

Guide d'utilisation des routeurs série Vigor2700e/Ge

Version : 1.0

Date : 11/01/2008

Copyright 2008 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. Le lot de livraison et d'autres détails sont susceptibles d'être modifiés sans préavis.

Microsoft est une marque déposée de Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP et Explorer sont des marques de Microsoft Corp. Apple et Mac OS sont des marques déposées d'Apple Inc. Les autres produits peuvent être des marques ou des marques déposées de leurs fabricants respectifs. Page laissée intentionnellement vierge.

Table des matières



Préambule	.1
1.1 Voyants lumineux, prises et interfaces	. 1
1.1.1 Vues avant et arrière du Vigor2700e 1.1.2 Vue arrière du Vigor2700Ge	. 1 . 2
1.2 Installation du matériel	. 3



Configuration de base	5
2.1 Changement de mot de passe	5
2.2 Assistant de démarrage rapide	7
2.2.1 Choix du type de protocole/encapsulation 2.2.2 PPPoE/PPPoA 2.2.3 IP ponté 2.2.4 IP routé	
2.3 État en ligne propre à chaque protocole	
2.4 Barre d'état	



Configuration web avancé	15
3.1 Accès à l'internet	15
 3.1.1 Principes de base d'un réseau à protocole internet (IP) 3.1.2 PPPoE/PPPoA 3.1.3 MPoA 3.1.4 Multi-PVC 	15 16 19 21
3.2 Réseau local (LAN)	22
 3.2.1 Principes du réseau local 3.2.2 Configuration générale 3.2.3 Route statique 3.2.4 VLAN 	22 24 27 29
3.3 NAT	32
 3.3.1 Redirection de port 3.3.2 Configuratin de l'hôte DMZ 3.3.3 Ouverture de ports 3.3.4 Liste des ports connus 	32 34 36 38
3.4 Pare-feu	38
 3.4.1 Principes du pare-feu 3.4.2 Configuration générale 3.4.3 Paramétrage des filtres 3.4.4 Blocage des applications de messagerie instantanée (IM) 3.4.5 Blocage des applications de partage de fichiers entre homologue (P2P)	

3.4.7 Filtre de contenu d'URL 3.4.8 Filtre de contenu web	51 53
3.5 Gestion de la bande passante	53
3.5.1 Limite des sessions 3.5.2 Limite de bande passante	53 55
3.6 Applications	56
3.6.1 Dynamic DNS 3.6.2 Plages horaires 3.6.3 UPnP	56 57 59
3.7 LAN sans fil	61
 3.7.1 Principe de base 3.7.2 Paramètres généraux 3.7.3 Sécurité 3.7.4 Contrôle d'accès 3.7.5 WDS 3.7.6 Découverte d'AP 3.7.7 Liste des stations 	62 63 64 66 66 66 69 70
3.8 Maintenance du système	71
 3.8.1 État du système	
3.9 Diagnostics	78
 3.9.1 Connexion WAN 3.9.2 Trigger de sortie. 3.9.3 Table de routage. 3.9.4 Table de cache ARP (protocole de résolution d'adresse) 3.9.5 Table DHCP. 3.9.6 Table des sessions actives NAT 3.9.7 Diagnostic par « ping ». 3.9.8 Surveillance des flux de données 	
3.9.9 Trace route	



Application et Exemples	85
4.4 Création d'un LAN avec NAT	85
4.2 Mise à jour du firmware de votre routeur	87



Dépannage	91
4.1 Le matériel est-il installé correctement ?	91
4.2 Les paramètres de connexion réseau de votre ordinateur sont-ils corrects ?	91
4.3 Le routeur répond-t-il à un « ping » de votre ordinateur ?	94

4.4 Les paramètres FAI sont-ils corrects ?	96
4.5 Rétablissement des paramètres par défaut si nécessaire	97
4.6 Contacter votre revendeur	98



Destinés à répondre aux besoins des utilisateurs résidentiels, des travailleurs indépendants et des professions libérales (SOHO) et des entreprises, le routeur Vigor2700e/2700Ge est un équipement d'accès intégré (IAD) compatible ADSL 2/2+. Avec une vitesse descendante pouvant atteindre 12 Mbit/s (ADSL2) ou 24 Mbit/s (ADSL2+), le routeur Vigor2700e/2700Ge fournit une bande passante exceptionnelle pour l'accès à l'internet.

Pour sécuriser votre réseau, le routeur Vigor est doté de fonctions de pare-feu avancées, comme le filtrage adaptatif (SPI) pour détecter et bloquer les paquets malveillants ou parer les attaques de type « déni de service » (DoS), le filtrage web configurable par l'utilisateur pour le contrôle parental de l'accès à l'internet, etc.

Le modèle Vigor2700Ge comportent une interface sans fil compatible 802.11g pour l'accès avec LAN sans fil avec un débit pouvant atteindre 54 Mbit/s. Pour garantir la confidentialité des communications sans fil, le modèle Vigor2700Ge peut soumettre toutes les données transmises à un cryptage WEP standard ou à un cryptage WPA2 (IEEE 802.11i) de classe industrielle. Les autres fonctionnalités sont la liste des clients sans fil et le contrôle d'adresse MAC pour contrôler l'habilitation des utilisateurs au sein de votre réseau et le SSID masqué pour être à l'abri des scrutations d'intrus extérieurs.

1.1 Voyants lumineux, prises et interfaces

1.1.1 Vues avant et arrière du Vigor2700e

Pour Vigor2700Ge					
		ADSL2+	LAN		ADSL2/2+ Router
		🔘 Link	1 :	3	
	⊖ WLAN	🔘 Data	2 4	4	

Pour Vigor2700e

	ADSL2+	LA	N	ADSL2/2+ Router
⊖ ACT	🔘 Link	1	3	
	🔘 Data	2	4	

Voyant	État	Explication
ACT	Clignotant	Le routeur est allumé et fonctionne correctement.
(Activité)	Allumé	Le routeur est allumé
WLAN	Allumé	Le point d'accès sans fil est prêt.
	Clignotant	Des paquets Ethernet sont en cours de transmission sur le LAN sans fil.
	Éteint	La fonction LAN sans fil est inactive.
ADSL2+	Allumé	La ligne ADSL est en service.
	Clignotant	Dialogue initial en cours.
ADSL2+	Clignotant	Données en cours de transmission.

LAN (1, 2, 3, 4)	Vert	Une connexion normale est établie sur le port correspondant.
	Clignotant	Des paquets Ethernet sont en cours de transmission.

1.1.2 Vue arrière du Vigor2700Ge

Pour Vigor2700Ge



Pour Vigor2700e



Interface	Description
ADSL 2+	Branchement de la ligne ADSL2/2+ pour accéder à l'internet.
LAN 4 – 1	Branchement des équipements du réseau local.
Factory Reset	Rétablissement des paramètres par défaut. Utilisation : Allumez le routeur (le voyant ACT clignote), appuyez sur le bouton en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant ACT commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec la configuration par défaut.
ON/OFF	Interrupteur marche-arrêt.
PWR	Prise pour un adaptateur secteur 7 à 7.5V DC.

1.2 Installation du matériel

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

- 1. Reliez la prise ADSL au coupleur ADSL externe avec un câble ADSL.
- 2. Reliez l'un des ports du commutateur 4 ports à votre ordinateur avec un câble RJ-45. Vous pouvez relier directement 4 PC à ce routeur.
- 3. Enfoncez la fiche du câble d'alimentation dans la prise PWR du routeur et branchez l'autre extrémité sur la prise de courant secteur.
- 4. Allumez le routeur.
- 5. Vérifiez l'état des voyants ACT, ADSL2+ et LAN.

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



Page laissée intentionnellement vierge .

2 Configuration de base

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

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

2.1 Changement de mot de passe

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

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

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

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

Mot de pa	sse réseau		<u>?</u> ×		
<u> (</u>	Tapez votre nom d'utilisateur et votre mot de passe.				
1	Site :	192.168.1.1			
	Domaine	Login to the Router Web Configurator			
	<u>N</u> om d'utilisate	ur			
	<u>M</u> ot de passe		-		
	Enregistrer	ce mot de passe dans votre liste de mots de pa	asse		
		OK Ann	uler		
	Enregistrer	ce mot de passe dans votre liste de mots de pa OK Annu	asse uler		

3. L'écran principal apparaît.

Vigor270	DO Series	(\bigcirc)		Dray T www.draytek.	ek ^{com}
Assistant de démarrage rapide État en ligne	État du système Nom de modèle	: Vigor2700 series			
Accès à l'internet LAN NAT Pare-feu	Date/Heure de création ADSL Firmware Version	: Dec 28 2006 10:02:11 : 121201_A Annex A			
Gestion de la bande passante Applications LAN sans fil Maintenance du système Diagnostics	LAN Adresse MAC : 00-5 Ire adresse IP : 192. Premier masque de sous-réseau : 255. Serveur DHCP : Oui	0-7F-01-53-BB 168.1.1 255.255.0	WAN État de la connexion Adresse MAC Connexion Adresse IP Passerelle par défaut DNS	: Disconnected : 00-50-7F-01-53-BC : : : : 194.109.6.66	
Tous droits réservés.			LAN sans fil Adresse MAC Domaine de fréquence Version du firmware	: 00-50-7f-01-53-bb : Europe : 1.0.4.0	
	<				~

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

Maintenance du système >> Configuration du mot de passe administrateur

Ancien mot de passe	
Nouveau mot de passe	
Retapez le nouveau mot de passe	

- 5. Entrez le mot de passe de connexion (rien par défaut) dans le champ **Ancien mot de passe**. Tapez un nouveau mot de passe dans le champ **Nouveau mot de passe** et retapez-le dans le champ **Confirmer le nouveau mot de passe**. Puis cliquez sur **Suivant** pour continuer.
- 6. La prochaine fois, utilisez le nouveau mot de passe pour accéder au configurateur web pour ce routeur.

Connect to 192.168.1.1 ? 🔀
Login to the Router Web Configurator
User name:
Password: ••••
Remember my password
OK Cancel

2.2 Assistant de démarrage rapide

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

ssistant de demarrage rapide	
. Tapez le mot de passe	
Veuillez saisir une chaine de cara mot de passe (23 caractères m	actères alphanumériques pour votre naximum).
Nouveau mot de passe	
Confirmer le mot de passe	
	< Précédent Suivant > Terminer Annulei

2.2.1 Choix du type de protocole/encapsulation

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

Assis	tant de démarrage rapide				
2. Co	nnexion à l'internet				
	VPI VCI	0 33	Détection autor	matique	
	Protocole / Encapsulation	PPPoE LLC/SNAF	v		
	Adr IP fixe Adresse IP Masque de sous-réseau Passerelle par défaut DNS primaire DNS secondaire	Oui Oui Non(IF	9 Dynamique)		
		< Retour	Suivant >	Terminer	Annuler

Il vous faut maintenant choisir un type de connexion WAN approprié pour vous connecter à l'internet par l'intermédiaire de ce routeur selon les paramètres que votre FAI vous a fournis.

VPI

Virtual Path Identifier (identificateur de conduit virtuel). C'est un champ de 8 bits dans l'en-tête de chaque cellule ATM. Il indique où la cellule doit être routée. L'ATM est une méthode de transmission de données par petits paquets de taille fixe. Elle sert à transférer des données à des ordinateurs clients.

Adr IP fixe	Cliquez sur Oui pour spécifier une adresse IP fixe pour le routeur. Sinon, cliquez sur Non (Adr IP dynamique) pour permettre au routeur de choisir une adresse IP dynamique. Si vous choisissez Non , l'adresse IP, le masque de sous-réseau et la passerelle par défaut suivants ne seront pas modifiés.
Adresse IP	Spécifiez une adresse IP pour le protocole choisi.
Masque de sous-réseau	Spécifiez un masque de sous-réseau pour le protocole IP routé ou IP ponté.
Passerelle par défaut	Spécifiez une adresse IP de passerelle pour le protocole IP routé ou IP ponté.
DNS primaire	Spécifiez une adresse IP pour le DNS primaire.
DNS secondaire	Spécifiez une adresse IP pour le DNS secondaire.

2.2.2 PPPoE/PPPoA

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

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

Si votre FAI vous fournit la connexion PPPoE ou PPPoA, choisissez PPPoE ou PPPoA pour ce routeur. La page suivante apparaît: Assistant de démarrage rapide

Nom du fournisseur d'accès	
Nom d'utilisateur	
Mot de passe	
Confirmer le mot de passe	
🔲 Toujours actif	
Délai d'inactivité	180 Secondes

Nom du FAI Tapez un nom spécifique propre à votre FAI. Nom d'utilisateur Tapez un nom d'utilisateur (identifiant) valable fourni par votre FAI. Mot de passe Tapez un mot de passe valable fourni par votre FAI.

Confirmer le mot de passe	Retapez le mot de passe.
Connexion permanente	Cochez cette case pour que le routeur reste connecté en permanence à l'internet.
Délai d'inactivité	Tapez le délai (en secondes) au bout duquel la connexion internet sera coupée en l'absence d'activité.

Cliquez sur Suivant. La page suivante apparaît.

Assistant de démarrage rapide

4. Me	erci de valider vos paramètres:	
	VPI VCI Protocole / Encapsulation Adr IP fixe DNS primaire DNS secondaire Toujours actif Délai d'inactivité	: 8 : 35 : PPPoE / LLC : Non : : Non : 180 Secondes
1		< Retour Suivant > Terminer Annuler

Cliquez sur Terminer. La page État en ligne propre à ce protocole apparaît.

État du systè	me				Sys	stème	démarré	depuis: 2:27:58
État LAN		DNS	primaire: 16	8.95.192.1		DNS se	condaire	: 168.95.1.1
Adresse IP		Paquets	TX Pa	quets RX				
192,168,1,1		9071	169	945				
État WAN			Adresse I passerelle	P 61.230.1	92.254			Drop PPPoE
Mode	Adresse	IP	Paquets TX	Vitesse TX	Paquets	s RX	Vitesse RX	Temps actif
PPPoE	61.230.20	02.155	159	1023	97		390	0:00:31
Information	ADSL	(version du	firmware ADSL	.: 121201_	_A)			
Statistiques ATM	s Bloc	s TX	Blocs RX		Blocs cor	rigés	Blocs	non corrigés
	3252	37670	577675847	7	0		0	
État ADSL	Mode G.DMT	<mark>État</mark> SHOWTIN	V mont 1E 256000	ante Vic 204	lescend. 48000	Marg 31	ge RSB	Aff. boucle 26

2.2.3 IP ponté

Choisissez **IP ponté 1483** comme protocole. Tapez toutes les informations que votre FAI vous a fournies pour ce protocole.

Assistant de démarrage rapide

VPI	0 Détection automatique
YCI Protocole / Encapsulation	LLC IP en pont 1483
Adr IP fixe	⊙ Oui
Adresse IP	172.16.3.222
Masque de sous-réseau	255.255.0.0
Passerelle par défaut	
DNS primaire	
DNS secondaire	

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

Assistant de démarrage rapide

4. Merci de valider vos paramètres	s:
VPI VCI Protocole / Encapsulation Adr IP fixe DNS primaire DNS secondaire	: 8 : 35 : 1483 Bridge LLC : Non :
	<pre>< Retour Suivant > Terminer Annuler</pre>

Cliquez sur **Terminer.** La page État en ligne propre à ce protocole apparaît.

État du systè	me				Sys	tème	démarré (depuis: 2:27:58
État LAN		DNS	primaire: 168	8.95.192.1		DNS se	econdaire	168.95.1.1
Adresse IP		Paquets	rx Paq	uets RX				
192.168.1.1		194	215					
État WAN			Adresse IF passerelle	202.211	.100.1			Renouveler
Mode	Adresse	IP	Paquets TX	Vitesse TX	Paquets	RX	Vitesse RX	Temps actif
DHCP Client	202.211.	100.54	159	1023	97		390	0:00:31
Information #	DSL	(version du	firmware ADSL	: 121201	_A)			
Statistiques	Blocs	5 TX	Blocs RX		Blocs cor	rigés	Blocs	non corrigés
	23		42	I	D		157	
État ADSL	Mode	État	V monta	ante Vo	lescend.	Mar	ge RSB	Aff. boucle
	G.DMT	SHOWTIM	1E 256000	20	48000	31		26

2.2.4 IP routé

Choisissez **IP routé 1483** comme protocole. Tapez toutes les informations que votre FAI vous a fournies pour ce protocole.

nnexion à l'internet	
VPI	D Détection automatique
VCI	34
Protocole / Encapsulation	LLC IP routé 1483
Adr IP fixe	💿 Oui Non(IP Dynamique)
Adresse IP	172.16.3.152
Masque de sous-réseau	255.255.0.0
Passerelle par défaut	
DNS primaire	
DNS secondaire	

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

Assistant de démarrage rapide

4.	Merci de valider vos paramètres	:
	VPI VCI Protocole / Encapsulation Adr IP fixe Adresse IP Masque de sous-réseau Passerelle par défaut DNS primaire DNS secondaire	: 0 : 34 : 1483 Route LLC : Oui : 172.16.3.152 : 255.255.0.0 : :
		< Retour Suivant > Terminer Annuler

Cliquez sur Terminer. La page État en ligne propre à ce protocole apparaît.

État LAN		DNS	primaire: 168	.95.192.1	D	NS se	econdaire	: 168.95.1.1
Adresse IP		Paquets [•]	FX Paq	uets RX				
192,168,1,1		137	191					
État WAN			Adresse IP passerelle:	61.230.1	.92.254			
Mode	Adresse	IP	Paquets TX	Vitesse TX	Paquets	RX	Vitesse RX	Temps actif
Static IP	202.211.1	00.54	26	36	0		0	0:00:35
Information a	ADSL (version du	firmware ADSL:	121201_	_A)			
Statistiques	5 Blocs	тх	Blocs RX		Blocs corri	igés	Blocs	non corrigé
	0		0		0		1	
État ADSL	Mode	État	V monta	inte Vic	lescend.	Mar	qe RSB	Aff. boucle
	ADSI 2±	SHOWTIN	IE 992000	24	168000	5		0

2.3 État en ligne propre à chaque protocole

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

État en ligne pour PPPoA/PPPoE

État en ligne

État du systè	me				Sys	stème c	lémarré	depuis: 2:27:5
État LAN		DNS	primaire: 16	3.95.192.1		DNS se	condaire	: 168.95.1.1
Adresse IP		Paquets 1	TX Pa	quets RX				
192.168.1.1		9071	169	45				
État WAN			Adresse II passerelle	61.230.1	.92.254			Drop PPPoE
Mode	Adresse	IP	Paquets TX	Vitesse TX	Paquets	RX	Vitesse RX	Temps actif
PPPoE	61.230.20	02.155	159	1023	97		390	0:00:31
Information /	ADSL	(version du	firmware ADSL	: 121201	_A)			
Statistiques ATM	Blocs	s TX	Blocs RX		Blocs cor	rigés	Blocs	non corrigés
	3252	37670	577675847	,	0		0	
État ADSL	Mode	État	V monta	ante Vo	lescend.	Marg	je RSB	Aff. boucle

État en ligne pour IP ponté

État en ligne

État du systè	me					Système	e démarré	depuis: 2:27:58
État LAN		DNS	primaire:	168.95.1	92.1	DNS s	econdaire	: 168.95.1.1
Adresse IP		Paquets	тх	Paquets	RX			
192.168.1.1		194		215				
État WAN			Adress passer	e IP elle: ²⁰²	211.100.1			Renouveler
Mode	Adresse	IP	Paquets T	x <mark>Vite</mark> TX	sse Paq	uets RX	Vitesse RX	Temps actif
DHCP Client	202.211.	100.54	159	1023	97		390	0:00:31
Information A	ADSL	(version du	firmware A	DSL: 121	201_A)			
Statistiques	Blocs	тх	Blocs I	RX	Blocs	corrigés	Blocs	non corrigés
	23		42		0		157	
État ADSL	Mode G.DMT	<mark>État</mark> SHOWTI	V mo 4E 2560	ontante 100	V desce 2048000	nd. Ma 31	rge RSB	Aff. boucle 26

État en ligne pour IP routé

État du systè	eme				Sys	tème di	émarré d	lepuis: 2:27:58
État LAN Adresse IP		DNS Paquets T	primaire: 168 X Pac	3.95.192.1 Juets RX	E	ONS sec	ondaire	168.95.1.1
192.168.1.1		137	191					
État WAN			Adresse II passerelle	61.230.1	92.254			
Mode	Adresse	IP	Paquets TX	Vitesse TX	Paquets	RX R	itesse X	Temps actif
Static IP	202.211.1	.00.54	26	36	0	C)	0:00:35
Information	ADSL	(version du	firmware ADSL	: 121201_	_A)			
Statistique: ATM	s Blocs	тх	Blocs RX		Blocs corr	igés	Blocs	non corrigés
	0		0		0		1	
État ADSL	Mode	État	V monta	ante Vo	lescend.	Marqe	e RSB	Aff. boucle
	ADSL2+	SHOWTIM	E 992000	24:	168000	5		0

DNS primaire	Affiche l'adresse IP du DNS primaire.
DNS secondaire	Affiche l'adresse IP du DNS secondaire.
Adresse IP (dans LAN)	Affiche l'adresse IP de l'interface LAN.
Paquets TX	Affiche le nombre total de paquets émis au niveau de l'interface LAN.
Paquets RX	Affiche le nombre total de paquets reçus au niveau de l'interface LAN.
Adresse IP passerelle	Affiche l'adresse IP de la passerelle par défaut.
Adresse IP (dans WAN)	Affiche l'adresse IP de l'interface WAN.
Vitesse TX	Affiche la vitesse d'émission des paquets au niveau de l'interface WAN.
Vitesse RX	Affiche la vitesse de réception des paquets au niveau de WAN interface.
Temps actif	Affiche le temps total de connexion de l'interface.
Information ADSL	Affiche la version du firmware du routeur.

2.4 Barre d'état

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

État: Prêt

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

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

Page laissée intentionnellement vierge.

3 Configuration web avancé

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

3.1 Accès à l'internet

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

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

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

Adresse IP publique et adresse IP privée

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

Comment obtenir une adresse IP publique de votre FAI

Pour obtenir une adresse IP publique de votre FAI pour le routeur Vigor en tant qu'équipement d'installation d'usager (CPE), il existe trois protocoles courants : le protocole point à point sur Ethernet (**PPPoE**), le protocole point à point sur couche d'adaptation à l'ATM 5 (**PPPoA**) et le multiprotocole sur ATM (**MpoA**). Le protocole **multi-PVC** est fourni pour une configuration plus évoluée.

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

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

Votre adresse IP, votre serveur DNS et autres informations sont généralement fournies par votre FAI

3.1.2 PPPoE/PPPoA

Le protocole PPPoA, inclus dans RFC 1483, peut être mis en œuvre en mode encapsulation LLC-SNAP (commande logique de liaison – protocole d'accès à un sous-réseau) ou en mode multiplexage par circuits virtuels. En tant qu'équipement d'installation d'usager (CPE), le routeur Vigor encapsule la session PPP pour son transport sur la boucle ADSL jusqu'au multiplexeur d'accès DSL (DSLAM) de votre FAI.

Vous pouvez choisir PPPoE ou PPPoA comme protocole d'accès à l'internet à partir du menu **Accès à l'internet**. La page web suivante apparaît.

Accès à l'internet >> PPPoE / PPPoA

Client PPPoE/PPPo	Activer	Configuration de l'accès au FAI			
 Désactiver 		Nom du FAI			
Paramètres du mo	dem DSL	Nom d'utilisateur			
Canal multi-PVC	Canal 1 💌	Mot de passe			
VPI	8	Authentification PPP PAP ou CHAP	*		
VCI	35	🗖 Toujours actif			
Type d'encapsulatio	n	Délai d'inactivité 180 sec	conde(s)		
Type d'encapsulation VC MUX Protocole PPPoA Modulation Multimode Mode pass-through PPPoE Pour LAN filaire Remarque: si l'une de ces options est activée lors de l'utilisation du protocole PPPoA, alors le routeur se comportera comme un modem qui servira uniquement les clients PPPoE du LAN		Adresse IP fournie par le FAI Alias de l'IP du WAN Adr IP fixe Oui Oui Non (IP dynamique) Adresse IP fixe Oui Adresse MAC par défaut Spécifier une adresse MAC Adresse MAC: 00.50.7F:87.14.79 Index(1-15) dans Horaire Configuration: , , , , ,			

Client PPPoE/PPPoA	Cliquez sur Activer pour activer cette fonction. Si vous cliquez sur Désactiver , vous perdrez tous les paramètres que vous avez définis dans cette page.
Paramètres du modem DSL	Configurez les paramètres DSL selon les informations fournies par votre FAI. Ils sont essentiels pour établir la connexion DSL à votre FAI. Canal multi-PVC – Les sélections affichées ici sont déterminées par la page Accès à l'internet – Multi-PVC . Sélectionner le canal M-PVC signifie qu'il n'est pas fait de choix. VPI – Tapez la valeur fournie par le FAI. VCI - Tapez la valeur fournie par le FAI. VCI - Tapez la valeur fournie par le FAI. VCI - Tapez la valeur fournie par le FAI. Type d'encapsulation – Déroulez la liste pour choisir le type d'encapsulation indiqué par le FAI. Protocole – Déroulez la liste pour choisir celui indiqué par le FAI. Si vous avez déjà utilisé l' assistant de démarrage rapide pour

	définir le protocole, il n'y a rien à changer dans cette zone.
PPPoE Pass-through	Le routeur offre une connexion commutée PPPoE. En outre, vous pouvez établir la connexion PPPoE directement entre des clients locaux et votre FAI par l'intermédiaire du routeur Vigor. Pour LAN filaire – Si vous cochez cette case, les PC du même réseau pourront utiliser d'autres sessions PPPoE (différentes de celle du PC hôte) pour accéder à l'internet. Pour LAN sans fil – Si vous cochez cette case, les PC du même réseau pourront, via une connexion sans fil, utiliser d'autres sessions PPPoE (différentes de celle du PC hôte) pour accéder à l'internet.
Configuration de l'accès au FAI	 Entrez le nom d'utilisateur, le mot de passe et les paramètres d'authentification qui vous ont été fournis par votre FAI. Si vous voulez rester connecté à l'internet en permanence, vous pouvez cocher Connexion permanente Nom du FAI – Tapez dans ce champ le nom que vous a fourni le FAI. Nom d'utilisateur – Tapez l'identifiant que vous a fourni le FAI. Mot de passe – Tapez le mot de passe que vous a fourni le FAI. Authentification PPP– Sélectionnez PAP seulement ou PAP ou CHAP pour PPP. Connexion permanente – Cochez cette case si vous voulez que le routeur reste connecté à l'internet en permanence. Délai d'inactivité – Spécifiez le délai en secondes au bout duquel la connexion internet sera coupée en l'absence d'activité.
Adresse IP fournie par le FAI	D'une manière générale, le FAI vous attribue dynamiquement une adresse IP chaque fois que vous vous connectez et que vous demandez une adresse IP. Dans certains cas, votre FAI vous attribue la même adresse IP chaque fois que vous en demandez une. Dans ce cas, vous pouvez taper cette adresse IP dans le champ Adresse IP fixe. Contactez votre FAI avant d'utiliser cette fonction. IP fixe– Cliquez sur Oui pour utiliser cette fonction et tapez une adresse IP fixe dans le champ Adresse IP fixe. Alias IP WAN - Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction Alias IP WAN . Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement.
	🗿 http://192.168.1.1 - Alias de lTP du WAN - Microsoft Internet Ex 🔳 🗖 🔀
	Alias de l'IP du WAN (multi-NAT) Index Activer Adresse IP WAN aux. Joindre le pool IP NAT 1. v v 2.

Si vous cochez **Joindre le pool IP NAT**, les données provenant des hôtes NAT sont transmises cycliquement session par session.



Si vous ne cochez pas **Joindre le pool IP NAT**, vous pouvez néanmoins utiliser ces adresses IP publiques à d'autres fins : hôte DMZ, ouverture de ports.



Adresse MAC par défaut	Tapez l'adresse MAC du routeur dans les champs. Vous pouvez utiliser l'adresse MAC par défaut ou spécifier une autre adresse MAC. Adresse MAC – Tapez l'adresse MAC du routeur dans les champs.
Plages horaires (1-15)	Vous pouvez spécifier quatre plages horaire définies précédemment dans la page web Applications – Plages horaire en tapant les numéros d'index correspondants.

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

3.1.3 MPoA

Le protocole MPoA permet d'intégrer les services ATM aux LAN existants utilisant le protocole Ethernet, Token Ring ou TCP/IP. Le but de MPoA est de permettre à des LAN différents d'échanger des paquets par l'intermédiaire d'une dorsale ATM.

Pour utiliser **MPoA** comme protocole d'accès à l'internet, choisissez l'option **MPoA** du menu **Accès à l'internet**. La page web suivante apparaît.

MPoA (RFC1483/	2684)	Paramètres de réseau IP WAN	
	💿 Activer 🔘 Désactiver	Obtenir une adresse IP automatiquem	ent
Paramètres du m Capal multi-PVC	Canal 2	Nom du routeur* Nom de domaine	*
Encapsulation	C IP en pont 1483	Spécifier une adresse IP Alias de l'IP du WAN	
VPI VCI Modulation Protocole RIP	8 36 Multimode	Adresse IP 0.0.0.0 Masque de sous-réseau 0.0.0.0 Adresse IP de la passerelle]]]
Mode Pont	e pont	 * : Nécessaire pour certains FAI Adresse MAC par défaut Spécifier une adresse MAC Adresse MAC : 00 · 50 · 7F :87 · 14 · 79 Adresse IP du serveur DNS Adresse IP primaire Adresse IP secondaire]

Accès à l'internet >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Cliquez sur Activer pour activer cette fonction. Si vous cliquez sur Désactiver, vous perdrez tous les paramètres que vous avez définis dans cette page.

OK

Paramètres du modem DSL	Configurez les paramètres DSL selon les informations fournies par votre FAI. Ils sont essentiels pour établir la connexion DSL à votre FAI. Canal multi-PVC – Les sélections affichées ici sont déterminées par la page Accès à l'internet – Multi-PVC. Sélectionner le canal M-PVC signifie qu'il n'est pas fait de choix. Type d'encapsulation – Déroulez la liste pour choisir le type d'encapsulation indiqué par le FAI. VPI – Tapez la valeur fournie par le FAI. VCI - Tapez la valeur fournie par le FAI.
Protocole RIP	Le protocole d'information de routage ou RIP (RFC1058) définit comment les routeurs échangent les informations des tables de routage. Cliquez sur Activer RIP pour activer cette fonction.
Mode pont	Si vous choisissez IP ponté comme protocole, vous pouvez cocher cette case. Le routeur fonctionnera comme un modem en pont.

Paramètres de réseau IP WAN

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

Obtenir une adresse IP automatiquement – Cliquez sur ce bouton pour obtenir l'adresse IP automatiquement. **Nom de routeur** – Tapez le nom de routeur fourni par le FAI.

Nom de domaine – Tapez le nom de domaine qui vous a été attribué.

Alias IP WAN - Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction Alias IP WAN. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement



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

	Adresse IP– Tapez l'adresse IP privée. Masque de sous-réseau – Tapez le masque de sous-réseau. Adresse IP de la passerelle – Tapez l'adresse IP de la passerelle.
Adresse MAC par défaut	Tapez l'adresse MAC du routeur dans les champs. Vous pouvez utiliser l'adresse MAC par défaut ou spécifier une autre adresse MAC. Adresse MAC – Tapez l'adresse MAC du routeur dans les champs.
Adresse IP du serveur DNS	Tapez l'adresse IP primaire du routeur. Au besoin, tapez une adresse IP secondaire qui pourra être nécessaire ultérieurement.

Quand vous avez terminé de définir tous les paramètres, cliquez sur OK pour les activer.

3.1.4 Multi-PVC

Ce routeur vous permet de créer des multi-PVC. Pour cela, choisissez l'option **Paramétrage de multi-PVC** du menu **Accès à l'internet**.

```
Accès à l'internet >> Multi-PVC
```

 14.1	nu	0	

Général	QoS A1	ſM	Mode po	nt (port	-ba	sed)	
Canal	Activer	VPI	VCI	Type Qos	de S	Protocole	Encapsulation
1.		8	35	UBR	*	PPP0A 🔽	VC MUX 💌
2.		8	36	UBR	~	MPoA 🔽	1483 Bridged IP LLC 💌
з.		8	37	UBR	~	PPPoA 🔽	VC MUX
4.		8	38	UBR	~	PPPoA 🔽	VC MUX
5.		8	39	UBR	~	PPPoA 🔽	VC MUX
6.		8	40	UBR	~	PPPoA 🔽	VC MUX
7.		8	41	UBR	~	PPPoA 🔽	VC MUX
8.		8	42	UBR	~	PPPoA 🔽	VC MUX

Remarque: VPI/VCI doit être unique pour chaque canal.

OK	Effacer	Annuler

Activer	Cochez cette case pour activer le canal correspondant. Les canaux que vous activez ici apparaîtront dans la liste déroulante Canal multi-PVC de la page web Accès à l'internet . Vous pouvez activer ici huit canaux mais vous ne pouvez en choisir qu'un seul sur la page web Accès à l'internet
VPI	Tapez la valeur fournie par votre FAI.
VCI	Tapez la valeur fournie par votre FAI.
Type de QoS	Choisissez un type de QoS approprié pour le canal. Type de QoS UBR UBR CBR ABR nrtVBR rtVBR
Protocol	Choisissez un protocole approprié pour le canal. PPPoE PPPoE MPoA

Encapsulation

Choisissez un type d'encapsulation approprié pour le canal. Le type d'encapsulation varie selon le protocole.

	1483 Route IP LLC	*
	1483 Bridged IP LLC	
	1483 Route IP LLC	
VC MUX 🛛 🚩	1483 Bridged IP VC-Mux	
VC MUX	1483 Routed IP VC-Mux(IPoA)	
LLC/SNAP	1483 Bridged IP(IPoE)	

3.2 Réseau local (LAN)

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

3.2.1 Principes du réseau local

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



V

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



Protocole d'information de routage (RIP)

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

Routes statiques

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

LAN virtuels

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



3.2.2 Configuration générale

Cette page comporte les paramètres généraux du LAN.

Cliquez sur LAN pour ouvrir la page de configuration du LAN et choisissez Configuration générale.

Configuration du rés	eau IP LAN	Configuration du serve	ur DHCP
?usage NAT		💿 Activer le serveur 🔘 🛛	Désactiver le serveur
1re Adresse IP	192.168.1.1	Agent relais:	
1re Masque de sou	is-réseau	🔵 1re sous-réseau 🔾 2e	: sous-réseau
	255.255.255.0	Adresse IP de début	192.168.1.10
Utilisation du routage	IP 🔘 Activer 💿 Désactiver	nbr d'adresses du récorvoir ID	50
2e adresse IP	192.168.2.1	Adresse IP de la passerel	le
2e masque de sous·	-réseau		192.168.1.1
	255.255.255.0	Adresse IP du serveur DH	ICP pour agent relais
2e servi	eur DHCP de sous-réseau		
Contrôle de protocole	RIP Désactiver 💌	Adresse IP du serveur l	DNS
		Adresse IP primaire	
		Adresse IP secondaire	

ΟK

1 ^{re} adresse IP	Adresse IP privée permettant de se connecter à un réseau local (valeur par défaut : 192.168.1.1).
1 ^{er} masque de sous-réseau	Code d'adresse qui détermine la taille du réseau (valeur par défaut : 255.255.255.0/24)
Pour routage IP	Cliquer sur Activer pour activer cette fonction. Par défaut, cette fonction est désactivée .
2 ^e adresse IP	Adresse IP secondaire permettant de se connecter à un sous-réseau (valeur par défaut : 192.168.2.1/24)
2 ^e masque de sous-réseau	Code d'adresse qui détermine la taille du réseau. (valeur par défaut : 255.255.255.0/24)
2 ^e serveur DHCP	Vous pouvez configurer le routeur pour qu'il serve de serveur DHCP pour le deuxième sous-réseau.

LAN >> Paramètre général

Adresse IP de démarrage
Nombre d'IP dans le 0 (10 maxi) réservoir
Index Adresse MAC correspondante Adresse IP donné
Adresse MAC : : : : : : : : : : : : : : : : : : :
 OK Effacer tout Fermer

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

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

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

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

Contrôle de protocole RIF	Désactiver 🛛 🔽
	Désactiver
	1re sous-réseau
	2e sous-réseau

 1^{er} sous-réseau - Sélection du routeur pour modifier les informations RIP du 1^{er} sous-réseau avec information des routeurs voisins. 2^e sous-réseau - Sélection du routeur pour modifier les informations RIP du 2^e sous-réseau avec information des routeurs voisins.

Configuration du
serveur DHCPLe 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 transmet automatiquement les paramètres IP à tout utilisateur local configuré en client DHCP. Il est vivement recommandé de laisser le routeur configuré en serveur DHCP en l'absence de serveur DHCP dans votre réseau.

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

Activer le serveur - Le routeur attribue automatiquement une adresse IP à tous les hôtes du réseau local.

Désactiver le serveur – Vous attribuez manuellement une adresse IP à tous les hôtes du réseau local.

Agent relais – $(1^{er} \text{ sous-réseau}/2^e \text{ sous-réseau})$ Spécifiez le sous-réseau où se trouve le serveur DHCP vers lequel l'agent relais doit rediriger la requête DHCP.

Adresse IP de début - Tapez une valeur du pool d'adresses IP pour définir le début de la plage d'adresses IP qu'attribuera le serveur DHCP. Si la 1^e adresse de votre routeur est 192.168.1.1, l'adresse IP de début doit être égale ou supérieure à 192.168.1.2 mais inférieure à 192.168.1.254.

Nombre d'adresses du pool IP - Tapez le nombre maximum de PC auquel le serveur DHCP doit attribuer une adresse IP. La valeur par défaut est 50 et la valeur maximale est 253.

Adresse IP de la passerelle - Tapez l'adresse IP de passerelle pour le serveur DHCP. Cette adresse est généralement la même que la 1^{re} adresse IP du routeur, ce qui veut dire que le routeur est la passerelle par défaut.

Adresse IP du serveur DHCP pour l'agent relais - Spécifiez l'adresse IP du serveur DHCP que vous allez utiliser pour que l'agent relais aide à transmettre la requête DHCP au serveur DHCP.

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

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

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

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

État du système			Système démarré depuis: 0:22:3
État LAN	DNS prima	aire: 194.109.6.66	DNS secondaire: 194.98.0.1
Adresse IP	Paquets TX	Paquets RX	
192.168.1.1	1048	3587	

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

Configuration du serveur DNS

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

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

3.2.3 Route statique

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

LAN >> Configuration de route statique

onfiguration de route statique			Afficher la table de routa		
Index	Adresse de destination	État	Index	Adresse de destination	État
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?

État: v --- Actif, x --- Inactif, ? --- Vide

Index	Le numéro d'index (1 à 10) vous permet de configurer une route statique.
Adresse de destination	Adresse de destination de la route statique.
État	État de la route statique.
Afficher la table de routage	Affiche la table de routage.

Diagnostics >> Afficher la table de routage



Ajout de routeurs statiques à des réseaux privés et publics

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

- utilisez le routeur principal pour naviguer sur l'internet.
- créez un sous-réseau privé 192.168.10.0 à l'aide d'un routeur interne A (192.168.1.2)
- créez un sous-réseau public 211.100.88.0 à l'aide d'un routeur interne B (192.168.1.3).

• vous avez configuré le routeur principal 192.168.1.1 comme passerelle par défaut pour le routeur A 192.168.1.2.

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



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

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

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

ndex nº	1	
	État/Action	Active/Ajouter 🗠
	Adresse IP de destination	192.168.10.0
	Masque de sous-réseau	255.255.255.0
	Adresse IP de la passerelle	192.168.1.2
	Interface réseau	LAN 🐱

3. Retournez à la page de **Configuration de route statique**. Cliquez sur un autre **Index n**° pour ajouter une autre route statique comme indiqué ci-dessous ; tous les paquets destinés à 211.100.88.0 seront transmis à 192.168.1.2.

LAN >> Configuration de routes statique

Diagnostics >> Afficher la table de routage

État/Action	Active/Ajouter
Adresse IP de destination	211.100.88.0
Masque de sous-réseau	255.255.255.0
Adresse IP de la passerelle	192.168.1.3
Interface réseau	LAN 🐱

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

Key: C	- connected, S -	static, R - RIP, * - default, ~ - private	
C~	192.168.1.0/	255.255.255.0 is directly connected, IFO	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3, IFO	

Désactivation de route statique

- 1. Cliquez sur le numéro d'index que vous voulez désactiver dans la page de configuration de route statique.
- 2. Sélectionnez l'option **Inactive/Désactiver** du menu déroulant, puis cliquez sur le bouton **OK** pour désactiver la route.

ndex nº 1		
É	itat/Action	Active/Ajouter 😪
A	dresse IP de destination	Vider/Effacer Active/Ajouter
N	1asque de sous-réseau	Inactive/Désactiver
A	dresse IP de la passerelle	192.168.1.3
I	nterface réseau	LAN 🛩

3.2.4 VLAN

La fonction LAN virtuel vous permet de gérer commodément les hôtes en les groupant dans le port physique. Vous pouvez également gérer le débit d'entrée/sortie de chaque port. Sélectionnez l'option **VLAN** du menu **LAN**. La page suivante apparaît. Cliquez sur **Activer** pour activer la fonction VLAN.

LAN >> Configuration de VLAN

🗹 Activer				
	P1	P2	P3	P4
VLANO				
VLAN1				
VLAN2				
VLAN3				

Pour ajouter or supprimer un VLAN, procédez comme indiqué ci-après.

1. On suppose que VLAN 0 est constitué par les hôtes reliés à P1 et à P2 et que VLAN 1 est constitué par les hôtes reliés à P3 et à P4.



LAN >> Configuration de VLAN

2. Après avoir coché la case pour activer la fonction VLAN, cochez les cases appropriées du tableau.

🗸 Activer				
	P1	P2	P3	P4
VLANO		 Image: A start of the start of		
VLAN1				
VLAN2				
VLAN3				

- 3. Pour désactiver la fonction VLAN, décochez la case Activer et cliquez sur OK pour sauvegarder.
- 4. Cette fonction sert à lier les adresses IP-MAC au sein du LAN pour contrôler plus étroitement le réseau. Lorsque cette fonction est activée, il est impossible de modifier les adresses IP et MAC liées. Si vous modifiez l'adresse IP ou l'adresse MAC, vous risquez de ne plus pouvoir accéder à l'internet.
5. Cliquez sur LAN, puis sur Association IP-MAC pour ouvrir la page de configuration

Association IP - MAC Remarque: L'association IP-MAC prévaut sur les allocations DHCP. Dans le mode « associée uniquement », seule les IP associées à une adresse MAC auront accès à Internet ⊙ Activer ○ Désactiver ○ Associée uniquement Table ARP Liste des IP associées <u>Tout sélectionner | Trier</u> <u> Tout sélectionner</u> | <u>Trier</u> | <u>Rafraichir</u> Index Adresse IP Adresse MAC Adresse IP 192.168.1.10 Adresse MAC 00-0E-A6-2A-D5-A1 Ajouter et éditer Adresse IP Adresse MAC Ajouter Éditer supprimer

ΟK

Activer	Cliquez sur ce bouton d'option pour activer la fonction. Les adresses IP/MAC qui ne figurent pas dans la liste des liens IP-MAC pourront, elles aussi, se connecter à l'internet.
Désactiver	Cliquez sur ce bouton d'option pour désactiver la fonction. Tous les paramètres de cette page sont alors ignorés.
Lien strict	Cliquez sur ce bouton d'option pour interdire la connexion des adresses IP/MAC qui ne figurent pas dans la liste des associations IP-MAC.
Table ARP	C'est la table ARP du routeur. Elle contient les adresses IP et MAC. Chaque couple d'adresses IP et MAC de la table ARP peut être sélectionnée et ajoutée à la liste des liens IP-MAC en cliquant sur Ajouter .
Tout sélectionner	Cliquer sur ce lien pour choisir tout contenu dans la table ARP ou liste de lien-IP.
Trier	Cliquez sur ce lien pour afficher la liste par l'usage d'adresse IP.
Rafraîchir	Actualise la table ARP. Lorsqu'un nouveau PC est ajouté au LAN, vous pouvez cliquer sur ce lien pour obtenir la table ARP actualisée.
Ajouter et modifier	Tapez l'adresse IP à lier à l'adresse Mac spécifiée. Adresse Mac – Tapez l'adresse MAC à lier à l'adresse IP spécifiée.
Liens IP-MAC	Affiche une liste des adresses IP et MAC liées.

LAN >> Association IP - MAC

Ajouter	Ce bouton vous permet d'ajouter la couple d'adresses choisie dans la table ARP où les adresses IP/MAC entrées dans la zone Ajouter et modifier à la Liste des liens IP-MAC.
Modifier	Ce bouton vous permet de modifier les adresses IP et MAC sélectionnées.
Supprimer	Vous pouvez supprimer n'importe quel élément de la liste des liens IP-MAC . Cliquez sur la ligne à supprimer, puis sur Supprimer .

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

3.3 NAT

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

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

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

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

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

3.3.1 Redirection de port

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



La redirection de ports ne s'applique qu'au trafic entrant. L'utilisateur de serveur à l'intérieur de LAN ne peuvent pas accéder à l'adresse IP du serveur. L'itinéraire correct est d'accéder au serveur en utilisant l'IP address privé local du serveur, ou vous devriez établir un nom d'emprunt dans un dossier de centres serveurs de Windows. Veuillez réorienter seulement les ports que vous connaissez que vous devez expédier plutôt que vers l'avant tous les ports. Autrement, vous compromettrez le type du pare-feu de sécurité déployé initialement par la service NAT.

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

Index	Nom du service	Protocole	Port public	Adr IP privé	Port privé	Acti
1		💙	0		0	
2		💙	0		0	
3		💙	0		0	
4		💙	0		0	
5		💙	0		0	
6		💙	0		0	
7		💙	0		0	
8		💙	0		0	
9		💙	0		0	
10		🗸	0		D	

NAT >> Configurer la table de redirection de ports

Protocole

apez la designation du service de réseau.

Sélectionnez le protocole de transport (TCP ou UDP).

Port public	Spécifiez quel port doit être redirigé vers l'adresse IP privée et le port privé spécifiés.
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.

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

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

Maintenance du système >> Gestion

Paramètres de gestion				
Contrôle d'accès pour la gestion	Paramétrage du port de gestion			
Activer la mise à jour à distance du firmware (FTP)	 Ports par défaut (Telnet: 23, HTTP: 80, FTP: 21) 			
🔲 Autoriser la gestion à partir de l'internet	💿 Ports définis par l'utilisateur			
☑ Désactiver le PING en provenance de l'internet	Port Telnet 23			
Liste des accès	Port HTTP 80			
Liste IP Masque de sous-réseau	Port FTP 21			
	Paramètres SNMP Activer l'agent SNMP Communauté pour GET public Communauté pour SET private Adr IP du gestionnaire			
	K			

3.3.2 Configuratin de l'hôte DMZ

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



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

Cliquez sur Configuration de l'hôte DMZ pour ouvrir la page suivante:

NAT >> Configuration de l'hôte DMZ

Néant 🔽	
Adresse IP privée	Choisir un PC
Adresse MAC du vrai hôte DMZ IP	00 . 00 . 00 .00 .00 .00
Remarque: Lorsqu'un hôte DMZ est a toujours active.	allumé, cela rendra automatiquement la connexion WAN

Si vous avez déjà configuré Alias WAN dans Accès internet>>PPPoE/PPPoA ou Accès internet >>MPoA, vous les trouverez dans Aux. WAN IP list à votre choix.

NAT >> Configuration de l'hôte DMZ

Configura	ition de l'hôt	e DMZ		
Index	Activer	IP WAN aux.	Adresse IP privée	
1.		192.168.1.55		Choisir un PC
			OK Effacer	
Activer		Cochez c	ette case pour active la fo	nction Hôte DMZ.
Adresse	IP privée	Entrez l'a PC pour s	adresse IP privée de l'hôte sélectionner une adresse I	e DMZ ou cliquez sur Choisir un P privée.
Choisir u	ın PC	Cliquez s liste des a	ur ce bouton pour faire aj adresses IP privées de tou	pparaître une fenêtre affichant une s les hôtes de votre réseau local.

Sélectionnez-en une comme adresse de l'hôte DMZ.

🕘 h	ttp://19 📃 🗖	
ſ		_
	192.168.1.11	

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

Adresse IP privée 🐱	
Adresse IP privée	192 . 168 . 1 . 10 Choisir un PC
Adresse MAC du vrai hôte DMZ IP	00,00,00,00,00,00
Remarque: Lorsqu'un hôte DMZ est allu toujours active.	umé, cela rendra automatiquement la connexion WAN

3.3.3 Ouverture de ports

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

Cliquez sur Ouverture de Ports pour ouvrir la page suivante :

NAT >> Configuration de l'ouverture de ports

Index	Commentaire	Adresse IP locale	État	
<u>1.</u>			×	
<u>2.</u>			×	
<u>3.</u>			×	
<u>4.</u>			×	
<u>5.</u>			×	
<u>6.</u>			×	
<u>7.</u>			×	
<u>8.</u>			×	
<u>9.</u>			×	
<u>10.</u>			×	
	Effac	er tout		
dex	Numéro d'ordre numéro appropr correspondante.	de la redirection de port à défin ié pour modifier ou effacer la red	ir. Cliquez s direction	
nmentaire Spécifiez le nom du service réseau.				

Adr. IP WAN aux.	Affiche l'adresse IP privée de l'hôte local que vous spécifiez dans Alias WAN. Ce champ n'apparaît pas si vous n'avez pas spécifié d'adresse IP WAN dans la page Alias WAN.
Adresse IP locale	Adresse IP privée de l'hôte local pour un service.
État	État de la redirection correspondante. X = redirection inactive, V = redirection active.

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

NAT >> ouverture de ports >> paramétrage de l'ouverture de ports

Index nº 1					
🗹 Activer l'ouvert	ture de ports				
	Commentaire	P2P-Emule			
	Ordinateur local	192 168	1 10 Choisir	un PC	
Protocole	Du port	Au port	Protocole	Du port	Au port
1. TCP 🛩	4500	4700	6. 🖳 😽	0	0
2. UDP 🚩	4500	4700	7. 🔜 💌	0	0
3. 🔜 🖌	0	0	8. 🖳 🖌	0	0
4 💌	0	0	9 💌	0	0
5 🚩	0	0	10. 🖳 🖌	0	0
		OK Effa	acer Annuler		

Toutefois, si vous avez défini précédemment des **alias WAN** dans **Accès à l'internet>>PPPoE/PPPoA** ou **Accès à l'internet>>MPoA**, vous les trouverez dans la liste déroulante **IP WAN**.

Activer l'ouverture de ports	Cochez cette case pour activer cet index
Commentaire	Tapez la désignation de l'application ou du service de réseau.
Ordinateur local	Tapez l'adresse IP privée de l'hôte local ou cliquez sur Choisir un PC pour en sélectionner une.
Choisir un PC	Cliquez sur ce bouton pour faire apparaître une fenêtre affichant la liste des adresses IP privées des hôtes locaux. Sélectionnez une adresse IP appropriée dans la liste.
Protocole	Spécifiez le protocole de couche transport : TCP, UDP ou (NÉANT).
Du Port	Spécifiez le numéro du premier port de la plage de ports.
Au Port	Spécifiez le numéro du dernier port de la plage de ports.

NAT >> Configuration de l'ouverture de ports

Configuration de	e l'ouverture de ports		
Index	Commentaire	Adresse IP locale	État
<u>1.</u>	P2P-Emule	192.168.1.10	V
<u>2.</u>			×
<u>3.</u>			×
<u>4.</u>			×
<u>5.</u>			×
<u>6.</u>			×
<u>7.</u>			×
<u>8.</u>			×
<u>9.</u>			×
<u>10.</u>			×

Effacer tout

3.3.4 Liste des ports connus

Cette page affiche une liste des ports connus.

NAT >> Afficher la liste des ports 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
Données pcANYWHERE	TCP	5631
Statistiques pcANYWHERE	UDP	5632
WinVNC	TCP	5900

3.4 Pare-feu

3.4.1 Principes du pare-feu

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

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

Assistant de démarrage rapide

Tapez le mot de passe Veuillez saisir une chaine de car mot de passe (23 caractères r	actères alphanuméric naximum).	ques pour votre		
Nouveau mot de passe Confirmer le mot de passe				
	< Précédent	Suivant >	Terminer	Annuler

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



Ancien mot de passe	
Nouveau mot de passe	
Retapez le nouveau mot de passe	

Fonctionnalités de pare-feu

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

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

Filtres IP

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

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



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

Filtrage adaptatif (SPI)

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

Blocage des applications de messagerie instantanée (IM) et de partage de fichiers (P2P)

Avec la popularité croissante des applications de messagerie instantanée, les communications peuvent devenir beaucoup plus faciles. Néanmoins, si certaines industries peuvent mettre à profit cet outil pour communiquer avec leurs clients, d'autres peuvent adopter une attitude plus réservée afin de réduire son utilisation abusive par les employés pendant les heures de travail ou pour éviter les failles de sécurité inconnues. Il en va de même pour les applications « peer to peer » car les partages de fichiers, s'ils peuvent être commodes, peuvent aussi poser des problèmes de sécurité. C'est pourquoi le routeur Vigor comporte une fonction de blocage d'IM et de P2P.

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

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

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

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

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

- 1. attaque par inondation SYN
- 2. attaque par inondation UDP
- 3. attaque par inondation ICMP
- 4. scrutation de flag TCP
- 5. « trace route »
- 6. options IP
- 7. protocole inconnu
- 8. attaque « land »

- 9. attaque « smurf » (attaque par surcharge
- 10. fragments SYN
- 11. fragments ICMP
- 12. attaque « tear drop »
- 13. attaque « fraggle »
- 14. attaque « ping of death »
- 15. scrutation de port TCP/UDP

Filtrage de contenu

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

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

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

Filtrage web

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

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

3.4.2 Configuration générale

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

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

Filtre d'appel	 Activer 	Début du filtrage à partir du Filtre n°1 💌
	🔘 Désactiver	
Filtre de données	 Activer 	Début du filtrage à partir du Filtre n°2 👻
	🔘 Désactiver	
Journalisation	Néant 👻	
🔲 Activer la protect	tion SPI (stateful pa	cket inspection)
🔲 Terminer toute co	onnection non-http :	sur le port TCP 80
🗹 Accepter les paqi	uets UDP fragmentés	5 (pour certains jeux en ligne, par ex. CS)

Pare-feu >> Configuration générale

Filtre d'appel

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

Filtre de données	Cochez Activer pour activer la fonction Filtre de données et spécifiez un filtre de début.
Journalisation	 Vous pouvez définir ici les conditions de journalisation. Néant Néant Autoriser Bloquer Indéterminé Néant - La fonction de journalisation n'est pas activée. Bloquer - Les paquets bloqués seront journalisés. Laisser passer - Les paquets passés seront journalisés. Pas de correspondance - La fonction de journalisation enregistrera tous les paquets qui ne correspondent pas aux règles de filtrage. À noter que, si vous tapez la commande <i>log −f</i>, le « log » de filtrage s'affichera sur le terminal Telnet.
Certains ieux en ligne	(nar exemple Half Life) utilisent un grand nombre de paquets LIDP

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

3.4.3 Paramétrage des filtres

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

Paramé	trage des filtres		Paramètres par défaut
Set	Commentaires	Set	Commentaires
<u>1.</u>	Default Call Filter	<u>7.</u>	
<u>2.</u>	Default Data Filter	<u>8.</u>	
<u>3.</u>		<u>9.</u>	
<u>4.</u>		<u>10.</u>	
<u>5.</u>		<u>11.</u>	
<u>6.</u>		<u>12.</u>	

Pare-feu >> Paramétrage des filtres

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

Pare-feu >> Paramétrage des filtres >> Editer les règles du filtre

Filtre 1				
Commentaires :	Default Call Filter			
Règle de filtrage	Actif	Commentaires		
1		Block NetBios		
2				
3				
4				
5				
6				
7				
		Filtre suivant	Néant	*



Règle de filtrage	Cliquez sur l'un des boutons 1 à 7 pour éditer/modifier la règle de filtrage. Cela a pour effet d'ouvrir la page web Modifier la règle de filtrage. Pour plus de détails, voir la page suivante.
Actif	Active ou désactive la règle de filtrage.
Commentaires	Tapez des commentaires ou une description du filtre (longueur maximale : 23 caractères).
Filtre suivant	Spécifie le filtre qui doit suivre le filtre actuel. Les filtres ne peuvent pas être appliqués en boucle.

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

Filtre 1 Règle 1 Commentaires : Block NetBios Cocher pour activer la règle de filtrage Appliquer un autre filtre Autoriser ou bloquer ~ Bloquer immédiatement Néant ~ 📃 Journaliser Protocole TCP/UDP 🔽 Sens Entrant ¥ Masque de sous-Adresse IP Opérateur Du port Au port . réseau Source any 255.255.255.255 (/32) 137 139 - ~ 255.255.255.255 (/32) 🗸 Destination any = 🗸 📃 Garder l'état Néant ¥ Fragments Effacer Annuler ΟK **Commentaires**

Pare-feu >> Editer les règles du filtre >> Modifier la règle de filtrage

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

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

règle de filtrage	
Laisser passer ou bloquer	 Spécifiez l'action que doit avoir la règle sur les paquets. Laisser passer immédiatement - Les paquets correspondants à la règle sont passés immédiatement. Bloquer immédiatement - Les paquets correspondants à la règle sont rejetés immédiatement. Laisser passer si plus de corresp Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est passé. Bloquer si plus de corresp Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est rejeté.
Appliquer un autre filtre	Si le paquet correspond à la règle de filtrage, la règle de filtrage suivante fait passer au filtre spécifié. Sélectionnez la règle de filtrage suivante dans le menu déroulant.
Journal	Cochez cette case pour activer la fonction de journalisation. Pour visualiser les journaux, utilisez la commande Telnet log-f .
Sens	Définit la direction des paquets. Concerne uniquement le filtre de données . Pour le filtre d'appel, ce paramètre n'est pas disponible puisque le filtre d'appel est appliqué au trafic sortant.
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. Pour appliquer la règle à toutes les adresses IP, tapez « n'importe laquelle » ou laissez le champ vide.
Masque de sous-réseau	Sélectionnez le masque de sous-réseau correspondant aux adresses IP auxquelles s'applique cette règle de filtrage dans le menu déroulant.
Opérateur, Du Port et Au Port	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 supérieurs.
Garder l'état	Cette fonction utilise les paramètres Sens, Protocole, Adresse IP, Masque de sous-réseau, Opérateur, Port de début et Port de fin. Concerne uniquement le filtre de données.
	La fonction Garder l'état est du même ordre que la fonction de filtrage adaptatif. Elle contrôle les paquets et accepte ceux qui ont

	des caractéristiques appropriées l'identifiant comme licite selon le protocole. Elle rejette les données entrantes non sollicitées. Vous pouvez choisir les protocoles suivants : any (n'importe lequel), TCP, UDP, TCP/UDP, ICMP et IGMP.
Fragments	Spécifiez une action sur les paquets fragmentés. Concerne uniquement le filtre de données .
	Néant - Aucune action sur les paquets fragmentés.
	Non fragmenté - Applique la règle aux paquets non fragmentés.
	Fragmenté - Applique la règle aux paquets fragmentés.
	Trop court - Applique la règle uniquement aux paquets qui sont trop
	courts pour avoir un en-tête complet.

Exemple

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



3.4.4 Blocage des applications de messagerie instantanée (IM)

Cliquez sur **Pare-feu** puis sur **Blocage d'IM** pour afficher la fenêtre de configuration. Celle-ci contient une liste des applications de messagerie instantanée courantes (MSN, Yahoo, ICQ/AQL, etc.). Cliquez sur **Activer le blocage d'IM** et sélectionnez la ou les applications de messagerie instantanée que vous voulez bloquer. Pour bloquer les applications de messagerie instantanée sélectionnées pendant des périodes spécifiques, tapez le numéro de plage horaire défini dans **Applications>>Plages horaires**.

Pare-feu >> Gestion du blockage d'IM
Paramétrage du blocage des applications de messagerie instantanée (IM)
Activer le blocage d'IM
Bloquer MSN Messenger
Bloquer Yahoo Messenger
Bloquer ICQ/AOL
Horaire
Index (1-15) dans <u>Horaire</u> Configuration :,,,,
Remarque:Les paramètres Action et Délai d'inactivité seront ignorés.
OK Annuler

3.4.5 Blocage des applications de partage de fichiers entre homologue (P2P)

Cliquez sur **Pare-feu**, puis sur **Blocage de P2P** pour afficher la fenêtre de configuration. Cette fenêtre contient une liste des applications P2P courantes. Cliquez sur **Activer le blocage de P2P** et sélectionnez la ou les applications P2P à bloquer. Pour bloquer les applications P2P sélectionnées pendant des périodes déterminées, tapez le numéro de plage horaire défini dans **Applications>>Plages horaires**.

Pare-feu >> Ge	estion du blockage de P2P	
Paramétrage d	lu blocage des applications de partage de fichiers P	eer-to-Peer
Activer le bl	ocage des applications P2P	
Protocole	Applications	Action
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	 Autoriser Interdire Interdire les téléchargements montants
FastTrack	KazaA, iMesh, MLDonkey	⊙ Autoriser ○ Interdire
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	⊙ Autoriser ○ Interdire
BitTorrent	BitTorrent	 Autoriser Interdire
Horaire Index (1-1 Remarque	.5) dans <u>Horaire</u> Configuration :,, ,,, , ,, , ,, , , , , , , , , , , , , , , , , , , ,	norés.

ActionSpécifie l'action pour chaque protocole.
Autoriser – Le client est autorisé à accéder à l'application avec le protocole
spécifié.Interdire – Le client n'est pas autorisé à accéder à l'application avec le
protocole spécifié.Interdire téléchargement – Le client n'est pas autorisé à accéder à
l'application avec le protocole spécifié pour effectuer des téléchargements
descendants. Les téléchargements montants sont néanmoins autorisés.

3.4.6 Protection anti-DoS

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

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

Pare-feu >> Configuration de la protection anti-DoS

Configuration de la protection anti-DoS			
Activer la protection anti-DoS			
Activer la protection contre l'inondation SYN	Seuil	50	paquets / s
	Temporisation	10	s
Activer la protection contre l'inondation UDP	Seuil	150	paquets / s
	Temporisation	10	s
Activer la protection contre l'inondation ICMP	Seuil	50	paquets / s
	Temporisation	10	s
Activer la détection de la scrutation de port	Seuil	150	paquets / s
Bloquer les options IP	📃 Bloquer la scrut	ation de fl	ag TCP
🔲 Bloquer le "land"	📃 Bloquer le "tear	drop"	
🔲 Bloquer le "smurf"	📃 Bloquer le "ping	of Death"	
🔲 Bloquer le "trace route"	🔲 Bloquer les frag	ments ICM	P
🔲 Bloquer les fragments SYN	🔲 Bloquer les inco	nnusProto	cole
🔲 Bloquer le "fraggle"			
Activer la fonction de defense DoS pu nitates	our prévenir des	attaques	
prodoco.			~
OK Efface	r tout Annuler		

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

	valeur 150 paquets par seconde et 10 secondes.
Activer la protection contre l'inondation ICMP	Cochez la case pour activer la fonction de protection contre l'inondation ICMP. Lorsque le nombre de paquets ICMP provenant de l'internet dépasse le seuil défini, le routeur rejette toutes les requêtes d'écho ICMP qui suivent pendant le temps défini par le paramètre Temporisation. Le seuil et la temporisation ont respectivement pour valeur par défaut 50 paquets par seconde et 10 secondes.
Activer la détection de la scrutation de port	Une attaque par scrutation de port consiste à envoyer un grand nombre de paquets à de nombreux ports pour tenter de déterminer à quels services un port répond. Pour activer la fonction de détection de scrutation de port, cochez la case. S'il détecte une telle tentative (dépassement du seuil), le routeur Vigor émet un message d'avertissement. Le seuil par défaut est de 150 paquets par seconde.
Bloquer les options IP	Cochez la case pour activer la fonction de blocage des options IP. Le routeur Vigor ignorera tous les paquets IP dans l'en-tête desquels figurent des options IP. Les options IP constituent une vulnérabilité du LAN car elles véhiculent des informations importantes, telles que des paramètres de sécurité, de compartimentage, TCC (groupe fermé d'utilisateurs), une série d'adresses internet, des messages de routage, etc. Un attaquant potentiel peut obtenir des renseignements sur vos réseaux privés.
Bloquer le « Land »	Cochez la case pour activer la protection contre les attaques de type « land ». L'attaque de type « land » combine l'attaque SYN avec l'usurpation d'adresse IP. Une attaque de type « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que les numéros de port sont identiques à ceux de la victime.
Bloquer le « smurf »	Cochez la case pour activer la fonction de blocage de « smurf ». Le routeur Vigor rejettera toute requête d'écho ICMP.
Bloquer le « trace route »	Cochez la case pour que le routeur Vigor ne laisse pas passer les paquets « trace route ».
Bloquer les fragments SYN	Cochez la case pour activer la fonction de blocage des fragments SYN. Le routeur Vigor rejettera tous les paquets dont l'indicateur SYN et le bit MF (more fragments) sont à 1.
Bloquer le « Fraggle »	Cochez la case pour activer la fonction de blocage de « fraggle ». Tous les paquets UDP de diffusion provenant de l'internet sont bloqués. Il se peut que la protection anti-DoS/DDoS bloque certains paquets licites. Par exemple, lorsque vous activez la protection contre le « fraggle », tous les paquets UDP de diffusion provenant de l'internet sont bloqués. Par conséquent, il se peut que les paquets RIP soient bloqués.
Bloquer la scrutation de flag TCP	Cliquez sur la case à cocher pour activer la fonction de blocage de la scrutation de flag TCP. Tout paquet TCP présentant une anomalie au niveau des indicateurs (« flags » est rejeté. Les anomalies sont, entre autres : absence d'indicateurs, <i>FIN sans ACK, SYN FIN ensemble, Xmas (indicateurs FIN URG et PSH à 1)</i> et <i>full Xmas (tous les indicateurs à 1)</i> .
Bloquer le « Tear	Cliquez sur la case à cocher pour activer la fonction de blocage de

Drop »	« tear drop ». De nombreuses machines peuvent se bloquer à la réception de datagrammes (paquets) ICMP qui dépassent la longueur maximale. Pour éviter ce type d'attaque, le routeur Vigor est capable de rejeter les paquets ICMP fragmentés dont la longueur dépasse 1024 octets.
Bloquer le « Ping of Death »	Cliquez sur la case à cocher pour activer la fonction de blocage du « ping of death ». Dans ce type d'attaque, l'attaquant envoie des paquets qui se chevauchent aux machines hôtes cibles, lesquelles se bloquent lorsqu'elles reconstituent les paquets. Les paquets de ce type sont bloqués par le routeur Vigor.
Bloquer les fragments ICMP	Cliquez sur la case à cocher pour activer la fonction de blocage des fragments ICMP. Les paquets ICMP dont le bit MF (« more fragments ») est à 1 sont rejeté.
Bloquer le « Land »	Cochez la case pour activer la protection contre les attaques de type « land ». L'attaque de type « land » combine l'attaque SYN avec l'usurpation d'adresse IP. Une attaque de type « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que les numéros de port sont identiques à ceux de la victime.
Bloquer les protocoles inconnus	Cochez la case pour activer la fonction de blocage des protocoles inconnus. Dans l'en-tête de chaque paquet IP, il y a un champ qui indique le type de protocole de couche supérieure. Toutefois, les types de protocole supérieurs à 100 sont réservés et non définis pour l'instant. Par conséquent, le routeur doit pouvoir détecter et rejeter ce genre de paquet.
Messages d'avertissement	La fonction SysLog permet à l'utilisateur de visualiser les messages du routeur Vigor. L'utilisateur, en tant que serveur SysLog, reçoit les rapports émis par le routeur Vigor qui est un client SysLog. (Reportez-vous au Chapitre Maintenance du système pour plus de détails).
	Tous les messages d'avertissement liés à la protection anti-DoS sont envoyés à l'utilisateur qui peut les visualiser à l'aide du démon SysLog. Ces messages ont comme préfixe le mot-clé « DoS », suivi d'un nom qui indique le type d'attaque détecté.
	Daramétrago do Sust og / Alorto nar mail

Paramétrage de SysLog / Alerte par mail Paramétrage de SysLog Paramét

arametrage ac oystog		
🗹 Activer		🔲 Active
Adresse IP du serveur	192.168.1.15	Serveur
Port de destination	514	Envoyer
Activer le message Syslo	Chemin c	
🖾 Log Firewall		

DrayTek Syslo	g					
LAN Status TX Pa	ackets	192.168. Vigor 3100 RX Pao 118	1.1 v loss compared to the series of the series of the series of the series compared to the series of the series o	WAN Status Getway IP (Fixed) WAN IP (Fixed)	TX Packets 0 RX Packets 0 0	RX Rate 0 TX Rate 0
irewall Log VP1 Time Jan 1 00:00:42	I Log U Host Vigor	iser Access Log C Message DoS syn flood Bl	Call Log WAN Lo	ng Budget Log Network	Minformation Net Stat	e 10 -S 3943751
Jan 1 00:00:34	Vigor	DoS icmp_flood H	Block(10s) 192.168	.1.115 -> 192.168.1.1 PR	1(icmp) len 20 60 icmp	0/8
<						>
DSL Status Mode T1.413	- 「	State HANDSHAKE	Up Speed	Down Speed	SNR Margin	Loop Att

3.4.7 Filtre de contenu d'URL

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

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

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

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

Paramétrage du filtre de o	contenu			
Activer le contrôle d'a	ccès URL			
 Liste noire (bloquer ce 	lles contenant ces m	ots)		
🔘 Liste blanche (autorise	er celles contenant c	es mots)		
No. ACT	Mot-clé	No.	ACT	Mot-clé
1		5		
2		6		
3		7		
4		8		
À noter que de multiples	mots-clés sont auto	risés. Par	exemple:	hotmail vahoo msn
Empêcher l'accès au w	veb à partir de l'adr	esse IP		
Activer la fonction de l	restriction web			
🗌 Java	ActiveX	🗌 Fichi	ers compre	essés 🗌 Fichiers exécutables
🗌 Fichiers multimédias	🗌 Cookie	Proxy	y	
Sous-réseaux d'excep	tion			
No. Act	Adresse IP			Masque de sous-réseau
1		~	,	
2		~	,	
3		~	,	
4		~	,	
Horaire				
Index (1-15) du <u>Horaire</u> C	onfiguration:	,	,,	
Remarque : les paramètres	Action et Temps d'ina	activité se	eront ignor	és.
		ffacer tout	Anr	uler
A stiven le contrôle	Coobor lo coco		tivon la	contrôle d'aceòs UDI
d'accès UDI	Cochez la case	pour ac	liver le	controle d'acces UKL.
u acces UKL				
Liste noire (bloquer	Cliquez sur ce	bouton	pour int	erdire l'accès à une page web
ces mots-clés	contenant les m	nots-clé	s spécifi	és.
I ista hlancha	Cliquez sur ce	houton	nour auf	oriser l'accès à une page web
Liste Dianche	contonant los m	ote alá	o onácifi	ón
(autoriser ces	contenant les n	1015-010	s specifi	es.
mots-cles)				
Mot-clé	Le routeur Vige	or perm	et de dé	finir des mots-clés dans 8 trames,
	chacune pouva	nt en co	ontenir p	lusieurs. Le mot-clé peut être un nom,
	une partie de no	om ou u	ine URL	complète. Dans une trame, les
	mots-clés sont	séparés	par un e	space, une virgule ou un point-virgule.
	De plus, la long	gueur m	aximale	de chaque trame est de 32 caractères.
	Une fois les mo	ts-clés	spécifiés	s, le routeur Vigor interdit l'accès à tout
	site dont tout of	u partie	de l'UF	L correspond à un mot-clé défini par
	l'utilisateur. À	noter qu	ue plus l	a liste des mots-clés de blocage est
	simple, plus le	routeur	Vigor s	era efficace.
Empôchar Pacoàs au	Cookar ootto o		- intondi	a l'aggès au mah à l'aida d'una
Empecher racces au		ise pour		2.2. Il s'a sit d'avant alle d'une
web a partir de	auresse IP, com	inte fitt	µ.//∠U∠.(ontrôlo	b.5.2. It's agit a empecter que
r auresse in	queiqu un esqu	ive le co	ontrole (TACCES UKL.
	Vous devez effa	acer le c	cache de	votre navigateur pour que le filtrage
	de contenu d'U	RL fond	ctionne o	correctement sur une page web que
	vous avez déjà	visitée.		
Activon la fonction J-	Cooker la sec		tinan 1-	fonction
Acuver la lonction de	Cocnez la case	pour ac	uver la	ioncuon.

restriction web	<i>Java</i> - Cochez la case pour activer la fonction de blocage d'objet Java. Le routeur Vigor rejettera les objets Java provenant de l'internet.			
	<i>ActiveX</i> - Cliquez sur la case à cocher pour activer la fonction de blocage des objets ActiveX. Tout objet ActiveX provenant de l'internet sera refusé.			
	<i>Fichiers compressés</i> - Cochez la case pour activer la fonction de blocage des fichiers compressés et donc empêcher le téléchargement de fichiers compressés. Le routeur Vigor peut bloquer les types de fichiers compressés suivants.			
	zip, rar, .arj, .ace, .cab, .sit			
	Fichiers exécutables - Cochez la case pour empêcher le			
	téléchargement de fichiers exécutables à partir de l'internet.			
	.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg			
	<i>Cookie</i> - Cochez la case pour bloquer la transmission d'informations			
	vers l'extérieur via les cookies afin de protéger votre vie privée.			
	Proxy - Cochez la case pour rejeter toute transmission via un proxy. Pour maîtriser l'utilisation de la bande passante, il peut être très intéressant de bloquer le téléchargement de fichiers multimédias à partir de pages web. Les fichiers ayant les extensions suivantes seront bloqués par le routeur Vigor.			
	.mov .mp3 .rm .ra .au .wmv			
	.wav .asf .mpg .mpeg .avi .ram			
Sous-réseau d'exception	Vous pouvez spécifier jusqu'à 4 adresses IP ou sous-réseaux pour les exempter du <i>contrôle d'accès URL</i> . Pour activer une entrée, cochez la case « ACT » correspondante.			
Horaire	Spécifiez l'horaire de mise en œuvre de la fonction de filtrage de contenu d'URL.			

3.4.8 Filtre de contenu web

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

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

3.5 Gestion de la bande passante

3.5.1 Limite des sessions

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

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

Gestion de la bande passante >> Limite de session

Limite de session
Nombre maximum de sessions: 100
Liste des limitations
Index Première IP Dernière IP Sessions maximum
Limitation spécifique
Première IP: IP finale:
Maximum Sessions:
Ajouter Editer Supprimer
Planification de l'heure
Index (1-15) dans Horaire Configuration:
Remarque: L'action et les paramètres du timeout Idle seront ignorés
Kennarque, L'action et les parametres du timeout fuie seront ignores
OK

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

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

3.5.2 Limite de bande passante

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

Cliquez sur l'option **Limite de bande passante** du menu **Gestion de la bande passante** pour ouvrir la page web

suivante

Gestion de la bande passante >> Limite de bande passante

Lir Lir I:	mite d'émission par défaut (TX): 200 Kbps mite de réception par défaut (RX): 800 Kbps <mark>ste des limitations</mark> ndex Première IP IP finale Limite d'émission (
Lir Lir	mite de réception par défaut (RX): <mark>800 K</mark> bps <mark>ste des limitations</mark> ndex Première IP IP finale Limite d'émission (
	ste des limitations ndex Première IP IP finale Limite d'émission (
Ī	ndex Première IP IP finale Limite d'émission (
1	ndex fremiere if if finale Limite d emission (
Lii Pr	mitation spécifique remière IP: IP finale:
Lir	nite d'émission (TX): Kbps Limite de réception (RX):
	Kbps
	Ajouter Éditer Supprimer
anification	ı de l'heure
Index (1	1-15) dans Heraire Configuration:
Remar	que: L'action et les naramètres du timeout Idle seront ignorés
Kennun	quer 2 de les rectes parametres du cincour faie serent igneres.

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

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

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

3.6 Applications

3.6.1 Dynamic DNS

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

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

Activer la fonction et ajouter un compte DNS dynamique

- 1. Supposons que vous ayez enregistré un nom de domaine auprès du fournisseur de service DDNS *hostname.dyndns.org* et ouvert un compte dont le nom d'utilisateur est *test* et dont le mot de passe est *test*.
- 2. Dans le menu de paramétrage du DNS dynamique, cochez Activer le paramétrage du DNS dynamique.

🛛 Activer le paramétrag	e du DNS dynamique	
	Afficher le journal	Forcer la mise à jour
omptes :		
Index	Nom de domaine	Actif
<u>1.</u>		×
<u>2.</u>		х
<u>3.</u>		х

Applications >> Paramétrage du DNS dynamique

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

Applications >> Paramétrage du DNS dynamique >> Configuration de compte DNS

uynannque	
Index : 1	
🗹 Activer le compte DNS	3 dynamique
Fournisseur de service	dyndns.org (www.dyndns.org)
Type de service	Dynamique 💌
Nom de domaine	chrono01 💌
Nom d'utilisateur	chrono6853 (23 caractères maximum)
Mot de passe	(23 caractères maximum)
📃 Alias (wildcard	ds)
📃 Secours de me	essagerie (Backup MX)
Extension de courrier	
	OK Effacer Annuler
ournisseur de serv	ice Sélectionnez le fournisseur de service DNS dynamiq
ype de service	Sélectionnez un type de service (Dynamique, Personnalisé, Statique).
om de domaine	Tapez un nom de domaine choisi précédemment.
om d'utilisateur	Tapez le nom d'utilisateur choisi pour le domaine.

- Mot de passeTapez le mot de passe choisi pour le domaine.
- 4. Cliquez sur le bouton **OK** pour activer les paramètres. Vous pouvez voir que vos paramètres ont été enregistrés.

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

Désactiver la fonction et effacer tous les comptes DNS dynamique

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

Supprimer un compte DNS dynamique

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

3.6.2 Plages horaires

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

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

Applications >> Horaire

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

Effacer tout

Vous pouvez paramétrer jusqu'à 15 plages horaires. Vous pouvez ensuite les appliquer à votre **accès à l'internet**.

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

Applications >> Horaire

Index nº 1			
🗹 Activer cet	te plage horaire		
	Date de début ((aaaa-mm-jj)	2000 🗸 - 1 🔽 - 1 🔽
Heure de début		(hh:mm)	
	Durée (hh:mm)		0 🕶 : 0 💌
	Action		Forcer la connexion 💌
	Délai d'inactivite	é	minute(s).(255 maxi, 0 par défaut)
	Fréquence		
	🔘 Une fois		
	Jours de la s	semaine	
	🗌 Dim 💽	🛛 Lun 🗹 M	lar 🗹 Me 🗹 Je 🗹 Ven 🔲 Sam
Activer cette horaire	plage	Cochez la	case pour activer la plage horaire.
[aaaa-mm-jj])	specificzi	a date de debut de la plage horane.
Heure de déb hh:mm)	out	Spécifiez l	'heure de début de la plage horaire.
Durée (hh:m	m)	Spécifiez l	a durée de la plage horaire.
Action		Spécifiez o Forcer la horaire. Forcer la horaire.	quelle action doit être effectuée durant la plage horaire. connexion - Connexion permanente durant la plage déconnexion - Connexion interdite durant la plage
		Activer à	la demande - Connexion établie à la demande avec un

	Délai d'inactivité.
	Désactiver à la demande - Connexion établie tant qu'il y a du trafic sur la ligne. Déconnexion à l'expiration du délai d'inactivité, d'autres connections étant impossible durant la plage horaire.
Délai d'inactivité	Spécifiez la durée propre à la plage horaire. Fréquence - Nombre de fois que la plage horaire sera appliquée Une fois - La plage horaire sera appliquée une seule fois Jours de la semaine - La plage horaire sera appliquée les jours spécifiés.

Exemple

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

Heures de bureau:	$10 \frac{11}{9} \frac{12}{3} \frac{1}{3}$		10 ¹¹ 12 -9	1 2 3
(Forcer la connexion)	87654		8 7 6	5
Lun - dim	9h 00	à	18h	00

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

3.6.3 UPnP

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

Applications >> UPnP

Activer le service UPnP	
	Activer le service de contrôle de connexion
	Activer le service d'état de connexion

sélectionner ci-dessus le service approprié pour autoriser le contrôle, 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**.

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

Address 🔕 Network Connections		📜 IP Broadband Connection on	Router Status 🔽 🕅
Network Tasks	Broadband		
Create a new connection Set up a home or small office network	hinet Disconnected WAN Miniport (PPPOE)	Internet Gateway Status:	Connected
0	Diai-up	Duration:	00:19:06
See Also 📀	test	Speed:	100.0 Mbps
Other Places	Internet Gateway	Activity Internet Internet Gatew	ay My Computer
Control Panel My Network Places My Documents My Computer	IP Broadband Connection on Router Enabled	Packets: Sent: 404 Received: 1,115	734 666
Details (*) Network Connections System Folder	Local Area Connection Enabled Realtek RTL8139/810x Family	Properties Disable	

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

	Colorite and the second s
onnect to the Internet using:	access.
IP Broadband Connection on Router	Services
his connection allows you to connect to the Internet through a hared connection on another computer.	 □ Ftp Example ☑ msnmsgr (192.168.29.11:13135) 60654 UDP ☑ msnmsgr (192.168.29.11:7824) 13251 UDP ☑ msnmsgr (192.168.29.11:8789) 63231 TCP

Rappel concernant le pare feu et UPnP:

Impossibilité d'utiliser la function UPnP avec le logiciel pare

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

Considérations de sécurité

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

- Certains systèmes d'exploitation Microsoft ont identifié les points faibles du protocole UPnP. Assurez-vous que vous avez appliqué les packs de service et les correctifs les plus récents.
- Les utilisateurs non privilégiés peuvent contrôler certaines fonctions du routeur et notamment enlever et ajouter des mappages de ports.

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

3.7 LAN sans fil

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

Les routeurs sans fil Vigor sont dotés d'une interface LAN sans fil conforme au protocole IEEE 802.11n. Pour améliorer encore les performances, le routeur Vigor est également doté de la technologie sans fil évoluée qui permet d'atteindre 300 Mbit/s*. Vous pouvez enfin profiter de la musique et de la vidéo en flux.

3.7.1 Principe de base

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



Cryptage materiel en temps réel

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

Choix complet de normes de sécurisation

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

- Le cryptage WEP (Wireless Equivalent Privacy) crypte chaque trame transmise par radio à l'aide d'une clé de 64 bits ou de 128 bits. Normalement, le point d'accès préétablit un jeu de quatre clés et communique avec chaque station en utilisant l'une de ces quatre clés.
- Le cryptage WPA (Wi-Fi Protected Access), le mécanisme de sécurisation dominant dans l'industrie, a deux formes : WPA-personnel ou WPA Pre-Share Key (WPA/PSK) et WPA-entreprise ou WPA/802.1x.
- Dans WPA-personnel, une clé préétablie est utilisée pour le cryptage pendant la transmission des données. Le WPA utilise le protocole d'intégrité de clé temporelle (TKIP) pour le cryptage, tandis que WPA2 utilise AES. WPA-entreprise combine le cryptage et l'authentification.

Comme le WEP s'est avéré vulnérable, vous pouvez envisager d'utiliser WPA pour une meilleure sécurité. Choisissez le mécanisme de sécurisation qui correspond à vos besoins.

Quels que soient les mécanismes de sécurisation que vous choisissez, ils amélioreront tous la protection des données radio et/ou la confidentialité de vos réseaux sans fil. Le routeur sans fil Vigor est très souple et peut prendre en charge de multiples connexions sécurisées mettant en œuvre simultanément WEP et WPA.



Liste des stations affiche toutes les stations de votre réseau sans fil et l'état de connexion. Par ailleurs, vous pouvez permettre la connexion de l'utilisateur que vous avez la confiance avec la fonctionalité de **Contrôle d'accès MAC**.

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

3.7.2 Paramètres généraux

La page web qui apparaît suivant vous permet d'activer le LAN sans fil.

LAN	sans	fil >>	Paramètre	dénéral
				general

ctiver le LAN sans fil	
Mode :	Mixte(11b+11g)
Index(1-15) dans <u>Horaire</u> Configuration:	
SSID :	default
Canal :	Channel 6 💌
Masquer le SSID	
📃 Préambule long	
Masquer le SSID : emp Préambule long : néc (performances plus faib	pêcher le SSID d'être scanné. essaire seulement pour certains vieux périphériques 802.11b les).

Enable Wireless LAN Check the box to enable wireless function.

Mode

Select an appropriate wireless mode.

Mixed (11b+11g)-The router communicates with standard 802.11b and standard 802.11g STAs simultaneously. *11g only*-The router communicates with standard 802.11b STAs.

11b only-The router communicates with standard 802.11b STAs.

Mode :

Mixte(11b+11g)	*
Mixte(11b+11g)	
11g seulement	
11b seulement	

Index (1-15)Vous pouvez limiter le fonctionnement du LAN sans fil à certaines
plages horaires. Vous pouvez choisir jusqu'à 4 plages horaires parmi
les 15 définies dans Applications >> Plages horaires. Par défaut, ce
champ est vide et la fonction est activée en permanence.

SSID et canal	 Par défaut, le SSID est « valeur par défaut ». Nous vous suggérons de le changer. SSID – Identifie le LAN sans fil. Le SSID peut se composer d'un nombre quelconque de caractères ou de divers caractères spéciaux. Canal – Canal radio du LAN sans fil. Le canal par défaut est 6. Vous pouvez en spécifier un autre si le canal sélectionné est gravement perturbé.
Masquer le SSID	Cochez cette case pour prévenir toute scrutation malveillante et rendre difficile à des clients non autorisés de joindre votre LAN sans fil. Selon l'utilitaire sans fil, l'utilisateur pourra visualiser les informations à l'exception du SSID ou n'avoir aucune information concernant le routeur sans Vigor.
Préambule long	Cette option définit la longueur du champ de synchronisation d'un paquet 802.11. La plupart des réseaux sans fil modernes utilisent un préambule court constitué d'un champ de synchronisation de 56 bits au lieu d'un préambule long de 128 bits. Toutefois, certains équipements de réseau sans fil 11b originel ne prennent en charge que le préambule long. Cochez la case Préambule long s'il cela est nécessaire pour communiquer avec ce type d'équipement.

3.7.3 Sécurité

Cette page vous permet de définir les paramètres de sécurité. Une fois ces paramètres définis, cliquez sur **OK** pour qu'ils soient pris en compte.

	Mode:	WEP	*
WPA	:		
	Clé prépartagée (PSK):	*****	
	Tapez 8 à 63 caractères AS par exemple, "cfgs01a2" o	CII ou 64 chiffres he> u "0x655abcd".	xadécimaux commençant par "Ox",
WEP	:		
	Longueur de la clé	64 bits 💌	
	⊙Clé 1 :	**********	
	◯Clé 2 :	**********	
	◯Clé 3 :		
	◯Clé 4 :	**********	
Pour Tape exem Pour Tape	clé WEP de 64 bits z 5 caractères ASCII ou 10 cl ple, "AB312" ou "0x414233313 clé WEP de 128 bits z 13 caractères ASCII ou 26	hiffres hexadécimaux 32". chiffres hexadécimaux	commençant par "Ox", par < commençant par "Ox", par

ΟK

Annuler

LAN sans fil >> Paramètres de sécurité

Mode

Désactiver - Désactive le mécanisme de cryptage. Pour la sécurité de votre routeur, choisissez l'un des modes de cryptage suivants. **WEP -** Accepte uniquement les clients WEP. La clé doit être tapée dans Clé WEP.

WPA/PSK - Accepte les clients WPA. La clé doit être tapée dans PSK.

WPA2/PSK - Accepte les clients WPA2. La clé doit être tapée dans PSK.

Mixte (WPA+ WPA2)/PSK - Accepte simultanément les clients WPA et WPA2. La clé doit être tapée dans le PSK.

Mode:

WEP	~
Désactiver	
WEP	
WPA/PSK	
WPA2/PSK	
Mixed(WPA+WPA2)/PSI	<

WPAWPA crypte chaque trame transmise par radio à l'aide de la clé
entrée manuellement dans le champ ou négociée automatiquement
via l'authentification 802.1x. Entrez 8 à 63 caractères ASCII, par
exemple 012345678 (soit 64 chiffres hexadécimaux commençant par
0x, par exemple « 0x321253abcde... »).

WEPPour une clé de 64 bits - Pour le WEP 64 bits, entrez 5 caractères
ASCII, comme 12345 (ou 10 chiffres hexadécimaux commençant
par 0x, par exemple 0x4142434445F).Pour une clé de 128 bits - Pour le WEP 128 bits, entrez 13
caractères ASCII, comme ABCDEFGHIJKLM (ou 26 chiffres
hexadécimaux commençant par 0x, par exemple
0x4142434445464748494A4B4C4D)

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

3.7.4 Contrôle d'accès

LAN sans fil >> Contrôle d'accès

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

🗹 Activer le contrôle d'accè	ès
Politiqu	e : Active le filtrage par adresse MAC 💌
	Attribut d'index Adresse MAC
Index	Attribute Adresse MAC
Adrees	
Auress	s: Isoler la station du LAN
4	sjouter Supprimer Modifier Annuler
	OK Effacer tout
ctiver le contrôle d'a	ccès Cochez cette case pour activer la fonction de contrôle d'a par adresse MAC.
dresse MAC	Entrez manuellement l'adresse MAC du client sans fil.

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

3.7.5 WDS

OK

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

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

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


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



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

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



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

LAN sans fil >> Paramètres WDS

Paramètres WDS				
	Pont			
Mode: Désactiver 💙	Activer Adresse MAC homologue			
Sécurité:				
● Désactiver ○ WEP ○ Clé partagée				
WEP:				
Utiliser le jeu de clés WEP défini dans <u>Paramètres</u> <u>de sécurité</u> .	Nota: Désactiver les liens inutilisés pour améliorer les performances.			
Clé partagée :	Relais			
Туре : ТКІР	Activer Adresse MAC homologue			
Clé . **********				
Tapez 8 à 63 caractères ASCII ou 64 chiffres hexadécimaux commençant par " 0x ", par exemple " cfgs01a2 " ou" 0x655abcd ".	Fonction de point d'accès :			
OK Effacer Annuler				

Mode

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

Mode:

Désactiver	*	
Désactiver		
Pont		
Relais		

Sécurité	Il y a trois options :, Désactivé , WEP et Clé prépartagée . Le choix fait ici validera le champ WEP ou Clé prépartagée qui suit.
WEP	Cochez cette case pour utiliser la clé WEP qui a été spécifiée dans la page Paramètres de sécurité . Si vous n'avez pas spécifié de clé dans la page Paramètres de sécurité , cette case à cocher est estompée.
Paramètres	Mode de cryptage – Si vous avez coché la case Utilisation de la même clé WEP, inutile de choisir 64 bits ou 128 bits comme mode de cryptage. Si vous ne cochez pas cette case, vous pouvez spécifier maintenant la clé WEP dans cette page. Index de clé – Choisissez la clé que vous voulez utiliser après avoir choisi le mode de cryptage approprié. Clé – Tapez la clé.
Clé prépartagée	Tapez 8 à 63 caractères ASCII ou 64 chiffres hexadécimaux commençant par « 0x ».
Pont	Si vous choisissez le mode pont, tapez l'adresse MAC d'homologue dans ces champs. Vous pouvez entrer jusqu'à six adresses MAC d'homologue. Pour que les performances soient meilleures, désactivez les liens non utilisés. Si vous voulez invoquer l'adresse MAC d'homologue, n'oubliez pas vous pouvez entrer au maximum deux adresses MAC d'homologue. Si vous voulez invoquer l'adresse MAC d'homologue, n'oubliez pas de cocher la case Activer en face de l'adresse MAC.
Fonction de point d'accès	Cliquez sur Activer pour indiquer que le routeur fonctionnera comme un point d'accès ; cliquez sur Désactiver pour annuler cette fonction.
État	Vous permet d'envoyer un message « hello » aux homologues. Il faut que l'homologue prennent en charge cette fonction.

3.7.6 Découverte d'AP

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

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

LAN sans fil >> Découverte de points d'accès

В	SSID	SSID Canal	
		Scruter	
Voir <u>Statistique</u>	es.		
Nota: Pendant autorisée à se	le processu connecter a	us d'analyse (~5 secondes), aucune station n'est au routeur.	
Ajouter à <u>Par</u>	amètres WD	<u>s</u> :	
Adresse MAC d	e l'AP	Ajouter	
er		Lance une recherche de points d'accès. L	les résultat

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

3.7.7 Liste des stations

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

LAN sans fil >> Liste des stations	
Liste des stations	
État Adresse MAC	
Actualiser	
Codes d'état :	
C: connecté, sans cryptage. E: connecté, WEP.	
P: connecté, WPA. A: connecté, WPA2.	
B: Bloqué par le contôle d'accès.	
F: L'authentification 802.1X ou WPA a échoué.	
Nota: Après qu'une station s'est connectée avec succès au routeur, elle peut être coupée sans préavis. Dans ce cas, elle figure toujours dans la liste jusqu'à l'expiration de la connexion.	
Ajouter à <u>Contrôle d'accès</u> :	
Adresse MAC du client	
Ajouter	

Actualiser

Cliquez sur ce bouton pour actualiser la liste des stations.

Ajouter

Cliquez sur ce bouton pour ajouter l'adresse MAC actuellement sélectionnée au **Contrôle d'accès**.

3.8 Maintenance du système

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

3.8.1 État du système

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

: Vigor2700 series

: Dec 28 2006 10:02:11

: 121201_A Annex A

: 2.7.1.1

État du système

Nom de modèle Version du firmware Date/Heure de création ADSL Firmware Version

```
LAN
```

```
Adresse MAC : 00-50-7F-87-14-78

1re adresse IP : 192.168.1.1

Premier masque de

sous-réseau : 255.255.255.0

Serveur DHCP : Oui
```

```
WAN
État de la
connexion
Adresse MAC
Connexion
Adresse IP
Passerelle par
défaut
```

DNS

```
: Disconnected

: 00-50-7F-87-14-79

: ---

: ---

: ---

: 194,109,6,66
```

Nom de modèle	Affiche la désignation de modèle du routeur.	
Version du firmware	Affiche la version du firmware du routeur.	
Date et heure de création	Affiche la date et l'heure de création du firmware.	
Adresse MAC	Affiche l'adresse MAC de l'interface LAN.	
1 ^{re} adresse IP	Affiche l'adresse IP de l'interface LAN.	
1 ^{er} masque de sous-réseau	Affiche le masque de sous-réseau de l'interface LAN.	
Serveur DHCP	Affiche l'état actuel du serveur DHCP de l'interface LAN.	
Adresse MAC	Affiche l'adresse MAC de l'interface WAN.	
Adresse IP	Affiche l'adresse IP de l'interface WAN.	
Passerelle par défaut	Affiche l'adresse IP de la passerelle par défaut.	
DNS	Affiche l'adresse IP du DNS primaire.	
Adresse MAC	Affiche l'adresse MAC de l'interface sans fil.	
Domaine de fréquence	Affiche le nombre de canaux utilisables par le produit sans fil. Ce nombre varie suivant les pays : Europe (13 canaux utilisables), Etats-Unis (11 canaux utilisables).	
Version du firmware	Affiche des informations sur le pilote WLAN.	

3.8.2 Mot de passe administrateur

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

istrateur du mot de passe	
Ancien mot de passe	
Nouveau mot de passe	
Retapez le nouveau mot de passe	

Ancien mot de passe Tapez l'ancien mot de passe. Le mot de passe par défaut est vide.

Nouveau mot de passe Tapez le nouveau mot de passe.

Retaper le nouveau mot de Retapez le nouveau mot de passe. **passe**

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

3.8.3 Sauvegarde des configurations

Sauvegarde de la configuration

Pour sauvegarder votre configuration :

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

Maintenance du système >> Sauvegarde des configurations

Sauvegarde/	restauration des configurations
Restauration	
	Sélectionner un fichier de configuration.
	瀏覽
	Cliquer sur Restaurer pour restaurer le fichier.
	Restaurer
Sauvegarder	
	Cliquer sur Sauvegarder pour télécharger les configurations
	actuellement actives sous la forme d'un fichier.
	Sauvegarder Annuler

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



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

Save As						? 🗙
Save in:	🞯 Desktop		~	GOE	• 🛄 •	
My Recent Documents Desktop My Documents	My Document My Computer My Network F RVS-COM Lite Annex A MWSnap300 TeleDanmark Tools E v2k2_232_co V2k6_250_co	:s Places ; nfig_1 nfig_1				
My Computer						
	File name:	config		•	- (Save
My Network	Save as type:	Configuration file			• (Cancel

3. 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

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

Maintenance du système >> Sauvegarde des configurations		
Sauvegarde/	restauration des configurations	
Restauration		
	Sélectionner un fichier de configuration.	
	(瀏覽	
	Cliquer sur Restaurer pour restaurer le fichier.	
	Restaurer	
Sauvegarder		
_	Cliquer sur Sauvegarder pour télécharger les configurations	
	actuellement actives sous la forme d'un fichier.	
	Sauvegarder Annuler	

2. Cliquez sur le bouton **Parcourir** pour choisir le fichier de configuration correct.

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

3.8.4 Syslog/Alerte par mail

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

```
Maintenance du système >> Paramétrage de SysLog / Alerte par mail
```

Paramétrage de SysLog	Paramétrage de Alerte par mail
🗹 Activer	🗖 Activer
Adresse IP du serveur	Serveur SMTP
Port de destination 514	Envoyer à
Activer le message Syslog:	Chemin de retour
🗹 Log Firewall	Authentification
🗹 Log VPN	Nom d'utilisateur
🗹 Log d'accès utilisateur	
🗹 Log d'appel	Mot de passe
🗹 Log WAN	
🗹 Information du Routeur/DSL	



Pour visualiser le SysLog:

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

🛅 Router Tools V2.5.4	١	🕥 About Router Tools
		🏘 Ez Configurator Vigor2100 Series
		🐴 Firmware Upgrade Utility
		🔟 Syslog
		🥑 Uninstall Router Tools V2.5.4
		🍯 Visit DrayTek Web Site

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

		Vicor cerie	c Dept. Ric	Gateway IP (Fixed	d) TX Packet	s RX Rate
AN Status		Ngor serie:	S DITICIDIS		0	0
TX Pa	ickets	RX Pack	ets	WAN IP (Fixed)	RX Packet	ts TX Rate
9	š1	759			0	0
wall Log VP	Log User Acce	s Log Ca	ILOS WAN LO	Network Infomatio	0. Net State	
n Line Routers		whore ou	Host Name:	niki-pc		
IP Address	Mask	MAC	NIC Descriptio	n: Realtek R TL813	9 Family PCI Fast F	Sthemet NIC - '
92.168.1.1	255.255.255.0	00-50-	-NIC Informatio	n		
			MAC Address:	00-0E-A6-2A-D5-A1	Default Geteway:	192.168.1.1
			IP Address:	192.168.1.10	DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Wed Apr 06
		>	DNS Servers:	168.95.1.1	Lease Expires:	Sat Apr 09
	R	efresh		192.100.1.1		16:59:40 2005

3.8.5 Réglage de l'heure et de la date

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

ormation sur le fuseau		
Heure système actuelle	2000 Jan 1 Sat 4 : 31 : 53 Demander l'heure	
jlage de l'heure		
💿 Utiliser l'heure du navig	ateur	
O Utiliser le client d'heure) internet	
Protocole d'heure	NTP (RFC-1305)	
Adresse IP du serveur		
Fuseau horaire	(GMT) Heure de Greenwich : Dublin	-
Activer la fonction heur d'été	e	
Intervalle de mise à jour	- 30 s 💌	

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

Cliquez sur OK pour enregistrer ces paramètres.

3.8.6 Gestion

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

Maintenance du système >> Gestion

Parametres de gestior	1			
Contrôle d'accès pour la gestion		Paramétrage du port de gestion		
Activer la mise à jour à distance du firmware (FTP)		 Ports par défaut (Telnet: 23, HTTP: 80, FTP: 21) 		
📃 Autoriser la gestion à partir de l'internet		💿 Ports définis par l'utilisateur		
☑ Désactiver le PING en provenance de l'internet		Port Telnet	23	
Liste des accès		Port HTTP	80	
Liste IP	Masque de sous-réseau	Port FTP	21	
1 192.168.1.56 2 3	255.255.255.255 / 32 💌	Paramètres SNMP Activer l'agent SNMP Communauté pour GET Communauté pour SET Adr IP du gestionnaire Communauté notifié Adr IP de notification Temporisation des "traps"	public private public 10 secondes	

Autoriser la mise à jour à
distance du firmwareCliquez sur la case pour autoriser la mise à jour à distance du
firmware via le protocole de transfert de fichier (FTP).Autoriser la gestion à partirCochez la case pour autoriser les administrateurs système à

0K

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

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

de l'internet

3.8.7 Réinitialisation du système

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



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

3.8.8 Mise à jour du firmware

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

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

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

```
      Mise à jour du firmware

      Version actuelle du firmware :

      0.1. Cliquez sur "OK" pour lancer le serveur TFTP.

      0.2. Ouvrir l'utilitaire de mise à jour du firmware ou tout autre client TFTP.

      0.3. Contrôler que le nom du firmware est correct.

      0.4. Cliquez sur "Mettre à jour" dans la fenêtre du programme de mise à jour de firmware pour lancer la mise à jour.

      0.5. Après la mise à jour, le serveur TFTP s'arrête automatiquement.

      Voulez-vous mettre à jour le firmware ?
```

Cliquez sur OK. L'écran suivant apparaît.

Maintenance du système >> Mise à jour du firmware

Maintenance du système >> Mise à jour du firmware

Le serveur TFTP est actif. Veuillez exécuter un programme de mise à jour de firmware pour mettre à jour le firmware du routeur. Le serveur s'arrêtera automatiquement à la fin de la mise à jour.

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

3.9 Diagnostics

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

3.9.1 Connexion WAN

Cliquez sur **Diagnostics**, puis sur **Diagnostics PPPoE/PPPoA** pour ouvrir la page web suivante.

Diagnostics >> Connexion WAN

Diagnostics PPPoE/PPPoA	Actualiser
Mode/état de l'accès à haut débit	
Accès à l'internet	>> Appel PPPoE/PPPoA
WLAN IP Address	
Abandon de la connexion	>> Abandoner PPPoE/PPPoA

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 est inactive, "" est affiché.
Adresse IP WAN	Adresse IP WAN pour la connexion active.
Appel PPPoE ou PPPoA	Cliquez sur cette option pour que routeur établisse une connexion PPPoE ou PPTP.

3.9.2 Trigger de sortie

Cliquez sur Diagnostics, puis sur Trigger de sortie pour ouvrir la page web.

Diagnostics >> Trigger de sortie		
En-tête de paquet ayant déclenché la co	onnexion	Actualiser
Format hexadécimal:		
00 50 7F 87 14 78-00 0E A	6 2A D5 A1-08 00	
45 00 00 43 15 79 00 00-7 AC 10 03 12 04 13 00 35-0 00 01 00 00 00 00 00 00 00-0 65 72 07 68 6F 74 6D 61-6 01 00 01 00 00 00 00 00-0	F 11 B5 5C CO A8 01 0A 00 2F C7 38 49 9F 01 00 9 6D 65 73 73 65 6E 67 9 6C 03 63 6F 6D 00 00 0 00 00 00 00 00 00 00	
Format décodé:		
192.168.1.10,1043 -> 172. Pr udp HLen 20 TLen 67	16.3.18,domain	

Refresh

Click it to reload the page.

3.9.3 Table de routage

Diagnostics >> Afficher la table de routage

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

```
      Table de routage actuellement active
      Actualiser

      Key: C - connected, S - static, R - RIP, * - default, ~ - private
      C

      C~
      192.168.1.0/
      255.255.255.0 is directly connected, IFO
```

Actualiser

Cliquez sur ce lien pour recharger la page.

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

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

Diagnostics >> Af	ficher la table ARP		
Table ARP Etherne	t	<u>Effacer</u> <u>Actualiser/Rafraichir</u>	
IP Address	MAC Address	▲ ■	
192.168.1.10	00-0E-16-21-D5-11		
		<u>▼</u>	

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

3.9.5 Table DHCP

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

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

Diagnostics >> Afficher les adresses IP attribuées par DHCP

DHCP s	erver: Running				1
Index 1	IP Address 192.168.1.1	MAC Address 00-50-7F-87-14-78	Leased Time ROUTER IP	HOST ID	
2	192.168.1.10	00-0E-A6-2A-D5-A1	0:00:03.850	ok-leegjyiy075u	

Actualiser

Cliquez sur ce lien pour recharger la page.

3.9.6 Table des sessions actives NAT

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

Diagnostics >> Table des sessions NAT		
Table des sessions actives NAT		Actualiser
Private IP :Port #Pseudo Port	Peer IP :Port Ifno Statu	3

Adr. IP :port privés	Indique l'adresse IP source et le port du PC local.				
#Pseudo-port	Indique le port temporaire du routeur utilisé pour la fonction NAT.				
Adr. IP :port homologue	Indique l'adre	sse IP de destination et le port de l'hôte distant.			
Ifno	Affiche le numéro représentatif de différentes interfaces.0:LAN1~2:ISDN3:WAN4 ou above :VPN				
État	Les valeurs d' 0: 1: 2: 3: 4: 5: 6:	état sont les suivantes : autre état TCP TCP fin incoming TCP fin out TCP fin closing TCP syn TCP syn,ack TCP ack			
Actualiser	Cliquez sur ce	lien pour recharger la page.			

3.9.7 Diagnostic par « ping »

Cliquez sur l'option **Diagnostic par ping** du menu **Diagnostics.** La page suivante apparaît. Diagnostic >> Diagnostic de Ping

Diagnostic de Ping	
Ping: Hôte / IP 🔽 Hôte / IP Passerelle	Adresse IP:
Résultat DNS	effacer
	<u>^</u>
	<u>~</u>

Ping vers	Choisissez la destination du ping dans la liste déroulante.
Adresse IP	Tapez l'adresse IP de l'hôte/IP auquel vous voulez envoyer le ping.
Exécuter	Cliquez sur ce bouton pour envoyer le ping. Le résultat est affiché sur l'écran.

3.9.8 Surveillance des flux de données

Cette page affiche le déroulement du processus de surveillance et permet de définir une fréquence d'actualisation des données. Les adresses IP de cet écran sont configurées dans la gestion de la bande passante. Vous devez définir une limitation de la bande passante IP et une limitation des sessions IP avant d'activer la surveillance. Sinon, une boîte de dialogue apparaît pour vous inviter à le faire.

Gestion de la bai	nde passante >>	Limite de session
-------------------	-----------------	-------------------

Limite de :	session
	Activer O Désactiver
	Nombre maximum de sessions: 100
	Liste des limitations
	Index Première IP Dernière IP

Cliquez sur l'option **Surveillance des flux de données** du menu **Diagnostics** pour ouvrir la page web suivante.

Diagnostics >> Surveillance du flux de données

_				
6	Activor	la cumunillanno.	due fluise	do donnáoc
	ALUVEL	ia suiveillallice.	uu nux	ue uonnees

Trié par	: IP	۲ I	ntervalle d	l'actualis	ation: 5	~			Page:	1 🗸		<u>Raf</u>	raichir
Index	Adresse IP	Tau	x d'émiss	ion (TX,	Kbps)	Taux	de rece	ption ((RX, Kb	ps)	Sessio	ons	Action

Remarque: 1. Cliquer sur « bloquer » pour empécher le PC spécifié de naviguer sur Internet durant 5 minutes.

2. L'IP bloquée par le routeur est affichée en rouge, et dans la colonne session sera affiché le temps restant durant lequel l'IP spécifiée sera bloquée.

Activer la surveillance des Cochez cette case pour activer cette fonction. flux de données

Trié Utilisez la liste déroulante pour choisir un critère de tri des données.



Fréquence d'actualisation Utilisez la liste déroulante pour choisir la fréquence d'actualisation des données.

Intervalle d'actualisation: 5 💌

5	
10	
15	
30	

Actualiser	Cliquez sur ce lien pour actualiser manuellement la page.				
Index	Affiche un numéro d'ordre.				
Adresse IP	Affiche l'adresse IP de l'équipement surveillé				
Débit d'émission (kbit/s)	Affiche la vitesse d'émission de l'équipement surveillé.				
Débit de réception (kbit/s)	Affiche la vitesse de réception de l'équipement surveillé.				
Sessions	Affiche le nombre de sessions specifies dans la page Limitation des sessions.				
Action	Bloquer – Empêcher le PC spécifié d'accéder à l'internet pendant 5 mintes. Débloquer –L'éauipement spécifié sera débloqué dans cinq				

minutes. Le temps restant est affiché dans la colonne Sessions.



3.9.9 Trace route

Diagnostic >> Trace route

Cliquez sur l'option **Trace route** du menu **Diagnostics** pour ouvrir la page web suivante. Cette page vous permet de retracer le chemin parcouru par les informations du routeur jusqu'à l'hôte. Tapez l'adresse IP de l'hôte dans la zone de saisie et cliquez sur **Exécuter**. Le résultat est affiché sur l'écran.

Hôte / Adresse IP:	Lancer
Résultat	Effacer
	~

Hôte/adresse IP	Adresse IP de l'hôte
Exécuter	Cliquez sur ce bouton pour lancer l'opération « trace route ».
Effacer	Cliquez sur ce lien pour effacer le résultat

4 Application et Exemples

4.4 Création d'un LAN avec NAT

Un exemple de paramétrage par défaut avec la topologie correspondante est donné ci-dessous. Par défaut, le routeur Vigor a pour adresse IP privée 192.168.1.1 et comme masque de sous-ré seau 255.255.255.0. Le serveur DHCP intégré est activé et attribue à chaque hôte NAT local une adresse IP 192.168.1.x à partir de 192.168.1.10.



Vous pouvez adapter les paramètres à l'intérieur des rectangles rouge pour l'usage NAT.

LAN >> Paramètre général

Configuration du rése	au IP LAN	Configuration du serv	eur DHCP
?usage NAT 1re Adresse IP 1re Masque de sous∙	192.168.1.1 réseau 255.255.255.0	 Octiver le serveur Agent relais: ○ 1re sous-réseau Adresse IP de début 	Désactiver le serveur 2e sous-réseau 192.168.1.10
Utilisation du routage IF 2e adresse IP 2e masque de sous-r	 Activer Désactive 192.168.2.1 	nbr d'adresses du réservoir IP Adresse IP de la passer	50 relle 192.168.1.1
2e serveu	r DHCP de sous-réseau		
Contrôle de protocole R	IP Désactiver 💌	Adresse IP du serveu	r DNS
		Adresse IP primaire Adresse IP secondaire	

Pour utiliser un autre serveur DHCP du réseau à la place du serveur intégré au routeur Vigor, il vous faut modifier les paramètres comme indiqué ci-dessous.



Vous pouvez adapter les paramètres à l'intérieur des rectangles rouge pour l'usage NAT.

LAN >> Paramètre général

On affermation do afrecast TD (14)	Qfl
Configuration du reseau IP LAN	Configuration du serveur DHCP
?usage NAT	OActiver le serveur 💿 Désactiver le serveur
1re Adresse IP 192.168.1.1	Agent relais:
1re Masque de sous-réseau	◯ 1re sous-réseau
255.255.255.0	Adresse IP de début 192.168.1.10
Utilisation du routage IP 🔘 Activer 💿 Désactiver	nbr d'adresses du 50
2e adresse IP 192.168.2.1	Adresse IP de la passerelle
2e masque de sous-réseau	192.168.1.1
255.255.255.0	Adresse IP du serveur DHCP nour agent relais
2e serveur DHCP de sous-réseau	192.168.3.11
Contrôle de protocole RIP Désactiver 💌	Adresse IP du serveur DNS Adresse IP primaire Adresse IP secondaire

4.2 Mise à jour du firmware de votre routeur

Avant de mettre à jour le firmware de votre routeur, il vous faut installer les Router Tools. L'utilitaire de mise à jour du firmware fait partie des outils.

- 1. Mettez le CD du routeur dans votre lecteur de CD-ROM.
- 2. Sur la page web, cliquez sur le menu Utility.
- 3. Sur la page web Utility, cliquez sur **Install Now!** (sous la description SysLog) pour installer le programme correspondant.

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

Install Now!

- 4. Le fichier **RTSxxx.exe** est copié sur votre ordinateur. Rappelez-vous de l'endroit où est copié le fichier .exe.
- 5. Connectez-vous à **www.draytek.com** pour rechercher la version la plus récente du firmware de votre routeur.
- Cliquez sur Support Center >> Downloads. Recherchez le modèle de votre routeur et cliquez sur le lien. La fenêtre ci-dessous apparaît. Note: Brief introduction for Tools

Tools of Vigor						
Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	<u>hqx</u>	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	<u>hqx</u>	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	<u>zip</u>	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	<u>zip</u>	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	<u>zip</u>	0.65 MB
LPR	1.0	English	20/06/2005	Windows	<u>zip</u>	0.54 MB
TOP						

- 7. Choisissez les outils qui correspondent à votre système d'exploitation et cliquez sur le lien correspondant pour télécharger le firmware (fichier zip).
- 8. Décompressez le fichier zip.

9. Double-cliquez sur l'icône des outils du routeur. L'assistant de configuration apparaît.



- 10. Suivez les instructions qui s'affichent pour installer les outils. Enfin, cliquez sur **Finish** pour terminer l'installation.
- 11. À partir du menu **Démarrer**, sélectionnez **Programmes**, puis **Router Tools XXX** >> **Firmware Upgrade Utility**.

៉ DrayTek Firmware I	Ipgrade Utility 📃 🗖 🔀
Operation Mode Oupgrade Backup Setting Time Out(Sec.)	Router IP: Firmware file:
5 Port 69	Password: Abort Send

12. Tapez l'adresse IP de votre routeur, généralement 192.168.1.1.

13. Cliquez sur le bouton à droite de Firmware file. Recherchez les fichiers à télécharger. Vous trouverez deux fichiers dont les extensions diffèrent, **xxxx.all** (conserver les anciens paramètres personnalisés) et **xxxx.rst** (rétablir tous les paramètres par défaut). Choisissez l'un de ces fichiers.

៉ DrayTek Firmware I	Jpgrade Utility 📃 🗖 🔀
Operation Mode Ouggrade Backup Setting Time Out(Sec.) 5	Router IP: 192.168.1.1 Firmware file: C:\Documents and Settings\Carrie Password:
Port 69	Abort Send

14. Cliquez sur Envoyer.

🛳 DrayTek Firmware Upgrade Utility 📃 🗖 🗙		
Operation Mode	Router IP: 192.168.1.1 Firmware file:	
Time Out(Sec.)	C:\Documents and Settings\Carrie	
5 Port	Password:	
69 Sending	Abort Send	

15. La mise à jour du firmware est terminée.

Page laissée intentionnellement vierge.



Ce chapitre vous aidera à résoudre certains problèmes après l'installation du routeur et sa configuration. Veuillez suivre les étapes ci-dessous pour vérifier votre installation de base.

- Le matériel est-il installé correctement ?
- Les paramètres de connexion réseau de votre ordinateur sont-ils corrects ?
- Le routeur répond-t-il à un « ping » de votre ordinateur ?
- Les paramètres FAI sont-ils corrects ?
- Rétablissement des paramètres par défaut si nécessaire.

Si, après cela, le routeur ne fonctionne toujours pas normalement, contactez votre revendeur.

4.1 Le matériel est-il installé correctement ?

- 1. Vérifiez le branchement du câble d'alimentation et du câble WLAN/LAN. Reportez-vous à « **2.1 Installation du matériel** » pour plus de détails.
- 2. Allumez le routeur. Vérifiez que le voyant **ACT** clignote et que le voyant **LAN** est allumé.



3. Si tel n'est pas le cas, c'est que le matériel n'est pas installé correctement. Reportez-vous à « 2.1 Installation du matériel » pour réeffectuer l'installation.

4.2 Les paramètres de connexion réseau de votre ordinateur sont-ils corrects ?

Il se peut que la liaison ne s'établisse pas parce que les paramètres de connexion réseau sont incorrects. Si, après les vérifications de la section 5.1, la liaison ne s'établit toujours pas, vérifiez les paramètres de connexion réseau comme indiqué ci-après.

Cas de Windows



L'exemple vaut pour Windows XP. Pour les autres systèmes d'exploitation, reportez-vous aux exemples ou notes qui se trouvent sur le site **www.draytek.com**.

1. Dans la fenêtre Panneau de configuration, double-cliquez sur Connexions réseau.



2. Faites un clic droit sur Connexion au réseau local et cliquez sur Propriétés.



3. Sélectionnez Protocole internet (TCP/IP), puis cliquez sur Propriétés.

Général
Se connecter en utilisant :
Carte PCI Fast Ethernet à base Realtek RTL8139(A)
<u>C</u> onfigurer
Les composants sélectionnés sont utilisés par cette connexion :
 Client pour les réseaux Microsoft Partage de fichiers et d'imprimantes pour les réseaux Micr Protocole Internet (TCP/IP)
Installer Désinstaller Propriétés
Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Le protocole de réseau étendu par défaut qui permet la communication entre différents réseaux interconnectés.
Afficher une icône dans la Barre des tâches une fois connecté
OK Annuler

4. Sélectionnez Obtenir une adresse IP automatiquement et Obtenir une adresse de serveur DNS automatiquement.

Propriétés de Protocole Internet (TCP/I	P) ? X
Général	
Les paramètres IP peuvent être déterminés réseau le permet. Sinon, vous devez demar appropriés à votre administrateur réseau.	automatiquement si votre nder les paramètres IP
Obtenir une adresse IP automatiquem	ient
C Utiliser l'adresse IP suivante :	
Adresse [P :	
Masque de <u>s</u> ous-réseau :	
Passerelle par <u>d</u> éfaut :	
 Obtenir les adresses des serveurs DN 	S automatiquement
☐ ☐ Utiliser l'adresse de serveur DNS suiv.	ante :
Serveur DNS préféré :	
Serve <u>u</u> r DNS auxiliaire :	
	<u>Avancé</u>
	OK Annuler

Cas de MacOs

- 1. Double-cliquez sur l'icône MacOs du bureau.
- 2. Ouvrez le dossier Application et sélectionnez Réseau.
- 3. Sur l'écran **Réseau**, sélectionnez **Utilisation de DHCP** dans la liste déroulante Configuration IPv4.

<u> </u>		Netw	ork		
now All Dis	plays Sound	Network Startup Dis	k		
	Loc	ation: Automatic		;	
		Show: Built-in Ethe	rnet	•	
	TCP/IP	PPPoE AppleT	alk Proxies	Ethernet	
Config	ure IPv4:	Using DHCP		•	
IP .	Address:	192.168.1.10		Renew DH	CP Lease
Subn	et Mask: 2	255.255.255.0	DHCP Client II	D:	
	Router:	192.168.1.1		(If required)
DNS	Servers:				(Optional)
Search E	Domains:				(Optional)
IPv6	Address: fe	80:0000:0000:0000	:020a:95ff:fe8d	:72e4	
	,	Configure IPv6			(?)

4.3 Le routeur répond-t-il à un « ping » de votre ordinateur ?

L'adresse IP par défaut du routeur est 192.168.1.1. Vous pouvez vérifier l'état de la liaison avec le routeur en utilisant la commande « ping ». Ce qui importe c'est que l'ordinateur reçoive une réponse 192.168.1.1. Si tel n'est pas le cas, vérifiez l'adresse IP de votre ordinateur. Nous vous suggérons de paramétrer la connexion au réseau pour l'obtention automatique d'une adresse IP. (Voir la section 4.2)

Pour envoyer un ping au routeur, procédez de la manière décrite ci-après.

Cas de Windows

- 1. Ouvrez la fenêtre **Exécuter** à partir du **menu Démarrer**.
- 2. Tapez **command** (Windows 95/98/ME) ou **cmd** (Windows NT/2000/XP). La boîte de dialogue suivante apparaît.



- 3. Tapez ping 192.168.1.1 et appuyez sur [Entrée]. Si la liaison est bonne, la ligne « Reply from 192.168.1.1:bytes=32 time<1ms TTL=255 » apparaît.
- 4. Si cette ligne n'apparaît pas, vérifiez l'adresse IP de votre ordinateur.

Cas de MacOs (Terminal)

- 1. Double-cliquez sur l'icône MacOs du bureau.
- 2. Ouvrez le dossier **Application** et sélectionnez **Utilitaires**.
- 3. Double-cliquez sur **Terminal**. La fenêtre Terminal apparaît.
- 4. Tapez **ping 192.168.1.1** et appuyez sur [Entrée]. Si la liaison est bonne, la ligne **« 64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms** » apparaît.

$\Theta \Theta \Theta$	Terminal — bash — 80x24	
Last login: Sat Jar Welcome to Darwin! Uiger10:: drautek\$	n 3 02:24:18 on ttyp1	S
VIGOLID:~ ULUVCEK\$ DING 192 168 1 1 /1	92 168 1 1): 56 data bytes	
64 bytes from 192.1	.68.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 192.1	.68.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 192.1	.68.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 192.1	.68.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 192.1 ^C	.68.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
192.168.1.1 pir	ng statistics	
5 packets transmitt round-trip min/avg/ Vigor10:~ draytek\$	ed, 5 packets received, 0% packet loss /max = 0.697/0.723/0.755 ms	
00 0101		

4.4 Les paramètres FAI sont-ils corrects ?

Cliquez sur Accès à l'internet, puis vérifiez les paramètres FAI.



Pour les utilisateurs de PPPoE/PPPoA

Accès à l'internet >> PPPoE / PPPoA

- 1. Vérifiez que l'option Activer est sélectionnée.
- 2. Vérifiez que le **nom d'utilisateur** et **le mot de passe** ont bien les valeurs qui vous ont été données par votre **FAI**.

Client PPPoE/PPI	PoA OActiver	Configuration de l'accé	ès au FAI
Désactiver		Nom du FAI	
Paramètres du m	odem DSL	Nom d'utilisateur	
Canal multi-PVC	Canal 1 🛛 👻	Mot de passe	
VPI	8	Authentification PPP	PAP ou CHAP 🔽
VCI	35	🗖 Toujours actif	
Type d'encapsulat	ion	Délai d'inactivité	180 seconde(s)
Protocole	VC MUX V PPPoA V	Adresse IP fournie par FAI Alias de l'IP du	WAN
Modulation	Multimode 💌	Adr IP fixe O Oui O	Non (IP dynamique)
Mode pass-throu Pour LAN filai Remarque: si l'un lors de l'utilisation alors le routeur se qui servira uniquer	gh PPPoE re e de ces options est activée du protocole PPPoA, comportera comme un modem nent les clients PPPoE du LAN	 Adresse MAC par d Spécifier une adres Adresse MAC: 00 · 50 · 7F :8; Index(1-15) dans Horain , , , , , , , , , , , , , , , , , , ,	éfaut se MAC 7 . 14 . 79 re Configuration:

ΟK

Pour les utilisateurs de MPoA

1. Vérifiez que l'option Activer est sélectionné.

Accès à l'internet >>	MPoA (RFC1483/2684)
-----------------------	---------------------

Mode MPoA (RFC1483/2684)	
MPeA (RFC1483/2684)	Paramètres de réseau IP WAN
💿 Activer 🔘 Désactiver	O Obtenir une adresse IP automatiquement
Paramètres du modem DSL	Nom du routeur *
Canal multi-PVC Canal 2 👻	Spécifier une adresse IP
Encapsulation LLC IP en pont 1483	Alias de l'IP du WAN
VPI 8	Adresse IP 0.0.0.0
VCI 36	Masque de sous-réseau
Modulation Multimode 💙	0.0.0
	Adresse IP de la passerelle
Activer RIP	
Mode Pont	 * : Nécessaire pour certains FAI Adresse MAC par défaut Spécifier une adresse MAC Adresse MAC : 00 · 50 · 7F :87 · 14 · 79 Adresse IP du serveur DNS Adresse IP primaire

- 2. Vérifiez que tous les paramètres du **Modem DSL** ont bien les valeurs qui vous ont été données par votre FAI. Vérifiez notamment que le type d'encapsulation est le bon (il doit être identique à celui de l'**Assistant de démarrage rapide**).
- 3. Vérifiez que l'**adresse IP**, le **masque de sous-réseau** et **l'adresse IP de la passerelle** sont corrects (ces paramètres doivent être identiques aux valeurs fournies par votre FAI) si vous avez choisi **Spécifier une adresse IP**.

4.5 Rétablissement des paramètres par défaut si nécessaire

Parfois, on peut améliorer les choses en rétablissant les paramètres par défaut. Tentez une réinitialisation logicielle ou matérielle du routeur.



Attention : Si vous cliquez sur **Paramètres par défaut**, vous perdrez tous les paramétrages effectués jusqu'ici. Veillez à noter tous les paramètres utiles. Le mot de passe par défaut est vide.

Réinitialisation logicielle

Vous pouvez rétablir les paramètres par défaut de votre routeur à l'aide d'une page web.

Sélectionnez **Maintenance du système**, puis **Réinitialiser le système** sur la page web. L'écran suivant apparaît. Choisissez **Utilisation de la configuration par défaut** et cliquez sur **OK**. Au bout de quelques secondes, les paramètres usine sont rétablis.

Voulez-vous réinitialiser votre routeur ?
Otilisation de la configuration actuelle
O Utilisation de la configuration par défaut

Réinitialisation matérielle

Le routeur étant en marche (voyant ACT clignotant), appuyez sur le bouton **Factory Reset** en le maintenant enfoncé pendant plus de 5 secondes. Lorsque le voyant **ACT** commence à clignoter rapidement, relâchez le bouton. Le routeur redémarre avec les paramètres par défaut.



Après avoir rétabli les paramètres par défaut, vous pouvez reconfigurer le routeur.

4.6 Contacter votre revendeur

Si le routeur ne fonctionne toujours pas correctement, contactez votre revendeur. Pour d'autres questions, n'hésitez pas à envoyer un courriel à support@draytek.com.