encore n'importe quelle adresse IP. Si vous choisissez LAN comme **interface** ici et LAN comme sens dans la page **Modifier la règle de filtrage**, vous pourrez choisir dans celle-ci toutes les adresses IP spécifiées avec l'interface LAN.
Type d'adresse	Type d'adresse IP. Sélectionnez **Adresse unique** si cet objet contient une seule adresse IP. Sélectionnez **Plage d'adresses** si cet objet contient plusieurs adresses IP d'une plage. Sélectionnez **Adresse de sous-réseau** si cet objet contient un sous-réseau. Sélectionnez **N'importe quelle adresse** si cet objet contient n'importe quelle adresse.
Adresse IP de début	Tapez l'adresse IP unique si Adresse unique a été sélectionnée comme type d'adresse ou l'adresse IP de début si Plage d'adresses a été sélectionnée comme type d'adresse.
Adresse IP de fin	Tapez l'adresse IP de fin si Plage d'adresses a été sélectionnée comme type d'adresse.
Masque de sous-réseau	Tapez le masque de sous-réseau si Adresse de sous-réseau a été sélectionnée comme type d'adresse.
Inverser la sélection	Si cette case est cochée, toutes les adresses IP seront appliquées à l'exception de celles spécifiées ci-dessus.

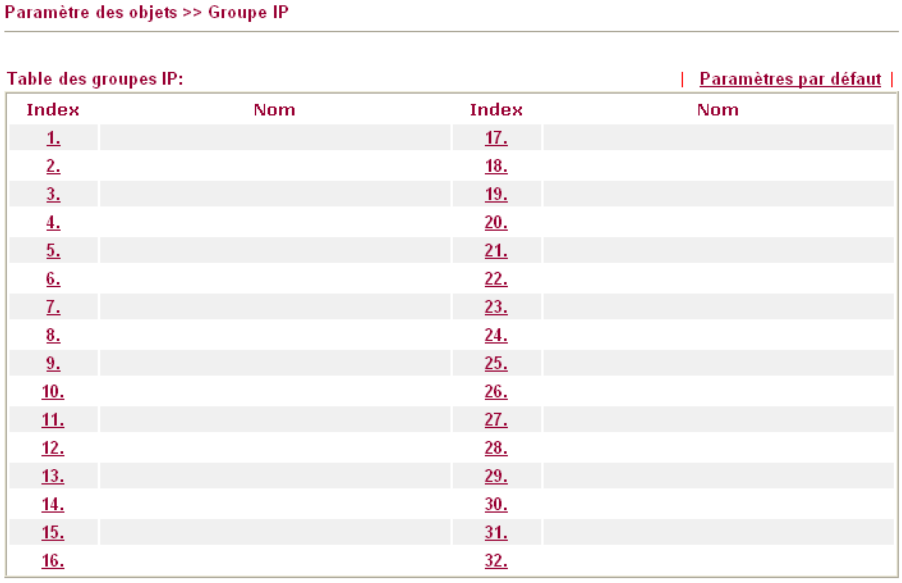
Exemple d'objets IP paramétrés.

Profiles des objets IP:

Index	Nom	Index
1.	RD Department	17.
2.	Financial Dept.	18.
3.	HR Department	19.
4.		20.
5.		21.

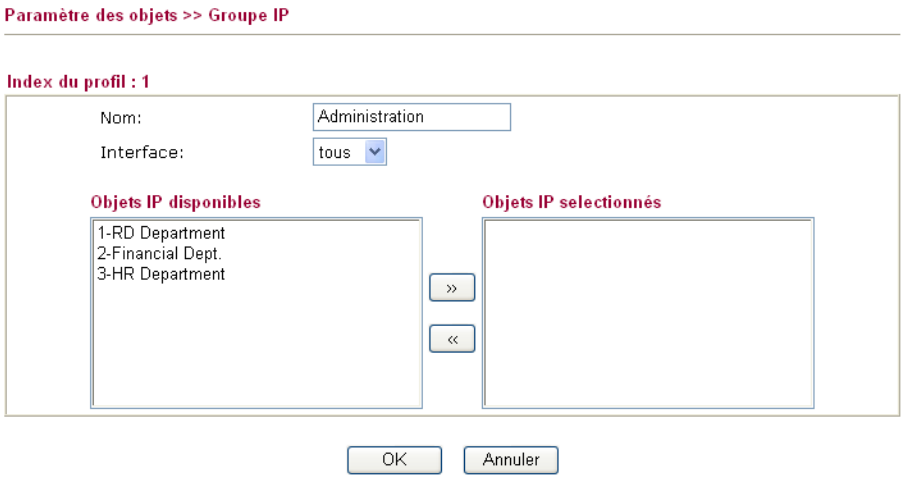
3.4.2 Groupe IP

Cette page vous permet de lier plusieurs objets IP à un groupe IP.



Paramètres par défaut Effacer tous les profils.

Cliquez sur le numéro qui se trouve dans la colonne Index pour paramétrer un profil.



Nom Tapez un nom pour le profil (15 caractères maximum).

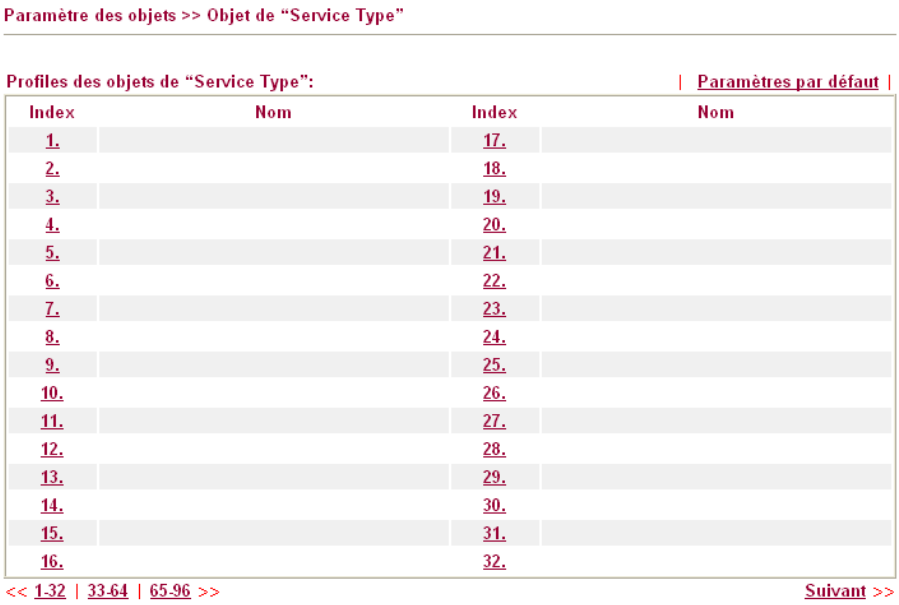
Interface Choisissez WAN, LAN ou encore Any (c'est-à-dire n'importe laquelle) pour afficher tous les objets IP disponibles avec l'interface spécifiée.

Objets IP disponibles Tous les objets IP disponibles avec l'interface spécifiée sont affichés dans cette boîte de liste.

Objets IP spécifiés Cliquez sur le bouton >> pour ajouter les objets IP sélectionnés dans cette boîte de liste.

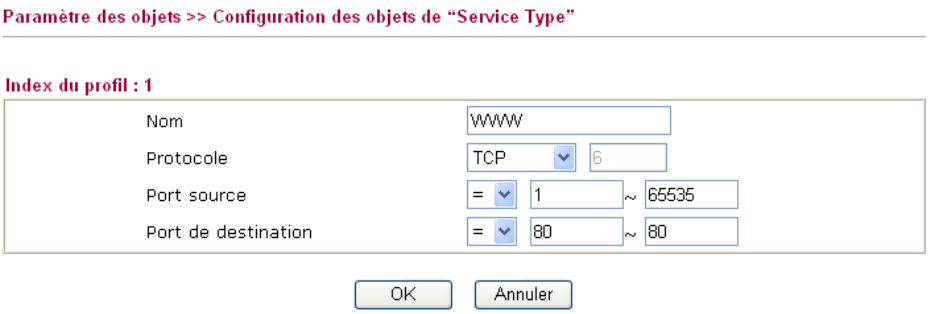
3.4.3 Objet type de service

Vous pouvez paramétrer 96 objets type de service avec des conditions différentes.



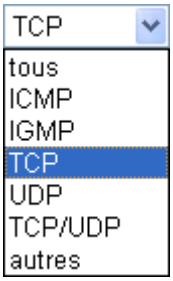
Paramètres par défaut Effacer tous les profils.

Cliquez sur le numéro qui se trouve dans la colonne Index pour paramétrer un profil.



Nom Tapez un nom pour ce profil.

Protocole Spécifiez le ou les protocoles auxquels ce profil s'appliquera.



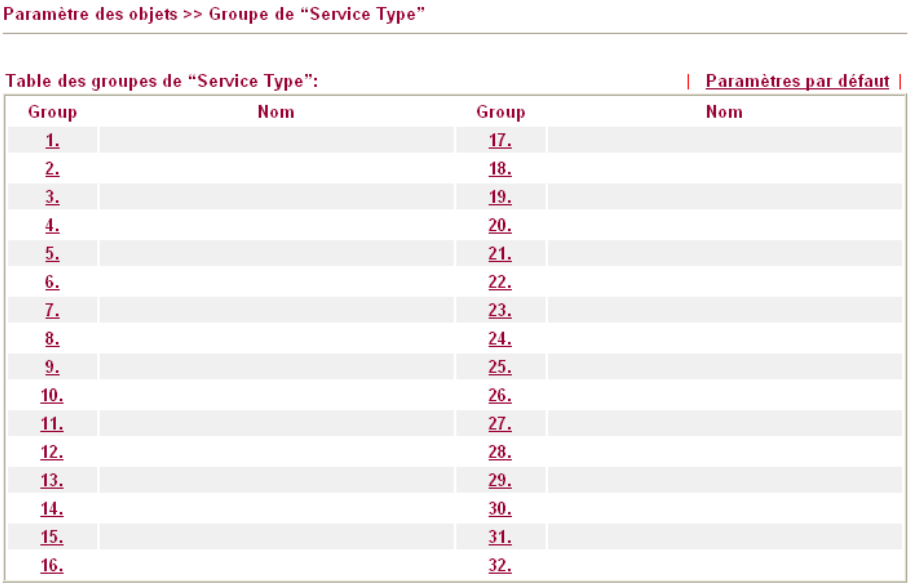
Port de source/ Port de destination Ces deux paramètres sont là pour le protocole TCP/UDP. Ils peuvent être ignorés pour les autres protocoles.
(=) – si les deux valeurs sont identiques, ce profil vaut pour un seul port ; si les deux valeurs sont différentes, ce profil vaut pour une plage de ports.
(!=) – si les deux valeurs sont identiques, ce profil vaut pour tous les ports à l'exception du port défini ici ; si les deux

valeurs sont différentes, ce profil vaut pour tous les ports à l'exception de la plage de ports définie ici.
(>) – ce profil vaut pour tous les ports de numéro supérieur à cette valeur.
(<) – ce profil vaut pour tous les ports de numéro inférieur à cette valeur.

Exemple d'objets type de service paramétrés.

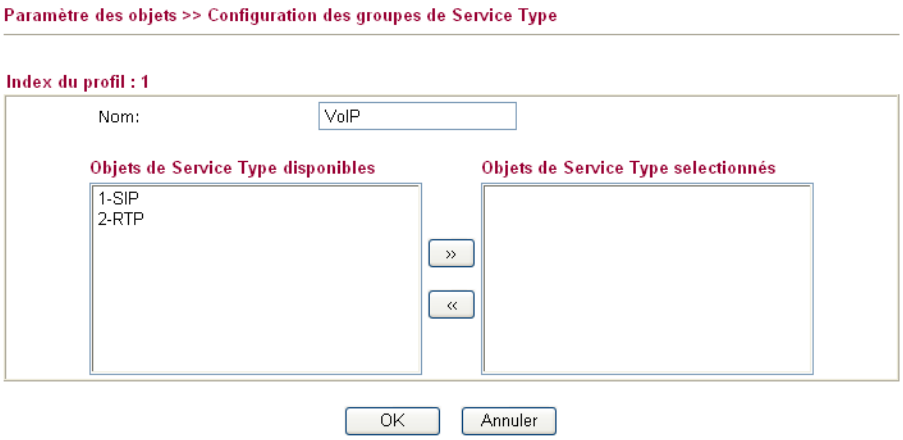
3.4.4 Groupe type de service

Cette page vous permet de lier plusieurs objets type de service à un groupe.



Paramètres par défaut Effacer tous les profils.

Cliquez sur le numéro qui se trouve dans la colonne Index pour paramétrer un profil.



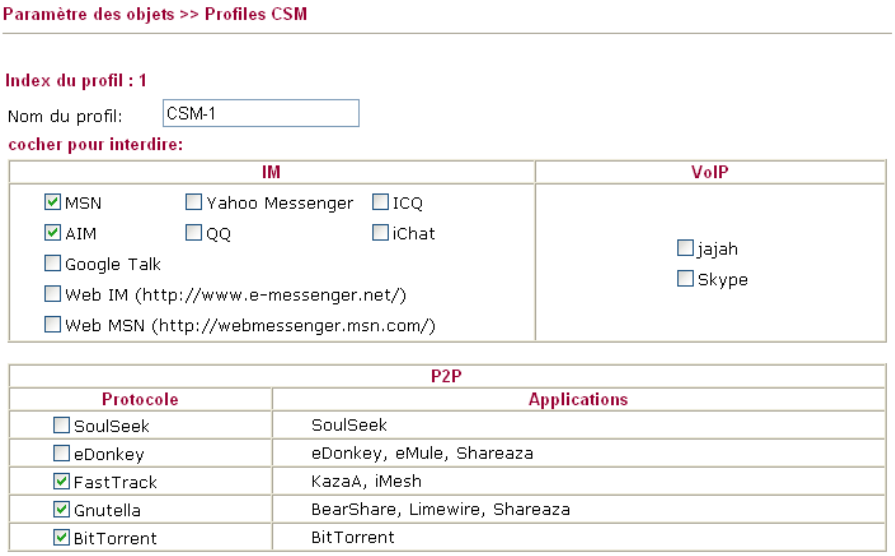
Nom	Tapez un nom pour ce profil.
Objets type de service disponibles	Tous les objets type de service disponibles sont affichés dans cette boîte de liste.
Objets type de service sélectionnés	Cliquez sur le bouton >> pour ajouter les objets type de service sélectionnés dans cette boîte de liste.

3.4.5 Profil CSM

Vous pouvez définir des profils de règles applicables aux applications de messagerie instantanée (IM) et de partage de fichiers entre homologues (P2P). Un profil CSM peut être utilisé dans la page Paramétrage des filtres.

Paramètres par défaut	Effacer tous les profils.

Cliquez sur le numéro qui se trouve dans la colonne Index pour paramétrer un profil.



Nom de profil	Tapez un nom pour le profil CSM.

Vous pouvez interdire l'utilisation de différentes applications de messagerie instantanée (IM), de téléphonie sur IP (VoIP) et de partage de fichiers entre homologues (P2P). Cochez la ou

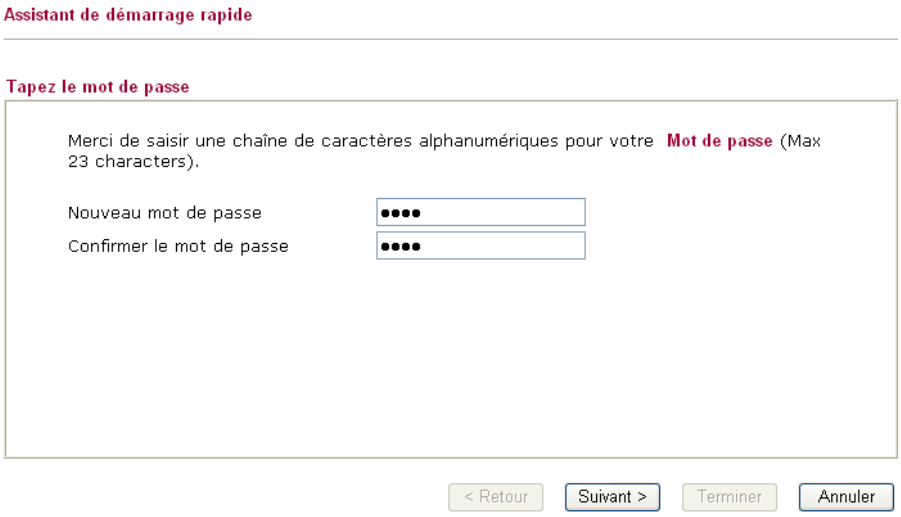
les cases correspondantes, puis cliquez sur **OK**. Par la suite, dans la page **Pare-feu>>Modifier le filtre>>Modifier la règle de filtrage**, vous pourrez choisir dans la liste déroulante **Gestion de contenu** le profil CSM approprié.

3.5 Pare-feu

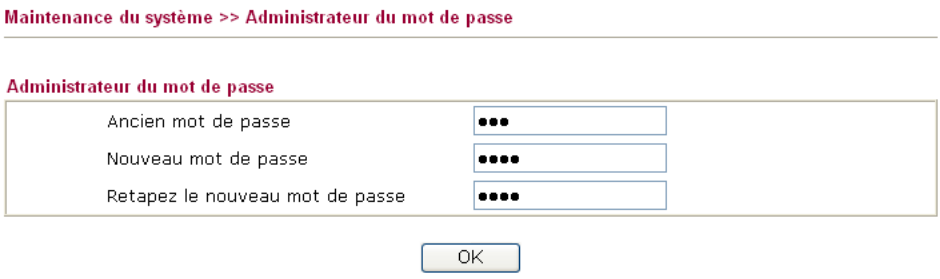
3.5.1 Principes du pare-feu

À l'heure où les utilisateurs d'accès à haut débit demandent plus de bande passante pour le multimédia, les applications interactives ou le téléenseignement, la sécurité devient la priorité des priorités. Le pare-feu du routeur Vigor contribue à protéger votre réseau local contre les attaques extérieures. Il permet également de restreindre l'accès des utilisateurs locaux à l'internet. En outre, il permet d'identifier des paquets spécifiques à la réception desquels le routeur va établir une connexion de départ.

La mesure de sécurité la plus élémentaire consiste à définir un nom d'utilisateur et un mot de passe lors de l'installation de votre routeur. En définissant un nom d'utilisateur et un mot de passe administrateur, vous empêcherez l'accès non autorisé aux menus de configuration du routeur à partir de votre routeur.



Si vous n'avez pas défini de mot de passe lors de l'installation, passez en mode **Maintenance du système**.



Fonctionnalités de pare-feu

Les utilisateurs en réseau sont protégés par les fonctions de pare-feu suivantes :

- Filtre de paquets configurable par l'utilisateur (filtre d'appel/filtre de données).
- Inspection des paquets en fonction de l'état de la connexion (filtrage adaptatif) : refus des données entrantes non sollicitées.
- Protection anti-DoS/DdoS.

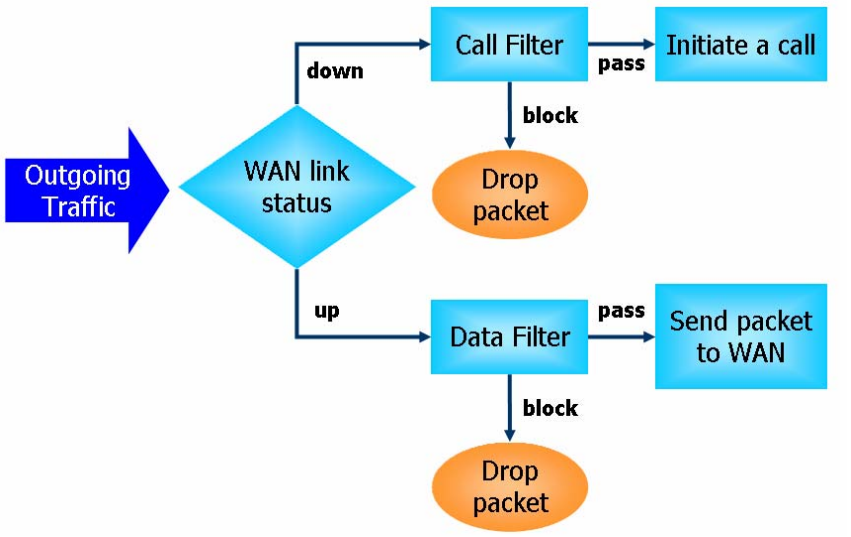
- Filtre de contenu d'URL.

Filtres IP

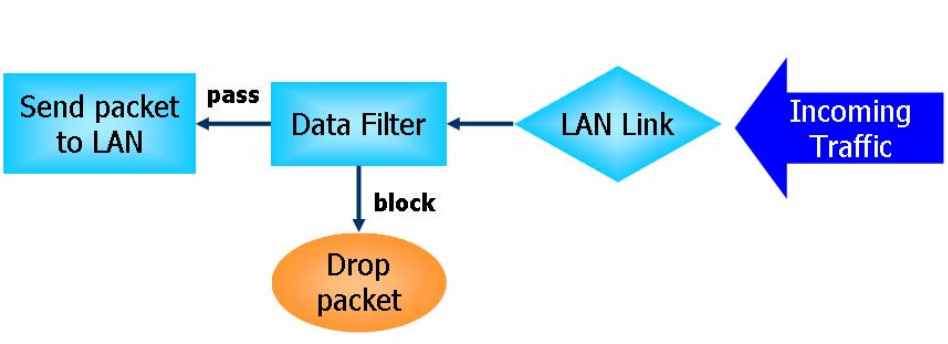
Selon qu'une connexion internet est active ou non ou, en d'autres termes, selon que « la connexion WAN est établie ou non », l'architecture des filtres IP met en œuvre deux types de filtres : le **filtre d'appel** et le **filtre de données.**

- **Filtre d'appel -** En l'absence de connexion internet active, le **filtre d'appel** est appliqué à tout le trafic, lequel, en l'occurrence, est du trafic de départ. Il vérifie chaque paquet selon les règles de filtrage et laisse passer le paquet s'il est licite. Le routeur déclenche alors un **appel** pour établir la connexion internet et transmettre le paquet.
- **Filtre de données** - Si une connexion internet est active, le **filtre de données** est appliqué au trafic d'arrivée et de départ. Il vérifie les paquets selon les règles de filtrage et les transmet au routeur s'ils sont licites.

Le processus de filtrage du trafic entrant et du trafic sortant est représenté schématiquement ci-après.



down	*inactif*
Call Filter	*Filtre d'appel*
pass	*laisse passer*
Initiale a call	*Déclenchement d'un appel*
block	*bloque*
Outgoing Traffic	*Trafic sortant*
WAN link status	*État de la connexion WAN*
Drop packet	*Rejet du paquet*
up	*actif*
Data Filter	*Filtre de données*
pass	*laisse passer*
block	*bloque*
Send packet to WAN	*Envoi du paquet sur le WAN*
Drop packet	*Rejet du paquet*



Send packet to WAN	*Envoi du paquet sur le WAN*
pass	*laisse passer*
Data Filter	*Filtre de données*
block	*bloque*
Drop packet	*Rejet du paquet*
LAN Link	*Connexion LAN*
Incoming Traffic	*Trafic entrant*

Filtrage adaptatif (SPI)

L'inspection des paquets en fonction de l'état de la connexion ou filtrage adaptatif est une architecture de pare-feu qui fonctionne au niveau de la couche réseau. À la différence du filtrage statique des paquets qui examine un paquet sur la base des informations de son en-tête, le filtrage adaptatif crée une machine à états qui contrôle la connexion via toutes les interfaces du pare-feu. Le pare-feu adaptatif du routeur Vigor ne se contente pas d'examiner l'en-tête ; il contrôle également l'état de la connexion.

Gestion de la sécurité des contenus (CSM)

Avec la popularité croissante des applications de messagerie instantanée, les communications peuvent devenir beaucoup plus faciles. Néanmoins, si certaines industries peuvent mettre à profit cet outil pour communiquer avec leurs clients, d'autres peuvent adopter une attitude plus réservée afin de réduire son utilisation abusive par les employés pendant les heures de travail ou pour éviter les failles de sécurité inconnues. Il en va de même pour les applications « peer to peer » car les partages de fichiers, s'ils peuvent être commodes, peuvent aussi poser des problèmes de sécurité. C'est pourquoi le routeur Vigor comporte une fonction CSM.

Protection contre les attaques de type « déni de service » (DoS)

La **protection anti-DoS** vous aide à détecter les attaques de type « déni de service » (DoS) et à en atténuer les effets. Les attaques sont généralement de deux types : les attaques de type inondation et les attaques qui exploitent des failles de sécurité. Les attaques par inondation visent à saturer votre système, tandis que les attaques de vulnérabilité tentent de paralyser le système en exploitant les failles du protocole ou du système d'exploitation.

La fonction de protection **anti-DoS** permet au routeur Vigor de confronter chaque paquet entrant avec la base de données de signatures d'attaque. Tout paquet susceptible de se dupliquer pour paralyser la machine hôte au sein du LAN sécurisé est bloqué et un message SysLog est envoyé, si toutefois vous avez configuré le serveur SysLog.

Le routeur Vigor surveille également le trafic. Tout trafic anormal violant un paramètre préétabli, comme le nombre de seuils, est identifié comme une attaque et le routeur Vigor active son mécanisme de protection en temps réel.

La fonction de protection anti-DoS/DDoS peut détecter et contrer les attaques suivantes :

1. attaque par inondation SYN
2. attaque par inondation UDP
3. attaque par inondation ICMP
4. scrutation de flag TCP
5. « trace route »
6. options IP
7. protocole inconnu
8. attaque « land »
9. attaque « smurf » (attaque par surcharge)
10. fragments SYN
11. fragments ICMP
12. attaque « tear drop »
13. attaque « fraggle »
14. attaque « ping of death »
15. scrutation de port TCP/UDP

Filtrage de contenu

Pour fournir aux utilisateurs un cyberespace approprié, le routeur Vigor est doté d'un outil de **filtrage de contenu d'URL** qui non seulement limite le trafic illégal en provenance ou à destination de certains sites web mais également interdit d'autres fonctionnalités web susceptibles de comporter du code malveillant.

Lorsqu'un utilisateur tape des mots-clés douteux ou clique sur une adresse universelle (URL) comportant des mots-clés douteux, la fonction de blocage par mots-clés refuse la demande HTTP d'accès à la page web concernée et peut donc limiter l'accès de l'utilisateur au site. Le **filtrage de contenu d'URL** peut être assimilé au comportement du commerçant qui refuse de vendre des magazines pour adultes à des adolescents. Au bureau, le **filtrage de contenu d'URL** peut également être utilisé pour augmenter le rendement des employés en les empêchant d'accéder à des ressources internet qui n'ont pas de rapport avec leur travail. Comment le filtrage de contenu d'URL peut-il être plus efficace qu'un pare-feu traditionnel ? Parce qu'il vérifie les chaînes d'URL ou certaines données HTTP cachées dans la charge utile des paquets TCP, tandis que le pare-feu traditionnel se contente d'analyser les champs des en-têtes TCP/IP.

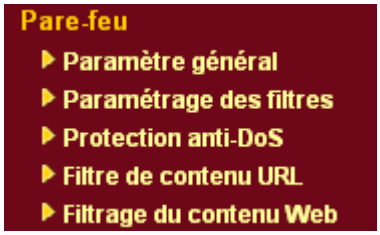
D'autre part, le routeur Vigor peut empêcher un utilisateur de télécharger accidentellement du code malveillant à partir de pages web. Il est très courant que du code malveillant se cache dans les objets exécutables, comme les contrôles ActiveX, les applets Java, les fichiers comprimés et autres fichiers exécutables. Le téléchargement de ces types de fichiers à partir de sites web peut faire courir des risques à votre système. Par exemple, un contrôle ActiveX est généralement utilisé pour fournir une fonction web interactive. Si du code malveillant s'y cache, il peut se retrouver dans le système de l'utilisateur.

Filtrage web

Nous savons tous que le contenu de l'internet, comme celui d'autres types de média, peut quelquefois être inconvenant. En tant que parent ou employeur responsable, vous devez protéger ceux dont vous avez la charge contre les dangers éventuels. Avec le service de filtrage web du routeur Vigor, vous pouvez protéger votre entreprise contre les menaces courantes, notamment contre les menaces pour la productivité, la responsabilité civile, le réseau et la sécurité. En tant que parent, vous pouvez empêcher vos enfants d'accéder à des sites pour adultes ou à des sites de messagerie en temps réel (« cybersalons » ou « chat rooms »).

Une fois que vous avez activé le service de filtrage web du routeur Vigor et choisi les catégories de sites que vous voulez rendre inaccessibles, chaque adresse URL demandée (par exemple, www.bbc.co.uk) sera vérifiée par rapport à notre base de données sous le contrôle de SurfControl. La base de données, qui couvre plus de 70 langues et 200 pays, contient plus de 1 milliards de pages web classées en 40 catégories explicites. Cette base de données est mise à jour quotidiennement par une équipe mondiale de chercheurs internet. Le serveur examine l'URL et informe votre routeur de la catégorie à laquelle elle appartient. Votre routeur Vigor décide alors d'autoriser ou non l'accès à ce site selon les catégories que vous avez sélectionnées. À noter que cette opération ne ralentit en rien votre navigation sur l'internet car chacun des multiples serveurs de base de données à équilibre de charge peut traiter des millions de requêtes.

Les options du menu Pare-feu sont les suivantes.



3.5.2 Configuration générale

La page Configuration générale vous permet de paramétrer les filtres IP et les options communes. Vous pouvez activer ou désactiver le **filtre d'appel** ou le **filtre de données**. Dans certaines circonstances, vous pouvez enchaîner les filtres. Ici, vous activez uniquement le **filtre de début**. Vous pouvez également configurer la **journalisation**, **activer le filtrage adaptatif**, **supprimer les connexions non http sur le port TCP 80** et **accepter les paquets UDP fragmentés entrants**.

Cliquez sur **Pare-feu,** puis sur **Configuration générale** pour ouvrir la page de configuration générale.

Filtre d'appel — Cochez **Activer** pour activer la fonction Filtre d'appel et spécifiez un filtre de début.

Filtre de données — Cochez **Activer** pour activer la fonction Filtre de données et spécifiez un filtre de début.

Journalisation — Vous pouvez définir ici les conditions de journalisation.
Néant - La fonction de journalisation n'est pas activée.
Bloquer - Les paquets bloqués seront journalisés.
Laisser passer - Les paquets passés seront journalisés.
Pas de correspondance - La fonction de journalisation enregistrera tous les paquets qui ne correspondent pas aux règles de filtrage.
À noter que, si vous tapez la commande ***log –f,*** le « log » de filtrage s'affichera sur le terminal Telnet.

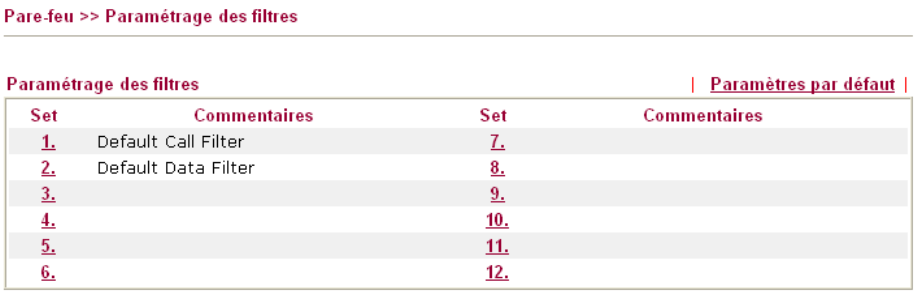
Laisser passer ou bloquer — Sélectionnez **Laisser passer** ou **Bloquer** pour les paquets qui ne correspondent pas aux règles de filtrage.

Gestion de contenu Sélectionnez un profil CSM pour le blocage des applications IM/P2P. Tous les autres du LAN doivent respecter le profil CSM sélectionné ici. Pour plus de détails, reportez-vous à la section concernant le paramétrage du profil CSM.

Certains jeux en ligne (par exemple, Half Life) utilisent un grand nombre de paquets UDP fragmentés pour le transfert des données de jeu. Instinctivement, en tant que pare-feu sécurisé, le routeur Vigor rejette ces paquets fragmentés pour éviter les attaques, sauf si vous cochez la case **« Accepter les paquets UDP fragmentés entrants ».** En cochant cette case, vous pouvez participer à ce type de jeu en ligne. Si la sécurité est votre souci principal, ne cochez pas la case **« Accepter les paquets UDP fragmentés entrants »**.

3.5.3 Paramétrage des filtres

Cliquez sur **Pare-feu,** puis sur **Paramétrage des filtres** pour ouvrir la page de paramétrage des filtres.



Pour modifier ou ajouter un filtre, cliquer sur numéro de filtre. La page ci-dessous apparaît. Chaque filtre comporte jusqu'à 7 règles. Cliquez sur le numéro de règle pour la modifier. Cliquez sur **Active** pour activer la règle.

Règle de filtrage Cliquez sur l'un des boutons **1 à 7** pour éditer/modifier la règle de filtrage. Cela a pour effet d'ouvrir la page web Modifier la règle de filtrage. Pour plus de détails, voir la page suivante.

Actif Active ou désactive la règle de filtrage.

Commentaires Tapez des commentaires ou une description du filtre (longueur maximale : 23 caractères).

Déplacer vers le haut/vers le bas Utilisez le lien **Haut** ou **Bas** pour changer l'ordre des règles de filtrage.

Filtre suivant Spécifie le filtre qui doit suivre le filtre actuel. Les filtres ne peuvent pas être appliqués en boucle.

Pour éditer les **règles de filtrage**, cliquez sur le numéro de **règle de filtrage** pour afficher la page de configuration des règles de filtrage.

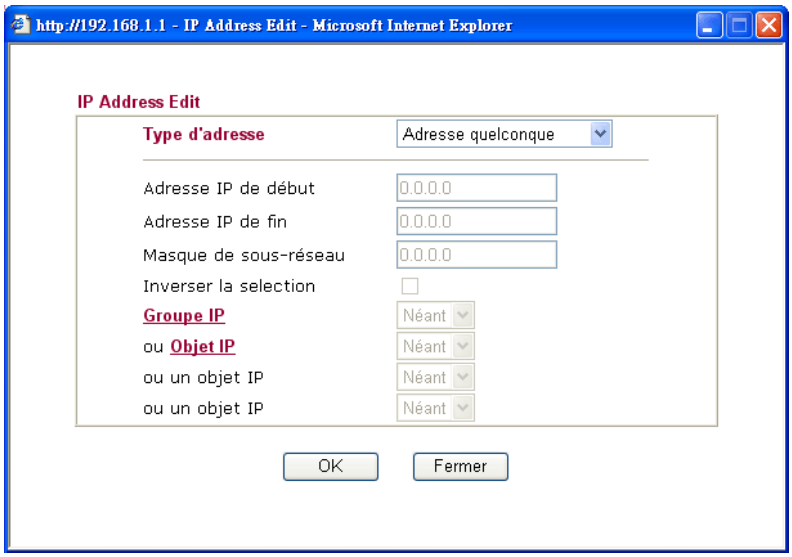
Cocher pour activer la règle de filtrage Cocher cette case pour activer la règle de filtrage

Commentaires Tapez des commentaires ou une description de la règle de filtrage (longueur maximale : 14 caractères).

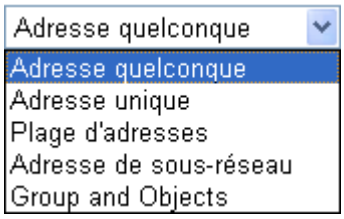
Index(1-15) Vous pouvez choisir jusqu'à 4 plages horaires parmi les 15 définies dans **Applications >> Plages horaires**. Par défaut, ce champ est vide et la fonction est active en permanence.

Sens Définit la direction des paquets. Concerne uniquement **le filtre de données**. Pour le filtre d'appel, ce paramètre n'est pas disponible puisque le filtre d'appel est appliqué au trafic sortant.

IP source/IP destination Cliquez sur **Modifier** pour accéder à la boîte de dialogue suivante et choisir les adresses IP ou les plages d'adresses IP de source/destination.



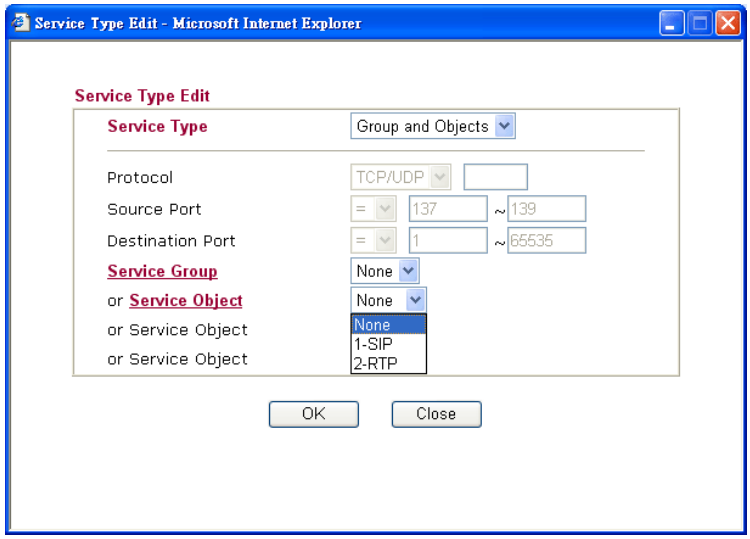
Pour définir manuellement l'adresse IP, choisissez **N'importe quelle adresse/Adresse unique/Plage d'adresses/Adresse de sous-réseau** comme type d'adresse et tapez les adresses dans cette boîte de dialogue. Vous pouvez également utiliser une plage d'adresses IP définie pour un groupe ou un objet. Dans ce cas, choisissez **Groupe et Objets** comme type d'adresse.

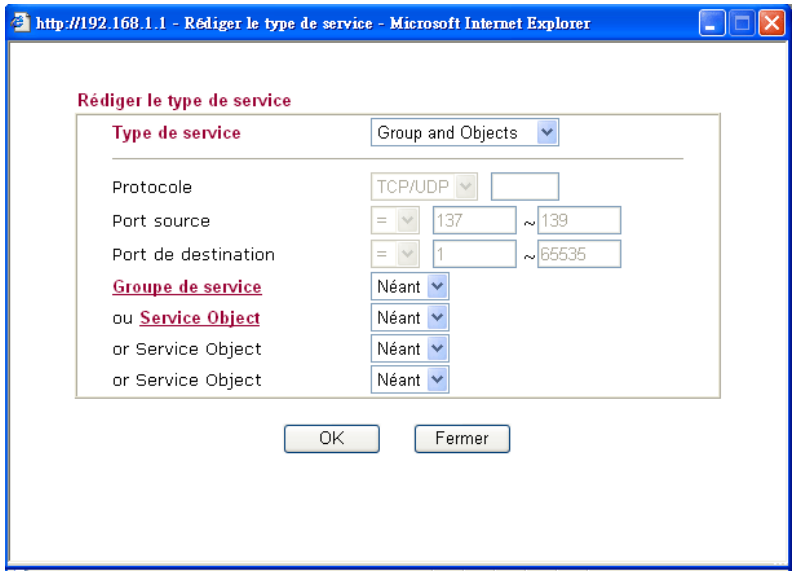


Dans la liste déroulante **Groupe IP**, choisissez le groupe que vous voulez appliquer. Ou bien choisissez un objet dans la liste dé roulante **Objet IP**.

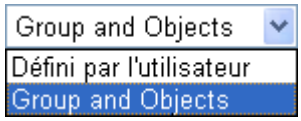
Type de service

Cliquez sur **Modifier** dans la boîte de dialogue suivante pour choisir un type de service approprié.





Pour définir manuellement le type de service, choisissez **Défini par l'utilisateur** comme type de service et complétez cette boîte de dialogue. Si vous voulez utiliser le type de service défini pour un groupe ou un objet, choisissez **Groupe et Objets** comme type de service.



Protocole – Spécifiez le ou les protocoles auxquels cette règle de filtrage s'appliquera.
Port de source/ Port de destination -
Ces deux paramètres sont là pour le protocole TCP/UDP. Ils peuvent être ignorés pour les autres protocoles.
(=) – Si les deux valeurs sont identiques, ce profil vaut pour un seul port ; si les deux valeurs sont différentes, ce profil vaut pour une plage de ports.
(!=) – Si les deux valeurs sont identiques, ce profil vaut pour tous les ports à l'exception du port défini ici ; si les deux valeurs sont différentes, ce profil vaut pour tous les ports à l'exception de la plage de ports définie ici.
(>) – Ce profil vaut pour tous les ports de numéro supérieur à cette valeur.
(<) – Ce profil vaut pour tous les ports de numéro inférieur à cette valeur.
Groupe/Objet service – Utilisez la liste déroulante pour choisir un groupe ou un objet.

Fragments

Spécifiez une action sur les paquets fragmentés. Concerne uniquement le **filtre de données**.
***Néant* -** Aucune action sur les paquets fragmentés.
***Non fragmenté* -** Applique la règle aux paquets non fragmentés.
***Fragmenté* -** Applique la règle aux paquets fragmentés.
***Trop court* -** Applique la règle uniquement aux paquets qui sont trop courts pour avoir un en-tête complet.

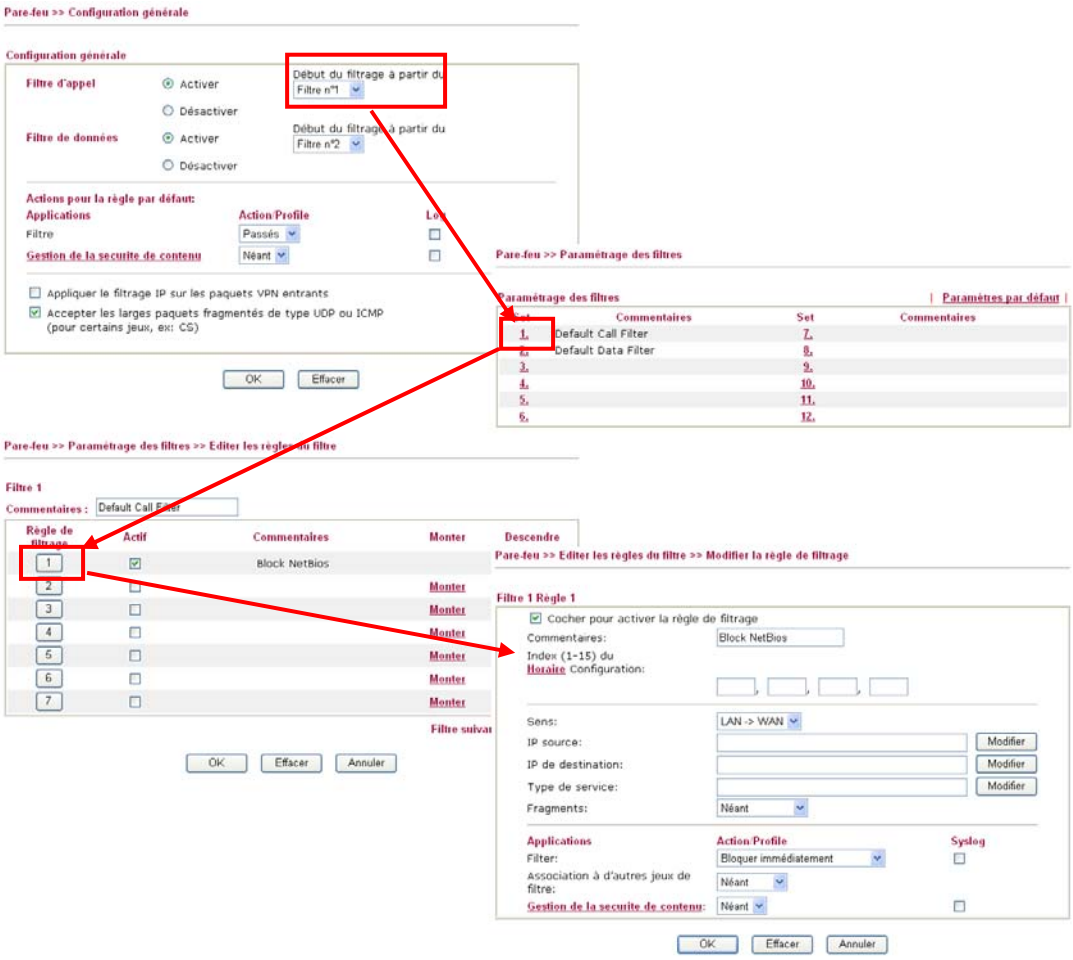
Laisser passer ou bloquer

Spécifiez l'action que doit avoir la règle sur les paquets.
Laisser passer immédiatement - Les paquets correspondants à la règle sont passés immédiatement.

	Bloquer immédiatement - Les paquets correspondants à la règle sont rejetés immédiatement. **Laisser passer si plus de corresp. -** Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est passé. **Bloquer si plus de corresp. -** Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est rejeté.
Appliquer un autre filtre	Si le paquet correspond à la règle de filtrage, la règle de filtrage suivante fait passer au filtre spécifié. Sélectionnez la règle de filtrage suivante dans le menu déroulant.
Journal	Cochez cette case pour activer la fonction de journalisation. Pour visualiser les journaux, utilisez la commande Telnet **log-f**.
Adresse IP	Spécifiez une adresse IP d'origine et une adresse IP de destination auxquelles s'applique cette règle de filtrage. Le symbole **!** devant une adresse IP particulière empêche l'application de la règle à cette adresse IP. Il est équivalent à l'opérateur logique NON. Pour appliquer la règle à toutes les adresses IP, tapez « n'importe laquelle » ou laissez le champ vide.
Gestion de contenu	Tous les hôtes de la plage configurée doivent respecter le profil CSM sélectionné ici. Pour plus de détails, reportez-vous à la section concernant le paramétrage du profil CSM.

Exemple

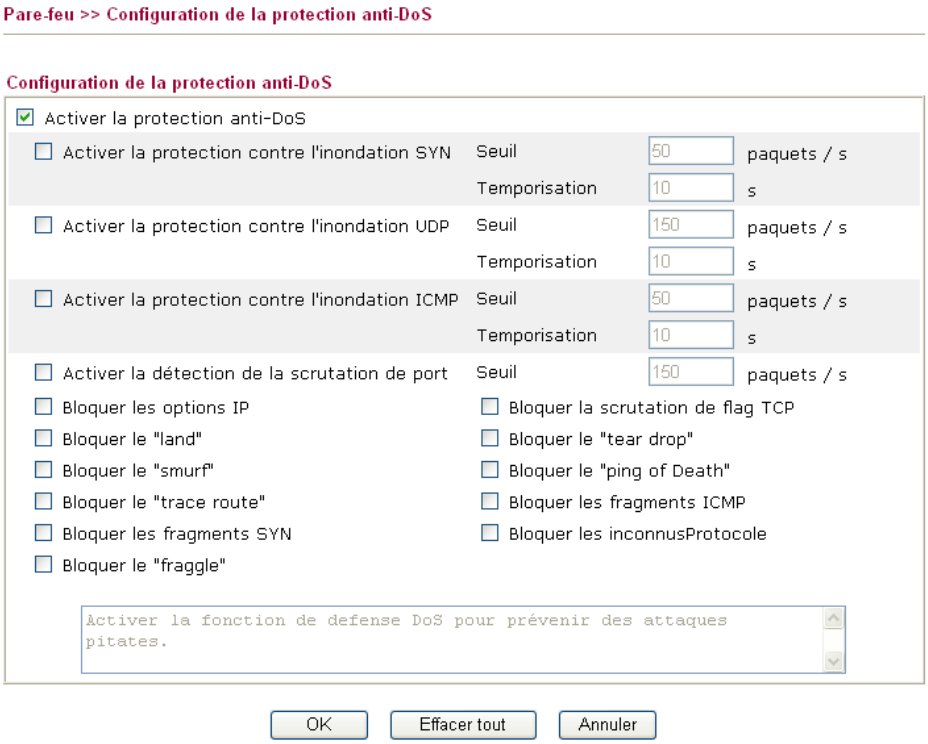
Comme indiqué plus haut, il existe deux types de filtres IP : le filtre d'appel et le filtre de données. Vous pouvez configurer 12 filtres d'appel ou de données dans **Paramétrage des filtres** et les enchaîner. Pour chaque filtre, vous pouvez définir 7 règles de filtrage. Puis, dans **Configuration générale**, vous pouvez spécifier un filtre d'appel de début et un filtre de données de début.



3.5.4 Protection anti-DoS

Il y a quinze sortes de protection au total. Par défaut, la fonctionnalité de **protection anti-DoS** est désactivée.

Cliquez sur **Pare-feu**, puis sur **Protection anti-DoS** pour ouvrir la page de configuration.



Activer la protection anti-DoS
Cliquez sur la case à cocher pour activer la protection anti-DoS.

Activer la protection contre l'inondation SYN
Cochez la case pour activer la protection contre l'inondation SYN. Si le nombre de paquets SYN TCP provenant de l'internet dépasse le seuil défini, le routeur Vigor rejette les paquets SYN TCP qui suivent pendant le temps défini par le paramètre Temporisation. Le but est d'empêcher la saturation du routeur Vigor par les paquets SYN TCP. Par défaut, le seuil et la temporisation ont respectivement pour valeur 50 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation UDP
Cochez la case pour activer la protection contre l'inondation UDP. Si le nombre de paquets UDP provenant de l'internet dépasse le seuil défini, le routeur Vigor rejette les paquets UDP qui suivent pendant le temps défini par le paramètre Temporisation. Le but est d'empêcher la saturation du routeur Vigor par les paquets UDP. Par défaut, le seuil et la temporisation ont respectivement pour valeur 150 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation ICMP
Cochez la case pour activer la fonction de protection contre l'inondation ICMP. Lorsque le nombre de paquets ICMP provenant de l'internet dépasse le seuil défini, le routeur rejette toutes les requêtes d'écho ICMP qui suivent pendant le temps défini par le paramètre Temporisation. Le seuil et la temporisation ont respectivement pour valeur par défaut 50 paquets par seconde et 10 secondes.

Activer la détection de
Une attaque par scrutation de port consiste à envoyer un grand

la scrutation de port	nombre de paquets à de nombreux ports pour tenter de déterminer à quels services un port répond. Pour activer la fonction de détection de scrutation de port, cochez la case. S'il détecte une telle tentative (dépassement du seuil), le routeur Vigor émet un message d'avertissement. Le seuil par défaut est de 150 paquets par seconde.
Bloquer les options IP	Cochez la case pour activer la fonction de blocage des options IP. Le routeur Vigor ignorera tous les paquets IP dans l'en-tête desquels figurent des options IP. Les options IP constituent une vulnérabilité du LAN car elles véhiculent des informations importantes, telles que des paramètres de sécurité, de compartimentage, TCC (groupe fermé d'utilisateurs), une série d'adresses internet, des messages de routage, etc. Un attaquant potentiel peut obtenir des renseignements sur vos réseaux privés.
Bloquer le « land »	Cochez la case pour activer la protection contre les attaques de type « land ». L'attaque de type « land » combine l'attaque SYN avec l'usurpation d'adresse IP. Une attaque de type « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que les numéros de port sont identiques à ceux de la victime.
Bloquer le « smurf »	Cochez la case pour activer la fonction de blocage de « smurf ». Le routeur Vigor rejettera toute requête d'écho ICMP.
Bloquer le « trace route »	Cochez la case pour que le routeur Vigor ne laisse pas passer les paquets « trace route ».
Bloquer les fragments SYN	Cochez la case pour activer la fonction de blocage des fragments SYN. Le routeur Vigor rejettera tous les paquets dont l'indicateur SYN et le bit MF (more fragments) sont à 1.
Bloquer le « fraggle »	Cochez la case pour activer la fonction de blocage de « fraggle ». Tous les paquets UDP de diffusion provenant de l'internet sont bloqués. Il se peut que la protection anti-DoS/DDoS bloque certains paquets licites. Par exemple, lorsque vous activez la protection contre le « fraggle », tous les paquets UDP de diffusion provenant de l'internet sont bloqués. Par conséquent, il se peut que les paquets RIP soient bloqués.
Bloquer la scrutation de flag TCP	Cliquez sur la case à cocher pour activer la fonction de blocage de la scrutation de flag TCP. Tout paquet TCP présentant une anomalie au niveau des indicateurs (« flags » est rejeté. Les anomalies sont, entre autres : absence d'indicateurs, *FIN sans ACK*, *SYN FIN ensemble, Xmas (indicateurs FIN URG et PSH à 1)* et *full Xmas (tous les indicateurs à 1).*
Bloquer le « tear drop »	Cliquez sur la case à cocher pour activer la fonction de blocage de « tear drop ». De nombreuses machines peuvent se bloquer à la réception de datagrammes (paquets) ICMP qui dépassent la longueur maximale. Pour éviter ce type d'attaque, le routeur Vigor est capable de rejeter les paquets ICMP fragmentés dont la longueur dépasse 1024 octets.
Bloquer le « ping of death »	Cliquez sur la case à cocher pour activer la fonction de blocage du « ping of death ». Dans ce type d'attaque, l'attaquant envoie des paquets qui se chevauchent aux machines hôtes cibles, lesquelles se bloquent lorsqu'elles reconstituent les paquets. Les paquets de ce

type sont bloqués par le routeur Vigor.

Bloquer les fragments ICMP

Cliquez sur la case à cocher pour activer la fonction de blocage des fragments ICMP. Les paquets ICMP dont le bit MF (« more fragments ») est à 1 sont rejeté.

Bloquer le « land »

Cochez la case pour activer la protection contre les attaques de type « land ». L'attaque de type « land » combine l'attaque SYN avec l'usurpation d'adresse IP. Une attaque de type « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que les numéros de port sont identiques à ceux de la victime.

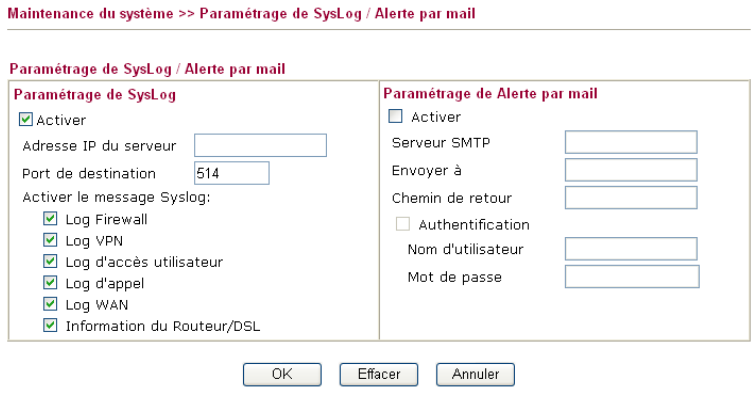
Bloquer les protocoles inconnus

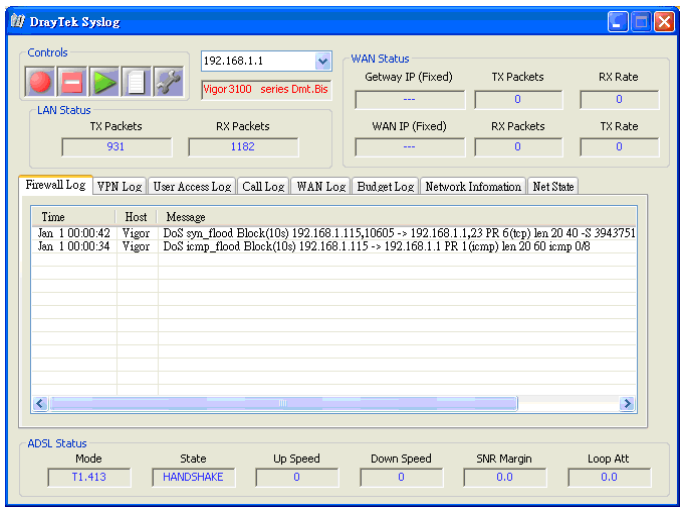
Cochez la case pour activer la fonction de blocage des protocoles inconnus. Dans l'en-tête de chaque paquet IP, il y a un champ qui indique le type de protocole de couche supérieure. Toutefois, les types de protocole supérieurs à 100 sont réservés et non définis pour l'instant. Par conséquent, le routeur doit pouvoir détecter et rejeter ce genre de paquet.

Messages d'avertissement

La fonction SysLog permet à l'utilisateur de visualiser les messages du routeur Vigor. L'utilisateur, en tant que serveur SysLog, reçoit les rapports émis par le routeur Vigor qui est un client SysLog.

Tous les messages d'avertissement liés à la **protection anti-DoS** sont envoyés à l'utilisateur qui peut les visualiser à l'aide du démon SysLog. Ces messages ont comme préfixe le mot-clé « DoS », suivi d'un nom qui indique le type d'attaque détecté.





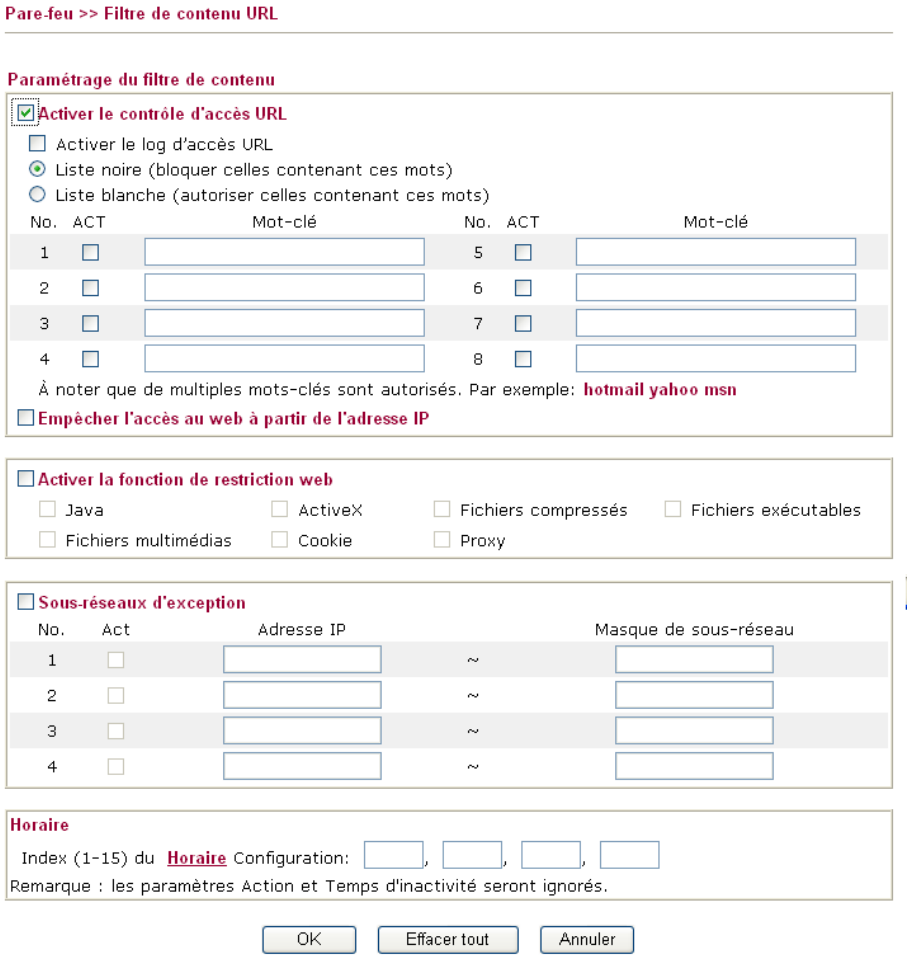
3.5.5 Filtre de contenu d'URL

La fonction de **filtrage de contenu d'URL** du routeur Vigor inspecte chaque chaîne d'URL de la requête HTTP entrante par rapport à la liste de mots-clés. Si tout ou partie de l'URL correspond à un mot-clé, le routeur Vigor la bloque.

Par exemple, si vous ajoutez le mot-clé « sexe », le routeur Vigor interdit l'accès à des sites ou pages web, tels que « www.sex.com », « www.backdoor.net/images/sex/p_386.html ». Vous pouvez simplement spécifier l'URL complète ou partielle, comme « www.sex.com » ou « sex.com ».

Par ailleurs, le routeur Vigor rejette toute requête qui tente de récupérer du code malveillant.

Cliquez sur **Pare-feu,** puis sur **Filtre de contenu d'URL** pour ouvrir la page de configuration.



Activer le contrôle d'accès URL — Cochez la case pour activer le contrôle d'accès URL.

Liste noire (bloquer ces mots-clés — Cliquez sur ce bouton pour interdire l'accès à une page web contenant les mots-clés spécifiés.

Liste blanche (autoriser ces mots-clés) — Cliquez sur ce bouton pour autoriser l'accès à une page web contenant les mots-clés spécifiés.

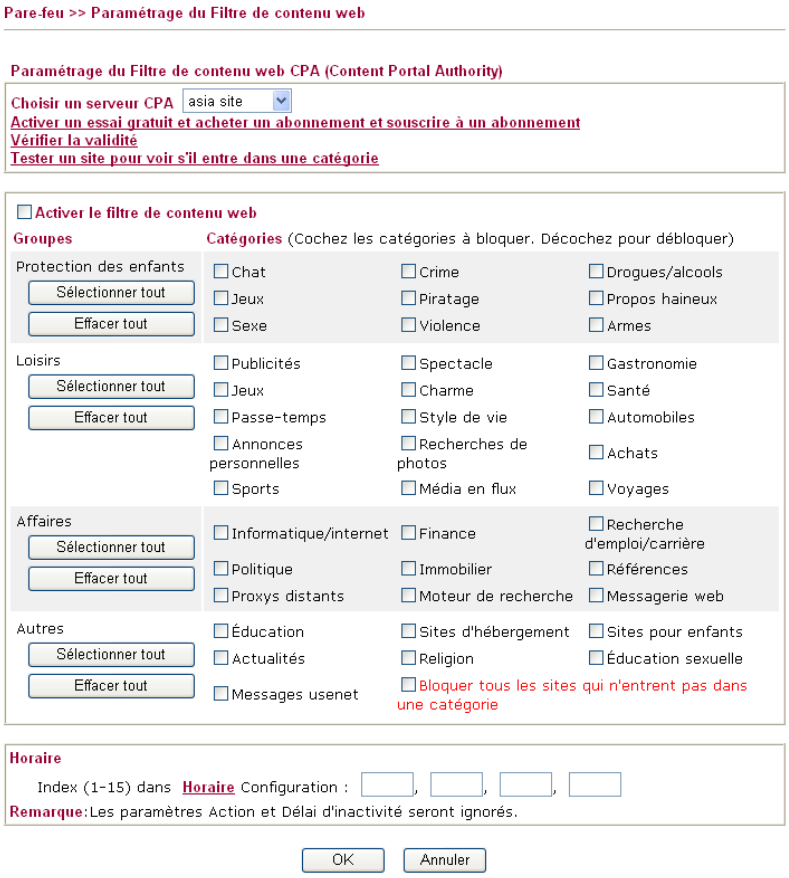
Mot-clé — Le routeur Vigor permet de définir des mots-clés dans 8 trames, chacune pouvant en contenir plusieurs. Le mot-clé peut être un nom, une partie de nom ou une URL complète. Dans une trame, les mots-clés sont séparés par un espace, une virgule ou un

	point-virgule. De plus, la longueur maximale de chaque trame est de 32 caractères. Une fois les mots-clés spécifiés, le routeur Vigor interdit l'accès à tout site dont tout ou partie de l'URL correspond à un mot-clé défini par l'utilisateur. À noter que plus la liste des mots-clés de blocage est simple, plus le routeur Vigor sera efficace.
Empêcher l'accès au web à partir de l'adresse IP	Cochez cette case pour interdire l'accès au web à l'aide d'une adresse IP, comme http://202.6.3.2. Il s'agit d'empêcher que quelqu'un esquive le contrôle d'accès URL. Vous devez effacer le cache de votre navigateur pour que le filtrage de contenu d'URL fonctionne correctement sur une page web que vous avez déjà visitée.
Activer la fonction de restriction web	Cochez la case pour activer la fonction. ***Java*** - Cochez la case pour activer la fonction de blocage d'objet Java. Le routeur Vigor rejettera les objets Java provenant de l'internet. ***ActiveX*** - Cliquez sur la case à cocher pour activer la fonction de blocage des objets ActiveX. Tout objet ActiveX provenant de l'internet sera refusé. ***Fichiers compressés*** - Cochez la case pour activer la fonction de blocage des fichiers compressés et donc empêcher le téléchargement de fichiers compressés. Le routeur Vigor peut bloquer les types de fichiers compressés suivants. **zip, rar, .arj, .ace, .cab, .sit** ***Fichiers exécutables*** - Cochez la case pour empêcher le téléchargement de fichiers exécutables à partir de l'internet. **.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg** ***Cookie*** - Cochez la case pour bloquer la transmission d'informations vers l'extérieur via les cookies afin de protéger votre vie privée. ***Proxy*** - Cochez la case pour rejeter toute transmission via un proxy. Pour maîtriser l'utilisation de la bande passante, il peut être très intéressant de bloquer le téléchargement de fichiers multimédias à partir de pages web. Les fichiers ayant les extensions suivantes seront bloqués par le routeur Vigor. **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**
Sous-réseau d'exception	Vous pouvez spécifier jusqu'à 4 adresses IP ou sous-réseaux pour les exempter du *contrôle d'accès URL*. Pour activer une entrée, cochez la case « **ACT** » correspondante.
Horaire	Spécifiez l'horaire de mise en œuvre de la fonction de filtrage de contenu d'URL.

3.5.6 Filtre de contenu web

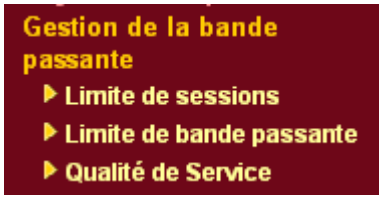
Cliquez sur **Pare-feu,** puis sur **Filtre de contenu web** pour ouvrir la page de configuration.

Reportez-vous au guide d'utilisation du **filtre de contenu web** pour plus de détails.



3.6 Gestion de la bande passante

Les options du menu Gestion de la bande passante sont les suivantes.



3.6.1 Limitation des sessions

Un PC doté d'une adresse IP privée peut accéder à l'internet via un routeur NAT. Celui-ci enregistre les sessions NAT d'une telle connexion. Les applications de partage de fichiers entre homologues (P2P), comme BitTorrent, nécessitent toujours un grand nombre de sessions et monopolisent des ressources, ce qui peut avoir un impact important sur la rapidité d'accès. Pour résoudre le problème, vous pouvez limiter le nombre de sessions pour certains hôtes.

Cliquez sur l'option **Limitation des sessions** du menu **Gestion de la bande passante** afin d'ouvrir la page web suivante.

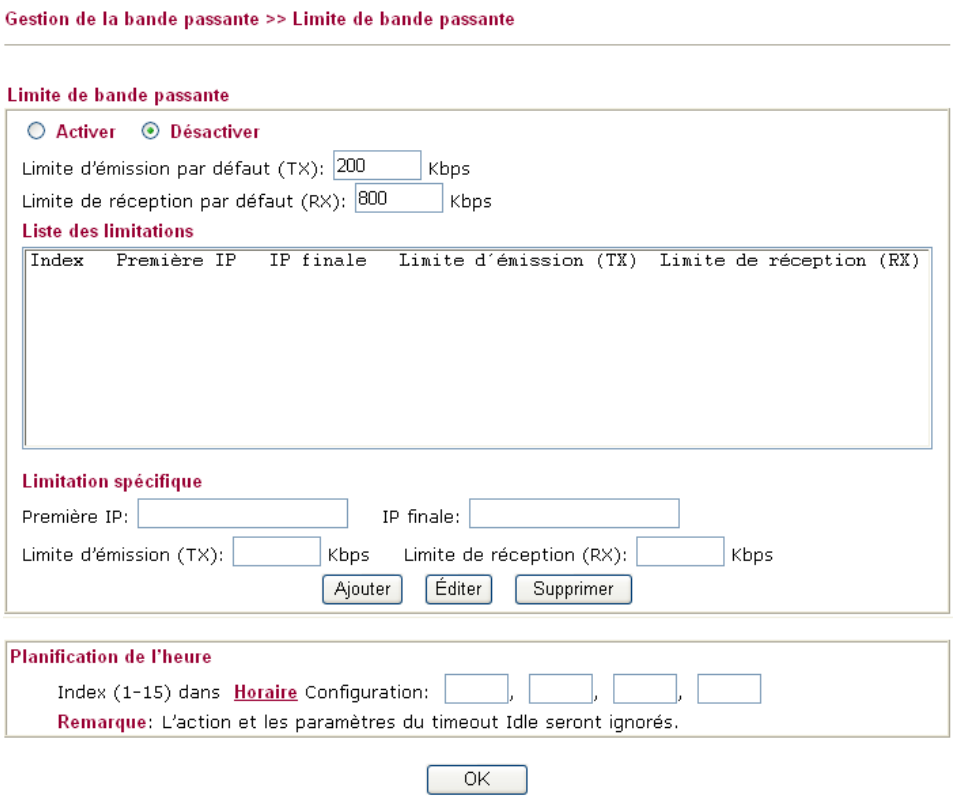
Pour activer la fonction de limitation des sessions, cliquez sur **Activer** et spécifiez la limite par défaut.

Activer	Cliquez sur ce bouton pour activer la fonction de limitation des sessions.
Désactiver	Cliquez sur ce bouton pour désactiver la fonction de limitation des sessions.
Limite par défaut	Définit le nombre de sessions par défaut pour chaque ordinateur du LAN.
Liste des limitations	Affiche une liste des limitations que vous définissez ici.
IP début	Définit l'adresse IP de début.
IP fin	Définit l'adresse IP de fin.
Nombre de sessions	Définit le nombre de sessions pour une plage spécifique d'adresses IP. Si vous ne spécifiez pas de nombre de sessions dans ce champ, le système utilisera la limite par défaut.
Ajouter	Ajoute la limitation de sessions spécifique à la liste ci-dessus.
Modifier	Vous permet de modifier les paramètres de la limitation sélectionnée.
Supprimer	Supprime la limitation sélectionnée de la liste.
Index (1-15) dans Plages horaires	Vous pouvez spécifier quatre plages horaires. Les plages ont été définies précédemment dans **Application – Plages horaires**.

3.6.2 Limitation du débit

Les téléchargements amont ou aval des applications FTP, HTTP ou de certaines applications P2P occupent beaucoup de bande passante, ce qui a des conséquences sur les autres programmes. Utilisez la fonction de limitation du débit pour faire un usage plus efficace de la bande passante.

Cliquez sur l'option **Limitation du débit** du menu **Gestion de la bande passante** pour ouvrir la page web suivante.



Pour activer la fonction de limitation du débit, cliquez sur **Activer** et définissez les limites montante et descendante par défaut.

Activer	Cliquez sur ce bouton pour activer la fonction de limitation du débit.
Désactiver	Cliquez sur ce bouton pour désactiver la fonction de limitation du débit.
Limite émission par défaut	Définit le débit montant par défaut pour chaque ordinateur du LAN.
Limite réception par défaut	Définit le débit descendant par défaut pour chaque ordinateur du LAN.
Liste des limitations	Affiche une liste des limitations définies ici.
IP début	Définit l'adresse IP de début.
IP fin	Définit l'adresse IP de fin.
Limite émission	Définit la limite de débit montant. Si vous n'indiquez rien dans ce champ, le système utilisera la limite de débit par défaut.

Limite réception	Définit la limite de débit descendant. Si vous n’ indiquez rien dans ce champ, le système utilisera la limite de débit par défaut.
Ajouter	Ajoute la limitation de débit à la liste ci-dessus.
Modifier	Vous permet de modifier les paramètres de la limitation sélectionnée.
Supprimer	Supprime la limitation sélectionnée de la liste.
Index (1-15) dans Plages horaires	Vous pouvez spécifier quatre plages horaires. Les plages ont été définies précédemment dans **Application – Plages horaires**.

3.6.3 Qualité de Service (QoS)

La gestion de la qualité de service (QoS) pour garantir à toutes les applications les niveaux de service voulus et une bande passante suffisante pour que les objectifs de performance soient remplis constitue l'un des aspects importants des réseaux d'entreprise modernes.

L'une des raisons qui expliquent l'importance de la QoS est que de nombreuses applications TCP augmentent sans cesse leur vitesse de transmission et consomment toute la bande passante disponible. Si les autres applications ne sont pas protégées par la fonction QoS, elles perdent beaucoup en performances dans le réseau encombré. C'est particulièrement essentiel pour les applications qui tolèrent mal les pertes de paquets, les délais de transmission ou la gigue (variations de délai).

Une autre raison est l'encombrement aux intersections de réseau où les vitesses respectives des circuits interconnectés diffèrent et où les trafics s'agrègent. La file d'attente des paquets s'allonge et le trafic peut être ralenti. Si aucun ordre de priorité n'a été défini pour spécifier quels paquets doivent être supprimés d'une file d'attente saturée, ce sont les paquets des applications sensibles mentionnées plus haut qui risquent d'être rejetés. Cela peut affecter les performances de ces applications.

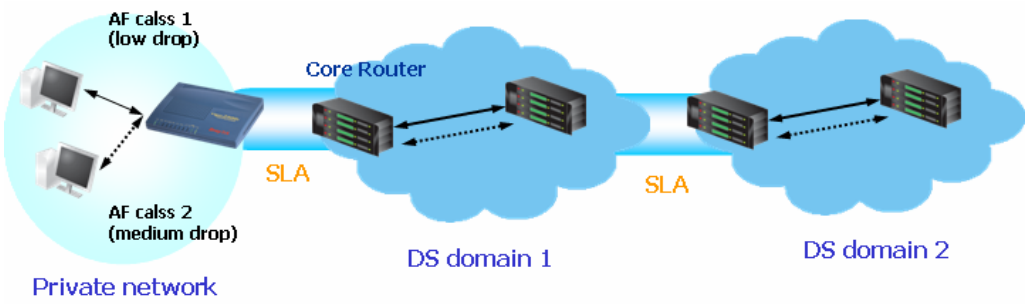
Il existe deux composantes dans la configuration primaire de la QoS :

- Classification : identification des applications à faible latence ou cruciales et marquage de ces applications pour la mise en œuvre d'un niveau de service prioritaire dans tout le réseau.
- Ordonnancement : sur la base de la classification des niveaux de service, affectation des paquets à des files d'attente et à des types de services associés.

Dans les routeurs Vigor, l'implémention de base de la QoS consiste à classer et à ordonnancer les paquets en fonction de l'information de type de service de l'en-tête IP. Par exemple, pour sa connexion avec le siège, un télétravailleur peut appliquer un index de contrôle de QoS pour réserver de la bande passante pour la connexion HTTPS tout en utilisant simultanément un grand nombre d'applications.

Une implémentation de réseau à QoS à plus grande échelle consiste à appliquer un code d’accès services différenciés (DSCP) et la priorité IP au niveau de la couche 3. Par comparaison avec la priorité IP antérieure qui utilise le champ « type de service » (ToS) de l'en-tête IP pour définir 8 classes de service, le DSCP crée 64 classes possibles rétrocompatibles. Dans un réseau à QoS, ou dans le cadre de services différenciés (DiffServ ou DS), un propriétaire de domaine DS signe un contrat de niveau de service (SLA) avec d'autres propriétaires de domaine DS pour définir le niveau de service fourni pour des trafics issus de domaines différents. Chaque nœud DS de ces domaines effectue un traitement différencié. C’est le comportement de commutation de proche en proche (PHB). La définition du PHB comprend la commutation diligentée (EF), l'acheminement assuré (AF) et l'acheminement au mieux (BE). L'acheminement assuré (AF) définit 4 classes d'acheminement avec chacune trois niveaux de priorité de rejet de paquets.

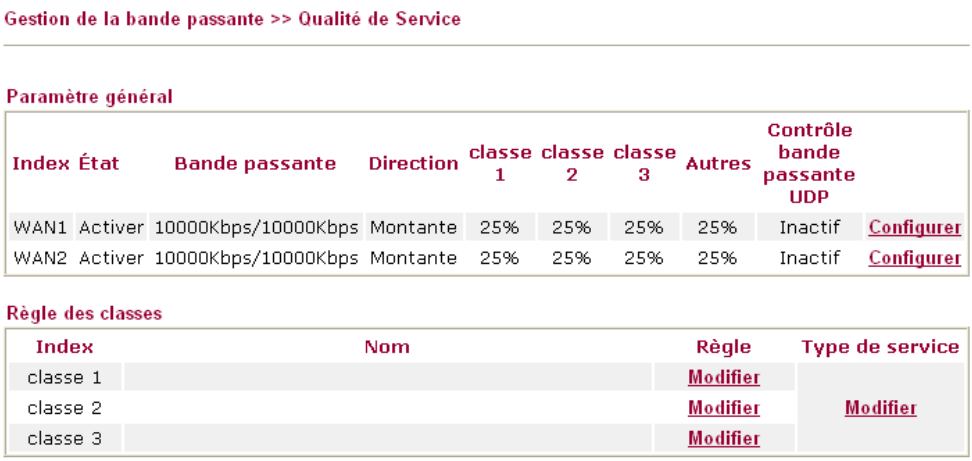
Les routeurs Vigor, en tant que routeurs périphériques de domaine DS, vérifient la valeur du champ DSCP de l'en-tête des paquets IP afin d'allouer une certaine quantité de ressources et d'exécuter les opérations de police, de classification ou d'ordonnancement appropriées. Les routeurs de cœur de réseau effectuent la même vérification avant d'exécuter les traitements afin d'assurer la cohérence du niveau de service dans tout le réseau à QoS.



AF class 1 (low drop)	*AF classe 1 (niveau de rejet bas)*
Core Router	*Routeur de cœur de réseau*
AF class 2 (medium drop)	*AF classe 2 (niveau de rejet moyen)*
DS domain 1	*Domaine DS 1*
DS domain 2	*Domaine DS 2*
Private network	*Réseau privé*

Toutefois, chaque nœud peut se comporter différemment vis-à-vis des paquets marqués comme prioritaires car il peut dépendre des modalités commerciales propres aux différents propriétaires de domaine DS. Il ne dépend pas que du routeur Vigor de garantir un trafic prioritaire à QoS homogène et déterministe dans l'ensemble du réseau.

Cliquez sur l'option **Qualité de service** du menu **Gestion de la bande passante** pour ouvrir la page web suivante.

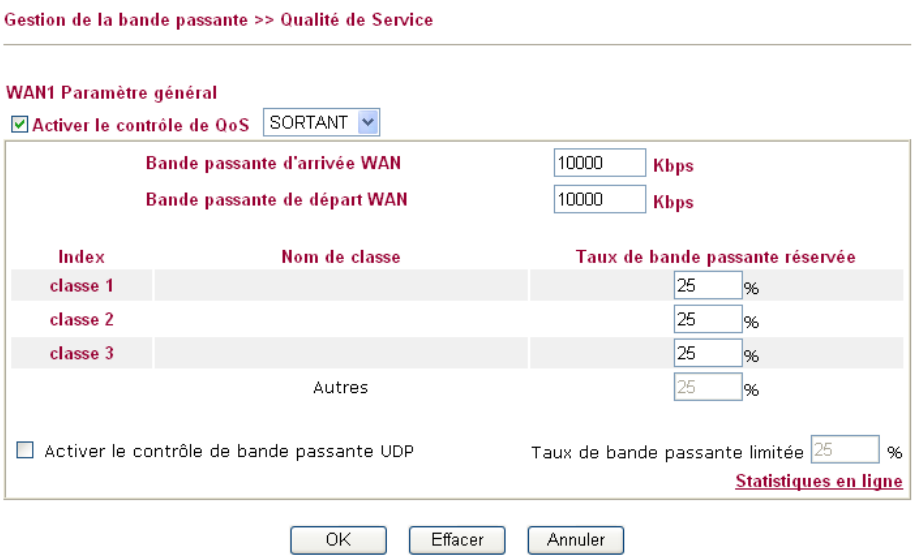


Cette page affiche les paramètres de qualité de service de l'interface WAN. Cliquez sur le lien **Configurer** pour accéder à la page de configuration générale de l'interface WAN (1/2). Pour ce qui est de la règle de classe, cliquez sur le lien **Modifier**.

Vous pouvez définir la configuration générale de l'interface WAN, modifier la règle de classe et modifier le type de service pour la règle de classe.

Configuration générale de l'interface WAN

Lorsque vous cliquez sur **Configurer**, vous pouvez définir le taux de bande passante pour le contrôle de QoS de l'interface WAN. Il y a quatre fils d'attente pour la gestion de la qualité de service. Les trois premières règles de classe (Classe 1 à Classe 3) peuvent être adaptées à vos besoins. Mais la dernière est réservée aux paquets qui ne relèvent pas des règles de classe définies par l'utilisateur.



Activer le contrôle de QoS Cette case est cochée par défaut.
Définissez le type de trafic auquel les paramètres de contrôle de QoS s'appliquent.
ENTRÉE - trafic entrant seulement.
SORTIE - trafic sortant seulement.
LES DEUX - trafic entrant et trafic sortant.
Cochez cette case et cliquez sur **OK**, puis cliquez de nouveau sur le lien **Configurer**. Le lien **Statistiques en ligne** apparaît.

Bande passante d'arrivée WAN Ce champ vous permet de spécifier le débit d'arrivée pour l'interface WAN. Par exemple, si votre connexion ADSL autorise 1 M dans le sens descendant et 256 K dans le sens montant, tapez 10000 kbit/s. La valeur par défaut est 10000 kbit/s.

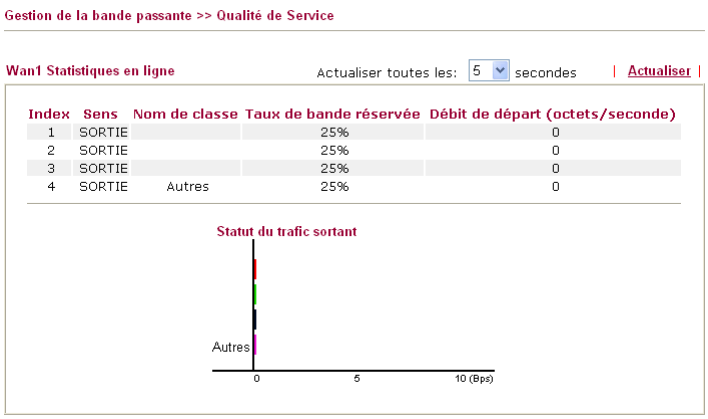
Bande passante de départ WAN Ce champ vous permet de spécifier le débit de départ de l'interface WAN. Par exemple, si votre connexion ADSL autorise 1 M dans le sens descendant et 256 K dans le sens montant, tapez 256 kbit/s. La valeur par défaut est 10000 kbit/s.

Taux de bande passante réservée Bande passante réservée à l'index de groupe sous la forme du rapport de **la bande passante réservée dans le sens montant à la bande passante réservée dans le sens descendant**.

Activer le contrôle de bande passante UDP Cochez cette case et entrez le taux de bande passante limitée dans le champ de droite. Cela constitue une protection du trafic d'application du TCP car le trafic d'application UDP, comme la vidéo en flux, consomme beaucoup de bande passante.

Taux de bande passante limitée La valeur tapée ici sert à limiter la bande passante totale de l'application UDP.

Statistiques en ligne Affiche des statistiques de qualité de service pour votre information.



Modification d'une règle de classe pour QoS

Les trois premières règles de classe (Classe 1 à Classe 3) sont adaptables à vos besoins. Pour cela, cliquez sur **Modifier**.

La page suivante apparaît alors. Vous pouvez taper un nom pour cette classe. Ici, la première règle de classe a pour nom « Test ».

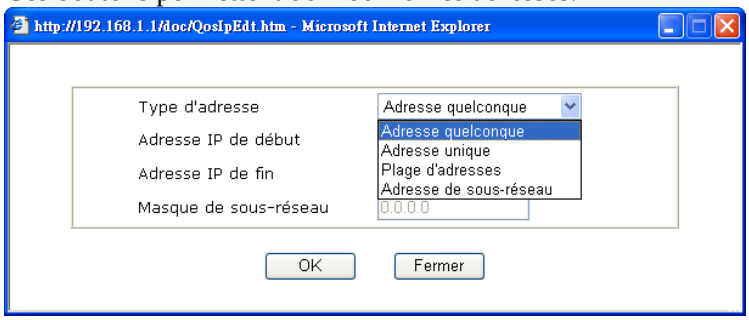
Pour ajouter une nouvelle règle, cliquez sur **Ajouter**. La page suivante apparaît.

ACT — Cochez cette case pour que les paramètres de cette page soient pris en compte.

Adresse de source — Cliquez sur le bouton **ModifSrc** pour spécifier l'adresse de source pour la règle.

Adresse de destination — Cliquez sur le bouton **ModifDest** pour spécifier l'adresse de destination pour la règle.

ModifSrc/Dest — Ces boutons permettent de modifier les adresses.



Type d'adresse – Détermine le type d'adresse de source.
Si le type d'adresse est **Adresse unique**, tapez l'adresse dans le champs adresse IP de début.
Si le type d'adresse est **Plage d'adresses**, tapez une adresse IP de début et une adresse IP de fin.
Si le type d'adresse est **Adresse de sous-réseau**, remplissez les champs Adresse IP de début et Masque de sous-réseau.

Code d'accès DiffServ — Tous les paquets de données sont divisés en différents niveaux et traités selon le type de niveau. Choisissez l'un des niveaux pour le traitement avec contrôle de QoS.

Type de service — Détermine le type de service pour le traitement avec contrôle de QoS. Il peut être modifié. Vous pouvez choisir un type de service préétabli dans la liste déroulante Type de service. Ces types sont préétablis en usine. Choisissez celui que vous voulez utiliser.

Vous pouvez paramétrer 20 règles pour une classe. Si vous voulez modifier une règle existante, sélectionnez le bouton d'option correspondant et cliquez sur **Modifier** pour ouvrir la page de modification de règle.

Gestion de la bande passante >> Qualité de Service

Index de classe N°1

Nom test

Non	État	Adresse locale	Adresse distante	DiffServ CodePoint	Type de service
1 ○	Active	tous	tous	IP precedence 2	SYSLOG(UDP:514)
2 ○	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)

Ajouter Modifier Supprimer

OK Annuler

Modification du type de service pour une règle de classe

Pour ajouter un nouveau type de service ou pour modifier ou supprimer un type de service existant, cliquez sur le lien Modifier qui se trouve sous le champ Type de service.

Gestion de la bande passante >> Qualité de Service

Paramètre général

Index	État	Bande passante	Direction	classe 1	classe 2	classe 3	Autres	Contrôle bande passante UDP	
WAN1	Activer	10000Kbps/10000Kbps	Montante	25%	25%	25%	25%	Inactif	Configurer
WAN2	Activer	10000Kbps/10000Kbps	Montante	25%	25%	25%	25%	Inactif	Configurer

Règle des classes

Index	Nom	Règle	Type de service
classe 1		Modifier	Modifier
classe 2		Modifier	
classe 3		Modifier	

Quand vous cliquez sur le lien **Modifier**, la page suivante apparaît.

Gestion de la bande passante >> Qualité de Service

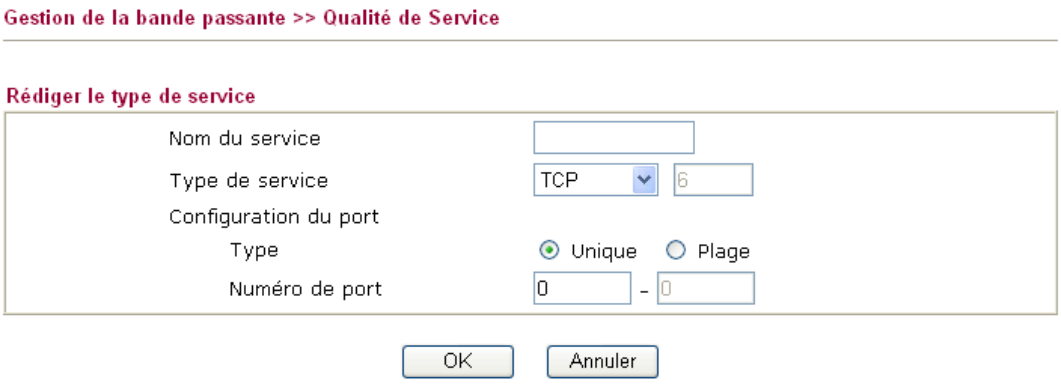
Type de service défini par l'utilisateur

Non	Nom	Protocole	Port
1	Vide	-	-

Ajouter Modifier Supprimer

Annuler

Pour ajouter une nouvelle règle, cliquez sur **Ajouter** pour ouvrir la page suivante. Si vous voulez modifier un type de service existant, sélectionnez le bouton d'option correspondant et cliquez sur **Modifier** pour ouvrir la page de modification.



Nom de service Tapez le nom du nouveau service.

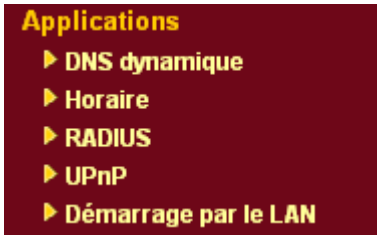
Type de service Choisissez le type de service (TCP, UDP ou TCP/UDP).

Configuration des ports Cliquez sur **Unique** ou **Plage**. Si vous choisissez Plage, spécifiez un numéro de port de début et un numéro de port de fin dans les champs **Numéro de port**.

Vous pouvez paramétrer jusqu'à 40 types de services. Si vous voulez Modifier/Supprimer un type de service existant, sélectionnez le bouton d'option correspondant et cliquez sur **Modifier**.

3.7 Applications

Les options du menu Applications sont les suivantes.



3.7.1 DNS dynamique

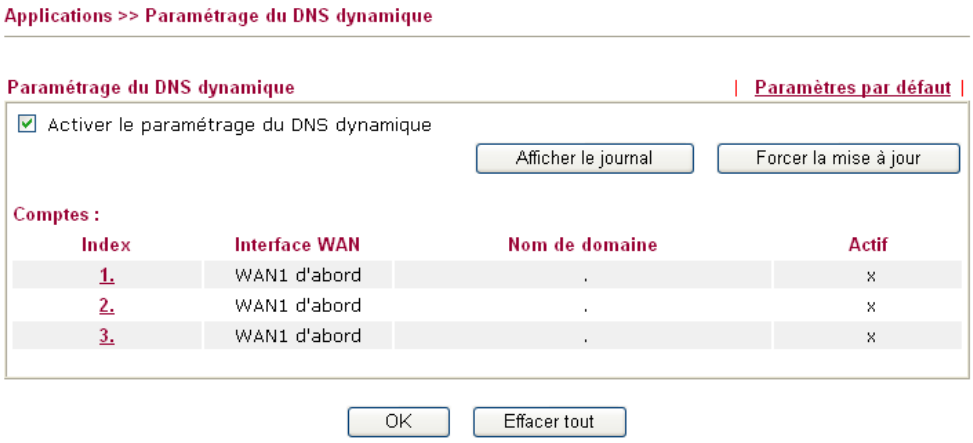
Le FAI vous fournit souvent une adresse IP dynamique au moment où vous vous connectez à l'internet. Cela veut dire que l'adresse IP publique de votre routeur change chaque fois où vous accédez à l'internet. La fonction DNS dynamique vous permet d'affecter un nom de domaine à une adresse IP WAN dynamique. Elle permet au routeur de mettre à jour son adresse IP WAN sur le serveur DNS dynamique spécifié. Une fois le routeur en ligne, vous pourrez utiliser le nom de domaine enregistré pour accéder au routeur ou à des serveurs virtuels internes à partir de l'internet. Cette fonction est particulièrement utile si vous hébergez un serveur web, un serveur ftp ou autre derrière le routeur.

Avant de pouvoir utiliser la fonction DNS dynamique, il faut demander un service DNS dynamique gratuit aux fournisseurs de service DNS dynamique. Le routeur Vigor permet d'ouvrir jusqu'à trois comptes auprès de trois fournisseurs de service DNS dynamique différents. Les routeurs Vigor sont donc compatibles avec les services DNS dynamiques fournis par la plupart des fournisseurs de service DNS dynamique, tels que **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** Visitez leur site pour enregistrer votre nom de domaine pour le routeur.

Activer la fonction et ajouter un compte DNS dynamique

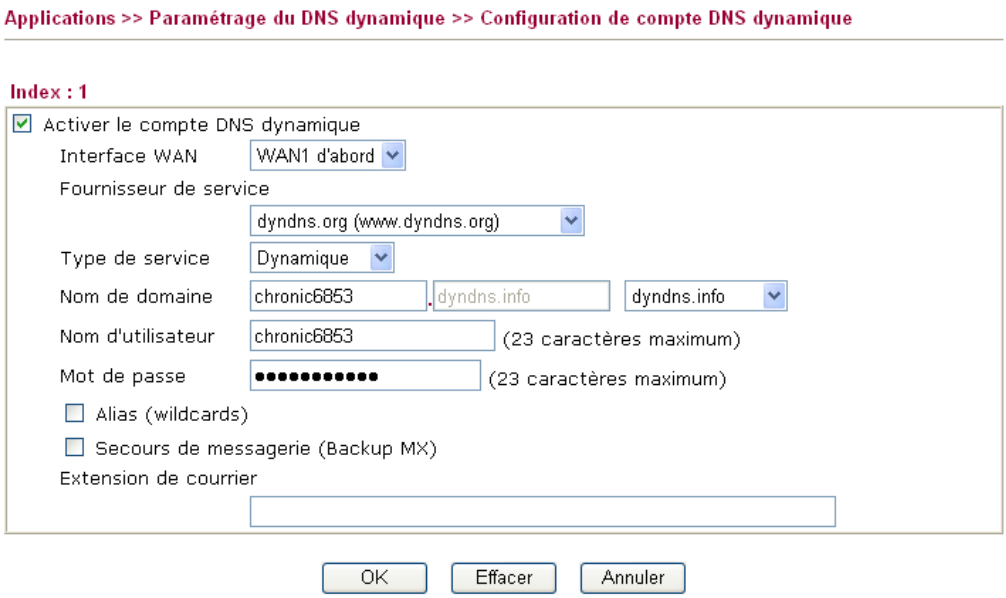
1. Supposons que vous ayez enregistré un nom de domaine auprès du fournisseur de service DDNS ***hostname.dyndns.org*** et ouvert un compte dont le nom d'utilisateur est ***test*** et dont le mot de passe est ***test***.

2. Dans le menu de paramétrage du DNS dynamique, cochez **Activer le paramétrage du DNS dynamique.**



Paramètres par défaut	Efface tous les profils et rétablit les paramètres par défaut.
Activer le paramétrage du DNS dynamique	Cochez cette case pour activer la fonction DNS dynamique.
Index	Cliquez un numéro sous Index pour accéder à la page de paramétrage d'un compte DNS dynamique.
Interface WAN	Affiche l'interface WAN actuelle utilisée pour accéder à l'internet.
Nom de domaine	Affiche le nom de domaine que vous avez entré dans la page de paramétrage du compte DNS dynamique.
Actif	Indique si ce compte est actif ou inactif.
Afficher le journal	Affiche le journal DNS dynamique.
Forcer la mise à jour	Oblige le routeur à se mettre à jour auprès du serveur DNS dynamique.

3. Sélectionnez l'index n°**1** pour ajouter un compte pour le routeur. Cochez **Activer le compte DNS dynamique** et sélectionnez le **fournisseur de service approprié** : **dyndns.org**. Tapez le nom de domaine enregistré : ***hostname*** et le suffixe du nom de domaine : **dyndns.org** dans le champ **Nom de domaine**. Dans les deux champs suivants, tapez votre **nom d'utilisateur** : ***test*** et votre **mot de passe** : ***test***.



Activer le paramétrage du DNS dynamique	Cochez cette case pour activer le compte actuel. Si cette case a été cochée, une coche apparaît dans la colonne Actif de la page web précédente (voir étape 2).
Interface WAN	Sélectionnez l'interface WAN à laquelle s'applique les paramètres.
Fournisseur de service	Sélectionnez le fournisseur de service DNS dynamique.
Type de service	Sélectionnez un type de service (Dynamique, Personnalisé, Statique). Si vous choisissez Personnalisé, vous pouvez modifier le domaine indiqué dans le champ Nom de domaine.
Nom de domaine	Tapez un nom de domaine choisi précédemment. Utilisez la liste déroulante pour choisir le domaine désiré.
Nom d'utilisateur	Tapez le nom d'utilisateur choisi pour le domaine.
Mot de passe	Tapez le mot de passe choisi pour le domaine.

4. Cliquez sur le bouton **OK** pour activer les paramètres. Vous pouvez voir que vos paramètres ont été enregistrés.

Les fonctions Alias et Secours de messagerie ne sont pas prises en charge pour tous les fournisseurs de service DNS dynamique. Visitez leur site pour plus de détails.

Désactiver la fonction et effacer tous les comptes DNS dynamique

Dans le menu de paramétrage du DDNS dynamique, décochez **Activer le paramétrage du DNS dynamique** et cliquez sur le bouton **Effacer tout** pour désactiver la fonction et effacer tous les comptes.

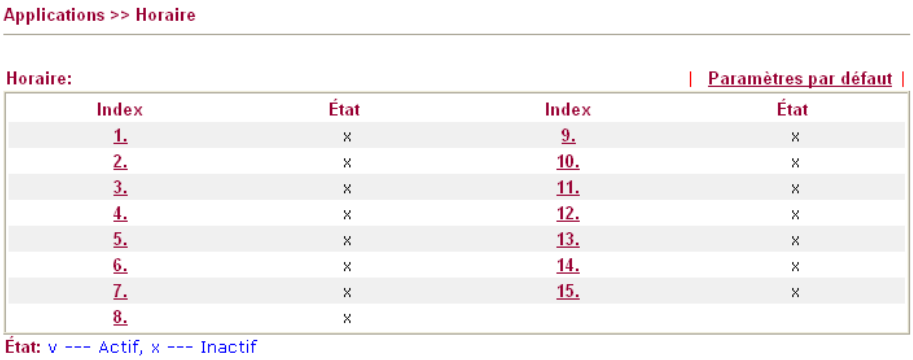
Supprimer un compte DNS dynamique

Dans le menu de paramétrage du DNS dynamique, cliquez sur le numéro d'**index** que vous voulez supprimer, puis cliquez sur le bouton **Effacer tout** pour supprimer le compte.

3.7.2 Plages horaires

Le routeur Vigor a une horloge temps réel intégrée qui peut être mise à jour manuellement ou automatiquement à partir d'un serveur de synchronisation internet (NTP). Vous pouvez donc faire en sorte que le routeur se connecte à l'internet à une certaine heure ou bien limiter l'accès à l'internet à certaines heures (par exemple, aux heures ouvrables). La fonction de gestion des plages horaires est également applicable à d'autres fonctions.

Vous devez vous synchroniser avant de paramétrer une plage horaire. Dans le menu **Maintenance du système>>Réglage de l'heure**, cliquez sur le bouton **Demander l'heure** pour régler l'horloge du routeur Vigor sur l'heure actuelle de votre PC. L'horloge se réinitialise si vous éteignez ou réinitialisez le routeur. Vous pouvez aussi utiliser un serveur NTP sur l'internet pour synchroniser l'horloge du routeur. Pour cela, il faut que la connexion WAN soit établie.



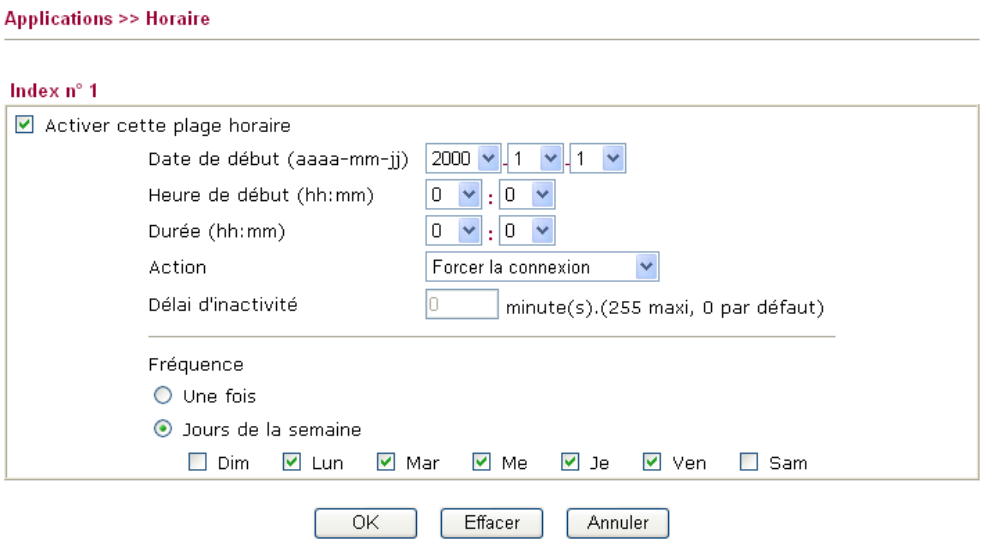
Paramètres par défaut Efface tous les profils et rétablit les paramètres par défaut.

Index Cliquez sur le numéro sous Index pour accéder à la page de paramétrage des plages horaires.

État Indique si cette plage horaires est active ou inactive.

Vous pouvez paramétrer jusqu'à 15 plages horaires. Vous pouvez ensuite les appliquer à vos paramètres d'**accès à l'internet** ou à vos paramètres d'interconnexion de LAN.

Pour ajouter une plage horaire, cliquez sur un numéro d'index, par exemple 1. Les paramètres de la plage horaire correspondante sont affichés.



Activer cette plage horaire Cochez la case pour activer la plage horaire.

Date de début (aaaa-mm-jj)	Spécifiez la date de début de la plage horaire.
Heure de début (hh:mm)	Spécifiez l'heure de début de la plage horaire.
Durée (hh:mm)	Spécifiez la durée de la plage horaire.
Action	Spécifiez quelle action doit être effectuée durant la plage horaire. **Forcer la connexion -** Connexion permanente durant la plage horaire. **Forcer la déconnexion -** Connexion interdite durant la plage horaire. **Activer à la demande -** Connexion établie à la demande avec un **Délai d'inactivité**. **Désactiver à la demande -** Connexion établie tant qu'il y a du trafic sur la ligne. Déconnexion à l'expiration du délai d'inactivité, d'autres connections étant impossible durant la plage horaire.
Délai d'inactivité	Spécifiez la durée propre à la plage horaire. **Fréquence -** Nombre de fois que la plage horaire sera appliquée **Une fois -** La plage horaire sera appliquée une seule fois **Jours de la semaine -** La plage horaire sera appliquée les jours spécifiés.

Exemple

Si vous voulez que la connexion internet PPPoE soit permanente (Force On) de 9 h 00 à 18 h 00 toute la semaine et qu'elle soit impossible (Force Down) en dehors de ces heures.

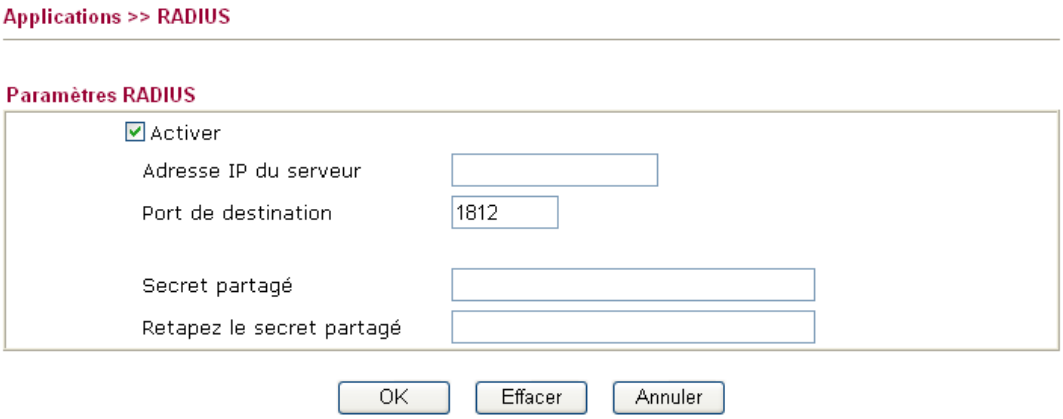
Heures de bureau :			
(Forcer la connexion)			
lun - dim	**9 h 00**	**à**	**18 h 00**

1. Vérifiez que la connexion PPPoE fonctionne correctement et que le routeur est à l'heure (voir **Réglage de l'heure**).
2. Configurez la connexion PPPoE en connexion permanente de 9 h 00 à 18 h 00 toute la semaine.
3. **Forcez la déconnexion** de 18 h 00 à 9 h 00 le jour suivant pendant toute la semaine.
4. Affectez ces deux profils au profil d'accès internet PPPoE. La connexion internet PPPoE respectera les conditions de **connexion ou de déconnexion** définies pour les plages horaires.

3.7.3 RADIUS

Le service d'usager commuté à authentification distante (RADIUS) est un protocole client-serveur d'authentification qui prend en charge l'authentification, l'autorisation et la comptabilité et qui est largement utilisé par les fournisseurs d'accès internet. C'est la méthode la plus courante d'authentification et d'autorisation des utilisateurs à accès commuté ou par tunnel.

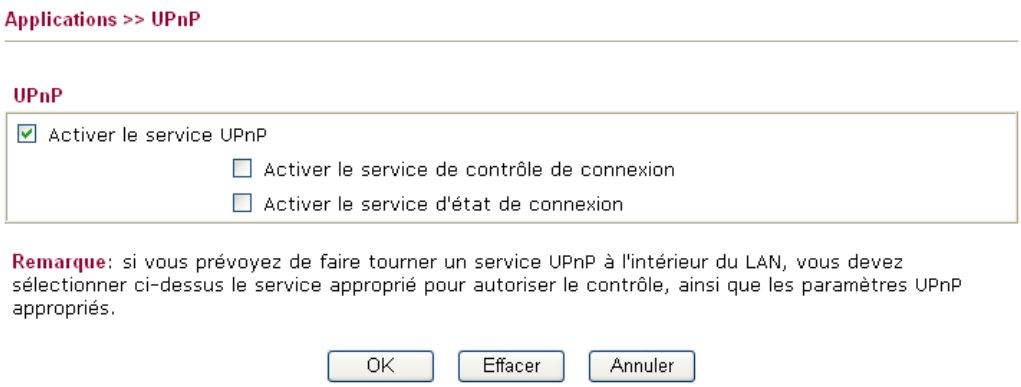
Le client RADIUS intégré permet au routeur d'aider l'utilisateur distant ou une station sans fil et le serveur RADIUS à effectuer une authentification mutuelle. Il permet l'authentification centralisée des accès à distance pour la gestion du réseau.



Activer	Cochez cette case pour activer la fonction client RADIUS
Adresse IP du serveur	Tapez l'adresse IP du serveur RADIUS
Port de destination	Numéro de port UDP utilisé par le serveur RADIUS. La valeur par défaut est 1812 (RFC 2138).
Secret partagé	Le serveur et le client RADIUS partagent un secret qui est utilisé pour authentifier les messages qu'ils s'échangent. Les deux côtés doit être configurés pour utiliser le même secret partagé.
Retaper le secret partagé	Retapez le secret partagé pour confirmer.

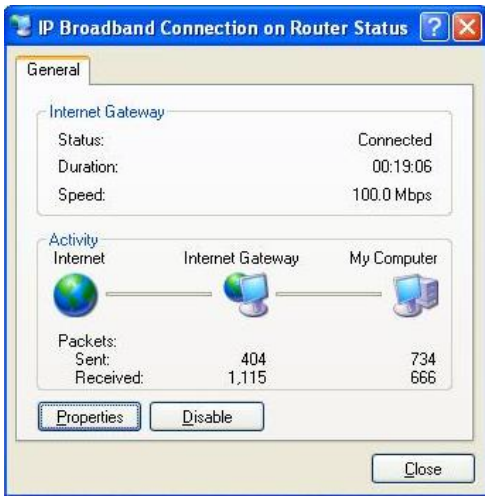
3.7.4 UPnP

Le protocole **UPnP** (Universal Plug and Play) apporte aux périphériques reliés au réseau la faciliter d'installation et de configuration dont bénéficient déjà les périphériques raccordés à un PC avec le système « Plug and Play » Windows existant. Dans le cas des routeurs NAT, la principale fonction du protocole UPnP est le « NAT Traversal ». Elle permet aux applications situées derrière le pare-feu d'ouvrir automatiquement les ports dont elles ont besoin pour passer. C'est plus sûr que de demander à un routeur de déterminer lui-même quels ports ouvrir. De plus, l'utilisateur n'a pas besoin de configurer manuellement des mappages de ports ou un DMZ. Le protocole UPnP est disponible sous Windows XP et le routeur assure la prise en charge de MSN Messenger pour permettre d'exploiter pleinement les fonctionnalités de téléphonie, de vidéo et de messagerie.

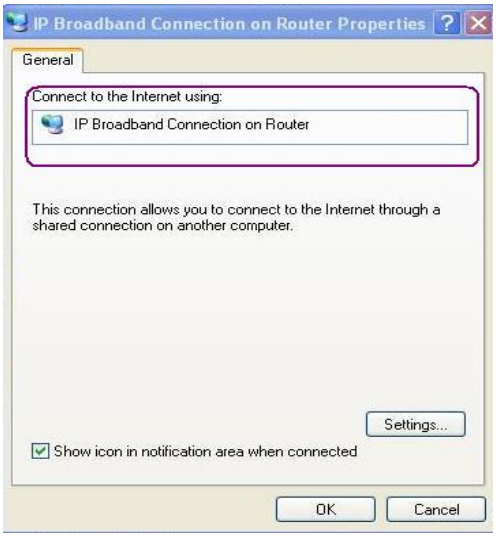


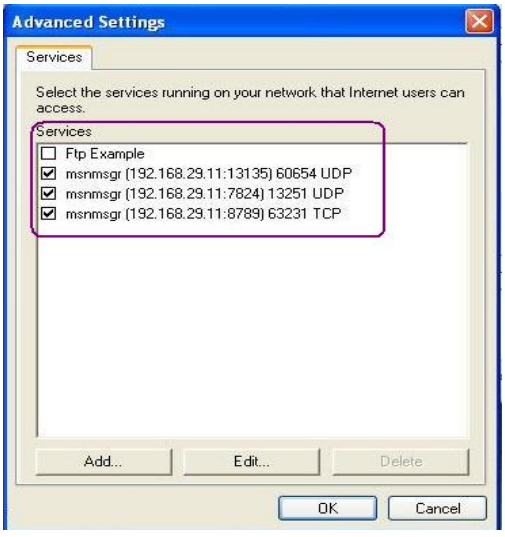
Activer le Service UPNP Vous pouvez activer soit le **Service de contrôle de connexion,** soit le **Service d'état de connexion**.

Après l'activation du **service UPNP**, une icône **IP Broadband Connection on Draytek Router** apparaît dans Windows XP/Favoris réseaux. Vous pourrez activer le service d'état et le service de contrôle de la connexion. La fonction NAT Traversal d'UPnP permet le fonctionnement des fonctionnalités multimédias de vos applications. Il faut paramétrer manuellement les ports ou utiliser d'autres méthodes semblables. Les écrans qui suivent montrent des exemples de cette fonctionnalité.



La fonctionnalité UPnP du routeur permet à des applications compatibles UPnP, comme MSN Messenger, de découvrir ce qu'il y a derrière un routeur NAT. L'application prendra également connaissance de l'adresse IP externe et configurera les mappages de ports sur le routeur. Cette fonctionnalité transmet ensuite les paquets des ports externes du routeur vers les ports internes utilisés par l'application.





Rappel concernant le pare feu et UPnP

Impossibilité d'utiliser la fonction UpnP avec le logiciel pare-feu
L'activation d'applications de pare-feu sur votre PC peut entraîner un mauvais fonctionnement de la fonction UPnP. Cela est dû au fait que ces applications bloquent l'accès à certains ports de réseau.

Considérations de sécurité
L'activation de la fonction UPnP sur votre réseau peut compromettre dans une certaine mesure la sécurité et peut vous faire courir certains risques. Vous devez peser soigneusement ces risques avant d'activer la fonction UpnP.

- Certains systèmes d'exploitation Microsoft ont identifié les points faibles du protocole UPnP. Assurez-vous que vous avez appliqué les packs de service et les correctifs les plus récents.

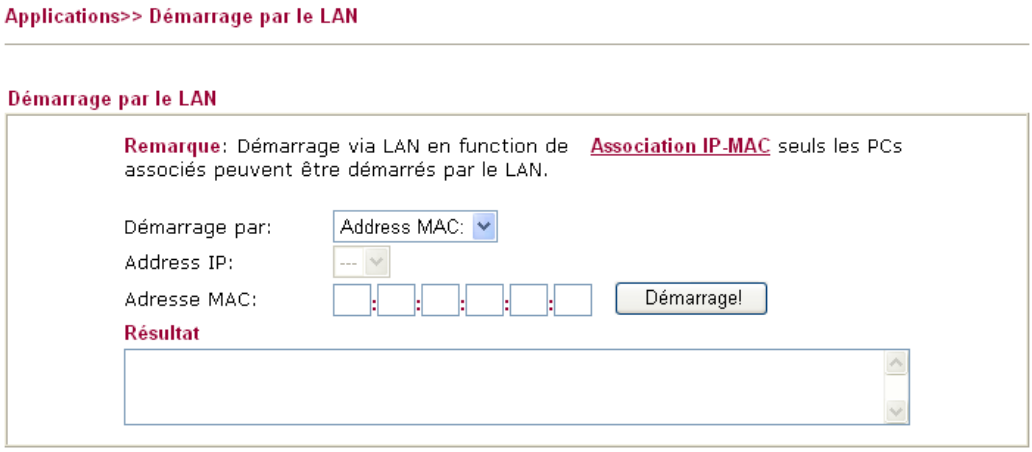
- Les utilisateurs non privilégiés peuvent contrôler certaines fonctions du routeur et notamment enlever et ajouter des mappages de ports.

La fonction UPnP ajoute dynamiquement des mappages de ports pour certaines applications compatibles UPnP. Lorsque les applications se terminent anormalement, ces mappages ne peuvent pas être supprimés.

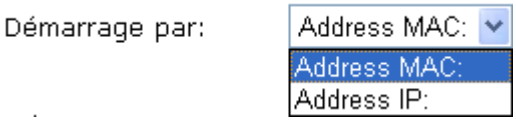
3.7.5 Réveil sur LAN (WOL)

Un PC client du LAN peut être réveillé par le routeur. Lorsqu'un utilisateur veut réveiller un PC particulier via le routeur, il doit taper l'adresse MAC correcte du PC sur la page **Réveil sur LAN**.

Ce PC doit être équipé d'une carte réseau prenant en charge la fonction WOL. Cette fonction doit être activée dans le BIOS.



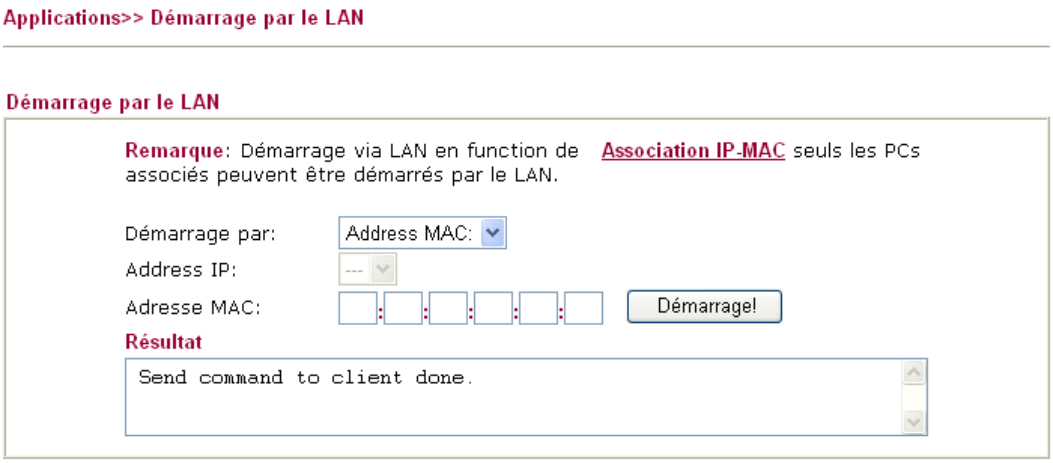
Réveil par — Vous pouvez réveiller le PC lié soit par son adresse MAC, soit par son adresse IP. Dans le premier cas il faut taper l'adresse MAC correct dans les zones Adresse MAC. Dans le deuxième cas, il faut choisir l'adresse IP correcte.



Adresse IP — Les adresses IP configurées dans **Pare-feu>>Lien IP-MAC** apparaissent dans cette liste déroulante. Choisir l'adresse IP du PC que vous voulez réveiller.

Adresse MAC — Tapez l'adresse MAC de l'un des PC liés.

Réveil Cliquez sur ce bouton pour réveiller le PC sélectionné. Voir la figure ci-dessous. Le résultat est affiché dans la zone de texte.

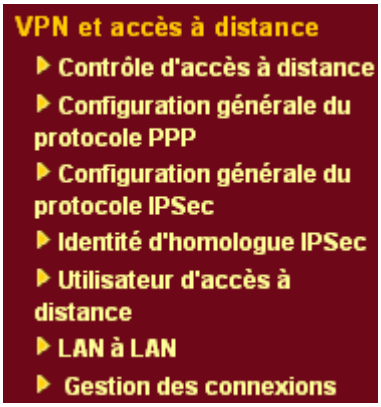


3.8 VPN et accès à distance

Un réseau privé virtuel (RPV ou VPN en anglais) est l'extension d'un réseau privé qui englobe des liaisons appartenant à des réseaux partagés ou publics, comme l'internet. En bref, la technologie de VPN permet l'échange de données entre deux ordinateurs via un réseau partagé ou public dans des conditions analogues à celles d'une liaison privée point à point.

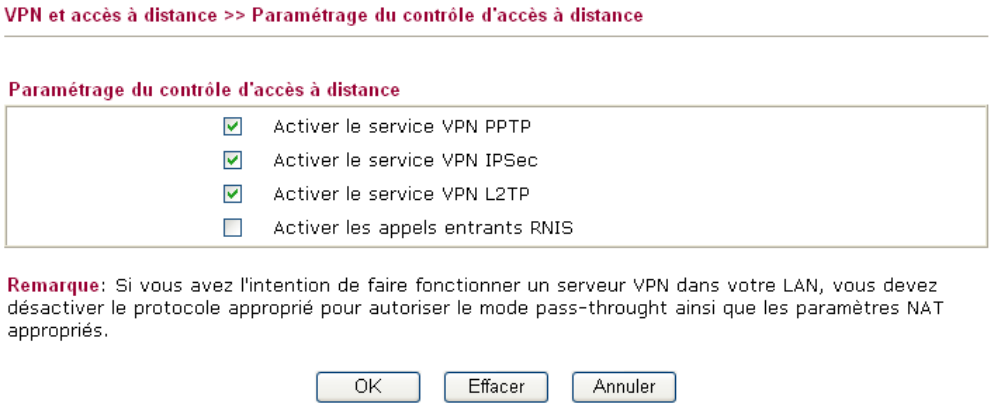
Vous disposez également des fonctions d'interconnexion de LAN RNIS et d'accès à distance (modèle *i* seulement).

Les options du menu VPN et accès à distance sont les suivantes :



3.8.1 Contrôle d'accès à distance

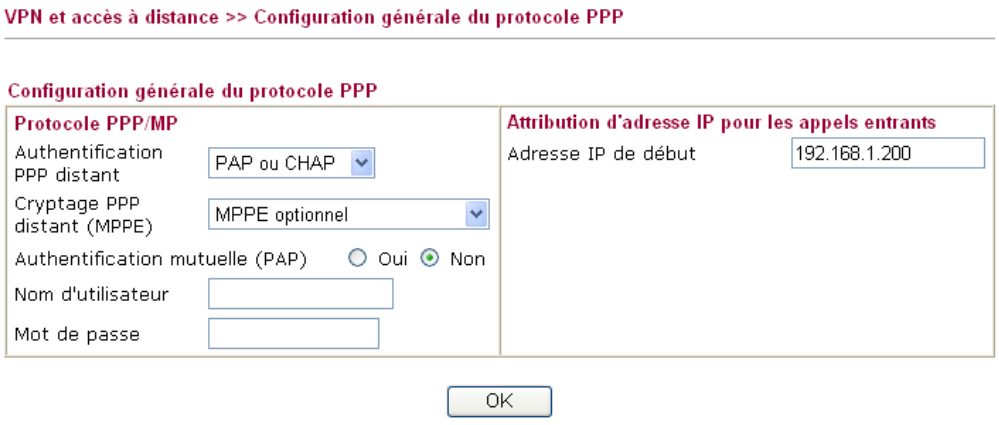
Activez le service VPN dont vous avez besoin. Si vous voulez faire fonctionner un serveur VPN dans votre LAN, vous devez désactiver le service VPN du routeur Vigor pour autoriser le mode transit de VPN, ainsi que les paramètres NAT appropriés, comme les paramètres DMZ ou d'ouverture de ports. Si vous voulez activer les appels entrants RNIS, cochez « Activer les appels entrants RNIS » dans cette page.



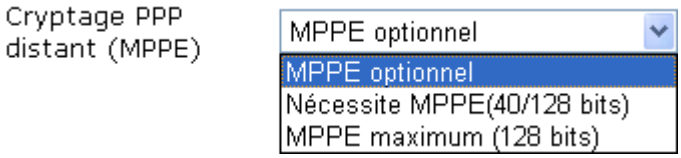
Activer le service VPN PPTP	Cochez cette case pour activer le service VPN avec le protocole PPTP.
Activer le service VPN IPSec	Cochez cette case pour activer le service VPN avec le protocole IPSec.
Activer le service VPN L2TP	Cochez cette case pour activer le service VPN avec le protocole L2TP.
Activer les appels entrant RNIS	Cette case sera utile aux utilisateurs européens.

3.8.2 Configuration générale du protocole PPP

Ce sous-menu s'applique uniquement aux connections PPP, comme PPTP, L2TP, L2TP sur IPSec du VPN ou RNIS.



Authentification PPP distant PAP seulement	Choisissez cette option pour que le routeur authentifie les utilisateurs distants avec le protocole PAP
PAP ou CHAP	Si vous choisissez cette option, le routeur tentera d'authentifier les utilisateurs distants d'abord avec le protocole CHAP. Si l'utilisateur distant ne prend pas en charge ce protocole, le routeur utilisera le protocole PAP pour l'authentification.
Cryptage PPP distant (MPPE) MPPE optionnel	Cette option signifie que la méthode de cryptage MPPE sera employée facultativement par le routeur pour l'utilisateur distant. Si l'utilisateur distant ne prend pas en charge l'algorithme de cryptage MPPE, le routeur transmettra « paquets non cryptés par MPPE ». Autrement, l'algorithme de cryptage MPPE sera utilisé.



Nécessite MPPE (40/128 bits) - Choisissez cette option pour que le routeur crypte les paquets à l'aide de l'algorithme de cryptage MPPE. L'utilisateur distant utilisera un cryptage sur 128 bits avant d'utiliser un cryptage sur 40 bits. En d'autres termes, si le cryptage MPPE sur 128 bits n'est pas disponible, c'est le cryptage sur 40 bits qui sera appliqué aux données.
MPPE maximum - Cette option indique que le routeur utilisera le cryptage MPPE sur 128 bits.

Authentification mutuelle (PAP)	La fonction d'authentification mutuelle est surtout utilisée pour communiquer avec d'autres routeurs ou clients qui ont besoin d'une authentification bidirectionnelle pour renforcer la sécurité, par exemple, les routeurs Cisco. Par conséquent, vous devez activer cette fonction si le routeur homologue demande une authentification mutuelle. Dans ce cas, vous devez également spécifier le **nom d'utilisateur** et le **mot de passe** de l'homologue.
Adresse IP de début	Entrez une adresse IP de début pour la connexion PPP entrante. Vous pouvez choisir une adresse IP du réseau privé local. Par exemple, si le réseau privé local est 192.168.1.0/255.255.255.0, vous pouvez choisir 192.168.1.200 comme adresse IP de début. Les adresses 192.168.1.200 et 192.168.1.201 sont réservées aux appels entrants RNIS.

3.8.3 Configuration générale IPSec

Dans **Configuration générale IPSec,** on distingue deux parties principales.

La négociation IKE/IPSec comporte deux phases.

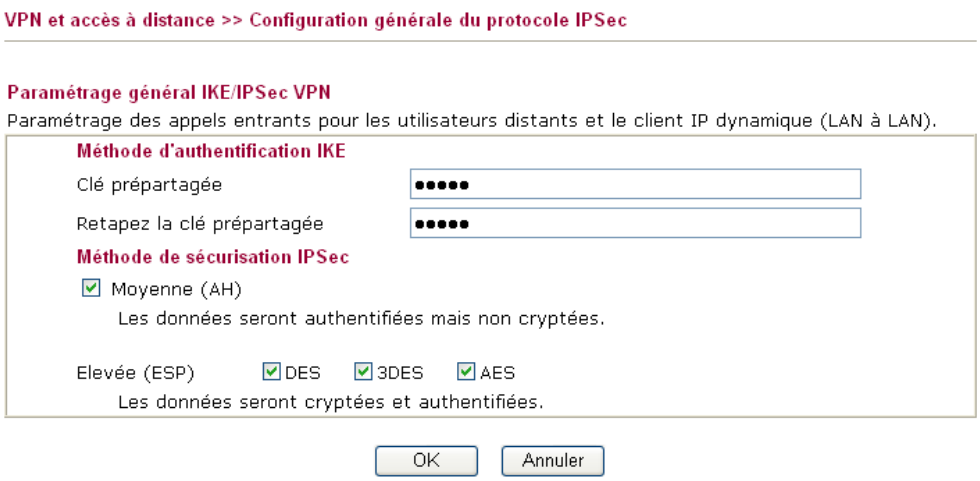
- Phase 1 : négociation des paramètres IKE, notamment les paramètres de cryptage, de hachage, Diffie-Hellman et de durée de vie pour protéger l'échange IKE qui suit, l'authentification des deux interlocuteurs à l'aide d'une clé prépartagée ou d'une signature numérique (X.509). L'interlocuteur qui entame la négociation propose toutes ses règles à l'interlocuteur distant, puis celui-ci tente de trouver une correspondance prioritaire avec ses règles. À la fin, un tunnel sécurisé est établi pour la phase 2 IKE.
- Phase 2 : négociation des méthodes de sécurisation IPSec, notamment l'en-tête d'authentification (AH) et/ou la charge utile de sécurité d'encapsulation (ESP) pour l'échange IKE suivant et le contrôle mutuel de l'établissement du tunnel sécurisé.

Dans IPSec, il y a deux modes d'encapsulation : **transport** et **tunnel**. Le mode **transport** ajoute la charge utile AH/ESP et utilise l'en-tête IP originel pour encapsuler uniquement la charge utile. Il n'est applicable qu'à un paquet local, par exemple L2TP sur IPSec. Le mode **tunnel** non seulement ajoute la charge utile AH/ESP mais également utilise un nouvel en-tête IP (en-tête IP de mode tunnel) pour encapsuler le paquet IP originel complet.

L'en-tête d'authentification (AH) assure l'authentification des données et l'intégrité des paquets IP échangés par les homologues VPN. Pour cela, une fonction de hachage à sens unique est appliquée aux paquets pour créer un condensé de message. Ce condensé est placé

dans l'AH et transmis avec les paquets. Côté réception, l'homologue applique la même fonction de hachage aux paquets et compare la valeur avec celle de l'AH reçu.

La charge utile de sécurité d'encapsulation (ESP) est un protocole de sécurisation qui assure la confidentialité et la protection des données avec un service optionnel d'authentification et de détection de rejet.



Méthode d'authentification IKE	Cette méthode s'applique généralement à un utilisateur distant ou à un nœud d'interconnexion de LAN qui utilise une adresse IP dynamique et des connexions de VPN liées à IPSec, comme L2TP sur IPSec et les tunnels IPSec. **Clé prépartagée –** Prend en charge actuellement uniquement l'authentification par clé prépartagée. **Clé prépartagée -** Spécifiez une clé pour l'authentification IKE. **Retapez la clé prépartagée -** Confirmez la clé prépartagée.
Méthode de sécurisation IPSec	En-tête d'authentification (AH) : les données seront authentifiées mais non cryptées. Par défaut, cette option est active **Élevée** - Charge utile de sécurité d'encapsulation (ESP) : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES.

3.8.4 Identité d'homologue IPSec

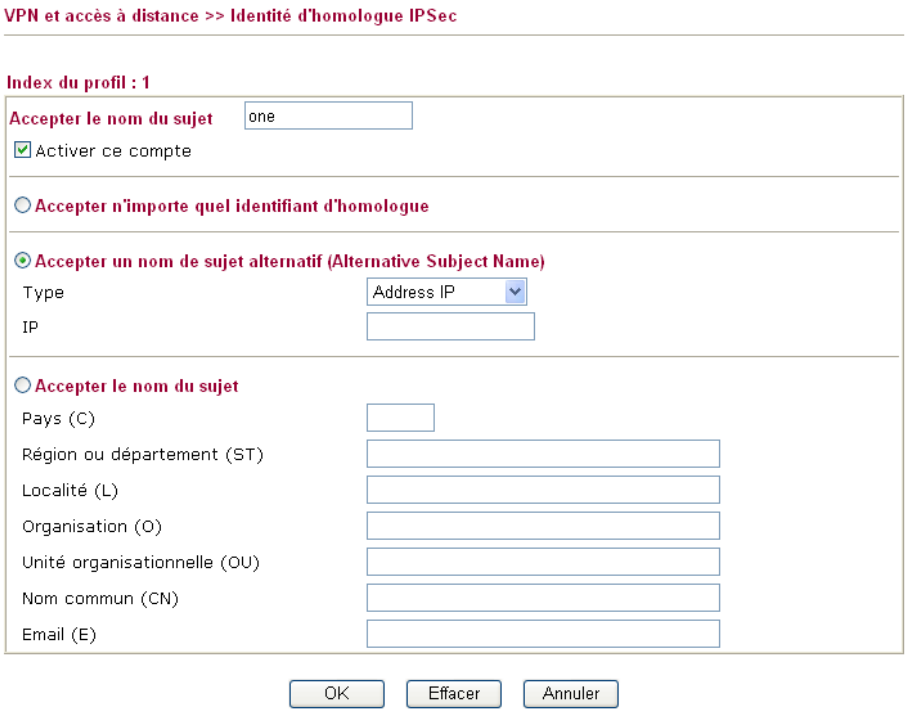
Pour utiliser un certificat numérique pour l'authentification d'un homologue en mode interconnexion de LAN ou accès à distance, vous pouvez éditer une table de certificats d'homologue. Le routeur permet de spécifier 32 certificats numériques pour les appels entrants.

Paramètres par défaut Cliquez ici pour effacer tous les numéros d'index.

Index Cliquez un numéro d'index pour accéder à la page de paramétrage de l'identifiant d'homologue IPSec.

Nom Nom de profil correspondant à ce numéro d'index.

Pour éditer un certificat numérique, cliquez sur le numéro d'index correspondant. Il existe trois niveaux de sécurité pour l'authentification des signatures numériques : remplissez chaque champ nécessaire pour authentifier l'homologue distant. L'explication suivante vous aidera à remplir tous les champs nécessaires.



Nom du profil Tapez un nom dans ce champ.

Accepter n'importe quel Cliquez pour accepter n'importe quel homologue, quel que

identifiant d'homologue	soit son identifiant.
Accepter un nom alternatif de sujet	Cliquez pour vérifier un champ spécifique de la signature numérique afin d'accepter l'homologue qui a une valeur concordante. Le champ peut être **Adresse IP, Domaine** ou **Adresse e-mail**. Selon le type sélectionné, la zone sous Type apparaît pour que vous la complétiez.
Accepter un nom de sujet	Cliquez pour vérifier des champs spécifiques de la signature numérique afin d'accepter l'homologue qui a une valeur concordante. Les champs peuvent être les suivants : **Pays (C), Région ou département (ST), Localité (L), Organisation (O), Unité organisationnelle (OU), Nom commun (CN)** et **E-mail (E)**.

3.8.5 Compte d'appel entrant

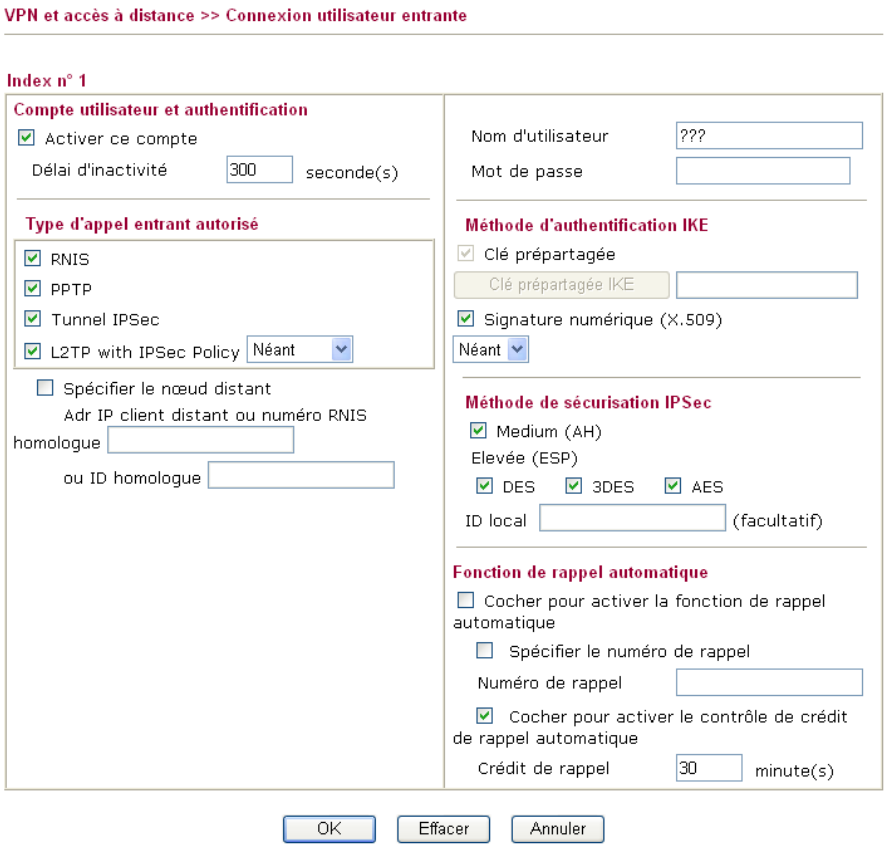
Vous pouvez gérer l'accès à distance à l'aide d'une table de profils d'utilisateur distant permettant d'authentifier l'utilisateur et d'établir la connexion de VPN. Vous pouvez définir des paramètres comme identifiant d'homologue, le type de connexion (RNIS, VPN avec PPTP, tunnel IPSec, L2TP ou L2TP sur IPSec), les méthodes de sécurisation correspondantes, etc.

Le routeur permet de créer 32 comptes d'utilisateur distant. En outre, vous pouvez étendre les comptes utilisateurs au serveur RADIUS grâce à la fonction client RADIUS intégré. L'écran récapitulatif est représenté ci-dessous.

Index	utilisateur	État	Index	utilisateur	État
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Paramètres par défaut	Cliquez ici pour effacer tous les numéros d'index.
Index	Cliquez sur un numéro d'index pour accéder à la page de paramétrage d'un utilisateur distant.
Utilisateur	Affiche le nom d'utilisateur de l'utilisateur distant ou du profil d'interconnexion de LAN. Le symbole ??? signifie que le profil est vide.
État	Affiche l'état de l'accès de l'utilisateur distant spécifié. V indique que l'utilisateur distant est actif. X indique que l'utilisateur distant est inactif.

Cliquez sur chaque numéro d'index pour éditer l'un des profils d'utilisateur distant. **Pour chaque type d'appel entrant, vous devez remplir les différents champs à droite.** Si les champs sont grisés, c'est que vous pouvez les laisser de côté. L'explication qui suit vous aidera à remplir tous les champs nécessaires.



Activer ce compte

Cochez la case pour activer cette fonction.
Délai d'inactivité - Délai d'inactivité à l'expiration duquel le routeur déconnectera l'utilisateur distant. Par défaut, le délai d'inactivité est de 300 secondes.

RNIS

Permet d'établir une connexion RNIS. Vous pouvez également paramétrer la fonction de rappel automatique. Vous devez spécifier le nom d'utilisateur et le mot de passe de l'utilisateur distant. Cette fonction ne concerne que les modèles ***i***.

PPTP

Permet à l'utilisateur distant d'établir une connexion de VPN PPTP via l'internet. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant.

Tunnel IPSec

Permet à l'utilisateur distant d'établir une connexion de VPN IPSec via l'internet.

L2TP

Permet à l'utilisateur distant d'établir une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP ou L2TP sur IPSec. Sélectionnez l'une des options suivantes :
Néant - ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure.
Souhaitée - appliquer d'abord la politique IPSec si elle est applicable pendant la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure.

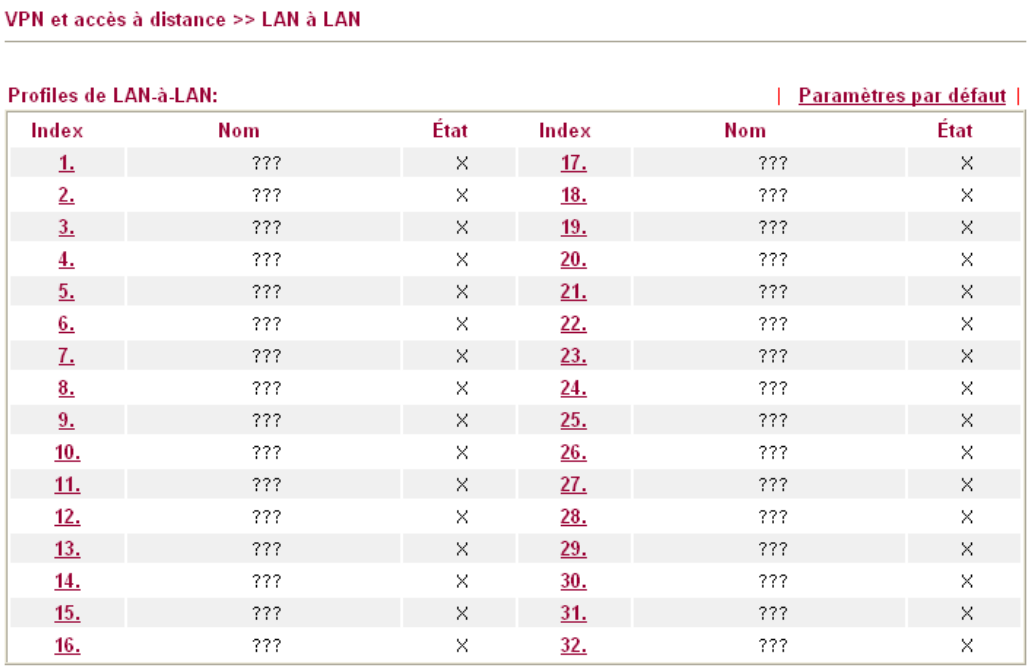
	Imposée - appliquer systématiquement la politique IPSec à la connexion L2TP.
Spécifier le nœud distant	**Cocher la case -** vous pouvez spécifier l'adresse IP de l'utilisateur distant ou l'identifiant d'homologue (utilisé en mode agressif IKE). **Décocher la case -** le type de connexion que vous avez sélectionné plus haut appliquera les méthodes d'authentification et de sécurisation définies dans les **Paramètres généraux**.
Nom d'utilisateur	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Mot de passe	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Méthode d'authentification IKE	Ce groupe de champs est applicable aux tunnels IPSec et à L2TP avec politique IPSec **lorsque vous spécifiez l'adresse IP du nœud distant**. La seule exception est la signature numérique (X.509) qui peut être spécifiée lorsque vous sélectionnez le tunnel IPSec avec ou sans l'adresse IP du nœud distant. **Clé prépartagée –** Cochez la case clé prépartagée pour activer cette fonction et tapez les caractères voulus (1 à 63) et tapez les 1 à 63 caractères de la clé prépartagée. **Signature numérique (X.509) –** Cochez la case Signature numérique pour activer cette fonction et sélectionnez l'une des signatures préétablies dans les profils ID homologue X.509.
Méthode de sécurisation IPSec	Ce groupe de champs est obligatoire pour les tunnels IPSec et L2TP avec politique IPSec lorsque vous spécifiez le nœud distant. Cochez la case Moyenne, DES, 3DES ou AES. **Moyenne - En-tête d'authentification (AH)** : les données seront authentifiées mais non cryptées. C'est l'option par défaut. Vous pouvez la désactiver. **Élevée - Charge utile de sécurité d'encapsulation (ESP)** : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES. **ID local -** Spécifiez un identifiant local à utiliser pour le paramétrage des appels entrants dans le profil d'interconnexion de LAN. Ce paramètre est facultatif et n'est utilisable qu'en mode agressif IKE.
Fonction de rappel automatique	La fonction de rappel automatique n'est applicable qu'aux appels entrants RNIS (pour modèles *i* seulement). Le coût de la connexion est facturé au propriétaire du routeur. **Cocher pour activer la fonction de rappel automatique** - Active la fonction de rappel automatique. **Spécifier le numéro de rappel automatique** - Cette option est destinée à renforcer la sécurité. Si elle est activée, le routeur rappelle UNIQUEMENT le **numéro de rappel automatique spécifié**. **Cocher pour activer le contrôle de crédit de rappel automatique** - Par défaut, la fonction de rappel automatique

comporte une limite de temps. Une fois le crédit de rappel automatique épuisé, le mécanisme de rappel automatique est désactivé automatiquement.
Crédit de rappel automatique (unité : minutes) : spécifiez le crédit de rappel automatique de l'utilisateur distant. Ce crédit est diminué automatiquement à chaque connexion de rappel automatique.

3.8.6 Profils d'interconnexion de LAN

Ici, vous pouvez gérer des interconnexions de LAN à l'aide d'une table de profils d'interconnexion. Vous pouvez définir des paramètres d'appel entrant ou sortant, des identifiants de connexion, des types de connexion (RNIS, VPN avec PPTP, tunnel IPSec, L2TP ou L2TP sur IPSec), les méthodes de sécurisation correspondantes, etc.

Le routeur permet de créer 32 profils, ce qui implique la prise en charge de 32 tunnels de VPN simultanés. La table des profils d'interconnexion de LAN est représentée ci-dessous.


VPN et accès à distance >> LAN à LAN

Profiles de LAN-à-LAN: | Paramètres par défaut |

Index	Nom	État	Index	Nom	État
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

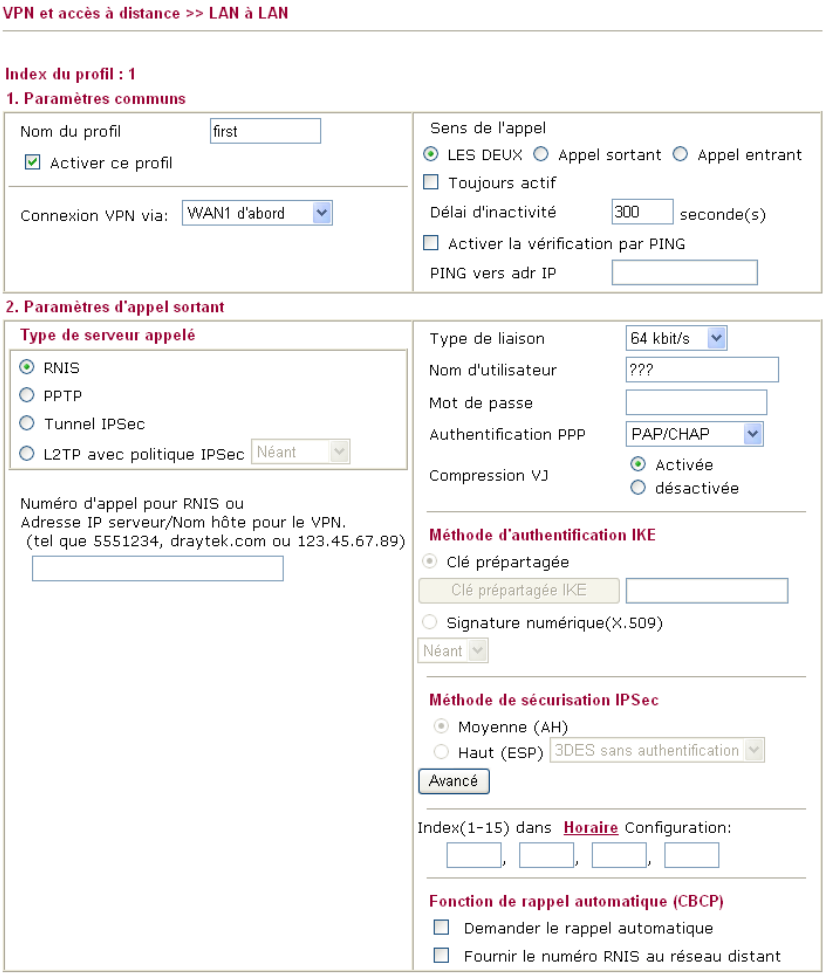
Paramètres par défaut Cliquez pour effacer tous les numéros d'index.

Nom Affiche le nom du profil d'interconnexion de LAN. ??? signifie que le profil est vide.

État Affiche l'état du profil. V indique que le profil est actif, X indique que le profil est inactif.

Cliquez sur chaque numéro d'index pour éditer un profil d'interconnexion de LAN. La page suivante apparaît. Chaque profil d'interconnexion de LAN comprend 4 sous-groupes de paramètres. Pour le sous-groupe Type d'appel entrant, il faut remplir les différents champs correspondants à droite. Si les champs sont grisés, c'est que vous pouvez les laisser tels que. L'explication suivante vous aidera à remplir les champs nécessaires.

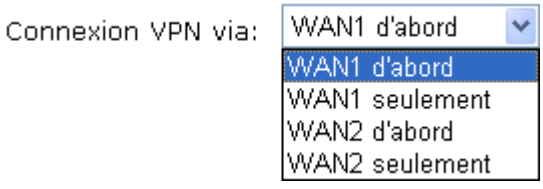
Comme la page web est trop longue, on l'a divisée en plusieurs parties.



Nom du profil Spécifiez un nom pour le profil d'interconnexion de LAN.

Activer ce profil Cochez cette case pour activer le profil.

Connexion VPN via Utilisez le menu déroulant pour choisir une interface WAN appropriée. Ce paramètre n'est utile que pour les appels sortants.



WAN1 d'abord – Lors de la connexion, le routeur utilisera l'interface WAN1 comme premier canal pour la connexion de VPN. Si l'interface WAN1 est défaillante, le routeur utilisera une autre interface WAN.
WAN1 seulement – Lors de la connexion, le routeur utilisera uniquement l'interface WAN1 pour la connexion de VPN.
WAN2 d'abord - Lors de la connexion, le routeur utilisera l'interface WAN2 comme premier canal pour la connexion de VPN. Si l'interface WAN2 est défaillante, le routeur utilisera une autre interface WAN.
WAN2 seulement - Lors de la connexion, le routeur utilisera uniquement l'interface WAN2 pour la connexion de VPN.

Connexion permanente ou **Connexion permanente** - cochez cette case pour que le

délai d'inactivité	routeur maintienne la connexion de VPN en permanence. **Délai d'inactivité :** la valeur par défaut est 300 secondes. Si la connexion est restée inactive jusqu'à l'expiration du délai d'inactivité, le routeur la libère.
Vérification par PING	Cette fonction permet au routeur de déterminer l'état de la connexion de VPN IPSec. Elle est particulièrement utile en cas d'interruption anormale du tunnel IPSec. Pour plus de détails, reportez-vous aux nota ci-dessous. Cochez cette case pour autoriser la transmission de paquets PING à une adresse IP spécifiée.
PING vers IP	Entrez l'adresse IP de l'hôte distant situé à l'autre extrémité du tunnel de VPN. **Activer la vérification par PING** : option utilisée pour traiter les interruptions anormales de connexions de VPN IPSec. Cette option permet de connaître l'état d'une connexion de VPN et d'apprécier l'opportunité de la rétablir. Normalement, si l'un des homologues VPN veut libérer la connexion, il doit échanger des paquets avec l'autre pour l'informer. Toutefois, si l'homologue distant libère la connexion sans préavis, le routeur Vigor ne s'en apercevra pas. Pour résoudre ce problème, le routeur Vigor vérifie l'état de la connexion de VPN en envoyant continuellement des paquets PING à l'hôte distant. Ceci est indépendant de la détection d'indisponibilité DPD (Dead Peer Detection).
RNIS	Si vous voulez relier deux réseaux en mode RNIS, sélectionnez le bouton d'option RNIS pour établir une connexion RNIS sortante avec le serveur. Vous pouvez également paramétrer la fonction de rappel automatique (CBCP). Cette fonction concerne uniquement les modèles ***i***.
PPTP	Établissement d'une connexion de VPN PPTP avec le serveur via l'internet. Vous devez spécifier le nom d'utilisateur et le mot de passe pour authentifier le serveur distant.
Tunnel IPSec	Établissement d'une connexion de VPN IPSec avec le serveur via l'internet.
L2TP avec …	Établissement d'une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP seul ou L2TP avec IPSec : **Néant :** ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure. **Souhaitée :** appliquer d'abord la politique IPSec si elle est applicable lors de la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure. **Imposée :** appliquer systématiquement à la connexion L2TP.
Nom d'utilisateur	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec.
Mot de passe	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec.
Authentification PPP	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous

sélectionnez RNIS. Normalement PAP/CHAP assure la compatibilité la plus large.

Compression VJ

Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS. La compression VJ est utilisée pour la compression de l'en-tête de protocole TCP/IP. Normalement **Oui** pour améliorer l'utilisation de la bande passante.

Méthode d'authentification IKE

Ce champ est applicable aux tunnels IPSec et à L2TP avec politique IPSec.
Clé prépartagée - Entrez une clé prépartagée (1 à 63 caractères).
Signature numérique (X.509) - Sélectionnez une signature numérique préétablie dans les profils d'ID homologue X.509.

Méthode de sécurisation IPSec

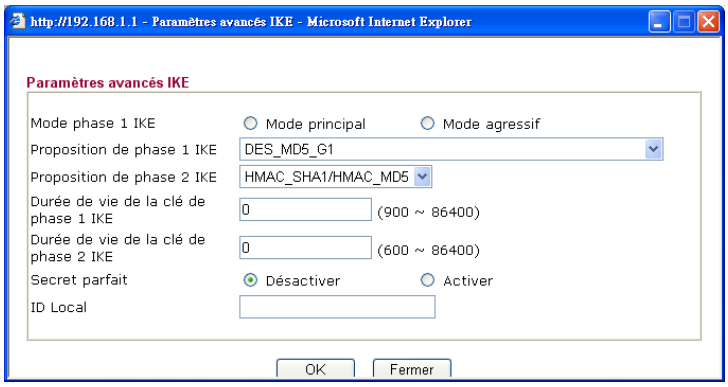
Ce champs est obligatoire pour les tunnels IPSec et pour L2TP avec politique IPSec.

Moyenne

En-tête d'authentification (AH) : les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée (ESP- Charge utile de sécurité d'encapsulation) : la charge utile (les données) sera cryptée et authentifiée.
Sélectionner un algorithme de cryptage :
DES sans authentification : utiliser l'algorithme de cryptage DES sans authentification.
DES avec authentification : utiliser l'algorithme de cryptage DES avec authentification.
3DES sans authentification : utiliser l'algorithme de cryptage 3DES sans authentification.
3DES avec authentification : utiliser l'algorithme de cryptage 3DES et appliquer l'algorithme d'authentification MD5 ou SHA-1.
AES sans authentification : utiliser l'algorithme de cryptage AES sans authentification.
AES avec authentification : utiliser l'algorithme de cryptage AES et appliquer l'algorithme d'authentification MD5 ou SHA-1.

Avancé

Spécifiez le mode, la proposition et la durée de vie des clés pour chaque phase IKE :



Mode phase 1 IKE : mode principal et mode agressif. Il s'agit d'échanger des propositions de sécurisation pour créer un

canal sécurisé. Le mode principal est plus sûr que le mode agressif car les échanges sont plus nombreux dans un canal sécurisé pour établir une session IPSec. Toutefois, le mode agressif est plus rapide. Le mode par défaut est le mode principal.

Proposition de phase 1 IKE : proposer aux homologues de VPN les mécanismes d'authentification et algorithmes de cryptage locaux et obtenir un retour pour trouver une correspondance. Il existe deux options pour le mode agressif et neuf options pour le mode principal. Nous suggérons de choisir l'option qui couvre le plus grand nombre d'algorithmes.

Proposition de phase 2 IKE : proposer aux homologues de VPN les algorithmes disponibles locaux et obtenir un retour pour trouver une correspondance. Il existe trois options pour les deux modes. Nous suggérons de choisir l'option qui couvre le plus grand nombre d'algorithmes.

Durée de vie de la clé de phase 1 IKE : pour des raisons de sécurité, la durée de vie de la clé doit être définie. La valeur par défaut est de 28800 secondes. Vous pouvez spécifier une valeur comprise entre 900 et 86400 secondes.

Durée de vie de la clé de phase 2 IKE : pour des raisons de sécurité, la durée de vie de la clé doit être définie. La valeur par défaut est de 3600 seconds. Vous pouvez spécifier une valeur comprise entre 600 et 86400 secondes.

Secret parfait (PFS) : la clé de phase 1 IKE est réutilisée pour éviter la complexité des calculs de la phase 2. Par défaut, cette fonction est inactive.

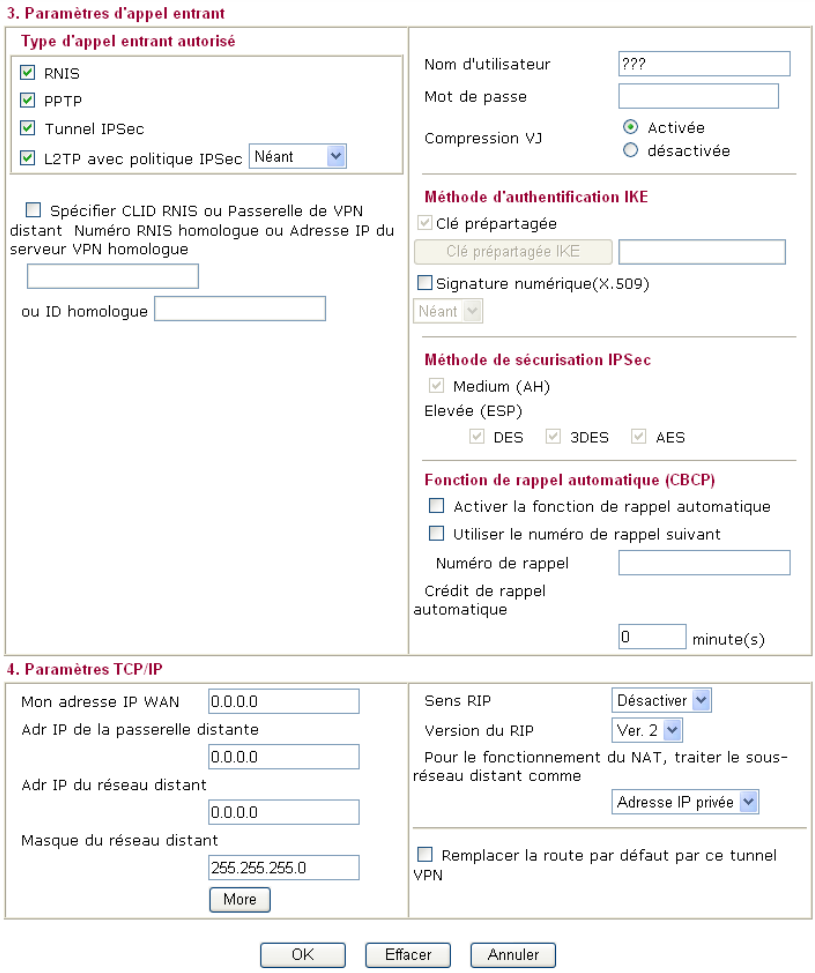
ID local : en mode **agressif**, l'ID local est l'adresse IP qui sert pour l'authentification avec le serveur de VPN distant.

Fonction de rappel automatique (modèles I seulement)

La fonction de rappel automatique fournit un service de rappel automatique pour les utilisateurs distants RNIS dans le cadre du protocole PPP. Le coût de la connexion est facturé au propriétaire du routeur.

Demander à l'homologue distant de rappeler - Activez cette option pour que le routeur demande à l'homologue distant de rappeler.

Fournir le numéro RNIS à l'homologue distant - Dans le cas où l'homologue distant demande au routeur Vigor de rappeler, le numéro RNIS local est fourni à l'homologue distant. Cliquez ici pour que le routeur Vigor envoie le numéro RNIS au routeur distant. Cette fonction concerne uniquement les modèles ***i***.



Type d'appel entrant autorisé — Définit le type d'appel entrant autorisé.

RNIS — Permet d'établir une connexion RNIS. Vous pouvez également paramétrer la fonction de rappel automatique. Vous devez spécifier le nom d'utilisateur et le mot de passe de l'utilisateur distant. Cette fonction concerne uniquement les modèles ***i***. Vous pouvez aussi paramétrer la fonction de rappel automatique plus loin.

PPTP — Permet à l'utilisateur distant d'établir une connexion de VPN PPTP via l'internet. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant.

Tunnel IPSec — Permet à l'utilisateur distant d'établir une connexion de VPN IPSec via l'internet.

L2TP — Permet à l'utilisateur distant d'établir une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP ou L2TP sur IPSec :
Néant- ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure.
Souhaitée- appliquer d'abord la politique IPSec si elle est applicable pendant la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure.

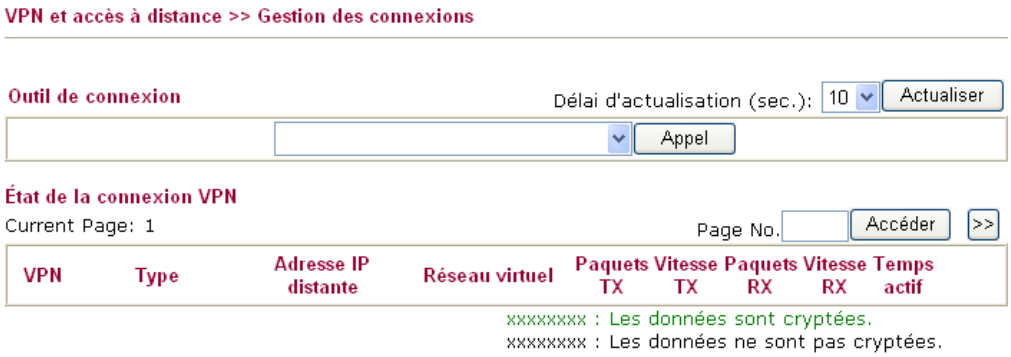
	Imposée- appliquer systématiquement la politique IPSec à la connexion L2TP.
Spécifier le CLID ou la passerelle de VPN distante	Vous pouvez spécifier l'adresse IP de l'utilisateur distant ou l'identifiant d'homologue (qui doit être le même que celui du type d'appel entrant) en cochant la case. Tapez le numéro RNIS d'homologue si vous avez sélectionné RNIS plus haut (Cette fonction ne concerne que les modèles ***i***.). Vous devez également spécifier les méthodes de sécurisation correspondantes à droite. Si vous décochez la case, le type de connexion que vous avez sélectionné plus haut appliquera les méthodes d'authentification et de sécurisation définies dans les paramètres généraux.
Nom d'utilisateur	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec.
Mot de passe	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec.
Compression VJ	La compression VJ est utilisée pour la compression de l'en-tête de protocole TCP/IP. Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec.
Méthode d'authentification IKE	Ce groupe de champs est applicable aux tunnels IPSec et à L2TP avec politique IPSec lorsque vous spécifiez le CLID RNIS (modèles *i* seulement) ou un numéro RNIS d'homologue de passerelle de VPN distante (modèles *i* seulement) ou encore une adresse IP de serveur de VPN d'homologue. La seule exception est la signature numérique (X.509) que vous pouvez spécifier lorsque vous sélectionnez le mode tunnel IPSec avec ou sans le CLID ou l'adresse IP du nœud distant. **Clé prépartagée –** Cochez la case Clé prépartagée pour activer cette fonction et tapez les caractères voulus (1 à 63). **Signature numérique (X.509) –** Cochez la case Signature numérique pour activer cette fonction et sélectionnez une signature numérique préétablie dans les profils d'ID homologue X.509.
Méthode de sécurisation IPSec	Ce groupe de champs est obligatoire pour les tunnels IPSec et pour L2TP avec politique IPSec lorsque vous spécifiez le nœud distant. **Moyenne -** En-tête d'authentification (AH) : les données seront authentifiées mais non cryptées. Par défaut, cette option est active. **Élevée -** Charge utile de sécurité d'encapsulation (ESP) : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES.
Fonction de rappel automatique	La fonction de rappel automatique n'est applicable qu'aux appels entrants RNIS (cette fonction est utile uniquement pour les modèles ***i***). Le coût de la connexion est facturé au propriétaire du routeur. **Cocher pour activer la fonction de rappel automatique** - Active la fonction de rappel automatique.

	Spécifier le numéro de rappel automatique - Cette option est destinée à renforcer la sécurité. Si elle est activée, le routeur rappelle UNIQUEMENT le numéro de rappel automatique spécifié. **Cocher pour activer le contrôle de crédit de rappel automatique** - Par défaut, la fonction de rappel automatique comporte une limite de temps. Une fois le crédit de rappel automatique épuisé, le mécanisme de rappel automatique est désactivé automatiquement. **Crédit de rappel automatique (unité : minutes)** - Spécifiez le crédit de rappel automatique de l'utilisateur distant. Ce crédit est diminué automatiquement à chaque connexion de rappel automatique.
Mon adresse IP WAN	Ce champ est applicable uniquement lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. La valeur par défaut est 0.0.0.0. Le routeur Vigor obtient une adresse IP WAN du routeur distant pendant la phase de négociation IPCP. Si l'adresse IP WAN est fixée par le routeur distant, spécifiez ici l'adresse IP fixe. Ne changez pas la valeur par défaut si vous ne sélectionnez pas RNIS, PPTP ou L2TP.
Ad. IP de la passerelle distante	Ce champ est applicable uniquement lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. La valeur par défaut est 0.0.0.0. Le routeur Vigor obtient une adresse IP de passerelle distante du routeur distant pendant la phase de négociation IPCP. Si l'adresse IP de WAN est fixée par le routeur distant, spécifiez ici l'adresse IP fixe. Ne changez pas la valeur par défaut si vous ne sélectionnez pas RNIS, PPTP ou L2TP.
Adr. IP du réseau distant/Masque du réseau distant	Ajoute un routeur statique pour aiguiller tout le trafic destiné à cette adresse IP de réseau distant ou à ce masque de réseau distant via la connexion de VPN. Pour IPSec, il s'agit de l'identifiant des clients de destination pour le mode rapide de phase 2.
Suite	Ajoute un routeur statique pour aiguiller tout le trafic destiné à cette adresse IP de réseau distant ou à ce masque de réseau distant via la connexion de VPN. Généralement utilisé lorsqu'il y a plusieurs sous-réseaux derrière le routeur de VPN distant.
Sens RIP	L'option spécifie le sens des paquets RIP (Routing Information Protocol). Vous pouvez activer/désactiver l'un des sens. Il y a quatre options : TX/RX, TX seulement, RX seulement et Désactiver.
Version du RIP	Sélectionnez la version du protocole RIP. Spécifiez Ver. 2 pour que la compatibilité soit la plus large possible.
Pour le fonctionnement du NAT, traiter le sous-réseau distant comme	Lorsqu'il communique avec le sous-réseau distant, le routeur peut le traiter comme un sous-réseau privé envoyant des paquets avec l'adresse IP¨privée du routeur ou le traiter comme un sous-réseau public envoyant des paquets avec l'adresse IP publique du routeur.
Remplacer la route par	Cochez cette case pour remplacer la route par défaut par ce tunnel VPN. À noter que ce paramètre n'est disponible que si

défaut par ce tunnel VPN une seule interface WAN est active. Si les deux interfaces WAN sont actives, il n'est pas disponible.

3.8.7 Gestion des connexions

Le tableau récapitulatif de toutes les connexions de VPN est donné ci-dessous. Vous pouvez libérer n'importe quelle connexion de VPN en cliquant sur le bouton **Suppr**. Vous pouvez également utiliser l'outil d'appel sortant et cliquez sur le bouton **Appel**.

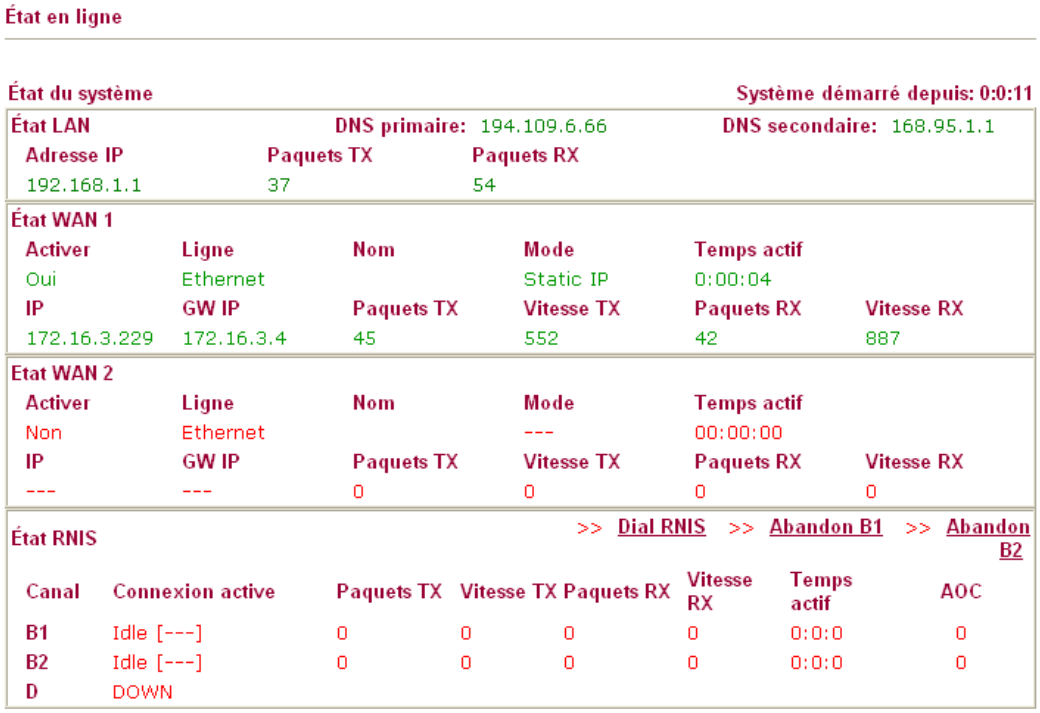


Appel Cliquez sur ce bouton pour appeler.

Intervalle d'actualisation Choisissez un intervalle d'actualisation des informations d'appel : 5, 10, ou 30 secondes.

Actualiser Cliquez sur ce bouton pour actualiser l'état de toute la connexion.

Nota : l'état de l'interconnexion de LAN pour RNIS est affiché sur la plage **État en ligne**.



3.9 Gestion des certificats

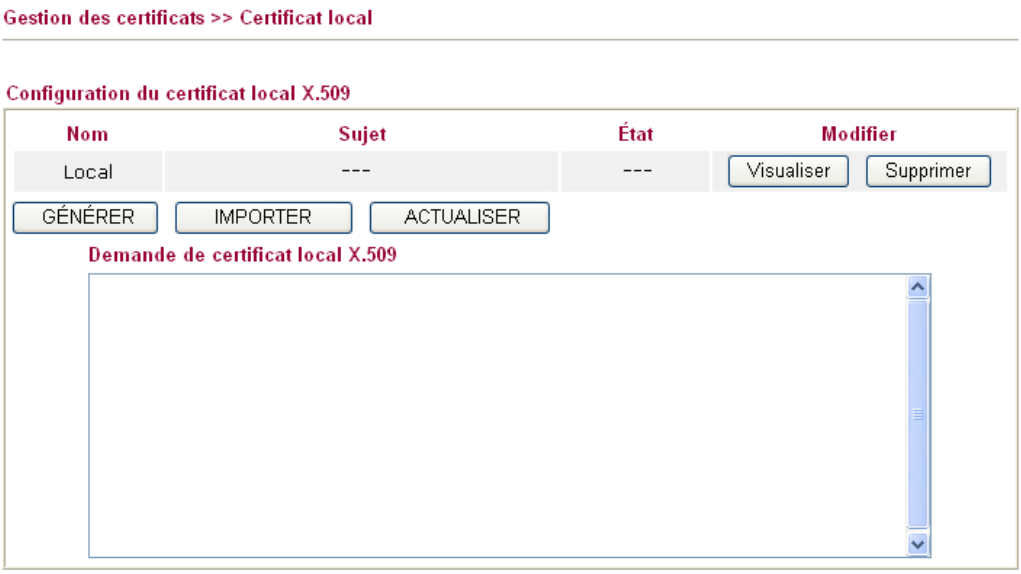
Un certificat numérique est un identifiant électronique délivré par une autorité de certification (AC). Il contient des informations telles que votre nom, un numéro de série, des dates d'expiration, etc., et la signature numérique de l'autorité de certification afin qu'un destinataire puisse vérifier que le certificat est authentique. Le routeur Vigor prend en charge les certificats numériques conformes à la norme X.509.

Une entité voulant utiliser des certificats numériques doit d'abord demander un certificat à un serveur d'AC. Il doit également se procurer les certificats d'autres serveurs d'AC de confiance afin de pouvoir authentifier l'homologue avec des certificats émis par ces serveurs d'AC de confiance.

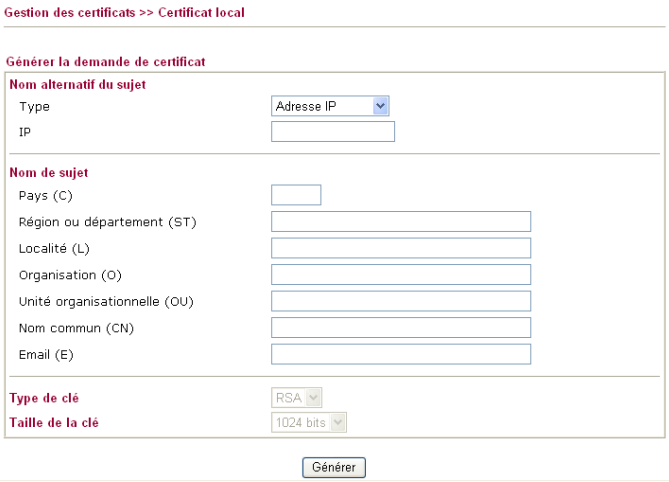
Ici, vous pouvez créer et gérer des certificats numériques locaux et des certificats d'AC de confiance. N'oubliez pas de mettre le routeur à l'heure avant d'utiliser le certificat pour que la période de validité du certificat soit correcte.

Les options du menu Gestion des certificats sont les suivantes :

3.9.1 Certificat local



Générer Cliquez sur ce bouton pour ouvrir la fenêtre **Générer la demande de certificat**.



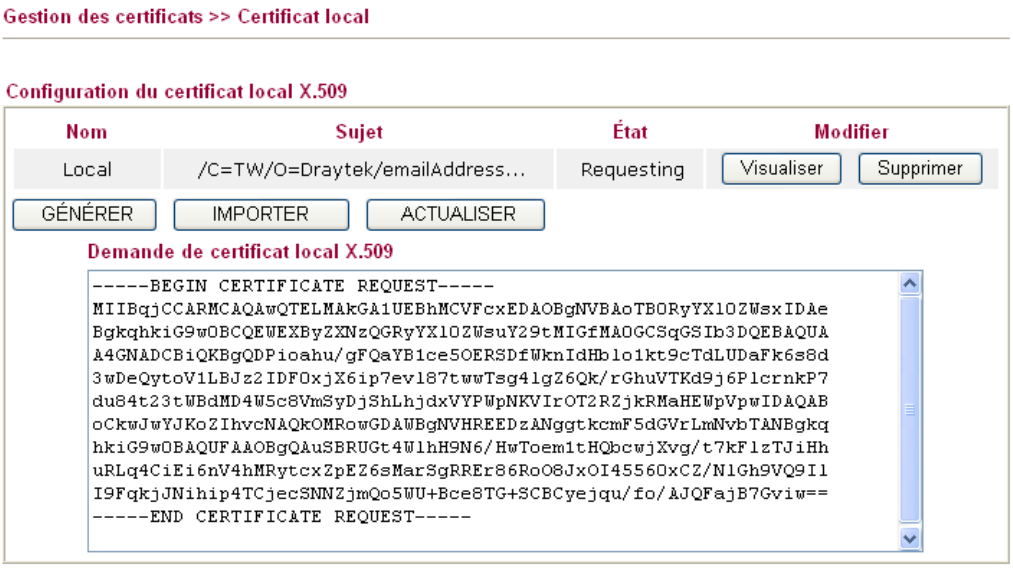
Remplissez la fenêtre, puis cliquez de nouveau sur **Générer**.

Importer Cliquez sur ce bouton pour importer un fichier enregistré comme fichier d'informations de certification.

Actualiser Cliquez sur ce bouton pour actualiser les informations.

Visualiser Cliquez sur ce bouton pour visualiser les paramètres de la demande de certificat.

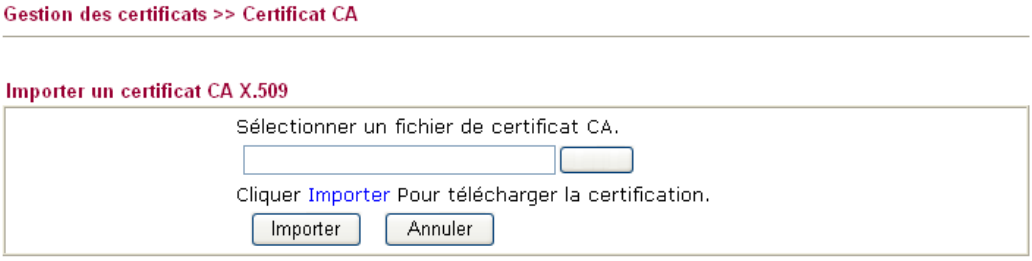
Quand vous cliquez sur **GENERER**, les informations générées sont affichées dans la fenêtre ci-dessous :



3.9.2 Certificat d’AC de confiance

La fonction Certificat d’AC de confiance affiche trois certificats d’AC de confiance.

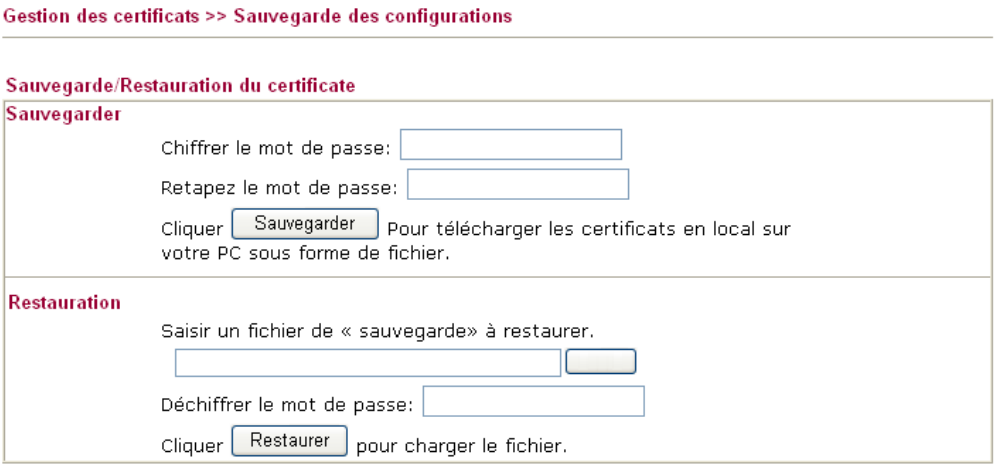
Pour importer un certificat d'AC de confiance préenregistré, cliquez sur **IMPORTER** pour ouvrir la fenêtre suivante. Cliquez sur **Parcourir…** pour rechercher le fichier texte enregistré. Puis cliquez sur Importer. Le certificat que vous avez importé apparaîtra dans la fenêtre Certificat d’AC de confiance. Cliquez sur **Importer** pour utiliser le fichier préenregistré.



Pour visualiser chaque certificat d’AC de confiance, cliquez sur **Visualiser**. Si vous voulez supprimer un certificat d’AC, choisissez-le dans la fenêtre et cliquez sur **Supprimer**.

3.9.3 Sauvegarde des certificats

Le certificat local et le certificat d'AC de confiance peuvent être sauvegardés dans un même fichier. Cliquez sur **Sauvegarde** dans l'écran suivant. Si vous voulez définir un mot de passe de cryptage pour ces certificats, tapez le mot de passe dans le champ **Mot de passe de cryptage** et dans le champ **Retaper le mot de passe**.



3.10 VoIP

La téléphonie sur IP (VoIP) vous permet d'utilise votre connexion à internet à haut débit pour téléphoner via l'internet.

Il existe de nombreux protocole de signalisation d'appel qui permettent à des équipements VoIP de converser. Les protocoles les plus répandus sont SIP, MGCP, Megaco et H.323. Ces protocoles ne sont pas tous compatibles entre eux (sauf si un serveur d'appels est utilisé).

Les modèles Vigor V prennent en charge le protocole SIP car c'est un protocole idéal pour le fournisseur de service téléphonique sur internet (ITSP) et pour les logiciels de téléphonie (« softphones ») et qu'il est très répandu. Le protocole SIP est un protocole de signalisation de bout en bout qui établit la présence et la mobilité des utilisateurs dans une structure VoIP. Pour converser, on utilise un identificateur uniforme de ressource (URI) (« adresse SIP »). Le format normalisé de l'URI SIP est

sip: user:password @ host: port

Certains champs peuvent être facultatifs selon l'utilisation. En général, « host » fait référence à un domaine. « userinfo » comprend le champ utilisateur, le champ mot de passe et le signe @. L'URI est très semblable à une adresse universelle (URL). C'est pourquoi certains l'appellent « URL SIP ». Le SIP permet l'appel direct d'homologue à homologue ainsi que l'appel via un serveur mandataire (proxy) SIP (qui joue un rôle semblable au portier des réseaux H.323), alors que le protocole MGCP utilise une architecture client-serveur, le scénario d'appel étant très semblable à celui du RTCP actuel.

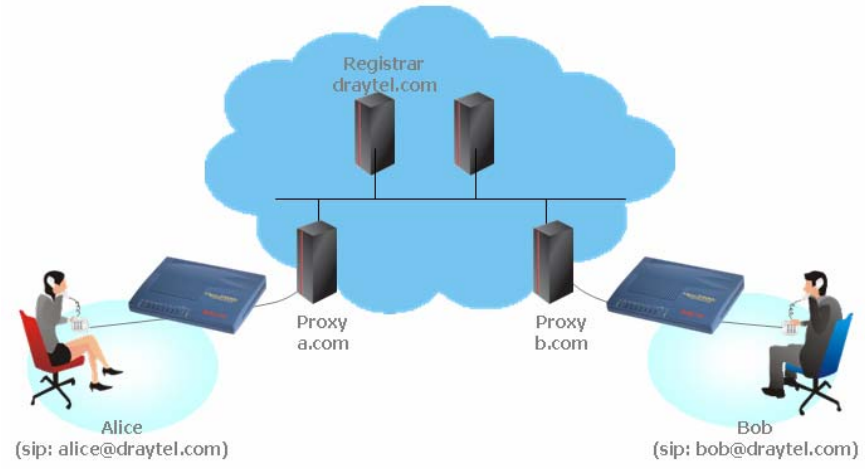
Après l'établissement d'un appel, les flux téléphoniques sont transmis via le protocole de transport en temps réel (RTP). Différents codecs (qui compriment et codent la voix) peuvent être intégrés aux paquets RTP. Les modèles Vigor V fournissent différents codecs, G.711 loi A/µ, G.723, G.726 et G.729 A & B. Chaque codec a une bande passante différente et donc donne une qualité vocale différente. Plus la bande passante d'un codec est large, meilleure est la qualité vocale. Toutefois, le codec utilisé doit être approprié à votre débit internet.

Il y a normalement deux scénarios d'appel possible :

- **Appel via des serveurs SIP**

  Tout d'abord, vos Vigor V doivent s'inscrire sur un serveur registre SIP en envoyant des messages d'inscription. Puis les serveurs mandataires SIP des deux correspondants transmettent la suite de message à l'appelant pour établir la session.

  Si les deux correspondants s'inscrivent sur le même serveur registre SIP les choses se passent comme ci-dessous :



  Le principal avantage de ce scénario est que vous n'avez pas à mémoriser l'adresse IP de votre correspondant, qui peut changer très fréquemment si elle est dynamique. Au lieu de cela, il vous suffit d'utiliser le **plan de numérotation** ou d'appeler directement le **nom de compte** de votre correspondant si vous êtes inscrit sur le même serveur registre SIP. Reportez-vous aux **exemples 1 et 2** du **scénario d'appel.**

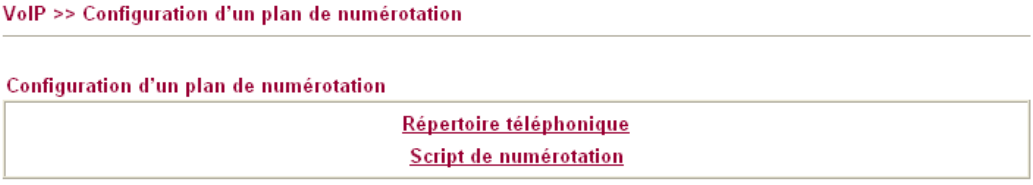
- **Communication d'homologue à homologue (P2P)**

  Pour appeler, vous devez connaître l'adresse IP de votre correspondant. Les routeurs VoIP Vigor établissent la connexion. Reportez-vous à l'**exemple 3 du scénario d'appel.**

  Nos modèles Vigor V mettent d'abord en œuvre des codecs efficaces conçus pour utiliser au mieux la bande passante disponible. Ils sont également dotés d'une fonction d'assurance automatique de la qualité de service. L'assurance de la qualité de service permet de donner la priorité au trafic téléphonique. Votre bande passante d'arrivée et de départ donne la priorité au trafic téléphonique mais vos données subissent un léger retard, tolérable pour le trafic de données.

3.10.1 DialPlan (plan de numérotation)

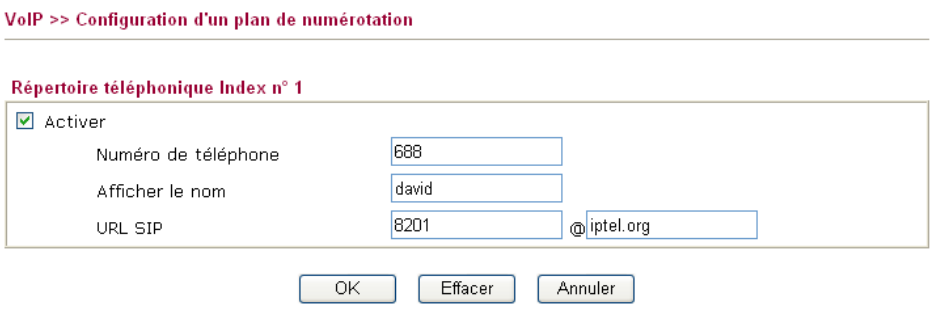
Cette page vous permet de configurer le répertoire téléphonique et le script de numérotation pour la fonction VoIP. Pour accéder aux pages de configuration du plan de numérotation, cliquez sur les liens **Répertoire téléphonique** et **Script de numérotation**.



Répertoire téléphonique

Vous pouvez mettre vos contacts VoIP dans le « répertoire téléphonique » appelé DialPlan. Cela vous permettra d'appeler rapidement et facilement en utilisant la **numérotation abrégée**. Dans le DialPlan, vous pouvez enregistrer jusqu'à 60 adresses IP d'amis ou de parents. Si vous utilisez un routeur Vigor 2910VGi pour configurer le répertoire téléphonique, les colonnes **Bouclage** et **Numéro de téléphone de secours** sont affichées.

Cliquez sur un index pour afficher la page de configuration d'un plan de numérotation.



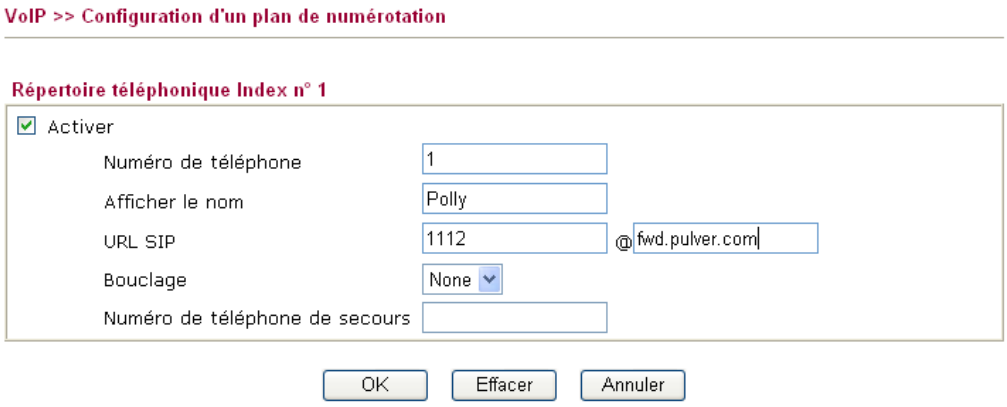
Activer Cochez la case pour activer cette entrée.

Numéro de téléphone Numéro abrégé. N'importe quelle combinaison des chiffres **0** à **9** et de ***** .

Afficher le nom Identifiant d'appelant qui s'affichera sur l'écran de votre contact, ce qui lui permettra de savoir d'emblée qui appelle sans avoir à mémoriser une multitude d'URL SIP.

URL SIP Tapez l'adresse SIP de votre contact.

Cette page diffère selon les modèles. La page ci-dessous est celle affichée dans le cas d'un routeur Vigor 2910VGi. Les paramètres **Bouclage** et **Numéro de téléphone de secours** n'existent que pour le modèle 2910VGi.



Activer Cochez la case pour activer cette entrée.

Numéro de téléphone Numéro abrégé. N'importe quelle combinaison des chiffres **0** à **9** et de ***** .

Afficher le nom Identifiant d'appelant qui s'affichera sur l'écran de votre contact, ce qui lui permettra de savoir d'emblée qui appelle sans avoir à mémoriser une multitude d'URL SIP.

URL SIP Tapez l'adresse SIP de votre contact.

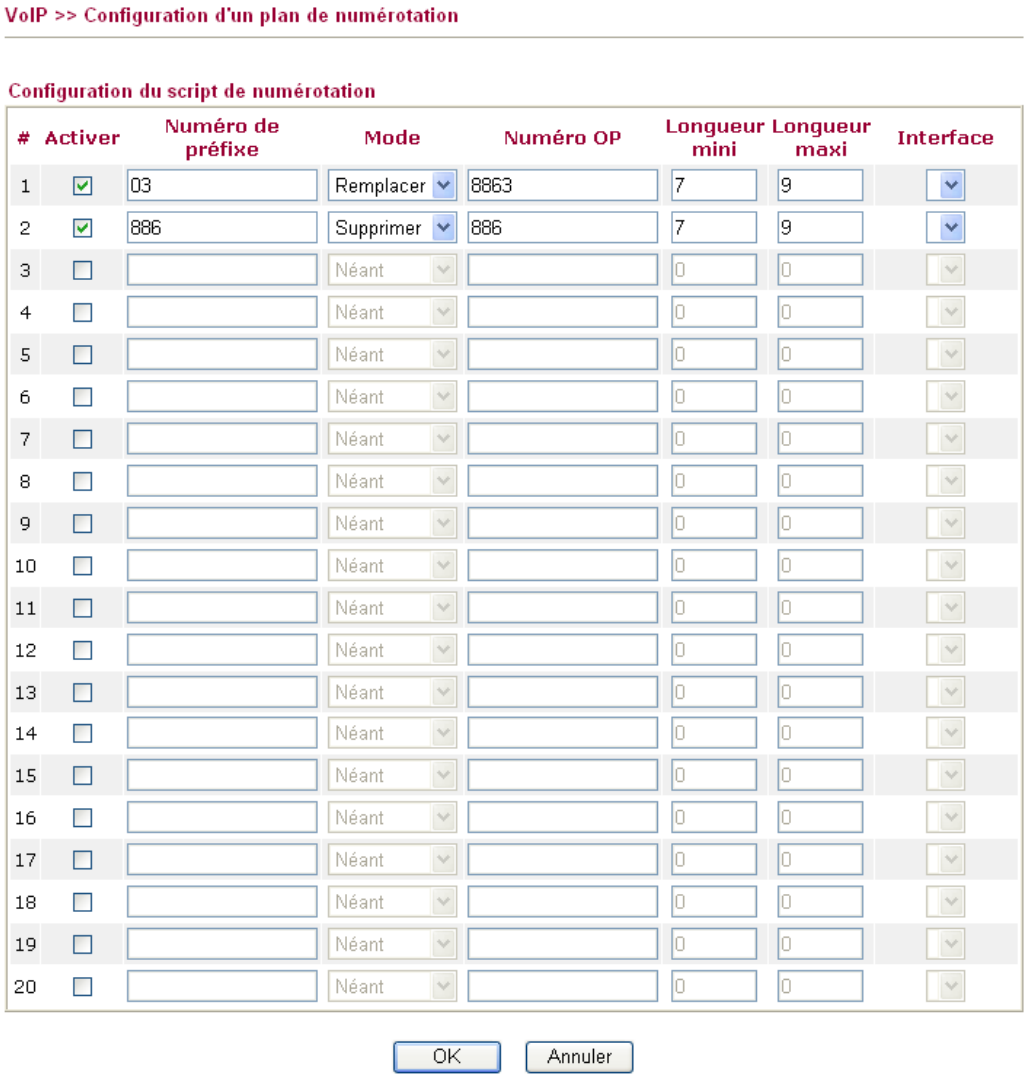
Bouclage Dans le cas du Vigor 2910VGi, le choix doit être le suivant :

Numéro de téléphone de secours Lorsque le téléphone VoIP ne fonctionne pas ou qu'il est impossible d'accéder à l'internet pour une raison ou pour une autre, c'est le numéro de téléphone de secours qui est composé à la place du numéro VoIP. L'appel est alors transformé en un appel RTCP selon le sens de bouclage choisi. Le changement

peut entraîner la taxation de votre numéro de téléphone RTCP. Tapez ici le numéro de téléphone de secours (numéro RTCP).

Script de numérotation

Cette page permet d'éditer des préfixes pour le compte SIP et notamment d'ajouter, de supprimer ou de remplacer un numéro. Elle vous aidera à établir des appels via l'interface VoIP.



Activer — Cochez cette case pour activer les paramètres de la ligne correspondante.

Préfixe — Le préfixe téléphonique entré ici est ajouté au numéro OP, le supprime ou le remplace.

Mode — **Néant** – Aucune action.
Ajouter – Le préfixe sera ajouté au numéro OP pour appeler via l'interface VoIP spécifique.
Supprimer – Le numéro OP sera supprimé par le préfixe pour appeler via l'interface VoIP spécifique. Dans l'exemple ci-dessus, le numéro OP *886* sera supprimé car le préfixe est *886*.
Remplacer – Le numéro OP sera remplacé par le préfixe pour

appeler via l'interface VoIP spécifique. Dans l'exemple ci-dessus, le numéro OP *8863* sera remplacé par *03*, valeur du préfixe.

Numéro OP — Première partie du numéro de compte servant à exécuter une fonction spéciale (selon le mode choisi) à l'aide du préfixe.

L mini — Longueur minimale du numéro pour l'application du préfixe. Dans l'exemple ci-dessus, si la longueur du numéro est comprise entre 7 et 9, l'application du préfixe est possible.

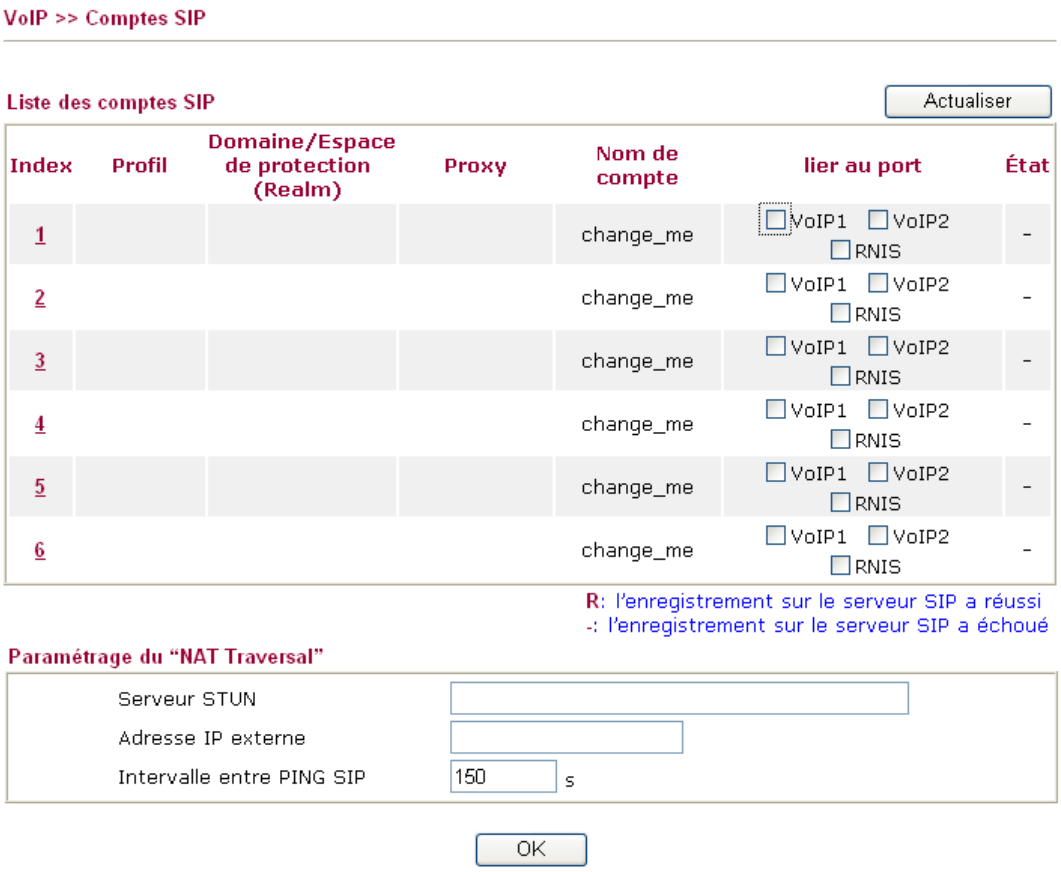
L maxi — Longueur maximale du numéro pour l'application du préfixe.

Interface — Choisissez l'un des **six** comptes SIP préenregistrés pour l'application du préfixe. Pour que cette interface soit disponible, il faut avoir paramétré un compte SIP.

3.10.2 Comptes SIP

Définissez ici vos propres paramètres SIP. Lorsque vous demandez un compte, votre fournisseur de service SIP vous alloue un **nom de compte** ou nom d'utilisateur, un serveur **registre SIP,** un serveur **proxy SIP** et un **nom de domaine**. (Dans certains cas, il se peut que les trois derniers soient identiques). Vous pourrez alors donner à vos contacts votre adresse SIP. **Nom de compte@ Nom de domaine.**

Lorsque vous allumez le routeur VoIP Vigor, il s'inscrit d'abord sur le serveur registre avec Nom d'utilisateur autorisé@Domaine/Espace de protection (Realm). Puis votre appel est acheminé à destination par le serveur proxy SIP avec Nom de compte@Domaine/Espace de protection comme identifiant.



Index Cliquez sur un index pour accéder à la page de configuration d'un compte SIP.

Profil Nom de profil du compte.

Domaine/Espace de protection (Realm) Nom de domaine ou adresse IP du serveur registre SIP.

Proxy Nom de domaine ou adresse IP du serveur proxy SIP.

Nom de compte Nom de compte de votre adresse SIP avant @.

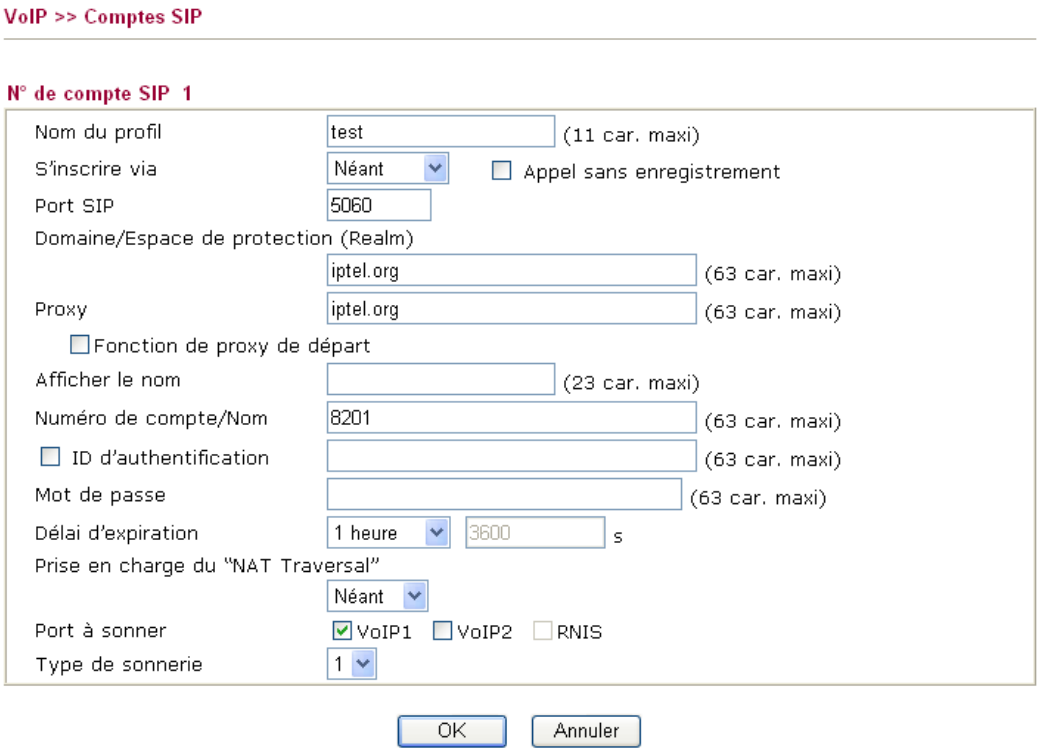
Port à sonner Spécifiez le port qui sonnera à la réception d'un appel téléphonique.

Serveur STUN Tapez l'adresse IP du serveur STUN.

Adresse IP externe Tapez l'adresse IP de passerelle.

Intervalle entre PING SIP La valeur par défaut est 150 s. Ce paramètre est utile pour la prise en charge du mécanisme « NAT Traversal » d'un serveur Nortel.

État Affiche l'état du compte SIP correspondant. **R** signifie que le compte est bien est enregistré sur le serveur SIP. **–** signifie que l'enregistrement du compte sur le serveur SIP a échoué.



Nom du profil

Donnez un nom à ce profil. Vous pouvez taper un nom semblable au nom de domaine. Par exemple, si le nom de domaine est *draytel.org*, vous pouvez tapez *draytel-1* dans ce champ.

S'inscrire via

Si vous voulez faire un appel VoIP sans vous inscrire, choisissez **Néant**. Certains serveurs SIP permettent d'utiliser la fonction VoIP sans s'inscrire. Avec un tel serveur, cochez la case **téléphoner sans s'inscrire**. Il est recommander de choisir **Auto**. Le système se chargera d'acheminer votre appel VoIP.

SIP Port

Port SIP Spécifiez le numéro de port pour l'envoi et la réception du message SIP d'ouverture de session. La valeur par défaut est **5060.** Votre homologue doit spécifier la même valeur dans son Registre.

Domaine/Espace de protection (Realm)

Tapez le nom de domaine ou l'adresse IP du serveur registre SIP.

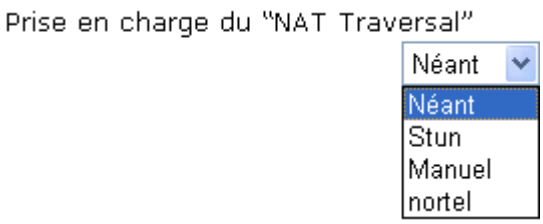
Proxy

Spécifiez le nom de domaine ou l'adresse IP du serveur proxy SIP. Vous pouvez maintenant faire suivre le nom de domaine du numéro de **port** de destination des données (par exemple, nat.draytel.org**:5065**).

Fonction de proxy de

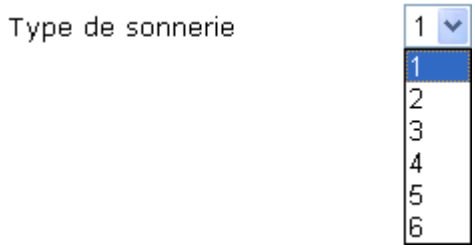
Cochez cette case pour que le serveur mandataire serve de

départ	mandataire de départ.
Nom affiché	Identifiant d'appelant qui s'affichera sur l'écran de votre correspondant.
Numéro/nom de compte	Tapez le nom de compte de votre adresse SIP, c'est-à-dire tout ce qui précède @.
ID d'authentification	Cochez la case pour activer la fonction d'authentification et tapez le nom ou le numéro pour l'authentification SIP sur le serveur registre SIP. S'il s'agit du numéro de compte, il n'est pas nécessaire de cocher la case ni de taper quoi que ce soit dans ce champ.
Mot de passe	Le mot de passe qui vous a été fourni lorsque vous vous êtes inscrit pour un service SIP.
Délai d'expiration	Période de temps pendant laquelle votre serveur registre SIP conserve votre inscription. Avant l'expiration du délai, le routeur enverra une autre demande d'inscription au serveur registre SIP.
Prise en charge du « NAT Traversal »	Si le routeur que vous utilisez (par exemple**,** un routeur à large bande) se connecte à l'internet pour un autre équipement, vous devez sélectionner l'option désirée.

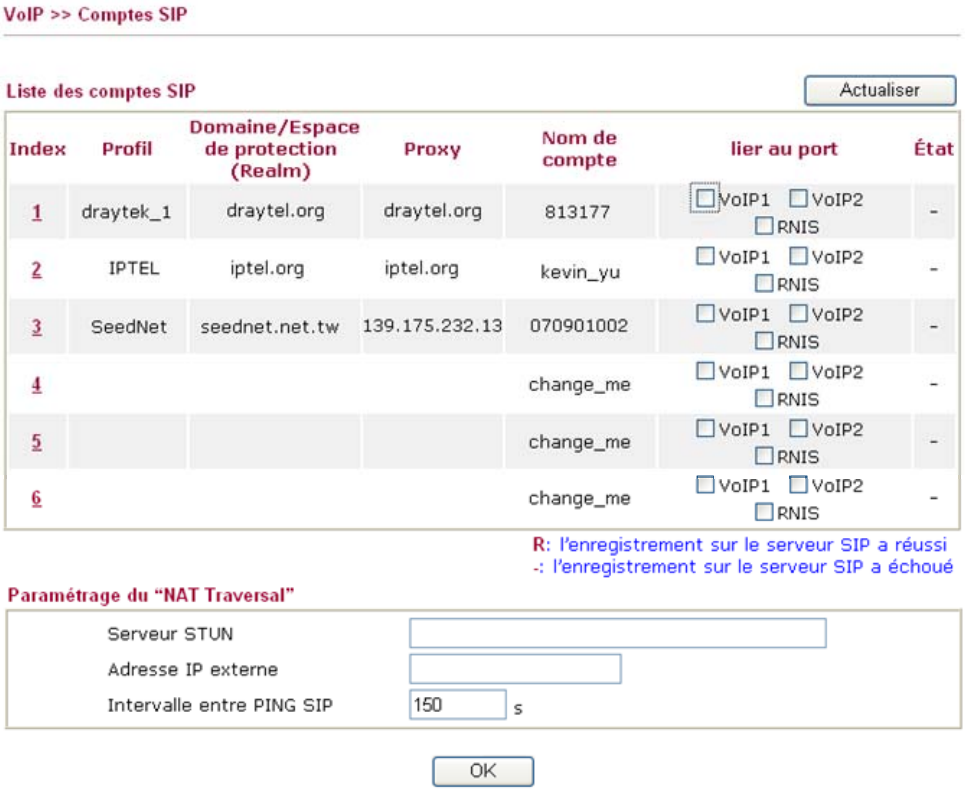


Néant – Désactiver cette fonction.
Stun – Choisissez cette option s'il y a un serveur STUN pour votre routeur.
Manuel – Choisissez cette option si vous voulez spécifier une adresse IP externe pour le « NAT Transversal ».
Nortel – Si le serveur d'appels que vous utilisez prend en charge la solution Nortel, vous pouvez choisir cette option.

Port à sonner	Choisissez VoIP 1 ou VoIP 2 comme port à sonner par défaut.
Type de sonnerie	Choisissez un type de sonnerie pour l'appel VoIP.

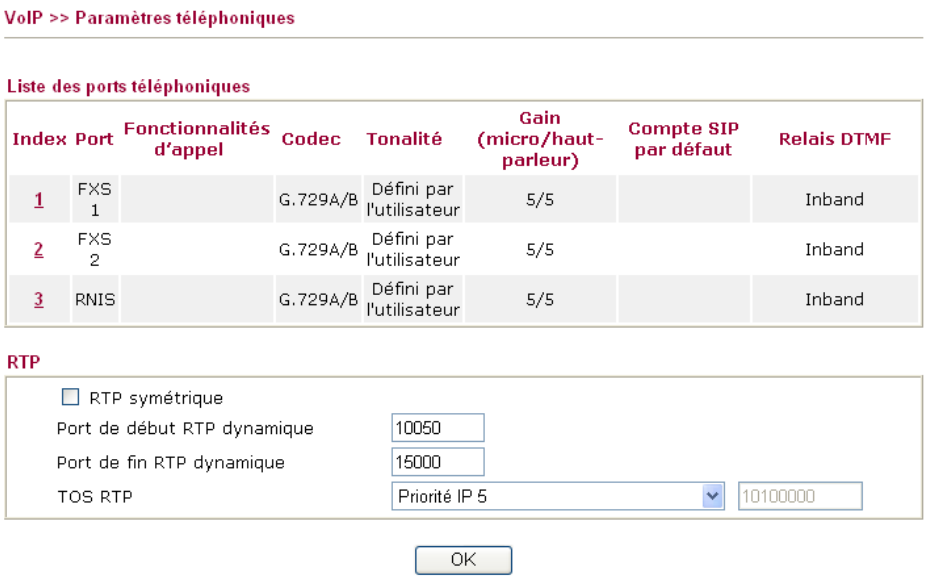


Le tableau ci-dessous donne des exemples de comptes SIP.



3.10.3 Paramètres téléphoniques

Cette page permet de définir les paramètres téléphoniques de VoIP 1 et VoIP 2.



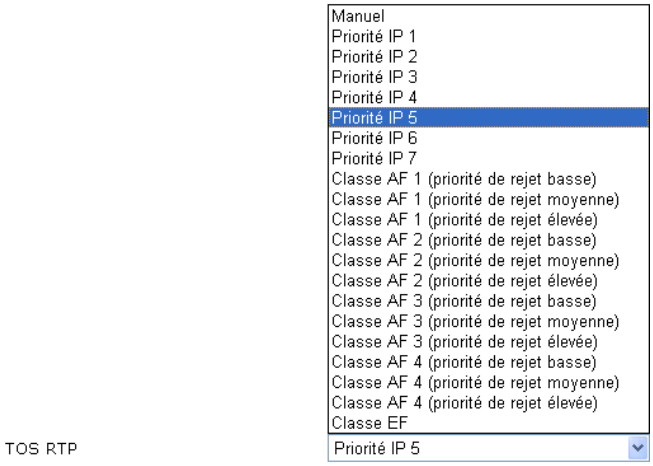
Liste des ports téléphoniques

Port – Il y a trois ports téléphoniques à configurer.
Caractéristique – Description succincte de la fonction d'appel pour votre information.
Codec –Codec par défaut de chaque port pour votre information. Vous pouvez changer de codec en cliquant sur le numéro sous Index.
Tonalités – Affichent la programmation effectuée dans les paramètres avancés.
Gain – Affiche les gains micro/haut-parleur définis dans les

paramètres avancés.
Compte SIP par défaut – « draytel_1 » est le compte SIP par défaut. Vous pouvez le changer en cliquant sur le numéro sous Index.
Relais DTMF– Affiche le mode DTMF défini dans les paramètres avancés.

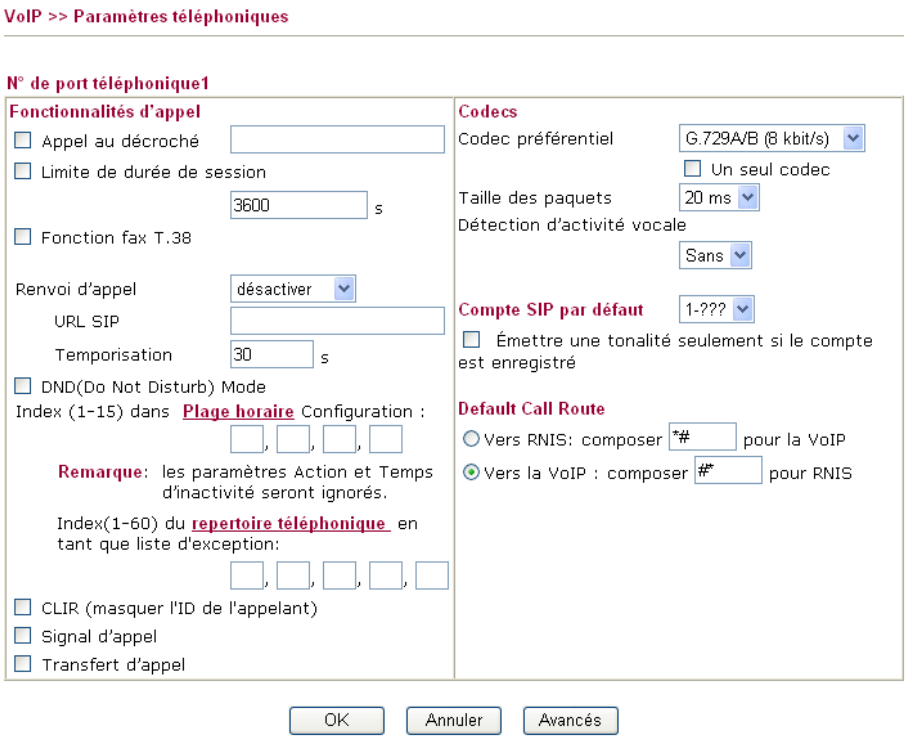
RTP

RTP symétrique – Cochez cette case pour éviter des anomalies de transmission de données au niveau du routeur local et du routeur distant du fait de la perte de paquets IP (par exemple, envoi de données de l'adresse IP publique du routeur distant à l'adresse IP privée du routeur local).
Port de début RTP dynamique – Port de début du flux RTP. La valeur par défaut est 10050.
Port de fin RTP dynamique – Port de fin du flux RTP. La valeur par défaut est 15000.
TOS RTP– Détermine le niveau de service VoIP. Utilisez la liste déroulante pour choisir l'un d'entre eux.



Paramètres des ports VoIP 1 et 2

Cliquez sur **1** ou **2** dans la colonne Index pour accéder aux pages de configuration des paramètres téléphoniques.

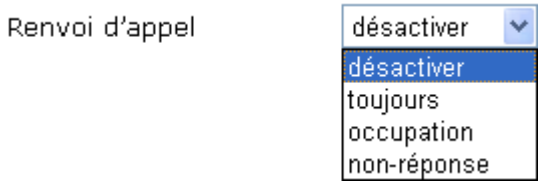


Appel au décroché — Cochez la case pour activer l'appel au décroché. Tapez dans le champ l'URL SIP à appeler automatiquement lorsque vous décrochez le téléphone.

Limite de durée de session — Cochez la case pour activer pour activer la fonction. En l'absence d'activité pendant la période spécifiée dans ce champ, la communication est coupée automatiquement.

Fonction fax T.38 — Si l'extrémité distante a également la fonction FAX, vous pouvez cocher cette case pour activer cette fonction.

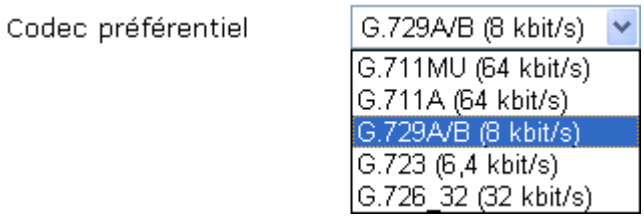
Renvoi d'appel — Il y a quatre options. **Désactiver :** désactive la fonction de renvoi d'appel. **Toujours :** tous les appels entrants sont renvoyés vers l'URL SIP. **Occupation :** les appels entrants sont renvoyés vers l'URL SIP uniquement lorsque le système local est occupé. **Non-réponse :** en l'absence de réponse, les appels entrants sont renvoyés vers l'URL SIP à l'expiration de la temporisation.



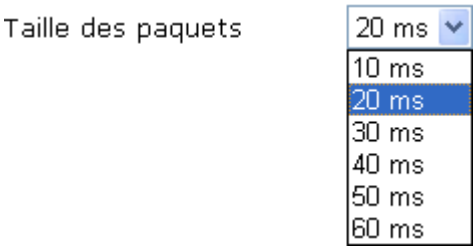
URL SIP – Tapez l'URL SIP (par exemple, aaa@draytel.org ou abc@iptel.org) vers laquelle les appels seront renvoyés.
Temporisation – Définissez la temporisation de renvoi d'appel. La valeur par défaut est 30 s.

Mode DND (ne pas — Permet de définir une période de repos téléphonique durant

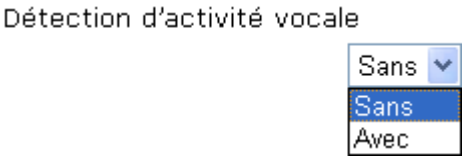
déranger)	laquelle l'appelant entend la tonalité d'occupation. L'utilisateur local n'est pas sonné.
Plages horaires (1-15)	Entrez des numéros de plage horaire pour activer le mode DND selon les plages horaires préconfigurées. Voir **Plages horaires**. **Répertoire téléphonique (1-60) –** Entrez des numéros de profil de répertoire téléphonique. Voir section **3.10.1 DialPlan – Répertoire téléphonique**.
Signal d'appel	Cochez la case pour activer cette fonction. Un signal est émis pour prévenir l'utilisateur de l'arrivée d'un nouvel appel. Utilisez la fonction « R » (flash) pour prendre l'appel en attente.
Transfert d'appel	Cochez la case pour activer cette fonction. Utilisez la fonction « R » (flash) pour appeler un autre interlocuteur. Lorsque la communication est établie, raccrochez. Les deux autres interlocuteurs sont en communication.
Codec préférentiel	Sélectionnez l'un des cinq codecs pour vos appels VoIP. Le codec utilisé pour chaque appel sera négocié avec l'homologue avant chaque session et peut donc ne pas être celui choisi par défaut. Le codec par défaut est G.729A/B ; il occupe peu de bande passante tout en maintenant une bonne qualité vocale. Si votre vitesse montante ne dépasse pas 64 kbit/s, n'utilisez pas le codec G.711. Pour utiliser celui-ci, il vaut mieux avoir au moins 256 kbit/s dans le sens montant.



Un seul codec – Si la case est cochée, seul le codec sélectionné sera utilisé.
Taille des paquets - La valeur par défaut est 20 ms, ce qui signifie que le paquet de données contient 20 ms d'informations vocale.



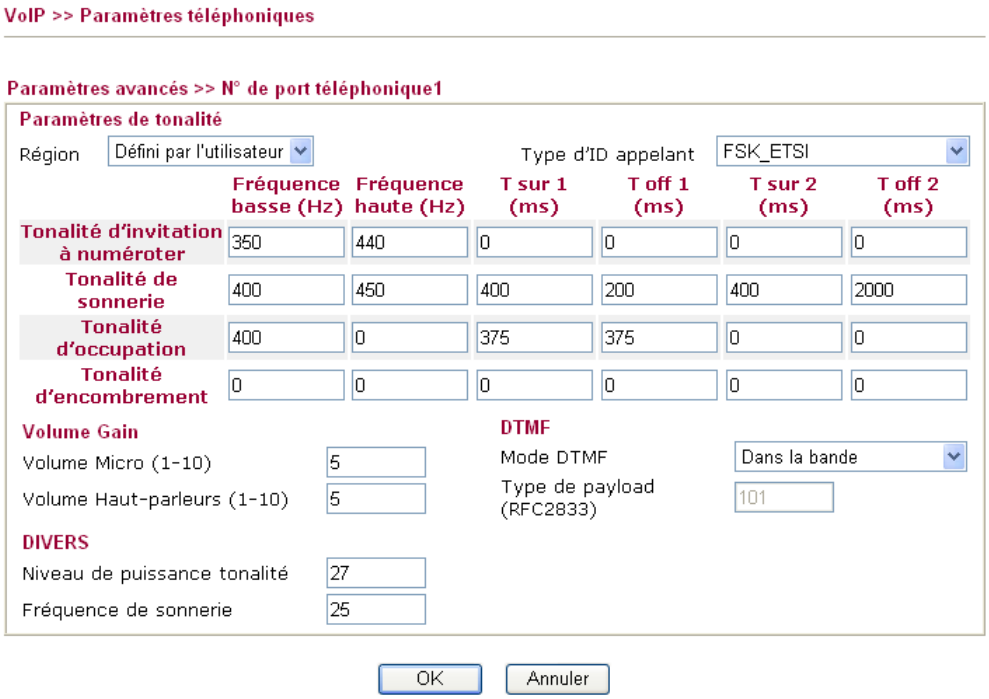
Détection d'activité vocale - Cette fonction détecte s'il y a une activité vocale des deux côtés. En l'absence d'activité vocale, le routeur fera en sorte d'affecter la bande passante à un autre usage. Cliquez sur Avec pour activer cette fonction ; cliquez sur Sans pour désactiver la fonction.



Compte SIP par défaut — Vous pouvez paramétrer jusqu'à six groupes de comptes SIP. Utilisez la liste déroulante pour choisir le nom de profil du compte par défaut.
Envoyer la tonalité uniquement quand le compte est enregistré - Cochez la case pour activer cette fonction.

Routage par défaut — Détermine le sens de routage des appels par défaut.
Vers RNIS (pour VoIP) – Le routeur est en mode RNIS. Pour passer en mode VoIP, il faudra composer le caractère qui se trouve dans ce champ. Ce caractère peut être *, #, ou un chiffre de 0 à 9.
Vers VoIP (pour RNIS) – Le routeur est en mode VoIP. Pour passer en mode RNIS, il faudra composer le caractère qui se trouve dans ce champ. Ce caractère peut être *, #, ou un chiffre de 0 à 9.

En outre, vous pouvez cliquer sur le bouton **Avancés** pour configurer les tonalités, le volume, le mode DTMF et plusieurs autres paramètres. Les paramètres **Avancés** ont pour but d'adapter le fonctionnement au lieu d'installation du routeur. Des tonalités incorrectes peuvent gêner les utilisateurs. Choisissez la région appropriée et le système trouvera automatiquement les tonalités préétablies qui conviennent et le type d'identification de l'appelant. Vous pouvez également régler manuellement les tonalités si vous choisissez Défini par l'utilisateur. TOn1, TOff1, TOn2 et TOff2 déterminent la cadence de la tonalité. TOn1 et TOn2 sont des laps de temps avec son, tandis que TOff1 et TOff2 sont des laps de temps sans son.



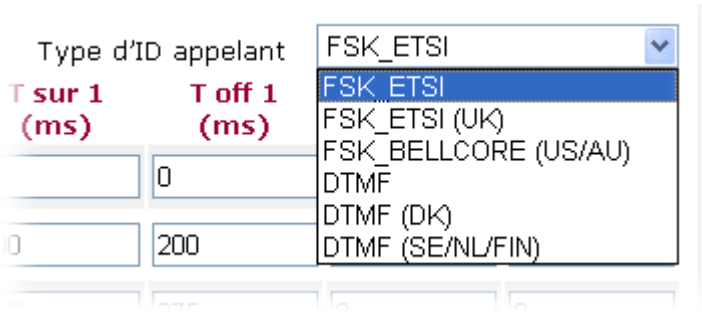
Région — Sélectionnez la région où vous vous trouvez. Les valeurs courantes du **type d'identification de l'appelant**, de la **tonalité d'invitation à numéroter**, du **signal de retour**

d’appel, du **signal d’occupation** et du **signal d’encombrement** sont affichées automatiquement sur la page. Si vous ne trouvez pas une région qui convient, choisissez **Défini par l’utilisateur** et spécifiez les valeurs des différents paramètres.

Vous pouvez aussi spécifiez chaque paramètre selon vos besoins. Il est recommandé d’utiliser les paramètres par défaut pour les communications VoIP.

Type d’identification de l’appelant

Il existe plusieurs normes pour l’affichage du numéro et/ou du nom de l’appelant sur l’écran du téléphone. Choisissez celle qui convient pour le lieu d’installation du routeur. Si vous ne savez quelle norme le téléphone prend en charge, utilisez la valeur par défaut.



Gain

Gain micro (1-10)/Gain haut-parleur (1-10) – Réglez le volume du microphone et du haut-parleur en tapant un nombre de 1 à 10. Plus le nombre est grand, plus le volume est fort.

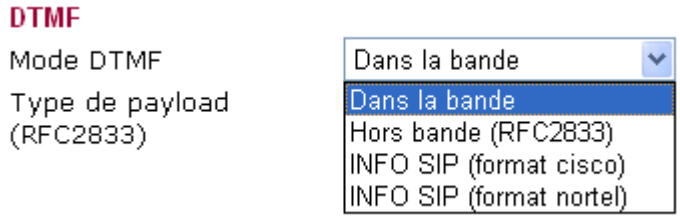
Divers

Puissance de tonalité – Ce paramètre règle l’intensité sonore de la tonalité. Plus le nombre est petit, plus le niveau sonore de la tonalité est élevé. Il est recommandé d’utiliser la valeur par défaut.
Fréquence de sonnerie – Ce paramètre détermine la fréquence du signal de sonnerie. Il est recommandé d’utiliser la valeur par défaut.

DTMF

Dans la bande – Si cette option est sélectionnée, le Vigor envoie directement les tonalités DTMF dans le flux téléphonique lorsque vous appuyez sur les touches du clavier

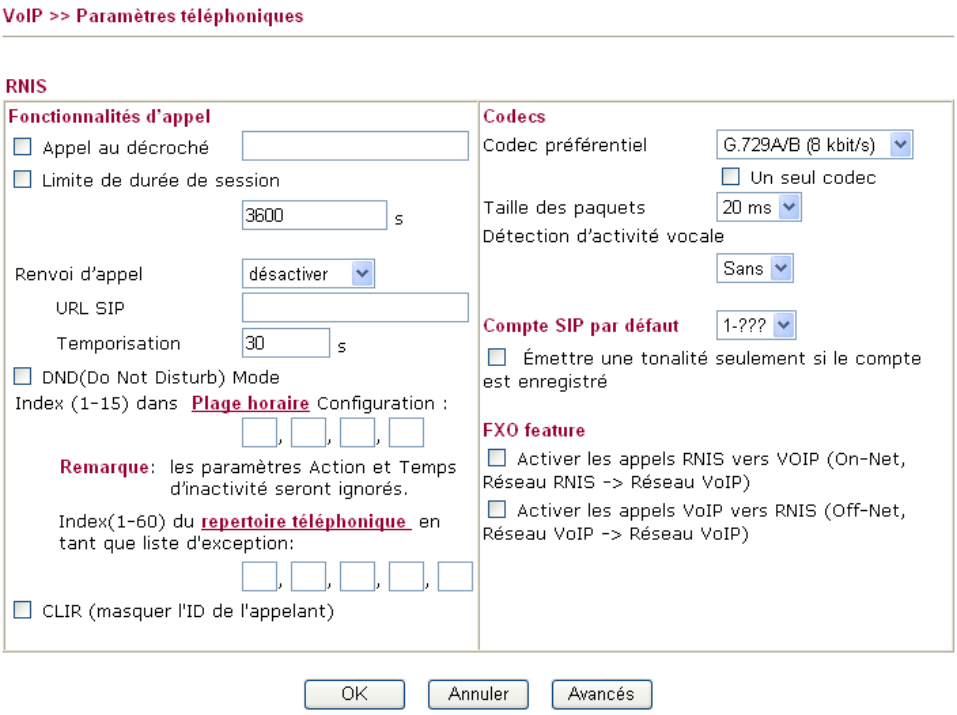
du téléphone.
Hors bande – Si cette option est sélectionnée, le Vigor capture le numéro composé au clavier, le numérise et l'envoie de l'autre côté. Le récepteur produit la tonalité à partir des données numériques qu'il reçoit. Cette fonction est très utile en cas d'encombrement du réseau pour maintenir l'exactitude des tonalités DTMF.
Info SIP – Choisissez cette option pour que le Vigor capture les tonalités DTMF et les envoie à l'extrémité distante avec un message SIP.



Type de charge utile (rfc2833) Choisissez un nombre de 96 à 127 (la valeur par défaut est 101). Ce paramètre est disponible pour le mode hors bande (RFC2833).

Paramètres pour le RNIS (modèle *VGi* seulement)

Cliquez sur le numéro **3** sous Index pour accéder à la page de paramétrage suivante :

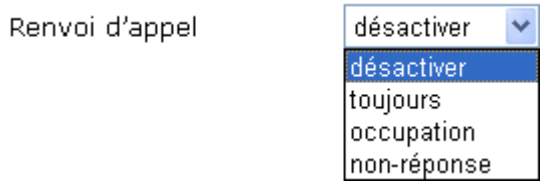


Appel au décroché Cochez la case pour activer l'appel au décroché. Tapez dans le champ l'URL SIP à appeler automatiquement lorsque vous décrochez le téléphone.

Limite de durée de session Cochez la case pour activer pour activer la fonction. En l'absence d'activité pendant la période spécifiée dans ce champ, la communication est coupée automatiquement.

Renvoi d'appel

Il y a quatre options. **Désactiver :** désactive la fonction de renvoi d'appel. **Toujours :** tous les appels entrants sont renvoyés vers l'URL SIP. **Occupation :** les appels entrants sont renvoyés vers l'URL SIP uniquement lorsque le système local est occupé. **Non-réponse :** en l'absence de réponse, les appels entrants sont renvoyés vers l'URL SIP à l'expiration de la temporisation.



URL SIP – Tapez l'URL SIP (par exemple, aaa@draytel.org ou abc@iptel.org) vers laquelle les appels seront renvoyés.
Temporisation – Définissez la temporisation de renvoi d'appel. La valeur par défaut est 30 s.

Mode DND (ne pas déranger)

Permet de définir une période de repos téléphonique durant laquelle l'appelant entend la tonalité d'occupation. L'utilisateur local n'est pas sonné.

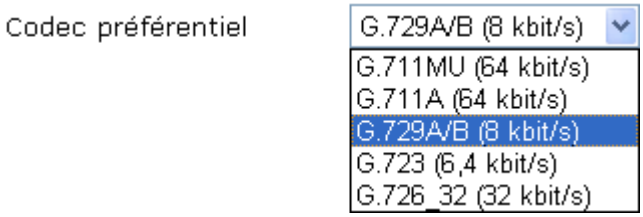
Plages horaires (1-15) - Entrez des numéros de plage horaire pour activer le mode DND selon les plages horaires préconfigurées. Voir **Plages horaires**.
Répertoire téléphonique (1-60) – Entrez des numéros de profil de répertoire téléphonique. Voir section **3.10.1 DialPlan – Répertoire téléphonique**.

CLIR (masquer le numéro appelant)

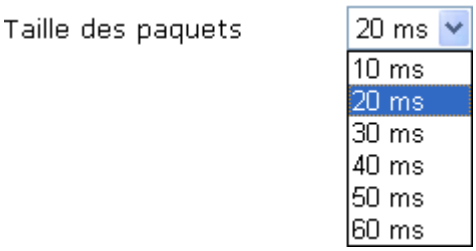
Cochez cette case pour que l'identification de l'appelant ne s'affiche pas sur l'écran du téléphone.

Codec préférentiel

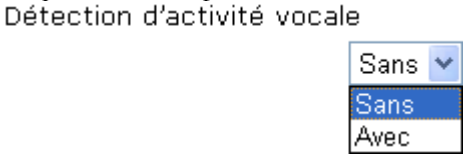
Sélectionnez l'un des cinq codecs pour vos appels VoIP. Le codec utilisé pour chaque appel sera négocié avec l'homologue avant chaque session et peut donc ne pas être celui choisi par défaut. Le codec par défaut est G.729A/B ; il occupe peu de bande passante tout en maintenant une bonne qualité vocale.
Si votre vitesse montante ne dépasse pas 64 kbit/s, n'utilisez pas le codec G.711. Pour utiliser celui-ci, il vaut mieux avoir au moins 256 kbit/s dans le sens montant.



Un seul codec – Si la case est cochée, seul le codec sélectionné sera utilisé.
Taille des paquets - La valeur par défaut est 20 ms, ce qui signifie que le paquet de données contient 20 ms d'informations vocale.

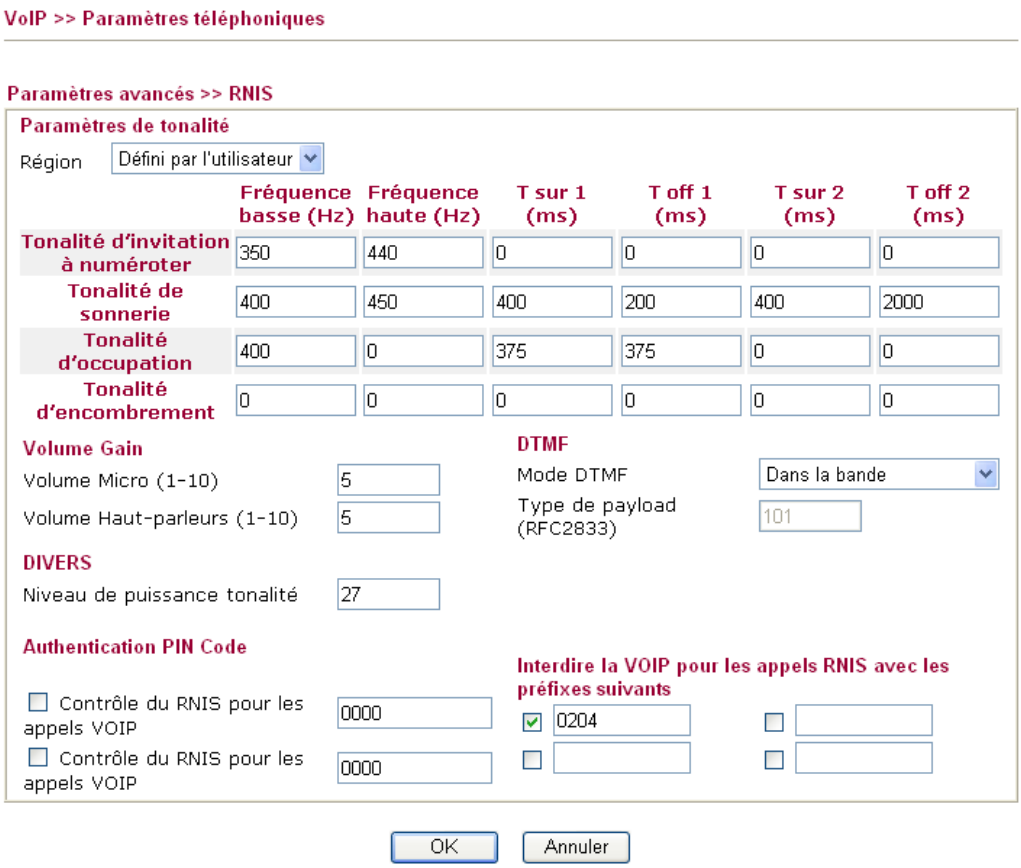


Détection d'activité vocale - Cette fonction détecte s'il y a une activité vocale des deux côtés. En l'absence d'activité vocale, le routeur fera en sorte d'affecter la bande passante à un autre usage. Cliquez sur Avec pour activer cette fonction ; cliquez sur Sans pour désactiver la fonction.



Compte SIP par défaut	Vous pouvez paramétrer jusqu'à six groupes de comptes SIP. Utilisez la liste déroulante pour choisir le nom de profil du compte par défaut.
Envoyer la tonalité uniquement quand le compte est enregistré	Cochez la case pour activer cette fonction.
Fonctions FXO	**Appels RNIS par VoIP (sur réseau)** – Cochez cette case pour que tous les appels sortants RNIS soient acheminés jusqu'à leur destination par l'internet. **Appels VoIP par RNIS (hors réseau)** – Cochez cette case pour que tous les appels entrants venant de l'internet soient acheminés jusqu'à leur destination par ligne RNIS.

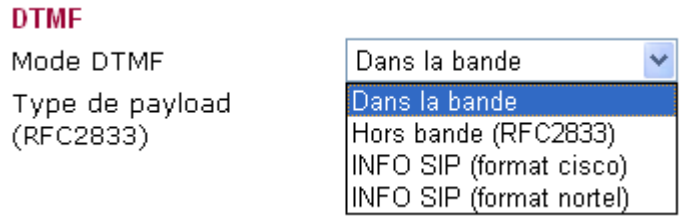
En outre, vous pouvez cliquer sur le bouton **Avancés** pour configurer les tonalités, le volume, le mode DTMF et plusieurs autres paramètres. Les paramètres **Avancés** ont pour but d'adapter le fonctionnement au lieu d'installation du routeur. Des tonalités incorrectes peuvent gêner les utilisateurs. Choisissez la région appropriée et le système trouvera automatiquement les tonalités préétablies qui conviennent et le type d'identification de l'appelant. Vous pouvez également régler manuellement les tonalités si vous choisissez Défini par l'utilisateur. TOn1, TOff1, TOn2 et TOff2 déterminent la cadence de la tonalité. TOn1 et TOn2 sont des laps de temps avec son, tandis que TOff1 et TOff2 sont des laps de temps sans son.



Région

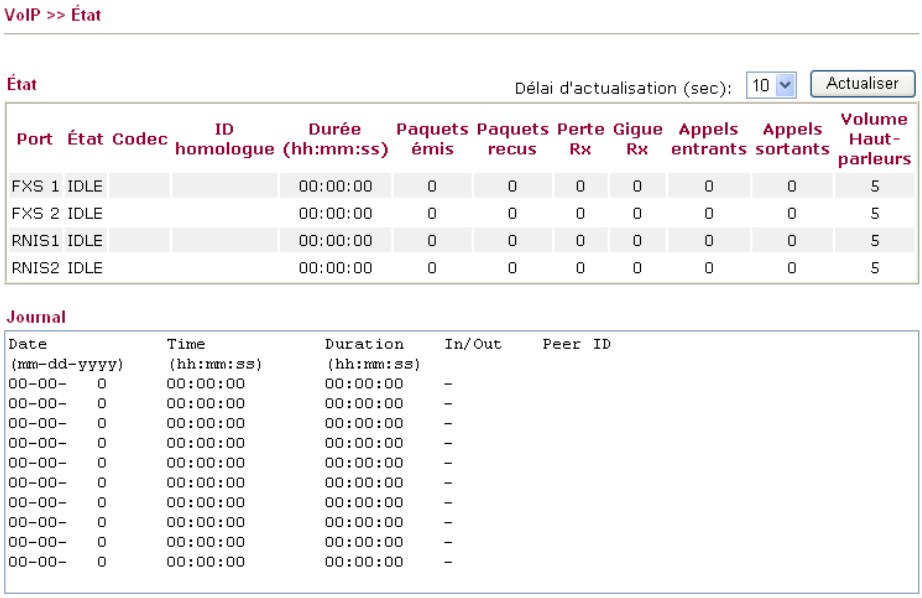
Sélectionnez la région où vous vous trouvez. Les valeurs courantes du **type d'identification de l'appelant**, de la **tonalité d'invitation à numéroter**, du **signal de retour d'appel**, du **signal d'occupation** et du **signal d'encombrement** sont affichées automatiquement sur la page. Si vous ne trouvez pas une région qui convient, choisissez **Défini par l'utilisateur** et spécifiez les valeurs des différents paramètres.

Vous pouvez aussi spécifiez chaque paramètre selon vos besoins. Il est recommandé d'utiliser les paramètres par défaut pour les communications VoIP.

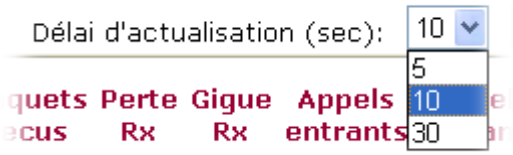
Gain	**Gain micro (1-10)/Gain haut-parleur (1-10)** – Régler le volume du microphone et du haut-parleur en tapant un nombre de 1 à 10. Plus le nombre est grand, plus le volume est fort.
Divers	**Puissance tonalité** – Ce paramètre règle l'intensité sonore de la tonalité. Plus le nombre est petit, plus le niveau sonore de la tonalité est élevé. Il est recommandé d'utiliser la valeur par défaut.
Code confidentiel d'authentification	**Vérifiez pour les appels RNIS -> VoIP** – Code confidentiel qui servira au routeur à identifier qui est autoriser à faire des appels RNIS -> VoIP. Tapez un code de trois à huit chiffres. **Vérifiez pour les appels VoIP -> RNIS** - Code confidentiel qui servira au routeur à identifier qui est autoriser à faire des appels VoIP -> RNIS. Tapez un code de trois à huit chiffres.
DTMF	**Mode DTMF** : **Dans la bande –** Si cette option est sélectionnée, le Vigor envoie directement les tonalités DTMF dans le flux téléphonique lorsque vous appuyez sur les touches du clavier du téléphone. **Hors bande –** Si cette option est sélectionnée, le Vigor capture le numéro composé au clavier, le numérise et l'envoie de l'autre côté. Le récepteur produit la tonalité à partir des données numérique qu'il reçoit. Cette fonction est très utile en cas d'encombrement du réseau pour maintenir l'exactitude des tonalités DTMF. **Info SIP** – Choisissez juste cette option pour que le Vigor capture les tonalités DTMF et les envoie à l'extrémité distante avec un message SIP.  **Type de charge utile (rfc2833) –** Choisissez un nombre de 96 à 127 (la valeur par défaut est 101). Ce paramètre est disponible pour le mode hors bande (RFC2833).
Interdire les appels VoIP -> RNIS avec les préfixes suivants	Définissez un préfixe de numéro de téléphone interdisant les appels VoIP -> RNIS à partir des numéros commençant par ce préfixe. Si un utilisateur force le numéro, le routeur le coupe automatiquement. Vous pouvez tapez dans ce champ un nombre de un à onze chiffres (de 0 à 9).

3.10.4 État

La fonction État de l'appel téléphonique vous permet de visualiser des informations d'état relatives notamment au codec et à la connexion pour les ports VoIP 1 et VoIP 2.



Intervalle d'actualisation Spécifiez l'intervalle d'actualisation. Les informations sont mises à jour immédiatement lorsque vous cliquez sur le bouton **Actualiser.**



Port VoIP1, VoIP2, RNIS1 et RNIS2. Les ports RNIS1/2 n'apparaissent que si le routeur a une interface RNIS. RNIS1 correspond au canal B1 du port RNIS physique ; RNIS2 correspond au canal B2 du port RNIS physique. Les ports RNIS1/2 sont disponibles pour les utilisateurs européens du Vigor 2910VGi. Dans le cas des autres modèles Vigor 2910V, seul l'état des ports VoIP1 et VoIP2 est affiché dans cette page.

État Pour visualiser l'état de la connexion VoIP
IDLE - Indique que la fonction VoIP est active.
HANG_UP - Indique que la connexion n'est pas établie (tonalité d'occupation).
CONNECTING - Indique que l'utilisateur appelle.
WAIT_ANS - Indique qu'une connexion est établie et qu'une réponse de l'utilisateur distant est attendue.
ALERTING - Indique qu'un appel arrive.
ACTIVE - Indique que la connexion VoIP est activée.

Codec Indique que le codec vocal utilisé par le canal actuel.

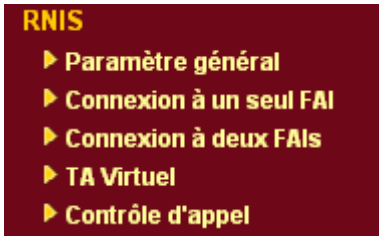
ID homologue L'ID homologue entrant ou sortant (le format peut être IP ou Domaine).

Temps de connexion	Le temps est exprimé en secondes.
Paquets émis	Nombre total de paquets téléphoniques émis pendant la communication.
Paquets reçus	Nombre total de paquets reçus pendant la communication téléphonique.
Perte Rx	Nombre total de paquet perdus pendant la communication.
Gigue Rx	Gigue des paquets téléphoniques reçus.
Appels entrants	Durée cumulée des appels entrants.
Appels Sortants	Durée cumulée des appels sortants.
Gain	Volume de l'appel actuel.
Journal	Journal des communications VoIP.

3.11 RNIS

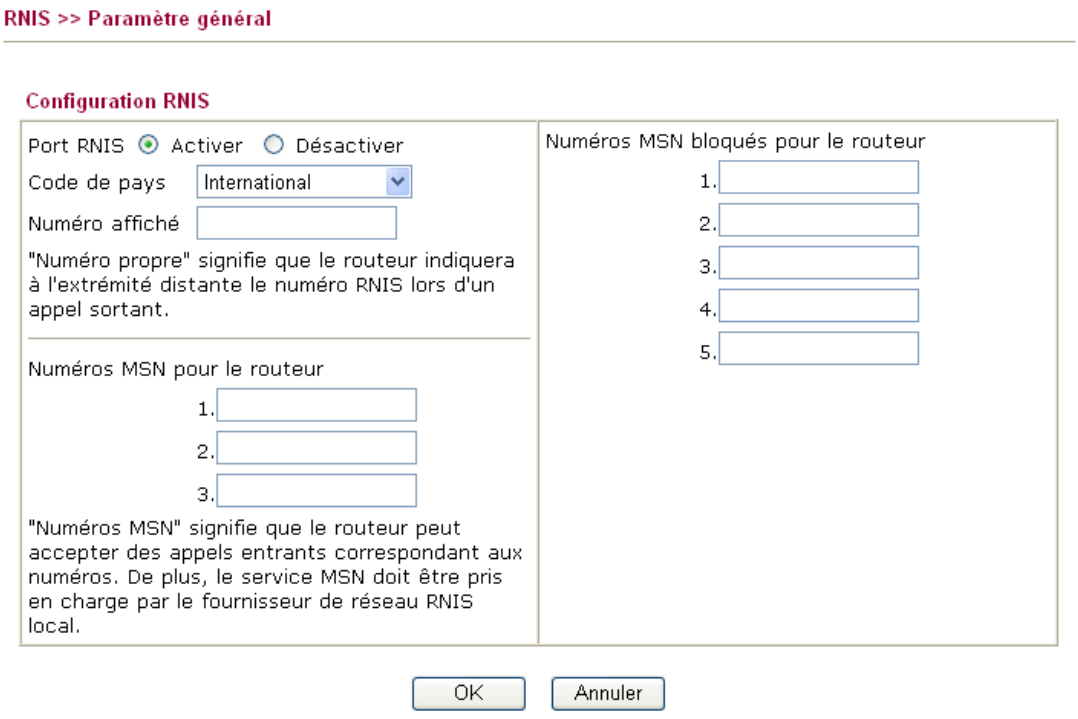
Les pages web RNIS ne sont disponibles que pour les routeurs Vigor 2910i/2910VGi. Si vous utilisez un autre modèle, sautez cette section.

Les options du menu RNIS des modèles ***i*** sont les suivantes :



3.11.1 Configuration générale

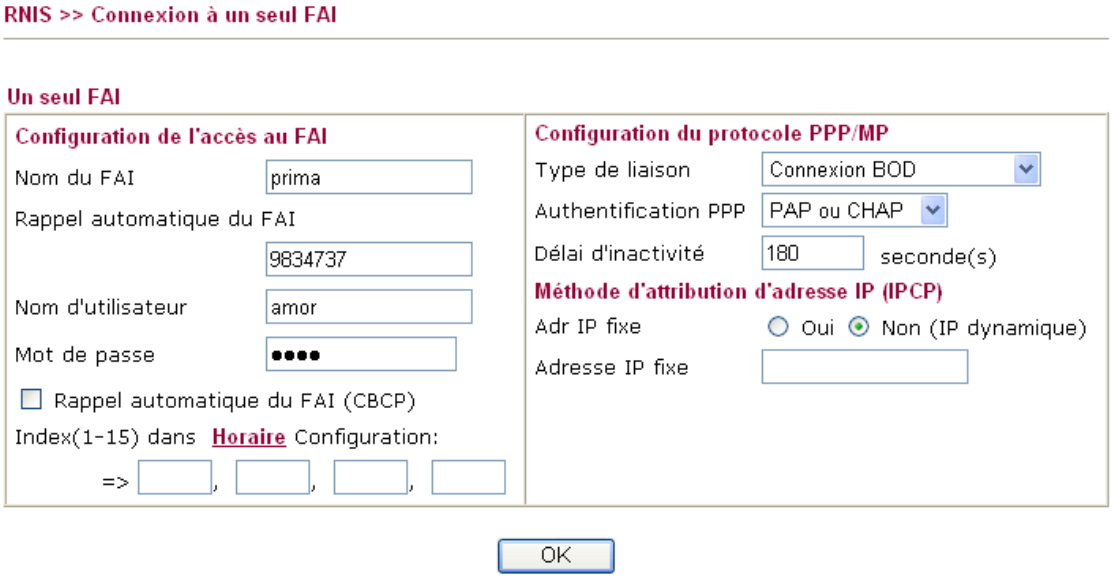
Cette page comporte certains paramètres RNIS de base et permet notamment d'activer ou non le port RNIS ou de spécifier des numéros MSN ou des numéros MSN bloqués.



Port RNIS	Cliquez sur **Activer** pour ouvrir le port RNIS et sur **Désactiver** pour le fermer.
Code du pays	Pour que le routeur fonctionne correctement sur votre réseau RNIS local, vous devez choisir le bon code de pays.
Numéro propre	Tapez votre numéro RNIS. À chaque appel sortant, le numéro sera envoyé au destinataire.
Numéros MSN pour le routeur	Le routeur accepte uniquement les appels entrants dont le numéro concorde. De plus, les services MSN doivent être pris en charge par le fournisseur local de réseau RNIS. Le routeur permet de spécifier trois numéros MSN. À noter que les services MSN doivent être fournis par vos opérateurs de télécommunications locaux. Par défaut, la fonction MSN est désactivée. Si vous laissez les champs vides, tous les appels entrants seront acceptés.
Numéros MSN bloqués pour le routeur	Tapez les numéros MSN dans les champs pour empêcher le routeur d'appeler ces numéros.

3.11.2 Connexion à un seul FAI

Si vous accédez à l'internet par l'intermédiaire d'un seul FAI, cliquez sur ce lien.

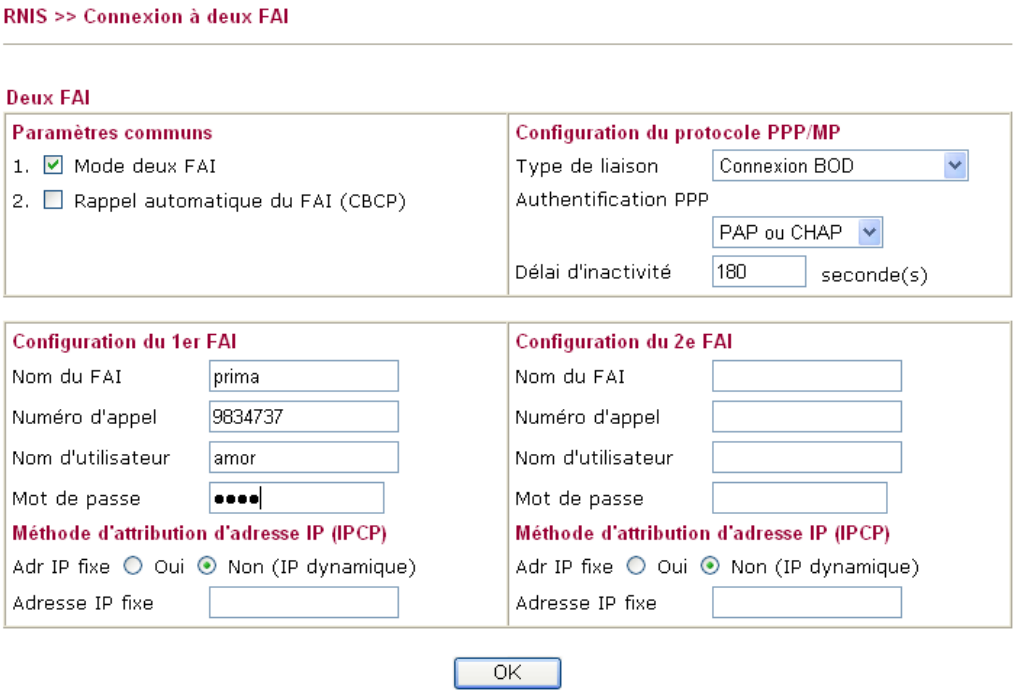


Nom du FAI	Tapez le nom de votre FAI.
Numéro d'appel	Tapez le numéro d'accès RNIS fourni par votre FAI.
Nom d'utilisateur	Tapez le nom d'utilisateur fourni par votre FAI.
Mot de passe	Tapez le mot de passe fourni par votre FAI.
Demander le rappel automatique (CBCP)	Si votre FAI prend en charge la fonction de rappel automatique, cochez cette case pour activer le protocole CBCP pendant la négociation PPP.
Plages horaires (1-15)	Entrez le numéro d'index des plages horaires pour contrôler l'accès à l'internet selon les plages horaires préconfigurées.
Type de liaison	Il y a quatre options : désactivation de la liaison, connexion à 64 kbit/s, connexion à 128 kbit/s et connexion BOD.

	Désactivation de la liaison : désactivation de la connexion RNIS. **Connexion à 64 kbit/s :** utilisation d'un canal B RNIS pour l'accès à l'internet. **Connexion à 128 kbit/s :** utilisation des deux canaux B RNIS pour l'accès à l'internet. **Connexion BOD :** BOD signifie « bandwidth-on-demand » (bande passante à la demande). Le routeur utilise uniquement un canal B lorsque le trafic est faible. Lorsque le canal B arrive à saturation, l'autre canal B est activé automatiquement. Pour plus de détails sur le paramétrage BOD, se reporter à **Configuration avancée** > Paramétrage du **contrôle d'appel et PPP/MP**.
Authentification PPP	**PAP seulement :** configuration de la session PPP pour l'utilisation du protocole PAP pour la négociation du nom d'utilisateur et du mot de passe avec le FAI. **PAP ou CHAP :** configuration de la session PPP pour l'utilisation des protocoles PAP ou CHAP pour négocier le nom d'utilisateur et le mot de passe avec le FAI.
Délai d'inactivité	Le routeur se déconnecte au bout d'un certain temps d'inactivité. La valeur par défaut est 180 secondes. Si vous spécifiez 0, la connexion RNIS au FAI est permanente.
IP fixe	Dans la plupart des environnements, vous ne devriez pas avoir à modifier ces paramètres car la plupart des FAI fournissent une adresse IP dynamique au routeur lorsqu'il se connecte. Si votre FAI fournit une adresse IP fixe, cliquez sur **Oui** pour activer cette fonction et tapez l'adresse IP dans le champ **Adresse IP fixe**.
Adresse IP fixe	Tapez l'adresse IP.

3.11.3 Connexion à deux FAI

Si vous avez deux FAI, cliquez sur Connexion à deux FAI pour configurer deux profils de connexion. Vous pourrez vous connecter simultanément aux deux FAI. Cette fonction est utilisée principalement pour les FAI qui ne prennent pas en charge le protocole PPP multilien (ML-PPP). Dans un tel cas, la connexion à deux FAI peut porter le débit des canaux RNIS à 128 kbit/s.

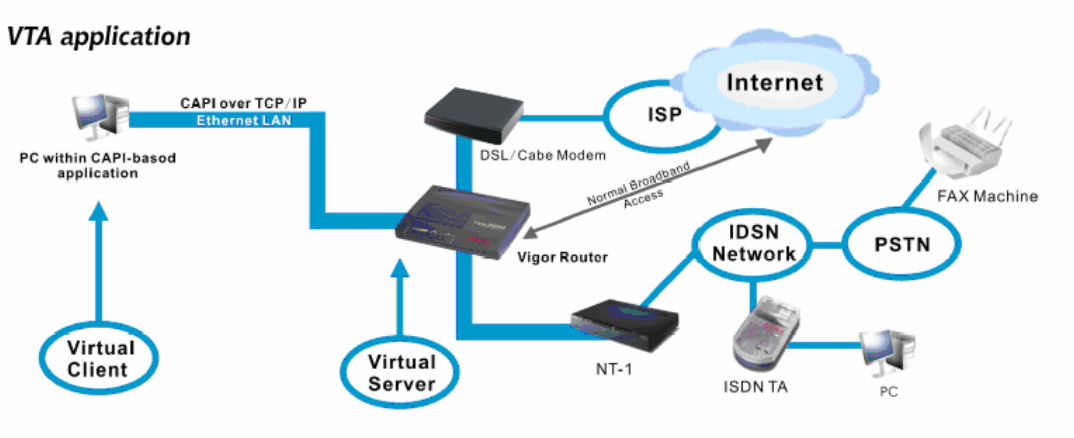


La plupart des paramètres configuration sont les mêmes que ceux de la connexion à un seul FAI. Il y a en plus une case à cocher pour activer la fonction de connexion à deux FAI et une fenêtre de configuration de l'accès au deuxième FAI. Cochez la case correspondante et entrez les informations concernant l'accès au deuxième FAI. Reportez-vous à la description de la connexion à un seul FAI.

3.11.4 TA virtuel (CAPI distant)

Les hôtes ou PC locaux du réseau qui utilisent un logiciel CAPI courant, comme RVS-COM ou BVRP, pour accéder au routeur, peuvent fonctionner comme des TA RNIS locaux pour envoyer ou recevoir des télécopies sur la ligne RNIS. C'est essentiellement un modèle de réseau client-serveur. Le serveur TA virtuel intégré gère l'établissement et la libération des connexions. Le client TA virtuel, installé sur les hôtes ou PC locaux, crée un pilote CAPI pour relayer les messages CAPI entre les applications et le module CAPI du routeur. Avant de passer à la configuration du **TA virtuel**, notez les limites suivantes :

- Le client TA virtuel n'est utilisable qu'avec les plates-formes MicrosoftTM Windows 95 OSR2.1/98/98SE/Me/2000.
- Le client TA virtuel n'est utilisable qu'avec le protocole CAPI 2.0 et n'a pas de moteur fax intégré.
- Une interface au débit de base RNIS comporte deux canaux B. Le nombre maximal de clients actifs est également de 2.
- Avant de configurer le TA virtuel, vous devez spécifier le bon code de pays dans les Paramètres RNIS.



VTA application	*Application de TA virtuel*
CAPI over TCP/IP	*CAPI sur TCP/IP*
PC within CAPI-based application	*PC de l'application CAPI*
Virtual Client	*Client virtuel*
Virtual Server	*Serveur virtuel*
Vigor Router	*Routeur Vigor*
DSL/Cable Modem	*Modem DSL/câble*
ISP	*FAI*
FAX Machine	*Télécopieur*
PSTN	*RTPC*
ISDN Network	*Réseau RNIS*
ISDN TA	*TA RNIS*

Comme le montre le scénario d'application ci-dessus, le client TA virtuel peut appeler un télécopieur, un TA RNIS, etc. ou recevoir un appel.

Avant de configurer le TA virtuel (CAPI distant), installez le client TA virtuel. Pour cela, mettez en place le CD fourni avec votre routeur Vigor ou bien double-cliquez directement sur l'un des fichiers d'installation : **Vsetup95.exe** pour Windows 95 OSR2.1 et version suivantes, **Vsetup98.exe** pour Windows 98, 98SE et Me et **Vsetup2k.exe** pour Windows 2000. Suivez les instructions qui s'affichent. À la fin, vous êtes invité à redémarrer votre ordinateur. Cliquez sur **OK** pour redémarrer votre ordinateur.

Après le redémarrage de l'ordinateur, il y a une icône VT dans la barre des tâches (généralement en bas à droite de l'écran, près de l'horloge).

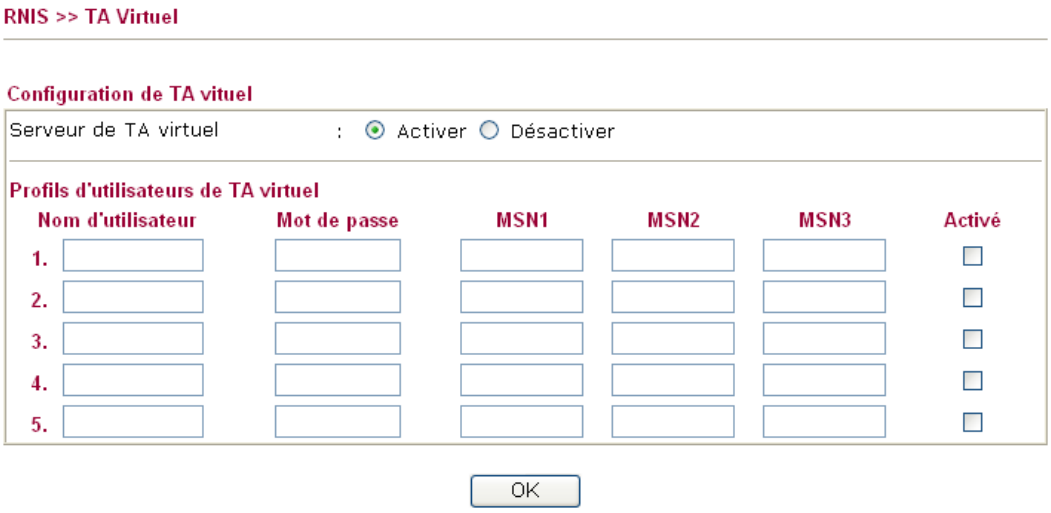
Si le texte de l'icône est VERT, le client TA virtuel est connecté au serveur TA virtuel et vous pouvez lancer votre logiciel CAPI et utilisez le client pour accéder au routeur. Lisez le guide d'utilisation du logiciel pour procéder à la configuration détaillée. Si le texte de l'icône est ROUGE, c'est que le client n'est pas connecté au serveur. Dans ce cas, vérifiez la connexion Ethernet physique.

Cliquez sur le lien **Configuration de TA virtuel (CAPI distant)** du groupe **Installation rapide** pour configurer le TA virtuel.

Comme l'application de TA virtuel est un modèle de réseau client-serveur, vous devez la configurer aux deux extrémités pour que votre application de TA virtuel fonctionne correctement.

Par défaut, le serveur TA virtuel est activé et les champs nom d'utilisateur/mot de passe sont vides. N'importe quel client TA virtuel peut se connecter au serveur. Une fois qu'un champ

nom d'utilisateur/mot de passe a été rempli, le serveur TA virtuel autorise uniquement les clients dont le nom d'utilisateur/mot de passe est correct à se connecter. L'écran de configuration du TA virtuel est présenté ci-dessous.



Serveur TA virtuel	**Activer :** Cliquez pour activer le serveur. **Désactiver :** Cliquez pour désactiver le serveur. Toutes les applications de TA virtuel se termineront.
Nom d'utilisateur	Tapez le nom d'utilisateur d'un client spécifique.
Mot de passe	Tapez le mot de passe d'un client spécifique.
MSN1/ MSN2/MSN3	MSN est l'abréviation de Multiple Subscriber Number. Cela signifie que vous pouvez disposer de plusieurs numéros RNIS sur une seule ligne d'abonné. Ce service est fourni par votre opérateur de télécommunications. Spécifiez les numéros MSN pour un client spécifique. Si vous n'avez pas de service MSN, laissez ce champ vide.
Active	Cliquez pour permettre au client d'accéder au serveur.

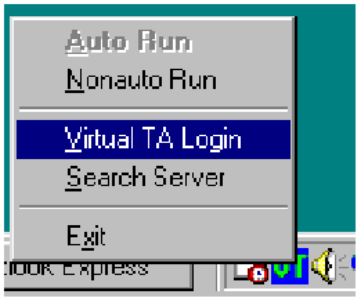
Profil d'utilisateur

À noter que la création d'un unique compte d'accès limitera l'accès au serveur TA virtuel au détenteur du compte spécifié.

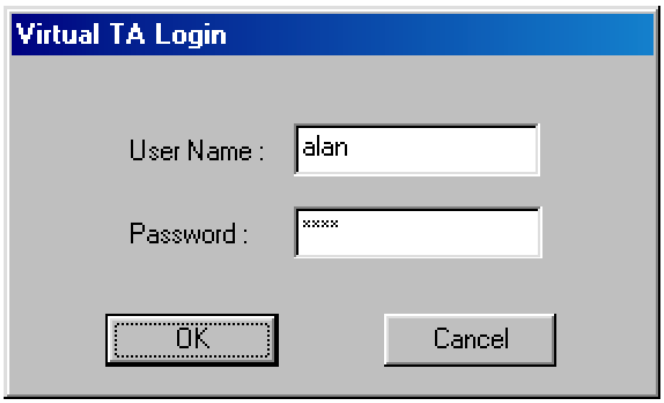
Dans l'exemple ci-dessous, nous supposons que vous n'avez pas obtenu le service MSN de votre fournisseur de réseau RNIS.

Sur le serveur – Cliquez sur **Configuration de TA virtuel (CAPI distant)** et remplissez les champs Nom d'utilisateur et Mot de passe. Cochez la case **Active** pour activer le compte.

Sur le client - faites un clic droit sur l'icône VT. Le menu suivant apparaît.



Cliquez sur **Virtual TA Login** pour lancer la boîte de connexion.



Tapez le Nom d'utilisateur et le Mot de passe, puis cliquez sur **OK**. Peu de temps après, le texte de l'icône VT devient vert.

Configuration de numéro MSN

Si vous avez demandé un service MSN, le serveur TA virtuel peut déterminer quel client a le numéro MSN spécifié. À l'arrivée d'un appel, le serveur informe le client approprié. Voici un exemple de configuration de numéro MSN.

Supposons que vous vouliez attribuer le numéro MSN **123** au client « alan ».

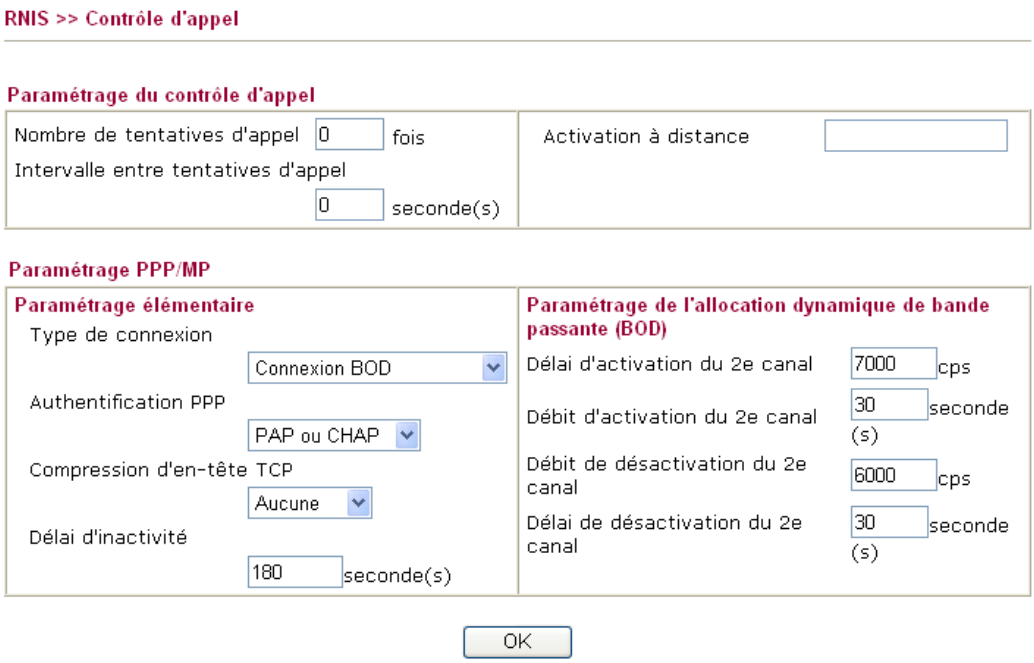
Tapez le numéro MSN dans le logiciel CAPI. Lorsque le serveur TA virtuel envoie un avis au client TA virtuel spécifié, le logiciel CAPI le reçoit également et n'accepte pas l'appel entrant.

3.11.5 Contrôle d'appel

Certaines applications demandent que le routeur (seulement pour les modèles *i*) puisse être activé à distance ou puisse se connecter au FAI via l'interface RNIS. Les routeurs Vigor fournissent cette fonctionnalité qui vous permet d'appeler le routeur et de lui demander d'appeler le FAI.

> **Nota :** le contrôle d'appel n'est disponible que pour les modèles *i* dotés de l'interface RNIS.

Avant de configurer cette page web, sélectionnez d'abord **Connexion à un seul FAI**.



Nombre de tentatives d'appel

C'est le nombre de tentatives d'appel par paquet déclenché. Un paquet déclenché est le paquet dont la destination est extérieure au réseau local. Par défaut, il n'est pas effectué de nouvelle tentative d'appel. Si la valeur 5 est spécifiée, pour chaque paquet déclenché, le routeur appelle 5 fois jusqu'à ce qu'il soit connecté au FAI ou au routeur d'accès à distance.

Intervalle entre tentatives d'appel

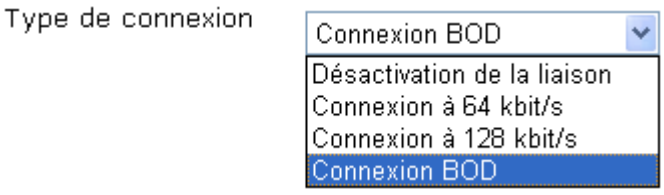
Intervalle entre tentatives d'appel. Par défaut, l'intervalle est de 0 seconde.

Activation à distance

Un numéro de téléphone est tapé dans le champ Activation à distance pour activer la fonction d'activation à distance. Si le routeur accepte un appel du numéro 12345678, il met fin immédiatement à l'appel entrant et appelle le FAI.

Type de liaison

Comme le RNIS comporte deux canaux B (64 kbit/s par canal), vous pouvez spécifier si vous voulez utiliser un canal B, deux canaux B ou la bande passante à la demande (BOD). Il y a quatre options : désactivation de la liaison, connexion à 64 kbit/s, connexion à 128 kbit/s, connexion BOD.

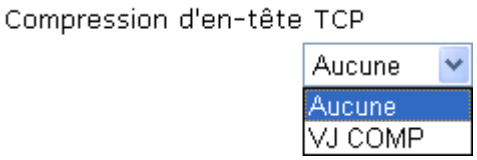


Authentification PPP

Spécifiez la méthode d'authentification PPP pour les connexions PPP/MP. PAP/CHAP assure une meilleure compatibilité.

Compression de l'en-tête TCP

Compression VJ : utilisée pour la compression de l'en-tête TCP/IP. Sélectionnez Oui pour améliorer l'utilisation de la bande passante.



Délai d'inactivité	Comme notre liaison RNIS est du type « Appel à la demande », la connexion n'est déclenchée que lorsqu'elle est nécessaire.
Délai d'activation du 2e canal et débit d'activation du 2e canal	BOD signifie « bandwith-on-demand » - (bande passante à la demande). Les paramètres **Débit d'activation du deuxième canal/Délai d'activation du deuxième canal/Débit de désactivation du deuxième canal/Délai de désactivation du deuxième canal** ne sont pris en compte que si vous avez choisi **Connexion BOD** comme type de liaison. Le RNIS utilise généralement un canal B pour accéder à l'internet ou au réseau distant lorsque vous choisissez Connexion BOD comme type de liaison. Le routeur utilise les paramètres suivants pour décider de l'activation ou de la désactivation du canal B supplémentaire. À noter que le paramètre **cps** (caractères par seconde) mesure l'utilisation globale de la liaison. Ces paramètres précisent les conditions d'activation du 2e canal. Si le temps d'utilisation du 1e canal dépasse le débit d'activation du 2e canal pendant un temps supérieur au délai d'activation du 2e canal, le 2e canal est activé. Le débit total de la liaison est alors de 128 kbit/s (deux canaux B).
Débit de désactivation du 2e canal et délai d'activation du 2e canal	Ces paramètres précisent les conditions de désactivation du 2e canal. Si le taux d'utilisation des deux canaux B est inférieur au débit de désactivation du 2e canal, et ce, pendant un temps supérieur au délai de désactivation du 2e canal, le 2e canal est désactivé. Par suite, le débit total de la liaison est de 64 kbit/s (un canal B).

Nota : si vous n'êtes pas certain que votre FAI prenne en charge les fonctions BOD et/ou ML-PPP, adressez-vous à votre FAI, à votre revendeur ou contactez notre site : **support@draytek.com**.

3.12 LAN sans fil

Cette fonction ne concerne que les modèles G.

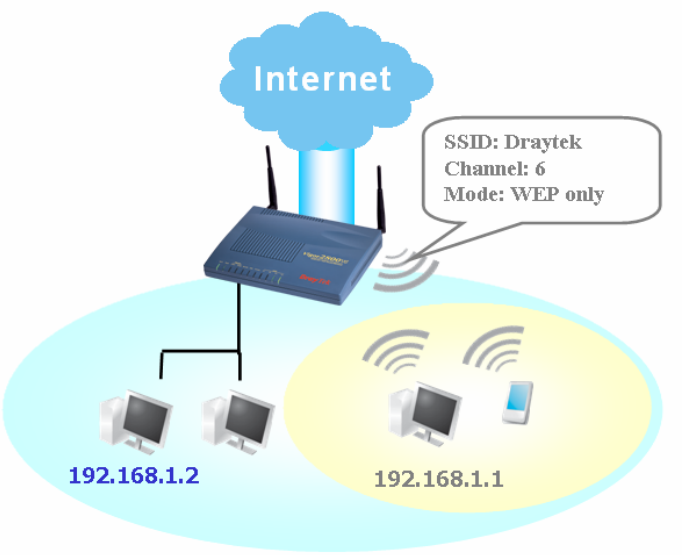
3.12.1 Principe de base

Ces dernières années, le marché des télécommunications sans fil a connu un essor extraordinaire. La technologie sans fil permet actuellement de joindre pratiquement n'importe quel point du globe terrestre. Des centaines de millions de personnes échangent des informations à l'aide de produits de télécommunication sans fil. Le modèle Vigor G, le routeur sans fil Vigor, est conçu pour maximiser la souplesse et l'efficacité des communications pour les professions indépendantes et les particuliers. N'importe quelle personne autorisée peut amener un PDA ou un ordinateur bloc-notes sans fil dans une salle de conférence sans avoir à poser un câble réseau ou à percer des trous. Le LAN sans fil procure une haute mobilité aux utilisateurs, leur permettant d'accéder simultanément à toutes les fonctionnalités du LAN et à l'internet.

Les routeurs sans fil Vigor sont dotés d'une interface LAN sans fil conforme au protocole IEEE 802.11g. Pour améliorer encore les performances, le routeur Vigor est également doté de la technologie sans fil évoluée Super G™ qui permet d'atteindre 108 Mbit/s*. Vous pouvez enfin profiter de la musique et de la vidéo en flux.

> Nota : * Le débit effectif varie selon divers facteurs, notamment le volume de trafic sur le réseau, la bande passante consommée hors charge utile et les matériaux de construction des bâtiments.

En mode infrastructure, le routeur sans fil Vigor sert de point d'accès (AP) en se connectant à de nombreux clients sans fil ou stations (STA). Toutes les stations partagent la même connexion à internet avec d'autres hôtes filaires par l'intermédiaire du routeur sans fil Vigor. Les **Paramètres généraux** définissent notamment le SSID du réseau sans fil, le canal radio du routeur, etc.



SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WEP only	*Mode : WEP seulement*

Généralités sur la sécurité

Cryptage matériel en temps réel : Le routeur Vigor est doté d'un moteur de cryptage AES matériel qui assure le plus haut degré de protection.

Choix complet de normes de sécurisation : Pour assurer la sécurité et la confidentialité de vos communications sans fil, nous fournissons plusieurs normes qui ont la faveur du marché.

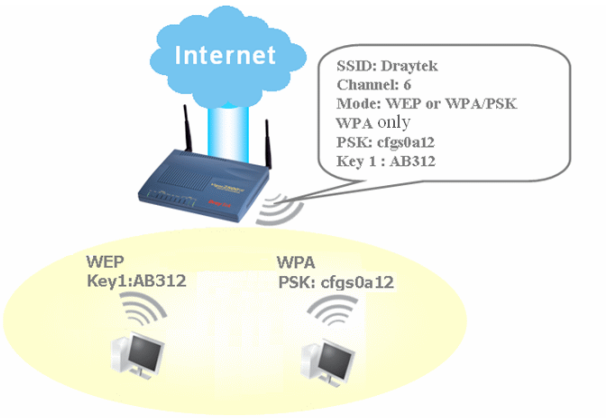
Le cryptage WEP (Wireless Equivalent Privacy) crypte chaque trame transmise par radio à l'aide d'une clé de 64 bits ou de 128 bits. Normalement, le point d'accès préétablit un jeu de quatre clés et communique avec chaque station en utilisant l'une de ces quatre clés.

Le cryptage WPA (Wi-Fi Protected Access), le mécanisme de sécurisation dominant dans l'industrie, a deux formes : WPA-personnel ou WPA Pre-Share Key (WPA/PSK) et WPA-entreprise ou WPA/802.1x.

Dans WPA-personnel, une clé préétablie est utilisée pour le cryptage pendant la transmission des données. Le WPA utilise le protocole d'intégrité de clé temporelle (TKIP) pour le cryptage, tandis que WPA2 utilise AES. WPA-entreprise combine le cryptage et l'authentification.

Comme le WEP s'est avéré vulnérable, vous pouvez envisager d'utiliser WPA pour une meilleure sécurité. Choisissez le mécanisme de sécurisation qui correspond à vos besoins. Quels que soient les mécanismes de sécurisation que vous choisissez, ils amélioreront tous la protection des données radio et/ou la confidentialité de vos réseaux sans fil. Le routeur sans fil Vigor est très souple et peut prendre en charge de multiples connexions sécurisées mettant en œuvre simultanément WEP et WPA.

Exemple 1

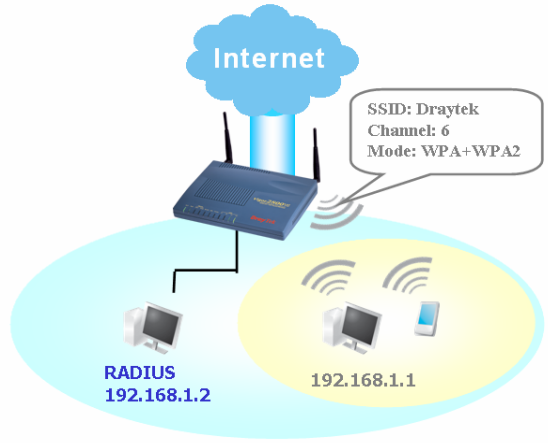


SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WEP or	*Mode : WEP ou*
WPA/PSK	*WPA/PSK*
Mixed (WPA+WPA2)	*Mixte : (WPA+WPA2)*
PSK: cfgs0a12	*PSK : cfgs0a12*
Key 1: AB312	*Clé 1 : AB312*

Exemple 2

SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WPA/PSK only	*Mode : WPA/PSK seulement*
WPA2 only	*WPA2 seulement*
Pre-shared key: cfgs0a12	*Clé prépartagée : cfgs0a12*

Exemple 3



SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WPA+WPA2	*Mode : WPA+WPA2*

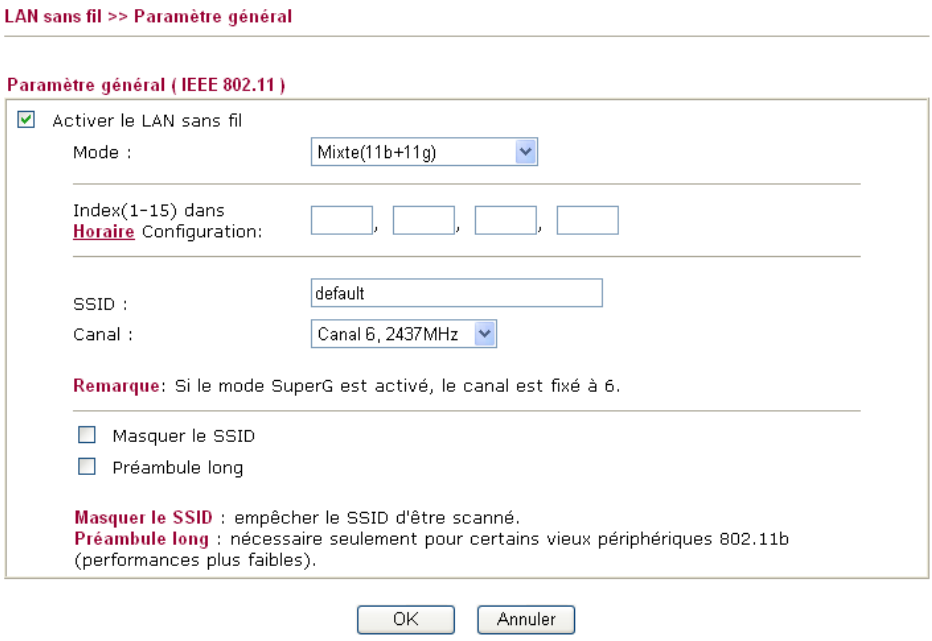
Séparation du sans fil et du filaire – Isolement de WLAN vous permet d'isoler votre LAN sans fil du LAN filaire pour des raisons de mise en quarantaine ou de limitations d'accès. Il s'ensuit qu'aucune communication n'est possible entre les deux LAN. À titre d'exemple, vous pouvez configurer un LAN sans fil uniquement pour les visiteurs de manière qu'ils puissent se connecter à l'internet sans craindre une fuite d'informations confidentielles. Vous pouvez aussi ajouter un filtre d'adresse MAC pour isoler un utilisateur particulier du LAN filaire.

Gestion de stations sans fil – Liste des stations affiche toutes les stations de votre réseau sans fil et l'état de connexion.

Les options du menu LAN sans fil sont les suivantes :

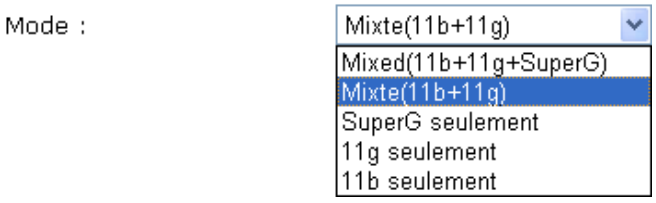
3.12.2 Paramètres généraux

La page web qui apparaît lorsque vous cliquez sur **Paramètres généraux** vous permet de configurer le SSID et le canal radio.



Activer le LAN sans fil Cochez la case pour activer la fonction sans fil.

Mode Sélectionner un mode sans fil approprié.
Mixte (11b+11g+SuperG) – La radio communique simultanément avec les stations IEEE802.11b, IEEE802.11g et SuperG.
Mixte (11b+11g) - La radio communique simultanément avec les stations 802.11b et 802.11g.
SuperG - La radio communique uniquement avec les stations SuperG.
11g only - La radio communique uniquement avec les stations IEEE802.11g.
11b only - La radio communique uniquement avec les stations IEEE802.11b.



Index(1-15)

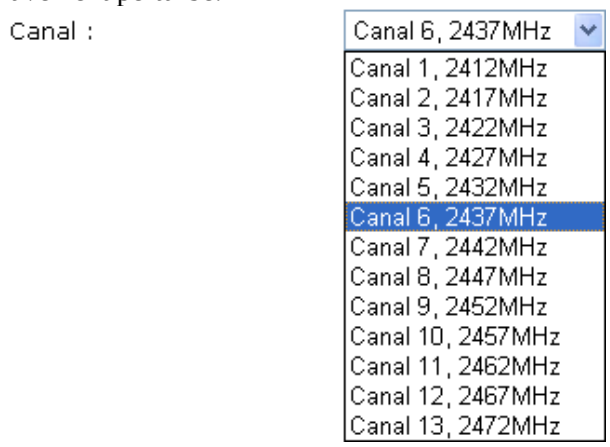
Vous pouvez limiter le fonctionnement du LAN sans fil à certaines plages horaires. Vous pouvez choisir jusqu'à 4 plages horaires parmi les 15 définies dans **Applications >> Plages horaires**. Par défaut, ce champ est vide et la fonction est activée en permanence

SSID

Par défaut, le SSID est « valeur par défaut ». Nous vous suggérons de lui donner un nom particulier. C'est l'identification du LAN sans fil. Le SSID peut se composer d'un nombre quelconque de caractères ou de divers caractères spéciaux.

Canal

Canal radio du LAN sans fil. Le canal par défaut est 6. Vous pouvez en spécifier un autre si le canal sélectionné est gravement perturbé.



Masquer le SSID

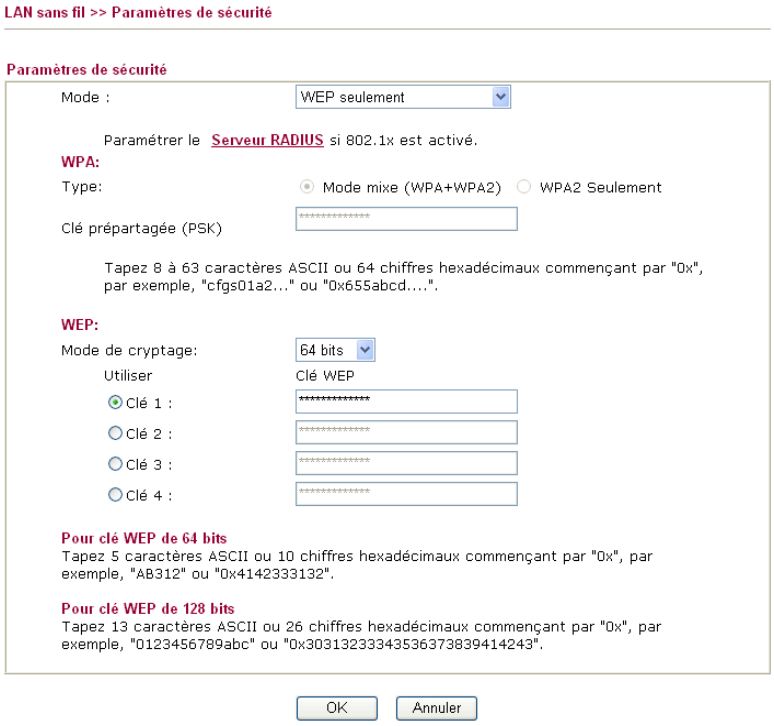
Cochez cette case pour prévenir toute scrutation malveillante et rendre difficile à des clients non autorisés de joindre votre LAN sans fil. Selon l'utilitaire sans fil, l'utilisateur pourra visualiser les informations à l'exception du SSID ou n'avoir aucune information concernant le routeur sans Vigor.

Préambule long

Cette option définit la longueur du champ de synchronisation d'un paquet 802.11. La plupart des réseaux sans fil modernes utilisent un préambule court constitué d'un champ de synchronisation de 56 bits au lieu d'un préambule long de 128 bits. Toutefois, certains équipements de réseau sans fil 11b originel ne prennent en charge que le préambule long. Cochez la case **Préambule long** s'il cela est nécessaire pour communiquer avec ce type d'équipement.

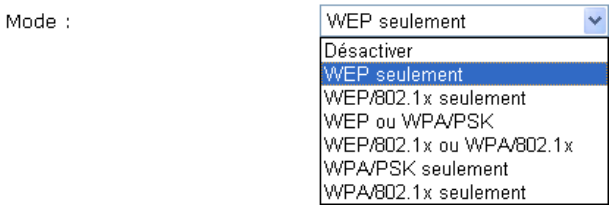
3.12.3 Sécurité

Si vous cliquer sur **Paramètres de sécurité**, une nouvelle page web apparaît vous permettant de configurer WEP et WPA.



Mode

Plusieurs modes sont offerts à votre choix.



Désactiver - Désactive le mécanisme de cryptage.

WEP seulement - Accepte uniquement les clients WEP. La clé doit être tapée dans Clé WEP.

WEP/802.1x seulement - Accepte les clients WEP avec authentification 802.1x. Comme la clé est négociée automatiquement lors de l'authentification, le champ de saisie de la clé n'est pas accessible.

WEP ou WPA/PSK - Accepte les clients WEP et WPA avec une clé valide. Seul le mode mixte (WPA+WPA2) est applicable si vous sélectionnez WPA/PSK.

WEP/802.1x ou WPA/802.1x – Accepte les clients WEP ou WPA avec authentification 802.1x. Seul le mode mixte (WPA+WPA2) est applicable si vous sélectionnez WPA/PSK. Comme la clé est négociée automatiquement lors de l'authentification, le champ de saisie de la clé n'est pas accessible.

WPA/PSK seulement - Accepte les clients WPA. La clé doit être tapée dans PSK. N'oubliez pas de sélectionner le type WPA pour définir un mode mixte ou WPA2 seulement dans le champ de dessous.

WPA/802.1x seulement - Accepte les clients WPA avec authentification 802.1x. N'oubliez pas de sélectionner le type

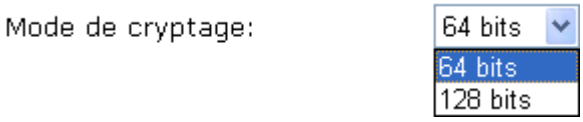
WPA pour définir un mode mixte ou WPA2 seulement dans le champ de dessous. Comme la clé est négociée automatiquement lors de l'authentification, le champ de saisie de la clé n'est pas accessible.

WPA

WPA crypte chaque trame transmise par radio à l'aide de la clé entrée manuellement dans le champ ou négociée automatiquement via l'authentification 802.1x.
Type – Choisir mixte (WPA+WPA2) ou WPA2 seulement.
Clé prépartagée (PSK) - Entrez **8 à 63** caractères ASCII, par exemple 012345678 (soit 64 chiffres hexadécimaux commençant par 0x, par exemple « 0x321253abcde... »).

WEP

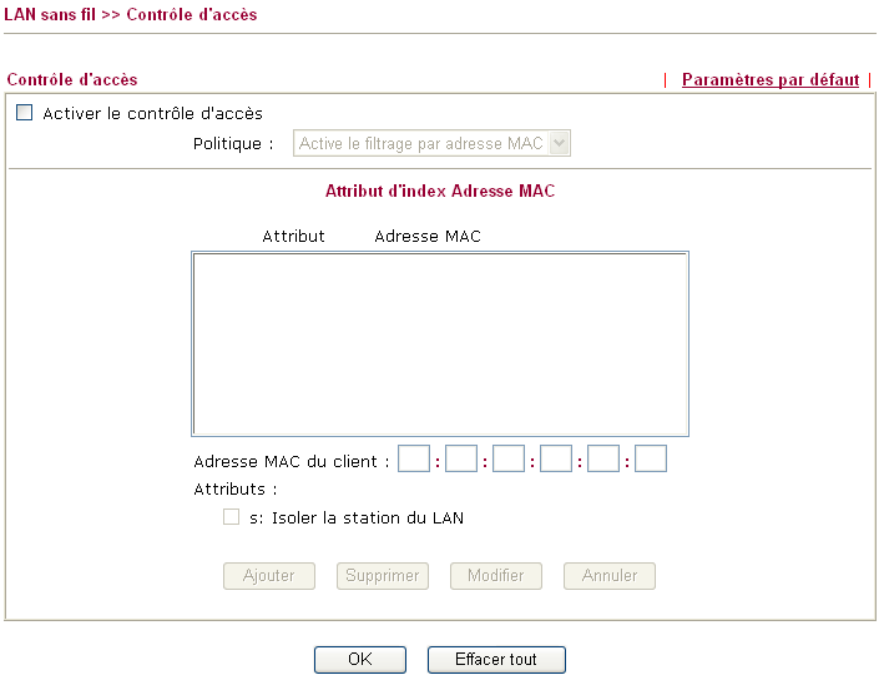
64 bits - Pour le WEP 64 bits, entrez **5** caractères ASCII, comme 12345 (ou 10 chiffres hexadécimaux commençant par 0x, par exemple 0x4142434445F).
128 bits - Pour le WEP 128 bits, entrez **13** caractères ASCII, comme ABCDEFGHIJKLM (ou 26 chiffres hexadécimaux commençant par 0x, par exemple 0x41424344454647484 94A4B4C4D).



Tous les équipements sans fil doivent avoir la même clé WEP. Vous pouvez entrer 4 clés ici mais vous ne pouvez en sélectionner qu'une seule à la fois. Les clés peuvent être entrées en ASCII ou en hexadécimal. Cochez la clé que vous voulez utiliser.

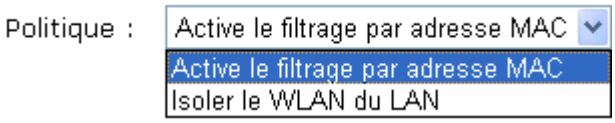
3.12.4 Contrôle d’accès

Pour renforcer la sécurité d’accès sans fil, la fonction de **Contrôle d’accès** vous permet de limiter l’accès au réseau à l’aide de l’adresse MAC du client de LAN sans fil. Seule l'adresse MAC valable configurée peut accéder à l’interface LAN sans fil. En cliquant sur **Contrôle d’accès**, vous obtenez une nouvelle page web qui vous permet d'éditer les adresses MAC de clients pour contrôler leur droit d’accès.



Activer le contrôle d’accès Cochez cette case pour activer la fonction de contrôle d'accès par adresse MAC.

Règle Sélectionnez l’une des règles suivantes. Choisissez **Activer le filtre d’adresses MAC** pour saisir les adresses MAC d’autres clients du réseau. Choisissez **Isoler le WLAN du LAN** pour séparer toutes les stations WLAN du LAN en fonction de la liste d’adresses MAC.



Filtre d’adresse MAC Affichage de toutes les adresses MAC éditées précédemment. Quatre boutons (Ajouter, Supprimer, Modifier, Annuler).

Adresse MAC de clients Saisissez manuellement l’adresse MAC du client sans fil.

Attribut **s –** Cochez cette case pour isoler la connexion sans fil du client sans fil de l’adresse MAC du LAN.

Ajouter Ajouter une nouvelle adresse MAC à la liste.

Supprimer Supprimer l’adresse MAC sélectionnée de la liste.

Modifier Modifier l’adresse MAC sélectionnée.

Annuler Annuler le contrôle d’accès.

OK Enregistrer la liste de contrôle d’accès.

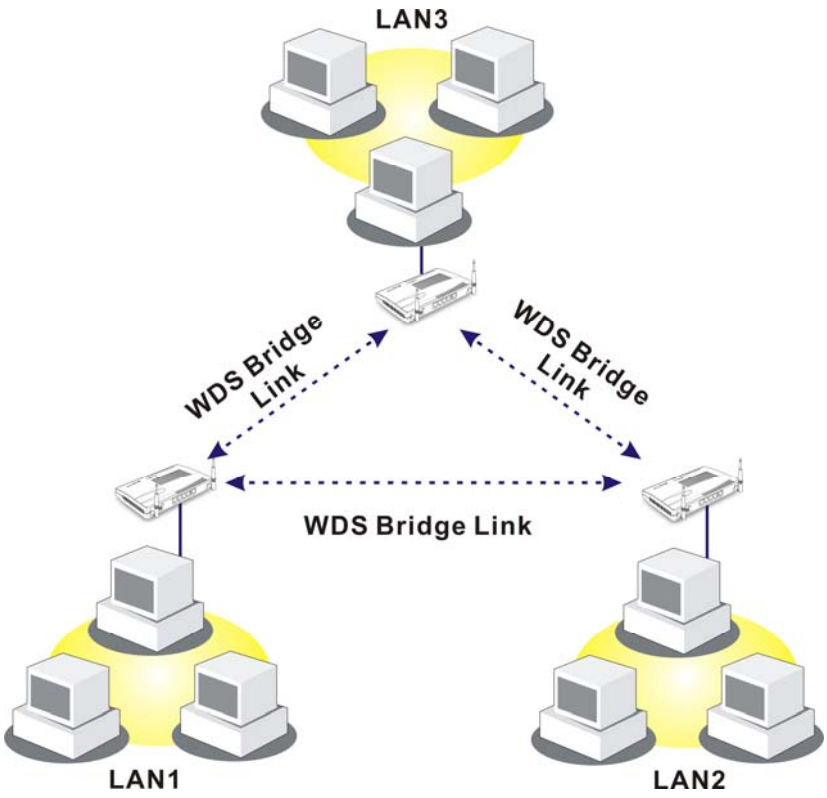
Supprimer tout Supprimer toutes les adresses MAC.

3.12.5 WDS

WDS est l'abréviation de Wireless Distribution System (système de distribution sans fil). C'est un protocole qui permet de relier deux points d'accès (AP) par radio. On l'utilise généralement pour :

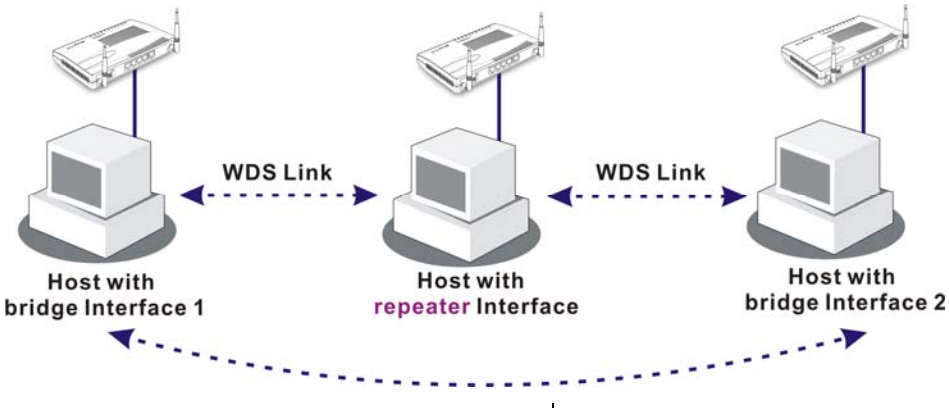
- acheminer le trafic entre deux LAN par radio.
- étendre la zone de couverture d'un LAN sans fil.

Pour réaliser la connectivité sans fil entre AP, le routeur Vigor peut être configuré en deux modes WDS : le mode **Pont** et le mode **Relais**. Le fonctionnement en mode pont est illustré ci-dessous :



WDS Bridge Link | *Mode Pont WDS*

Le fonctionnement en mode relais WDS est illustré ci-dessous :

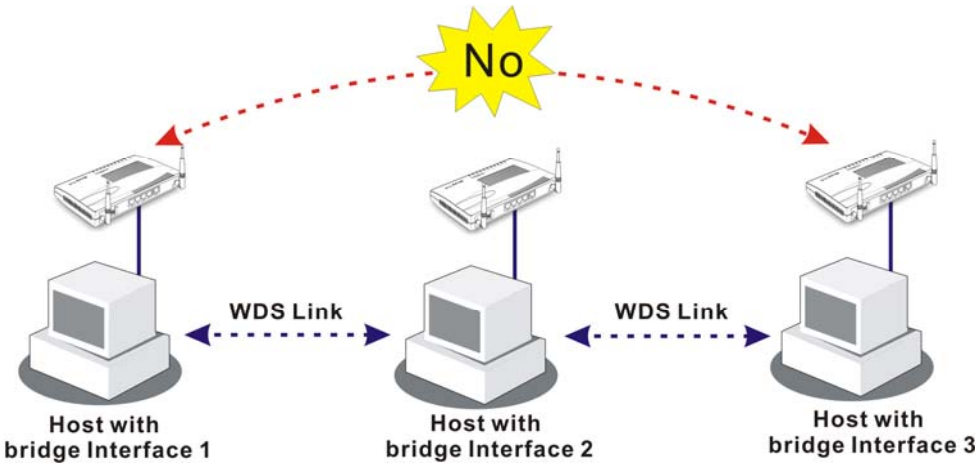


WDS Link | *Liaison WDS*

Host with bridge Interface 1	*Hôte avec interface pont 1*
Host with repeater Interface	*Hôte avec interface relais*
Host with bridge Interface 2	*Hôte avec interface pont 2*

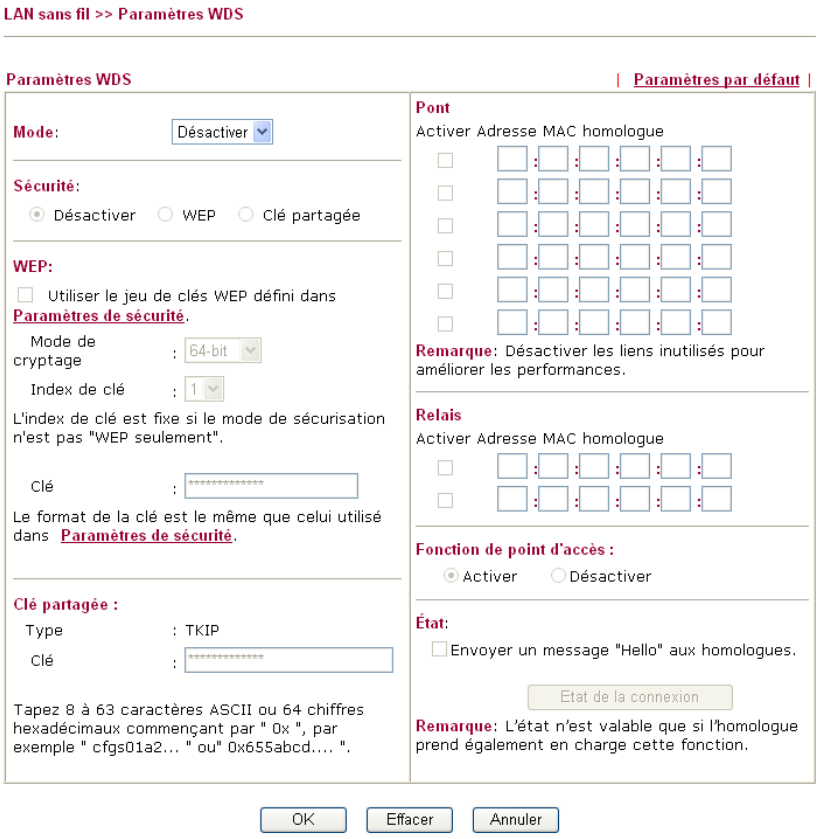
La principale différence entre les deux modes est la suivante : en mode **Relais**, les paquets reçus d'un AP homologue peuvent être relayés vers un autre AP homologue par des liaisons WDS, tandis qu'en mode **Pont**, les paquets reçus par une liaison WDS sont transmis uniquement à des hôtes sans fil ou filaires locaux.

Dans les exemples suivants, les hôtes connectés au Pont 1 ou 3 peuvent communiquer avec les hôtes connectés au Pont 2 par des liaisons WDS. Toutefois, les hôtes connectés au Pont 1 NE PEUVENT PAS communiquer avec les hôtes connectés au Pont 3 via le Pont 2.

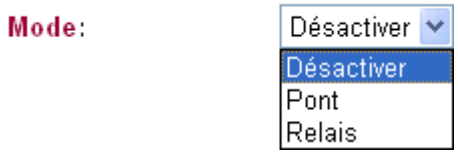


No	*Non*
WDS Link	*Liaison WDS*
Host with bridge Interface 1	*Hôte avec interface pont 1*

Cliquez sur l'option **WDS** du menu **LAN sans fil**. La page suivante apparaît.



Mode Choisissez le mode WDS. Le mode **Désactiver** désactive la fonction WDS. Vous avez, par ailleurs, le choix entre le mode **Pont** et le mode **Relais**.



Sécurité Il y a trois options :, **Désactivé**, **WEP** et **Clé prépartagée**. Le choix fait ici validera le champ WEP ou Clé prépartagée qui suit.

WEP Cochez cette case pour utiliser la clé WEP qui a été spécifiée dans la page **Paramètres de sécurité**. Si vous n'avez pas spécifié de clé dans la page **Paramètres de sécurité**, cette case à cocher est estompée.

Paramètres **Mode de cryptage** – Si vous avez coché la case **Utilisation de la même clé WEP…**, inutile de choisir 64 bits ou 128 bits comme mode de cryptage. Si vous ne cochez pas cette case, vous pouvez spécifier maintenant la clé WEP dans cette page.
Index de clé – Choisissez la clé que vous voulez utiliser après avoir choisi le mode de cryptage approprié.
Clé – Tapez la clé.

Clé prépartagée Tapez 8 à 63 caractères ASCII ou 64 chiffres hexadécimaux commençant par « 0x ».

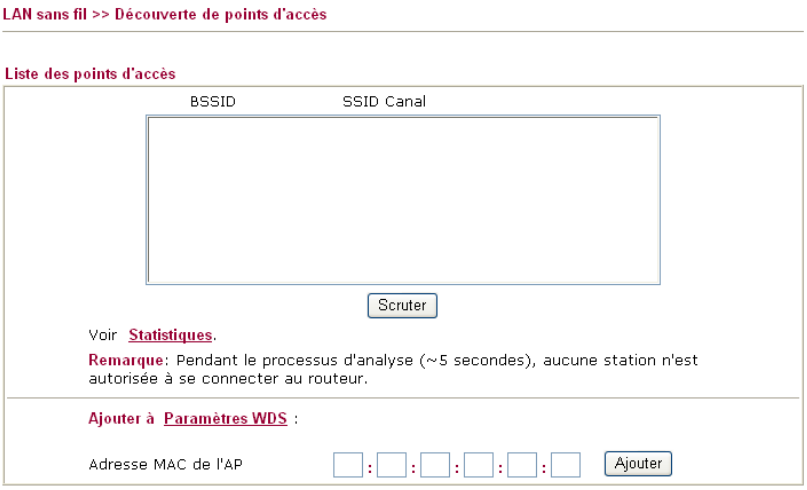
Pont Si vous choisissez le mode pont, tapez l'adresse MAC d'homologue dans ces champs. Vous pouvez entrer jusqu'à **six** adresses MAC d'homologue. Pour que les performances

	soient meilleures, désactivez les liens non utilisés. Si vous voulez invoquer l'adresse MAC d'homologue, n'oubliez pas vous pouvez entrer au maximum deux adresses MAC d'homologue. Si vous voulez invoquer l'adresse MAC d'homologue, n'oubliez pas de cocher la case **Activer** en face de l'adresse MAC.
Fonction de point d'accès	Cliquez sur **Activer** pour indiquer que le routeur fonctionnera comme un point d'accès ; cliquez sur **Désactiver** pour annuler cette fonction.
État	Vous permet d'envoyer un message « hello » aux homologues. Il faut que l'homologue prennent en charge cette fonction.

3.12.6 Découverte d'AP

Le routeur Vigor peut scruter tous les canaux et détecter les points d'accès actifs du voisinage. En fonction du résultat de la rechercher, vous savez quel canal est exploitable. Cette fonction permet également de recherche un point d'accès pour une liaison WDS. À noter que, pendant la scrutation (qui dure environ 5 secondes), aucun client ne peut se connecter au routeur Vigor.

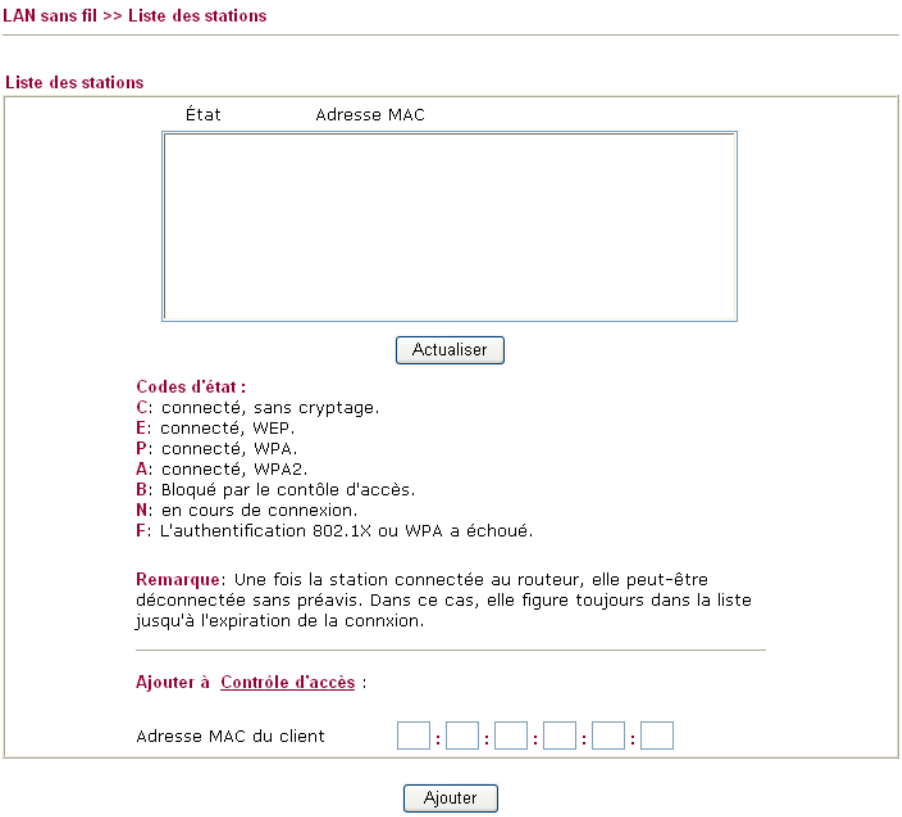
Cette page permet de rechercher les points d'accès du LAN sans fil. Seul un point d'accès calé sur le même canal que le routeur peut être détecté. Cliquez sur **Scruter** pour découvrir tous les points d'accès du voisinage.



Si vous voulez appliquer les paramètres WDS au point d'accès détecté, tapez l'adresse MAC du point d'accès en bas de la page et cliquez sur **Ajouter**. L'adresse MAC du point d'accès sera ajoutée à la page de paramétrage WDS.

3.12.7 Liste des stations

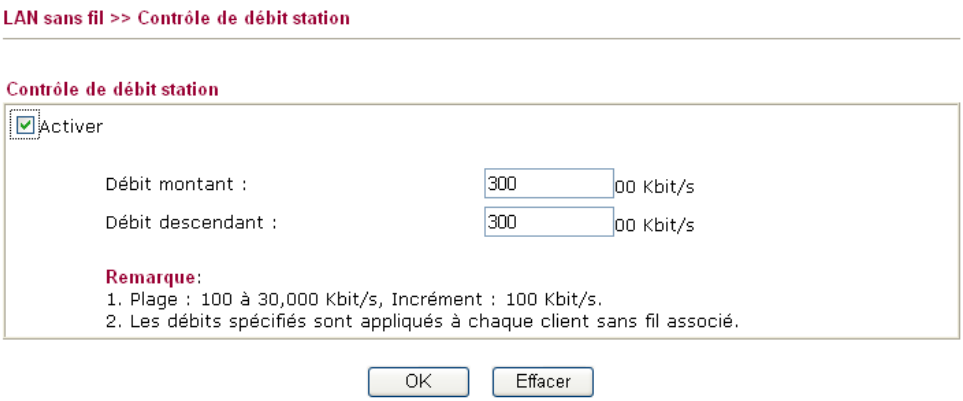
La **liste des stations** permet de connaître des clients sans fil qui se connectent actuellement avec leur code d'état. La signification des codes est indiquée au-dessous. Pour le **contrôle d'accès**, vous pouvez sélectionner station WLAN et cliquez sur **Ajouter au contrôle d'accès**.



Actualiser	Cliquez sur ce bouton pour actualiser la liste des stations.
Ajouter	Cliquez sur ce bouton pour ajouter l'adresse MAC actuellement sélectionnée au **Contrôle d'accès**.

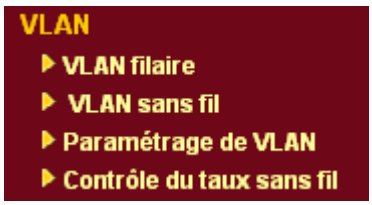
3.12.8 Contrôle de débit de station

Cette page vous permet de régler le débit montant et descendant de chaque client sans fil (station). Cochez la case **Activer** pour que ce paramétrage soit pris en compte. Le débit est réglable de 100 à 30000 kbit/s.



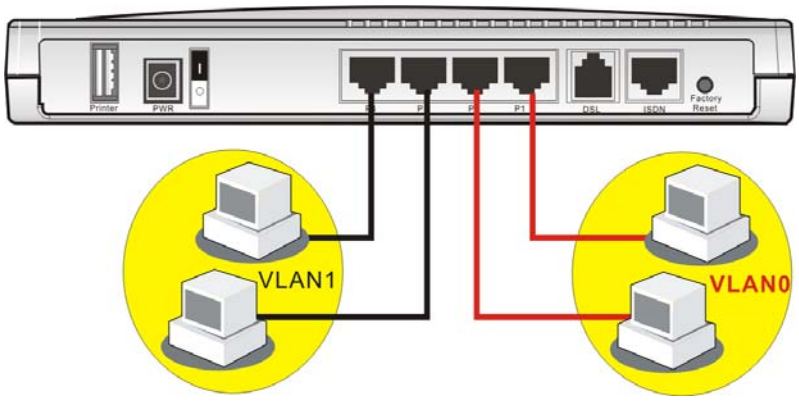
3.13 VLAN

La fonction LAN virtuel vous permet de gérer commodément les hôtes en les groupant par port physique.

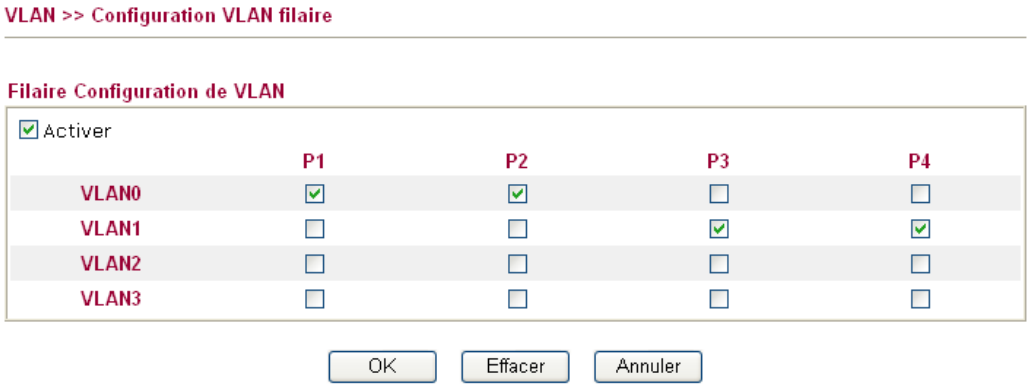


3.13.1 VLAN filaire

Les PC raccordés aux ports Ethernet du routeur peuvent être divisés en groupes pour constituer des LAN virtuels. Les PC appartenant à un même groupe peuvent partager des informations sans être épiés par ceux des autres groupes.

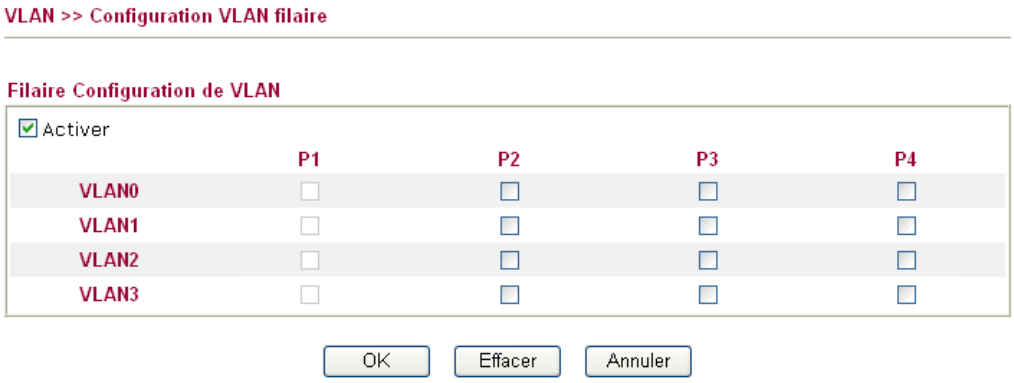


L'option **VLAN filaire** du menu **VLAN** vous permet de configurer des VLAN filaires. Par exemple, cochez les cases P1 et P2 pour VLAN0 et P3 et P4 pour VLAN1.



Activer	Cochez cette case pour activer cette fonction.
P1 – P4	Cochez la case pour que le PC relié au port soit inclus dans le VLAN spécifié. Vous pouvez inclure un port dans plusieurs VLAN. Par exemple, si vous cochez VLAN0-P1 et VLAN1-P1, P1 appartiendra simultanément à VLAN0 et à VLAN1.
VLAN0-3	Ce routeur vous permet de constituer quatre groupes et donc quatre LAN virtuels.

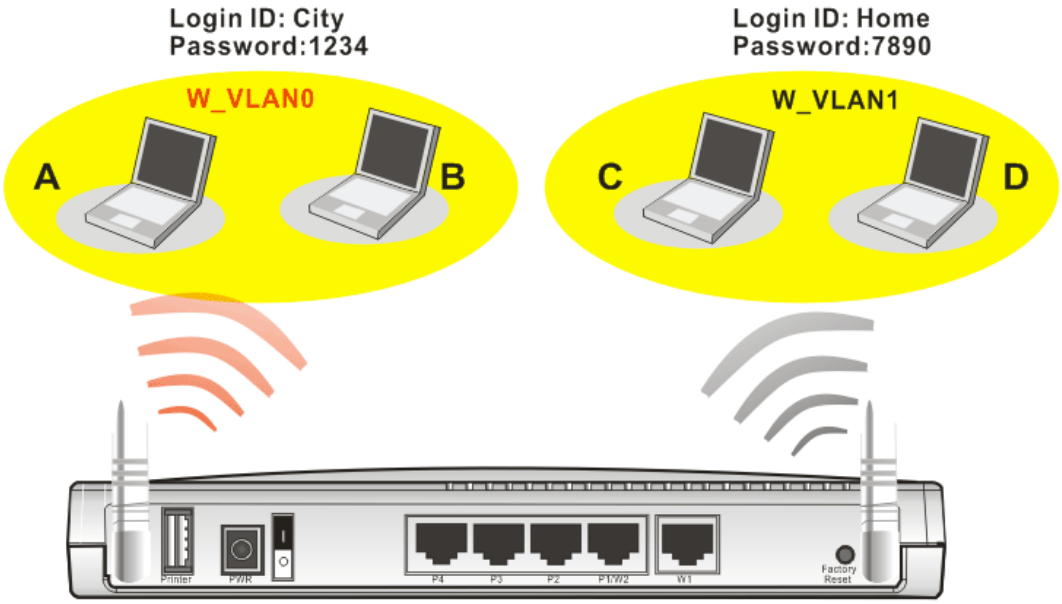
Nota : si l'interface WAN2 a été activée, le port P1 sert d'interface WAN et ne peut donc pas être inclus dans un VLAN, comme le montre la figure suivante.



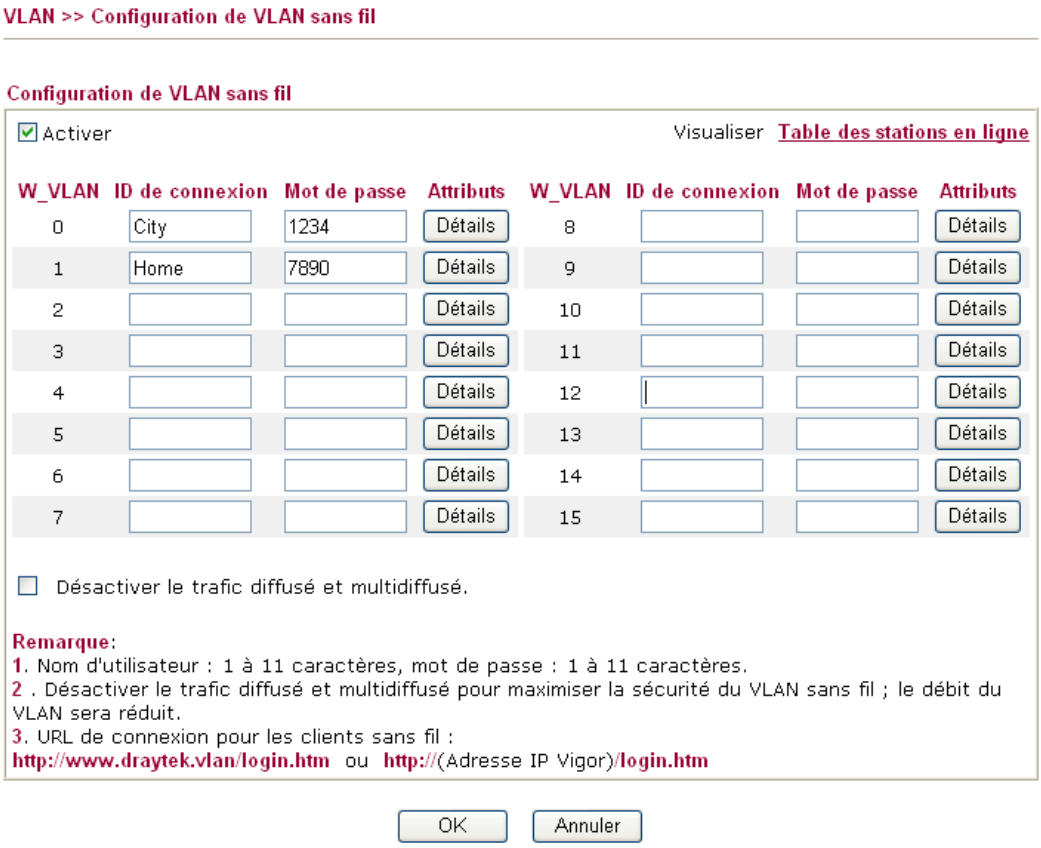
3.13.2 VLAN sans fil

Les PC (équipés d'une carte réseau sans fil) connectés au routeur via l'interface sans fil peuvent être divisés en groupes pour constituer des VLAN sans fil (W_VLAN). Les PC d'un même groupe peuvent partager des informations sans être épiés par ceux des autres groupes.

Les PC d'un même groupe peuvent utiliser le même nom d'utilisateur et le même mot de passe pour accéder à l'internet. Par exemple, dans la figure ci-dessous, A et B utilisent le même nom d'utilisateur (City) et le même mot de passe (1234). Ils appartiennent au même W_VLAN.



L'option **VLAN sans fil** du menu **VLAN** vous permet de configurer des VLAN sans fil. Tapez le nom d'utilisateur et le mot de passe (**City** et **1234**) dans les champs correspondants au W_VLAN0. Tapez le nom d'utilisateur et le mot de passe (**Home** and **7890**) dans les champs correspondants au W_VLAN1. Cette page permet de configurer quinze VLAN sans fil.

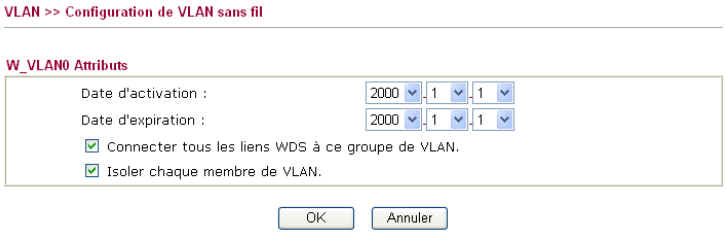


Activer Cochez cette case pour activer la fonction VLAN sans fil.

Nom d'utilisateur Nom d'utilisateur de 1 à 11 caractères des différents VLAN sans fil.

Mot de passe Mot de passe de 1 à 11 caractères des différents VLAN sans fil.

Détails Cliquez sur ce bouton pour définir d'autres paramètres de VLAN sans fil.



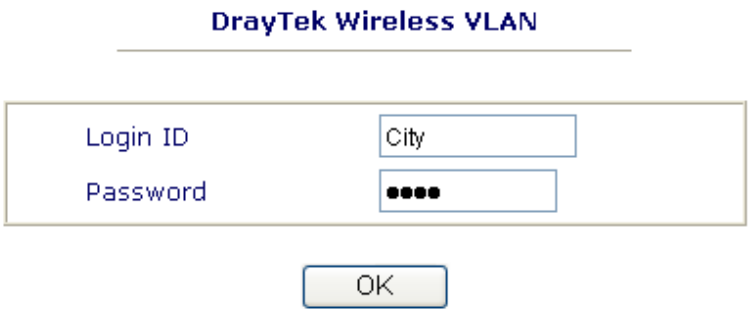
Date d'activation – Utilisez la liste déroulante pour spécifier la date d'activation du VLAN sans fil.
Date d'expiration – Utilisez la liste déroulante pour spécifier la date d'expiration du VLAN sans fil.
Connecter toutes les liaisons WDS à ce VLAN– Cochez cette case pour activer cette connexion.
Isoler chaque membre de ce VLAN – Cochez cette case pour isoler tous les membres de ce VLAN et empêcher qu'ils partagent des informations.

Inhiber le trafic diffusé et multidiffusé Cochez cette case pour empêcher l'acheminement de trafic diffusé ou multidiffusé jusqu'au VLAN sans fil.

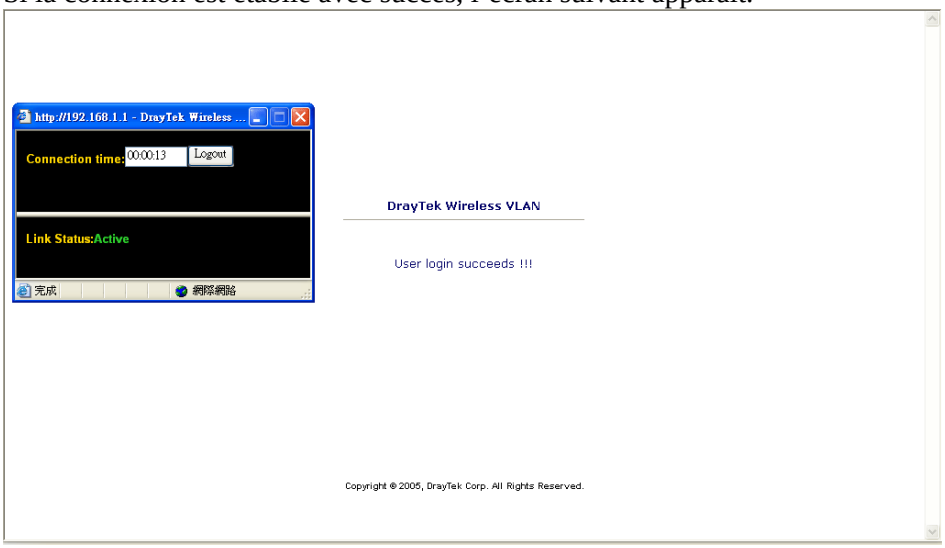
Accès d’un client sans fil à l’internet

Après avoir configuré un VLAN sans fil, les clients sans fil se connectant au routeur doivent effectuer les opérations suivantes pour accéder à l’internet.

1. Ouvrir un navigateur et taper http://www.draytek.vlan/login.htm or http://(adresse IP du routeur Vigor)/login.htm sur la ligne d’adresse.
2. L’écran suivant apparaît.



3. Taper le nom d’utilisateur et le mot de passe configurés dans la page de configuration du VLAN sans fil. Dans cette exemple, nous choisissons City et 1234.
4. Si la connexion est établie avec succès, l’écran suivant apparaît.

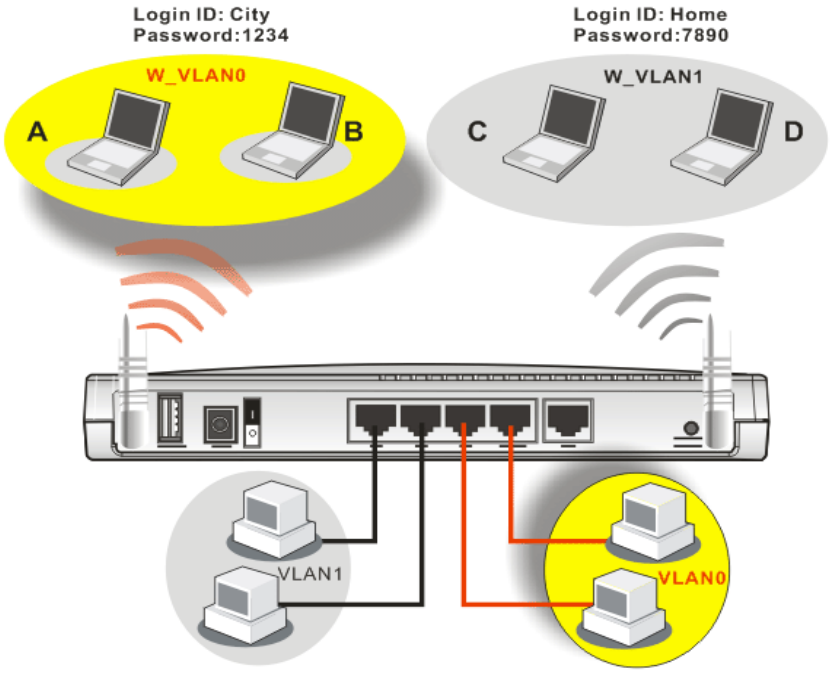


Nota : la fenêtre flottante indiquant le temps de connexion reste sur l’écran jusqu’à ce que vous vous déconnectiez.

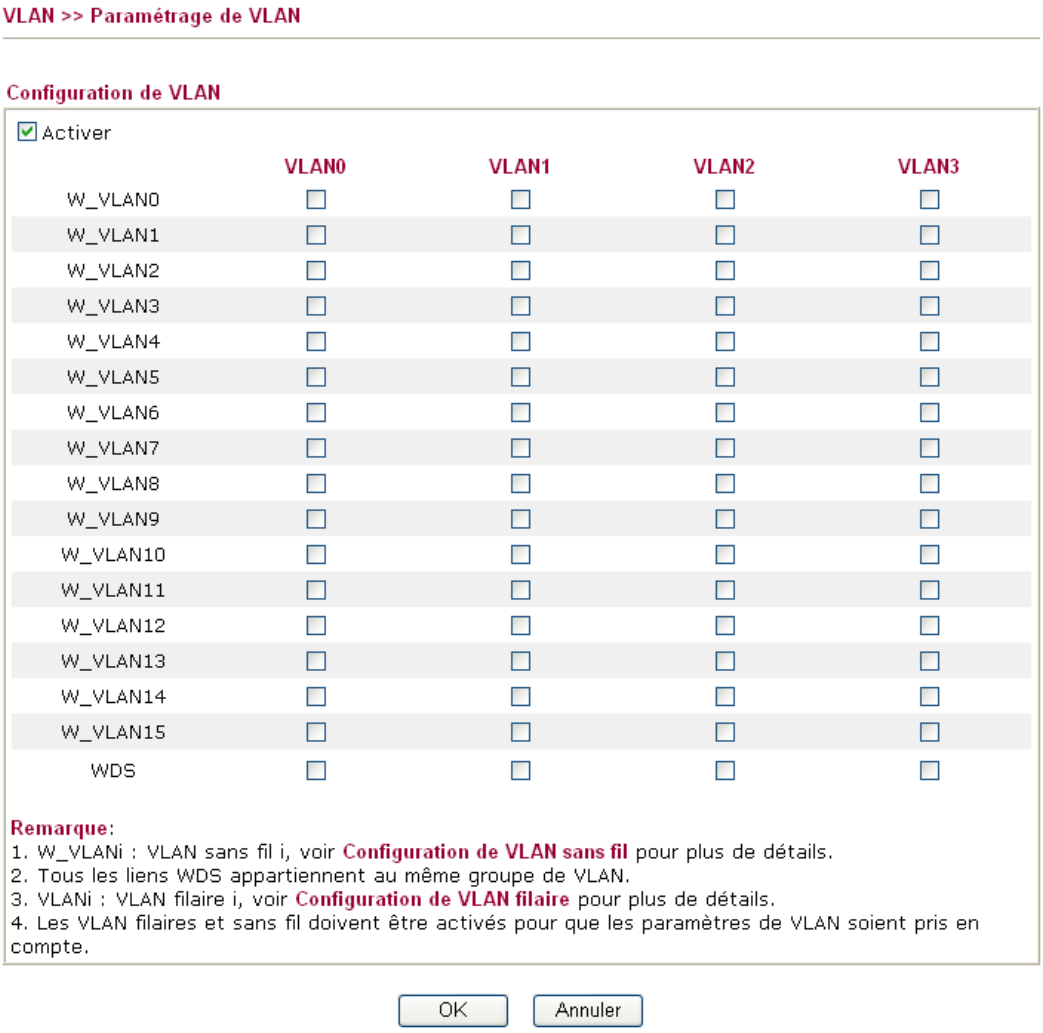
5. Vous pouvez aller à **Diagnostics>>Station en ligne de VLAN sans fil** pour visualiser l'état de la connexion.

3.13.3 Interconnexion de VLAN

Cette fonction permet d'interconnecter un VLAN filaire et un VLAN sans fil pour prendre en charge différents ordinateurs. Dans l'exemple ci-dessous, les portables A et B et les PC du VLAN0 peuvent partager des ressources sans difficultés.



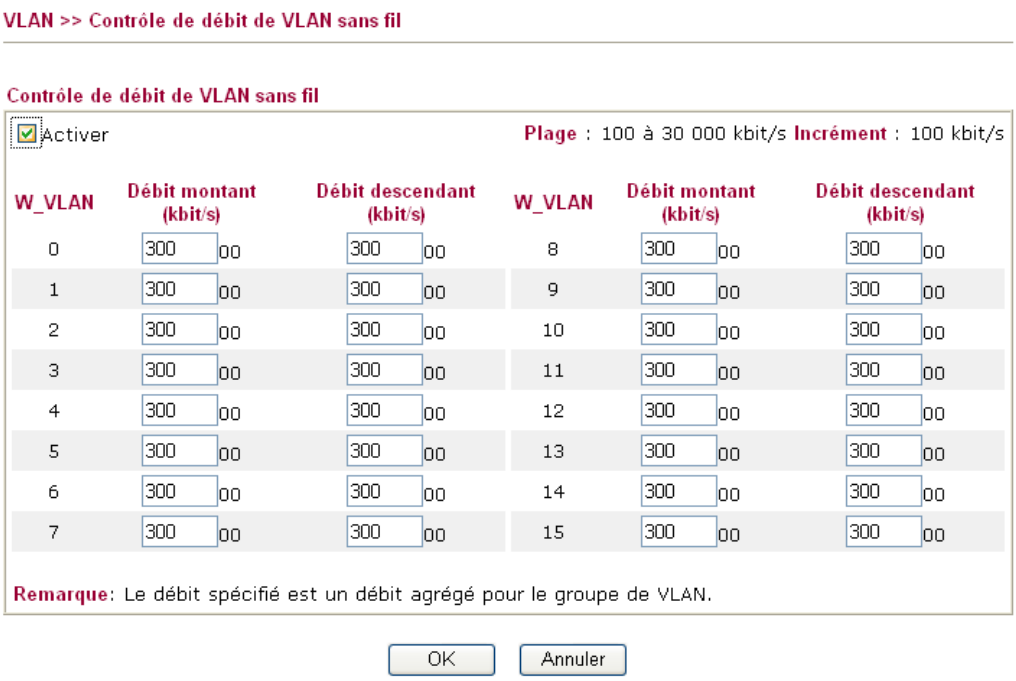
L'option **interconnexion de VLAN** du menu **VLAN** vous permet d'établir un pont de communication entre des ordinateurs appartenant à un VLAN sans fil et à un VLAN filaire. Il suffit, par exemple, de cocher la case sous VLAN0 de la ligne W_VLAN0.



Activer	Cochez cette case pour activer la fonction d'interconnexion de VLAN.
VLAN0-3	LAN virtuels reliés à une interface Ethernet.
W_VLAN0-15	LAN virtuels sans fil reliés à une interface sans fil.

3.13.4 Contrôle de débit sans fil

La fonction de **contrôle de débit** gère le débit à l'arrivée et au départ du routeur. Vous pouvez également gérer le débit à l'arrivée et au départ de chaque VLAN sans fil. Sélectionnez l'option **Contrôle de débit sans fil** du menu **VLAN.** La page suivante apparaît. Cliquez sur **Activer** pour activer le contrôle de débit sans fil.



Activer — Cochez cette case pour activer le contrôle de débit. Cette fonction limitera le débit montant et descendant.

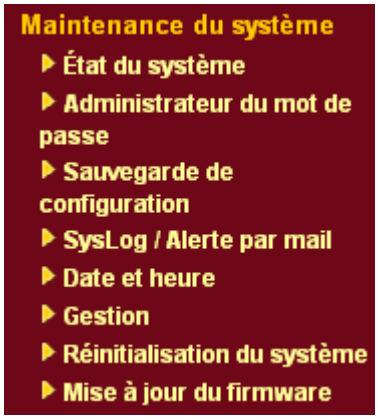
Débit montant — Détermine le débit sortant. La valeur par défaut est 300. Tapez une valeur comprise entre 100 kbit/s et 20 000 kbit/s.

Débit descendant — Détermine le débit entrant. La valeur par défaut est 300. Tapez une valeur comprise entre 100 kbit/s et 20 000 kbit/s.

3.14 Maintenance du système

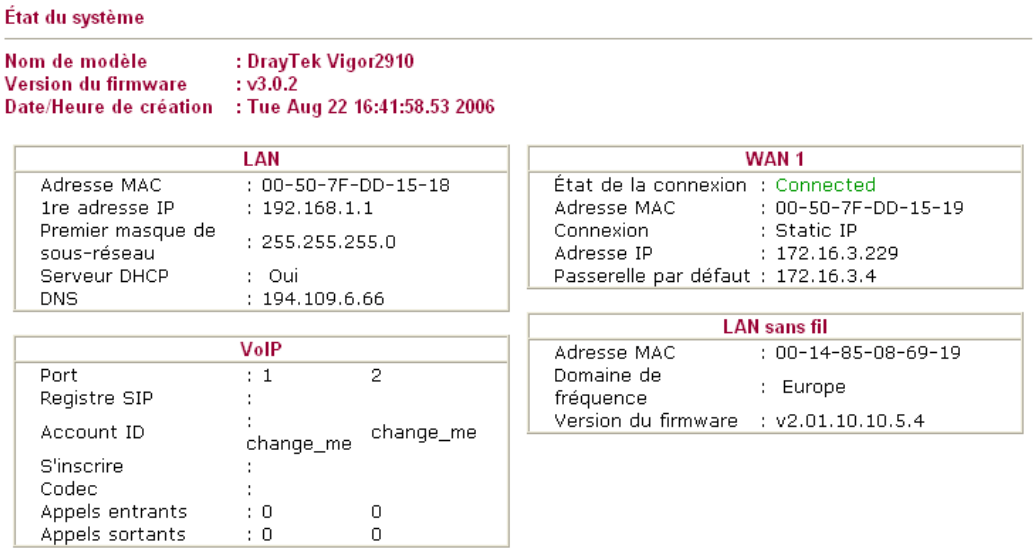
Plusieurs aspects de la configuration du système sont à connaître : comment visualiser l'état du système, comment définir ou modifier le mot de passe administrateur, comment sauvegarder ou restaurer une configuration, comment définir le serveur SysLog, comment régler la date et l'heure, comment réinitialiser le système et comment mettre à jour le firmware.

Les options du menu Maintenance du système sont les suivantes :



3.14.1 État du système

L'état du système fournit les paramètres réseau de base du routeur Vigor, notamment les informations relatives aux interfaces LAN et WAN. Vous pouvez également obtenir des informations sur la version actuelle du logiciel.

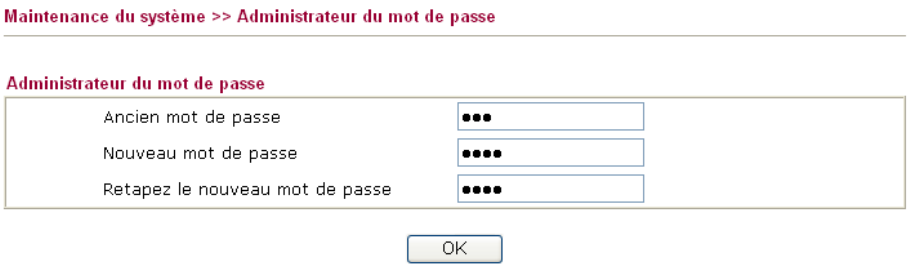


Nom de modèle	Affiche la désignation de modèle du routeur.
Version du firmware	Affiche la version du firmware du routeur.
Date et heure de création	Affiche la date et l'heure de création du firmware.
Adresse MAC	Affiche l'adresse MAC de l'interface LAN.
1re adresse IP	Affiche l'adresse IP de l'interface LAN.
1er masque de sous-réseau	Affiche le masque de sous-réseau de l'interface LAN.
Serveur DHCP	Affiche l'état actuel du serveur DHCP de l'interface LAN.

Adresse MAC	Affiche l'adresse MAC de l'interface WAN.
Adresse IP	Affiche l'adresse IP de l'interface WAN.
Passerelle par défaut	Affiche l'adresse IP de la passerelle par défaut.
DNS	Affiche l'adresse IP du DNS primaire.
Adresse MAC	Affiche l'adresse MAC de l'interface sans fil.
Domaine de fréquence	Europe (13 canaux utilisables), États-Unis (11 canaux utilisables), etc. Le nombre de canaux utilisables varie suivant les pays.
Version du firmware	Affiche des informations sur la carte miniPCI installée pour le LAN sans fil.

3.14.2 Mot de passe administrateur

Cette page vous permet de définir un nouveau mot de passe.



Ancien mot de passe	Tapez l'ancien mot de passe. Le mot de passe par défaut est vide.
Nouveau mot de passe	Tapez le nouveau mot de passe.
Retaper le nouveau mot de passe	Retapez le nouveau mot de passe.

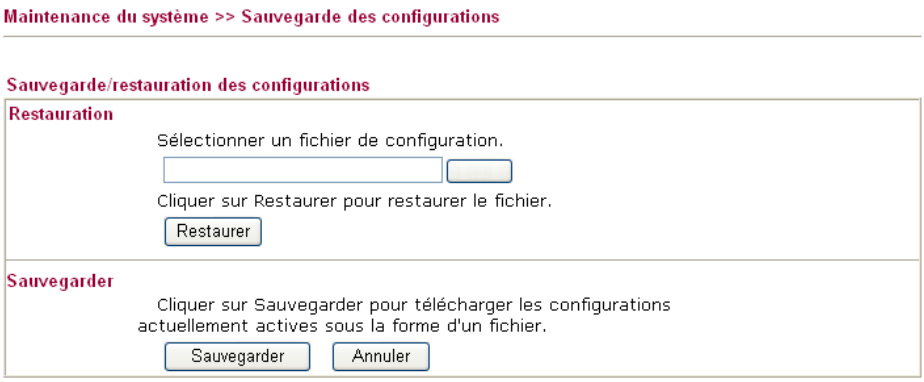
Lorsque vous cliquez sur OK, la fenêtre de connexion apparaît. Pour accéder de nouveau au configurateur web, servez-vous du nouveau mot de passe.

3.14.3 Sauvegarde des configurations

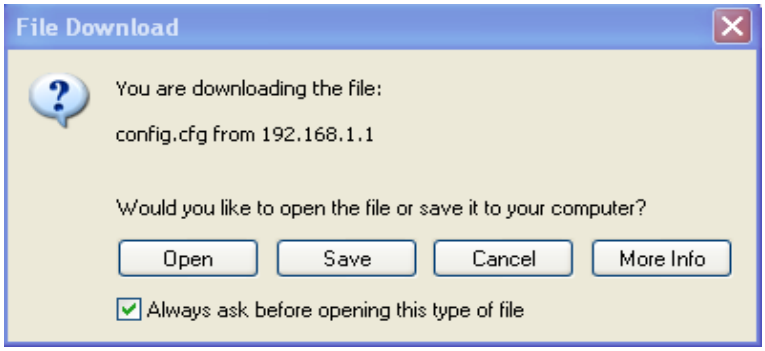
Sauvegarde de la configuration

Pour sauvegarder votre configuration :

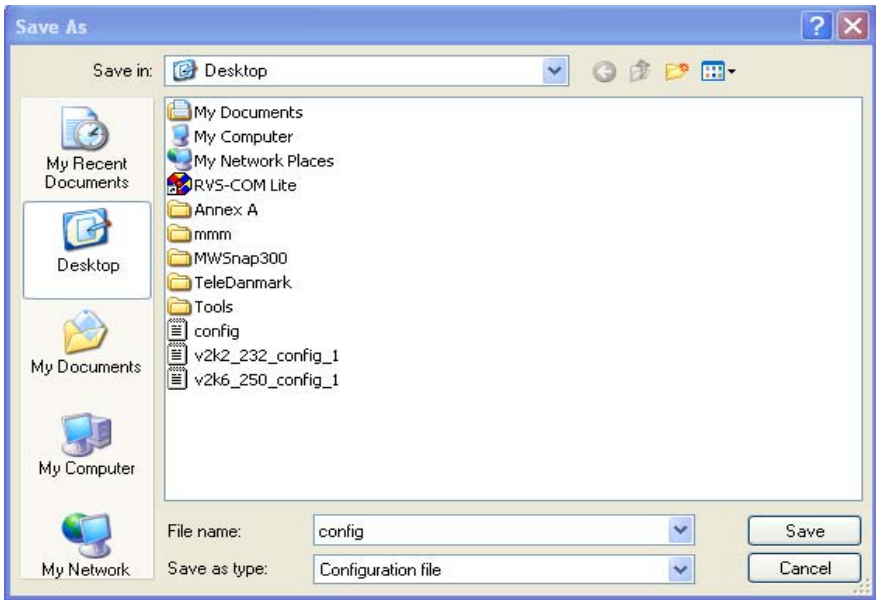
1. Allez à **Maintenance du système** > **Sauvegarde des configurations**. Les fenêtres suivantes apparaissent.



2. Cliquez sur le bouton **Sauvegarder** pour afficher la boîte de dialogue suivante. Cliquez sur le bouton **Enregistrer** pour ouvrir une autre boîte de dialogue vous permettant d'enregistrer la configuration sous la forme d'un fichier.



3. Dans la boîte de dialogue **Enregistrer sous**, le nom de fichier par défaut est **config.cfg**. Vous pouvez lui donner un autre nom.



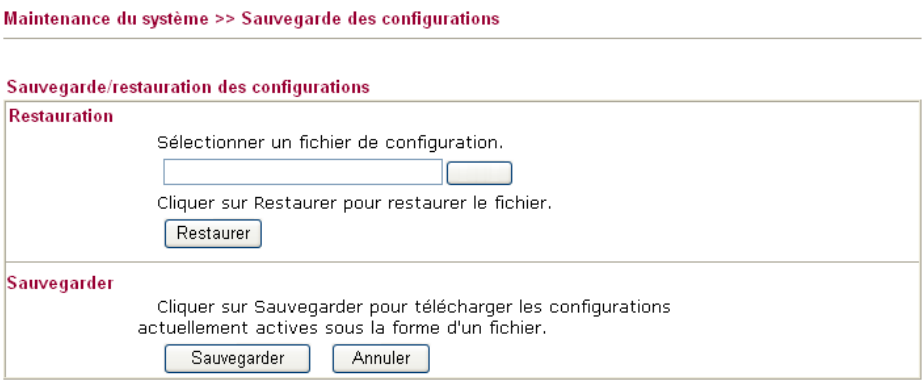
4. Cliquez sur le bouton **Enregistrer.** La configuration est téléchargée automatiquement sur votre ordinateur sous la forme d'un fichier **config.cfg**.

L'exemple ci-dessus vaut pour les plateformes **Windows**. La plateforme **Mac** ou **Linux** donne des fenêtres différentes mais la fonction de sauvegarde est la même.

Nota : la sauvegarde des certificats doit être effectuée indépendamment. La sauvegarde de la configuration n'inclut pas celle des certificats.

Restaurer la configuration

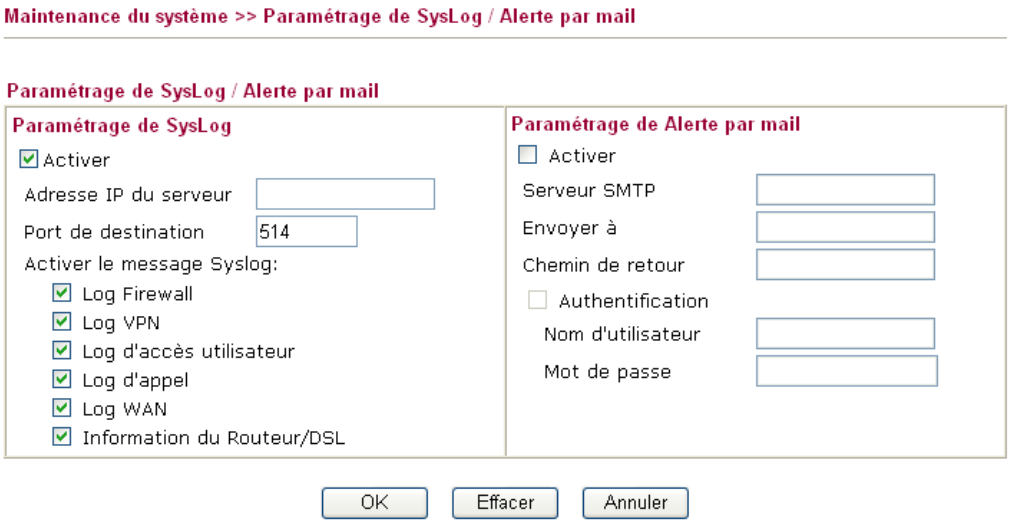
1. Allez à **Maintenance du système** > **Sauvegarde des configurations**. Les fenêtres suivantes apparaissent.



2. Cliquez sur le bouton **Parcourir** pour choisir le fichier de configuration correct.
3. Cliquez sur le bouton **Restaurer** et attendez quelques secondes. Vous êtes informé du succès de la restauration.

3.14.4 Syslog/Mail Alert

La fonction SysLog aide les utilisateurs à surveiller le routeur. Inutile d'aller dans le configurateur web du routeur ou de se procurer des équipements de débogage

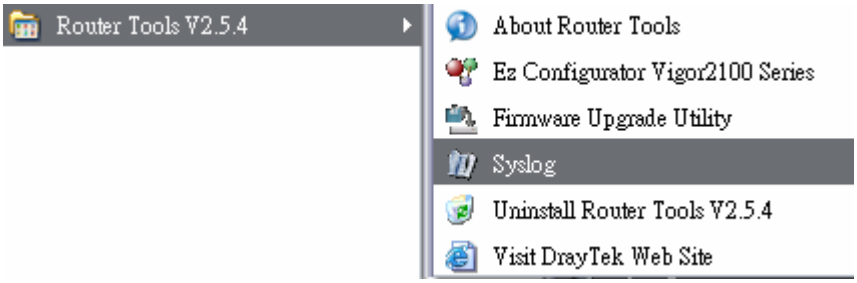


Activer	Cliquez sur « **Activer** » pour activer cette fonction.
Adresse IP du serveur SysLog	Adresse IP du serveur SysLog.
Port de destination	Spécifiez un port de destination pour le protocole SysLog.
Serveur SMTP	Adresse IP du serveur SMTP.
Envoyer à	Adresse e-mail du destinataire.
Chemin de retour	Adresse e-mail de l'émetteur.
Authentification	Cochez cette case pour activer cette fonction lors de l'utilisation d'une application de messagerie électronique.
Nom d'utilisateur	Nom d'utilisateur pour l'authentification.
Mot de passe	Mot de passe pour l'authentification.

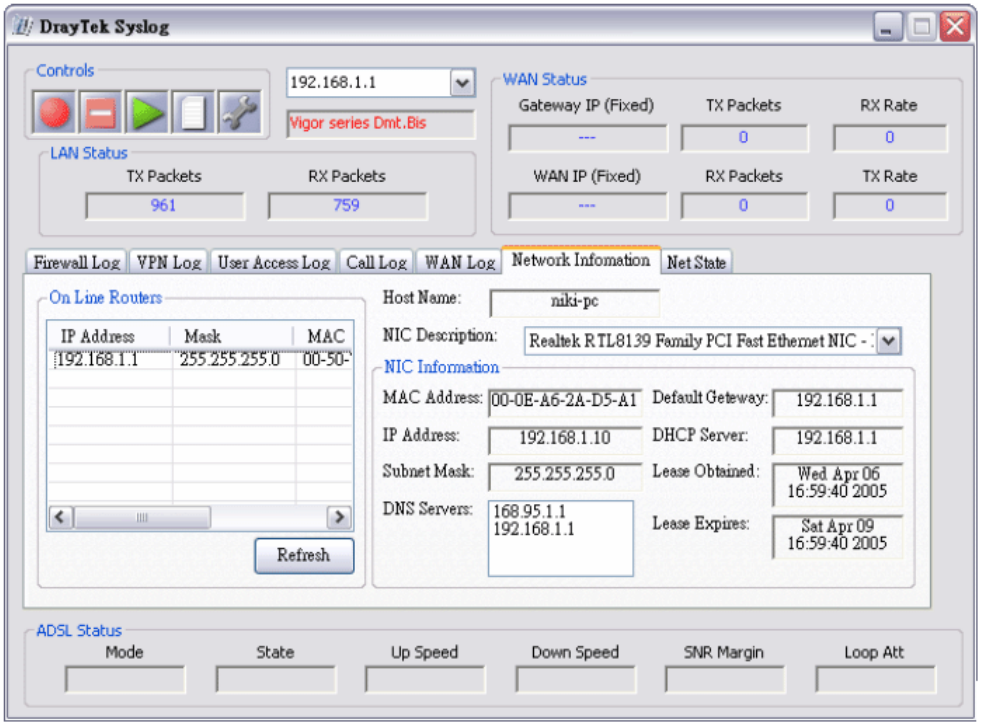
Cliquez sur **OK** pour enregistrer ces paramètres.

Pour visualiser le SysLog :

1. Tapez l’adresse IP de votre PC dans le champ Adresse IP du serveur.
2. Installez les outils du routeur dans l'utilitaire avec le CD fourni. Après l’installation, cliquez sur **Router Tools>>SysLog**.

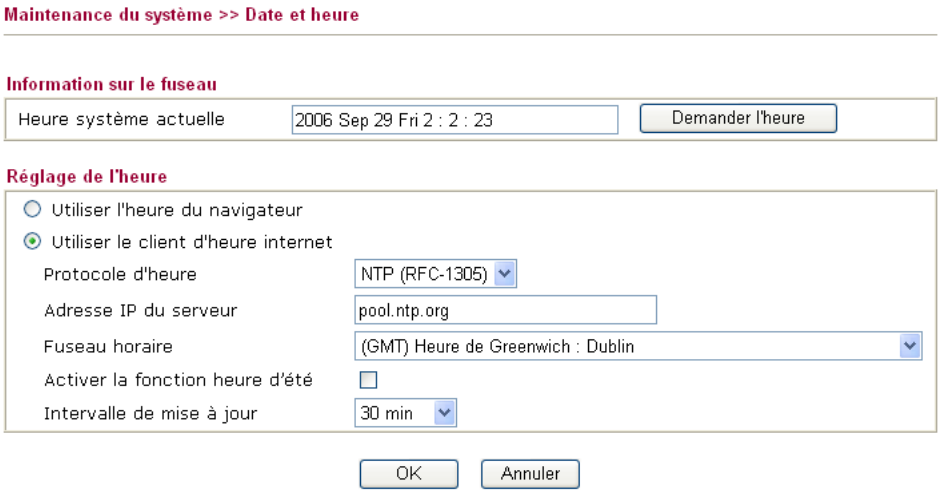


3. À partir de l’écran SysLog, sélectionnez le routeur que vous voulez observer. Dans **Network Information**, sélectionnez la carte réseau utilisée pour se connecter au routeur. Autrement, vous ne pourrez pas obtenir d’information u routeur.



3.14.5 Réglage de l'heure et de la date

Il s’agit de spécifier où le routeur doit obtenir l’heure et la date.

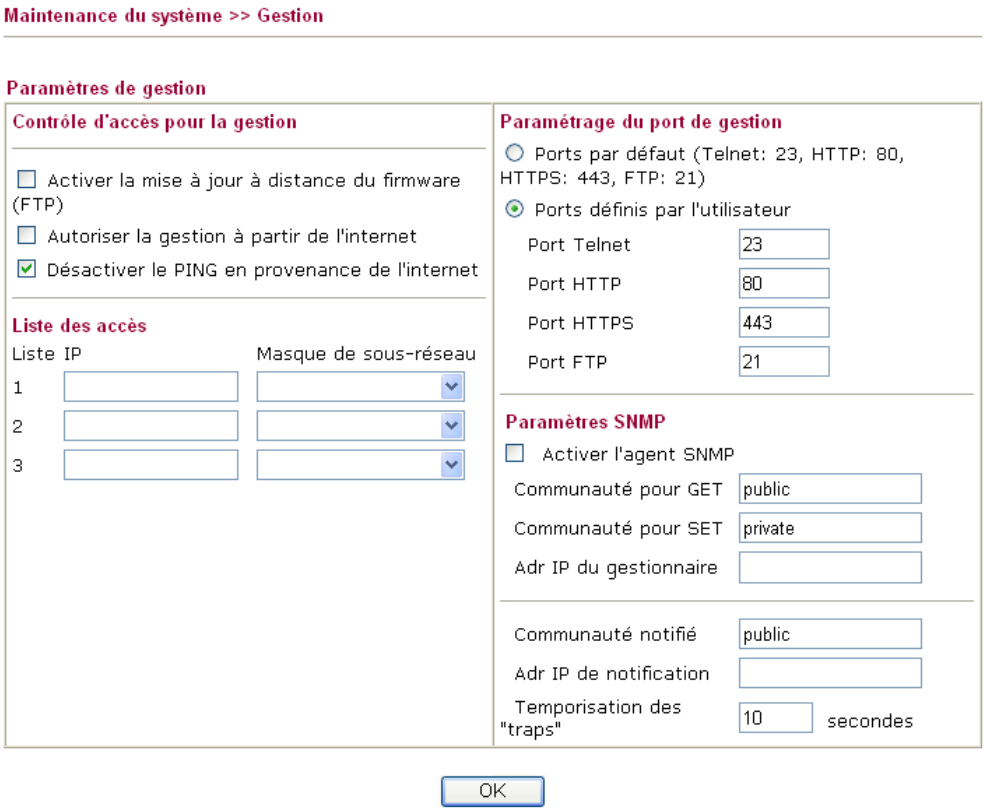


Heure système actuelle	Cliquez sur **Demander l’heure** pour obtenir l’heure actuelle.
Utiliser l'heure du navigateur	Sélectionnez cette option pour utiliser l’heure du navigateur du PC d’administration distant comme heure du routeur.
Utiliser le client d’heure internet	Sélectionnez l'heure à un serveur d'heure sur internet à l'aide du protocole défini.
Protocole d’heure	Sélectionnez un protocole d’heure.
Adresse IP du serveur	Tapez l’adresse IP du serveur d’heure.
Fuseau horaire	Sélectionnez le fuseau horaire du lieu d’installation du routeur.
[ntervalle de mise à jour	Sélectionnez un intervalle de mise à jour à partir du serveur NTP.

Cliquez sur **OK** pour enregistrer ces paramètres.

3.14.6 Gestion

Cette page vous permet de gérer les paramètres de contrôle d'accès, la liste d'accès, les paramètres du port de gestion et les paramètres SMP. Par exemple, en ce qui concerne la gestion du contrôle d'accès, le numéro de port est utilisé pour envoyer ou recevoir un message SIP afin d'établir une session. La valeur par défaut est 5060 et doit correspondre au registre homologue pour les appels VoIP.



Autoriser la mise à jour à distance du firmware — Cliquez sur la case pour autoriser la mise à jour à distance du firmware via le protocole de transfert de fichier (FTP).

Autoriser la gestion à partir de l'internet — Cochez la case pour autoriser les administrateurs système à se connecter à partir de l'internet. Par défaut, la connexion n'est pas autorisée.

Désactiver le PING en provenance de l'internet — Cochez la case pour rejeter tous les paquets PING provenant de l'internet. Pour des raisons de sécurité, cette fonction est activée par défaut.

Liste d'accès — Vous pouvez spécifier que l'administrateur système peut se connecter uniquement à partir d'un hôte ou d'un réseau spécifique défini dans la liste. Vous pouvez définir jusqu'à trois adresses IP/masques de sous-réseau.
Liste IP - Adresse IP autorisée à se connecter au routeur.
Masque de sous-réseau - Masque de sous-réseau autorisé à se connecter au routeur.

Ports par défaut — Cochez la case pour utiliser les numéros de ports standard pour les serveurs Telnet et HTTP.

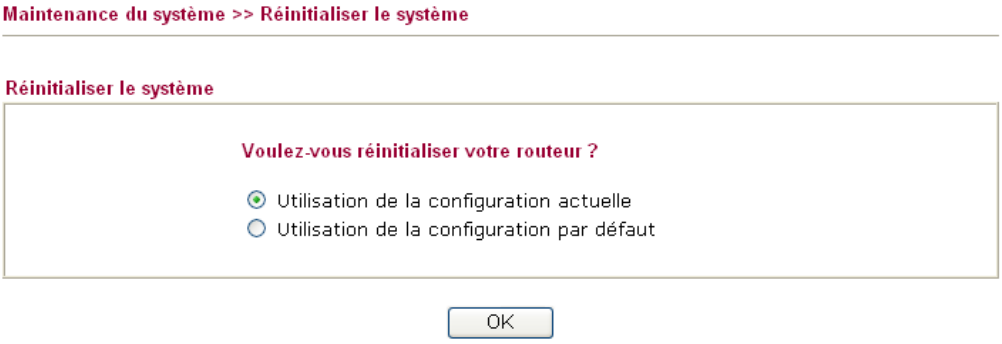
Ports définis par l'utilisateur — Cochez la case pour spécifier des numéros de port définis par l'utilisateur pour les serveurs Telnet, HTTP, HTTPS, FTP.

Activer l'agent SNMP — Cochez la case pour activer cette fonction.

Communauté pour GET	Nom que l'agent SNMP a utilisé pour exécuter l'action « Get ». La valeur par défaut est « public ».
Communauté pour SET	Tapez un nom approprié. Le nom par défaut est **privé.**
Adr IP du gestionnaire	Spécifiez un hôte comme gestionnaire pour l'exécution de la fonction SNMP. Tapez l'adresse IP de cet hôte.
Communauté notifiée	Tapez un nom approprié. Le nom par défaut est **public.**
Adr IP de notification	Adresse IP de l'hôte qui recevra la notification.
Temporisation des « traps »	La temporisation par défaut est de 10 secondes.

3.14.7 Réinitialisation du système

Le configurateur web peut être utilisé pour redémarrer votre routeur. Cliquez sur **Réinitialisation du système** dans le menu **Maintenance du système** pour ouvrir la page suivante.



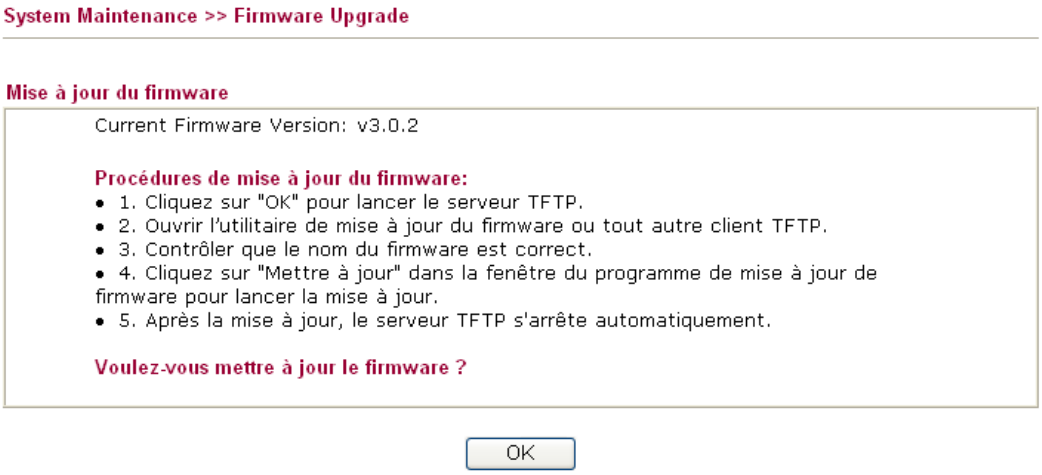
Si vous voulez réinitialiser le routeur avec la configuration courante, cochez **Utiliser la configuration courante** et cliquez sur **OK**. Pour rétablir les paramètres par défaut du routeur, cochez **Utiliser la configuration par défaut** et cliquez sur **OK**. La réinitialisation prend 5 secondes.

3.14.8 Mise à jour du firmware

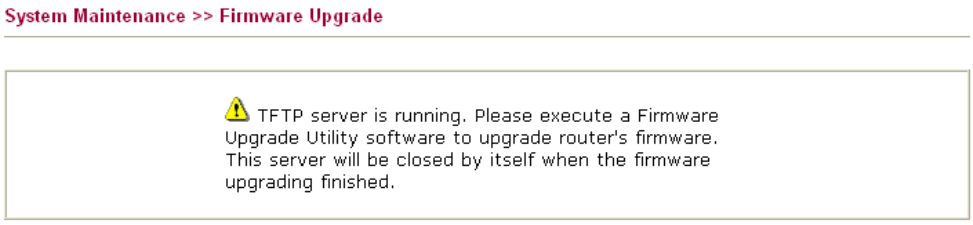
Avant de mettre à jour le firmware de votre routeur, vous devez installez les Router Tools. Les outils du routeur comprennent **l'utilitaire de mise à jour du Firmware (Firmware Upgrade Utility)**. La page web suivante vous explique comment mettre à jour le firmware à l'aide d'un exemple. Cet exemple vaut pour le système d'exploitation Windows.

Vous trouverez la dernière version du firmware sur le site web ou FTP de DrayTek. L'adresse du site web de DrayTek est www.draytek.com (ou l'adresse du site web local de DrayTek) et l'adresse du site FTP est ftp.draytek.com.

Cliquez sur **Maintenance du système>> Mise à jour du firmware** pour lancer l'utilitaire de mise à jour du firmware.



Cliquez sur **OK**. L'écran suivant apparaît. Exécutez d'abord l'utilitaire de mise à jour du firmware.



Pour plus de détails sur les mises à jour du firmware, reportez-vous au Chapitre 4.

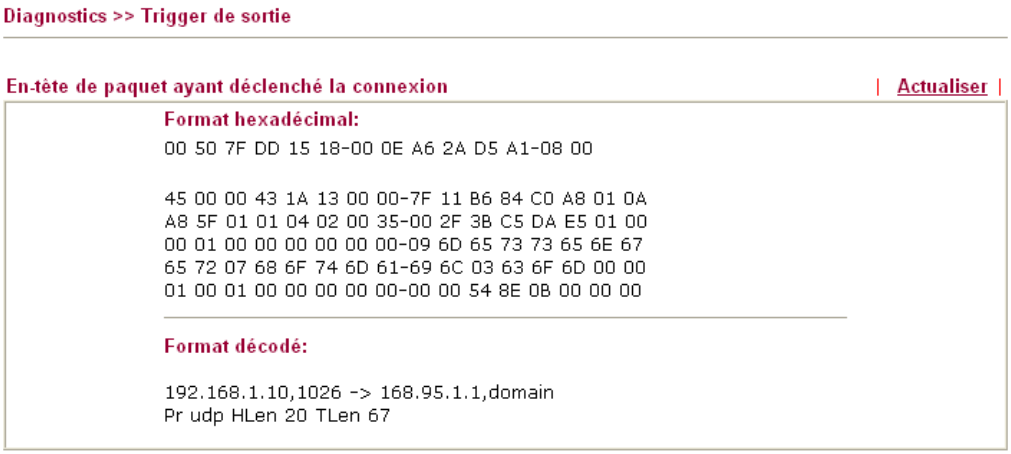
3.15 Diagnostics

Les outils de diagnostic vous permettent de visualiser ou de diagnostiquer l'état de votre routeur Vigor.

Les options du menu Diagnostics sont les suivantes :

3.15.1 Déclenchement de la connexion

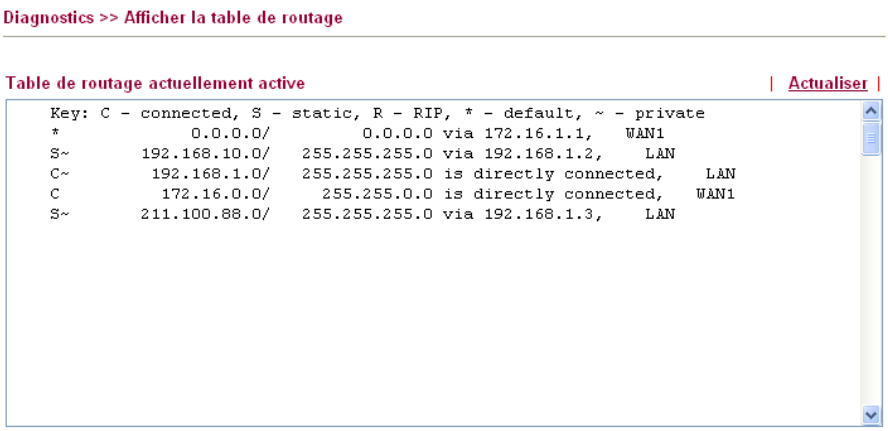
Cliquez sur **Diagnostics,** puis sur **Déclenchement de la connexion** pour ouvrir la page web. La connexion internet (RNIS, PPPoE, PPPoA, etc.) est déclenchée par un paquet provenant de l'adresse IP source.



Format décodé	Affiche l'adresse IP (locale), l'adresse IP de destination (distante), le protocole et la longueur du paquet.
Actualiser	Cliquez sur ce lien pour recharger la page.

3.15.2 Table de routage

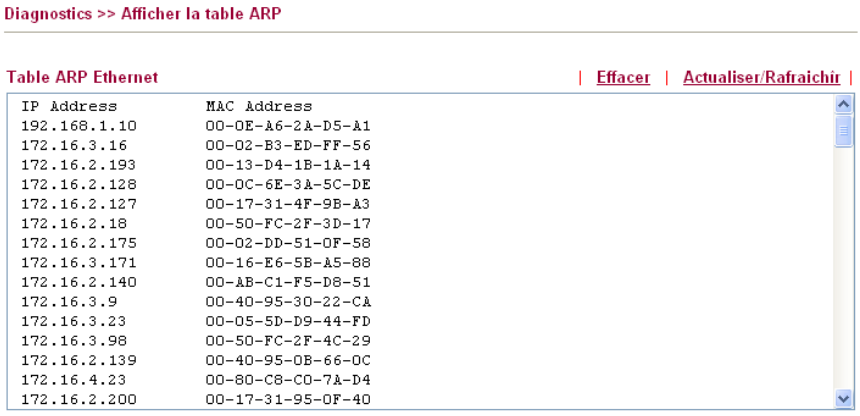
Cliquez sur **Diagnostics,** puis sur **Table de routage** pour ouvrir la page web.



Actualiser	Cliquez sur ce lien pour recharger la page.

3.15.3 Table de cache ARP (protocole de résolution d'adresse)

Cliquez **Diagnostics,** puis sur **Table de cache ARP** pour visualiser le contenu du cache ARP du routeur. La table affiche la correspondance entre une adresse matérielle Éthernet (adresse MAC) et une adresse IP.

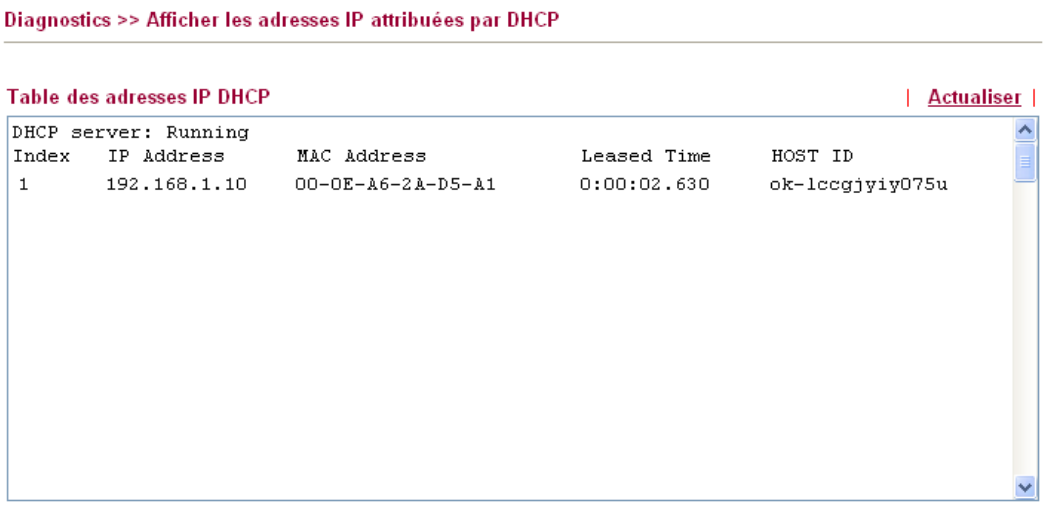


Actualiser	Cliquez sur ce lien pour recharger la page.
Effacer	Cliquez sur ce lien pour effacer complètement la table.

3.15.4 Table DHCP

Cette fonction fournit des informations sur les adresses IP attribuées. Ces informations sont utiles pour diagnostiquer les problèmes de réseau, comme les conflits d'adresse IP, etc.

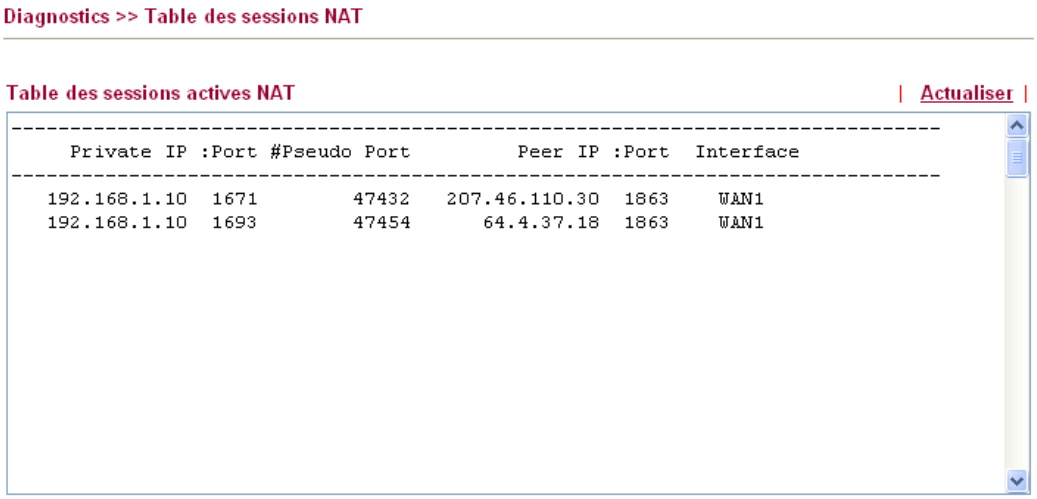
Cliquez sur **Diagnostics,** puis sur **Table DHCP** pour ouvrir la page web.



Index	Affiche le numéro de connexion.
Adresse IP	Affiche l'adresse IP attribuée par ce routeur à un PC spécifié.
Adresse MAC	Affiche l'adresse MAC du PC spécifié auquel a été attribuée une adresse IP par DHCP.
Durée du bail	Affiche la durée du bail du PC spécifié.
ID hôte	Affiche l'identifiant d'hôte du PC spécifié.
Actualiser	Cliquez sur ce lien pour recharger la page.

3.15.5 Table des sessions actives NAT

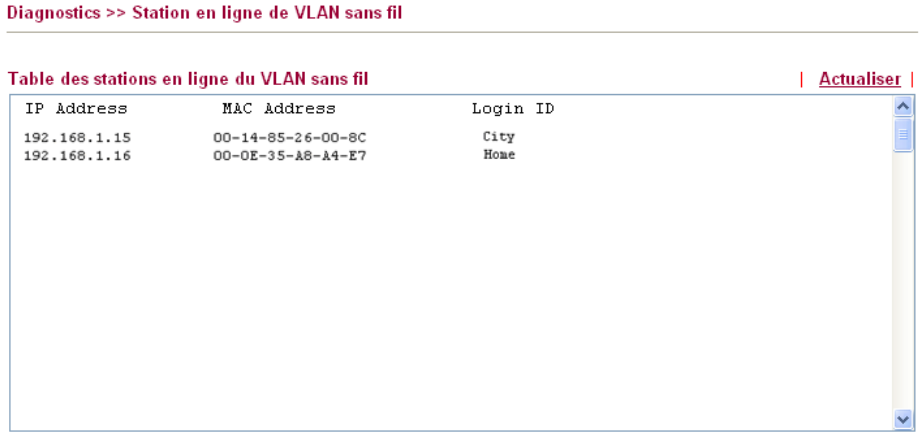
Cliquez sur **Diagnostics,** puis sur **Table des sessions active NAT** pour ouvrir la page de paramétrage.



Adr. IP :port privés	Indique l'adresse IP source et le port du PC local.
#Pseudo-port	Indique le port temporaire du routeur utilisé pour la fonction NAT.
Adr. IP :port homologue	Indique l'adresse IP de destination et le port de l'hôte distant.
Ifno	Affiche le numéro représentatif de différentes interfaces. 0: LAN 1~2: ISDN 3: WAN 4 ou above : VPN
État	Les valeurs d'état sont les suivantes : 0: autre état TCP 1: TCP fin incoming 2: TCP fin out 3: TCP fin closing 4: TCP syn 5: TCP syn,ack 6: TCP ack
Actualiser	Cliquez sur ce lien pour recharger la page.

3.15.6 Table des stations en ligne du VLAN sans fil

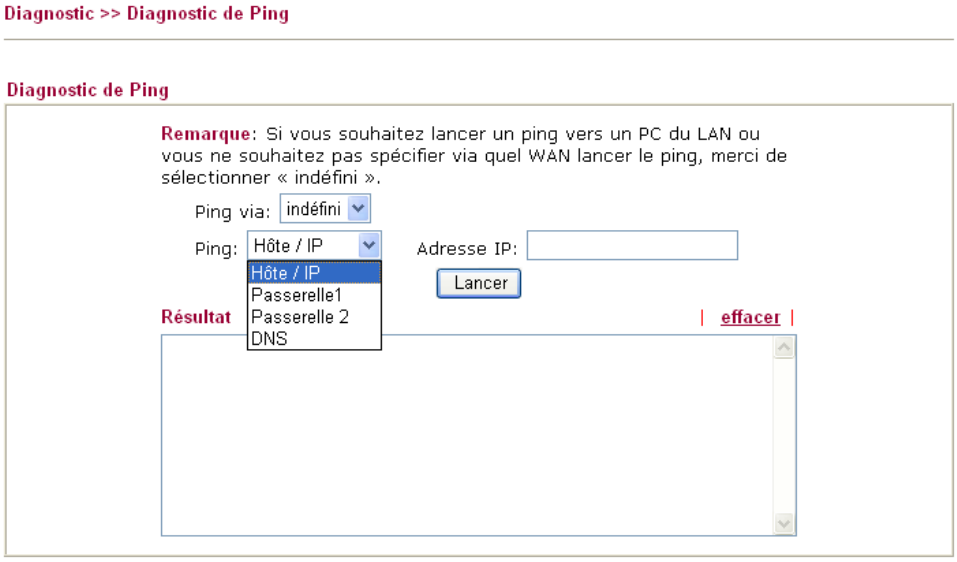
Cliquez sur l'option **Table des stations en ligne du VLAN sans fil** du menu **Diagnostics** pour ouvrir la page web suivante qui affiche l'adresse IP, l'adresse MAC et le nom d'utilisateur de toutes les stations VLAN sans fil.



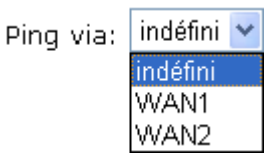
Adresse IP	Affiche l'adresse IP de la station sans fil.
Adresse MAC	Affiche l'adresse MAC de la station sans fil.
Nom d'utilisateur	Affiche le nom d'utilisateur auquel la station sans fil est rattachée.

3.15.7 Diagnostic par « ping »

Cliquez sur l'option **Diagnostic par ping** du menu **Diagnostics.** La page suivante apparaît.



Ping via	Utilisez la liste déroulante pour choisir l'interface WAN via laquelle vous voulez envoyer le « ping » ou choisissez **Non spécifié** pour que le routeur la détermine automatiquement.

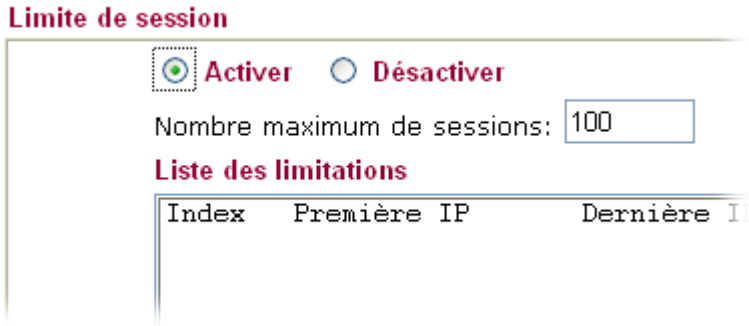


Ping vers	Choisissez la destination du ping dans la liste déroulante.

Adresse IP	Tapez l'adresse IP de l'hôte/IP auquel vous voulez envoyer le ping.
Exécuter	Cliquez sur ce bouton pour envoyer le ping. Le résultat est affiché sur l'écran.
Effacer	Cliquez sur ce lien pour effacer le résultat.

3.15.8 Surveillance des flux de données

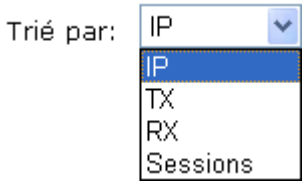
Cette page affiche le déroulement du processus de surveillance et permet de définir une fréquence d'actualisation des données. Les adresses IP de cet écran sont configurées dans la gestion de la bande passante. Vous devez définir une limitation de la bande passante IP et une limitation des sessions IP avant d'activer la surveillance. Sinon, une boîte de dialogue apparaît pour vous inviter à le faire.



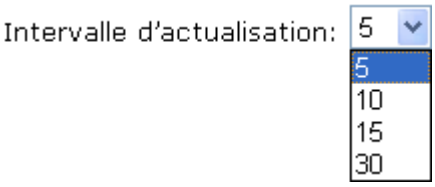
Cliquez sur l'option **Surveillance des flux de données** du menu **Diagnostics** pour ouvrir la page web suivante.

Activer la surveillance des flux de données	Cochez cette case pour activer cette fonction.

Ordonner par Utilisez la liste déroulante pour choisir un critère de tri des données.



Fréquence d'actualisation Utilisez la liste déroulante pour choisir la fréquence d'actualisation des données.



Actualiser Cliquez sur ce lien pour actualiser manuellement la page.

Index Affiche un numéro d'ordre.

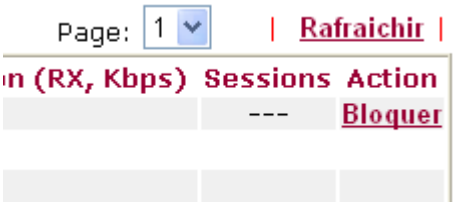
Adresse IP Affiche l'adresse IP de l'équipement surveillé.

Débit d'émission (kbit/s) Affiche la vitesse d'émission de l'équipement surveillé.

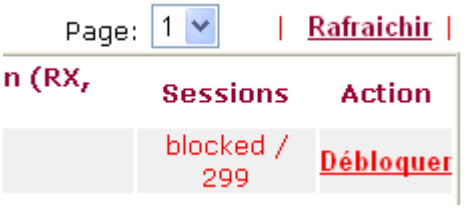
Débit de réception (kbit/s) Affiche la vitesse de réception de l'équipement surveillé.

Sessions Affiche le nombre de sessions spécifiées dans la page Limitation des sessions.

Action **Bloquer** – Empêche le PC spécifié d'accéder à l'internet pendant 5 minutes.

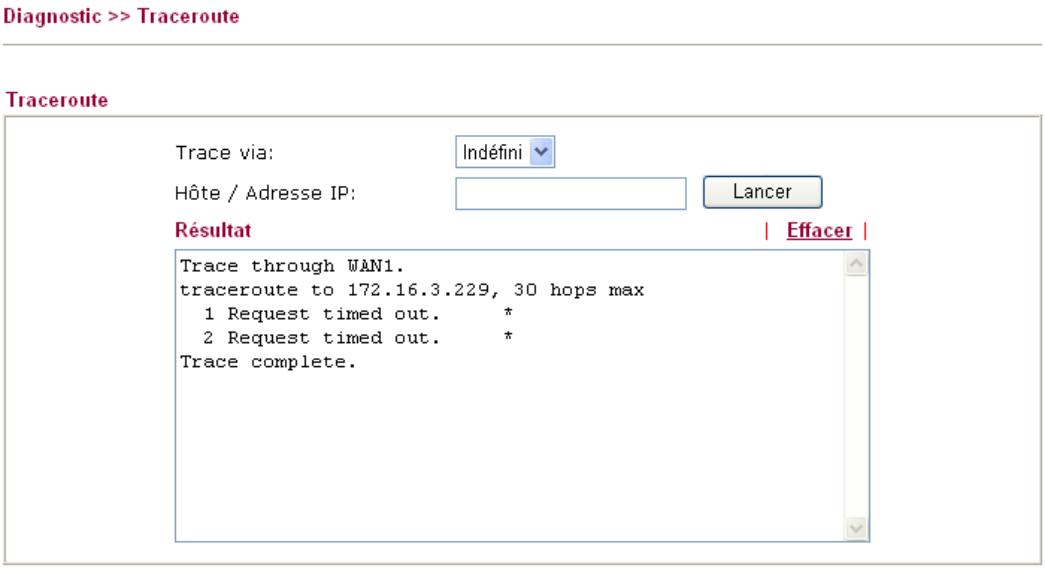


Débloquer – L'équipement spécifié sera débloqué dans cinq minutes. Le temps restant est affiché dans la colonne Sessions.



3.15.9 Trace route

Cliquez sur l'option **Trace route** du menu **Diagnostics** pour ouvrir la page web suivante. Cette page vous permet de retracer le chemin parcouru par les informations du routeur jusqu'à l'hôte. Tapez l'adresse IP de l'hôte dans la zone de saisie et cliquez sur **Exécuter**. Le résultat est affiché sur l'écran.

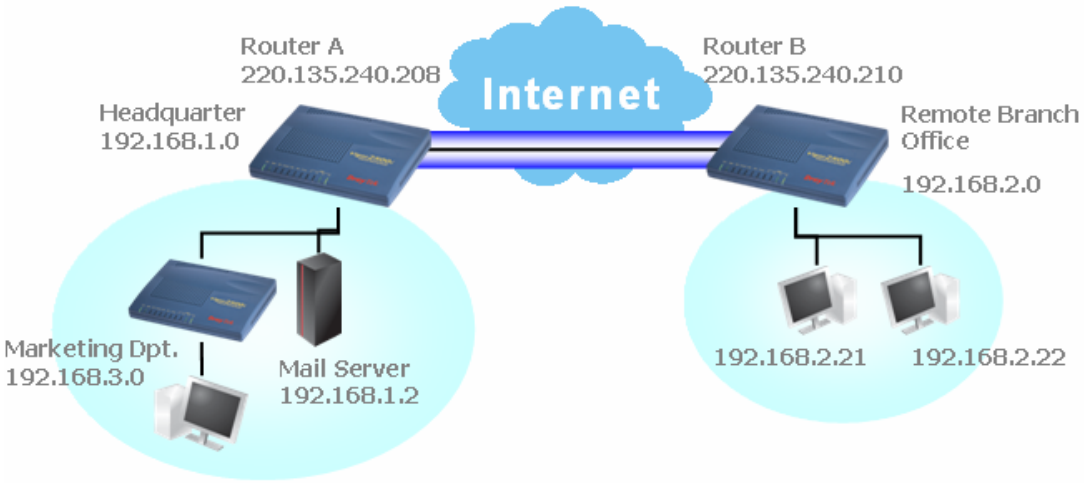


Trace via	Utilisez la lite déroulante pour choisir une interface WAN ou choisissez **Non spécifié** pour que cette interface soit déterminée automatiquement par le routeur.
Hôte/adresse IP	Adresse IP de l'hôte
Exécuter	Cliquez sur ce bouton pour lancer l'opération « trace route ».
Effacer	Cliquez sur ce lien pour effacer le résultat.

4 Application et exemples

4.1 Création d'une interconnexion de LAN entre un établissement secondaire et le siège

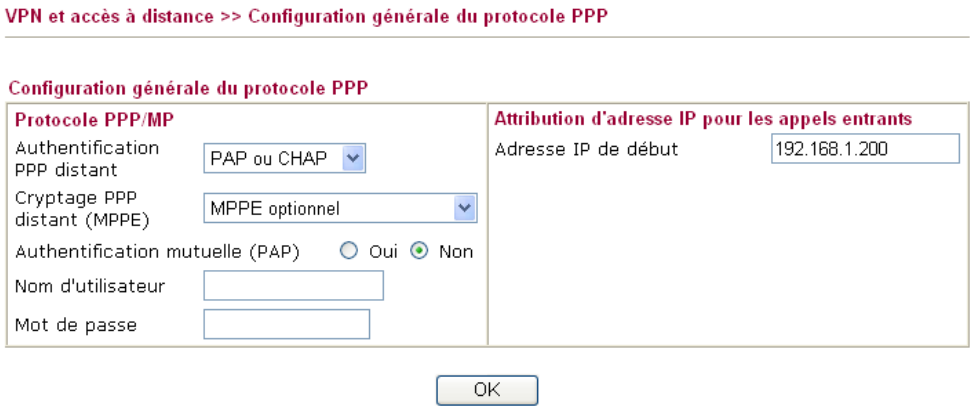
Vous pouvez vouloir établir une connexion sécurisée entre un établissement secondaire et le siège. Selon la structure de réseau illustrée ci-dessous, créez un profil d'interconnexion de LAN. Les deux réseaux (LAN) ne doivent pas avoir la même adresse réseau.



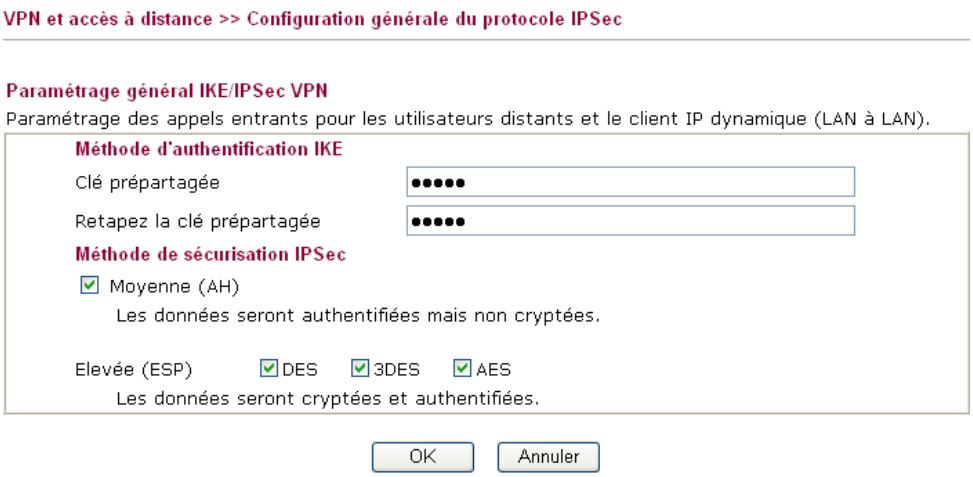
Router A	*Routeur A*
Router B	*Routeur B*
Headquarter	*Siège*
Remote Branch Office	*Établissement secondaire*
Marketing Dpt.	*Service marketing*
Mail Server	*Serveur de messagerie*

Paramétrage du routeur A au siège :

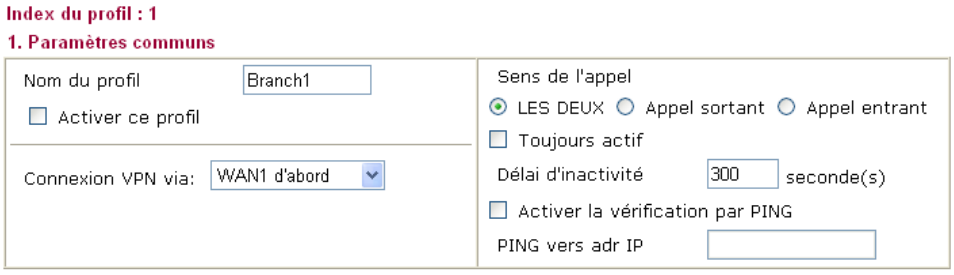
1. Sélectionnez l'option contrôle d'accès à distance du menu **VPN et accès à distance** pour activer le service de VPN nécessaire et cliquez sur **OK**.
2. Puis,
   Pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP.**



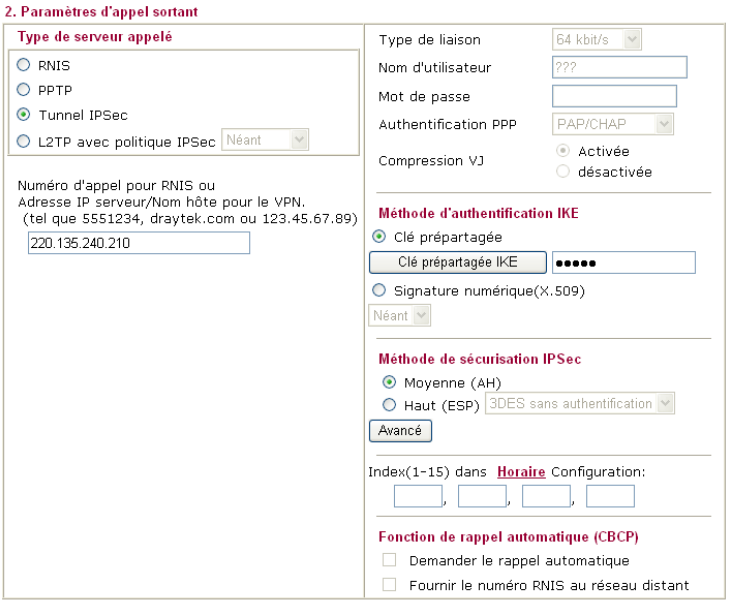
Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la clé prépartagée connue des deux correspondants.



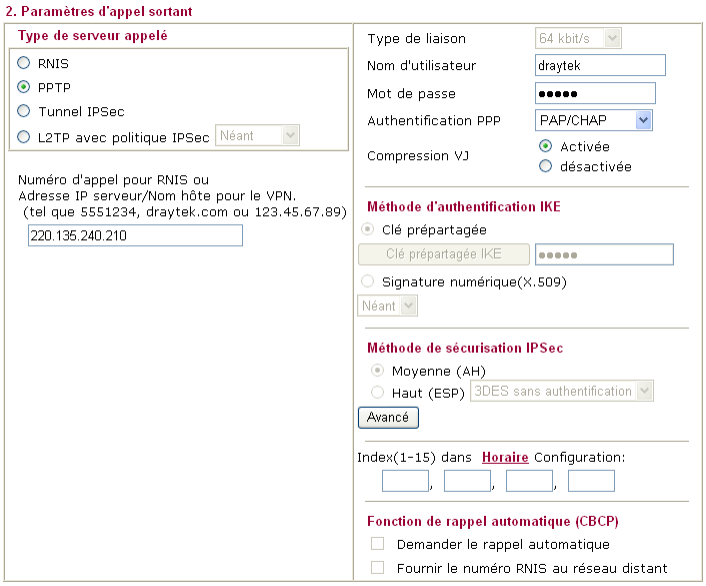
3. Sélectionnez **LAN à LAN**. Cliquez sur un numéro d'index pour éditer un profil.
4. Définissez les **Paramètres communs** comme indiqué ci-dessous. Il faut activer les deux connexions de VPN car n'importe lequel des correspondants peut déclencher la connexion de VPN.



5. Définissez les **paramètres d'appel sortant** pour vous connecter en mode agressif au routeur B avec la méthode d'appel sortant sélectionnée.
Si un service **basé sur IPSec** est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion sortante.

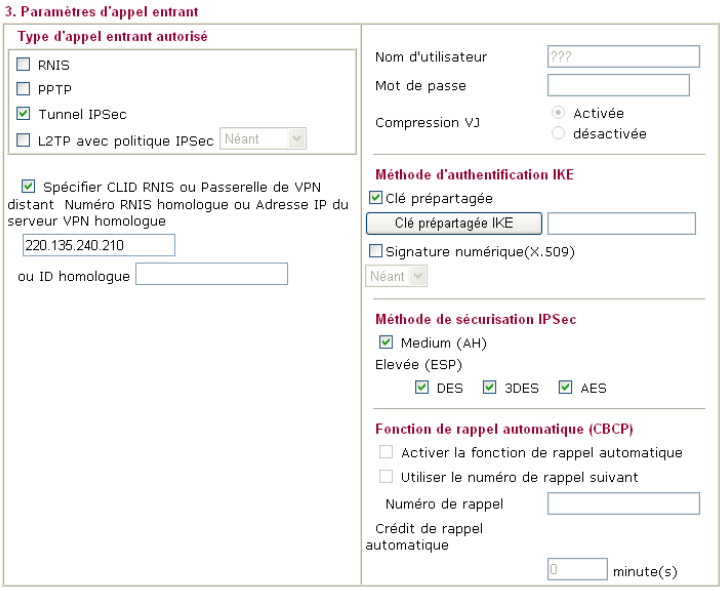


Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP de l'homologue distant, le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ pour cette connexion sortante.

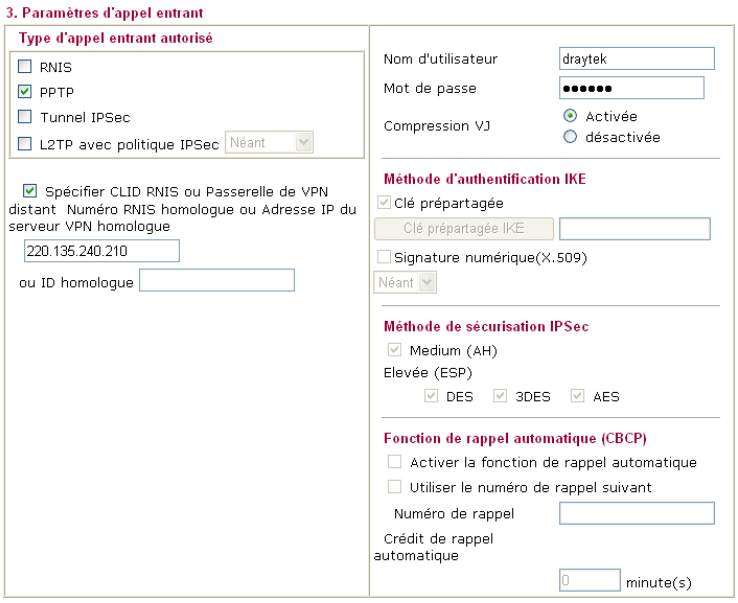


6. Définissez les paramètres d'appel entrant pour permettre au routeur B d'appeler la connexion de VPN.

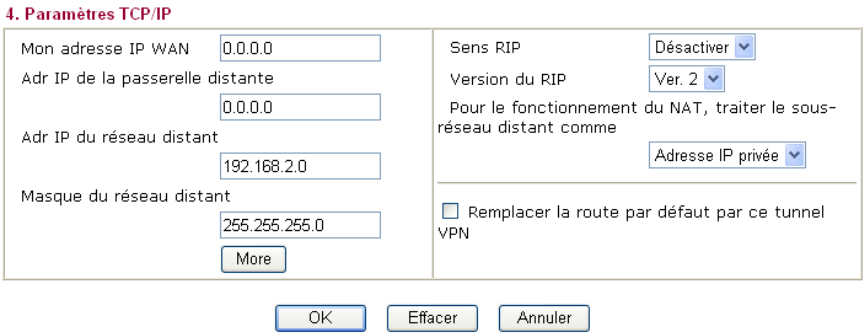
   Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion entrante. Autrement, les **paramètres généraux IPSec** seront appliqué.



Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.

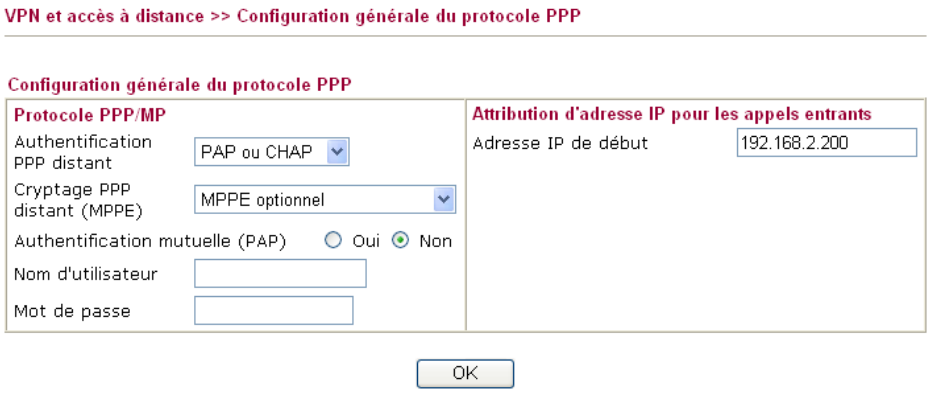


7. Enfin, spécifiez l'adresse IP de réseau distant et le sous-réseau dans les **Paramètres de réseau TCP/IP** pour que le routeur A puisse aiguiller les paquets destinés au réseau distant vers le routeur B via la connexion de VPN.

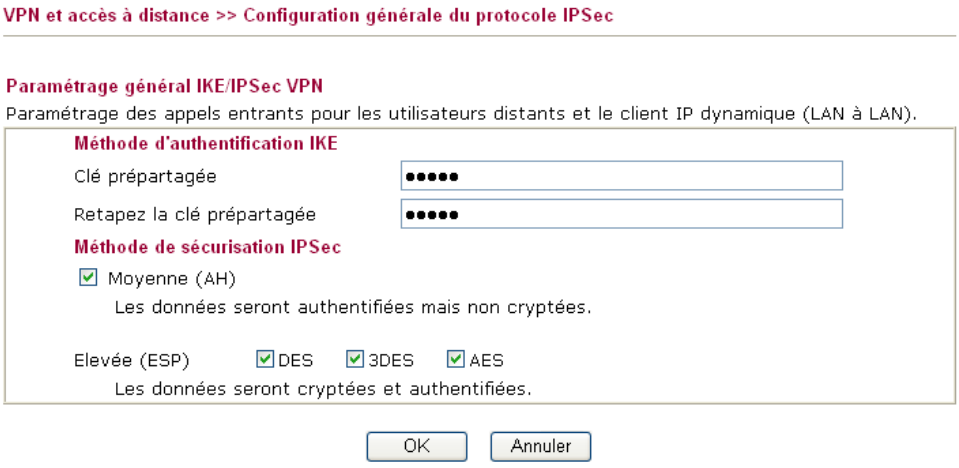


Paramétrage du routeur B de l'établissement secondaire :

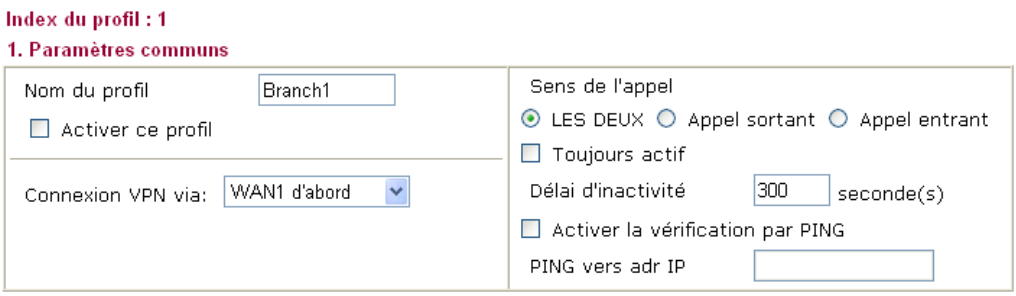
1. Sélectionnez l'option contrôle d'accès à distance du menu **VPN et accès à distance** pour activer le service de VPN nécessaire et cliquez sur **OK**.
2. Puis, pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP**.



Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la clé prépartagée connue des deux correspondants.



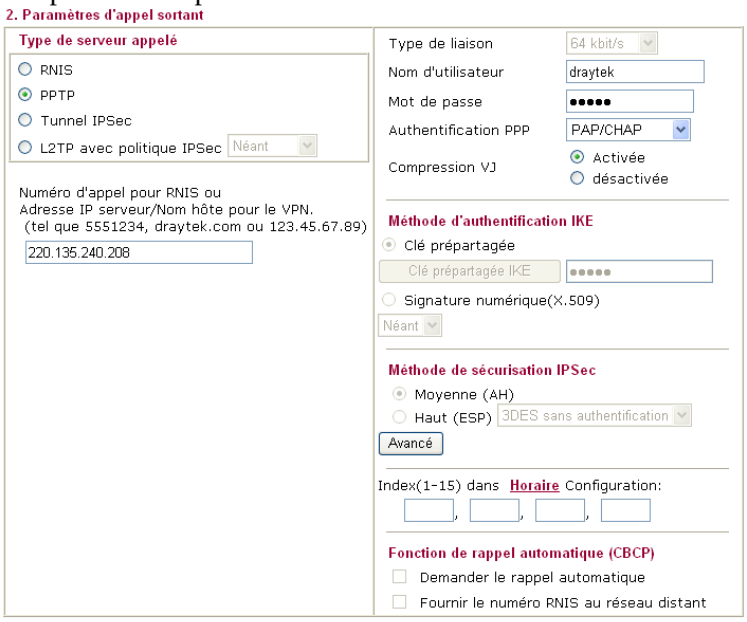
3. Sélectionnez **LAN à LAN**. Cliquez sur un numéro d'index pour éditer un profil.
4. Définissez les **Paramètres communs** comme indiqué ci-dessous. Il faut activer les deux connexions de VPN car n'importe lequel des correspondants peut déclencher la connexion de VPN.



5. Définissez les paramètres d'appel sortant pour vous connecter en mode agressif au routeur B avec la méthode d'appel sortant sélectionnée.

   Si un service basé sur IPSec est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion sortante.

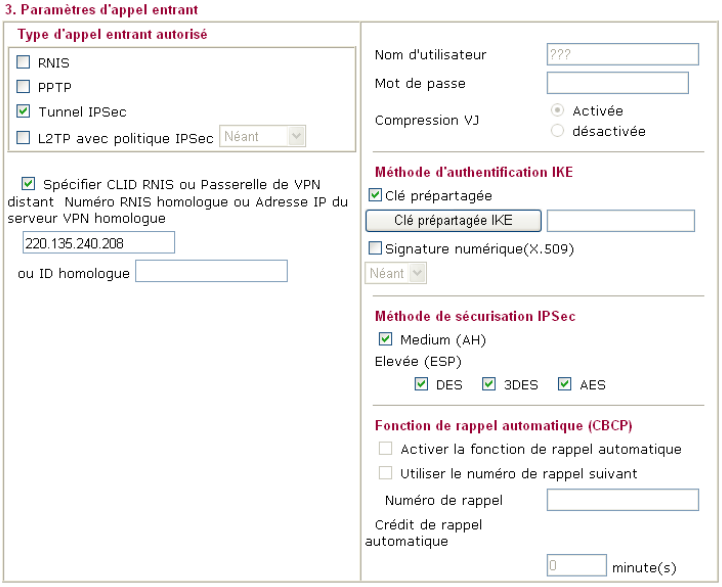
   Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP de l'homologue distant, le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ pour cette connexion sortante.



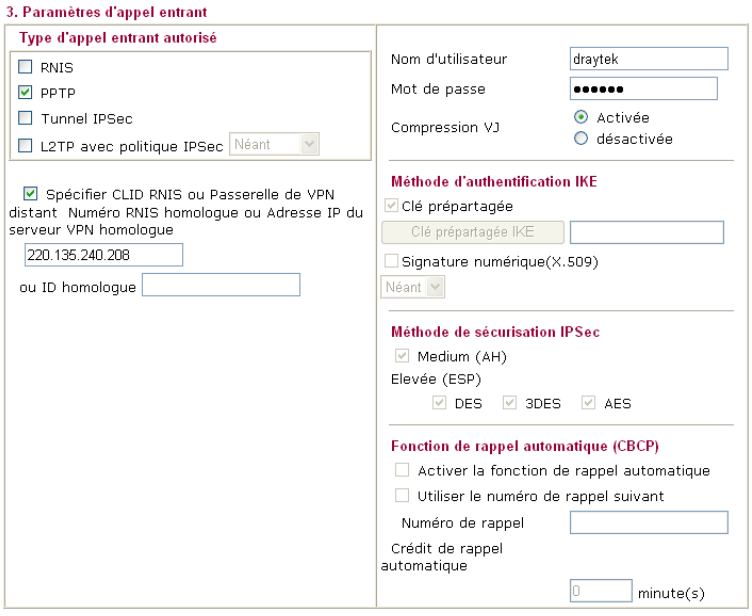
6. Définissez les paramètres d'appel entrant pour permettre au routeur B d'appeler la connexion de VPN.

   Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion entrante. Autrement, les **paramètres généraux**

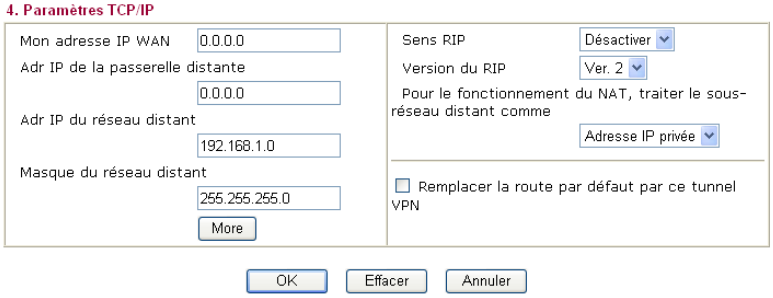
IPSec seront appliqués.



Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.

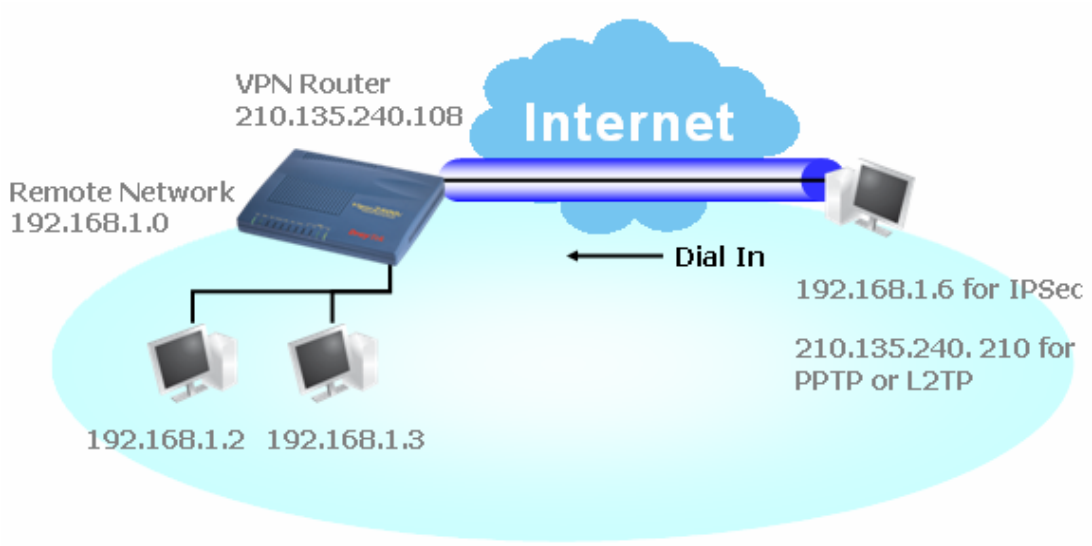


7. Enfin, spécifiez l'adresse IP de réseau distant et le sous-réseau dans les **Paramètres de réseau TCP/IP** pour que le routeur B puisse aiguiller les paquets destinés au réseau distant vers le routeur A via la connexion de VPN.



4.2 Création d'une connexion d'utilisateur distant entre télétravailleur et siège

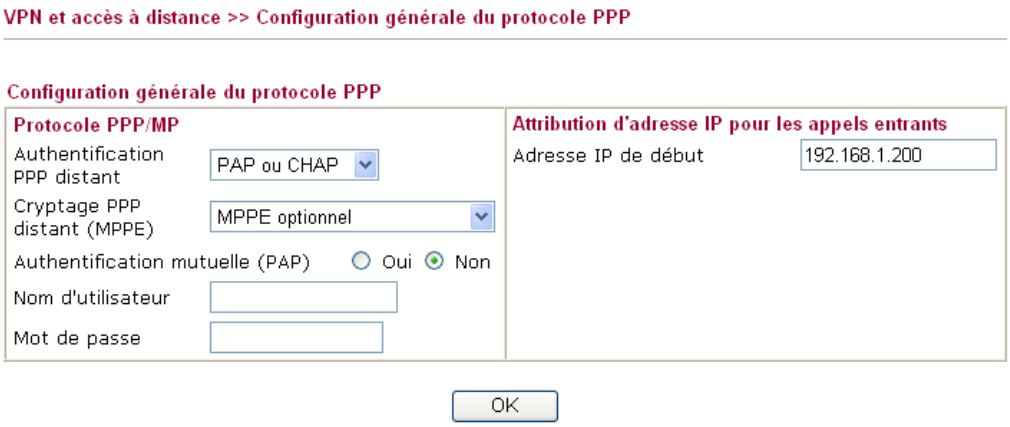
Autre cas courant, un télétravailleur veut se connecter au réseau d'entreprise en toute sécurité. Selon la structure de réseau, vous pouvez créer un profil d'utilisateur distant et installez le client de VPN intelligent sur l'hôte distant.



VPN Router	*Routeur de VPN*
Remote Network	*Réseau distant*
Dial In	*Appel entrant*
192.168.1.6 for IPSec	*192.168.1.6 pour IPSec*
210.135.240.210 for PPTP or L2TP	*210.135.240.210 pour PPTP ou L2TP*

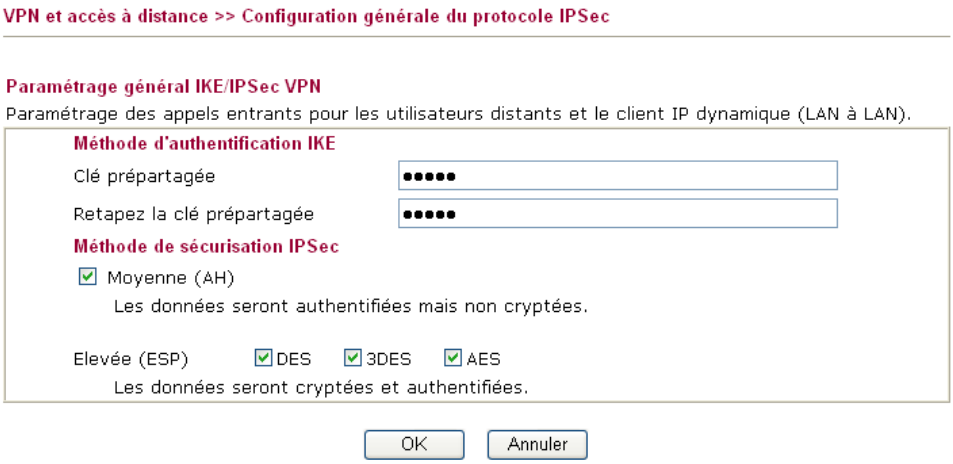
Paramétrage du routeur de VPN au siège :

1. Sélectionnez l'option contrôle d'accès à distance du menu **VPN et accès à distance** pour activer le service de VPN nécessaire et cliquez sur **OK**.
2. Puis, pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP**.



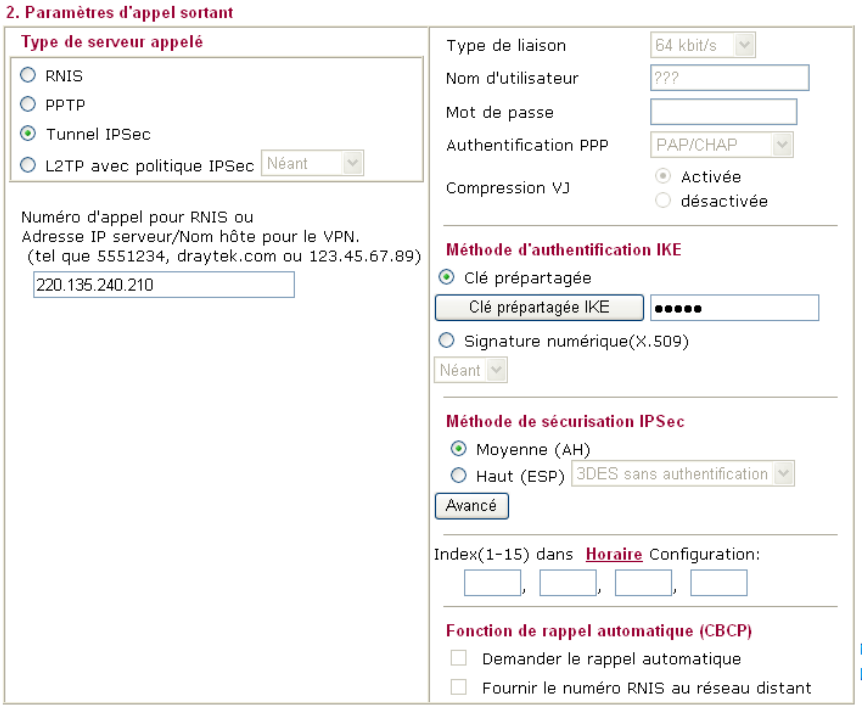
Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la

clé prépartagée connue des deux correspondants.

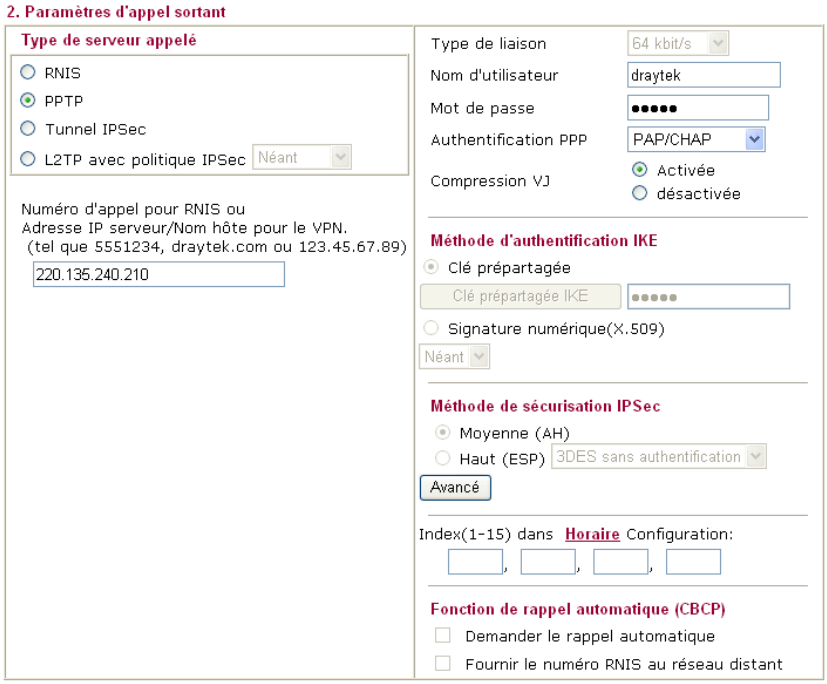


3. Sélectionnez **Comptes d'appel entrant**. Cliquez sur un numéro d'index pour éditer un profil.
4. Définissez les paramètres d'appel entrant pour permettre à l'utilisateur distant d'établir la connexion de VPN.

   Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion entrante. Autrement, les **paramètres généraux IPSec** seront appliqués.



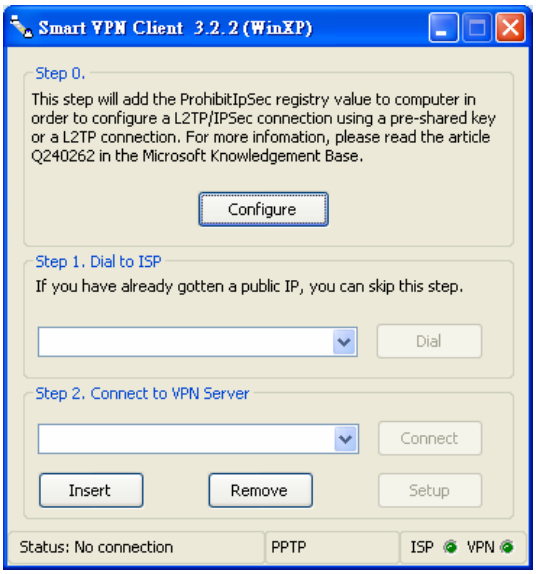
   Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.



Paramétrage de l'hôte distant :

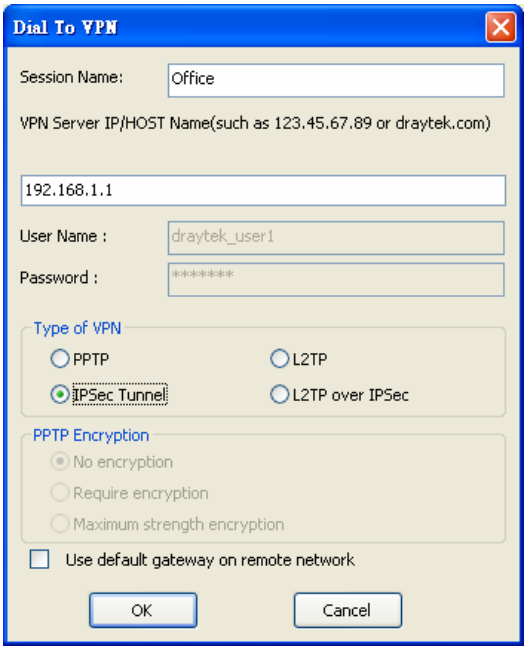
1. Dans le cas de Win98/ME, vous pouvez utiliser « Accès réseau à distance » pour créer le tunnel PPTP vers le routeur Vigor. Dans le cas de Win2000/XP, utilisez « Network and Dial-up connections » ou « Smart VPN Client » pour vous aider à créer un tunnel pour PPTP, L2TP et L2TP sur IPSec. Vous trouverez ce logiciel complémentaire sur le CD-ROM ou au centre de téléchargement www.draytek.com. Procédez à l'installation en suivant les instructions.

2. Après l'installation, vous devez cliquer sur le bouton **Étape 0. Configurer**. Redémarrez l'hôte.

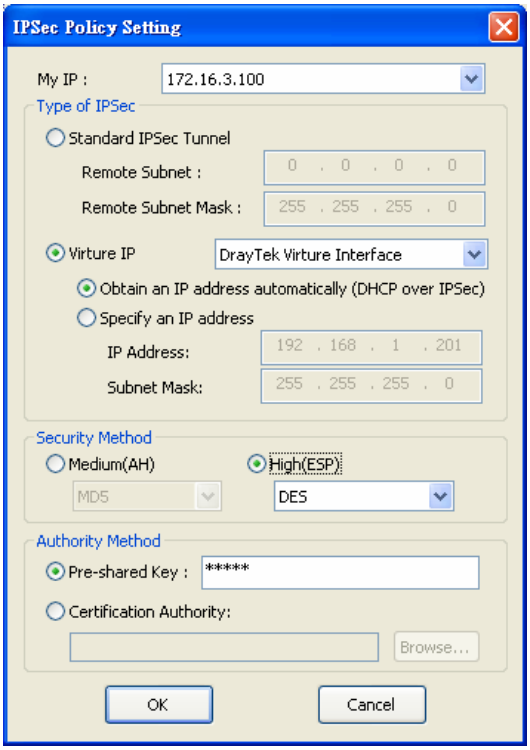


3. Dans l'**Étape 2. Se connecter au serveur de VPN**, cliquez sur le bouton **Insérer** pour ajouter une nouvelle entrée.

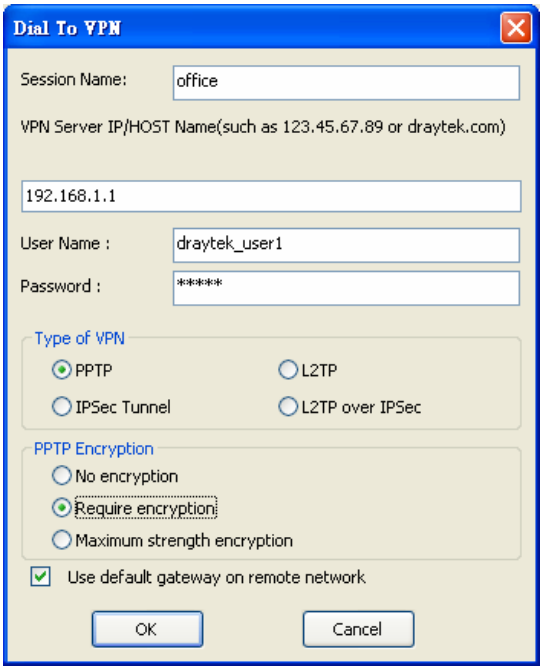
   Si un service basé sur IPSec est sélectionné comme indiqué ci-dessous,



Vous pouvez également spécifier la méthode que vous utilisez pour obtenir l'adresse IP, la méthode de sécurisation et la méthode d'authentification. Si la clé prépartagée est sélectionnée, elle doit concorder avec celle paramétrée dans le routeur de VPN.



Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP du serveur de VPN distant, le nom de l'utilisateur, le mot de passe et la méthode de cryptage. Le nom d'utilisateur et le mot de passe doivent concorder avec ceux paramétrés dans le routeur de VPN. Si vous utilisez la passerelle par défaut sur le réseau distant, tous les paquets de l'hôte distant seront aiguillés vers le serveur de VPN, puis transmis à l'internet. L'hôte distant semblera fonctionner au sein du réseau d'entreprise.

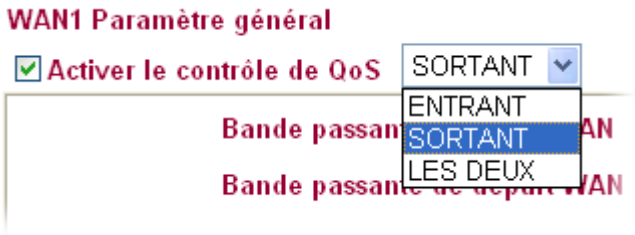


4. Cliquez sur le bouton **Se connecter** pour établir la connexion. Lorsque la connexion est établie, vous verrez un voyant vert dans l'angle inférieur droit.

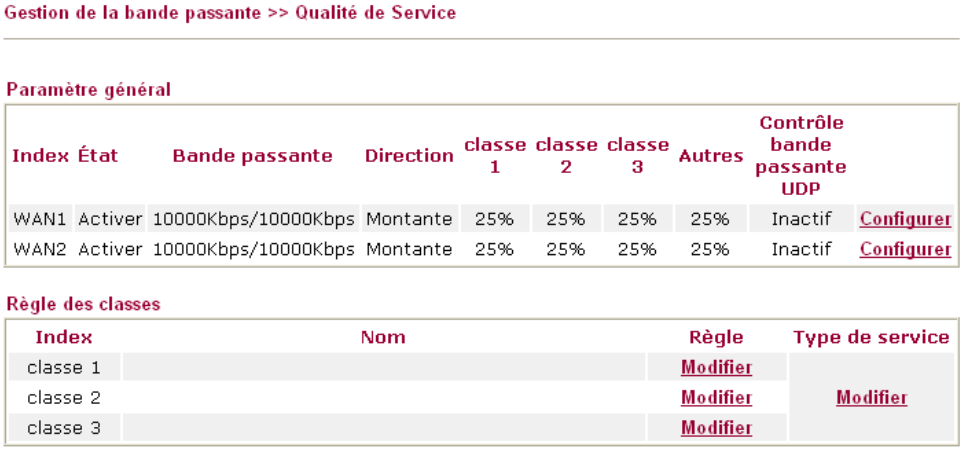
4.3 Exemple de paramétrage de la QoS

Supposons qu'un télétravailleur ou une télétravailleuse travaille à la maison et garde des enfants. Pendant son travail, il ou elle utilise le routeur Vigor à la maison pour se connecter au serveur de l'entreprise via HTTPS ou VPN pour lire ses courriels ou pour accéder à la base de données interne. Pendant ce temps, les enfants utilisent Skype au salon.

1. Vérifier que le contrôle de QoS est activé. Sélectionner LES DEUX pour **Sens**.



2. Cliquez sur le lien **Modifier** et tapez le nom de la classe 1. Vous allez définir la bande passante réservée pour la messagerie électronique utilisant le protocole POP3 et SMTP.



3. Cliquez sur le lien **Modifier** et tapez le nom de la classe 2. Vous allez définir la bande passante réservée pour HTTPS. Cliquer sur le bouton **Base** à droite.

4. Cliquez sur le lien **Paramétrage** pour WAN1. Cochez la case **Activer le contrôle de bande passante** UDP pour empêcher les autres applications d'être gênées par le trafic d'application UDP.

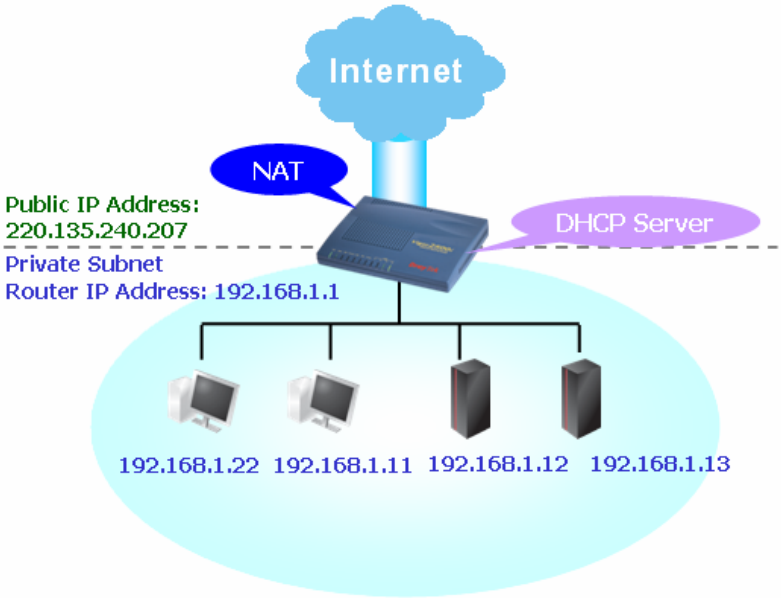
5. Si le télétravailleur ou la télétravailleuse s'est connectée au siège de l'entrepris à l'aide d'un tunnel de VPN (voir le Chapitre 3 VPN pour plus de détails), il ou elle peut configurer un index pour cette connexion. Il ou elle va entrer le nom de classe de l'index 3. Dans cet index, il ou elle va spécifier la bande passante réservée à un tunnel de VPN

Private network	*Réseau privé*
VPN tunnel	*Tunnel de VPN*
Cooperate network	*Réseau coopératif*

6. Cliquer sur Modifier pour ouvrir une nouvelle fenêtre. Cocher la case ACT, puis cliquer sur **SrcEdit** pour définir une adresse de sous-réseau. Cliquer sur **DestEdit** pour spécifier l'adresse de sous-réseau du siège. Laisser les autres champs et cliquer sur OK.

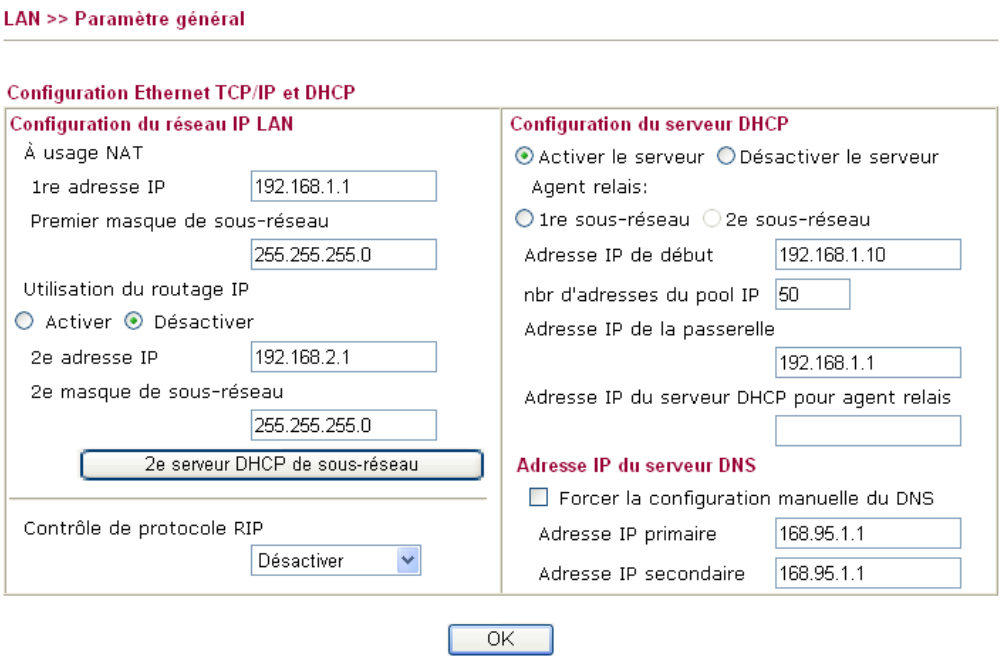
4.4 Création d'un LAN avec NAT

Un exemple de paramétrage par défaut avec la topologie correspondante est donné ci-dessous. Par défaut, le routeur Vigor a pour adresse IP privée 192.168.1.1 et comme masque de sous-réseau 255.255.255.0. Le serveur DHCP intégré est activé et attribue à chaque hôte NAT local une adresse IP 192.168.1.x à partir de 192.168.1.10.

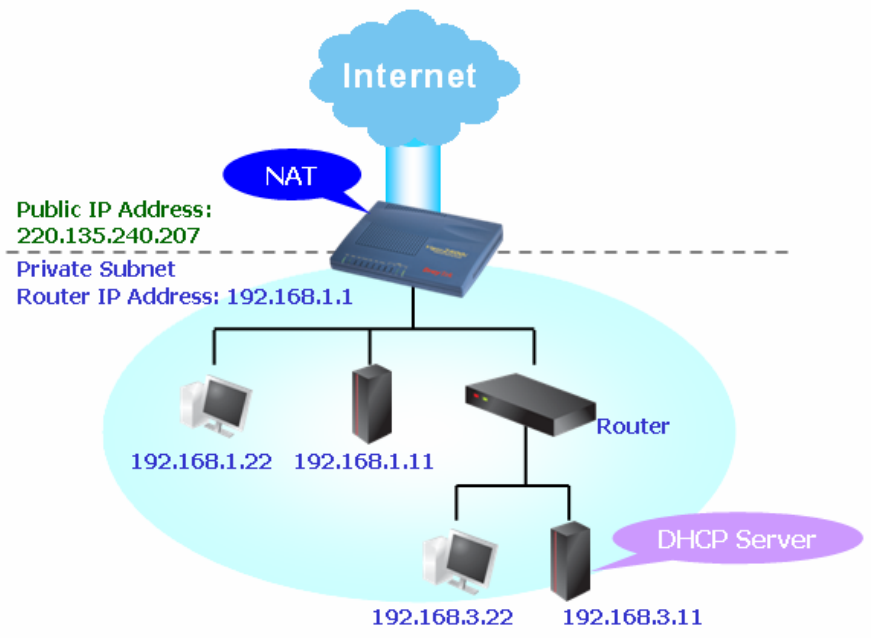


Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*

Vous pouvez adapter les paramètres à l'intérieur des rectangles rouge pour l'usage NAT.

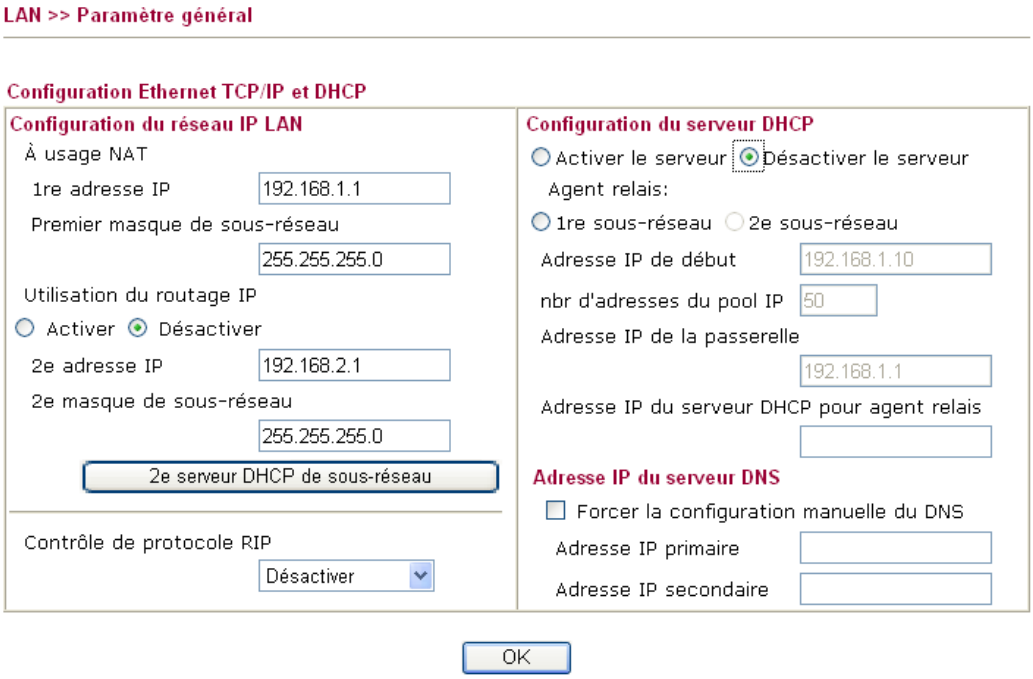


Pour utiliser un autre serveur DHCP du réseau à la place du serveur intégré au routeur Vigor, il vous faut modifier les paramètres comme indiqué ci-dessous.



Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*

Vous pouvez adapter les paramètres à l'intérieur des rectangles rouge pour l'usage NAT.


LAN >> Paramètre général
Configuration Ethernet TCP/IP et DHCP
Configuration du réseau IP LAN
À usage NAT
1re adresse IP
192.168.1.1
Premier masque de sous-réseau
255.255.255.0
Utilisation du routage IP
Activer
Désactiver
2e adresse IP
192.168.2.1
2e masque de sous-réseau
255.255.255.0
2e serveur DHCP de sous-réseau
Contrôle de protocole RIP
Désactiver
Configuration du serveur DHCP
Activer le serveur
Désactiver le serveur
Agent relais:
1re sous-réseau
2e sous-réseau
Adresse IP de début
192.168.1.10
nbr d'adresses du pool IP
50
Adresse IP de la passerelle
192.168.1.1
Adresse IP du serveur DHCP pour agent relais
Adresse IP du serveur DNS
Forcer la configuration manuelle du DNS
Adresse IP primaire
Adresse IP secondaire
OK

4.5 Scénario d'appel pour la fonction VoIP

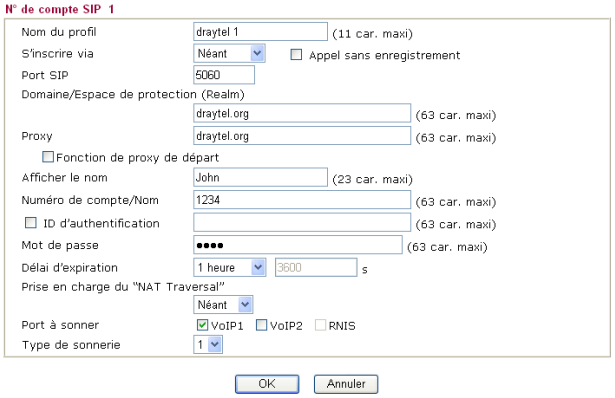
4.5.1 Appel via le serveur SIP

Exemple 1 : Jean et David ont une adresse IP provenant de fournisseurs de service différents.

URL SIP de Jean : 1234@draytel.org, URL SIP de David : 4321@iptel.org

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@iptel.org

Paramètres des comptes SIP ---
Nom du profil : draytel1
S'inscrire via : Auto
Port SIP : 5060 (valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy: draytel.org
Fonction de proxy de départ : non coché
Nom affiché : Jean
Numéro/nom de compte : 1234
ID authentification : non coché
Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)

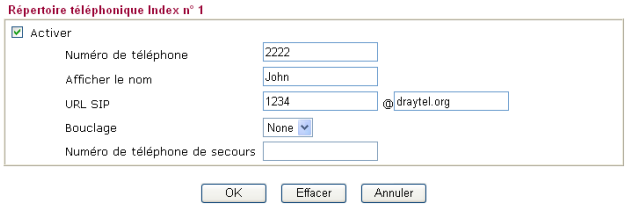


CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)

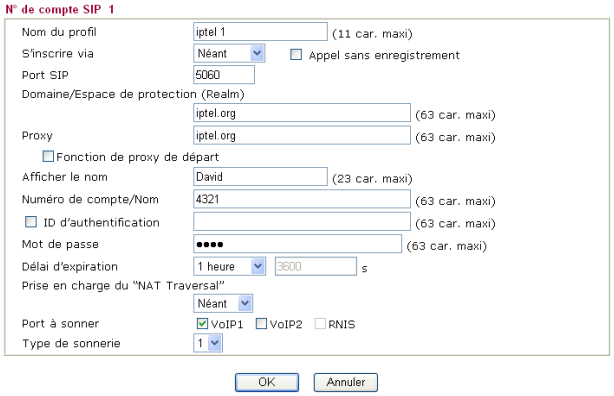
Jean appelle David ---

Il décroche le téléphone et compose **1111#**. (Numéro abrégé de David)

Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP :1234@draytel.org



Paramètres des comptes SIP ---
Nom du profil : iptel 1
S'inscrire via : Auto
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : iptel.org
Proxy : iptel.org
Fonction de proxy de départ : non coché
Nom affiché : David
Nom de compte : 4321
ID authentification : non coché
Mot de passe : ****
Délai d'expiration : (utiliser la



David appelle Jean

Il décroche le téléphone et compose 2222# (Numéro

valeur par défaut)

abrégé de Jean)

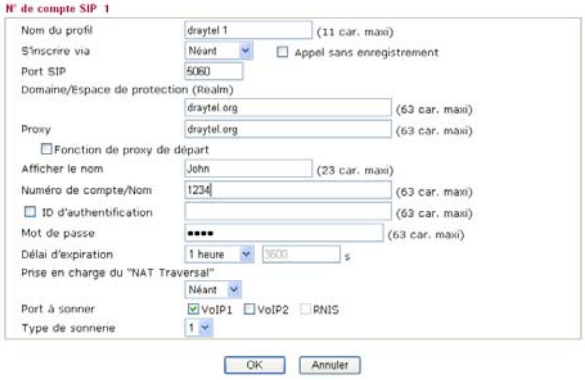
CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)

Exemple 2 : Jean et David ont une adresse IP provenant du même fournisseur de service.

URL SIP de Jean : 1234@draytel.org, URL SIP de David : 4321@draytel.org

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@iptel.org

Paramètres des comptes SIP ---
Nom du profil : draytel1
S'inscrire via : Auto
Port SIP : 5060 (valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy : draytel.org
Fonction de proxy de départ : non coché
Nom affiché : Jean
Numéro/nom de compte : 1234
ID authentification : non coché
Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)



CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)

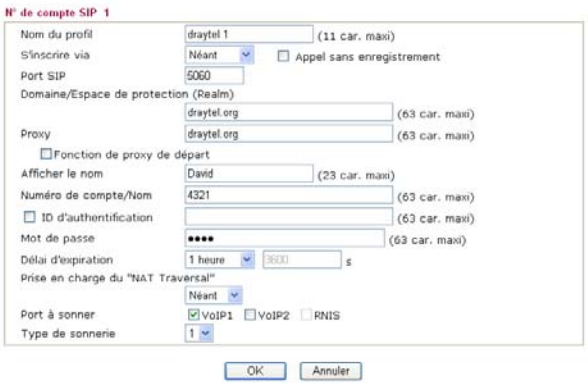
Jean appelle David

Il décroche le téléphone et compose **1111#**. (Numéro abrégé de David) Ou,

Il décroche le téléphone et compose **4321#**. (Nom de compte de David)

Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP :1234@draytel.org

Paramètres des comptes SIP ---
Nom du profil : iptel 1
S'inscrire via : Auto
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy : iptel.org
Fonction de proxy de départ : non coché
Nom affiché : David
Nom de compte : 4321
ID authentification : non coché
Mot de passe : ****
Délai d'expiration : (utiliser la



valeur par défaut)

CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)

David appelle Jean

Il décroche le téléphone et compose 2222# (Numéro abrégé de Jean) Ou,

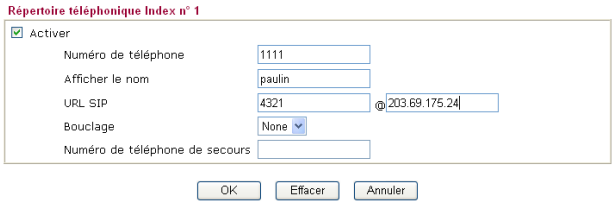
Il décroche le téléphone et compose 1234# (Nom de compte de Jean)

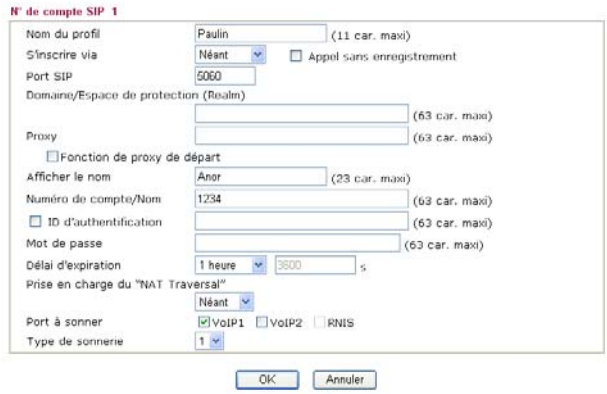
4.5.2 Communication d'homologue à homologue (P2P)

Exemple 3 : Jean et David ont chacun un routeur Vigor. Ils peuvent communiquer entre eux sans passer par un serveur registre SIP. Ils se communiquent au préalable leurs adresses IP respectives et attribuent un nom de compte au port qui sert à appeler.

URL SIP de Jean : 1234@214.61.172.53 URL SIP de David : 4321@ 203.69.175.24

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@ 203.69.175.24
Paramètres des comptes SIP ---
Nom du profil : David
S'inscrire via : Néant
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : (vide)
Proxy: (vide)
Fonction de proxy de départ : non coché
Nom affiché : Jean
Nom de compte : 1234
ID authentification : non coché
Mot de passe : (vide)
Délai d'expiration : (utiliser la valeur par défaut)



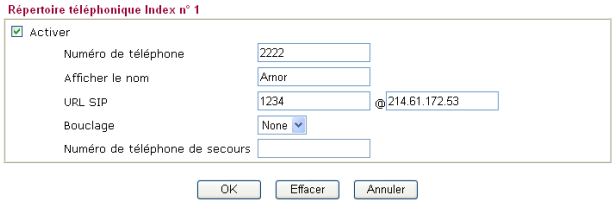


CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)

Jean appelle David

Il décroche le téléphone et compose **1111#**. (Numéro abrégé de David)

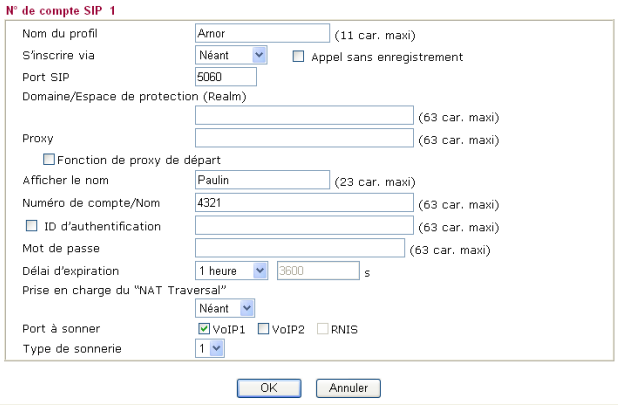
Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP: 1234@214.61.172.53



Paramètres des comptes SIP ---
Nom du profil : Jean
S'inscrire via : Néant
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : (vide)
Proxy: (vide)
Fonction de proxy de départ : non coché
Nom affiché : David

Nom de compte : 4321
ID authentification : non coché
Mot de passe : (vide)
Délai d'expiration : (utiliser la valeur par défaut)

CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)



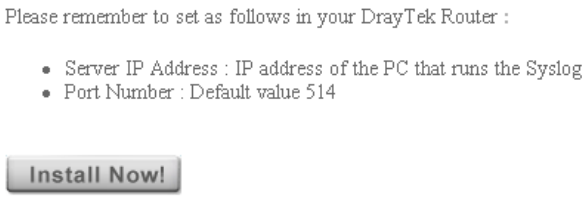
David appelle Jean

Il décroche le téléphone et compose 2222# (Numéro abrégé de Jean)

4.6 Mise à jour du firmware de votre routeur

Avant de mettre à jour le firmware de votre routeur, il vous faut installer les Router Tools. L'utilitaire de mise à jour du firmware fait partie des outils.

1. Mettez le CD du routeur dans votre lecteur de CD-ROM.
2. Sur la page web, cliquez sur le menu **Utility**.
3. Sur la page web Utility, cliquez sur **Install Now!** (sous la description SysLog) pour installer le programme correspondant.



4. Le fichier **RTSxxx.exe** est copié sur votre ordinateur. Rappelez-vous de l'endroit où est copié le fichier .exe.
5. Connectez-vous à **www.draytek.com** pour rechercher la version la plus récente du firmware de votre routeur.

6. Cliquez sur **Support Center >> Downloads**. Recherchez le modèle de votre routeur et cliquez sur le lien. La fenêtre ci-dessous apparaît.

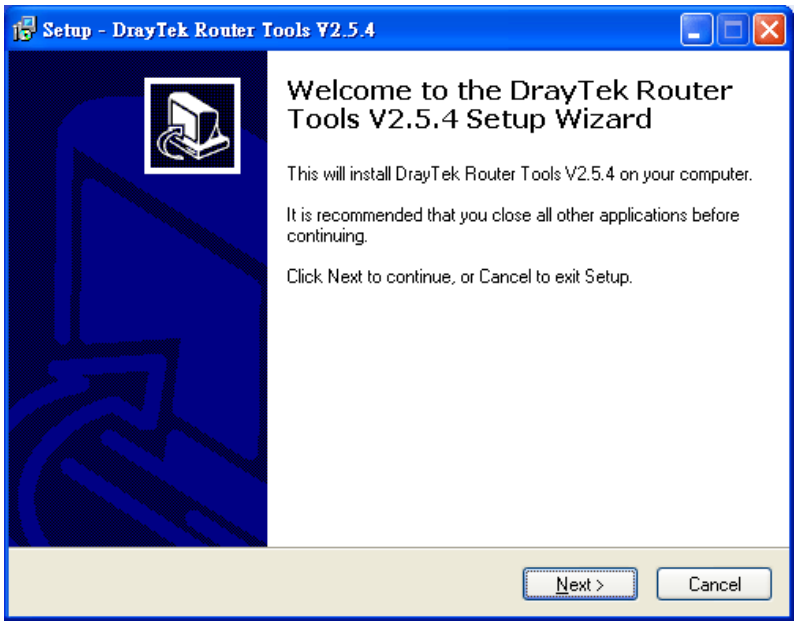
Note : Brief introduction for Tools

Tools of Vigor

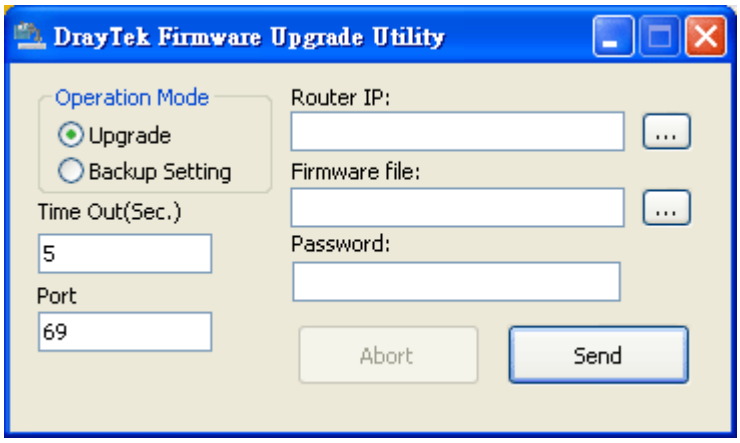
Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	hqx	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	hqx	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	zip	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	zip	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	zip	0.65 MB
LPR	1.0	English	20/06/2005	Windows	zip	0.54 MB

TOP

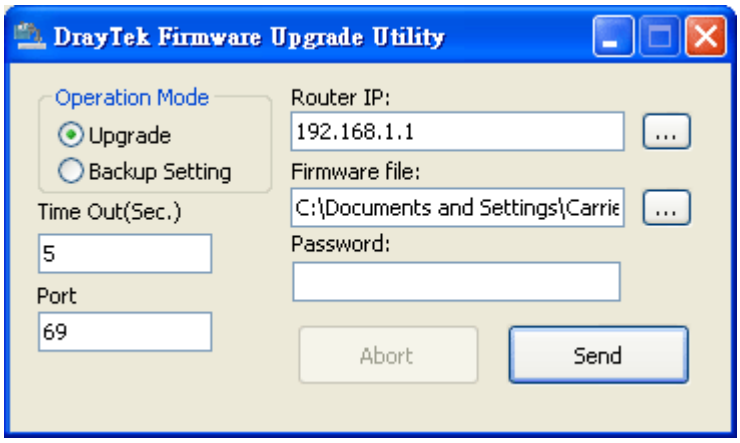
7. Choisissez les outils qui correspondent à votre système d'exploitation et cliquez sur le lien correspondant pour télécharger le firmware (fichier zip).
8. Décompressez le fichier zip.
9. Double-cliquez sur l'icône des outils du routeur. L'assistant de configuration apparaît.



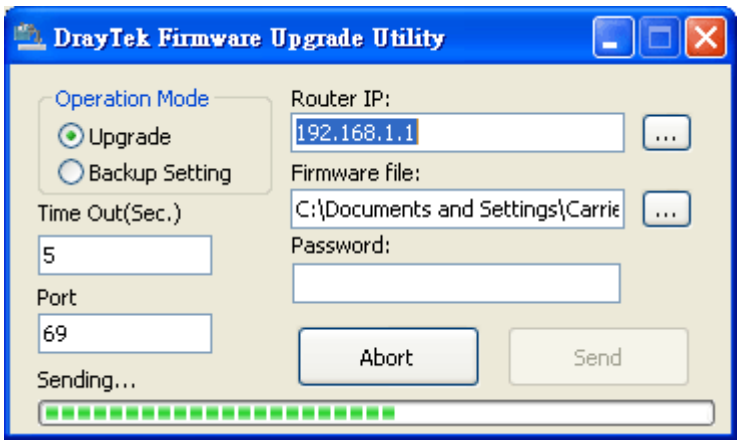
10. Suivez les instructions qui s'affichent pour installer les outils. Enfin, cliquez sur **Finish** pour terminer l'installation.
11. À partir du menu **Démarrer**, sélectionnez **Programmes,** puis **Router Tools XXX** >> **Firmware Upgrade Utility**.



12. Tapez l'adresse IP de votre routeur, généralement **192.168.1.1**.
13. Cliquez sur le bouton à droite de Firmware file. Recherchez les fichiers à télécharger. Vous trouverez deux fichiers dont les extensions diffèrent, **xxxx.all** (conserver les anciens paramètres personnalisés) et **xxxx.rst** (rétablir tous les paramètres par défaut). Choisissez l'un de ces fichiers.

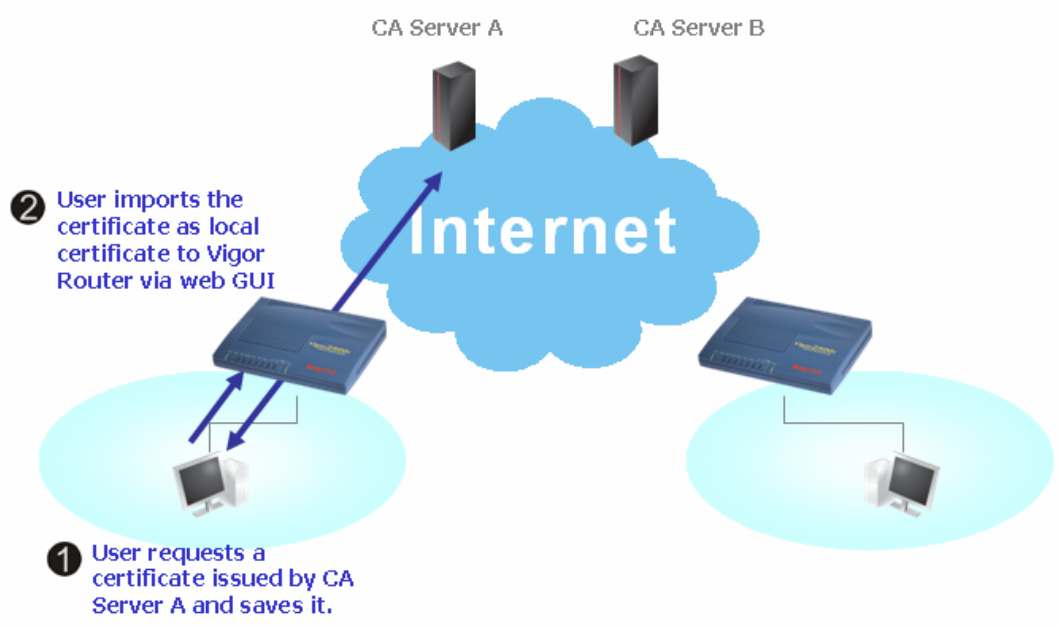


14. Cliquez sur **Envoyer**.



15. La mise à jour du firmware est terminée.

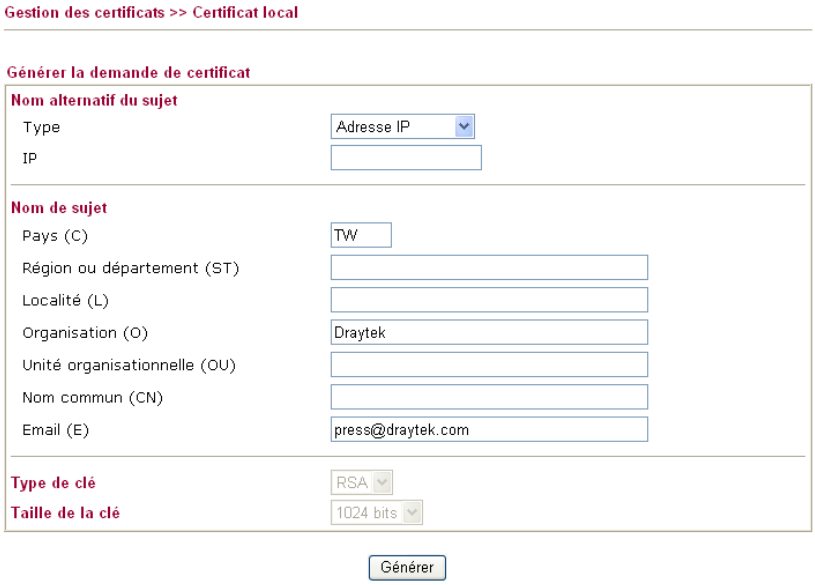
4.7 Demande de certificat d'un serveur d'AC sur un serveur d'AC Windows



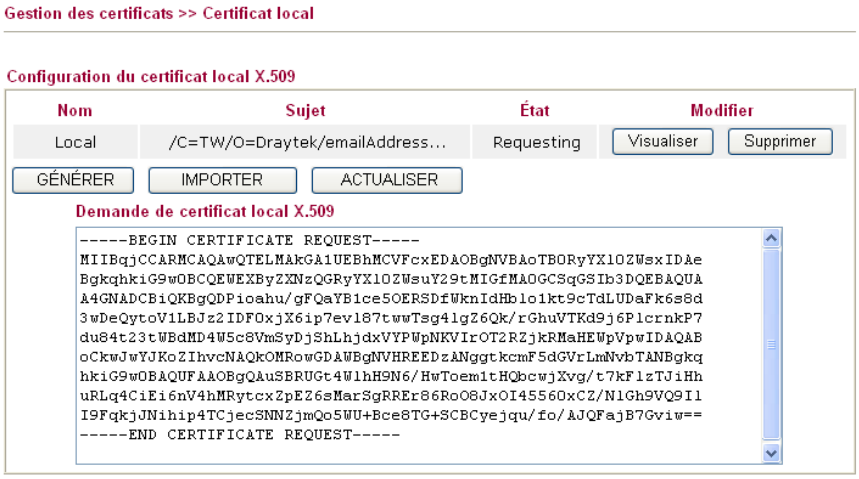
CA Server A	*Serveur d'AC A*
CA Server B	*Serveur d'AC B*
User requests a certificate issued by CA Server A and saves it.	*L'utilisateur demande un certificat émis par le serveur d'AC A et l'enregistre.*
User imports the certificate as local certificate to Vigor Router via web GUI.	*L'utilisateur importe le certificat en tant que certificat local du routeur Vigor via l'interface utilisateur web.*

1. Sélectionnez l'option **Certificat Local** du menu **Gestion des certificats.**

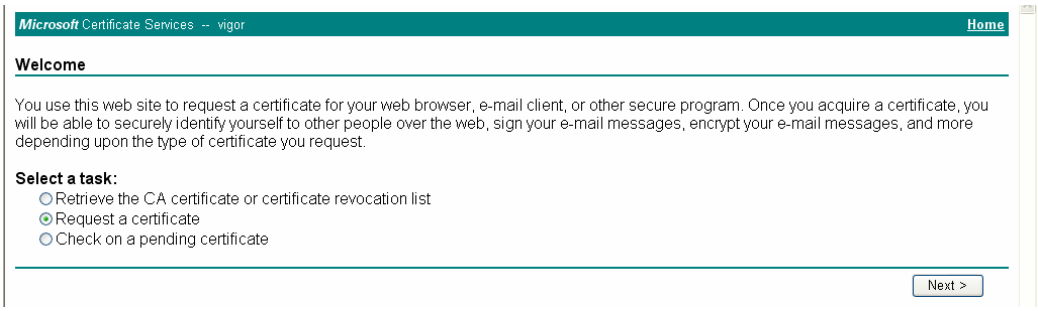
2. Vous pouvez cliquer sur le bouton **GÉNÉRER** pour commencer à éditer une demande de certificat.. Entrez les informations voulues dans la demande de certificat.



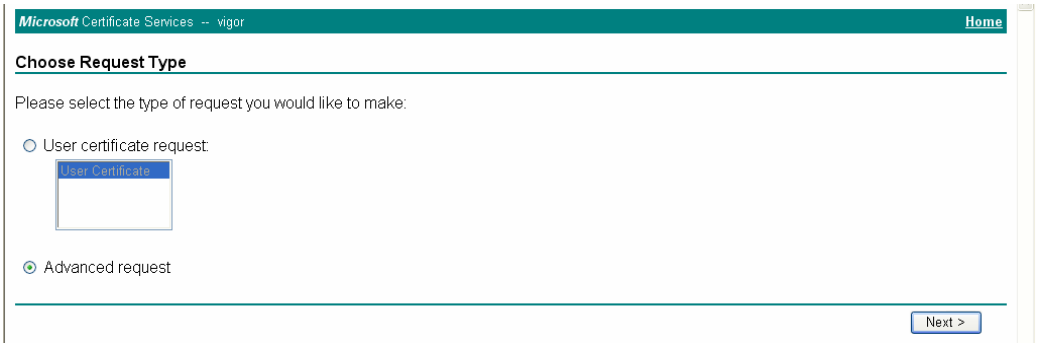
3. Copiez et enregistrez la demande de certificat local X509 sous la forme d'un fichier texte.



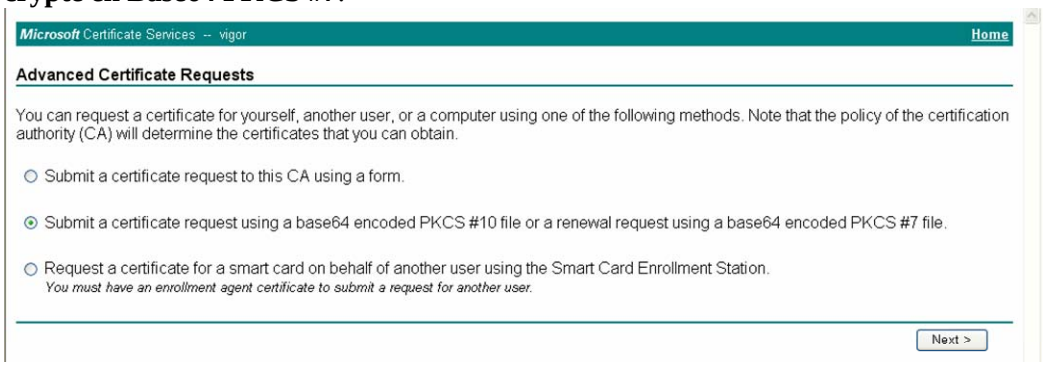
4. Connectez-vous au serveur d'AC à l'aide du navigateur internet. Suivez les instructions. Nous allons prendre l'exemple d'un serveur d'AC Windows 2000. Sélectionnez **Demander un certificat**.



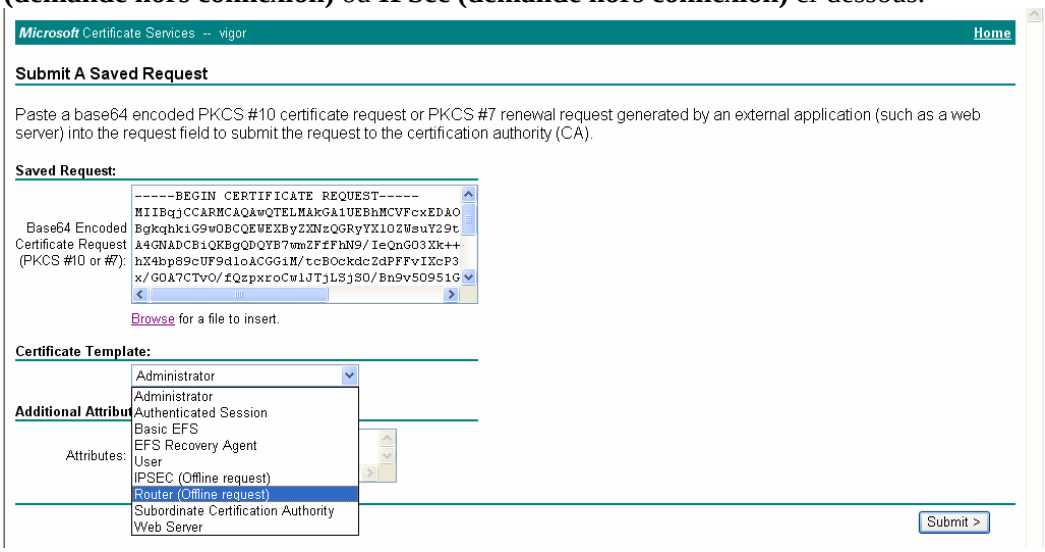
Sélectionnez **Demande avancée**.



Sélectionnez **Soumettre une demande de certificat en utilisant un fichier crypté en Base64 PKCS #10 ou une demande de renouvellement en utilisant un fichier crypté en Base64 PKCS #7**.



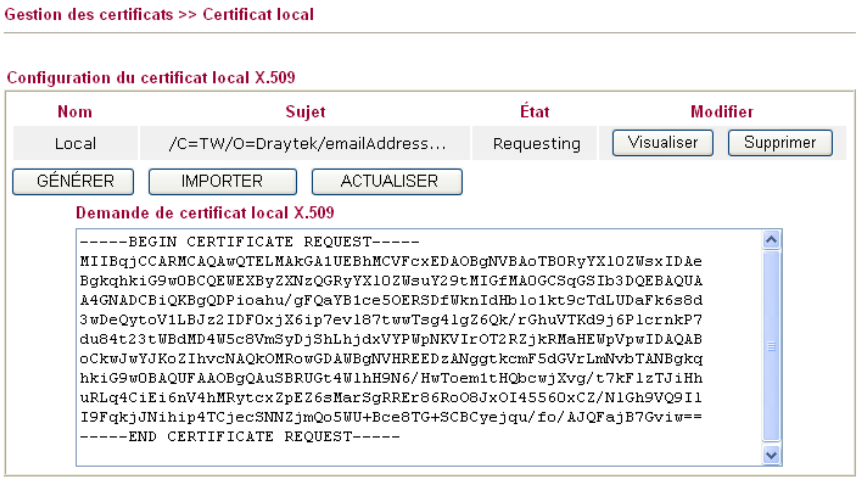
Importez le fichier texte de demande de certificat local X509. Sélectionnez **Routeur (demande hors connexion)** ou **IPSec (demande hors connexion)** ci-dessous.



Le serveur vous délivre un certificat. Sélectionnez **Crypté en Base64** et **Télécharger le certificat CA**. Vous obtenez un certificat (fichier .cer) que vous pouvez enregistrer.

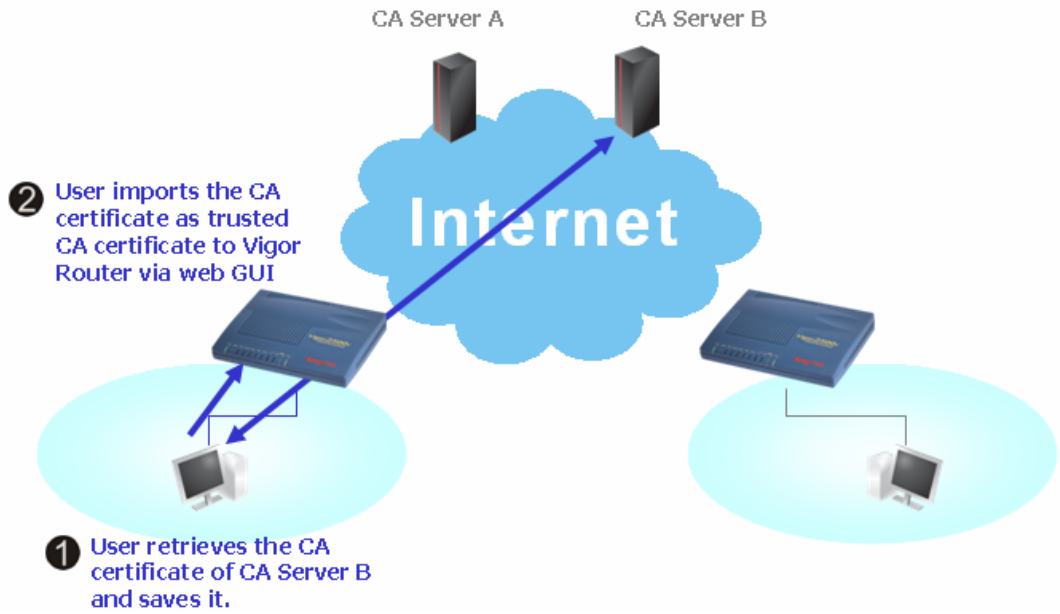
5. Retournez au routeur Vigor, cliquez sur **Certificat local**. Cliquez sur le bouton **IMPORTER** et recherchez le fichier .cer sur le routeur Vigor. Cela fait, cliquez sur ACTUALISER. La fenêtre suivante apparaît avec « ------BEGIN

CERTIFICATE------..... ».



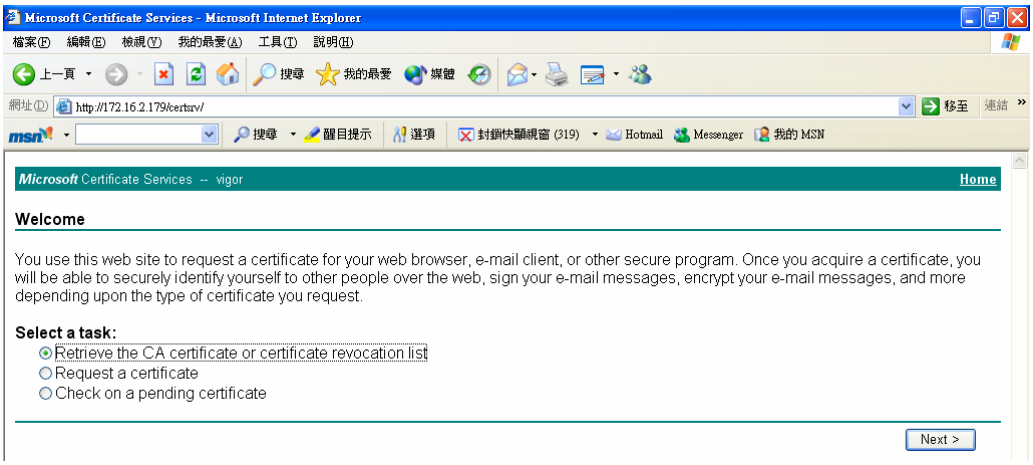
6. Vous pouvez visualiser les informations du certificat en cliquant sur le bouton **Visualiser**.

4.8 Demande de certificat d'AC pour le définir comme certificat de confiance sur un serveur d'AC Windows

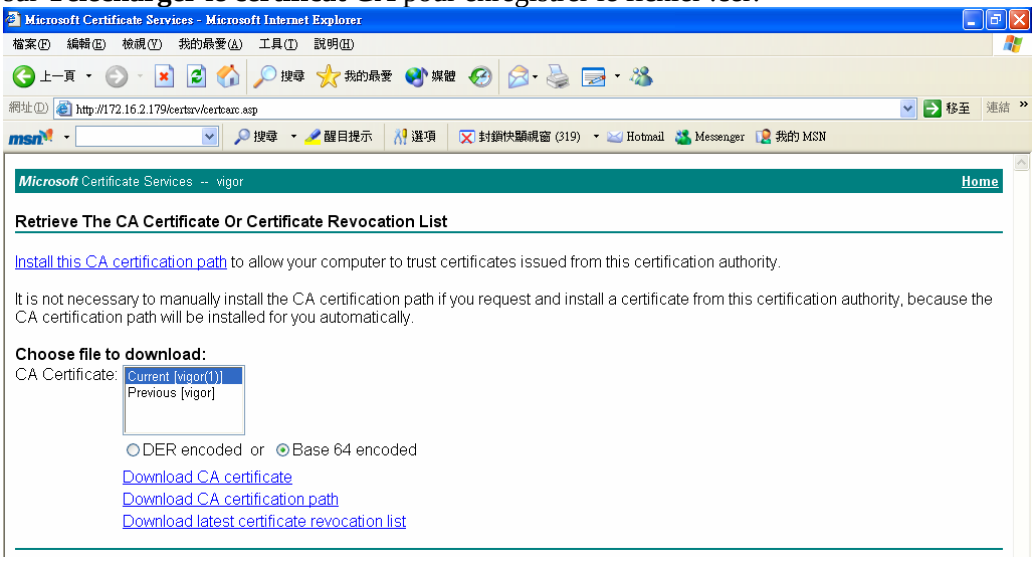


CA Server A	*Serveur d'AC A*
CA Server B	*Serveur d'AC B*
User retrieves the CA certificate of CA Server B and saves it.	*L'utilisateur récupère le certificat du serveur d'AC B et l'enregistre.*
User imports the CA certificate as trusted CA certificate to Vigor Router via web GUI.	*L'utilisateur importe le certificat comme certificat de confiance sur le routeur Vigor via l'interface utilisateur web.*

1. À l'aide du navigateur internet, connectez-vous au serveur d'AC dont vous voulez récupérer le certificat. Cliquez sur **Récupérer le certificat de l'autorité de certification ou la liste de révocation de certificats**.

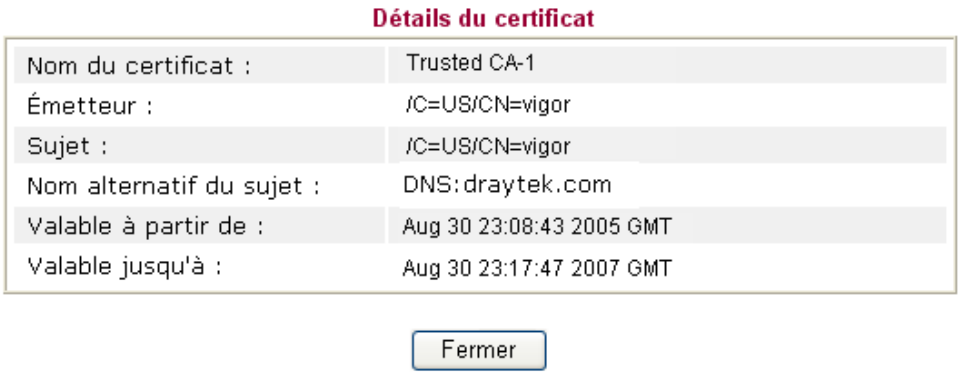


2. Sous **Choisir un fichier à télécharger**, cliquez sur **Courant** sur **Crypté en Base64** et sur **Télécharger le certificat CA** pour enregistrer le fichier .cer.



3. Retournez au routeur Vigor, sélectionnez **Certificat d'AC de confiance**. Cliquez sur le bouton **IMPORTER** et recherchez le fichier .cer sur le routeur Vigor. Cela fait, cliquez sur Actualiser. L'écran suivant apparaît.

4. Vous pouvez visualiser les informations du certificat en cliquant sur le bouton **Visualiser**.



Nota : avant de configurer le certificat, sélectionnez l'option **Maintenance du système >> Date et heure** pour remettre le routeur à l'heure.

5 Dépannage

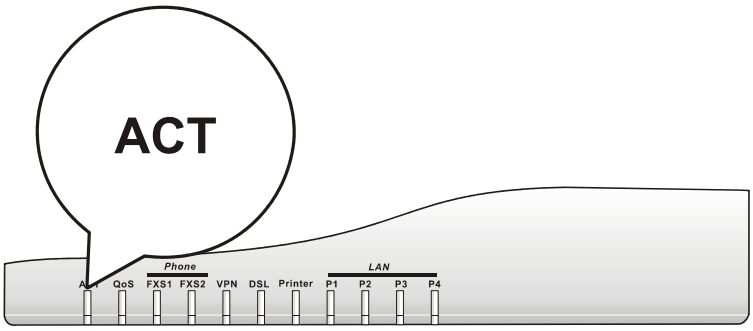
Ce chapitre vous aidera à résoudre certains problèmes après l'installation du routeur et sa configuration. Veuillez suivre les étapes ci-dessous pour vérifier votre installation de base.

- Le matériel est-il installé correctement ?
- Les paramètres de connexion réseau de votre ordinateur sont-ils corrects ?
- Le routeur répond-t-il à un « ping » de votre ordinateur ?
- Les paramètres FAI sont-ils corrects ?
- Rétablissement des paramètres par défaut si nécessaire.

Si, après cela, le routeur ne fonctionne toujours pas normalement, contactez votre revendeur.

5.1 Le matériel est-il installé correctement ?

1. Vérifiez le branchement du câble d'alimentation et du câble WLAN/LAN. Reportez-vous à « **2.1 Installation du matériel »** pour plus de détails.
2. Allumez le routeur. Vérifiez que le voyant **ACT** clignote et que le voyant **LAN** est allumé.



3. Si tel n'est pas le cas, c'est que le matériel n'est pas installé correctement. Reportez-vous à « **2.1 Installation du matériel »** pour réeffectuer l'installation.

5.2 Les paramètres de connexion réseau de votre ordinateur sont-ils corrects ?

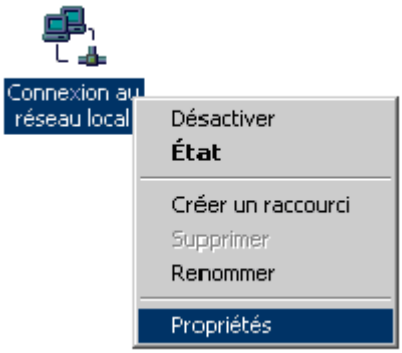
Il se peut que la liaison ne s'établisse pas parce que les paramètres de connexion réseau sont incorrects. Si, après les vérifications de la section 5.1, la liaison ne s'établit toujours pas, vérifiez les paramètres de connexion réseau comme indiqué ci-après.

Cas de Windows

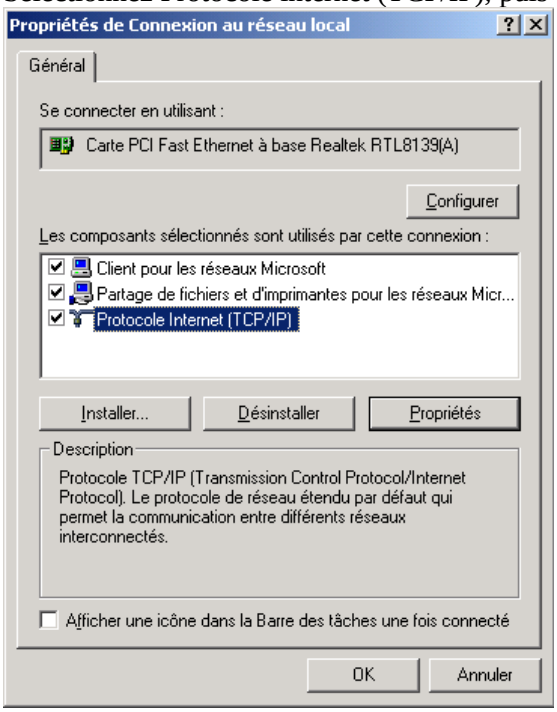
L'exemple vaut pour Windows XP. Pour les autres systèmes d'exploitation, reportez-vous aux exemples ou notes qui se trouvent sur le site **www.draytek.com**.

1. Dans la fenêtre Panneau de configuration, double-cliquez sur Connexions réseau.

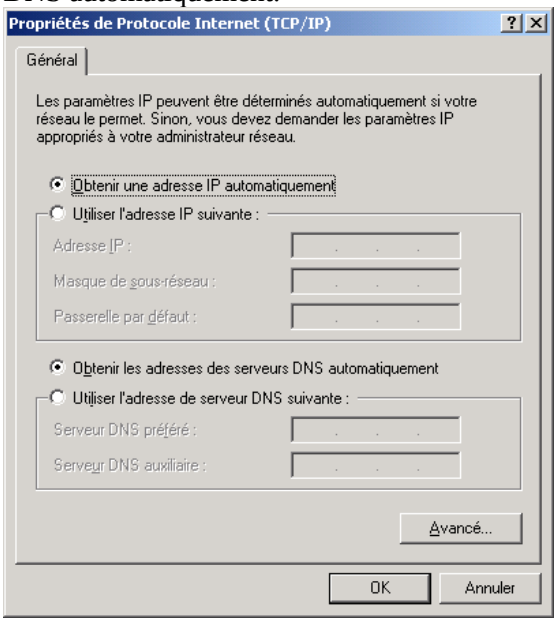
2. Faites un clic droit sur Connexion au réseau local et cliquez sur Propriétés.



3. Sélectionnez Protocole internet (TCP/IP), puis cliquez sur Propriétés.

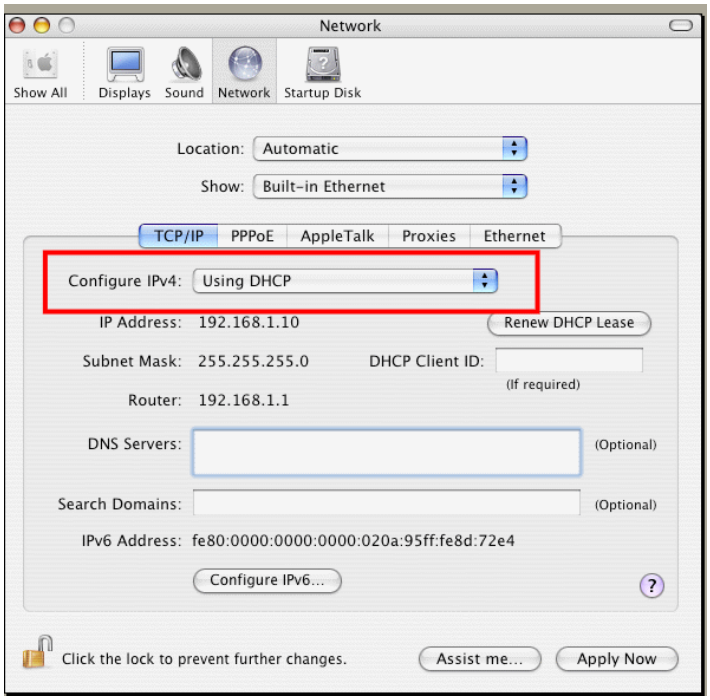


4. Sélectionnez Obtenir une adresse IP automatiquement et Obtenir une adresse de serveur DNS automatiquement.



Cas de MacOs

1. Double-cliquez sur l'icône MacOs du bureau.
2. Ouvrez le dossier **Application** et sélectionnez **Réseau**.
3. Sur l'écran **Réseau**, sélectionnez **Utilisation de DHCP** dans la liste déroulante Configuration IPv4.



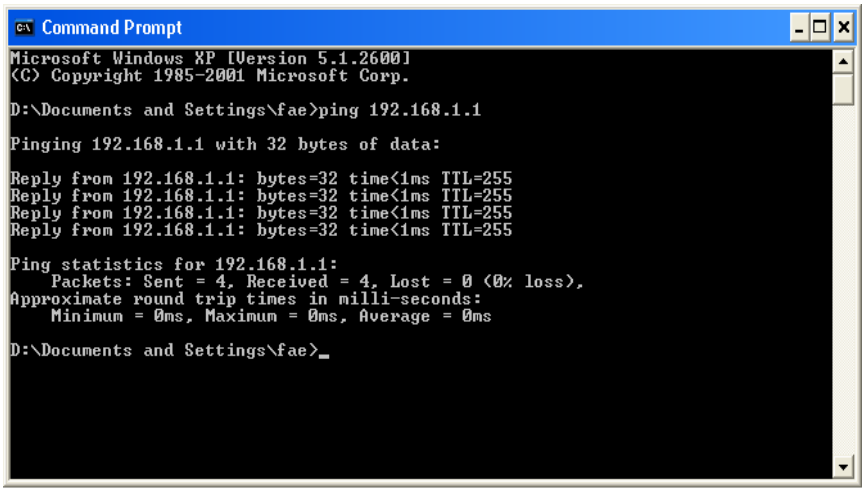
5.3 Le routeur répond-t-il à un « ping » de votre ordinateur ?

L'adresse IP par défaut du routeur est 192.168.1.1. Vous pouvez vérifier l'état de la liaison avec le routeur en utilisant la commande « ping ». **Ce qui importe c'est que l'ordinateur reçoive une réponse 192.168.1.1.** Si tel n'est pas le cas, vérifiez l'adresse IP de votre ordinateur. Nous vous suggérons de paramétrer la connexion au réseau pour l'**obtention automatique d'une adresse IP**. (Voir la section 4.2)

Pour envoyer un ping au routeur, procédez de la manière décrite ci-après.

Cas de Windows

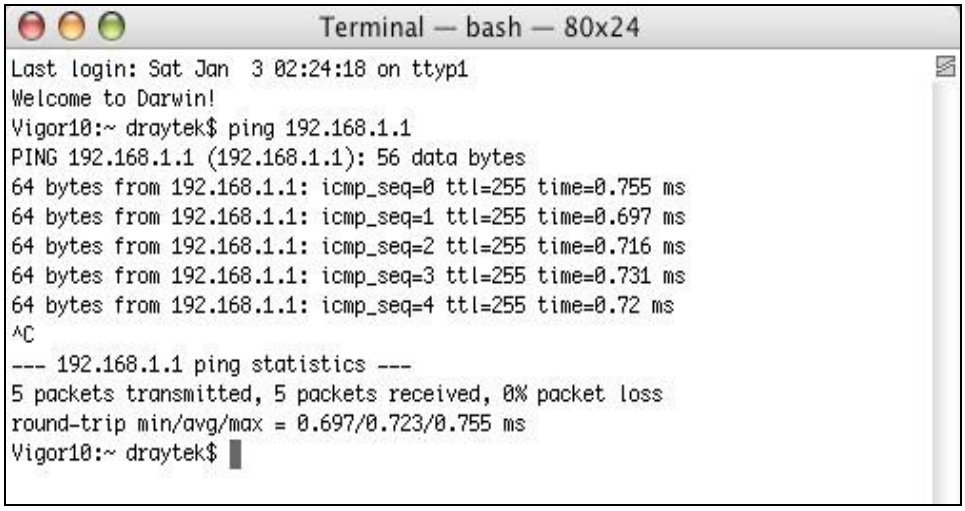
1. Ouvrez la fenêtre **Exécuter** à partir du **menu Démarrer**.
2. Tapez **command** (Windows 95/98/ME) ou **cmd** (Windows NT/2000/XP). La boîte de dialogue suivante apparaît.



3. Tapez **ping 192.168.1.1** et appuyez sur [Entrée]. Si la liaison est bonne, la ligne « **Reply from 192.168.1.1:bytes=32 time<1ms TTL=255** » apparaît.
4. Si cette ligne n'apparaît pas, vérifiez l'adresse IP de votre ordinateur.

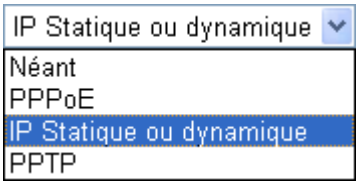
Cas de MacOs (Terminal)

1. Double-cliquez sur l'icône MacOs du bureau.
2. Ouvrez le dossier **Application** et sélectionnez **Utilitaires**.
3. Double-cliquez sur **Terminal**. La fenêtre Terminal apparaît.
4. Tapez **ping 192.168.1.1** et appuyez sur [Entrée]. Si la liaison est bonne, la ligne **« 64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms** » apparaît.



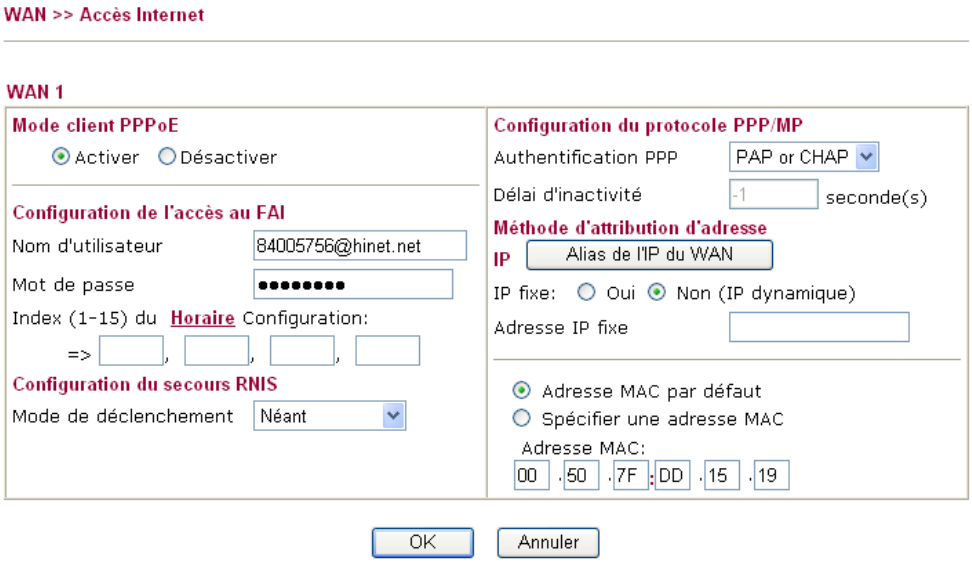
5.4 Les paramètres FAI sont-ils corrects ?

Cliquez sur **Accès à l'internet,** puis vérifiez les paramètres FAI.



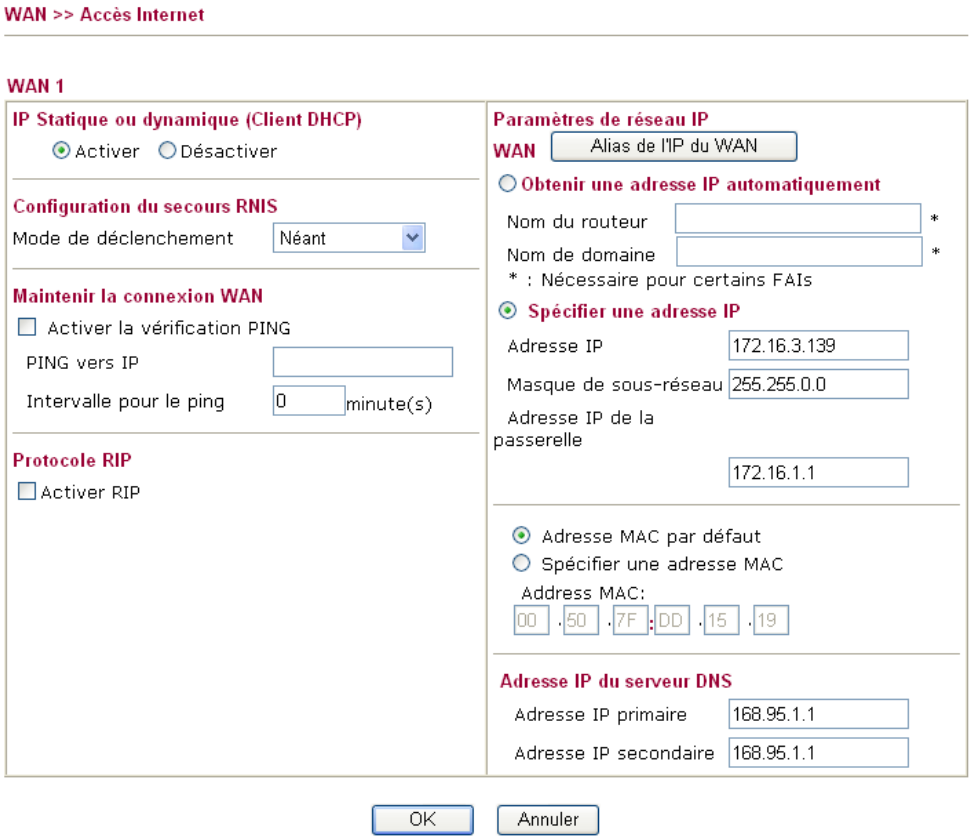
Pour les utilisateurs de PPPoE/PPPoA

1. Vérifiez que l'option **Activer** est sélectionnée.
2. Vérifiez que le **nom d'utilisateur** et **le mot de passe** ont bien les valeurs qui vous ont été données par votre **FAI**.



Pour les utilisateurs des modes IP statique/dynamique

1. Vérifiez que l'option **Activer** est sélectionnée.
2. Vérifiez que **l'adresse IP, le masque de sous-réseau** et l'adresse de la **passerelle** sont ceux que vous a fournis votre **FAI**.



5.5 Rétablissement des paramètres par défaut si nécessaire

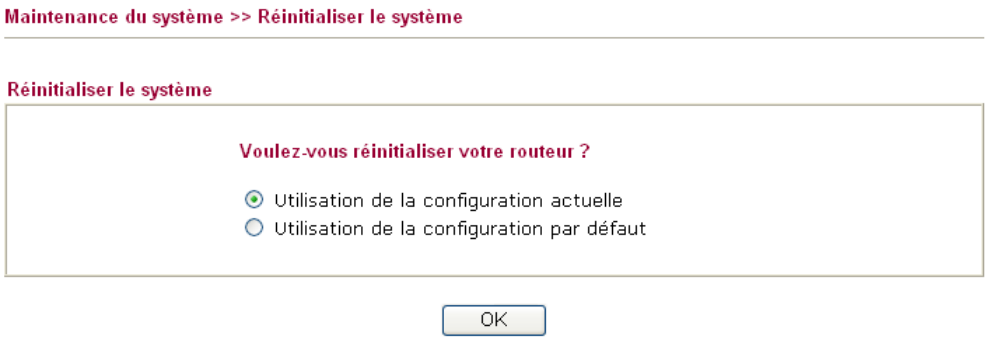
Parfois, on peut améliorer les choses en rétablissant les paramètres par défaut. Tentez une réinitialisation logicielle ou matérielle du routeur.

Attention : Si vous cliquez sur **Paramètres par défaut**, vous perdrez tous les paramétrages effectués jusqu'ici. Veillez à noter tous les paramètres utiles. Le mot de passe par défaut est vide.

Réinitialisation logicielle

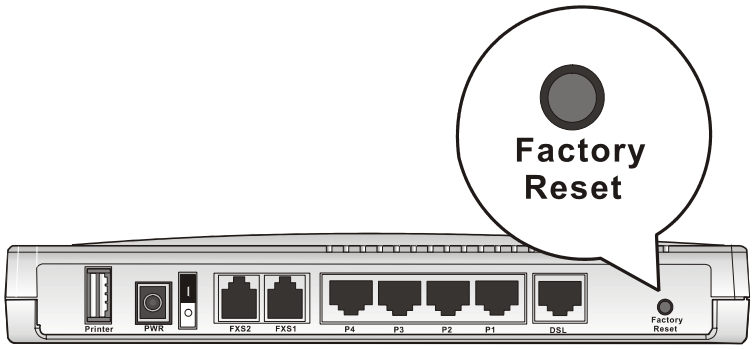
Vous pouvez rétablir les paramètres par défaut de votre routeur à l'aide d'une page web.

Sélectionnez **Maintenance du système,** puis **Réinitialiser le système** sur la page web. L'écran suivant apparaît. Choisissez **Utilisation de la configuration par défaut** et cliquez sur **OK**. Au bout de quelques secondes, les paramètres usine sont rétablis.



Réinitialisation matérielle

Le routeur étant en marche (voyant ACT clignotant), appuyez sur le bouton **Factory Reset** en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant **ACT** commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec les paramètres par défaut.



Après avoir rétabli les paramètres par défaut, vous pouvez reconfigurer le routeur.

5.6 Contacter votre revendeur

Si le routeur ne fonctionne toujours pas correctement, contactez votre revendeur. Pour d'autres questions, n'hésitez pas à envoyer un courriel à support@draytek.com.