


À propos de ce Guide de l'utilisateur

Ce guide a pour but de vous familiariser avec l'utilisation de l'un des routeurs résidentiels à haut débit série Vigor2200V/VG avec VoIP. Les informations contenues dans ce document ont été vérifiées avec soin, néanmoins aucune garantie n'est donnée quant à leur exactitude. Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis. N'hésitez pas à contacter notre support technique par courriel, par télécopie ou par téléphone. Pour connaître les informations les plus récentes sur nos produits, visitez notre site www.draytek.com.

Nous utilisons le visage souriant de VigorBoy  pour attirer votre attention sur certains points particuliers. Si vous avez des questions ou des suggestions, n'hésitez pas à contacter votre revendeur local ou DrayTek : support@draytek.com ou info@draytek.com.

La version de ce Guide d'utilisateur est la version numéro 1.

Copyright

Copyright © 2005, DrayTek Corporation

Tous droits réservés. Cette publication contient des informations protégées par un copyright. Toute reproduction, transmission, transcription, traduction ou mise à disposition intégrale ou partielle du présent document est interdite sans l'accord écrit des détenteurs du copyright.

Marques déposées

Microsoft est une marque déposée de Microsoft Corp. Windows et Windows 95/98/98SE/Me/NT/XP/2000 sont des marques de Microsoft Corp. Les autres marques déposées ou non de produits mentionnés dans ce manuel peuvent être la propriété de leurs propriétaires respectifs et ne sont utilisés qu'à des fins d'identification.

Garantie limitée de DrayTek

Ce routeur est garanti à l'utilisateur originel (c'est-à-dire à l'acheteur) contre tout vice de fabrication ou défaut de matière pendant une période de trois (3) ans à compter de la date d'achat au revendeur. Conservez votre justificatif d'achat en lieu sûr.

Pendant la période de garantie et sur présentation du justificatif d'achat, si le produit présente des dysfonctionnements dus à un vice de fabrication ou à défaut de matière, nous nous engageons à réparer ou à remplacer gratuitement les produits ou composants défectueux, pièces ou main-d'œuvre, dans la mesure que nous jugeons nécessaires pour remettre le produit en état. Tout remplacement consistera en un produit neuf ou remis en état, fonctionnellement équivalent et d'égale valeur, et sera proposé à notre seule discrétion. Cette garantie ne s'applique pas si le produit est modifié, mal utilisé, maltraité, endommagé par une catastrophe naturelle ou soumis à des conditions de fonctionnement anormales.

La garantie ne couvre pas les logiciels d'autres sources. Les défauts qui ne modifient pas sensiblement la valeur d'usage du produit ne sont pas couverts par la garantie.

Nous nous réservons le droit de réviser le manuel et la documentation en ligne et de leur apporter des modifications sans préavis.

Enregistrez votre routeur

Il est préférable d'enregistrer votre routeur via l'internet www.draytek.com. Vous pouvez également remplir la carte d'enregistrement et l'envoyer à l'adresse qui figure au verso. Les utilisateurs enregistrés seront informés de l'évolution des produits.

Consignes de sécurité

- Veuillez lire attentivement le guide d'installation avant d'installer le routeur.
- Le routeur est un équipement électronique compliqué qui ne peut être réparé que par des personnes autorisées et qualifiées. Ne tentez pas d'ouvrir ou de réparer le routeur vous-même.
- Ne placez pas le routeur dans un endroit humide, par exemple dans une salle de bain.
- Le routeur doit être utilisé dans un endroit abrité où la température est comprise entre +5 et +40 °C.
- N'exposez pas le routeur au soleil ou à une autre source de chaleur. Le boîtier et les composants électroniques peuvent être endommagés par les rayons de soleil ou les sources de chaleur.
- Tenez l'emballage hors de la portée des enfants.
- Pour l'élimination du routeur, respectez la réglementation locale sur la préservation de l'environnement.

Déclarations CE

Fabricant : DrayTek Corp.

Adresse : No. 26, Fu Shing Road, HuKou County, HsinChu
Industrial Park, Hsin-Chu, Taiwan 303

Produit : Routeurs résidentiels à haut débit série Vigor2200V/VG

DrayTek Corp. déclare que les routeurs série Vigor2200V/VG sont conformes aux exigences essentielles suivantes et autres dispositions de la directive 1999/5/CE concernant les équipements hertziens et les équipements terminaux de télécommunication.

Le produit est conforme aux exigences de la directive 89/336/CE concernant la compatibilité électromagnétique (CEM) ainsi qu'aux normes techniques EN 55022/Classe B et EN 55024/Classe B.

Le produit est conforme aux exigences de la directive basse tension (DBT) 73/23/CE et à la norme technique EN 60950.

Le routeur Vigor2200VG est conçu pour le réseau WLAN à 2,4 GHz dans toute l'Union européenne, en Suisse, et tiennent compte des restrictions propres à la France.

Avertissement de la Federal Communication Commission (FCC)

Le Vigor2200V et le Vigor2200VG ont été testés et trouvés conformes aux limites d'un équipement numérique de classe B selon la Part 15 des règles de la FCC. Son utilisation est soumise aux deux conditions suivantes :

(1) Cet appareil ne peut pas causer de perturbations nuisibles, et (2) Cet appareil peut accepter des perturbations, y compris des perturbations susceptibles d'entraîner des dysfonctionnements. Ces limites de classe B prémunissent raisonnablement contre les perturbations nuisibles dans une installation résidentielle. Cet équipement produit, utilise et peut rayonner de l'énergie radiofréquence et, s'il n'est pas installé ou utilisé conformément aux instructions, peut perturber les communications radio. Toutefois, il n'y a aucune garantie que des perturbations ne peuvent pas se produire dans une installation particulière. Si cet équipement perturbe la réception de radio ou de télévision, ce que l'on peut déterminer en éteignant puis en rallumant l'équipement, l'utilisateur est invité à y remédier en prenant l'une ou l'autre des mesures suivantes :

- Réorienter l'antenne de réception.
- Augmenter la distance séparant l'équipement du récepteur.
- Branchez l'équipement sur une prise de courant appartenant à un circuit différent de celui sur laquelle le récepteur est branché.
- Consultez le revendeur ou un radioélectricien expérimenté.

Support client

Lorsque vous contactez le support client, préparez les informations suivants :

- Modèle et numéro de série.
- Conditions de garantie.
- Date de réception de votre routeur.
- Description succincte du problème.
- Opérations que vous effectuées pour le résoudre et messages SysLog associés.

Vous pouvez contacter le support client et les représentants commerciaux respectivement aux adresses support@draytek.com et sales@draytek.com.

Table des matières

Introduction	i
Description succincte	ii
Caractéristiques marquantes	iii
Branchement	iv
Chapitre 1. Assistant de démarrage rapide	
1.1. Introduction	1-1
1.2. Configuration de votre routeur à l'aide de l'assistant de démarrage rapide.....	1-1
Chapitre 2. État en ligne	
2.1. Introduction	2-1
2.2. Paramètres	2-1
2.2.1. État du système	2-1
2.2.2. État LAN	2-2
2.2.3. État WAN	2-2
Chapitre 3. Configuration de l'accès à l'internet	
3.1. Introduction	3-1
3.2. Paramètres	3-2
3.2.1. Utilisation de PPPoE avec un modem DSL	3-3
3.2.2. Utilisation d'une adresse IP statique avec un modem DSL/câble	3-4
3.2.3. Utilisation d'une adresse IP dynamique (client DHCP) avec un modem DSL/câble	3-6
3.2.4. Utilisation du protocole PPTP avec un modem DSL	3-7

Chapitre 4. Configuration du LAN

4.1. Introduction	4-1
4.2. Paramètres	4-1
4.2.1 Paramètres TCP/IP et DHCP du LAN	4-1

Chapitre 5. Paramétrage du NAT

5.1. Introduction	5-1
5.2. Paramètres	5-1
5.2.1. Table de redirection de ports	5-2
5.2.2. Configuration de l'hôte DMZ	5-4
5.2.3. Ouverture de ports	5-5
5.2.4. Liste des ports connus	5-7

Chapitre 6. Paramétrage du pare-feu

6.1. Introduction	6-1
6.2. Paramétrage	6-2
6.2.1. Configuration générale	6-5
6.2.2. Paramétrage des filtres	6-7
6.2.3. Protection anti-DoS (déni de service)	6-12
6.2.4. Filtre de contenu d'URL	6-16

Chapitre 7. Paramétrage des applications

7.1. Introduction	7-1
7.2. Paramètres	7-2
7.2.1. DNS dynamique	7-2
7.2.2. Plages horaires	7-5
7.2.3. UPnP	7-9

Chapitre 8. Paramétrage du VPN et de l'accès à distance

8.1. Introduction	8-1
8.2. Paramètres	8-2
8.2.1. Contrôle d'accès à distance	8-3
8.2.2. Configuration générale du protocole PPP	8-3
8.2.3. Configuration générale IKE/IPSec	8-5
8.2.4. Profils d'utilisateur distant (Télétravailleurs)	8-5
8.2.5. Profils d'interconnexion de LAN	8-8

Chapitre 9. Paramètres VoIP

9.1. Introduction	9-1
9.2. Paramètres	9-2
9.2.1. DialPlan (plan de numérotation)	9-3
9.2.2. Configuration des fonctions liées au SIP	9-6
9.2.3. CODEC/RTP/DTM	9-8
9.2.4. État de l'appel téléphonique	9-12
9.2.5. QoS	9-14

Chapitre 10. LAN sans fil

10.1. Introduction	10-1
10.2. Paramètres	10-2
10.2.1. Paramètres généraux	10-2
10.2.2. Sécurité	10-3
10.2.3. Contrôle d'accès	10-5
10.2.4. Liste des stations	10-6

Chapitre 11. Maintenance du système

11.1. Introduction	11-1
11.2. Paramètres	11-2
11.2.1. État du système	11-3
11.2.2. Sauvegarde des configurations	11-3
11.2.3. Gestion	11-5

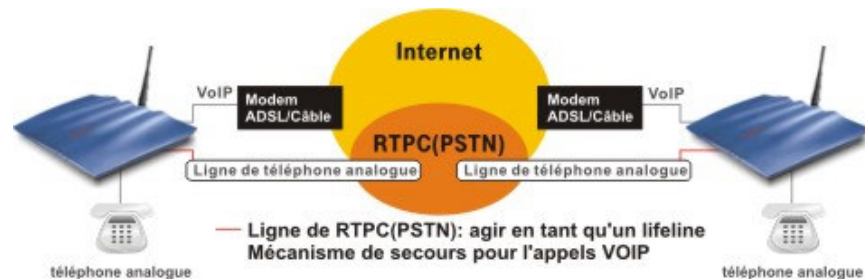
Chapitre 12. Paramétrage des diagnostics

12.1. Introduction	12-1
12.2. Paramètres	12-1
12.2.1. Diagnostics PPPoE/PPTP	12-1
12.2.2. Table de cache ARP	12-2
12.2.3. Adresses IP attribuées par DHCP	12-2

Présentation du routeur résidentiel à haut débit série Vigor2200V/VG

Introduction

- 🔗 Partagez facilement votre accès internet à haut débit*
- 🔗 Un pare-feu robuste protège votre réseau des attaques extérieures
- 🔗 Des fonctionnalités complètes de réseau privé virtuel (VPN) permettent de relier différents sites et des télétravailleurs
- 🔗 Les fonctionnalités VoIP intégrées permettent de déployer une infrastructure de téléphonie sur IP économique
- 🔗 Branchez un téléphone pour utiliser votre ligne à haut débit pour les appels téléphoniques ordinaires
- 🔗 Fonctionnement en symbiose avec votre ligne téléphonique existante, avec basculement automatique sur celle-ci en cas de coupure de courant
- 🔗 Priorité au trafic VoIP avec QoS assurée
- 🔗 Accès LAN sans fil 802.11g avec fonctions de sécurité (Vigor2200VG seulement)
- 🔗 Compatible avec Windows & MacOS



Analog Phone		Téléphone analogique
ADSL/Cable Modem		Modem ADSL/câble
Analog Phone Line		Ligne téléphonique analogique
PSTN		RTCP

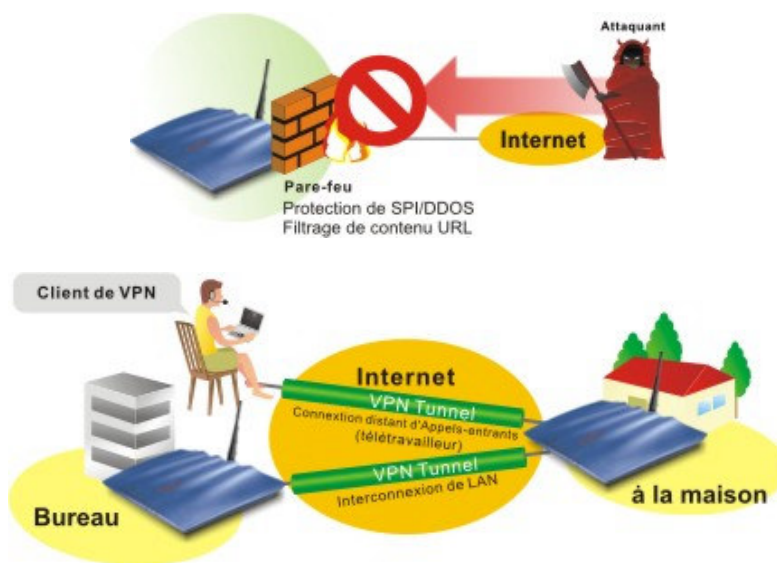
Description succincte

	Vigor2200V	Vigor2200VG
Routeur haut débit	*	*
Point d'accès WLAN 802.11g	-	*
Port VoIP	Un port FXS	Un port FXS
Port de secours	un	un

Le Vigor2200VG est un routeur à haut débit convivial doté d'un port téléphonique (VoIP) et d'un point d'accès de LAN sans fil 802.11g. Ses lignes modernes, agréables à l'œil permettent de l'installer n'importe où sans déparer l'environnement.

Les fonctionnalités VoIP du Vigor2200VG permettent de faire l'économie d'une ligne fixe. En utilisant la passerelle RTCP DrayTEL (ITSP), vous pouvez appeler n'importe quel téléphone ordinaire, y compris des mobiles, et recevoir des appels de n'importe qui – l'appel arrive par l'internet, de sorte que votre ligne téléphonique ordinaire reste libre pour d'autres appels.

La fonction ligne de secours permet le repli automatique sur votre ligne téléphonique ordinaire en cas de panne de courant ou d'impossibilité d'accès à l'internet. Vous pouvez utiliser le même téléphone pour accéder à votre ligne téléphonique ordinaire ou à la fonction VoIP.



Firewall	<i>Pare-feu</i>
SPI/DdoS protection/ URL content Filtering	<i>Protection anti-DdoS/ Filtrage de contenu d'URL</i>
Smart VPN client	<i>Client VPN</i>
PSTN	<i>RTCP</i>
VPN Tunnel	<i>Tunnel de VPN</i>
Remote Dial-in Connection (Teleworker)	<i>Utilisateur distant (télétravailleur)</i>
LAN-to-LAN Connection	<i>Interconnexion de LAN</i>

Caractéristiques marquantes

VoIP (Voix sur IP)

- ◆ Branchez un téléphone ordinaire pour appeler et recevoir des appels avec votre connexion à haut débit existante en gardant votre ligne normale libre
- ◆ Appelez et recevez des appels sur votre ligne téléphonique ordinaire ou via l'internet avec le même combiné téléphonique
- ◆ Repli automatique - Basculement sur le RTPC en cas de coupure de courant
Conformité aux protocoles SIP, RTP/RTCP

WAN/Internet

- ◆ Un port 10/100M Base-TX avec connecteur RJ-45
- ◆ Assistant de démarrage rapide pour l'accès à l'internet
Client DHCP pour le service câble
- ◆ Attribution d'adresse IP statique pour les réseaux IP fixes
- ◆ Client PPPoE/PPTP

Fonctionnalités de pare-feu

- ◆ Le filtrage adaptatif de paquets (SPI) bloque les données entrantes non sollicitées
- ◆ Protection DoS/DDoS
- ◆ Filtrage de contenu d'URL flexible
- ◆ Filtrage des paquets configurable par l'utilisateur
- ◆ Serveur virtuel NAT/PAT/Multi-NAT par redirection de ports/ouverture de ports, hôte DMZ
- ◆ Prise en charge de passerelles de couche application (ALG)

Détection d'e-mail

- ◆ Un voyant clignote pour vous indiquer qu'un courriel est en attente sur votre serveur de messagerie (POP3)

LAN

- ◆ Commutateur Ethernet 10/100M Base-TX 4 ports
- ◆ Serveur DHCP pour l'attribution d'adresses IP (jusqu'à 253 utilisateurs)
- ◆ Proxy et cache DNS

Réseau privé virtuel (VPN)

- ◆ Prise en charge du mode pass-through VPN
- ◆ Jusqu'à 8 tunnels de VPN simultanés
- ◆ Appels entrants ou sortants, interconnexion de LAN, interconnexion télétravailleur-LAN
- ◆ Prise en charge des protocoles PPTP, IPSec, L2TP, L2TP sur IPSec
- ◆ Cryptage : AES, MPPE et DES/3DES matériel
- ◆ Authentification : MD5 et SHA-1
- ◆ Gestion des clés IKE
- ◆ Interopérabilité avec les appareils ou logiciels de VPN tiers

Point d'accès sans fil (Vigor2200VG seulement)

- ◆ Prise en charge de la norme 802.11g (débit de 54 M bit/s)
- ◆ Compatibilité avec 802.11b
- ◆ Liste des stations
- ◆ Sécurité radio :
 - Cryptage radio WEP 64/128 bits
 - WPA/PSK
 - Verrouillage d'adresse MAC client
 - Masquage SSID

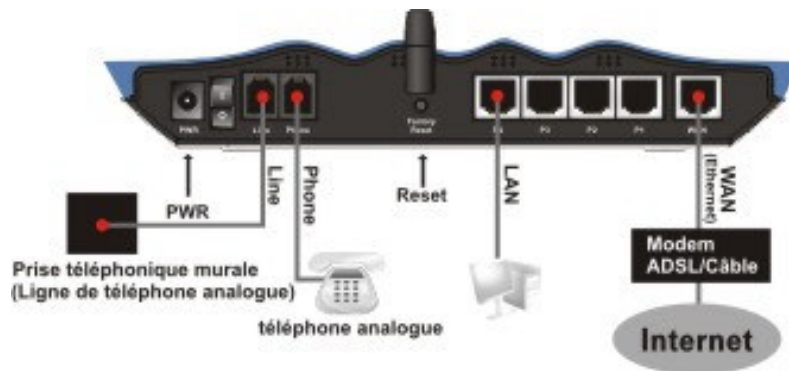
Applications prises en charge

- ◆ Prise en charge du mode pass-through VPN
- ◆ MSN Messenger V6.2, jeux en ligne et autres applications multimédias
- ◆ Protocole UPnP permettant la commande du routeur et améliorant l'accès pour les applications multimédias compatibles UPnP

Gestion du routeur

- ◆ Interface utilisateur sur web
- ◆ Interface de ligne de commande (Telnet)
- ◆ Accès à distance Telnet
- ◆ Fonction de diagnostic intégré
- ◆ Surveillance Syslog

Branchement



Analog Phone	Téléphone analogique
ADSL/Cable modem	Modem ADSL/câble
Land lin jack (Analog phone line)	Prise téléphonique (ligne téléphonique analogique)
Line	Ligne
Phone	Téléphone
LAN	LAN

Chapitre 1

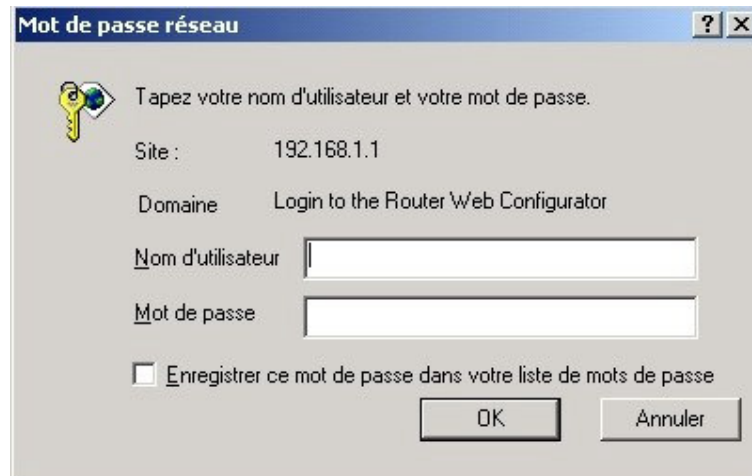
Assistant de démarrage rapide

1.1 Introduction

L'assistant de démarrage rapide est conçu pour que vous puissiez facilement configurer votre accès internet à haut débit. Nous avons déjà intégré l'assistant de démarrage rapide au configurateur web des routeurs Vigor2200V/VG. Vous pouvez accéder directement à l'assistant de démarrage rapide via le configurateur web.

1.2 Configuration de votre routeur à l'aide de l'assistant de démarrage rapide

- Étape 1.** Ouvrez le navigateur internet sur un PC relié au routeur, puis connectez-vous à l'adresse IP du routeur (l'adresse par défaut est **192.168.1.1**). Une fois la connexion établie (**http://192.168.1.1**), une fenêtre s'ouvre pour vous demander votre nom d'utilisateur et votre mot de passe. Laissez les deux champs vides et appuyez sur **OK** pour continuer.



Mot de passe réseau

Tapez votre nom d'utilisateur et votre mot de passe.

Site : 192.168.1.1

Domaine Login to the Router Web Configurator

Nom d'utilisateur

Mot de passe

Enregistrer ce mot de passe dans votre liste de mots de passe

OK Annuler



Si vous n'arrivez pas à accéder au configurateur web, reportez-vous au guide de dépannage.

Étape 2. Le **Menu principal** apparaît.



Étape 3. L'assistant de démarrage rapide est maintenant actif. Tapez un mot de passe. Puis cliquez sur **Suivant** pour continuer.

Tapez le mot de passe

Il n'y a pas de mot de passe par défaut. Pour votre sécurité, choisissez une série de chiffres ou de lettres (23 caractères maximum) comme **mot de passe** et tapez-les dans le champ Mot de passe.

Nouveau mot de
passe

Retapez le nouveau
mot de passe

Étape 4. Sélectionnez le FUSEAU HORAIRE approprié qui correspond à votre situation géographique.

Choisissez le fuseau horaire

Choisissez le fuseau horaire approprié.

Assistant de démarrage rapide

Étape 5 Sélectionnez le type de connexion internet approprié selon les informations fournies par votre FAI.

Connexion à l'internet

Choisissez l'un des types d'accès à l'internet suivants. En cas de doute, contactez votre FAI.

- PPPoE
- PPTP
- Adresse IP statique
- DHCP

L'écran qui apparaît est propre au type de connexion internet :

Utilisateurs de PPPoE Entrez votre nom d'utilisateur et votre mot de passe fournis par votre FAI.

Connexion à l'internet

Tapez le nom d'utilisateur et le mot de passe fournis par votre FAI.

Nom d'utilisateur

Mot de passe

Retapez le mot de passe

Type de connexion

- Connexion permanente
- Numérotation à la demande

Délai d'inactivité

Numérotation à la demande : Le routeur se connecte à votre FAI UNIQUEMENT à la demande, c'est-à-dire chaque fois qu'un utilisateur en réseau tente d'envoyer des données sur l'internet. En l'absence de trafic de données, le routeur ferme la connexion au FAI car il n'y a pas de demande.

Assistant de démarrage rapide

Délai d'inactivité : En l'absence de trafic internet, c'est le délai (en secondes) à l'expiration duquel le routeur ferme la connexion.

Connexion permanente : Le routeur maintient la connexion au FAI ouverte en permanence.

Utilisateurs PPTP Entrez votre nom d'utilisateur et votre mot de passe fournis par votre FAI.

Connexion à l'internet

Taper le nom d'utilisateur, le mot de passe, les configurations IP WAN et l'adresse IP de serveur PPTP fournis par votre FAI.

Nom d'utilisateur

Mot de passe

Retapez le mot de passe

Configurations IP WAN

Obtenir une adresse IP automatiquement

Spécifier une adresse IP

Adresse IP . . .

Masque de sous-réseau . . .

Adresse IP du serveur PPTP . . .

Obtenir une adresse IP automatiquement : L'interface WAN est configurée en client DHCP qui demandera les paramètres IP au serveur DHCP ou à un modem DSL prenant en charge le protocole PPTP.

Spécifier une adresse IP : Si vous n'êtes pas certain(e) qu'il y ait des services DHCP sur l'interface WAN, vous pouvez attribuer manuellement une adresse IP à l'interface. À noter que l'adresse IP et le masque de sous-réseau doivent être attribués au sein du même réseau que le modem DSL à protocole PPTP.

Assistant de démarrage rapide

Adresse IP statique Entrez l'adresse IP statique (fixe ou permanente) fournie par votre FAI.

Connexion à l'internet

Tapez la configuration IP statique fournie par votre FAI.

Adresse IP du WAN	<input type="text" value="172"/>	<input type="text" value="16"/>	<input type="text" value="2"/>	<input type="text" value="84"/>
Masque de sous-réseau	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Passerelle	<input type="text" value="172"/>	<input type="text" value="16"/>	<input type="text" value="2"/>	<input type="text" value="1"/>
DNS primaire	<input type="text" value="168"/>	<input type="text" value="95"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
DNS secondaire	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> (facultatif)

Adresse IP WAN : Adresse IP attribuée par votre FAI à votre routeur. Vous devez entrer ici l'adresse IP du routeur, par exemple, 172.16.2.84.

Masque de sous-réseau : Code d'adresse qui détermine la taille du réseau; c'est le masque de sous-réseau du routeur, vu par les utilisateurs externes sur l'internet (y compris votre FAI). Le masque de sous-réseau est fourni par votre FAI (exemple:255.255.255.0).

Adresse IP de la passerelle : Adresse IP de la passerelle de votre réseau local (LAN) vers l'internet, par exemple, 172.16.2.5.

Adresse IP du serveur DNS : Vous devez spécifier ici l'adresse IP du serveur DNS si votre FAI vous l'a communiquée. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut: 194.109.6.66

Assistant de démarrage rapide

DHCP

Certains FAI câble imposent à l'utilisateur de fournir ou de spécifier une adresse MAC à des fins d'authentification. Vous pouvez entrer manuellement l'adresse MAC dans les champs MAC ou la cloner à partir de votre carte réseau.

Connexion à l'internet

Si votre FAI vous impose d'entrer un nom d'hôte spécifique ou une adresse MAC spécifique, veuillez l'entrer ici. Le **Cloner l'adresse MAC** bouton sert à copier l'adresse MAC de votre carte ethernet sur le Vigor2200V.

Nom de l'hôte (facultatif)

MAC
(facultatif)

Étape 6

Vérifiez vos paramètres.

Résumé

Rechercher vos paramètres :

Accès à l'internet : DHCP

Fuseau horaire : (GMT+01:00) Madrid, Paris, Vilnius

Cliquer **Retour** pour effectuer des modifications.

Sinon, cliquez **Terminer** pour enregistrer les paramètres actuels et redémarrer le Vigor2200V.

Les modèles Vigor2200V/VG mettent en œuvre des codecs performants conçus pour que vous puissiez exploiter au mieux la bande passante disponible. Les modèles Vigor2200V/VG sont également dotés d'une fonction d'**assurance de QoS automatique**. L'assurance de QoS permet de donner la priorité au trafic vocal pour une meilleure qualité des communications. Pour cela, la bande passante d'arrivée et de départ voulue sera réservée au trafic téléphonique via internet (VoIP). Vos données arriveront un peu plus tard, avec un retard tolérable.

Assistant de démarrage rapide



En bas de la fenêtre du configurateur web, le système affiche des messages à votre intention.

- « **Prêt** » indique que le système est prêt et que vous pouvez définir vos paramètres.
- « **Paramètre enregistrés** » indique que vos paramètres seront enregistrés quand vous aurez cliqué sur le bouton « Terminer » ou « OK ».

Chapitre 2

État en ligne

2.1 Introduction

L'**État en ligne** fournit quelques informations utiles sur le routeur Vigor, sur le LAN et sur l'interface WAN. Vous pouvez également utiliser la page d'état pour voir quel est l'état de l'accès à l'internet.

2.2 Paramètres

Cliquez sur **État en ligne** pour ouvrir la page État en ligne.

Nous utilisons un exemple pour expliquer ce qu'est l'**État en ligne**. Dans l'exemple ci-dessous, le routeur fonctionne en mode adresse IP dynamique pour accéder à l'internet.

État du système

État LAN		DNS primaire	168.95.192.1	DNS secondaire		194.98.0.1
Adresse IP		Paquets TX	Paquets RX			
192.168.1.1		31	26			
État WAN		Adresse IP passerelle		172.16.3.1		
Mode	Adresse IP	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Temps actif
DHCP Client	172.16.3.60	0	0	9	113	0:00:04
>>Appeler PPPoE ou PPTP>>Abandon PPPoE ou PPTP						

2.2.1 État du système

Système démarré depuis : Il s'agit du temps de fonctionnement du routeur depuis son démarrage. Le format est HH:MM:SS, où HH, MM, et SS sont respectivement les heures, les minutes et les secondes.

2.2.2 État LAN

Adresse IP	Adresse IP de l'interface LAN.
Paquets TX	Nombre total de paquets IP émis depuis l'allumage du routeur.
Paquets RX	Nombre total de paquets IP reçus depuis l'allumage du routeur.
DNS primaire	Vous devez spécifier l'adresse IP du serveur DNS primaire si votre FAI vous l'a communiquée. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66.
DNS secondaire	Vous devez spécifier l'adresse IP du serveur DNS secondaire si votre FAI vous l'a communiquée. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.

2.2.3 État WAN

Mode	Indique que le mode d'accès à haut débit est actif. Selon le mode d'accès, on a PPPoE, PPTP, PPPoA, Adresse IP statique ou DHCP .
Adresse IP passerelle	Adresse IP de la passerelle.
Adresse IP	Adresse IP de l'interface WAN.
Paquets TX	Nombre total de paquets IP émis au cours de la présente session.
Vitesse TX	Vitesse d'émission en caractères par seconde (cps) pour les données sortantes.
Paquets RX	Nombre total de paquets IP reçus pendant la présente session.
Vitesse RX	Vitesse de réception en caractères par seconde (cps) pour les données entrantes.
Temps actif	Temps de connexion. Le format est HH:MM:SS, où HH, MM, et SS, sont respectivement les heures, les minutes et les secondes.
Abandon/Appel PPPoE ou PPTP	Cliquez sur le lien pour établir ou libérer la connexion PPPoE ou PPTP.

Chapitre 3

Configuration de l'accès à l'internet

3.1 Introduction

Le routeur relie les PC de votre domicile ou de votre bureau à l'internet. Il règle la circulation des données entre votre réseau local et l'internet. La fonctionnalité de traduction d'adresse réseau (NAT) du routeur traduit une adresse IP publique en plusieurs adresses privées d'un réseau local.

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 PC, ont besoin d'une adresse IP. Il existe 3 manières principales d'attribuer des adresses IP à votre routeur : PPPoE, Adresse IP dynamique ou statique et PPTP. L'écran de configuration et les fonctionnalités disponibles diffèrent selon le type de connexion que votre FAI propose.

Le router prend en charge l'interface WAN Ethernet pour l'accès à l'internet. Les paragraphes qui suivent, décrivent la manière de procéder pour configurer votre accès à haut débit.



Si vous avez déjà accès à l'internet (vous avez configuré votre routeur comme indiqué au « Chapitre 1 Assistant de démarrage rapide »), il est inutile de reparamétrer votre connexion internet sauf si vous voulez faire des modifications.

3.2 Paramètres

Pour l'accès à haut débit, vous devez connaître le type d'accès à l'internet fourni par votre FAI.

Cliquez sur **Accès à l'internet** pour ouvrir la page Accès à l'internet.



Les services d'accès à haut débit les plus répandus sont : **Client PPPoE**, **Client PPTP**, **IP statique** pour le DSL, et **IP dynamique (Client DHCP)** pour le câble. Dans la plupart des cas, le fournisseur d'accès à haut débit vous fournira un modem DSL ou câble.

PPPoE	Certains fournisseurs d'accès DSL utilisent le protocole point à point sur Ethernet (PPPoE). Tous les utilisateurs locaux peuvent partager une connexion PPPoE pour accéder à l'internet.
IP statique	L'adresse IP est fixe ou permanente. Choisir cette option si votre FAI vous fournit une adresse IP permanente.
IP dynamique	Choisissez cette option pour « obtenir une adresse IP automatiquement ». Dans la plupart des cas, le modem câble obtiendra une adresse IP dynamique du FAI.
PPTP	Certains fournisseurs d'accès DSL utilise le protocole de tunnel point à point (PPTP). Ce protocole est disponible en Europe et en Israël. Votre modem DSL ne peut accéder à l'internet que par le tunnel PPTP. Vous devez créer un tunnel PPTP qui transporte une session PPP et qui aboutit au modem DSL. Une fois le tunnel établi, ce type de modem transmet la session PPP au FAI. Tant que la session PPP est active, tous les utilisateurs locaux peuvent la partager pour accéder à l'internet.

3.2.1 Utilisation de PPPoE avec un modem DSL

Cliquez sur **Configuration de l'accès à l'internet > PPPoE**.

Mode client PPPoE

Configuration PPPoE Liaison PPPoE <input checked="" type="radio"/> Activer <input type="radio"/> Désactiver Configuration de l'accès au FAI Nom du FAI <input type="text"/> Nom d'utilisateur <input type="text"/> Mot de passe <input type="password"/> Plages horaires (1-15) => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	Configuration du protocole PPP/MP Authentification PPP <input type="text" value="PAP ou CHAP"/> <input type="checkbox"/> Connexion permanente Délai d'inactivité <input type="text" value="180"/> seconde(s) Méthode d'attribution d'adresse IP (IPCP) Adr IP fixe <input type="radio"/> Oui <input checked="" type="radio"/> Non (IP dynamique) Adresse IP fixe <input type="text"/> Type de WAN <input type="text" value="Négociation automatique"/>
---	---

Configuration du protocole PPPoE

Liaison PPPoE : Cliquez sur **Activer** pour activer le protocole de client PPPoE sur l'interface WAN.



N'oubliez pas de supprimer les applications PPPoE qui sont déjà installées sur vos PC s'il vous faut activer PPPoE et que vous êtes des utilisateurs DSL.

Configuration de l'accès au FAI

Nom du FAI : Entrez le nom du service s'il vous été communiqué par votre FAI.

Nom d'utilisateur/Mot de passe : Entrez le nom d'utilisateur et le mot de passe donnés par votre FAI

Plages horaires (1-15) : Entrez jusqu'à 4 numéros de plage horaire pour limiter l'accès à l'internet à ces plages horaires.

Configuration du protocole PPP/MP

Authentification PPP : Sélectionnez PAP ou CHAP pour la compatibilité la plus large possible.

Connexion permanente : Cochez la case si vous voulez une connexion permanente. Le champ **Délai d'inactivité** est alors inaccessible.

Délai d'inactivité : Le routeur se déconnectera automatiquement s'il n'y a pas d'activité pendant un temps déterminé (180 secondes par

défaut). Si vous entrez 0 dans ce champ, la session PPP ne se terminera pas d'elle même

Méthode d'attribution d'adresse IP (IPCP)

IP fixe : Cochez **Non (IP dynamique)**, sauf si votre FAI vous a fourni une adresse IP statique.

Adresse IP fixe : Si votre FAI vous a fourni une adresse IP statique, entrez-la dans ce champ.

Cliquez sur **OK**.

3.2.2 Utilisation d'une adresse IP statique avec un modem

DSL/câble

Vous pouvez recevoir une adresse IP publique fixe ou une adresse de sous réseau publique (c'est-à-dire des adresses IP multiples) de votre fournisseur d'accès DSL ou câble. Grâce au traducteur d'adresse réseau (NAT), il vous suffit d'attribuer une adresse IP publique fixe à l'interface WAN de votre routeur. Votre routeur permettra à tous vos PC de partager l'accès à haut débit car la fonction NAT transforme l'adresse IP fixe en plusieurs adresses IP privées. Cliquez sur **Configuration de l'accès à l'internet > IP statique ou dynamique**.

Contrôle d'accès

Accès à haut débit : Sélectionnez **Activer** pour activer l'accès à haut débit.

Maintenir la connexion WAN

Activer la vérification par PING : Si vous cochez cette case, le routeur vérifiera périodiquement votre connexion internet et la rétablira automatiquement en cas de déconnexion. Normalement, cette fonction est utilisée dans un environnement IP dynamique. Ici, les paramètres sont ignorés.

Configuration de l'accès à l'internet

IP statique ou dynamique (client DHCP)

Contrôle d'accès
 Accès à haut débit Activer Désactiver

Maintenir la connexion WAN
 Activer la vérification par PING
 PING vers IP
 Intervalle entre PING minute(s)

Type de WAN

Protocole RIP
 Activer RIP

Paramètres de réseau IP WAN
 Obtenir une adresse IP automatiquement
 Nom du routeur *
 Nom de domaine *
* : Nécessaire pour certains FAI
 Adresse MAC par défaut
 Spécifier une adresse MAC
 Adresse MAC:

Spécifier une adresse IP Alias IP WAN
 Adresse IP
 Masque de sous-réseau
 Adresse IP de la passerelle

Adresse IP du serveur DNS
 Adresse IP primaire
 Adresse IP secondaire

Paramètres de réseau IP WAN

<i>Spécifier une adresse IP</i>	Si votre FAI vous offre une adresse IP statique (fixe ou permanente), vous devez activer « <i>Spécifier une adresse IP</i> ».
<i>Adresse IP</i>	Adresse IP attribuée à votre routeur par votre FAI. Entrez l'adresse IP du routeur, par exemple, 172.16.2.84.
<i>Masque de sous-réseau</i>	Code d'adresse qui détermine la taille du réseau ; c'est le masque de sous-réseau du routeur, vu par les utilisateurs externes sur l'internet (y compris votre FAI) (par défaut : 255.255.255.0/ 24)
<i>Adresse IP de la passerelle</i>	Adresse IP de la passerelle de votre réseau local (LAN) vers l'internet, par exemple, 172.16.2.5.
<i>Adresse IP du serveur DNS</i>	Vous devez spécifier ici une adresse IP de serveur DNS car votre FAI vous en fournira au moins une. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66. Le système d'adressage par domaines (DNS) traduit les noms de domaine ou de site en adresses internet (URL).
<i>Adresse IP du serveur</i>	Vous pouvez spécifier une adresse IP de serveur

Configuration de l'accès à l'internet

DNS secondaire	secondaire si votre FAI vous en a communiqué une. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.
-----------------------	---

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

État du système

État LAN		DNS primaire 168.95.192.1		DNS secondaire 194.98.0.1		
Adresse IP	Paquets TX	Paquets RX				
192.168.1.1	1828	1570				
État WAN		Adresse IP passerelle 172.16.3.1				
Mode	Adresse IP	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Temps actif
DHCP Client	172.16.3.60	19	1	791	122	0:09:15
>>Appeler PPPoE ou PPTP>>Abandon PPPoE ou PPTP						

3.2.3 Utilisation d'une adresse IP dynamique (client DHCP) avec un modem DSL/câble

Cette application est surtout utilisée par les fournisseurs d'accès câble. Cliquez sur **Configuration de l'accès à l'internet > IP statique ou dynamique** pour afficher la page de paramétrage.

IP statique ou dynamique (client DHCP)

Contrôle d'accès Accès à haut débit <input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Paramètres de réseau IP WAN <input checked="" type="radio"/> Obtenir une adresse IP automatiquement
Maintenir la connexion WAN <input type="checkbox"/> Activer la vérification par PING PING vers IP <input type="text" value="0.0.0.0"/> Intervalle entre PING <input type="text" value="0"/> minute(s)	Nom du routeur <input type="text"/> * Nom de domaine <input type="text"/> * * : Nécessaire pour certains FAI <input checked="" type="radio"/> Adresse MAC par défaut <input type="radio"/> Spécifier une adresse MAC
Type de WAN Négociation automatique ▼	Adresse MAC: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="2E"/> <input type="text" value="A4"/> <input type="text" value="5F"/>
Protocole RIP <input type="checkbox"/> Activer RIP	<input type="radio"/> Spécifier une adresse IP <input type="text" value="Alias IP WAN"/> Adresse IP <input type="text"/> Masque de sous-réseau <input type="text"/> Adresse IP de la passerelle <input type="text"/>
	Adresse IP du serveur DNS Adresse IP primaire <input type="text"/> Adresse IP secondaire <input type="text"/>

Contrôle d'accès

Accès à haut débit : Sélectionnez **Activer** pour activer l'accès à haut débit.

Maintenir la connexion WAN

Activer la vérification par PING : Cochez cette case pour activer la vérification par PING. Normalement, cette fonction est utilisée dans un environnement IP dynamique. Si vous avez besoin de l'activer, entrez une adresse IP publique dans le champ **PING vers IP** et un délai dans le champ **Intervalle entre PING**.

Paramètres de réseau IP WAN

Obtenir une adresse IP automatiquement	Cette option doit être activée.
Nom du routeur	Selon votre fournisseur d'accès câble, ce champ peut ou non rester vide. Certains FAI exigent ce nom pour l'authentification de l'accès.
Nom de domaine	Selon votre fournisseur d'accès câble, ce champ peut ou non rester vide.
Adresse MAC par défaut & Spécifier une adresse MAC	Ces deux options s'excluent mutuellement. Certains fournisseurs d'accès câble utilisent un adresse MAC spécifique pour l'authentification de l'accès. Dans ce cas, vous devez cocher la case Spécifier une adresse MAC et entrez l'adresse MAC dans les champs Adresse MAC . Cliquez sur OK et redémarrez le routeur pour que les paramètres soient pris en compte.

3.2.4 Utilisation du protocole PPTP avec un modem DSL

Cliquez sur **Configuration de l'accès à l'internet > PPTP** pour afficher la page de paramétrage. Nous utilisons un exemple pour expliquer la manière de procéder. Les paramètres exacts devraient vous être fournis par votre fournisseur d'accès DSL.

Configuration de l'accès à l'internet

Mode client PPTP

Configuration PPTP Liaison PPTP <input checked="" type="radio"/> Activer <input type="radio"/> Désactiver Serveur PPTP <input type="text" value="10.0.0.138"/>	Configuration PPP Authentification PPP <input type="text" value="PAP ou CHAP"/> <input type="checkbox"/> Connexion permanente Délai d'inactivité <input type="text" value="180"/> seconde(s)
Configuration de l'accès au FAI Nom du FAI <input type="text"/> Nom d'utilisateur <input type="text"/> Mot de passe <input type="text"/> Plages horaires (1-15) => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	Méthode d'attribution d'adresse IP (IPCP) Adr IP fixe <input type="radio"/> Oui <input checked="" type="radio"/> Non (IP dynamique) Adresse IP fixe <input type="text"/> Paramètres du réseau IP LAN2/WAN <input type="radio"/> Obtenir une adresse IP automatiquement <input checked="" type="radio"/> Spécifier une adresse IP Adresse IP <input type="text" value="10.0.0.150"/> Masque de sous-réseau <input type="text" value="255.0.0.0"/>
	Type de WAN <input type="text" value="Négociation automatique"/>

Configuration protocole PPTP

Liaison PPTP	Cochez Activer pour permettre à un client PPTP d'établir un tunnel vers un modem DSL sur l'interface WAN.
Adresse IP du serveur PPTP	Spécifiez l'adresse IP du modem DSL prenant en charge le protocole PPTP. Reportez-vous au manuel d'utilisation de ce modem.

Configuration de l'accès au FAI

Nom du FAI : Entrez le nom du service s'il vous été communiqué par votre FAI.

Nom d'utilisateur/Mot de passe : Entrez le nom d'utilisateur et le mot de passe donnés par votre FAI

Plages horaires (1-15) : Entrez jusqu'à 4 numéros de plage horaire pour limiter l'accès à l'internet à ces plages horaires.

Configuration de l'accès à l'internet

Configuration PPP/MP

<i>Authentification PPP</i>	Sélectionnez PAP ou CHAP pour la compatibilité la plus large possible.
<i>Connexion permanente</i>	Cochez la case si vous voulez une connexion permanente. Le champ Délai d'inactivité est alors inaccessible.
<i>Délai d'inactivité</i>	Le routeur se déconnectera automatiquement s'il n'y a pas d'activité pendant un temps déterminé (180 secondes par défaut). Si vous entrez 0 dans ce champ, la session PPP ne se terminera pas d'elle-même.
<i>Méthode d'attribution d'adresse IP (IPCP)</i>	IP fixe : Cochez Non (IP dynamique), sauf si votre FAI vous a fourni une adresse IP statique. Adresse IP fixe : Si votre FAI vous a fourni une adresse IP statique, entrez-la dans ce champ.

Paramètres de réseau IP WAN

<i>Obtenir une adresse IP automatiquement</i>	L'interface WAN est configurée en client DHCP qui demandera les paramètres IP au serveur DHCP ou au modem DSL prenant en charge le protocole PPTP.
<i>Spécifier une adresse IP</i>	Si vous n'êtes pas certain(e) qu'il y ait des services DHCP sur l'interface WAN, vous pouvez attribuer manuellement une adresse IP à l'interface. À noter que l'adresse IP et le masque de sous-réseau doivent être attribués au sein du même réseau que le modem DSL à protocole PPTP.

Chapitre 4

Configuration du LAN

4.1 Introduction

Ce chapitre décrit la manière de procéder pour configurer le LAN.

4.2 Paramètres

Cliquez sur **LAN** pour ouvrir la page de configuration du LAN.



4.2.1 Paramètres TCP/IP et DHCP du LAN

Configuration du réseau IP LAN

L'adresse IP et le masque de sous-réseau servent à regrouper les utilisateurs sur votre LAN. Par exemple, vous pouvez mettre l'ordinateur de vos enfants en réseau avec votre propre ordinateur afin de partager l'accès à haut débit et les fichiers.

À usage NAT : (toujours activé par défaut)

Configuration TCP/IP et DHCP Ethernet	
Configuration du réseau IP LAN	
À usage NAT	
1re adresse IP	192.168.1.1
Premier masque de sous-réseau	255.255.255.0

Adresse IP : Adresse IP privée permettant de se connecter à un réseau local (valeur par défaut : 192.168.1.1).

Masque de sous-réseau : Code d'adresse qui détermine la taille du réseau ; c'est le masque de sous-réseau du routeur, vu par les utilisateurs externes sur l'internet (y compris votre FAI).

Configuration du LAN

(valeur par défaut : 255.255.255.0/ 24)

Configuration du serveur DHCP

Le sigle DHCP signifie Dynamic Host Configuration Protocol (protocole de configuration dynamique de machine hôte). Par défaut, le routeur joue le rôle de serveur DHCP pour votre réseau. Il peut donc transmettre automatiquement les paramètres IP appropriés à n'importe quel 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.

Pour la configuration du serveur DHCP, voir l'exemple ci-dessous.

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

Adresse IP primaire : 168.95.1.1

Adresse IP secondaire :

Activer le serveur	Le routeur attribue automatiquement une adresse IP à tous les PC du réseau local
Désactiver le serveur	Vous attribuez manuellement une adresse IP à tous les PC du réseau local à partir du routeur
Agent relais	Permet aux PC du réseau local de demander une adresse IP à un autre serveur DHCP ; par exemple, au serveur DHCP situé dans votre bureau.
Adresse IP de début	Adresse IP de début du pool d'adresses IP.
Nombre d'adresses du pool IP	Nombre d'adresses du pool IP.
Adresse IP de la passerelle	Adresse IP de passerelle pour le serveur DHCP. C'est généralement la même que celle du routeur lorsque celui-ci fonctionne en passerelle par défaut.
Adresse IP du serveur DNS	Le sigle DNS signifie Domain Name System (système d'adressage par domaines). Sur l'internet, chaque machine

Configuration du LAN

serveur DNS (par défaut : Néant)	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 au moins une. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66.
Adresse IP secondaire	Vous pouvez spécifier une adresse IP de serveur secondaire si votre FAI vous en a communiqué une. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.

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

État du système

Système démarré depuis:0:15:23

État LAN		DNS primaire	168.95.192.1	DNS secondaire	194.98.0.1	
Adresse IP		Paquets TX	Paquets RX			
192.168.1.1		2450	2093			
État WAN		Adresse IP passerelle		172.16.3.1		
Mode	Adresse IP	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Temps actif
DHCP Client	172.16.3.60	27	1	1275	279	0:15:16
>>Appeler PPPoE ou PPTP>> Abandon PPPoE ou PPTP						



Si les deux champs d'adresse IP primaire et secondaire sont laissés vides, le routeur attribue sa propre adresse IP aux utilisateurs 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).

Chapitre 5

Paramétrage du NAT

5.1 Introduction

Le traducteur d'adresse réseau (NAT) transpose une ou plusieurs adresses IP, un ou plusieurs ports de service en différents services. Il permet de traduire les adresses IP internes de nombreux ordinateurs d'un réseau local (LAN) en une seule adresse publique, ce qui fait faire des économies aux utilisateurs. Il joue également un rôle de sécurisation en cachant les adresses IP réelles de machines importantes aux fouineurs (« hackers ») potentiels. Par commodité, nous appelons un routeur doté de la fonctionnalité NAT un routeur NAT.

Vous utilisez normalement votre routeur Vigor comme un routeur NAT. Le routeur NAT obtient une adresse IP globalement reroutable du FAI et attribue aux hôtes locaux des adresses IP privées définies par le RFC 1918. Le routeur traduit les adresses IP privées en l'adresse IP globalement reroutable afin que les hôtes locaux puissent communiquer avec le routeur et accéder à l'internet.

5.2 Paramètres

Cliquez sur **Paramétrage du NAT** pour ouvrir la page de paramétrage.



Dans la page 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. D'autre part, 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 routeurs Vigor autorisent 3 méthodes de mappage de ports :

Redirection de ports, Ouverture de ports et Hôte DMZ

Redirection de ports	Le paquet est transmis à un hôte local spécifique si le numéro de port correspond à celui défini dans la table. Un utilisateur peut aussi rediriger localement le port vers un autre port.
Ouverture de ports	Cette fonction est semblable à la fonction de redirection de ports. Elle permet de définir une plage de ports.
Hôte DMZ	Cette fonction ouvre complètement une machine hôte particulière. Tous les paquets entrants sont transmis à la machine hôte dont vous avez spécifié l'adresse IP locale. Seules exceptions : les paquets reçus en réponse à des requêtes sortantes d'autres ordinateurs locaux ou les paquets entrants qui correspondent à des règles des deux autres méthodes.

À noter que si vous utilisez une combinaison de ces trois systèmes, il y a une hiérarchisation. Si une règle d'une méthode est en conflit avec une règle d'une autre méthode, il y a un ordre de priorité strict qui permet d'obtenir un résultat prévisible et la résolution du conflit. L'ordre de priorité est le suivant :

Redirection de ports > Ouverture de ports > Hôte DMZ

Exemple : Si le numéro de port d'un paquet entrant correspond à une règle édictée dans **Redirection de ports** et dans **Ouverture de ports**, le paquet est transmis à l'adresse locale indiquée dans **Redirection de ports**.

Nous allons maintenant passer au paramétrage de ces trois méthodes de mappage.

5.2.1 Table de redirection de ports

La **redirection de ports** sert à exposer des serveurs internes au domaine public. Par exemple, vous exploitez un serveur web et certains utilisateurs essaient d'accéder à ce serveur. Vous exploitez également un serveur de messagerie SMTP interne pour votre bureau et vous voulez permettre à votre FAI d'envoyer tout votre courrier électronique à votre serveur de messagerie SMTP. Par conséquent, vous affectez différents numéros de port de la **table de redirection de ports** à différents services, tels que http, smtp, ftp etc. Les utilisateurs externes, c'est-à-dire les autres internautes, peuvent alors accéder à votre serveur web en utilisant votre adresse IP publique. Même si votre adresse IP publique est une adresse IP dynamique, vous pouvez utiliser le service DNS dynamique pour obtenir une adresse IP de WAN en ligne (comme hostnmae.dyndns.org) pointant vers votre adresse IP dynamique actuelle. N'importe quel utilisateur externe pourra visiter votre serveur web en utilisant votre adresse IP de WAN en ligne.

Paramétrage du NAT

L'exemple suivant montre comment un serveur FTP interne est exposé au domaine public. Le serveur FTP interne fonctionne sur la machine hôte locale dont l'adresse est 192.168.1.10.

Table de redirection de ports

Index	Nom du service	Protocole	Port public	Adr IP privé	Port privé	Actif
1	FTP	TCP	21	192.168.1.10	21	<input checked="" type="checkbox"/>
2		---	0		0	<input type="checkbox"/>
3		---	0		0	<input type="checkbox"/>
4		---	0		0	<input type="checkbox"/>
5		---	0		0	<input type="checkbox"/>
6		---	0		0	<input type="checkbox"/>
7		---	0		0	<input type="checkbox"/>
8		---	0		0	<input type="checkbox"/>
9		---	0		0	<input type="checkbox"/>
10		---	0		0	<input type="checkbox"/>

Dans cet exemple, la **table de redirection de ports** permet de définir 10 redirections pour les machines hôte internes.

Nom du service	Spécifiez le nom du service réseau.
Protocole	Spécifiez le protocole de transport (TCP ou UDP).
Port public	Spécifiez quel port doit être redirigé vers la machine hôte interne.
Adresse IP privée	Spécifiez l'adresse IP privée de la machine hôte interne offrant le service.
Port privé	Spécifiez le numéro de port privé du service offert par la machine hôte interne.
Actif	Cochez cette case pour activer la redirection.



Comme le routeur possède son propre serveur web de configuration, si vous voulez accéder au configurateur web à distance et à un serveur web situé derrière le routeur, il vous faut définir comme « port » http du routeur un port autre que le **port par défaut 80**. Vous devez changer le port d'administration à partir du menu **Paramètres de gestion**, puis vous accédez à l'écran d'administration en faisant suivre l'adresse IP normale du configurateur web du routeur Vigor de 8080. Par exemple : **http://192.168.1.1:8080**

Paramétrage du NAT

Paramètres de gestion	
Contrôle d'accès pour la gestion	
<input type="checkbox"/>	Activer la mise à jour à distance du firmware (FTP)
<input type="checkbox"/>	Autoriser la gestion à partir de l'internet
<input checked="" type="checkbox"/>	Désactiver le PING en provenance de l'internet
Liste des accès	
Liste IP	Masque de sous-réseau
Paramétrage du port de gestion	
<input type="radio"/> Ports par défaut (Telnet:23, HTTP:80, FTP:21)	
<input checked="" type="radio"/> Ports définis par l'utilisateur	
Port Telnet	:23
Port HTTP	:80
Port FTP	:21



La redirection de ports n'est applicable qu'aux utilisateurs externes, c'est-à-dire au trafic entrant. Les utilisateurs internes, derrière votre LAN, ne peuvent pas accéder à vos adresses IP publiques externes ; ils accèdent au serveur par son adresse IP privée locale. Vous pouvez aussi définir un alias dans un fichier d'hôtes Windows. Redirigez uniquement les ports qui doivent l'être et non tous les ports. Autrement, vous compromettez la sécurité de type pare-feu mise en place initialement par la fonction NAT.

5.2.2 Configuration de l'hôte DMZ

La **redirection de ports** peut diriger le trafic UDP/TCP présent sur des ports particuliers vers des clients internes spécifiques du LAN. Cependant, d'autres protocoles IP, comme les protocoles 50 (ESP) et 51 (AH) n'ont pas de numéro de port et vous ne pouvez donc pas déterminer à quel client local transmettre les données. Le routeur Vigor a une fonction dite « hôte DMZ » qui vous permet de faire en sorte que TOUTES les données non sollicitées soient transmises, quel que soit le protocole, vers un client local déterminé (doté d'une adresse IP privée). La navigation normale sur l'internet et autres activités de ce genre des autres clients peuvent se poursuivre sans interruption intempestive.

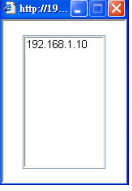


Si vous configurez un hôte DMZ, vous compromettez dans une certaine mesure les propriétés de sécurité inhérentes au NAT. Vous pouvez envisager d'ajouter des règles de filtrage supplémentaires ou un pare-feu secondaire.

Cliquez sur **Configuration de l'hôte DMZ** pour ouvrir la page de paramétrage. L'hôte DMZ permet d'exposer un utilisateur interne déterminé sur l'internet afin d'utiliser certaines applications spéciales, comme Netmeeting, des jeux, etc.

Configuration de l'hôte DMZ	
Activer	Adresse IP privée
<input checked="" type="checkbox"/>	192 168 1 10
	<input type="button" value="Choisir un PC"/>

Paramétrage du NAT

Activer	Cochez cette case pour activer la fonction Hôte DMZ.
Adresse IP privée	Entrez l'adresse IP privée de l'hôte DMZ.
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.

5.2.3 Ouverture de ports

Cette fonction est semblable à la redirection de ports (voir plus haut) mais elle vous permet de définir **une plage de ports**.

L'écran suivant montre la **configuration de l'ouverture de ports**. Dans le routeur Vigor, la fonction **Ouverture de ports** permet de définir 10 redirections pour les hôtes internes.

Configuration de l'ouverture de ports Effacer tout

Index	Commentaire	Adresse IP locale	État
1.			X
2.			X
3.			X
4.			X
5.			X
6.			X
7.			X
8.			X
9.			X
10.			X

Index	Numéro d'ordre de la redirection de port à définir. Cliquez sur le numéro approprié pour modifier ou effacer la redirection correspondante.
Commentaires	Spécifiez le nom du service réseau.
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.

Comme indiqué ci-dessus, lorsque vous cliquez sur un numéro d'index, par exemple « 1 », la page suivante apparaît. Pour chaque machine du réseau local, vous pouvez spécifier 10 plages de ports pour divers services. Les différentes possibilités sont décrites ci-dessous.

Paramétrage du NAT

Index n°1

Activer l'ouverture de ports

Commentaire

Ordinateur local

	Protocole	Du port	Au port		Protocole	Du port	Au port
1.	TCP	6005	6006	6.	----	0	0
2.	----	0	0	7.	----	0	0
3.	----	0	0	8.	----	0	0
4.	----	0	0	9.	----	0	0
5.	----	0	0	10.	----	0	0

Activer l'ouverture de ports	Cochez cette case pour activer la fonction d'ouverture de ports pour cette machine locale.
Commentaires	Spécifiez le nom du service réseau.
Ordinateur local	Entrez l'adresse IP privée de la machine locale.
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.

5.2.4 Liste des ports connus

Cette page donne la liste de certains numéros de port connus.

Liste des ports connus

Service/Application	Protocole	Numéro de port
Protocole de transfert de fichiers (FTP)	TCP	21
Protocole de connexion à distance SSH (exemple : pcAnywhere)	UDP	22
Telnet	TCP	23
Protocole de transport de message simple (SMTP)	TCP	25
Serveur de nom de domaine (DNS)	UDP	53
Serveur WWW (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

Chapitre 6

Paramétrage du pare-feu

6.1 Introduction

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

Avant tout, il est recommandé, lors de l'installation du routeur, de définir un nom d'utilisateur et un mot de passe pour empêcher l'accès non autorisé au routeur.

Tapez le mot de passe

Il n'y a pas de mot de passe par défaut. Pour votre sécurité, choisissez une série de chiffres ou de lettres (23 caractères maximum) comme **mot de passe** et tapez-les dans le champ Mot de passe.

Nouveau mot de
passe

Retapez le nouveau
mot de passe

Si un mot de passe n'a pas été défini lors de l'installation, vous pouvez en définir un en mode maintenance du système.

Mot de passe administrateur

Ancien mot de passe	:	<input type="text"/>
Nouveau mot de passe	:	<input type="text"/>
Retapez le nouveau mot de passe	:	<input type="text"/>

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

Paramétrage du pare-feu

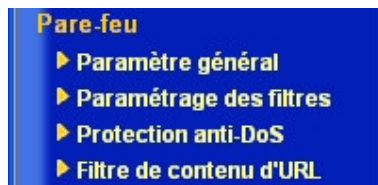
- Filtre IP
- Inspection des paquets en fonction de l'état de la connexion (filtrage adaptatif) : refus des données entrantes non sollicitées
- Protection anti-DoS/DDoS
- Filtre de paquets configurable par l'utilisateur



Pour activer la fonction SPI (Stateful Packet Inspection), suivez le chemin : Pare-feu>Modifier la règle de filtrage>Garder l'état

6.2 Paramétrage

Cliquez sur **Paramétrage du pare-feu** pour ouvrir la page de paramétrage.



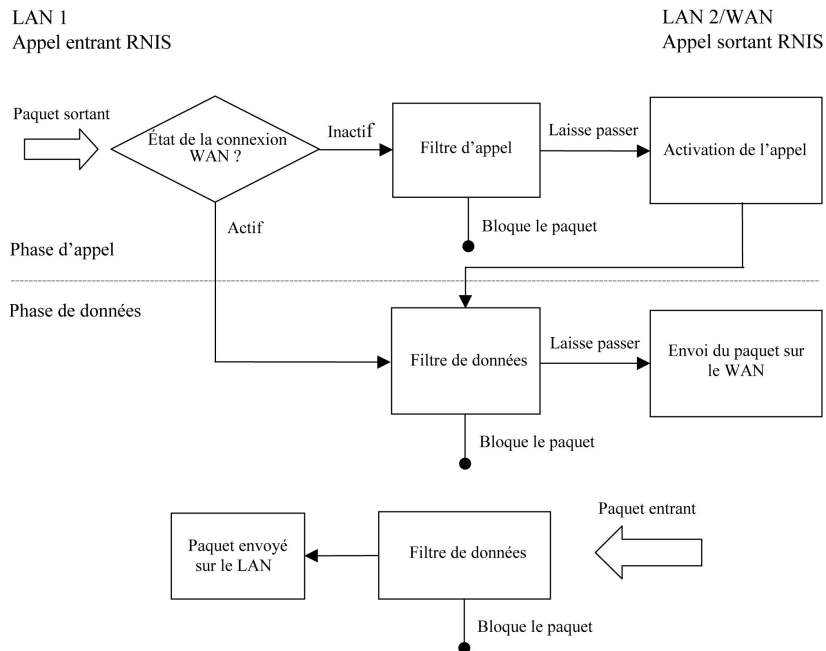
Configuration générale	Paramètres généraux du filtre d'appel et du filtre de données.
Paramétrage du filtre	Vous avez la possibilité de configurer 12 filtres IP.
Protection anti-DoS	Cliquez sur cette option pour paramétrer la protection anti-DoS afin de détecter les attaques de type DoS et d'en atténuer les effets.
Filtre de contenu d'URL	Permet de bloquer les données provenant de sites web indésirables afin de protéger les enfants à l'école ou à la maison.

La fonction de **configuration générale** permet d'activer, par défaut, deux types de filtre : un filtre d'appel et un filtre de données. Le filtre d'appel sert pour les utilisateurs qui tentent de se connecter à l'internet à partir du réseau local. Le filtre de données sert à déterminer quel type de paquet IP laisser passer par le routeur après l'établissement de la connexion WAN.

Conceptuellement, lorsqu'un paquet sortant doit être routé vers le WAN, le filtre IP décide s'il doit être transféré au filtre d'appel ou au filtre de données. Si la connexion WAN n'est pas établie, le paquet est transféré au filtre d'appel. Si le paquet n'est pas autorisé à déclencher un appel du routeur, il est rejeté. Autrement, il déclenche un appel pour établir la connexion WAN.

Paramétrage du pare-feu

Si la connexion WAN du routeur est active, le paquet est transféré au filtre de données. Si le type de paquet est censé être bloqué, il est rejeté. Sinon, il est envoyé à l'interface WAN. Si un paquet entrant arrive de l'interface WAN, il est transféré directement au filtre de données. Si le type de paquet est censé être bloqué, il est rejeté. Sinon, il est envoyé sur le LAN. Le processus de filtrage est représenté schématiquement ci-après.



Les paragraphes qui suivent décrivent la **configuration générale** et le **paramétrage des filtres**. Le routeur Vigor permet de configurer 12 filtres avec 7 règles de filtrage chacun. On a donc un total de 84 règles de filtrage.

Paramétrage du pare-feu

Filtre1		Paramétrage des filtres		
Commentaires : Default Call Filter		Set	Commentaires	Set
Règle de filtrage	Actif	1.	Default Call Filter	7.
1	<input checked="" type="checkbox"/>	2.	Default Data Filter	8.
2	<input type="checkbox"/>	3.		9.
3	<input type="checkbox"/>	4.		10.
4	<input type="checkbox"/>	5.		11.
5	<input type="checkbox"/>	6.		12.
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			

On a donc un total de 84 r. gles de filtrage

Par défaut, le filtre d'appel est le filtre 1 et le filtre de données est le filtre 2.

Configuration générale

Filtre d'appel	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Début du filtrage à partir du <input type="text" value="Filtre n°1"/>
Filtre de données	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Début du filtrage à partir du <input type="text" value="Filtre n°2"/>

La **protection anti-DoS** vous aide à détecter les attaques de type « déni de service » (DoS) et à en atténuer les effets. Ces attaques comprennent 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.

Le moteur de protection anti-DoS confronte chaque paquet entrant avec la base de données de signatures d'attaque. Tout paquet susceptible de paralyser la machine hôte dans la zone de sécurité est bloqué et un message SysLog est envoyé au client. Le moteur de protection anti-DoS surveille également le trafic. Toute situation anormale violant la configuration de l'administrateur est signalée et la fonction de protection correspondante est mise en œuvre.

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

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

Les systèmes de filtrage de contenu d'URL sont des outils qui équivalent dans le cyberspace aux barrières physiques employées pour limiter l'accès à certains documents. En déterminant que tel ou tel site est inconvenant et en refusant de l'afficher sur l'écran de l'ordinateur, les fonctions de filtrage de contenu d'URL permettent d'empêcher les enfants de voir des contenus que leurs parents jugent choquants. Le filtrage de contenu d'URL se comporte comme une version automatisée du commerçant qui refuse de vendre des magazines pour adultes à des collégiens. Le filtrage de contenu d'URL est également utilisé par les entreprises pour empêcher les employés d'accéder à des ressources internet qui n'ont pas de rapport avec le travail ou qui sont jugées inconvenantes.

Le filtrage de contenu d'URL vérifie le contenu des d'URL. Un pare-feu traditionnel inspecte les paquets sur la base des champs des en-têtes TCP/IP, tandis que le filtrage de contenu d'URL vérifie les URL ou la charge utile des paquets TCP/IP. Dans les routeurs Vigor, le filtrage de contenu d'URL inspecte la chaîne de l'URL et certaines données HTTP cachées dans la charge utile des paquets TCP.

6.2.1 Configuration générale

Dans la page Configuration générale, vous pouvez activer ou désactiver le filtrage d'appel ou le filtrage de données et spécifier un filtre de début dans chaque cas, configurer la journalisation et spécifier une adresse MAC pour la duplication des paquets journalisés.

Paramétrage du pare-feu

Configuration générale

Filtre d'appel	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Début du filtrage à partir du Filtre n°1
Filtre de données	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Début du filtrage à partir du Filtre n°2
Journalisation	Néant	
Adresse MAC pour la duplication des paquets journalisés		
<input type="text" value="0x000000000000"/>		
<input checked="" type="checkbox"/> Accepter les paquets UDP fragmentés entrants (pour certains jeux, ex. CS)		



Certains jeux en ligne (par exemple, Half Life) utilise des paquets UDP très longs. Ces paquets UDP doivent être fragmentés. Si vous ne cochez pas la case « Accepter les paquets UDP fragmentés entrants », le routeur Vigor rejettera ce type de paquet pour éviter les attaques extérieures. Vous pouvez activer l'option « Accepter les paquets UDP fragmentés entrants » et participer à ce type de jeux en ligne. Si la sécurité est votre souci principal, décochez la case « Accepter les paquets UDP fragmentés entrants ».

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 est inactive.
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.



Le fichier de journalisation sera affiché sur le terminal Telnet lorsque vous taperez la commande « log -f ».

Adresse MAC pour la duplication des paquets journalisés

Les paquets journalisés peuvent également être dupliqués ailleurs sur le réseau Ethernet. Si vous voulez dupliquer les paquets journalisés sur une autre machine du réseau, vous devez entrer l'adresse MAC de celle-ci (en format hexadécimal). Tapez « 0 » pour désactiver la fonction. Cette fonction est utile dans un environnement Ethernet.

6.2.2 Paramétrage des filtres

Filtre1

Commentaires : Default Call Filter

Règle de filtrage	Actif	Commentaires
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

Filtre suivant Néant ▼

Commentaires

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

Règles de filtrage

Cliquez sur l'un des boutons **1 à 7** pour éditer/modifier la règle de filtrage.

Actif

Active ou désactive la règle de filtrage.

Filtre suivant

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

Éditer/modifier les règles de filtrage

Cliquez sur le numéro de règle de filtrage pour afficher la page de configuration des règles de filtrage propres à chaque filtre

Filtre1Règle7

Commentaires : **Cocher pour activer la règle de filtrage**

Laisser passer ou bloquer		Appliquer un autre filtre			
Laisser passer immédiatement <input type="button" value="v"/>		Néant <input type="button" value="v"/>			
<input type="checkbox"/> Dupliquer sur LAN		<input type="checkbox"/> Journaliser			
Sens <input type="button" value="v"/>		Protocole n'importe laquelle <input type="button" value="v"/>			
	Adresse IP	Masque de sous-réseau	Opérateur	Du port	Au port
Source	any <input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	= <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
Destination	any <input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	= <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Garder l'état		Fragments Néant <input type="button" value="v"/>			

Commentaires

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

Cocher pour activer la règle de filtrage

Active la règle de filtrage.

Laisser passer ou bloquer

Spécifiez l'action que doit avoir la règle sur les paquets.

<i>Bloquer immédiatement</i>	Les paquets correspondants à la règle sont rejetés immédiatement.
<i>Laisser passer immédiatement</i>	Les paquets correspondants à la règle sont passés immédiatement.
<i>Bloquer si plus de corresp.</i>	Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est rejeté.
<i>Laisser passer si plus de corresp.</i>	Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est passé.

Appliquer un autre filtre

Si le paquet correspond à la règle de filtrage, la règle de filtrage suivante fait passer au filtre spécifié.

Dupliquer sur LAN

Si vous voulez que les paquets filtré soient enregistrés sur une autre machine du réseau, cochez cette case.

L'adresse MAC de la machine spécifiée est définie dans **Pare-feu >> Configuration générale >> Adresse MAC pour la duplication des paquets journalisés.**

Adresse MAC pour la duplication des paquets journalisés

0x

Journal

Cochez cette case pour activer la fonction de journalisation. Pour visualiser les journaux, utilisez la commande Telnet **log-f**.

Sens

Définit la direction des paquets. Dans le cas du filtrage d'appel, ce paramètre est sans objet.

Garder l'état et Fragments (filtrage de données seulement)

Ces options doivent être accompagnées des paramètres suivant :

E : Spécifie la règle de filtrage des paquets entrants.

S : Spécifie la règle de filtrage des paquets sortants.

Protocole : Spécifie le ou les protocoles auxquels s'applique cette règle de filtrage.

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.

Masque de sous-réseau : Spécifiez le masque de sous-réseau correspondant aux adresses IP

Paramétrage du pare-feu

Opérateur : La colonne opérateur précise les ports concernés. Si le champ **Du port** est vide, les colonnes **Du port** et **Au port** sont ignorées. La règle de filtrage s'applique à tous les ports.

= : Si le champ **Au port** est vide, la règle de filtrage s'applique au seul port dont le numéro figure dans le champ **Du port**. Sinon, la règle de filtrage s'applique à la plage de ports définie par les champs **Du port** et **Au port**.

!= : Si le champ **Au port** est vide, la règle de filtrage s'applique à tous les ports à l'exception de celui dont le numéro figure dans le champ **Du port**. Sinon, elle s'applique à tous les ports à l'exception de la plage de ports définie par les champs **Du port** et **Au port**.

> : La règle de filtrage s'applique au port dont le numéro figure dans le champ **Du port** et à tous les ports supérieurs.

< : La règle de filtrage s'applique au port dont le numéro figure dans le champ **Du port** et à tous les ports inférieurs.

Garder l'état : c'est-à-dire **Filtrage adaptatif des paquets**. Bloque les données entrantes non sollicitées. Comme protocole, vous pouvez choisir TCP ou UDP ou TCP/UDP ou ICMP.

Filtre1Règle2

Commentaires :

Cocher pour activer la règle de filtrage

Laisser passer ou bloquer		Appliquer un autre filtre	
<input type="button" value="Laisser passer immédiatement"/>		<input type="button" value="Néant"/>	
<input type="checkbox"/> Dupliquer sur LAN		<input type="checkbox"/> Journaliser	
Sens <input type="button" value="S"/>		Protocole n'importe laquelle	
		<input type="button" value="n'importe laquelle"/>	
	Adresse IP	Masque de sous-réseau	
Source	<input type="text" value="any"/>	<input type="button" value="255.255.255.255 (/32)"/>	
Destination	<input type="text" value="any"/>	<input type="button" value="255.255.255.255 (/32)"/>	
<input checked="" type="checkbox"/> Garder l'état		Fragments <input type="button" value="Néant"/>	

Paramétrage du pare-feu

Fragments : Spécifiez une action sur les paquets fragmentés.

Néant	Aucune option concernant les fragments dans la règle de filtrage.
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.

Exemple d'interdiction d'accès à des services internet non autorisés

Cette section décrit un exemple simple d'interdiction d'accès à des service WWW. Dans cet exemple, nous supposons que l'adresse IP de l'utilisateur à accès restreint est 192.168.1.10. La règle de filtrage est créée dans le filtre de donnée. Le port 80 correspond au port http.

Filtre2Règle2

Commentaires : Cocher pour activer la règle de filtrage

Laisser passer ou bloquer		Appliquer un autre filtre			
<input type="text" value="Bloquer immédiatement"/>		<input type="text" value="Néant"/>			
<input type="checkbox"/> Dupliquer sur LAN		<input type="checkbox"/> Journaliser			
Sens <input type="text" value="S"/>		Protocole <input type="text" value="TCP"/>			
	Adresse IP	Masque de sous-réseau	Opérateur	Du port	Au port
Source	<input type="text" value="192.168.1.10"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="any"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text" value="80"/>	<input type="text"/>
<input type="checkbox"/> Garder l'état		Fragments <input type="text" value="Néant"/>			

6.2.3 Protection anti-DoS (dénis de service)

Les paragraphes suivants décrivent la manière de procéder pour paramétrer la protection anti-DoS à l'aide du configurateur web. La protection anti-DoS est une sous-fonction de la fonctionnalité de filtre IP/pare-feu. Il y a 15 sortes de protection au total. Par défaut, la fonctionnalité de protection anti-DoS est désactivée. En outre, une fois la fonctionnalité de protection anti-DoS activée, les seuils et les temporisations que comportent certaines fonctions prennent leur valeurs par défaut, soit respectivement 300 paquets par secondes et 10 secondes. Une description succincte de chaque protection est donnée ci-après.

Configuration de la protection anti-DoS

<input type="checkbox"/> Activer la protection anti-DoS	
<input type="checkbox"/> Activer la protection contre l'inondation SYN	Seuil <input type="text" value="300"/> paquets / s Temporisation <input type="text" value="10"/> s
<input type="checkbox"/> Activer la protection contre l'inondation UDP	Seuil <input type="text" value="300"/> paquets / s Temporisation <input type="text" value="10"/> s
<input type="checkbox"/> Activer la protection contre l'inondation ICMP	Seuil <input type="text" value="300"/> paquets / s Temporisation <input type="text" value="10"/> s
<input type="checkbox"/> Activer la détection de la scrutation de port	Seuil <input type="text" value="300"/> paquets / s
<input type="checkbox"/> Bloquer les options IP	<input type="checkbox"/> Bloquer la scrutation de flag TCP
<input type="checkbox"/> Bloquer le "land"	<input type="checkbox"/> Bloquer le "tear drop"
<input type="checkbox"/> Bloquer le "smurf"	<input type="checkbox"/> Bloquer le "ping of Death"
<input type="checkbox"/> Bloquer le "trace route"	<input type="checkbox"/> Bloquer les fragments ICMP
<input type="checkbox"/> Bloquer les fragments SYN	<input type="checkbox"/> Bloquer les inconnusProtocole
<input type="checkbox"/> Bloquer le "fraggle"	

Activer la protection anti-DoS

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

Activer la protection contre l'inondation SYN

Cliquez sur la case à cocher pour activer la protection contre l'inondation SYN. Si le nombre de paquets SYN TCP provenant de l'internet dépasse le seuil défini par l'utilisateur, le routeur Vigor rejette les paquets SYN TCP qui suivent pendant le temps défini par l'utilisateur. L'objectif principal est de protéger le routeur Vigor contre les paquets SYN TCP qui visent à épuiser les ressources limitées du routeur. Par défaut, le seuil et la temporisation ont respectivement pour valeur 300 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation UDP

Cliquez sur la case à cocher pour activer la fonction de protection contre l'inondation UDP. Lorsque le nombre de paquets UDP provenant de l'internet dépasse le seuil défini par l'utilisateur, le routeur rejette tous les paquets UDP qui suivent pendant le temps défini par l'utilisateur. Le seuil et la temporisation ont respectivement pour valeur par défaut 300 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation ICMP

Cliquez sur la case à cocher pour activer la fonction de protection contre l'inondation ICMP. Lorsque le nombre de paquets ICMP provenant de l'internet dépasse le seuil défini par l'utilisateur, le routeur rejette tous les paquets ICMP qui suivent pendant le temps défini par l'utilisateur. Le seuil et la temporisation ont respectivement pour valeur par défaut 300 paquets par seconde et 10 secondes.

Activer la détection de la scrutation de port

Une attaque par scrutation de port consiste à envoyer des paquets avec différents numéros de port pour tenter de déterminer à quel services un port répond. Pour activer la fonction de détection de scrutation de port de votre routeur Vigor, cliquez sur la case à cocher. Le routeur Vigor détectera la tentative de scrutation et la signalera par un message d'avertissement si le nombre de paquets par seconde sur le port dépasse le seuil défini par l'utilisateur. Le seuil par défaut est de 300 paquets par seconde.

Bloquer les options IP

Cliquez sur la case à cocher 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 servent aux machines hôtes pour envoyer certaines informations importantes, tel que des paramètres de sécurité, de compartimentage, TCC (groupe fermé d'utilisateurs), une série d'adresses internet, des messages de routage, etc. qu'un attaquant potentiel peut analyser pour obtenir des renseignements sur vos réseaux privés.

Bloquer le « land »

Cliquez sur la case à cocher 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 « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que le numéro de port sont identiques à ceux de la victime.

Bloquer le « smurf »

Cliquez sur la case à cocher pour activer la fonction de blocage de « smurf ». Le routeur Vigor rejettera toute demande d'écho ICMP à destination de l'adresse de diffusion.

Bloquer le « trace route »

Cliquez sur la case à cocher pour activer cette fonction. Le routeur Vigor ne laissera pas passer les paquets « trace route ».

Bloquer les fragments SYN

Cliquez sur la case à cocher pour activer la fonction de blocage des fragments SYN. Les paquets dont l'indicateur SYN et le bit MF (« more fragments ») sont à 1 sont rejetés.

Bloquer le « fraggle »

Cliquez sur la case à cocher 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 les protocoles inconnus

Cliquez sur la case à cocher 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.

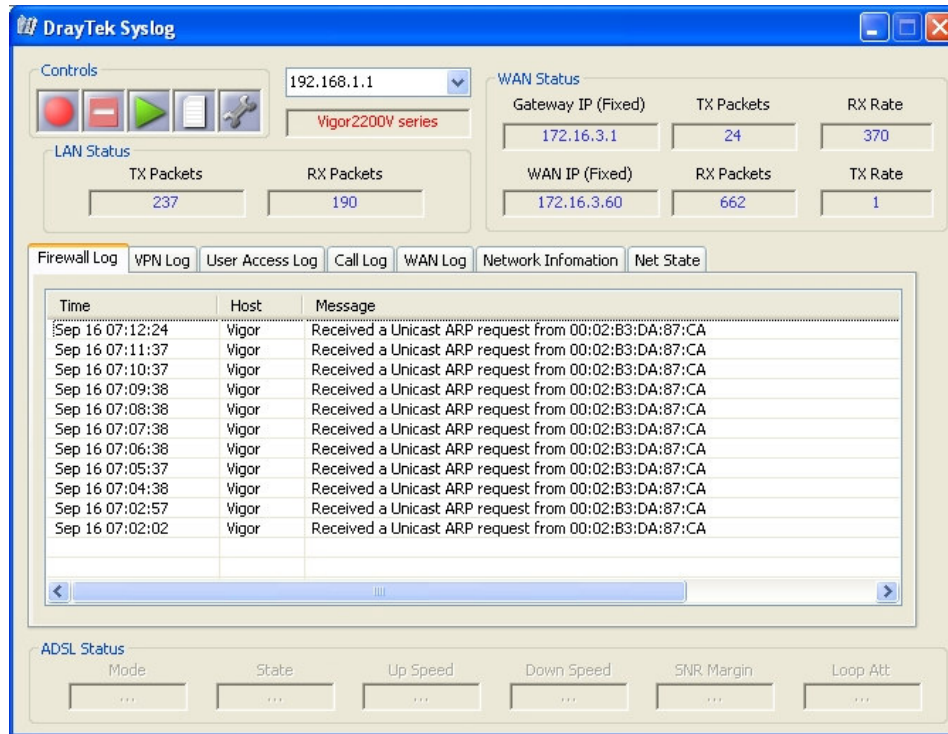
Messages d'avertissement

Tous les messages d'avertissement sont envoyés au client SysLog après l'activation de la fonction SysLog. L'administrateur peut configurer le client SysLog dans **Paramétrages de SysLog** à l'aide du configurateur web. Ainsi, l'administrateur peut visualiser les messages d'avertissement émis par la protection anti-DoS à l'aide du démon SysLog DrayTek. Ces messages d'avertissement ont la même structure que ceux de **Filtre IP pare-feu**, à cette exception près qu'ils ont comme préfixe le mot clé « DoS », suivi d'un nom qui indique le type d'attaque détecté.

Paramétrage de SysLog

<input checked="" type="checkbox"/> Activer	
Adresse IP du serveur	<input type="text" value="192.168.1.10"/>
Port de destination	<input type="text" value="514"/>

Paramétrage du pare-feu



6.2.4 Filtre de contenu d'URL

La fonction de filtrage de contenu URL des routeurs Vigor inspecte chaque chaîne d'URL de la requête http par rapport à la liste de mots-clés. Si tout ou partie de l'URL (par exemple, <http://www.ssex.com> comme indiqué) correspond à un mot clé activé, le routeur Vigor bloque la requête http associée et un message SysLog est envoyé automatiquement au client SysLog. Par ailleurs, toute requête qui tente de récupérer le code malveillant est rejetée par le routeur Vigor. Un message SysLog est également envoyé au client SysLog.



La fonction de filtrage de contenu d'URL empêche les utilisateurs d'accéder à des sites inconvenants dont les URL sont identifiées comme interdites.



Pour que la fonction de filtrage d'URL fonctionne correctement sur une page web que vous avez déjà visitée, vous devez effacer au préalable le cache de votre navigateur.

Activer le contrôle d'accès URL

Une case à cocher vous donne la possibilité d'activer ou non le *contrôle d'accès URL*. Pour l'activer, cliquer sur la case vide : une coche (✓) apparaît.

Paramétrage du filtre de contenu d'URL

<input checked="" type="checkbox"/> Activer le contrôle d'accès URL						
La liste des mots-clés de blocage						
	Non	ACT	Mot-clé	Non	ACT	Mot-clé
1		<input checked="" type="checkbox"/>	MSN	5	<input type="checkbox"/>	
2		<input type="checkbox"/>		6	<input type="checkbox"/>	
3		<input type="checkbox"/>		7	<input type="checkbox"/>	
4		<input type="checkbox"/>		8	<input type="checkbox"/>	
À noter que de multiples mots-clés sont autorisés. Par exemple: hotmail yahoo msn						
<input type="checkbox"/> Empêcher l'accès au web à partir de l'adresse IP						

Liste des mots-clés de blocage : 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.



Si vous voulez interdire l'accès à un site dont l'URL contient « sexe », « baise », « fusil » ou « drogue », vous devez ajouter ces mots dans les trames. Votre routeur Vigor interdira automatiquement l'accès aux sites dont l'URL contient l'un de ces mots-clés.

Supposons que l'utilisateur essaie d'accéder à www.backdoor.net/images/sexe/p_386.html, le routeur Vigor déconnectera l'utilisateur car ce site est interdit.

En outre, la fonction de filtrage de contenu d'URL vous permet également de spécifier une URL complète (par exemple, « www.whitehouse.com » et « www.hotmail.com ») ou une URL partielle (par exemple, « yahoo.com ») dans la liste des mots-clés de blocage.

Paramétrage du pare-feu

Empêcher l'accès au web à partir de l'adresse IP : Une case à cocher vous permet d'activer cette fonction, laquelle interdit l'accès au web en utilisant directement une adresse IP. Pour activer cette fonction, cliquer sur la case vide : une coche (✓) apparaît.

Paramétrage du filtre de contenu d'URL

Activer le contrôle d'accès URL

La liste des mots-clés de blocage

Non	ACT	Mot-clé	Non	ACT	Mot-clé
1	<input checked="" type="checkbox"/>	MSN	5	<input type="checkbox"/>	
2	<input type="checkbox"/>		6	<input type="checkbox"/>	
3	<input type="checkbox"/>		7	<input type="checkbox"/>	
4	<input type="checkbox"/>		8	<input type="checkbox"/>	

À noter que de multiples mots-clés sont autorisés. Par exemple: *hotmail yahoo msn*

Empêcher l'accès au web à partir de l'adresse IP

Activer la fonction de restriction web

Un mécanisme de protection empêchant le téléchargement de codes malveillants à partir de pages web est particulièrement utile. Les codes malveillants peuvent être intégrés à certains objets exécutables, comme *ActiveX*, les *applets Java*, les *fichiers comprimés* et les *fichiers exécutables* et, s'ils sont téléchargés à partir de sites web, peuvent constituer une menace pour le système de l'utilisateur. Par exemple, un objet ActiveX peut être téléchargé et exécuté à partir de la page web. Si l'objet ActiveX contient un code malveillant, il peut avoir un accès illimité au système de l'utilisateur.

Activer la fonction de restriction web

Java
 ActiveX
 Fichiers comprimés
 Fichiers exécutables
 Fichiers multimédias
 Cookie
 Proxy

Java	Cliquez sur la case à cocher 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 comprimés	Cliquez sur la case à cocher pour activer la fonction de blocage des fichiers comprimés et donc empêcher le téléchargement de fichiers comprimés. Le routeur Vigor peut bloquer les types de fichiers comprimés suivant : .zip, .rar, .arj, .ace, .cab, .sit
Fichiers exécutables	Comme dans le cas précédent, cliquez sur la case à cocher pour activer la fonction de blocage des fichiers exécutables et empêcher le téléchargement de fichiers exécutables à partir de l'internet. Le routeur Vigor bloquera les types de fichiers suivant : .exe, .com, .scr, .pif, .bas, .bat, .inf, .reg

Paramétrage du pare-feu

Une fonction *cookie* introduite par Netscape vous permet de surveiller étroitement les demandes et réponses http de sessions individuelles. De nombreux sites utilisent les cookies pour suivre les internautes à la trace, portant atteinte à leur vie privée. Le routeur Vigor comporte une *fonction de filtrage de cookies* qui vous permet de filtrer l'envoi d'informations vers l'extérieur via les cookies. En outre, le routeur Vigor permet également de bloquer toute transmission liée à un proxy afin de renforcer la sécurité.

Cookie	Cliquez sur la case à cocher pour activer le blocage de l'envoi d'informations via les cookies. Le routeur Vigor bloquera toute transmission d'informations vers l'extérieur via les cookies afin de protéger votre vie privée.
Proxy	Cliquez sur la case à cocher pour activer cette fonction.
Fichiers multimédias	Pour contrôler efficacement l'utilisation de cette ressource limitée qu'est la bande passante, un mécanisme empêchant le téléchargement de fichiers multimédias à partir de pages web est particulièrement utile. Pour activer cette fonction, cliquez sur la case vide : une coche (<input type="checkbox"/>) apparaît. 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-réseaux 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. Pour la désactiver, décochez la case.

<input checked="" type="checkbox"/> Sous-réseaux d'exception					
Non	Act	Adresse IP			Masque de sous-réseau
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	~	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	~	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	~	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	~	<input type="text"/>

Horaire

Spécifiez l'horaire de mise en œuvre de la fonction de filtrage de contenu d'URL.

Paramétrage du pare-feu

Horaire

Toujours bloquer

Bloquer à partir de 21:00 To 8:30

Jour de la semaine:

Tous les jours

Jours

Dim Lun Mar Mer Jeu Ven Sam

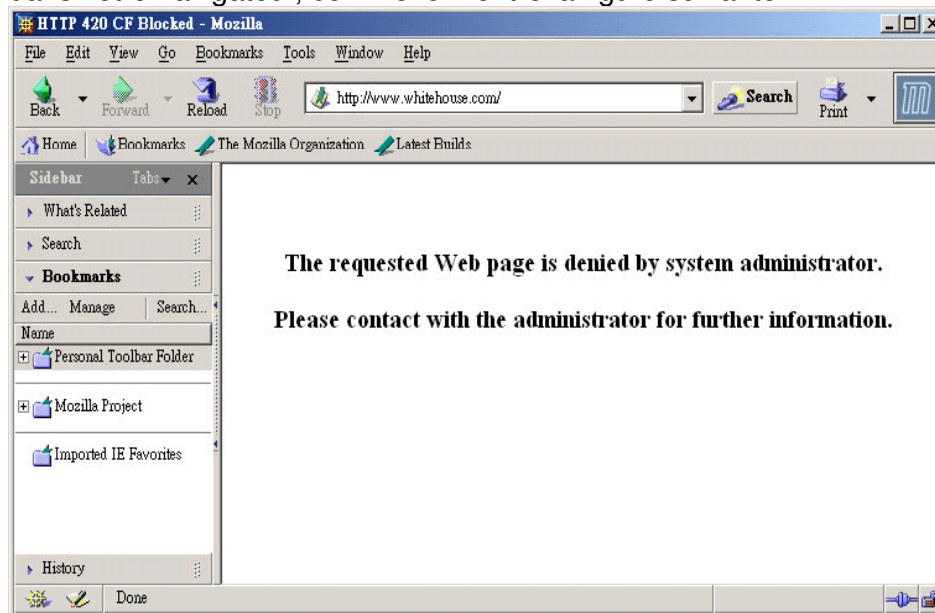
<i>Toujours bloquer</i>	Le filtrage de contenu d'URL est permanent.
<i>Bloquer à partir de H1:M1 à H2:M2</i>	Spécifiez une plage journalière de H1:M1 à H2:M2. H1 et H2 sont les heures. M1 et M2 sont les minutes.
<i>Jours de la semaine</i>	Spécifiez quels jours de la semaine le filtrage de contenu d'URL doit être mis en œuvre. Le routeur Vigor offre deux options exclusives : tous les jours ou certains jours. Si vous voulez que le filtrage de contenu d'URL soit actif toute la semaine, cliquez sur la case « Tous les jours ». Sinon, indiquez les jours de la semaine. Par exemple, si vous voulez que le filtrage de contenu d'URL fonctionne du lundi au mercredi, cliquez sur les cases appropriées (lundi, mardi et mercredi). Les autres jours, le filtrage de contenu d'URL sera inactif.



Si vous voulez que vos enfants ne s'adonnent pas aux jeux en ligne, activez la filtrage de contenu d'URL sur votre routeur et définissez l'horaire pour que le filtrage s'applique aux jours d'école.

Messages d'avertissement

Lorsqu'une requête http est rejetée, une page d'avertissement apparaît dans votre navigateur, comme le montre la figure suivante.



Par ailleurs, le message d'avertissement est envoyé automatiquement au client SysLog, si la fonction SysLog est activée. L'administrateur peut configurer le client SysLog dans **Paramétrage de SysLog** à l'aide du configurateur web. L'administrateur peut visualiser les messages d'avertissement provenant de la fonctionnalité **Filtrage de contenu d'URL** à l'aide du démon SysLog DrayTek. Ce type de message d'avertissement a une structure semblable à ceux de **Filtre IP/Pare-feu**, à cette différence près qu'il est préfixé par le mot clé « **CF** », suivi d'un nom indiquant le type de requête HTTP bloqué.

Paramétrage de SysLog

<input checked="" type="checkbox"/> Activer	
Adresse IP du serveur	<input type="text" value="192.168.1.10"/>
Port de destination	<input type="text" value="514"/>

Paramétrage du pare-feu

The screenshot displays the DrayTek Syslog interface. At the top, the title bar reads "DrayTek Syslog". Below the title bar, there are several sections:

- Controls:** Includes a red stop button, a green play button, a document icon, and a gear icon. A dropdown menu shows "192.168.1.1" and a text field contains "Vigor2200V series".
- LAN Status:** Shows TX Packets (224) and RX Packets (182).
- WAN Status:** Shows Gateway IP (Fixed) (172.16.3.1), TX Packets (24), RX Rate (27), WAN IP (Fixed) (172.16.3.60), RX Packets (554), and TX Rate (1).
- Log Tabs:** Includes Firewall Log (selected), VPN Log, User Access Log, Call Log, WAN Log, Network Information, and Net State.
- Log Table:** A table with columns Time, Host, and Message. It lists several entries for "Received a Unicast ARP request from 00:02:B3:DA:87:CA".
- ADSL Status:** Shows Mode, State, Up Speed, Down Speed, SNR Margin, and Loop Att, all with "..." values.

Time	Host	Message
Sep 16 07:11:37	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:10:37	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:09:38	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:08:38	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:07:38	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:06:38	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:05:37	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:04:38	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:02:57	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA
Sep 16 07:02:02	Vigor	Received a Unicast ARP request from 00:02:B3:DA:87:CA

Chapitre 7

Paramétrage des applications

7.1 Introduction

Ce chapitre traite du **DNS dynamique, des plages horaires, des paramètres RADIUS, et des paramètres UPnP.**

Avant de procéder au paramétrage du **DNS dynamique**, vous devez souscrire à des noms de domaine gratuits auprès de fournisseurs de service DNS dynamique. Le routeur Vigor permet d'ouvrir jusqu'à trois comptes auprès des fournisseurs suivants : www.dynsns.org, www.dynamic-nameserver.com, www.no-ip.com, www.dtdns.com, www.changeip.com. Visitez leur site pour enregistrer votre nom de domaine pour le routeur. La fonction DNS dynamique permet au routeur de mettre à jour son adresse IP WAN attribuée par le FAI pour 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.

La fonction de gestion de plages horaires permet de gérer les heures de connexion du routeur. Avant de configurer cette fonction, il faut régler l'heure et définir des horaires pour le profil d'accès à l'internet ou le profil d'interconnexion de LAN spécifié. Le routeur Vigor comporte une horloge temps réel qui peut être mise à jour manuellement à partir de votre navigateur 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).

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.

7.2 Paramètres

Cliquer sur une option du menu **Applications** pour ouvrir la page de paramétrage correspondante.



DNS dynamique	Paramétrage des noms de domaines souscrits auprès d'un maximum de trois fournisseurs de service DNS dynamique.
Plages horaires	Réglage d'une horloge temps réel qui se met à jour automatiquement à partir d'un serveur de synchronisation internet (NTP).
Paramètres RADIUS	Paramétrage du serveur RADIUS
UPnP	Paramétrage du protocole UPnP pour les périphériques raccordés directement à un PC avec le système « Plug and Play » Windows existant.

7.2.1 DNS dynamique

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** et cliquez sur le numéro d'index **1** pour ajouter un compte. La page web suivante s'affiche.

Paramétrage des applications

Paramétrage du DNS dynamique

Activer le paramétrage du DNS dynamique

Afficher le journal Forcer la mise à jour Effacer tout

Comptes

Index	Nom de domaine	Actif
1.	---	x
2.	---	x
3.	---	x

Index :1

Activer le compte DNS dynamique

Fournisseur de service : dyndns.org (www.dyndns.org)

Type de service : Dynamique

Nom de domaine : hostname . dyndns.org

Nom d'utilisateur : test (23 caractères maximum)

Mot de passe : ●●●● (23 caractères maximum)

Alias (wildcards)

Secours de messagerie (Backup MX)

Mail Extender :

Nota :Avant que ce compte puisse être activé, il faut activer le service DNS dynamique dans la table suivante!

3. 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**.
4. Cliquez sur le bouton **OK** pour valider.



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.

Validation et dépannage

Vérification du nom de domaine enregistré par PING

1. Le routeur étant en ligne, utilisez l'utilitaire PING pour vérifier le fonctionnement de votre nom de domaine enregistré.
2. Utilisez l'option **État en ligne** du menu principal pour vérifier que l'adresse IP envoyée par le serveur DNS dynamique est identique à l'adresse IP WAN du routeur.

Visualisez les journaux DDNS

1. Applications >> Paramétrage du DNS dynamique.
2. Cliquez sur le bouton **Afficher le journal**. Le journal des mises à jour DDNS est affiché :

```
Journal DDNS dynamique
07:14:03.7 A= , H= , U= 1
07:14:03.7 Account is not enabled.
07:17:43.0 >>>> DDNS is updating. <<<<<
07:17:43.0 A= , H= , U= 1
07:17:43.0 Account is not enabled.
07:17:43.0 A= , H= , U= 1
07:17:43.0 Account is not enabled.
07:17:43.0 A= , H= , U= 1
07:17:43.0 Account is not enabled.
```

Où A : Nom d'utilisateur

H : Nom de domaine sans suffixe.

Code de retour = bon 61.230.170.145



Si vous avez un problème de mise à jour DDNS, les journaux sont utiles pour déterminer où le problème se situe.

3. Cliquez sur **État en ligne** pour connaître l'adresse IP WAN actuelle.

État WAN

Mode	Adresse IP
PPPoE	61.230.170.145

L'adresse IP affichée ci-dessus est la même que le code de retour du journal DDNS. Cela indique que la mise à jour a réussi.

7.2.2 Plages horaires

Dans le menu **Réglage de l'heure**, si vous cliquez sur le bouton **Demander l'heure**, l'horloge du routeur est réglée sur l'heure actuelle de votre PC. L'horloge se réinitialise si vous éteignez ou réinitialisez le routeur, aussi pouvez-vous préférer utiliser un serveur NTP sur l'internet pour mettre à jour automatiquement l'horloge. Les mises à jour NTP ne se font que lorsque le routeur est en ligne ; elles ne déclenchent pas d'appel.

Vous pouvez définir jusqu'à 15 plages horaires différentes, que vous pouvez ensuite appliquer au FAI approprié en entrant le numéro de plage horaire :

Paramétrage des plages horaires Effacer tout

Index	État	Index	État
<u>1.</u>	x	<u>9.</u>	x
<u>2.</u>	x	<u>10.</u>	x
<u>3.</u>	x	<u>11.</u>	x
<u>4.</u>	x	<u>12.</u>	x
<u>5.</u>	x	<u>13.</u>	x
<u>6.</u>	x	<u>14.</u>	x
<u>7.</u>	x	<u>15.</u>	x
<u>8.</u>	x		

État: v --- Actif, x --- Inactif

Index n° 1

Activer cette plage horaire

Date de début (aaaa-mm-jj) 2005 | 9 | 16

Heure de début (hh:mm) 0 | 0

Durée (hh:mm) 0 | 0

Action Forcer la connexion

Délai d'inactivité 0 minute(s). (255 maxi, 0 par défaut)

Fréquence

Une fois

Jours de la semaine

Dim
 Lun
 Mar
 Mer
 Je
 Ve
 Sam

Paramétrage des plages horaires: Effacer tout

Index	État	Index	État
<u>1.</u>	x	<u>9.</u>	x
<u>2.</u>	x	<u>10.</u>	x

Paramétrage des applications

Cliquez sur le bouton **Effacer tout** pour effacer toutes les plages horaires.

Cliquez sur le bouton **Annuler** pour abandonner l'opération de modification actuelle et retourner au menu principal.

Ajouter une plage horaire

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

Index n° 1

Activer cette plage horaire

Date de début (aaaa-mm-jj) 2005 9 16

Heure de début (hh:mm) 0 : 0

Durée (hh:mm) 0 : 0

Action Forcer la connexion

Délai d'inactivité Forcer la connexion (0 par défaut)
Forcer la déconnexion
Activer à la demande
Désactiver à la demande

Fréquence
 Une fois
 Jours de la semaine

Dim Lun Mar Mer Je Ve Sam

2. Description détaillée de chaque paramètre :

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.

<i>Forcer la connexion</i>	Connexion permanente durant la plage horaire.
<i>Forcer la déconnexion</i>	Connexion interdite durant la plage horaire.

Paramétrage des applications

Activer à la demande	Connexion établie à la demande avec un Délai d'inactivité . <input checked="" type="checkbox"/> Activer cette plage horaire Date de début (aaaa-mm-jj) 2005 - 9 - 16 Heure de début (hh:mm) 0 : 0 Durée (hh:mm) 0 : 0 Action Forcer la déconnexion Délai d'inactivité <input type="text"/> minute(s). (255 maxi, 0 par défaut)
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 connexions 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.

3. Spécifiez la durée appropriée et l'action, puis cliquez sur le bouton **OK**.
4. Spécifiez les plages horaires propre à tel ou tel profil d'accès à l'internet ou à tel ou tel profil d'interconnexion de LAN.

Un exemple

Si vous voulez que la connexion internet PPPoE soit permanente de 9 h 00 à 18 h 00 toute la semaine et quelle soit impossible en dehors de ces heures :

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.

Paramétrage des applications

Activer cette plage horaire

Date de début (aaaa-mm-jj) 2005-9-16

Heure de début (hh:mm) 9:00

Durée (hh:mm) 9:00

Action Forcer la connexion

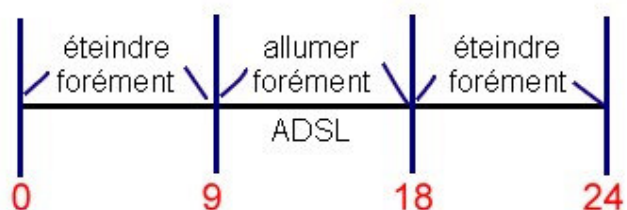
Délai d'inactivité 0 minute(s). (255 maxi, 0 par défaut)

Fréquence

Une fois

Jours de la semaine

Dim Lun Mar Mer Je Ve Sam



3. Forcez la déconnexion de 18 h 00 à 9 h 00 le jour suivant pendant toute la semaine.

Activer cette plage horaire

Date de début (aaaa-mm-jj) 2005-9-16

Heure de début (hh:mm) 18:00

Durée (hh:mm) 15:00

Action Forcer la déconnexion

Délai d'inactivité 0 minute(s). (255 maxi, 0 par défaut)

Fréquence

Une fois

Jours de la semaine

Dim Lun Mar Mer Je Ve Sam

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.

Paramétrage des applications

Mode client PPPoE	
Configuration PPPoE Liaison PPPoE <input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	Configuration du protocole PPP/MP Authentification PPP PAP ou CHAP <input type="button" value="v"/> <input type="checkbox"/> Connexion permanente Délai d'inactivité 180 seconde(s)
Configuration de l'accès au FAI Nom du FAI <input type="text" value="kk"/> Nom d'utilisateur <input type="text" value="ding@kk.com"/> Mot de passe <input type="password" value="••••••"/>	Méthode d'attribution d'adresse IP (IPCP) Adr IP fixe <input type="radio"/> Oui <input checked="" type="radio"/> Non (IP dynamique) Adresse IP fixe <input type="text"/>
Plages horaires (1-15) => 1 <input type="text"/> , 2 <input type="text"/> , <input type="text"/> , <input type="text"/>	Type de WAN Négociation automatique <input type="button" value="v"/>

7.2.3 UPnP

Vous pouvez entrer les **paramètres UPNP** comme indiqué ci-dessous.

[Applications >> Paramétrage UPnP](#)

Paramètres UPNP
<input type="checkbox"/> Activer le service UPnP <input type="checkbox"/> Activer le service de contrôle de connexion <input type="checkbox"/> Activer le service d'état de connexion

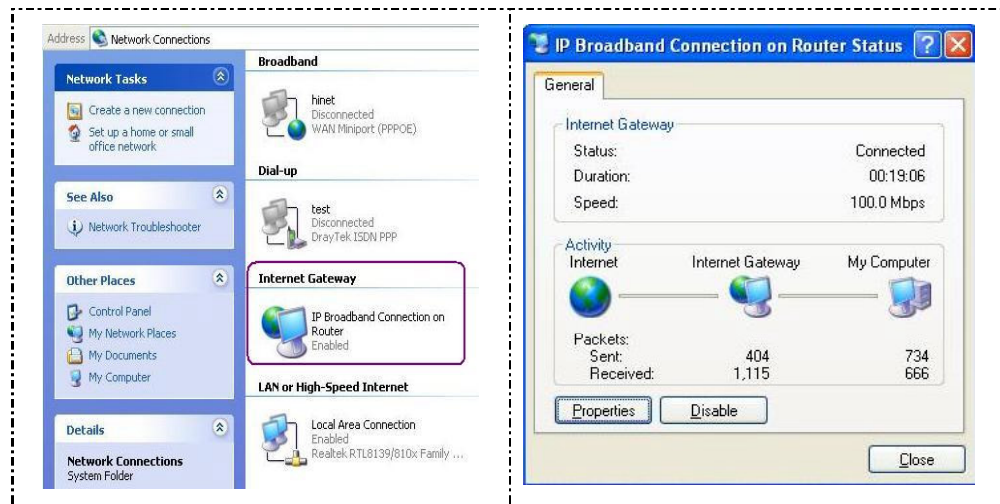
Nota : Si vous avez l'intention de faire fonctionner le service UPNP dans votre LAN, vous devez activer le service approprié pour autoriser le contrôle ci-dessus ainsi que les paramètres UPNP appropriés.

Activer le service UPNP :

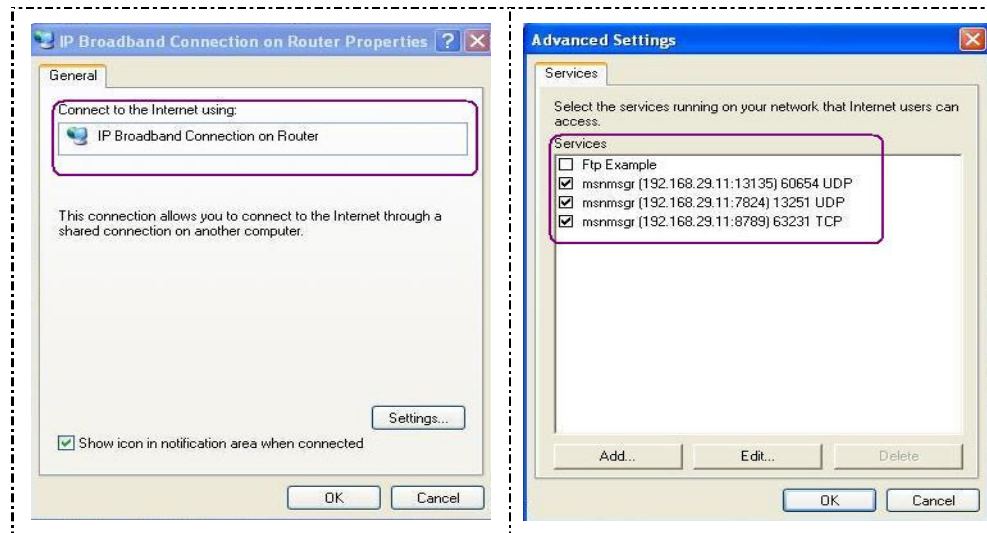
Vous pouvez activer soit le **Service de contrôle de connexion**, soit le **Service d'état de connexion**.

Cliquez sur **IP Broadband Connection on DrayTek Router** dans Windows XP/Favoris réseaux comme indiqué ci-dessous. 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.

Paramétrage des applications



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, de prendre connaissance de l'adresse IP externe et de configurer des mappages de ports. 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.

1. 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.
2. Les utilisateurs non privilégiés peuvent contrôler certaines fonctions du routeur et notamment enlever et ajouter des mappages de ports.
3. 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.

Chapitre 8

Paramétrage du VPN et de l'accès à distance

8.1 Introduction

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. Un 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.

Il existe deux types de connexions de VPN : la connexion de VPN d'accès à distance et la connexion de VPN d'interconnexion de LAN. La fonction d'accès à distance permet à un nœud d'accès à distance, à un routeur NAT ou à un ordinateur mono-utilisateur d'appeler un routeur VPN via l'internet pour accéder aux ressources du réseau distant. La fonction d'interconnexion de LAN permet de relier deux LAN indépendants entre eux pour le partage des ressources réseau. Par exemple, le réseau du siège peut accéder au réseau de l'établissement secondaire, et vice versa.

La technologie de VPN mise en œuvre par les routeurs Vigor prend en charge les protocoles courants du monde internet pour offrir des solutions de VPN interopérables : le protocole de sécurisation IP (IPSec), le protocole de tunnel de couche 2 (L2TP), et le protocole de tunnel point à point (PPTP).

Ce chapitre explique comment paramétrer le VPN et l'accès à distance.

8.2 Paramètres

Cliquez sur **Paramétrage du VPN et de l'accès à distance** pour ouvrir la page de paramétrage.

VPN et accès à distance
▶ Contrôle d'accès à distance
▶ Configuration générale du protocole PPP
▶ Paramétrage général IKE / IPSec
▶ Profils d'utilisateur distant (Télétravailleur)
▶ Profils d'interconnexion de LAN
▶ Gestion de connexion VPN

Contrôle d'accès à distance	Vous permet d'activer chaque type de service de VPN ou de le désactiver pour autoriser le mode pass-through VPN. Par exemple, vous pouvez activer les services de VPN IPSec et L2TP pour votre routeur et désactiver le service de VPN PPTP si vous voulez faire fonctionner un serveur PPTP dans votre LAN. Vous pouvez aussi activer ou désactiver l'accès à distance RNIS, dont la fonction utilisateur distant et l'interconnexion de LAN.
Configuration générale du protocole PPP	Vous permet de configurer le mode d'identification PPP de votre routeur et d'attribuer des adresses IP aux utilisateurs distants. Ce sous-menu ne s'applique qu'aux connexions de VPN liées à PPP comme PPTP, L2TP, L2TP sur IPSec et l'accès à distance RNIS.
Paramétrage général IKE/IPSec	Vous permet de configurer une clé prépartagée commune et une méthode de sécurisation pour un utilisateur ou un nœud distant (interconnexion de LAN) utilisant une adresse IP dynamique.
Profils d'utilisateur distant (Télétravailleurs)	Vous permet de créer des comptes utilisateurs distants. Le routeur Vigor prend en charge trois types d'appels entrants : PPTP, L2TP et L2TP sur IPSec et RNIS. La connexion de VPN PPTP est compatible avec toutes les plate-formes Windows comportant le protocole PPTP. L2TP et L2TP sur IPSec sont compatibles avec Windows 2000 et XP.
Profils d'interconnexion de LAN	Vous permet de créer des profils d'interconnexion de LAN. Le routeur Vigor prend en charge quatre types de VPN d'interconnexion de LAN : Tunnel IPSec, PPTP, L2TP, L2TP sur IPSec et RNIS. Vous pouvez établir simultanément jusqu'à 32 tunnels VPN incluant des utilisateurs distants.

8.2.1 Contrôle d'accès à distance

Supposons que vous ayez un nom de domaine à enregistrer auprès du fournisseur de service DDNS.

Comme indiqué ci-dessous, cliquez sur la case appropriée pour activer le type de service de VPN que vous voulez. Si vous avez l'intention de faire fonctionner un serveur de VPN dans votre LAN, vous devez désactiver le protocole approprié pour autoriser le mode pass-through ainsi que les paramètres NAT appropriés, par exemple, DMZ ou ouverture de ports. Vous pouvez également autoriser les appels entrants RNIS en cochant la case **Activer les appels entrants RNIS**.

Paramétrage du contrôle d'accès à distance

<input checked="" type="checkbox"/> Activer le service VPN PPTP
<input checked="" type="checkbox"/> Activer le service VPN IPSec
<input checked="" type="checkbox"/> Activer le service VPN L2TP
<input type="checkbox"/> Activer les appels entrants RNIS

Nota :Si vous avez l'intention de faire fonctionner un serveur VPN dans votre LAN, vous devez désactiver le protocole approprié pour autoriser le mode pass-through ainsi que les paramètres NAT appropriés.

8.2.2 Configuration générale du protocole PPP

Configuration générale du protocole PPP

Protocole PPP/MP	Attribution d'adresse IP pour les appels entrants
Authentification PPP distant : PAP ou CHAP	Adresse IP de début : 192.168.1.200
Cryptage PPP distant (MPPE) : MPPE optionnel	
Authentification mutuelle (PAP) : <input type="radio"/> Oui <input checked="" type="radio"/> Non	
Nom d'utilisateur : <input type="text"/>	
Mot de passe : <input type="text"/>	

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 :

<i>MPPE optionnel</i>	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 ».
<i>Nécessite MPPE (40/120bits)</i>	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 40 bits avant d'utiliser un cryptage sur 128 bits. En d'autres termes, si le cryptage MPPE sur 40 bits n'est pas disponible, c'est le cryptage sur 128 bits qui sera appliqué aux données.
<i>MPPE maximum</i>	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. N'activez cette fonction que si le routeur avec lequel vous communiquez exige une authentification mutuelle. Par défaut, la valeur de l'option est Non. À noter que si vous activez l'authentification mutuelle, vous devez en outre spécifier un nom d'utilisateur et un mot de passe.

<i>Nom d'utilisateur</i>	Spécifiez le nom d'utilisateur pour l'authentification mutuelle.
<i>Mot de passe</i>	Spécifiez le mot de passe pour l'authentification mutuelle.

Attribution d'adresse IP pour les appels entrants :

<i>Adresse IP de début</i>	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.
-----------------------------------	---

8.2.3 Configuration générale IKE/IPSec

Configuration d'une clé prépartagée commune et d'une méthode de sécurisation pour les utilisateurs distants ou les nœuds non spécifiés (interconnexion de LAN) qui n'ont pas d'adresse IP fixe. Ces paramètres ne s'appliquent qu'aux connexions de VPN liées à IPSec. Par exemple, L2TP sur IPSec et tunnel IPSec.

Paramétrage général IKE/IPSec VPN

Paramétrage des appels entrants pour les utilisateurs distants et le client IP dynamique (LAN à LAN).

Méthode d'authentification IKE	
Clé prépartagée	<input type="text"/>
Retapez la clé prépartagée	<input type="text"/>
Méthode de sécurisation IPSec	
<input checked="" type="checkbox"/> Moyenne (AH)	Les données seront authentifiées mais non cryptées.
Elevée (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Les données seront cryptées et authentifiées.

Méthode d'authentification IKE :

Seule l'authentification par clé prépartagée est prise en charge actuellement.

Clé prépartagée	Spécifiez une clé pour l'authentification IKE.
Mot de passe	Confirmez la clé prépartagée.

Méthode de sécurisation IPSec :

Moyenne (AH)	Les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée (ESP)	Les données seront cryptées et authentifiées. Les méthodes de cryptage DES, 3DES, et AES sont prises en charge. Par défaut, ces méthodes sont disponibles.

8.2.4 Profils d'utilisateur distant (Télétravailleurs)

Après la configuration générale, vous devez créer un compte pour chaque utilisateur distant. Le routeur permet de créer 32 comptes utilisateurs distants. En outre, vous pouvez étendre les comptes utilisateurs au serveur RADIUS grâce à la fonction client RADIUS intégrée. L'écran de paramétrage est représenté ci-dessous.

Paramétrage du VPN et de l'accès à distance

Comptes utilisateurs d'accès distant:

[Paramètres par défaut](#)

Index	Utilisateur	État	Index	Utilisateur	État
1.	???	x	11.	???	x
2.	???	x	12.	???	x
3.	???	x	13.	???	x
4.	???	x	14.	???	x
5.	???	x	15.	???	x
6.	???	x	16.	???	x
7.	???	x	17.	???	x
8.	???	x	18.	???	x
9.	???	x	19.	???	x
10.	???	x	20.	???	x

État: v --- Actif, x --- Inactif

Paramètres par défaut	Cliquez ici pour effacer tous les comptes utilisateurs distants.
Utilisateur	Affiche le nom d'utilisateur de l'utilisateur distant du profil d'interconnexion de LAN. ??? signifie que le profil est vide.
État	Affiche l'état d'accès de l'utilisateur distant. V indique que l'utilisateur distant est actif. X indique que l'utilisateur distant est inactif.
Index	Cliquez sur le numéro pour ouvrir une page de paramétrage de compte utilisateur distant.

Index n° 1

<p>Compte d'utilisateur et authentification</p> <p><input type="checkbox"/> Activer ce compte</p> <p>Délai d'inactivité <input type="text" value="300"/> seconde(s)</p> <p>Type d'appel autorisé</p> <p><input checked="" type="checkbox"/> RNIS</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> Tunnel IPSec</p> <p><input checked="" type="checkbox"/> L2TP avec règles IPSec <input type="text" value="Néant"/></p> <p><input type="checkbox"/> Spécifier le nœud distant</p> <p>Adr IP client distant ou numéro RNIS homologue <input type="text"/></p> <p>ou ID homologue <input type="text"/></p>	<p>Nom d'utilisateur <input style="width: 100px;" type="text" value="???"/></p> <p>Mot de passe <input style="width: 100px;" type="password"/></p> <p>Clé prépartagée IKE <input style="width: 100px;" type="text"/></p> <p>Méthode de sécurisation IPSec</p> <p><input checked="" type="checkbox"/> Moyen (AH)</p> <p>Elevée (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>ID locale <input style="width: 100px;" type="text"/> (optionnel)</p> <p>Fonction de rappel automatique</p> <p><input type="checkbox"/> Cocher pour activer la fonction de rappel automatique</p> <p><input type="checkbox"/> Spécifier le numéro de rappel</p> <p>Numéro de rappel <input style="width: 100px;" type="text"/></p> <p><input checked="" type="checkbox"/> Cocher pour activer le contrôle de crédit de rappel automatique</p> <p>Crédit de rappel <input type="text" value="30"/> minute(s)</p>
--	---

Compte utilisateur et authentification :

Activer ce compte	Cochez cette case pour activer le compte utilisateur distant.
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.

Type d'appel entrant autorisé :

Sélectionnez le type d'appel entrant autorisé. Les routeurs Vigor autorisent trois types d'appels entrants : PPTP, Tunnel IPSec, L2TP avec politique IPSec. Dans le cas de L2TP avec politique IPSec, vous avez trois options (Néant, Souhaitée, Imposée).

PPTP	Permet à l'utilisateur distant d'établir une connexion de VPN PPTP via l'internet.
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. Spécifiez la politique IPSec : « Néant », « Souhaitée » ou « Imposée ». 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 existe. Sinon, la connexion de VPN devient une connexion L2TP pure Imposée : appliquer systématiquement la politique IPSec à la connexion L2TP.



PPTP ou L2TP avec politique IPSec (Néant)

Spécifiez uniquement le nom d'utilisateur et le mot de passe.

PPTP ou L2TP avec politique IPSec (Souhaitée ou imposée)

Spécifiez le nom d'utilisateur et le mot de passe. Spécifiez également *la clé prépartagée IKE, la méthode de sécurisation IPSec, l'adresse IP client distant ou l'ID homologue, et l'ID local facultatif.*

Spécifier le nœud distant :

Pour renforcer la sécurité, activez l'option pour permettre au client distant de se connecter uniquement à partir d'une adresse IP spécifique.

Adresse IP client distant ou ID homologue	Spécifiez l'adresse IP du client distant ou l'ID homologue. Ensuite, spécifiez une clé prépartagée pour ce nœud spécifique.
--	---

Paramétrage du VPN et de l'accès à distance

Clé prépartagée IKE	Cliquez pour faire apparaître une fenêtre, entrez une clé prépartagée et confirmez-la pour ce nœud spécifique.
Méthode de sécurisation IPSec	Spécifiez la méthode de sécurisation IPSec (authentification ou de cryptage) afin de déterminer le niveau de sécurité. Vous ne devez choisir qu'une seule méthode. Moyenne (AH) : Spécifiez le protocole IPSec pour le protocole AH. Les données seront authentifiées mais non cryptées. Élevée (ESP) : Spécifiez le protocole IPSec pour le protocole EPS. Les données seront cryptées. Les algorithmes pris en charge sont DES, 3DES et AES. Par défaut, ces trois algorithmes sont disponibles.
ID local	Spécifiez un identifiant local à utiliser pour les appels entrants dans le profil d'interconnexion de LAN. Cet ID est facultatif.



Si vous n'activez pas « **Spécifier le nœud distant** » et laissez les champs « **Adresse IP client distant ou ID homologue** » vides, les paramètres **Clé prépartagée IKE**, **Méthode de sécurisation IPSec**, **Adresse IP client distant ou ID homologue** et **ID local** seront désactivés. Il ne sera pas possible d'établir une connexion de VPN liée à IPSec.



La fonction de rappel automatique n'est pas activée pour cette version.

8.2.5 Profils d'interconnexion de LAN

Cette section explique comment paramétrer un **profil d'interconnexion de LAN**. Vous pouvez créer jusqu'à 32 profils d'interconnexion de LAN.

Profils d'interconnexion de LAN:

Paramètres par défaut

Index	Nom	État	Index	Nom	État
<u>1.</u>	???	x	<u>9.</u>	???	x
<u>2.</u>	???	x	<u>10.</u>	???	x
<u>3.</u>	???	x	<u>11.</u>	???	x
<u>4.</u>	???	x	<u>12.</u>	???	x
<u>5.</u>	???	x	<u>13.</u>	???	x
<u>6.</u>	???	x	<u>14.</u>	???	x
<u>7.</u>	???	x	<u>15.</u>	???	x
<u>8.</u>	???	x	<u>16.</u>	???	x

État : v --- Actif, x --- Inactif

Paramètres par défaut	Cliquez ici pour effacer tous les profils d'interconnexion de LAN.
------------------------------	--

Paramétrage du VPN et de l'accès à distance

Index	Cliquez sur un numéro pour ouvrir une page de paramétrage de profil.
Nom	Affichez le nom du profil d'interconnexion de LAN. ??? signifie que le profil est vide.
État	Affichez l'état du profil. V indique que le profil est actif, X indique que le profil est inactif.

Chaque profil d'interconnexion de LAN comprend 4 sous-groupes de paramètres : **Paramètres communs**, **Paramètres d'appel sortant**, **Paramètres d'appel entrant** et **Paramètres TCP/IP**. Chaque sous-groupe est décrit en détail ci-après.

Paramètres communs

1. Paramètres communs

Nom du profil <input style="width: 100px;" type="text" value="???"/> <input type="checkbox"/> Activer ce profil	Sens de l'appel <input checked="" type="radio"/> Les deux <input type="radio"/> Appel sortant <input type="radio"/> Appel entrant <input type="checkbox"/> Connexion permanente Délai d'inactivité <input type="text" value="300"/> seconde(s) <input type="checkbox"/> Activer la vérification par PING PING vers adr IP <input style="width: 100px;" type="text"/>
--	---

Nom du profil	Spécifiez un nom pour le réseau distant.
Activer ce profil	Cochez cette case pour activer le profil
Sens de l'appel	Spécifiez le sens des appels pour ce profil. « Les deux » signifie que le profil peut être utilisé pour les appels sortants et entrants. « Sortant » signifie qu'il ne peut être utilisé que pour les appels sortants. « Entrant » autorise uniquement les appels entrants.
Connexion permanente	Cliquez sur cette case pour que ce profil soit activé en permanence. Le champ Délai d'inactivité est alors grisé et inaccessible.
Délai d'inactivité	300 secondes par défaut. Si la connexion du profil est restée inactive jusqu'à l'expiration du délai d'inactivité, le routeur la libère.
Vérification par PING	Cochez cette case pour autoriser la transmission de paquets PING à une adresse IP définie dans le champ « PING vers IP »
PING vers IP	Spécifiez l'adresse IP de l'hôte distant situé à l'autre extrémité du tunnel de VPN.

Paramétrage du VPN et de l'accès à distance



Dans des conditions normales, lorsque que l'hôte distant veut libérer sa connexion de VPN avec le routeur Vigor, il doit envoyer plusieurs paquets d'un type particulier pour en informer la routeur. Le routeur libère alors la connexion de VPN concernée et efface ses paramètres (par exemple, la clé de cryptage).

Toutefois, si l'hôte distant libère anormalement une connexion de VPN, le routeur ne s'en apercevra pas et supposera que la connexion est toujours établie. Pour résoudre ce problème, activez **Vérification par PING** afin que le routeur vérifie l'état de la connexion de VPN en envoyant continuellement des paquets PING à l'hôte distant.

Paramètres d'appel sortant

2. Paramètres d'appel sortant

Type de serveur appelé <input checked="" type="radio"/> RNIS <input type="radio"/> PPTP <input type="radio"/> Tunnel IPSec <input type="radio"/> L2TP avec politique IPSec <input type="text" value="Néant"/>	Type de liaison <input type="text" value="64 kbit/s"/> Nom d'utilisateur <input type="text" value="???"/> Mot de passe <input type="text"/> Authentification PPP <input type="text" value="PAP/CHAP"/> Compression VJ <input checked="" type="radio"/> Avec <input type="radio"/> Sans
Adresse IP serveur/Nom hôte pour le VPN. (tel quedraytek.com ou 123.45.67.89) <input type="text"/>	Clé prépartagée IKE <input type="text"/> Méthode de sécurisation IPSec <input checked="" type="radio"/> Moyenne (AH) <input type="radio"/> Elevée(ESP) <input type="text" value="DES sans authentification"/> <input type="button" value="Avance"/>
	Plages horaires (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	Fonction de rappel automatique (CBCP) <input type="checkbox"/> Demander le rappel automatique <input type="checkbox"/> Fournir le numéro RNIS au réseau distant

Choisissez l'une des trois options principales : PPTP, Tunnel IPSec et L2TP avec politique IPSec (sous-options : Néant, Souhaitée, Imposée).

N'oubliez pas de spécifier l'adresse IP serveur/Nom d'hôte pour le VPN comme adresse de destination.

Paramétrage :

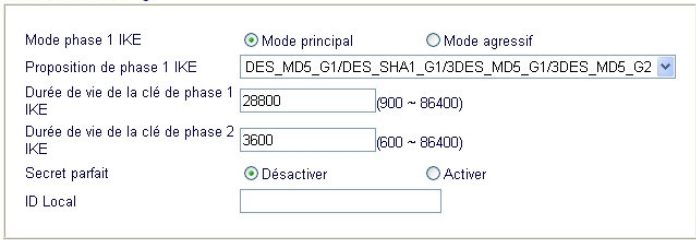
PPTP ou L2TP avec politique IPSec (Néant) Spécifiez l'adresse IP serveur/Nom d'hôte pour le VPN. Spécifiez le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ.

Paramétrage du VPN et de l'accès à distance

Tunnel IPSec ou L2TP avec politique IPSec (souhaitée ou imposée) Spécifiez l'adresse IP serveur/Nom d'hôte pour le VPN. Spécifiez le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ. Spécifiez également la *clé prépartagée IKE*, la *méthode de sécurisation IPSec* et les *plages horaires*

PPTP	La connexion de VPN sortante est une connexion PPTP.
Tunnel IPSec	La connexion de VPN sortante est un tunnel IPSec.
L2TP	Spécifiez la politique IPSec pour la connexion L2TP. 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 existe. Sinon, la connexion de VPN devient une connexion L2TP pure. Imposée : appliquer systématiquement à la connexion L2TP.
Adresse IP serveur/Nom hôte pour le VPN	Spécifiez l'adresse IP du serveur de VPN de destination ou le nom d'hôte.
Nom d'utilisateur	Spécifiez un nom d'utilisateur pour l'authentification par le routeur distant.
Mot de passe	Spécifiez un mot de passe pour l'authentification par le routeur distant.
Authentification PPP	Spécifiez la méthode d'authentification de PPP pour PPTP, et L2TP sur IPSec. Normalement PAP/CHAP pour assurer la compatibilité la plus large.
Compression VJ	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.
Clé prépartagée IKE	Cliquez pour faire apparaître une fenêtre, entrez une clé prépartagée et confirmez-la pour ce nœud spécifique.
Méthode de sécurisation IPSec	Spécifiez la méthode de sécurisation IPSec (authentification ou cryptage) afin de déterminer le niveau de sécurité. Vous ne devez choisir qu'une seule méthode. Moyenne (AH) : Spécifiez le protocole IPSec pour le protocole AH. Les données seront authentifiées mais non cryptées. Élevée (ESP) : Spécifiez le protocole IPSec pour le protocole EPS. Les données seront cryptées. Les algorithmes pris en charge sont les suivants : DES sans authentification : Utiliser l'algorithme de cryptage DES sans authentification. DES avec authentification : Utiliser l'algorithme de cryptage DES avec authentification et appliquer l'algorithme d'authentification MD5 ou SHA-1. 3DES sans authentification : Utiliser l'algorithme de cryptage

Paramétrage du VPN et de l'accès à distance

	<p>3 DES sans authentification.</p> <p>3DES avec authentification : Utiliser l'algorithme de cryptage 3 DES avec authentification et appliquer l'algorithme d'authentification MD5 ouSHA-1.</p>
Paramètres avancés	<p>Pour décider quel mode utiliser pour la phase1 du processus de négociation IKE, spécifiez les algorithmes d'authentification et de cryptage, spécifiez la durée de vie des clés de phase 1 et de phase 2 IKE, activez ou désactivez « Secret parfait » et spécifiez l'ID local de la passerelle de VPN distante.</p> <p>IKE advanced settings</p>  <p>Mode phase 1 IKE : Mode principal et mode agressif. La plupart des serveurs de VPN prennent en charge le mode principal et le mode agressif. Ce dernier, plus récent, accélère le processus de négociation mais au détriment de la sécurité. Le mode par défaut est le mode principal pour que la compatibilité soit la plus grande possible.</p> <p>Proposition de phase 1 IKE : Le routeur demande au serveur de VPN distant s'il prend en charge l'algorithme désigné. Il existe deux options pour le mode agressif, et neuf options pour le mode principal. Nous suggérons de choisir la dernière option : « DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2 », pour le mode principal.</p> <p>Durée de vie de la clé de phase 1 IKE : pour que la sécurité soit la plus grande possible, le routeur doit limiter la durée de vie de la clé. La durée de vie par défaut de la clé est de 28800 secondes. Nous suggérons de spécifier une valeur comprise entre 900 et 86400 secondes.</p> <p>Durée de vie de la clé de phase 2 IKE : pour que la sécurité soit la plus grande possible, le routeur doit limiter la durée de vie de la clé. La durée de vie par défaut de la clé est de 3600 secondes. Nous suggérons de spécifier une valeur comprise entre 600 et 86400 secondes.</p> <p>Secret parfait : si cette fonction est activée, la clé de phase 1 sera réutilisée pour réduire la complexité des calculs en phase 2. Sinon, une nouvelle clé est créée pour la phase 2. Par défaut, cette option est désactivée.</p> <p>ID local : Cette fonction est utilisée en mode agressif. C'est l'adresse IP qui sert pour l'authentification avec le serveur de VPN distant.</p>

Paramétrage du VPN et de l'accès à distance

Plages horaires	Spécifiez le numéro de la plage horaire.
------------------------	--

Paramètres d'appel entrant

3. Paramètres d'appel entrant

<p>Type d'appel entrant autorisé</p> <p><input checked="" type="checkbox"/> RNIS</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> Tunnel IPSec</p> <p><input checked="" type="checkbox"/> L2TP avec politique IPSec Néant</p> <p><input type="checkbox"/> Spécifier Passerelle de VPN distant</p> <p>Adresse IP du serveur VPN homologue</p> <p><input style="width: 100%;" type="text"/></p> <p>ou ID homologue <input style="width: 100%;" type="text"/></p>	<p>Nom d'utilisateur <input data-bbox="1122 485 1325 516" style="width: 100%;" type="text" value="???"/></p> <p>Mot de passe <input data-bbox="1122 522 1325 554" style="width: 100%;" type="password"/></p> <p>Compression VJ <input checked="" type="radio"/> Avec <input type="radio"/> Sans</p> <p>Clé prépartagée IKE <input data-bbox="1122 617 1325 648" style="width: 100%;" type="text"/></p> <p>Méthode de sécurisation IPSec</p> <p><input checked="" type="checkbox"/> Moyenne (AH)</p> <p>Elevée (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Fonction de rappel automatique (CBCP)</p> <p><input type="checkbox"/> Activer la fonction de rappel automatique</p> <p><input type="checkbox"/> Utiliser le numéro suivant pour rappeler</p> <p>Numéro de rappel <input data-bbox="1122 905 1325 936" style="width: 100%;" type="text"/></p> <p>Crédit de rappel automatique <input data-bbox="1122 947 1203 978" style="width: 50px;" type="text" value="0"/> minute(s)</p>
---	---

Le routeur accepte trois types d'appels entrants : PPTP, Tunnel IPSec et L2TP avec politique IPSec (sous-options : Néant, Souhaitée, Imposée). Par défaut, les trois options sont actives. Si vous n'en choisissez qu'une ou deux, lisez les instructions ci-après

PPTP	Cochez cette case pour autoriser les appels entrants PPTP.
Tunnel IPSec	Cochez cette case pour autoriser les appels entrants par tunnel IPSec.
L2TP	Spécifiez la politique IPSec pour la connexion L2TP. Néant : ne pas appliquer la politique IPSec. Souhaitée : appliquer d'abord la politique IPSec. En cas d'échec, la connexion de VPN entrante est la connexion L2TP sans politique IPSec. Imposée : imposer la politique IPSec à la connexion L2TP.
Spécifier la passerelle de VPN distant	Pour renforcer la sécurité, activez cette option pour que le client distant se connecte uniquement à partir d'une adresse IP spécifique.
Adresse IP du serveur VPN homologue ou ID homologue	Spécifiez l'adresse IP du serveur de VPN distant ou l'ID homologue. Il vous faudra ensuite spécifier une clé prépartagée pour ce nœud spécifique.

Paramétrage du VPN et de l'accès à distance

Nom d'utilisateur	Spécifiez un nom d'utilisateur pour l'authentification par le routeur distant.
Mot de passe	Spécifiez un mot de passe pour l'authentification par le routeur distant.
Authentification PPP	Spécifiez la méthode d'authentification PPP pour PPTP, L2TP et L2TP sur IPSec. Normalement PAP/CHAP pour assurer la compatibilité la plus large.
Compression VJ	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.
Clé prépartagée IKE	Cliquez pour faire apparaître une fenêtre, entrez une clé prépartagée et confirmez-la pour ce nœud spécifique.
Méthode de sécurisation IPSec	<p>Spécifiez la méthode de sécurisation IPSec (authentification ou cryptage) afin de déterminer le niveau de sécurité. Vous ne devez choisir qu'une seule méthode.</p> <p>Moyenne (AH) : Spécifiez le protocole IPSec pour le protocole AH. Les données seront authentifiées mais non cryptées.</p> <p>Élevée (ESP): Spécifiez le protocole IPSec pour le protocole ESP. Les données seront cryptées. Les algorithmes pris en charge sont DES, 3DES et AES. Par défaut, ces trois algorithmes sont disponibles.</p>



Si vous n'activez pas « **Spécifier le nœud distant** » et si vous laissez le champ « **Adresse IP du serveur VPN homologue ou ID homologue** » vide, les paramètres **Clé prépartagée IKE**, et **Méthode de sécurisation IPSec** seront désactivés et il sera impossible d'établir une connexion de VPN liée à IPSec.



La fonction de rappel automatique n'est pas prise en charge pour cette version.

Paramètres TCP/IP

4. Paramètres TCP/IP

Mon adresse IP WAN	<input type="text" value="0.0.0.0"/>	Sens RIP	<input type="button" value="TX/RX"/>
Adr IP de la passerelle distante	<input type="text" value="0.0.0.0"/>	Version du RIP	<input type="button" value="Ver. 2"/>
Adr IP du réseau distant	<input type="text" value="0.0.0.0"/>	Pour le fonctionnement du NAT, traiter le sous-réseau distant comme	
Masque du réseau distant	<input type="text" value="255.255.255.0"/>	<input type="button" value="Adresse IP privée"/>	
<input type="button" value="Suite"/>		<input type="checkbox"/> Remplacer la route par défaut par ce tunnel VPN	

Mon adresse IP WAN	Dans la plupart des cas, vous pouvez accepter la valeur par défaut 0.0.0.0. Le routeur 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.
Ad. IP de la	Dans la plupart des cas, vous pouvez accepter la valeur par défaut 0.0.0.0. Le routeur obtient une adresse IP de

Paramétrage du VPN et de l'accès à distance

passerelle distante	défaut 0.0.0.0. Le routeur obtient une adresse IP de passerelle distante du routeur distant pendant la phase de négociation IPCP. Si l'adresse IP de passerelle distante est fixe, spécifiez ici l'adresse IP fixe.
Adr. IP du réseau distant	Spécifiez l'identification du réseau distant. Par exemple, 192.168.1.0 est une identification réseau d'un sous-réseau de classe C dont le masque de sous-réseau est 255.255.255.0 (/24).
Masque du réseau distant	Spécifiez le masque de sous-réseau du réseau distant.
Suite	Pour ajouter une route statique lorsque cette connexion est établie, si besoin est.
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	Le routeur Vigor prend en charge deux réseaux IP locaux : le premier sous-réseau et le deuxième sous-réseau. Vous pouvez ainsi définir quel sous réseau sera utilisé comme réseau local pour la connexion de VPN et échanger des paquets RIP avec le réseau distant. L'option choisie est généralement « IP privé » pour le routage entre le premier sous-réseau et le réseau distant.

Exemple d'interconnexion de LAN

Cet exemple décrit la manière de procéder pour paramétrer un profil d'interconnexion de LAN permettant de relier entre eux deux réseaux privés via l'internet. Dans cet exemple, le réseau privé 192.168.1.0/24 est situé au siège. Le réseau de l'établissement secondaire a pour adresse 192.168.2.0/24.

1. En premier lieu, il faut configurer la clé prépartagée dans le menu **Configuration générale IKE/IPSec de Paramétrage du VPN et de l'accès à distance** : par exemple « ABC123 ».

Paramétrage du VPN et de l'accès à distance

2. Créez un profil d'interconnexion de LAN au siège.

VPN and Remote Access >> LAN-to-LAN Profile Setup

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="head"/>	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
	Idle Timeout <input type="text" value="300"/> second(s)
	<input type="checkbox"/> Enable PING to keep alive
	PING to the IP <input type="text"/>

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input checked="" type="radio"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="branch"/> Password <input type="password" value="....."/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="123.45.67.89"/>	<input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advance"/>
	Scheduler (1-15) <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/>	Username <input type="text" value="head"/> Password <input type="password" value="....."/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="123.45.67.89"/> or Peer ID <input type="text"/>	<input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="TX/RX Both"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	RIP Version <input type="text" value="Ver. 2"/>
Remote Network IP <input type="text" value="192.168.2.0"/>	For NAT operation, treat remote subnet as <input type="text" value="Private IP"/>
Remote Network Mask <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel
<input type="button" value="More"/>	

Paramétrage du VPN et de l'accès à distance

3. Créez un profil d'interconnexion de LAN dans l'établissement secondaire.

VPN and Remote Access >> LAN-to-LAN Profile Setup

Profile Index : 2

1. Common Settings

Profile Name <input type="text" value="branch"/> <input checked="" type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
---	---

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input checked="" type="radio"/> L2TP with IPsec Policy <input type="text" value="Must"/> Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="87.66.43.21"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="head"/> Password <input type="text" value="....."/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <input type="text" value="IKE Pre-Shared Key"/> IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advance"/> Scheduler (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote
--	---

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/> <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="97.65.43.21"/> or Peer ID <input type="text"/>	Username <input type="text" value="branch"/> Password <input type="text" value="....."/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <input type="text" value="IKE Pre-Shared Key"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)
--	--

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.1.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="TX/RX Both"/> RIP Version <input type="text" value="Ver. 2"/> For NAT operation, treat remote sub-net as <input type="text" value="Private IP"/> <input type="checkbox"/> Change default route to this VPN tunnel
---	--

Chapitre 9

Paramètres VoIP

9.1 Introduction

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

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

Les routeurs série Vigor2200V/VG prennent en charge le protocole SIP car c'est un protocole idéal pour le fournisseur de service téléphonique sur internet (ITSP) et pour le « softphone » et qu'il est très répandu. Le SIP permet l'appel direct d'homologue à homologue ainsi que l'appel via un serveur proxy SIP (qui joue un rôle semblable au portier des réseaux H.323). Le protocole MGCP utilise une architecture client-serveur, le scénario d'appel étant très semblable à celui du RTCP actuel.

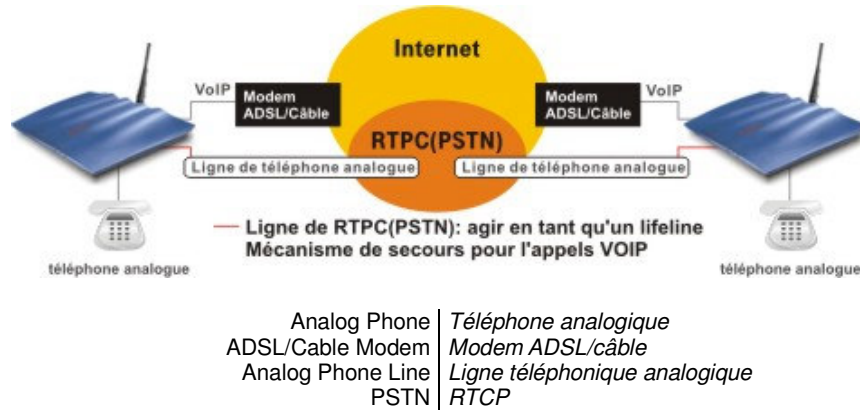
Après l'établissement d'un appel, les flux téléphoniques sont transmis via le protocole de transport en temps réel (RTP). Différents codecs (qui compriment et codent la voie) peuvent être intégrés aux paquets RTP. Les routeurs série Vigor2200V/VG fournissent différents codecs, G.711 loi A/μ, G.723, G.726 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.

Les fonctionnalités VoIP des séries Vigor2200V/VG permettent d'économiser le prix d'une ligne fixe supplémentaire. En utilisant l'ITSP (par exemple, [DrayTEL](http://DrayTEL.com), www.draytel.org), vous pouvez également appeler n'importe quelle ligne téléphonique ordinaire ou n'importe quel poste téléphonique ordinaire, y compris les mobiles, et recevoir des appels de n'importe qui – l'appel est acheminé vers votre téléphone via votre connexion internet, de sorte que votre ligne téléphonique ordinaire reste libre pour d'autres appels.

Vous pouvez appeler d'autres utilisateurs de routeurs VoIP Vigor de deux manières : en composant directement leur adresse IP sur le combiné téléphonique ou en utilisant un registre SIP. Un serveur SIP

Paramètre VoIP

sur l'internet permet à votre routeur d'enregistrer sa localisation actuelle (adresse IP) et sa disponibilité, de sorte que d'autres utilisateurs peuvent vous appeler à votre adresse SIP (par exemple, 98141@draytel.org)



Avant de paramétrer le routeur SIP, vous devez ouvrir un compte auprès d'un registre SIP (par exemple, IPTEL, DrayTEL, www.draytel.org).

Les routeurs série Vigor2200V/VG 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.

9.2 Paramètres

Cliquez sur **Paramètres VoIP** pour ouvrir la page de paramétrage.



DialPlan	Programmation d'un maximum de 60 adresses IP de contacts VoIP.
Configuration des fonctions liées au SIP	Paramétrage du port SIP du registre, du proxy, du domaine et du serveur « STUN ».
CODEC/RTP/DTMF	Paramètres par défaut du codec, DTMF et RTP

Paramètre VoIP

État de l'appel téléphonique	État de l'appel, notamment registre d'inscription, codec, connexion et autres.
QoS	Entrez la vitesse montante nécessaire pour l'appel VoIP.

9.2.1 DialPlan (plan de numérotation)

Les routeurs série Vigor2200V/VG ont un port FXS (« Phone » sur le panneau arrière) sur lequel vous branchez un téléphone analogique classique avec ou sans fil (DECT). Vous pouvez spécifier l'adresse SIP de vos contacts VoIP dans le plan de numérotation (DialPlan) du Vigor2200V/VG pour pouvoir les appeler rapidement et facilement. Vous pouvez enregistrer jusqu'à 60 adresses IP d'amis ou de parents.

Index n° 1

<input checked="" type="checkbox"/> Activer	
Numéro de téléphone	: 12
Afficher le nom	: Dolly
URL SIP	: 63065 @ fwd.pulver.com
Bouclage	: Néant
Sauvegarder le numéro de téléphone	: 34392034

Index n° 2

<input checked="" type="checkbox"/> Activer	
Numéro de téléphone	: 234
Afficher le nom	: Kathy
URL SIP	: 393910 @ draytel.org
Bouclage	: RTPC
Sauvegarder le numéro de téléphone	: 4632413

Configuration d'un plan de numérotation

Index	Numéro de téléphone	Afficher le nom	URL SIP	Bouclage	Sauvegarder le numéro de téléphone	État
1.	12	Dolly	63065@fwd.pulver.com	None	34392034	v
2.	234	Kathy	393910@draytel.org	PSTN	4632413	v
3.				None		x
4.				None		x
5.				None		x
6.				None		..

Activer

Paramètre VoIP

Cochez la case pour activer cette entrée.

Numéro de téléphone

Numéro à composer sur votre combiné pour appeler ce contact. N'importe quelle combinaison des chiffres 0 à 9 et de *

Afficher le nom

Ce champ contient un nom ou un numéro qui vous permet d'identifier facilement la personne que vous voulez appeler. Ce peut être aussi le nom à afficher.

Adresse URL SIP

Entrez l'adresse SIP de votre contact (par exemple, 393910@draytel.org)

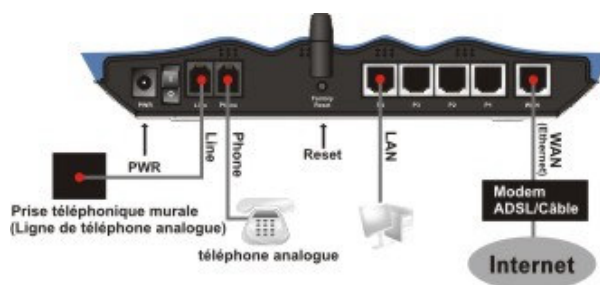
Bouclage

Les routeurs série Vigor2200V/VG ont un port « Line » à l'arrière pour le branchement d'une ligne téléphonique ordinaire (RTCP). L'option de bouclage peut être utilisée pour programmer un numéro de téléphone SIP alternatif pour votre contact sur le RTCP, que le routeur Vigor2200V/VG appellera au lieu du numéro SIP si votre accès à haut débit tombe en panne. Ainsi, la ligne RTCP peut servir de ligne de secours pour les appels VoIP. Le mode par défaut est le mode VoIP. Le mécanisme de ligne de secours est activé automatiquement si vous spécifiez « **RTCP** » et le **numéro de téléphone de secours**.

Exemple 1

Si Dolly vous donne son URL SIP (**sip:63065@fwd.pulver.com**), vous pouvez entrer ce numéro tel que. Vous pouvez appliquer un nom affiché et un numéro de téléphone.

Branchements du routeur Vigor2200V :



Land lin jack (Analog Phone)	Prise téléphonique (ligne téléphonique analogique)
Analog Phone	Téléphone analogique
Phone	Téléphone
Line	Ligne
ADSL/Cable Modem	Modem ADSL/câble

Numéro de téléphone de secours : Le numéro de téléphone alternatif à composer si « RTCP » est sélectionné dans **Bouclage**.

Index n° 2

<input checked="" type="checkbox"/> Activer	
Numéro de téléphone	: 234
Afficher le nom	: Kathy
URL SIP	: 393910 @ draytel.org
Bouclage	: RTCP
Sauvegarder le numéro de téléphone	: 4632413

Exemple 2

Si Kathy vous donne son URL SIP (**sip:39390@draytel.org**) et que son numéro de téléphone (RTCP) est **4632413**, vous pouvez enregistrer ce qui suit dans le plan de numérotation :

Numéro de téléphone : 234 (n'importe quel numéro)
Afficher le nom : Kathy
URL SIP : 39390 @draytel.org
Bouclage : RTCP
Numéro de téléphone de secours : 4632413

Exemple 3

Si Kathy vous donne son adresse IP (203.69.175.19) et que cette adresse ne figure pas dans votre DialPlan, vous pouvez composer sur le clavier du téléphone **#203*69*175*19#**



Pour composer manuellement le numéro de secours, entrez « **#0** » **sur votre combiné téléphonique**, puis composez un numéro de téléphone RTCP. Si vous avez peur que le bouclage automatique entraîne une surtaxation de votre numéro de téléphone RTCP, nous vous recommandons de ne pas entrer votre numéro de téléphone RTCP dans « Numéro de téléphone de secours ». Vous ne pourrez alors effectuer le bouclage qu'en composant manuellement un numéro RTCP.

9.2.2 Configuration des fonctions liées au SIP

SIP

Port SIP	: 5060
Registre	: draytel.org
Proxy	: draytel.org <input type="button" value="Dupliquer"/>
Domaine/Espace de protection (Realm)	: draytel.org <input type="button" value="Dupliquer"/>
<input checked="" type="checkbox"/> Désactiver le serveur	:

Paramétrage des ports

Port 1

<input checked="" type="checkbox"/> Utiliser le serveur Registrar	
Nom affiché	: Tina
Nom de compte	: 8999999
Nom d'utilisateur autorisé	: 8999999 <input type="button" value="Dupliquer"/>
Mot de passe	: ●●●●●●
Délai d'expiration	: 2 heures <input type="button" value="v"/>

Paramètre VoIP

Une fois que vous êtes inscrit sur un serveur SIP (par exemple, **DrayTEL**), spécifiez votre nom d'utilisateur et votre mot de passe SIP dans les champs appropriés (voir plus loin). Dans le champ Registre, entrez le nom de domaine du serveur SIP – tout ce qui suit le signe @ de votre adresse SIP. Cliquez sur **OK**. Votre routeur se connecte au serveur SIP. Dans le champ « **État appel VoIP** », un « **R** » indique que vous êtes inscrit sur votre serveur SIP.

VoIP >> État appel VoIP

État appel VoIP

Volume du canal: << >> Intervalle d'actualisation (s) : 10 v Actualiser Afficher le journal

Canal	État	Codec	ID pair	Temps de connexion	Émission de paquets	Paquets TX	Poquets perdus RX	Gigue (ms)	Appels entrants	Appels sortants	Gain
1(R)	ACTIVE	723M/B	sam543@iptel.org	91	9038	9076	0	9	2	0	6

(R) : Signifie que vous avez enregistré votre serveur SIP

Port SIP

Le numéro de port utilisé pour envoyer ou recevoir un message SIP. La valeur par défaut est 5060 et elle doit correspondre au registre homologue lors d'un appel VoIP.

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 Registrar.

Registre

Entrez le nom de domaine (ou l'adresse IP) de votre serveur Registrar SIP.

Proxy

Vous pouvez entrer le nom de domaine ou l'adresse IP du serveur proxy SIP. Si cette valeur est la même que pour le serveur registre, cliquez sur « Dupliquer ».

Domaine/Espace de protection (Realm)

Vous pouvez entrer le nom de domaine ou l'adresse IP de l'URL SIP, par exemple si l'URL SIP est **sip:63065@fwd.pulver.com**, ce champ contient **fwd.pulver.com**. Si cette valeur est la même que pour le serveur registre, cliquez sur « Dupliquer ».

Désactiver le serveur

Ce paramètre définit si le mécanisme « NAT Traversal » du Vigor2200V/VG est activé (case cochée) ou non. S'il est activé, spécifiez également l'adresse IP du serveur STUN. Dans ce mode,

Paramètre VoIP

les communications VoIP en provenance du Vigor2200V/VG peuvent passer avec le serveur STUN spécifié derrière le pare-feu/NAT.

Utiliser le serveur Registrar

Dans le domaine Registrar entré précédemment, cochez cette case pour que le Vigor2200V/VG utilise le Registrar SIP.

Afficher le nom

Ce champ contient un nom ou un numéro qui vous permet d'identifier facilement la personne que vous voulez appeler. Ce nom peut être aussi le nom affiché.

Nom de compte

Tapez le nom de compte de votre adresse SIP (la première partie de votre adresse IP, avant le signe @).

Nom d'utilisateur autorisé

Ce champ contient un nom ou un numéro. C'est le nom d'un utilisateur autorisé. Si cette valeur est la même que le nom de compte, cliquez sur « Dupliquer ».

Mot de passe

Votre adresse URL SIP obtenue lors de votre inscription 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 Vigor enverra une autre demande d'inscription au serveur registre SIP.

9.2.3 CODEC/RTP/DTMF

Codecs

Codec par défaut	:	G.729A/B (8 kbit/s) ▾
Taille des paquets	:	20ms ▾

DTMF

<input checked="" type="radio"/> Dans la bande	<input type="radio"/> Hors bande	Type de charge utile:	101	<input type="radio"/> INFO SIP
--	----------------------------------	-----------------------	-----	--------------------------------

RTP

Port de début RTP dynamique	:	10050
Port de fin RTP dynamique	:	15000

Codec par défaut

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 64kbit/s, n'utilisez pas le codec G.711. Si vous voulez utiliser le codec G.711, il vaut mieux avoir au moins 256kbit/s dans le sens montant.

Taille des paquets

La valeur par défaut est 20 ms, ce qui signifie que le paquet de données contient 20 ms d'informations vocale.

DTMF dans la bande

Si cette option est sélectionnée, le Vigor envoie directement des tonalités DTMF dans le flux téléphonique lorsque vous appuyez sur une touche du clavier.

DTMF hors bande

Si cette option est sélectionnée, le Vigor capture le numéro composé au clavier, le transforme, le numérise et l'envoie de l'autre côté, à l'extérieur du flux téléphonique. 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.

Type de charge utile DTMF

La valeur par défaut est 101 mais elle peut être comprise entre 96 et 127.

Info SIP

Activez cette option pour que le proxy SIP envoie des tonalités DTMF à l'homologue appelé.

RTP

Spécifiez le port de début et le port de fin du flux RTP. Les valeurs par défaut sont 10050 et 15000.

Scénario d'appel

Exemple d'appel d'homologue à homologue

Arnold et Pauline ont chacun un routeur Vigor2500V. Voici les paramètres qui leur permettent de converser.

Adresse IP d'Arnold : **214.61.172.53**

Adresse IP de Pauline : **203.69.175.24**

A. Paramètres d'Arnold

A-1. DialPlan n°1

Numéro de téléphone : **1234**

(n'importe quel numéro)

Nom affiché : **arnold**

Adresse IP / Domaine :

203.69.175.24

B. Paramètres de Pauline

B-1. DialPlan n°1

Numéro de téléphone : **123**

(n'importe quel numéro)

Nom affiché : **pauline**

Adresse IP / Domaine :

214.61.172.53

A-2. Fonction liée au SIP

Port SIP : **5060 (valeur par défaut)**

Registrar : **(vide)**

Port 1:

S'inscrire via : **(vide)**

Nom affiché : **arnold**

Mot de passe : **(vide)**

Délai d'expiration : **(utiliser la valeur par défaut)**

B-2. Fonction liée au SIP

Port SIP : **5060 (valeur par défaut)**

Registrar : **(vide)**

Port 1:

S'inscrire via : **(vide)**

Nom affiché : **pauline**

Mot de passe : **(vide)**

Délai d'expiration : **(utiliser la valeur par défaut)**

A-3. CODEC/RTP/DTMF

(utiliser la valeur par défaut)

B-3. CODEC/RTP/DTMF

(utiliser la valeur par défaut)

C. Maintenant, lorsque qu'Arnold veut appeler Pauline, il décroche le téléphone et compose **1234#**.

D. Quand Pauline désire appeler Arnold, elle décroche le téléphone et compose **123#**

Appel via le serveur SIP

Ci-dessous, les paramètres permettant à Jean et David de converser à l'aide de leur compte SIP enregistré sur DrayTEL car aucun des utilisateurs Vigor n'a une adresse IP publique fixe.

URL SIP de Jean : **john@draytel.org**

URL SIP de David : **david@draytel.org**

A. Paramètres de Jean

B. Paramètres de David

A-1. DialPlan n°1

B-1. DialPlan n°1

Numéro de téléphone : **2536**
(n'importe quel numéro)
Nom affiché : **david**
Adresse IP / Domaine : **draytel.org**

Numéro de téléphone : **8989**
(n'importe quel numéro)
Nom affiché : **jean**
Adresse IP / Domaine : **draytel.org**

A-2. Fonction liée au SIP

B-2. Fonction liée au SIP

Port SIP : **5060**
Registrar : **draytel.org**

Port SIP : **5090**
Registrar : **draytel.org**

Port 1:
S'inscrire via : **(coché)**
Nom affiché : **john**
Mot de passe : *********
(entrez le mot de passe de registre de Jean)
Délai d'expiration : **(utiliser la valeur par défaut)**

Port 1:
S'inscrire via : **(coché)**
Nom affiché : **david**
Mot de passe : *********
(entrez le mot de passe de registre de David)
Délai d'expiration : **(utiliser la valeur par défaut)**

A-3. CODEC/RTP/DTMF

B-3. CODEC/RTP/DTMF

(utiliser la valeur par défaut)

(utiliser la valeur par défaut)

C. Maintenant, lorsque John veut appeler David, il décroche le téléphone et compose **2536#**.

D. Quand David désire appeler John, il décroche le téléphone et compose **8989#**

9.2.4 État de l'appel téléphonique

La fonction État de l'appel téléphonique vous permet de visualiser le registre d'inscription, le codec, la connexion et d'autres informations d'état importantes. Comme le Vigor2200V/VG n'a qu'un seul port VoIP pour la téléphonie ordinaire, il n'y a qu'un seul canal VoIP.

VoIP >> État appel VoIP

État appel VoIP

Volume du canal: << >> Intervalle d'actualisation (s) : 10 Actualiser Afficher le journal

Canal	État	Codec	ID pair	Temps de connexion	Émission de paquets	Paquets TX	Paquets perdus RX	Gigue (ms)	Appels entrants	Appels sortants	Gain
1	(R) ACTIVE	723K/b	sam543@iptel.org	31	3038	3076	0	3	2	0	6

(R) :Signifie que vous avez enregistré votre serveur SIP

Volume du canal

Pour régler le volume de vos appels VoIP. Utilisez les deux boutons << >> pour régler le **volume**.

Intervalle d'actualisation

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

État

Permet de 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

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 perdu 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.

Afficher le journal

Visualisation du journal des appels VoIP.

Paramètre VoIP

L'état système vous permet de voir le registre et le codec utilisés pour les appels entrants et pour les appels sortants. Vous pouvez ainsi vérifier si votre inscription auprès du serveur SIP a réussi ou non.

État du système

Nom de modèle	:Vigor2200V series		
Version du firmware	:v2.5.5.4		
Date/Heure de création	:Mon May 9 17:54:8.85 2005		
<hr/>			
LAN		WAN	
Adresse MAC	:00-50-7F-2E-A4-5E	Adresse MAC	:00-50-7F-2E-A4-5F
Adresse IP	:192.168.1.1	Connexion	:---
Masque de sous-réseau	:255.255.255.0	Adresse IP	:---
Serveur DHCP	:Yes	Passerelle par défaut	:---
		DNS	:168.95.1.1
<hr/>			
VoIP		LAN sans fil	
Canal	: 1 → VoIP Mode	Adresse MAC	:00-11-09-f7-a6-91
Registre SIP	:	Domaine de fréquence	:Europe
Account ID	:p0	Version du firmware	:v1.42.8.16.04.2
S'inscrire	:Non		
Codec	:		
Appels entrants	:0		
Appels sortants	:0		

9.2.5 QoS

Entrez la vitesse montante pour que le Vigor2200V/VG donne la priorité aux appels VoIP.

Contrôle de QoS

Activer le contrôle de QoS

Vitesse montante kbit/s

Nota :Priorité QoS pour trafic VoIP.
Votre vitesse montante, par exemple, 256 kbit/s
(la 'vitesse montante' est la vitesse de transmission vers l'internet)

Chapitre 10

LAN sans fil

10.1 Introduction

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. Les routeurs à haut débit résidentiels série Vigor2200VG sont conçus pour accroître la souplesse et l'efficacité des communications pour les professions indépendantes et les particuliers en leur permettant de déployer un réseau local sans fil.

Ainsi, 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.

Autre exemple, des parents peuvent rédiger des messages électroniques dans leur bureau et les enfants peuvent naviguer sur l'internet dans leur chambre avec le Vigor2200VG quelque part dans la maison. Inutile de percer un trou pour installer un câble réseau dans la maison.

Les routeurs série Vigor2200VG sont dotés d'une interface LAN sans fil conforme au protocole IEEE 802.11g autorisant un débit de 54Mbit/s. Le LAN sans fil procure une haute mobilité à plusieurs utilisateurs, de sorte qu'ils peuvent accéder simultanément à toutes les fonctionnalités du LAN, à l'internet et au WAN.

10.2 Paramètres

Cliquez sur **LAN sans fil** pour ouvrir la page de paramétrage.



10.2.1 Paramètres généraux

Paramètre général (IEEE 802.11)

Activer le LAN sans fil

Mode :

Plages horaires (1-15)

SSID :

Canal :

Masquer le SSID

Préambule long

SSID :ID du jeu de services du LAN sans fil.
Masquer le SSID :l'outil de scrutation ne peut pas lire les SSID à la réception.
Canal :choisir le canal radio du LAN sans fil.
Préambule long :activez-le uniquement lorsqu'il y a des problèmes de connectivité pour certains anciens périphériques 802.11b ; sinon cela réduit les performances.

Activer le LAN sans fil

Cochez la case pour activer la fonction sans fil.

Mode

Sélectionner un mode sans fil approprié.

Mixte (11b+11g)	Les protocoles IEEE802.11b et IEEE802.11g sont pris en charge simultanément.
11g seulement	Seul le protocole IEEE802.11g est pris en charge.
11b seulement	Seul le protocole IEEE802.11b est pris en charge.

Plages horaires

Vous pouvez limiter le fonctionnement du LAN sans fil à certaines plages horaires.

SSID et Canal

Le SSID par défaut est « valeur par défaut ». Nous suggérons de remplacer « valeur par défaut » par une combinaison quelconque de caractères. En l'occurrence, le SSID a été remplacé par « DrayTek ».

Le SSID par défaut est « valeur par défaut ». Nous vous suggérons de remplacer « valeur par défaut » par une combinaison quelconque de caractères (lettres, chiffres ou caractères spéciaux).

SSID	Sert à identifier le LAN sans fil. Cet identifiant doit être le même sur la ou les cartes sans fil du PC/bloc-notes client. Le SSID peut se composer d'un nombre quelconque de caractères ou divers caractères spéciaux.
Canal	Canal radio du routeur. 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.

10.2.2 Sécurité

Pour renforcer la sécurité et la confidentialité de paquets de données sans fil, les fonctions de cryptage WEP et WPA peuvent être utilisées. La fonction WEP utilise quatre clés par défaut pour crypter chaque trame transmise par radio en utilisant uniquement l'une des clés données. Les clés par défaut sont partagées entre le routeur sans fil Vigor et la station WEP. Une fois qu'une station a obtenu les clés par défaut pour son ensemble de services, elle peut communiquer avec WEP. WPA (Wi-Fi Protected Access) utilise le protocole d'intégrité de clé temporelle (TKIP) pour le cryptage. Il renforce grandement la protection des données radio et le contrôle d'accès sur les réseaux Wi-Fi existants. Il pallie les faiblesses du WEP. Si vous cliquez sur **Paramètres de sécurité**, une nouvelle page web apparaît vous permettant de configurer WEP et WPA.

LAN sans fil

Paramètres de sécurité

Mode:	Désactiver
WPA:	
Mode de cryptage:	TKIP
Clé prépartagée (PSK)	*****
Tapez 8 à 63 caractères ASCII ou 64 chiffres hexadécimaux commençant par "0x", par exemple, "cfigs01a2..." ou "0x655abcd....".	
WEP:	
Mode de cryptage:	64 bits
Utiliser	Clé WEP
<input checked="" type="radio"/> Clé 1 :	*****
<input type="radio"/> Clé 2 :	*****
<input type="radio"/> Clé 3 :	*****
<input type="radio"/> Clé 4 :	*****

Mode

Sélectionnez un mode de cryptage approprié pour améliorer la sécurité et la confidentialité de vos paquets de données sans fil.

Désactiver	Désactive le mécanisme de cryptage.
WEP seulement	Accepte uniquement les clients WEP. La clé doit être tapée dans WEP Key.
WEP ou WPA/PSK	Accepte simultanément les clients WEP et WPA. La clé de cryptage doit être tapée dans WEP Key et dans PSK.
WPA/PSK	Accepte uniquement les clients WPA. La clé doit être tapée dans PSK.

Cryptage WPA

Le cryptage WPA crypte chaque trame transmise par radio à l'aide de la clé prépartagée (PSK) entrée ici.

Clé partagée (PSK): Entrez 8 à 63 caractères ASCII 64 chiffres hexadécimaux commençant par 0x, par exemple "0123456789ABCD...." ou "0x321253abcde.....".

Cryptage WEP

64 bits	Pour une clé WEP de 64 bits, entrez soit 5 caractères ASCII, soit 10 chiffres hexadécimaux commençant par 0x. Par exemple, ABCDE ou 0x4142434445.
128 bits	Pour une clé de cryptage de 128 bits, entrez soit 13 caractères ASCII, soit 26 caractères hexadécimaux commençant par 0x. Par exemple, ABCDEFGHIJKLM ou 0x4142434445464748494A4B4C4D.



Le cryptage WEP sur 128 bits est le plus sûr mais le surdébit de cryptage/décryptage est plus important. A noter que tous les équipements sans fil doivent prendre en charge le même nombre de bits de cryptage WEP et avoir la même clé. Quatre clés peuvent être entrées ici mais seule une clé peut être sélectionnée à un moment donné. Les clés peuvent être entrées en ASCII ou en hexadécimal. Cliquez sur le cercle Utilisation en regard de la clé que vous voulez utiliser.

10.2.3 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 en contrôlant l'adresse MAC du LAN sans fil. Seule l'adresse MAC valable configurée peut accéder à l'interface de 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.

Contrôle d'accès

Activer le contrôle d'accès

Index	Adresse MAC

Adresse MAC :

: : : : :

Nota :Ajoutez ou supprimez l'adresse MAC de l'utilisateur sans fil pour accepter ou refuser l'accès au réseau.

Activer le contrôle d'accès

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

Adresse MAC

Affichage de toutes les adresses MAC éditées précédemment. Quatre boutons (Ajouter, Supprimer, Modifier et Annuler) permettent d'éditer une adresse MAC.

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.
Supprimer tout	Supprimer toutes les adresses MAC.
OK	Enregistrer la liste de contrôle d'accès.

10.2.4 Liste des stations

Le routeur Vigor vous offre une **fonction liste des stations** qui vous permet de scruter tous les clients WLAN proches du routeur. Si des clients voisins ou autres clients WLAN sont actifs, vous pouvez cliquer sur « Actualiser » pour obtenir des informations sur les stations WLAN, notamment leur état et leur adresse MAC. Vous pouvez sélectionner une station WLAN dans la **liste des stations** pour l'ajouter à la liste de **Contrôle d'accès** en cliquant dessus, puis en cliquant sur « **Ajouter** ». Vous pouvez aussi modifier manuellement l'adresse MAC d'une station. Après ces opérations, vous pouvez aller dans **Contrôle d'accès** pour visualiser les stations WLAN autorisées à accéder aux ressources du réseau via le routeur Vigor.

État	Adresse MAC

Chapitre 11

Maintenance du système

11.1 Introduction

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.

La **sauvegarde de la configuration** vous permet de conserver les configurations de votre routeur sous la forme de fichiers ou de restaurer les configurations avec ces fichiers. Le routeur vous permet de sauvegarder ou de restaurer la configuration d'une manière très simple via l'internet.

Par défaut, le routeur peut être configuré et géré à l'aide de n'importe quel client Telnet ou de n'importe quel navigateur internet fonctionnant sous n'importe quel système d'exploitation. Aucun logiciel supplémentaire n'est nécessaire. Toutefois, dans certains environnements spécifiques, vous pouvez modifier les numéros de port pour le serveur Telnet ou http intégré, créer des listes de contrôle d'accès pour protéger le routeur ou empêcher l'administrateur système de se connecter à l'internet.

Par ailleurs, à l'aide des fonctions de réinitialisation du système et de mise à jour du logiciel, vous pouvez réinitialiser le système après certaines opérations de paramétrage et mettre à jour le logiciel via TFTP.

11.2 Paramètres

Cliquez sur **Maintenance du système** pour ouvrir la page de paramétrage.



État du système	Paramétrages d'un maximum de 60 adresses SIP de contacts VoIP.
Mot de passe administrateur	Paramétrages de port SIP, de registre, de proxy, de domaine et de serveur Stun.
Sauvegarde des configurations	Paramétrages de codec, DTMF et RTP par défaut
SysLog/Mail Alert	État d'appel, notamment registre d'inscription et autres.
Réglage de l'heure	Réglage de l'heure à partir du PC ou d'un serveur NTP.
Paramètres de gestion	Paramétrages du contrôle d'accès de gestion, SNMP et de port.
Réinitialisation du système	Réinitialisation du système.
Mise à jour du firmware (TFTP)	Mise à jour du logiciel via TFTP

11.2.1 État du système

Dans **État du système**, vous pouvez visualiser les informations suivantes.

État du système

Nom de modèle	:Vigor2200V series
Version du firmware	:v2.5.5.4
Date/Heure de création	:Mon May 9 17:54:8.85 2005

LAN		WAN	
Adresse MAC	:00-50-7F-2E-A4-5E	Adresse MAC	:00-50-7F-2E-A4-5F
Adresse IP	:192.168.1.1	Connexion	:---
Masque de sous-réseau	:255.255.255.0	Adresse IP	:---
Serveur DHCP	:Yes	Passerelle par défaut	:---
		DNS	:168.95.1.1

VoIP		LAN sans fil	
Canal	: 1 → VoIP Mode	Adresse MAC	:00-11-09-f7-a6-91
Registre SIP	:	Domaine de fréquence	:Europe
Account ID	:p0	Version du firmware	:v1.42.8.16.04.2
S'inscrire	:Non		
Codec	:		
Appels entrants	:0		
Appels sortants	:0		



La barre d'état du menu de paramétrage vous permet de voir les paramètres. « Prêt » indique que vous pouvez passer en mode paramétrage. « Paramètres enregistrés » signifie que vos paramètres seront enregistrés une fois que vous aurez cliqué sur « **Terminer** », ou sur « **OK** ». Si les paramètres sont erronés, un message d'échec s'affiche dans la barre **d'état**.

11.2.2 Sauvegarde des configurations

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

Sauvegarde/restauration des configurations

Restauration

Sélectionner un fichier de configuration.

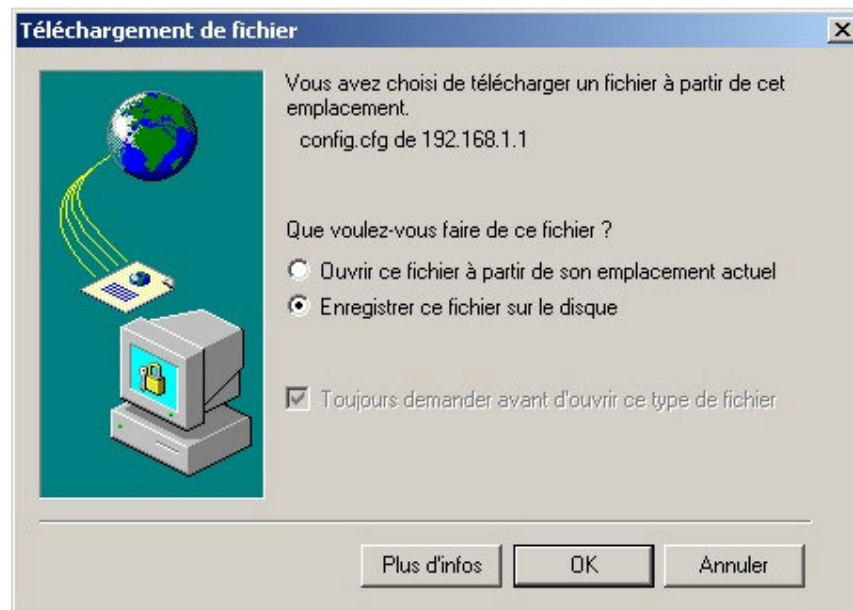
Cliquer sur Restaurer pour restaurer le fichier.

Sauvegarder

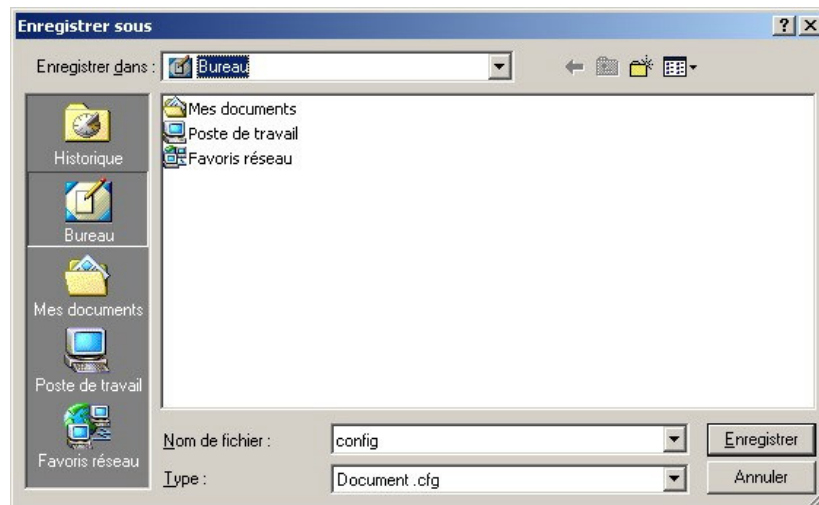
Cliquer sur Sauvegarder pour télécharger les configurations actuellement actives sous la forme d'un fichier.

Maintenance du système

2. Cliquez sur le bouton Sauvegarder.



3. Cliquez sur le bouton OK pour enregistrer la configuration sur la forme dans un fichier. Le nom du fichier par défaut est **config.cfg**. Vous pouvez lui donner un autre nom.



Maintenance du système

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.

Restaurer la configuration à partir d'un fichier de 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.

Sauvegarde/restauration des configurations

Restauration

Sélectionner un fichier de configuration.

Cliquer sur Restaurer pour restaurer le fichier.

Sauvegarder

Cliquer sur Sauvegarder pour télécharger les configurations actuellement actives sous la forme d'un fichier.

3. Cliquez sur le bouton **Restaurer** et attendez quelques secondes. Vous êtes informé du succès de la restauration.

11.2.3 Gestion

Cliquez sur **Paramètres de gestion**. La page de paramétrage suivante apparaît.

Paramètres de gestion

Contrôle d'accès pour la gestion

Activer la mise à jour à distance du firmware (FTP)

Autoriser la gestion à partir de l'internet

Désactiver le PING en provenance de l'internet

Liste des accès

Liste IP	Masque de sous-réseau
1	<input type="text"/> <input type="button" value="v"/>
2	<input type="text"/> <input type="button" value="v"/>
3	<input type="text"/> <input type="button" value="v"/>

Paramétrage du port de gestion

Ports par défaut (Telnet:23, HTTP:80, FTP:21)

Ports définis par l'utilisateur

Port Telnet

Port HTTP

Port FTP

Paramètres de gestion

Numéro de port utilisé pour envoyer/recevoir des messages SIP. La valeur par défaut est 5060 et doit correspondre avec le registre homologue pour les appels VoIP.

<i>Autoriser la mise à jour à distance du firmware</i>	Cliquez sur la case pour autoriser la mise à jour à distance du firmware via le protocole de transfert de fichier (FTP).
<i>Autoriser la gestion à partir de l'internet</i>	Cochez la case pour autoriser les administrateurs système à se connecter à partir de l'internet. Par défaut, la connexion n'est pas autorisée.
<i>Désactiver le PING en provenance de l'internet</i>	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.

<i>IP</i>	Adresse IP autorisée à se connecter au routeur.
<i>Masque de sous-réseau</i>	Masque de sous-réseau autorisé à se connecter au routeur.

Paramétrage du port de gestion

<i>Ports par défaut</i>	Cochez la case pour utiliser les numéros de ports standard pour les serveurs Telnet et HTTP.
<i>Ports définis par l'utilisateur</i>	Cochez la case pour spécifier des numéros de port définis par l'utilisateur pour les serveurs Telnet et HTTP.
<i>Activer l'agent SNMP</i>	Cochez la case pour activer l'agent SNMP intégré.
<i>Communauté pour GET</i>	Spécifiez une chaîne pour identifier les communautés de gestion pour la commande GET SNMP.
<i>Communauté pour</i>	Spécifiez une chaîne pour identifier les communautés de gestion pour la commande SET SNMP.

Maintenance du système

SET	de gestion pour la commande SET SNMP.
Adr IP du gestionnaire	Spécifiez l'adresse IP du gestionnaire SNMP.
Communauté notifiée	Spécifiez une chaîne pour identifier les communautés de gestion pour les notifications TRAP SNMP.
Adr IP de notification	Spécifiez l'adresse IP de la station qui veut recevoir les notifications TRAP.

Réinitialisation du système

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

Réinitialiser le système

Vouslez-vous réinitialiser votre routeur ?

Utilisation de la configuration actuelle

Utilisation de la configuration par défaut

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 de 3 à 5 secondes.

Mise à jour du firmware

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. L'exemple ci-dessous suppose que vous utilisez un système d'exploitation Windows.

1. Téléchargez le firmware le plus récent à partir du site de DrayTek ou du site FTP. Le site de DrayTek est www.draytek.com (ou le site local de DrayTek) et le site FTP est ftp.draytek.com

2. Cliquez sur Maintenance du système >> Utilitaire de mise à jour du firmware du routeur pour lancer l'utilitaire de mise à jour du firmware.

Maintenance du système

Mise à jour du firmware

Version actuelle du firmware:v2.5.5.4

Procédures de mise à jour du firmware:

- 1: Cliquez sur "OK" pour lancer le serveur TFTP.
- 2: Ouvrez le programme de mise à jour de firmware ou autre logiciel client TFTP tiers.
- 3: Vérifiez que le nom de fichier du firmware est correct.
- 4: Cliquez sur "Mettre à jour" dans la fenêtre du programme de mise à jour de firmware pour lancer la mise à jour.
- 5: Après la mise à jour, le serveur TFTP s'arrête automatiquement.

Voulez-vous mettre à jour le firmware ?

Cliquez sur le bouton **Parcourir** pour localiser le nouveau fichier de firmware. Le programme recherche les routeurs Vigor éventuels de votre LAN et affiche leur adresse IP. Sélectionner l'adresse IP du routeur à mettre à jour, puis cliquez sur **Mettre à jour**. Entrez le mot de passe du routeur (cliquez sur **OK** s'il n'y a pas de mot de passe). La mise à jour commence. Une fois la mise à jour terminée, attendez environ 30 secondes ; le routeur est prêt (le voyant ACT à l'avant de votre routeur recommence à clignoter normalement).

Chapitre 12

Paramétrage des diagnostics

12.1 Introduction

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

12.2 Paramètres

Cliquez sur **Diagnostics** pour ouvrir la page de paramétrage.



12.2.1 Diagnostics PPPoE/PPTP



Actualiser	Pour obtenir les informations les plus récentes, cliquez sur Actualiser.
Mode/État de l'accès à haut débit	Affiche le mode et l'état de l'accès à haut débit. Si la connexion à haut débit est active, on a PPPoE , PPTP , IP Statique , ou Client DHCP , selon le mode d'accès activé. Si la connexion est inactive, "---" est affiché.
Adresse IP WAN	Adresse IP WAN pour la connexion active.

Paramétrage des diagnostics

Appel PPPoE ou PPTP	Cliquez sur cette option pour que routeur établisse une connexion PPPoE ou PPTP.
----------------------------	--

12.2.2 Table de cache ARP

Cliquez sur **Visualiser la table de cache ARP** pour visualiser le contenu du cache ARP du routeur. La table affiche la correspondance entre une adresse matérielle Ethernet (adresse MAC) et une adresse IP.

Table ARP Ethernet [Actualiser/Rafraichir](#)

IP Address	MAC Address
192.168.1.10	00-0C-6E-E7-79-C0

Actualiser : Cliquez pour recharger la page.

12.2.3 Adresses IP attribuées par DHCP

La fonction de visualisation des adresses IP attribuées par DHCP fournit des informations sur l'attribution des adresses IP. Ces informations sont utiles pour diagnostiquer les problèmes de réseau, comme les conflits d'adresse IP, etc.

Table des adresses IP DHCP [Actualiser](#)

DHCP server: Running

Index	IP Address	MAC Address	Leased Time	HOST ID
1	192.168.1.1	00-50-7F-2E-A4-5E	ROUTER IP	
2	192.168.1.10	00-0C-6E-E7-79-C0	0:00:17.310	PEGGIE-XP