Routeur Internet, point d'accès sans fil 802.11g – 54 Mbps avec Modem ADSL, switch 4 ports et serveur VPN intégrés

Manuel de l'utilisateur

(Modèle WRM54)

Version 1.01 – Janv. 2004

Copyright

Marques déposées

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

Déclaration de conformité CE

Cet équipement est conforme aux exigences relatives à la compatibilité électromagnétique définies par la norme EN 55022/A1 Classe B, et EN 50082-1. Ce produit a été testé avec succès et satisfait aux exigences de protection définies dans la directive européenne 89/336/EEC.

Sommaire

Chapitre 1 Introduction

Félicitations pour l'acquisition de ce modem/routeur ADSL sans fil Comet Labs. Ce produit est conçu pour les besoins des particuliers et des petites entreprises. Facile à installer et à configurer, même pour une personne non technique, il fournit une solution complète pour surfer sur internet. Toutes les instructions pour installer et configurer ce produit se trouvent sur ce manuel. Avant d'installer et d'utiliser ce produit, veuillez lire ce manuel attentivement pour pouvoir exploiter au maximum toutes les fonctionnalités de ce produit.

Caractéristiques et fonctionnalités

Fonctions de base du routeur

- **Switch Ethernet 10/100 Mbps à auto négociation**
  4 ports Ethernet switchés 10/100 à auto négociation.
- **Partage d'imprimante**
  Intègre un serveur d'impression, permettant ainsi à tous les ordinateurs du réseau de partager une seule imprimante.
  Port USB intégré pour connecter une imprimante USB.
- **Connexion WAN supportée**
  Le routeur supporte: Ethernet Over ATM (RFC 1483 Bridged) sans le NAT, Ethernet Over ATM (RFC 1483 Bridged) avec le NAT, IP over ATM (RFC 1483 Routed), Classical IP over ATM (RFC 1577), PPP over ATM (RFC 2364), PPP over Ethernet (RFC 2516).
- **Firewall**
  Tous paquets indésirables provenant d'intrus extérieur sont bloqués pour protéger votre réseau intranet.
- **Intègre un serveur DHCP**
  Tous les ordinateurs du réseau peuvent obtenir automatiquement une adresse TCP/IP depuis ce produit.
- **Configuration par interface web**
  Le routeur peut-être paramétré depuis n'importe quel ordinateur du réseau avec un navigateur web comme Netscape ou Internet Explorer.
- **Supporte les serveurs virtuels**
  Permet aux utilisateurs d'Internet d'accéder à vos serveurs web, ftp et autres services de votre intranet.
- **Applications spéciales**
  L'utilisateur peut définir des règles pour supporter des applications spéciales nécessitant de multiples connexions, comme les jeux en réseau, la visioconférence, la téléphonie par

Internet, etc. Le routeur détecte automatiquement le type d'application puis ouvre les ports concernés.

- **DMZ**

  Permet d'exposer un ordinateur directement sur Internet: cette fonction est utilisée quand les règles de Spécial Application sont insuffisantes pour permettre à une application de fonctionner correctement.

- **Statistiques du port WAN**

  Pertmet de visualiser les paquets entrant et sortant.

Fonctions du mode sans fil

- **Connexion réseau sans fil haute vitesse**

  Taux de transfert jusqu'à 54 Mbps incorporant une transmission de type OFDM (Orthogonal Frequency Division Multiplexing).

- **Roaming / Déplacement**

  Permet la connexion automatique au point d'accès offrant la meilleure qualité de signal de communication en mode IEEE 802.11b (11M) et IEEE 802.11g (54M) WLAN.

- **Compatible IEEE 802.11b (11M) et IEEE 802.11b+ (22 Mbps)**

  Permet de multiple connexion avec d'autres fabricants.

- **Compatible IEEE 802.11g (54M)**

  Permet de multiple connexion avec d'autres fabricants.

- **Auto fallback / Repli automatique de la vitesse**

  Le taux de transfert se replie automatiquement de 54M, 48M, 36M, 24M, 22M, 18M, 12M, 11M, 6M, 5.5M, 2M à 1Mbps en mode 802.11g suivant la qualité du signal.

  Le taux de transfert se réduit automatiquement de 11M, 5.5M, 2M, 1M en mode 802.11b suivant la qualité du signal.

Fonctions de sécurité

- **Filtre par paquets**

  Le **Filtre par paquets** vous permet de contrôler l'accès à un réseau en analysant les paquets entrants et sortant, les laisse passer ou les bloque suivant l'adresse IP de la source et du destinataire.

- **Filtre par Nom De Domaine**

  Permet de contrôler l'accès à des adresses URL spécifiques.

- **Blocage d'adresse URL (Uniform Resource Locator)**

  Permet de bloquer des centaines de sites web simplement à partir de mots clé.

- **Serveurs VPN**

  Le routeur dispose de 3 serveurs VPN : IPSEC (Dynamic VPN), PPTP, et L2TP.

- **VPN Pass-through / Réseau privé virtuel traversant**

Le routeur supporte aussi le VPN pass-through. C'est à dire qu'il laisse passer les paquets encryptés générés par d'autres logiciels ou matériels qui existent au sein de votre réseau local.

NOTE : Si vous utilisez les protocoles ESP pour établir la connexion VPN traversant, vous devez définir une règle de filtrage autorisant l'ouverture du port 500. Pour d'autres protocoles tels que PPTP, vous devez également vous assurer que les ports nécessaires au Tunnel traversant sont également ouverts sur votre routeur Comet Labs.

- **802.1X**

  Quand cette fonction 802.1X est activée, l'utilisateur sans fil doit s'authentifier à ce routeur avant de pouvoir se connecter au réseau.
- **SPI**

  Quand le mode SPI est activé, le routeur vérifiera tous les paquets entrant pour détecter si les paquets sont valides.
- **Détection des attaques DoS**

  Quand cette fonction est activée, le routeur détectera et enregistrera toutes les attaques DoS provenant d'Internet.

Fonctions avancées

- **Horloge Système**

  Permet de synchroniser l'horloge système avec un serveur d'horloge réseau.
- **Envoi d'alertes par email**

  Le router peut envoyer des informations (fichier de log, par exemple) par email.
- **Dynamic DNS (DynDNS)**

  Pour le moment, le routeur dispose de 3 serveurs dyndns : DynDNS.org, TZO.com et dhs.org.
- **SNMP**

  Supporte SNMP version V1 et V2c.
- **Table de Routage**

  Le routeur supporte les routes statiques et 2 types de routes dynamiques: RIP1 et RIP2.
- **Règles programmées**

  Les utilisateurs peuvent contrôler certaines fonctions, comme les Serveurs Virtuels ou le Filtrage par paquets: ils peuvent créer des plages horaires d'accès ou de blocage à ces services.

Autres Fonctions

- **UPNP (Universal Plug and Play)**

  Le routeur supporte cette fonction. Les Applications: X-box, MSN Messenger.

Contenu de l'emballage

- Modem/Routeur ADSL sans fil
- CD-ROM d'installation
- Adaptateur secteur
- Câble réseau Fast Ethernet catégorie 5 UTP
- Câble ADSL

Chapitre 2 Installation Matériel

2.1 Identification des éléments externes

2.1.1. Face avant

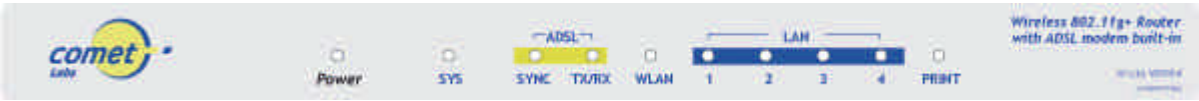


Figure 2-1 Face Avant

Témoins lumineux :

LED	Fonction	Couleur	Status	Description
POWER	Témoin d'alimentation	Vert	Allumée	Le routeur est bien alimenté
SYS	Témoin Système	Vert	Clignote	Le routeur fonctionne correctement
SYNC	Témoin Synchronisation ADSL	Vert	Allumée	La ligne ADSL est correctement connectée
			Clignote	Le routeur est en train de se connecter à la ligne ADSL
TX/RX	Témoin Transmission/Réception sur l'ADSL	Vert	Clignote	La ligne ADSL émet ou reçoit des paquets
WLAN	Témoin de l'Activité sans fil	Vert	Clignote	émet ou reçoit des paquets sur le réseau sans fil
L1~L4	Témoin connexion réseau	Vert	Allumée	Un ordinateur est connecté.
			Clignote	Le port envoie ou reçoit des paquets
Print	Témoin de l'activité du serveur d'impression	Vert	Clignote	émet ou reçoit des paquets sur le port d'impression USB

2.1.2. Face arrière

Figure 2-2 Face arrière

Ports:

Port	Description
5VDC	Connecteur d'alimentation: DC 5V, 1.5A (minimum)
ADSL	Connecteur pour la ligne ADSL
Port 1-4	Connecteurs réseau (ordinateurs et autres périphériques réseau)
USB	Connecteur pour l'imprimante USB

2.2 Procédure d'installation du matériel

1. Définissez l'endroit ou vous allez placer le modem/routeur ADSL sans fil

Vous pouvez placer le routeur sur une table, une surface plane ou le fixer au mur. Pour une performance optimale, placez le routeur au centre de votre bureau (ou de votre maison), dans un endroit loin de toutes sources d'interférences, comme un mur en métal ou un four à micro-ondes. Cet endroit doit aussi être proche d'une source d'alimentation électrique et connexion réseau.

2. Paramétrage des connexions réseau

a. Connexion réseau filaire: connectez un câble réseau depuis la carte réseau de votre ordinateur vers un des ports réseau du routeur.

b. Connexion réseau sans fil: placez-vous dans un endroit stratégique pour obtenir le meilleur gain de réception/transmission.

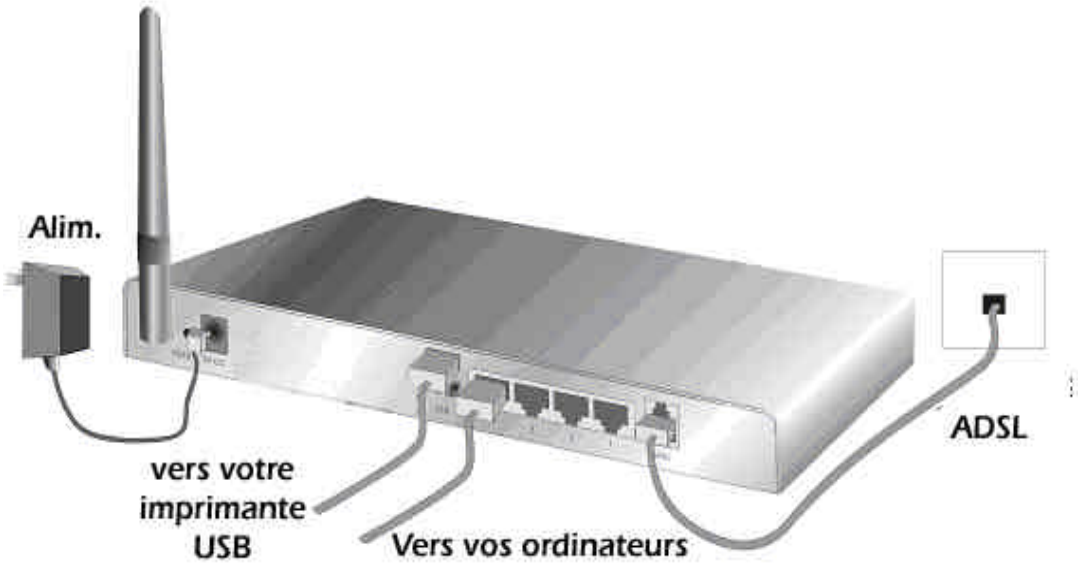


Figure 2-3 Paramétrage des connexion LAN et WAN.

3. Paramétrage de la connexion ADSL

Branchez le câble téléphonique sur le port ADSL puis l'autre extrémité à votre prise téléphonique

Figure 2-3 montre la connexion WAN.

4. Connectez ce produit à votre imprimante.

Utilisez le câble imprimante (livré avec votre imprimante) pour connecter votre imprimante au port imprimante du routeur.

5. Mise en route

Branchez l'adaptateur secteur, le routeur se met en route tout seul, il n'existe pas d'interrupteur marche/arrêt. En fonctionnement normal, la LED SYS clignote par intervalle d'une seconde.

Chapitre 3 Paramétrage réseau et Installation réseau

Pour utiliser ce produit de manière efficace, vous devez configurer correctement les paramètres réseau de votre ordinateur.

3.1 Configurez correctement vos paramètres réseau

L'adresse IP par défaut du routeur est **192.168.0.1** et son masque de sous réseau est **255.255.255.0**. Ces paramètres peuvent être modifiés à votre guise, mais ce sont les valeurs par défaut qui seront utilisées dans ce manuel. Si le protocole TCP/IP de votre ordinateur n'est pas encore configuré, veuillez vous référencer à l'**Annexe A** de ce manuel.

Par exemple,

1. Configurez l'adresse IP comme **192.168.0.2**, masque de sous réseau **255.255.255.0** puis la passerelle ou routeur comme 192.168.0.1,
   ou tout simplement,
2. Configurez votre ordinateur pour obtenir automatiquement une adresse IP, via DHCP.

Après l'installation du protocole TCP/IP, vous pouvez utiliser la commande **ping** pour vérifier si votre ordinateur s'est connecté correctement au routeur. Voir exemple ci-dessous:

Ping 192.168.0.1

Si vous avez le message suivant:

Envoi d'une requête 'ping' sur 192.168.0.1 avec 32 octets de données:

Réponse de 192.168.0.1 : octets=32 temps<10 ms TTL=64

La communication entre votre ordinateur et le routeur est correctement établie.

Sinon vous obtenez ce genre de message :

Envoi d'une requête 'ping' sur 192.168.0.1 avec 32 octets de données:

Impossible de joindre l'hôte de destination.

Dans ce cas, vous devez vérifier les points suivants :

1. Est-ce que le câble réseau est correctement connecté entre votre ordinateur et le routeur ?

   Note: La LED **LAN** du routeur et la LED **Link** de la carte réseau de votre ordinateur doivent être allumées.

2. Est-ce que le protocole TPC/IP de votre ordinateur est correctement configuré?

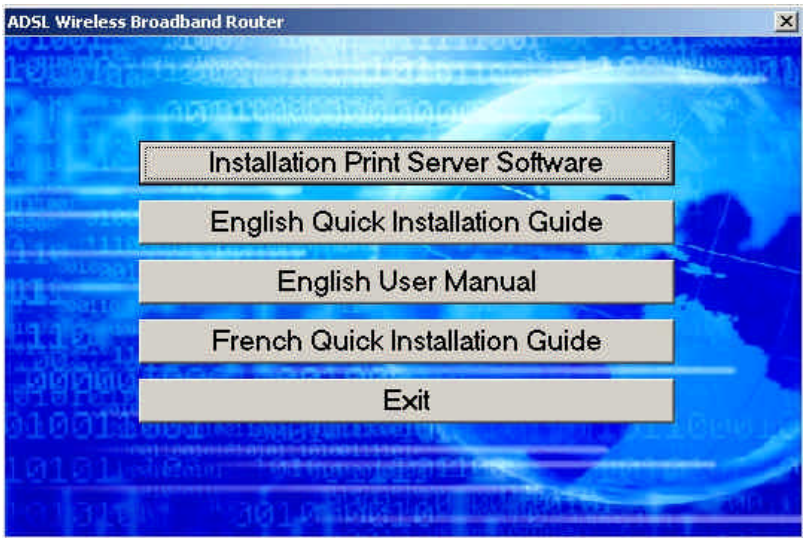
   Note: Si l'adresse IP du routeur est **192.168.0.1**, alors l'adresse IP de votre ordinateur doit être **192.168.0.X** (où **X** est différent de 1) et la passerelle par défaut (ou adresse du routeur) doit être **192.168.0.1**.

3.2 Installation logiciel

Ignorez cette section si vous ne désirez pas utiliser la fonction « Serveur d'impression » de ce routeur.

Note: Si vous êtes un utilisateur de Windows 2000 et de Windows XP, veuillez vous référencer au chapitre 5 – Serveur d'impression – 5.3 Windows 2000 et Windows XP. Il n'est pas nécessaire d'installer un programme de serveur d'impression.

Etape 1: Insérez le CD-ROM d'installation dans votre lecteur de CD-ROM. La fenêtre ci-dessous apparaît automatiquement. Si ce n'est pas le cas, double cliquez sur l'icône « **Install.exe** » se trouvant sur le CD-ROM d'installation.



Etape 2: Cliquez sur le bouton **Installation Print Server Software**. Puis cliquez sur le bouton **Next**.

Etape 3: Sélectionnez le dossier de destination puis cliquez sur le bouton **Next**. Le logiciel commence à s'installer.

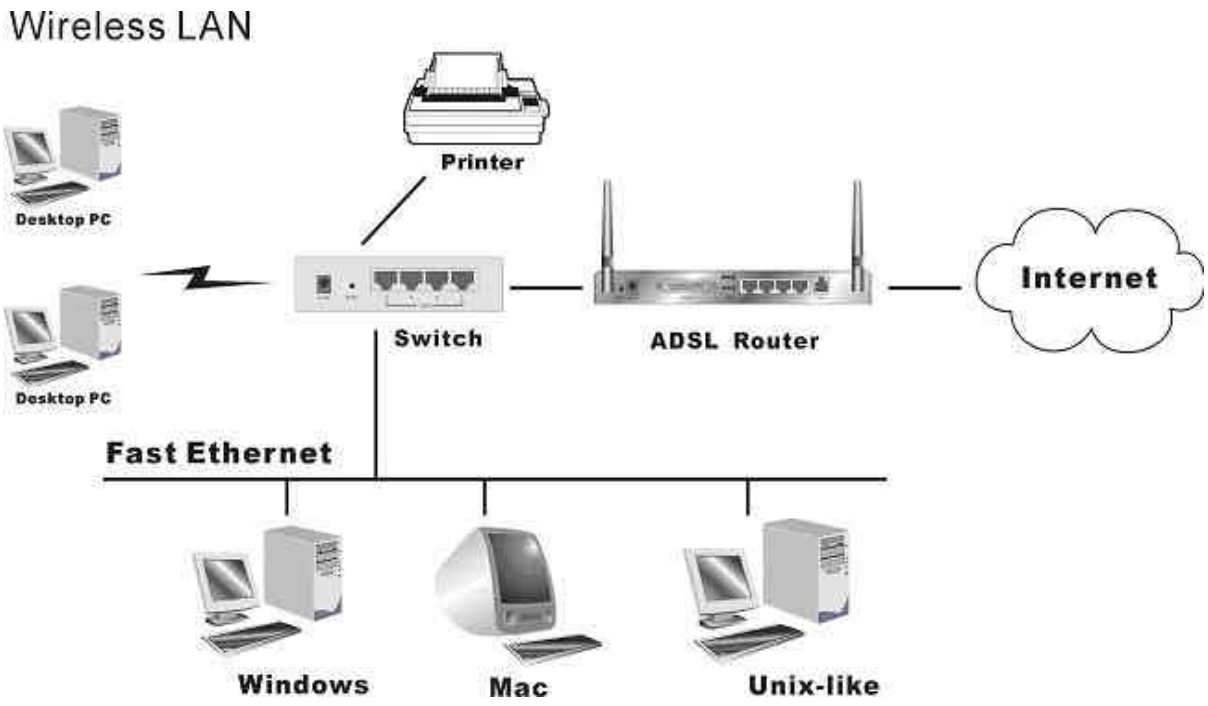
Etape 4: Dès que cette fenêtre apparaît, cliquez sur le bouton **Finish**. Sélectionnez le bouton pour redémarrer votre ordinateur puis cliquez sur le bouton **OK**.

Etape 5: Après avoir redémarrer votre ordinateur, la procédure d'installation est terminée.

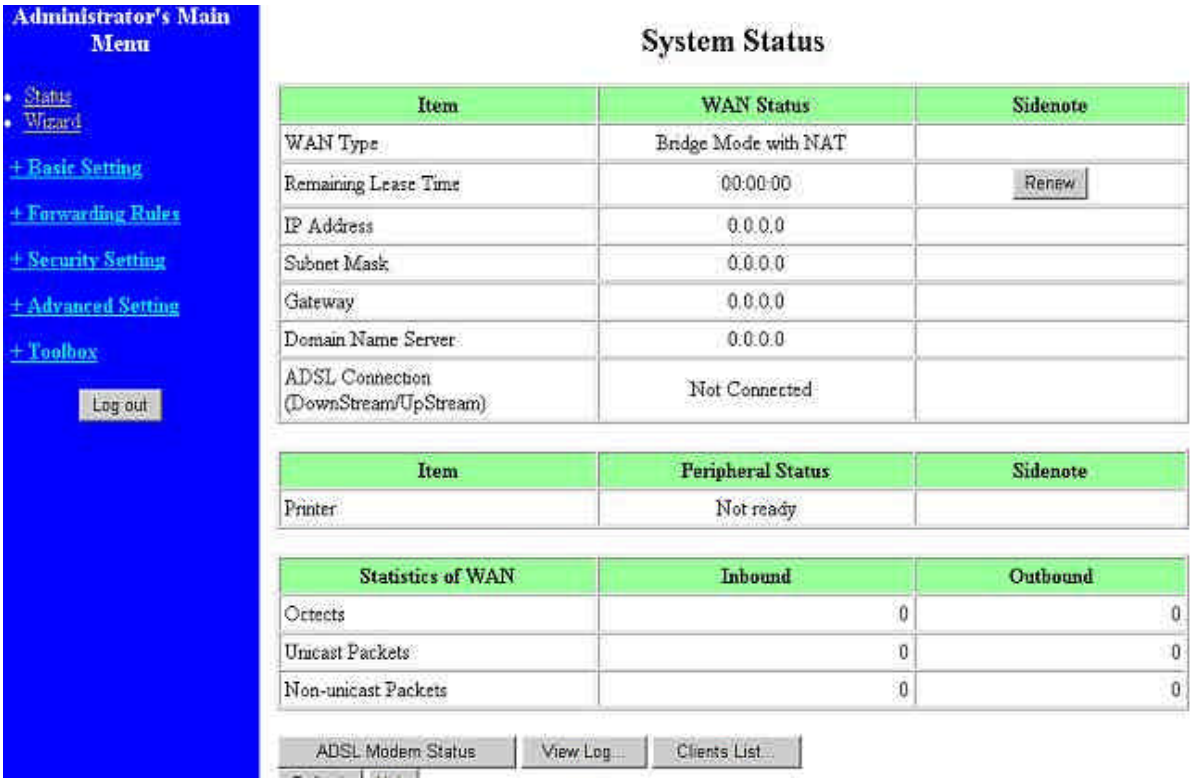
Vous pouvez maintenant paramétrer le routeur pour accéder à Internet (Chapitre 4) et puis paramétrer le serveur d'impression (Chapitre 5).

Chapitre 4 Configuration du modem/routeur ADSL sans fil

La configuration de ce produit se fait par une interface web, telle que Netscape Navigator ou Microsoft Internet Explorer. Vous pouvez donc paramétrer le routeur à partir de n'importe quelle machine Windows, Unix ou Macintosh.



4.1 Démarrage

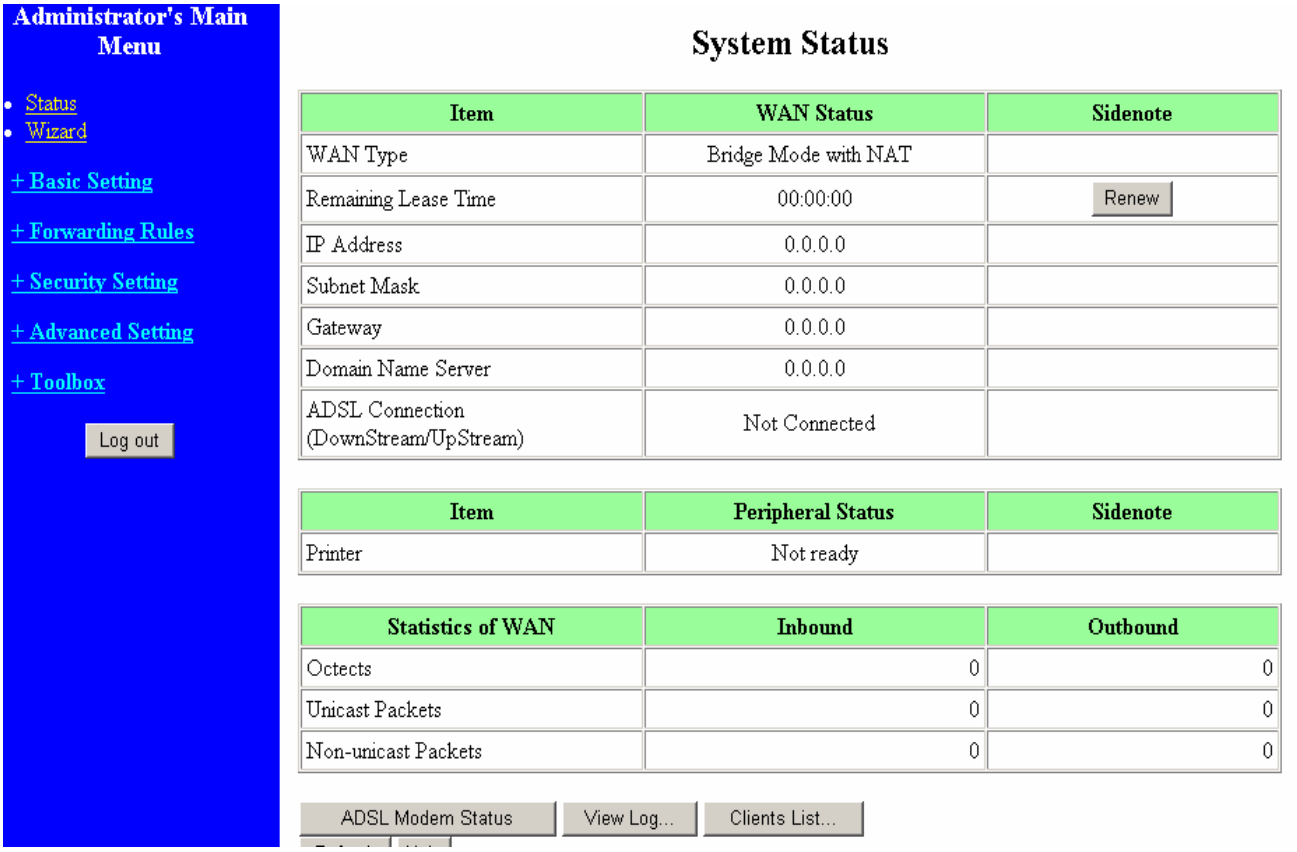


Démarrez votre navigateur Internet, **désactiver le Proxy** si vous utilisez un serveur Proxy ou **ajouter l'adresse IP du routeur dans la liste des exceptions**. Avec certain navigateur web, tel qu'Internet **Explorer**, il suffit de cocher la case «**Ne pas utiliser de serveur Proxy pour les adresses locales**». Puis, tapez l'adresse IP du routeur dans la partie **Adresse** de votre navigateur web, par exemple : **http://192.168.0.1**.

Dès que la connexion est effectuée, vous accédez à l'interface web utilisateur du routeur. Il existe 2 types d'interface web: pour l'utilisateur en général et pour l'administrateur. Système.

Pour se connecter en tant qu'**Administrateur**, entrez le mot de passe système (le mot de passe par défaut est **admin**). Dans la zone **System Password**, puis cliquez sur le bouton **Log in**. Si le mot de passe est correct, la page web change d'apparence et passe mode **Administrateur**.

4.2 Status



Cette option permet de vérifier l'état du routeur:

A. Etat du port WAN :

Si le port WAN est configuré pour obtenir une adresse IP dynamiquement, un bouton **Renew** ou **Release** apparaît dans la colonne **Sidenote**. Vous pouvez cliquer sur ce bouton pour libérer manuellement l'adresse IP ou pour obtenir une nouvelle adresse IP.

B. Etat de l'imprimante :

L'état de l'imprimante peut être: ***"Ready"*** (prêt), ***"Not ready"***(pas prêt), ***"Printing…(impression)"***, and ***"Device error"***(erreur matériel).

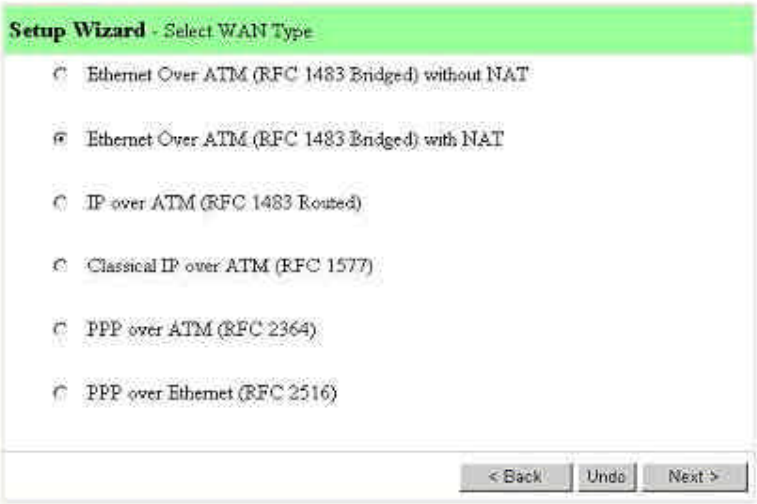
*Quand une impression est en cours, un bouton "**Kill Job**" apparaît dans la partie **Sidenote**. Vous pouvez cliquer sur ce bouton pour arrêter l'impression en cours.*

C. Statistiques du port WAN:

permet de voir le nombre de paquets entrant et sortant

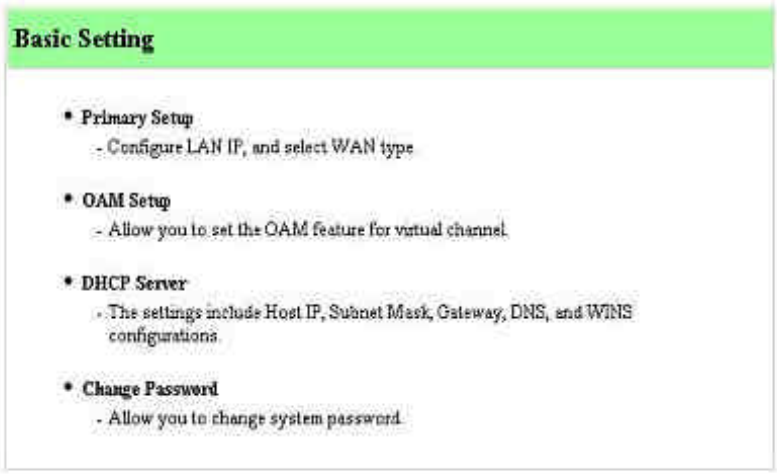
4.3 Wizard – Assistant de configuration

Le **Setup Wizard** vous guidera pas à pas dans la configuration basique du routeur. Cliquez sur le bouton '**Next**'.

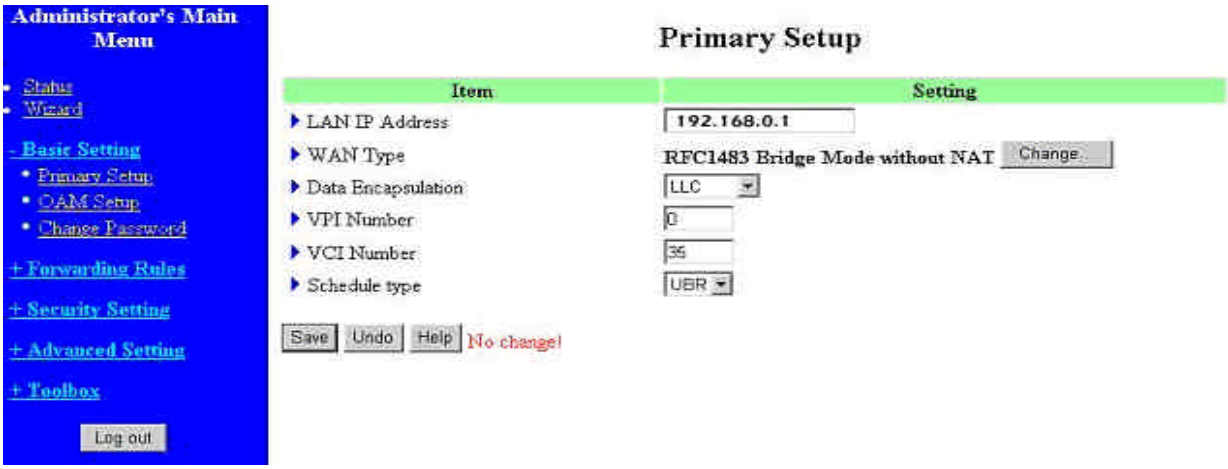


Setup Wizard - Select WAN Type: Pour plus de détails, voir chapitre **4.4.1 primary setup.**

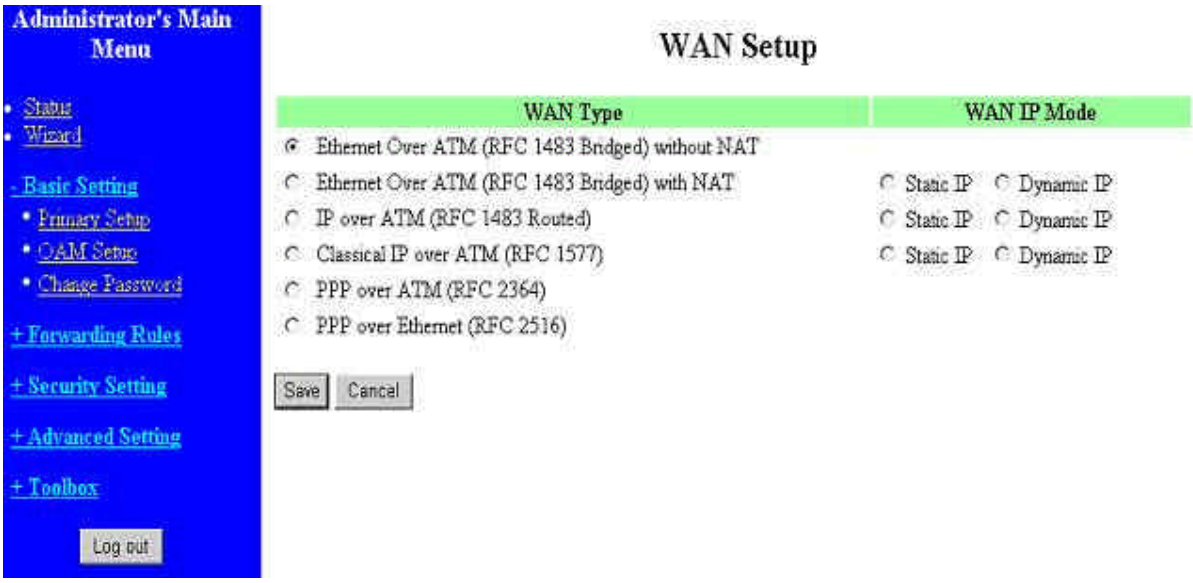
4.4 Basic Setting



4.4.1 Primary Setup – WAN Type



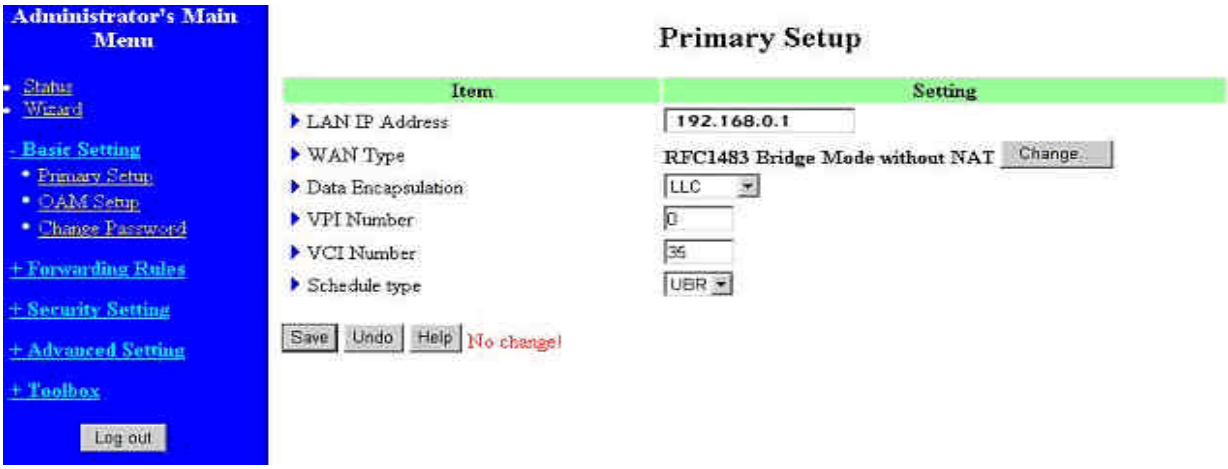
Cliquez sur le bouton **"Change"**



La bonne configuration de cette page est primordiale pour le bon fonctionnement du routeur. Sélectionnez correctement l'option WAN Type avant de commencer. Référez-vous à **l'Annexe d** de ce manuel pour connaître le type d'encapsulation utilisé par chaque FAI (Fournisseur d'Accès Internet) tel que : Wanadoo, Free, Liberty Surf, etc…

1. ***LAN IP Address***: Adresse IP locale du routeur. Les ordinateurs de votre réseau doivent utiliser l'adresse IP LAN du routeur en tant que leur passerelle par défaut. Vous pouvez la modifier si besoin.
2. ***WAN Type***: Type de protocole WAN utilisé par votre FAI (Fournisseur d'Accès Internet). Vous pouvez cliquer sur le bouton **Change** pour sélectionner le bon protocole parmi les 6 proposés. Pour connaître le type de protocole utilisé par votre FAI, référencez-vous à **l'Annexe d** de ce manuel :
   A. Ethernet Over ATM (RFC 1483 Bridged) without NAT
   B. Ethernet Over ATM (RFC 1483 Bridged) with NAT
   C. IP over ATM (RFC 1483 Routed).
   D. Classical IP over ATM (RFC 1577).
   E. PPP over ATM (RFC 2364).
   F. PPP over Ethernet (RFC 2516).
3. ***Data Encapsulation***: 2 types d'encapsulation sont supportés: **LLC** et **VC-MUX**. Votre FAI fournie ce genre d'information (voir aussi **l'annexe d** de ce manuel). Dès que vous avez terminé le paramétrage, vous pouvez cliquer sur le bouton '**Advanced Settings**' pour configurer d'autres options.

4.4.1.1 Ethernet Over ATM (RFC 1483 Bridged) without NAT



Cette option désactive la fonction NAT, le produit devient un pur pont (un simple modem ADSL) entre votre LAN et le WAN, tous les ordinateurs de votre LAN doivent avoir une IP publique. Si vous activez le NAT, vous devez configurer les paramètres IP WAN suivant :

WAN IP Address, WAN Subnet Mask, WAN Gateway, et Primary/Secondary DNS

Votre FAI vous fournit ces informations

VPI/VCI Numbers:

Valeurs utilisées par votre FAI. Fournit par votre FAI, sinon voir **Annexe d** de ce manuel.

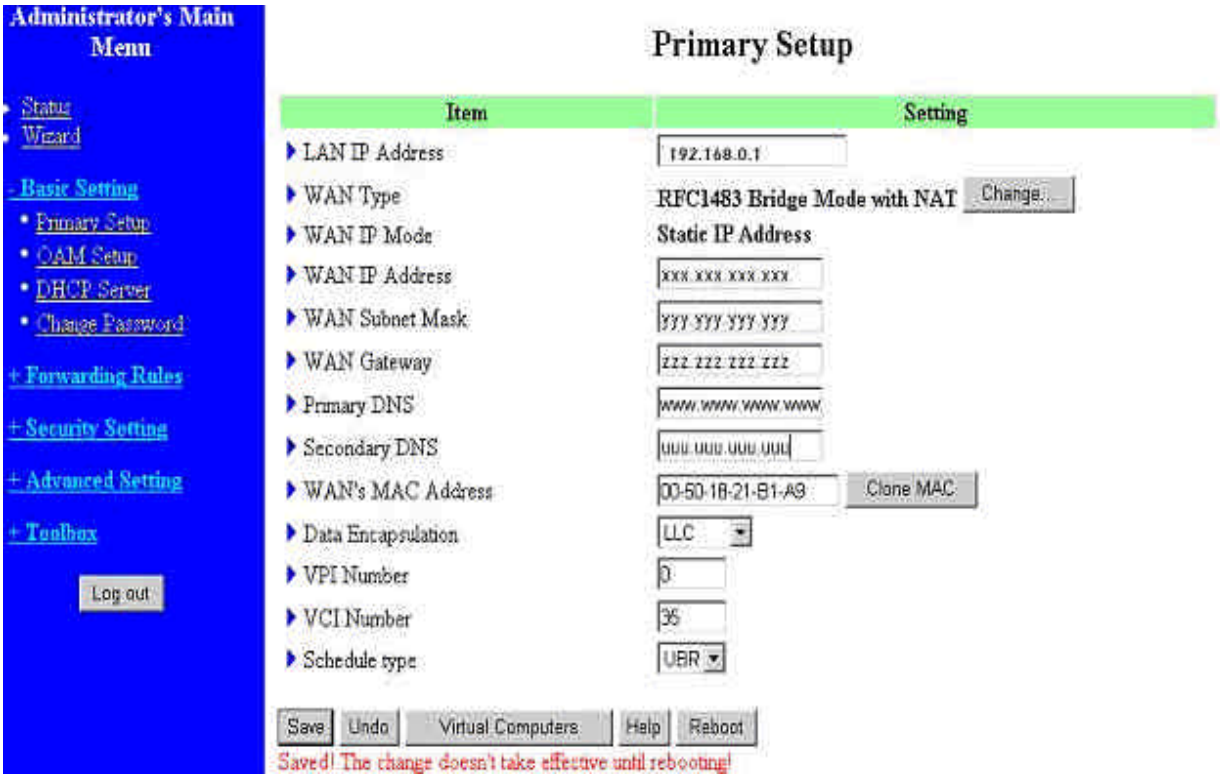
Quelques exemples en France :

- La plupart des FAIs en France utilisent les valeurs 8 et 35
- Si vous êtes connecté via Free en mode dégroupé les valeurs sont 8 et 36
- Si vous utilisez certaines autres lignes, les valeurs peuvent être 8 et 67

Schedule Type:

Paramètres du type de trafic ADSL. Ce produit supporte **UBR** (Un-specified bit rate) et **CBR** (Constant bit rate). Dès que vous avez fini, cliquez sur le bouton **Save** pour sauvegarder les changements dans la mémoire Flash du routeur. Puis redémarrez le routeur.

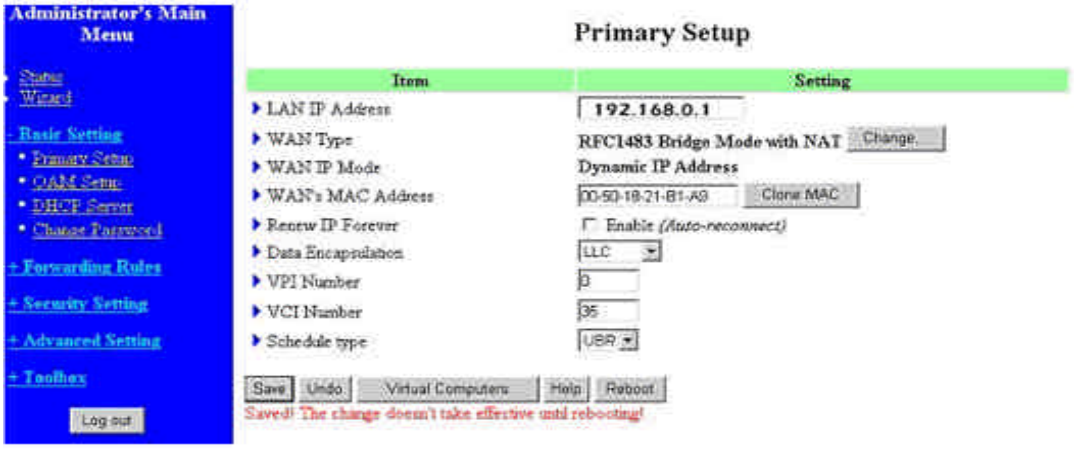
4.4.1.2 Ethernet Over ATM (RFC 1483 Bridged) with NAT



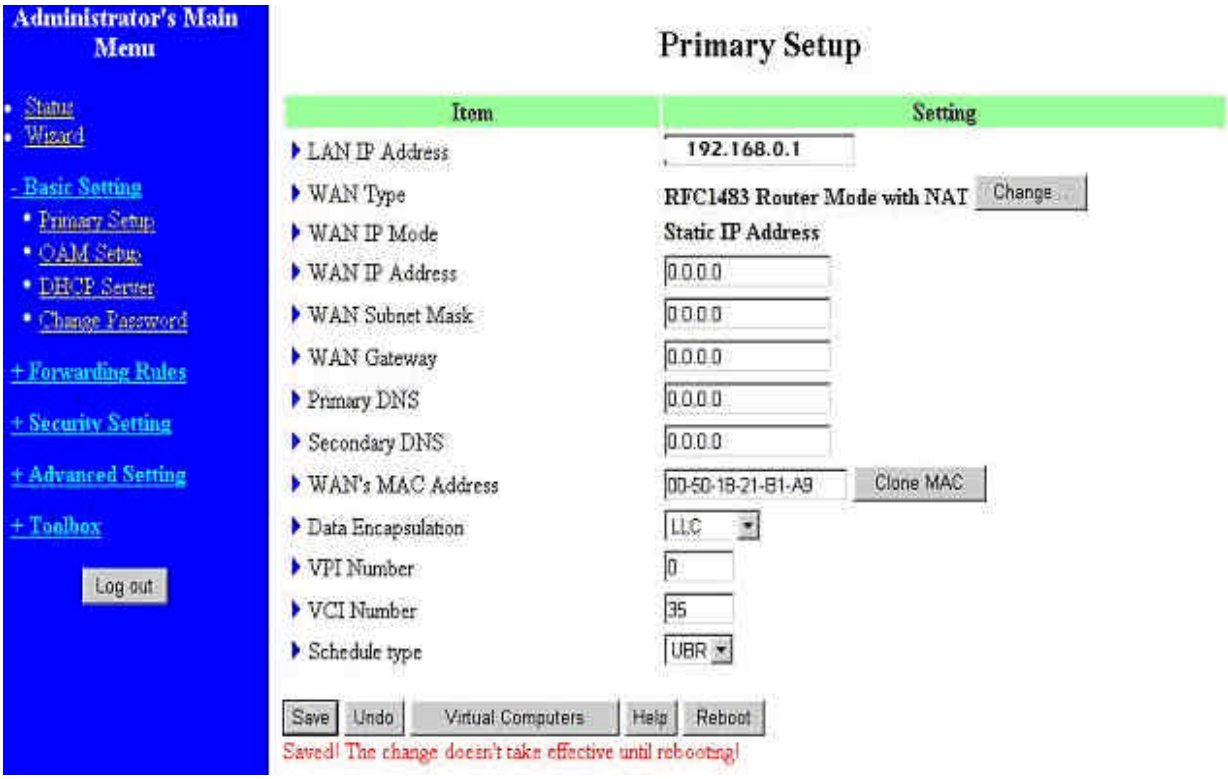
Dynamic IP Address: Obtient une adresse IP automatiquement du FAI.

Host Name: option. Peut être demandé par certain FAI, par exemple @domicile.

1. *Renew IP Forever*: Cette fonction permet au routeur d'obtenir une adresse IP automatiquement si la connexion ADSL est perdue.



4.4.1.3 IP over ATM (RFC 1483 Routed)



En mode routeur, le NAT est toujours activé. Vous devez configurer les paramètres IP WAN suivant :

WAN IP Mode:

Ce produit supporte 2 modes: IP statique et IP dynamique. Si vous sélectionnez le mode **dynamique**, le routeur va essayer d'obtenir une adresse IP automatiquement depuis le serveur de votre FAI. Si vous sélectionnez le mode **statique**, vous devez saisir les informations suivantes :

WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary/Secondary DNS

Votre FAI vous fournie les paramètres nécessaires.

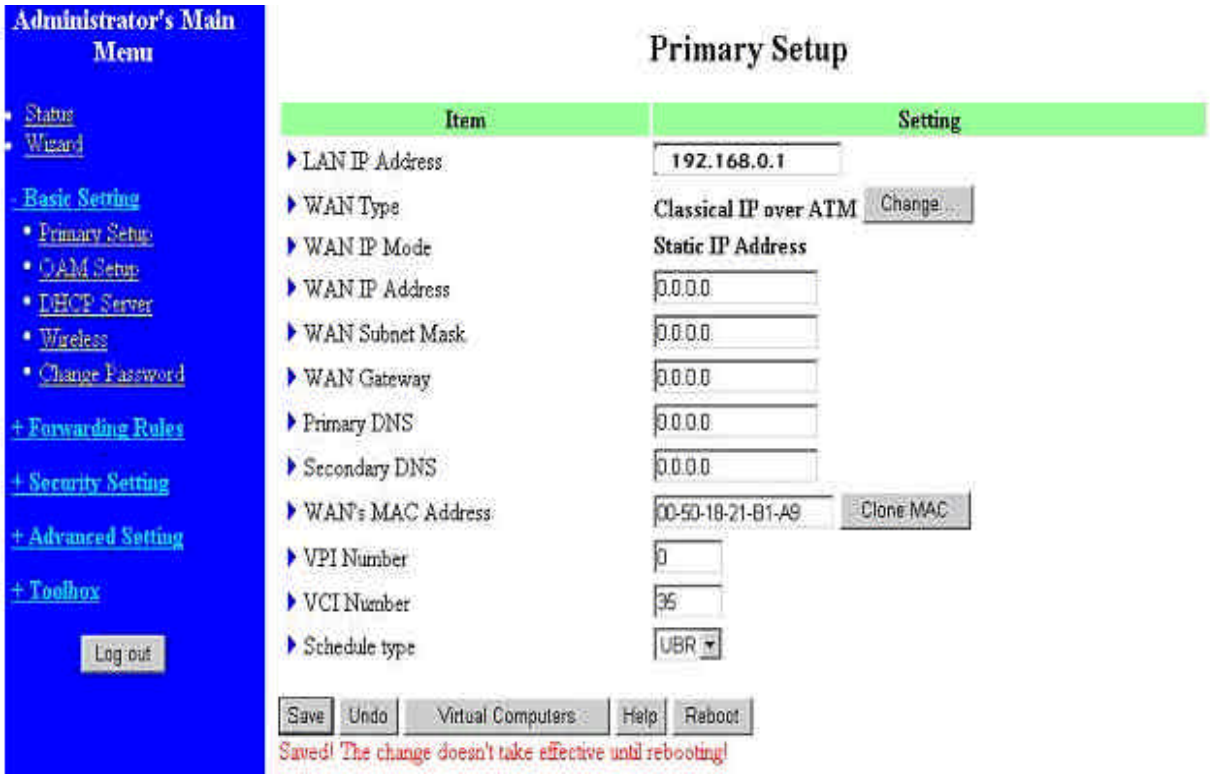
VPI/VCI Numbers:

Valeurs utilisées par votre FAI. Fournit par votre FAI, sinon voir **Annexe d** de ce manuel.

Schedule Type:

Paramètres du type de trafic ADSL. Ce produit supporte **UBR** (Un-specified bit rate) et **CBR** (Constant bit rate). Dès que vous avez fini, cliquez sur le bouton **Save** pour sauvegarder les changements dans la mémoire Flash du routeur. Puis redémarrez le routeur.

4.4.1.4 Classical IP over ATM (RFC 1577)



En mode **Classical IP over ATM**, le NAT est toujours activé. Vous devez configurer les paramètres IP WAN suivant :

WAN IP Mode:

Ce produit supporte 2 modes: IP statique et IP dynamique. Si vous sélectionnez le mode **dynamique**, le routeur va essayer d'obtenir une adresse IP automatiquement depuis le serveur de votre FAI. Si vous sélectionnez le mode **statique**, vous devez saisir les informations suivantes :

WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary/Secondary DNS

Votre FAI vous fournie les paramètres nécessaires.

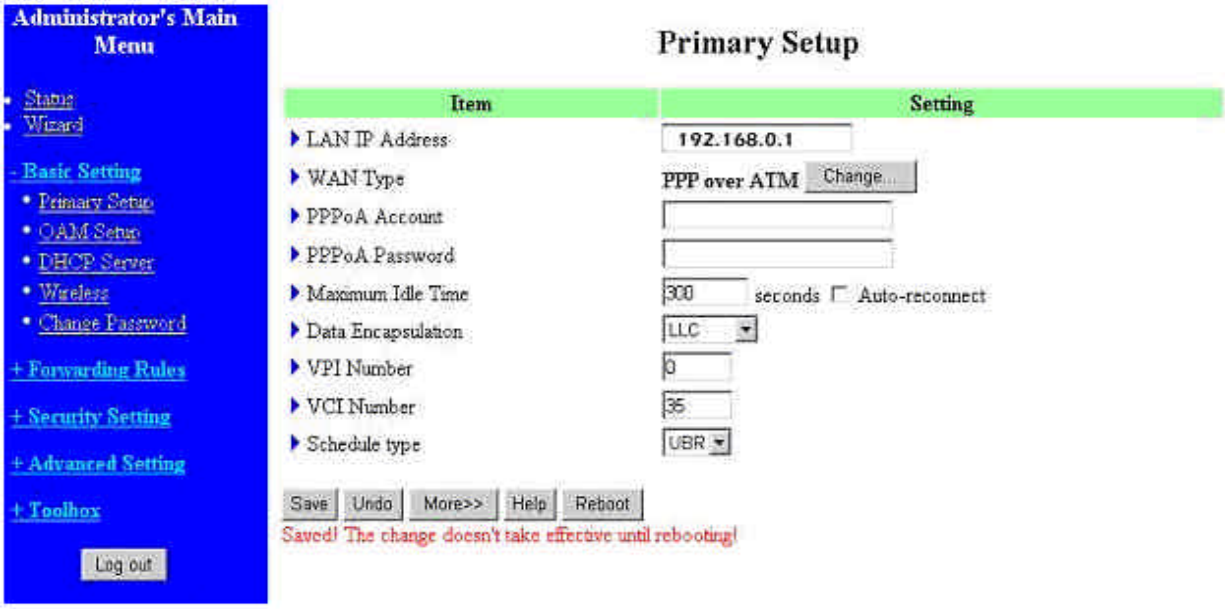
VPI/VCI Numbers:

Valeurs utilisées par votre FAI. Fournit par votre FAI, sinon voir **Annexe d** de ce manuel.

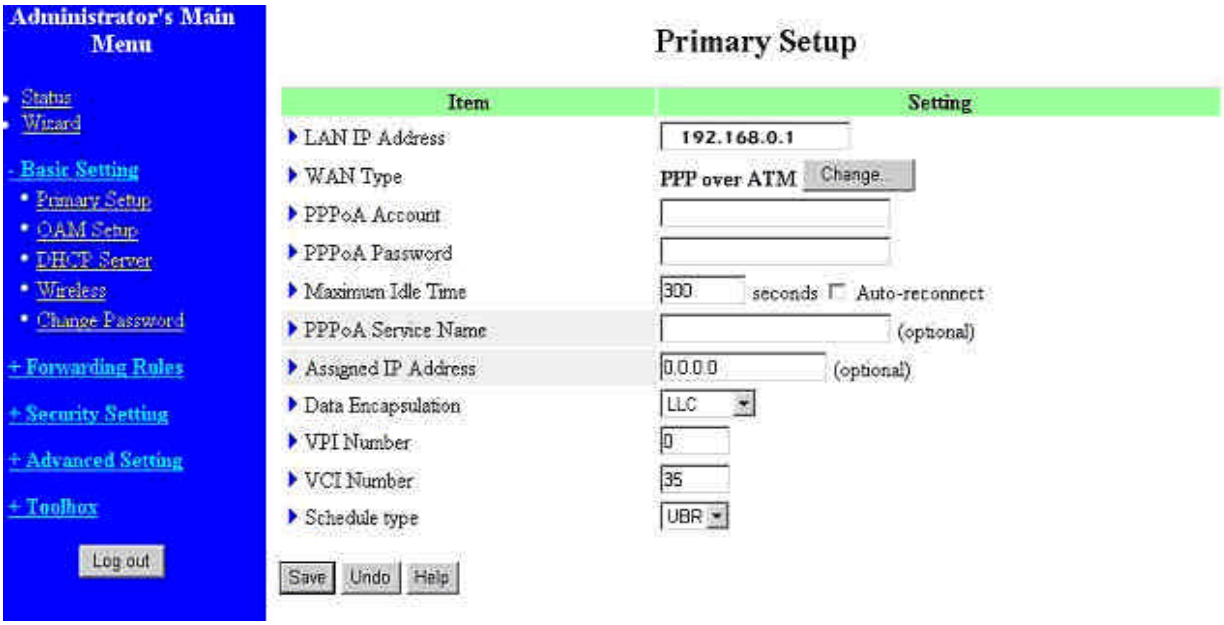
Schedule Type:

Paramètres du type de trafic ADSL. Ce produit supporte **UBR** (Un-specified bit rate) et **CBR** (Constant bit rate). Dès que vous avez fini, cliquez sur le bouton **Save** pour sauvegarder les changements dans la mémoire Flash du routeur. Puis redémarrez le routeur.

4.4.1.5 PPP over ATM (RFC 2364)



Cliquez sur le bouton **"More >>"**



PPPoA Account/Password:

Identifiant de connexion et mot de passe de connexion fournis par votre FAI.

Maximum Idle Time:

Période d'inactivité avant déconnexion de votre session PPPoA. Vous pouvez saisir la valeur zéro ou/et cocher **Auto-reconnect** pour désactiver cette fonction. Si la case **Auto-reconnect** est cochée, le routeur se reconnectera automatiquement à votre FAI après un redémarrage système ou après une

perte de connexion.

VPI/VCI Numbers:

Valeurs utilisées par votre FAI. Fournit par votre FAI, sinon voir **Annexe d** de ce manuel.

Schedule Type:

Paramètres du type de trafic ADSL. Ce produit supporte **UBR** (Un-specified bit rate) et **CBR** (Constant bit rate).

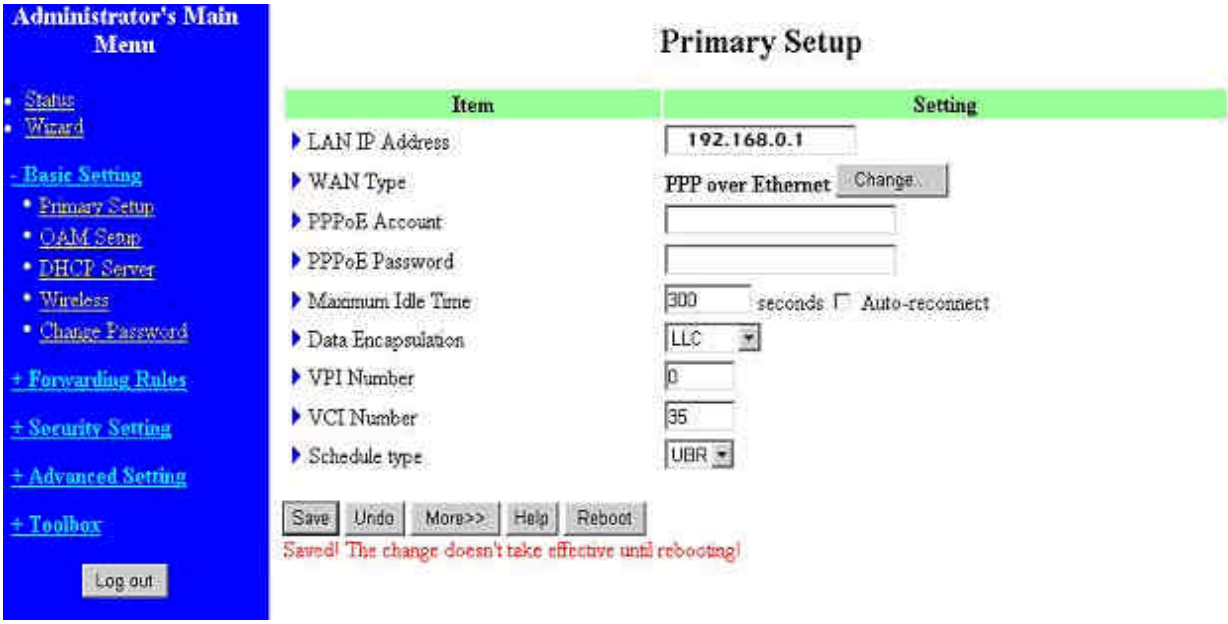
PPPoA Service Name:

Option. Saisissez le nom du service si votre FAI le demande.

Assigned IP Address:

Option. Certains FAI le demandent. Dès que vous avez fini, cliquez sur le bouton **Save** pour sauvegarder les changements dans la mémoire Flash du routeur. Puis redémarrez le routeur.

4.4.1.6 PPP over Ethernet (RFC 2516)



PPPoE Account/Password:

Identifiant de connexion et mot de passe de connexion fournis par votre FAI.

Maximum Idle Time:

Période d'inactivité avant déconnexion de votre session PPPoE. Vous pouvez saisir la valeur zéro ou cocher **Auto-reconnect** pour désactiver cette fonction. Si la case **Auto-reconnect** est cochée, le

routeur se reconnectera automatiquement à votre FAI après un redémarrage système ou après une perte de connexion.

VPI/VCI Numbers:

Valeurs utilisées par votre FAI. Fournit par votre FAI, sinon voir **Annexe d** de ce manuel.

Schedule Type:

Paramètres du type de trafic ADSL. Ce produit supporte **UBR** (Un-specified bit rate) et **CBR** (Constant bit rate).

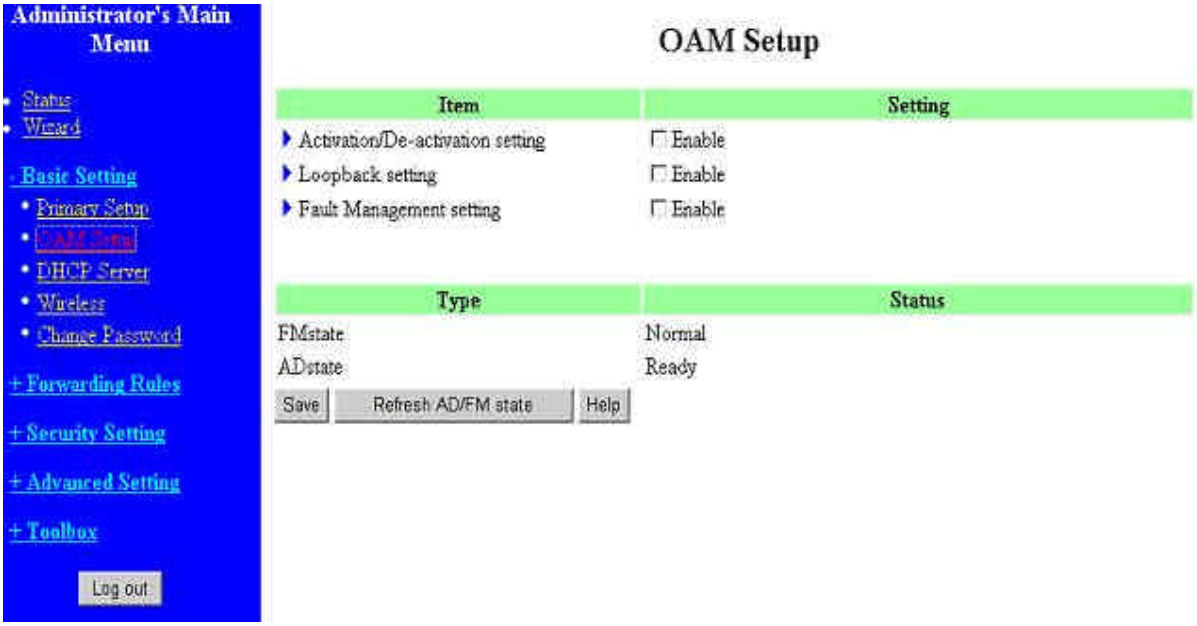
PPPoE Service Name:

Option. Saisissez le nom du service si votre FAI le demande.

Assigned IP Address:

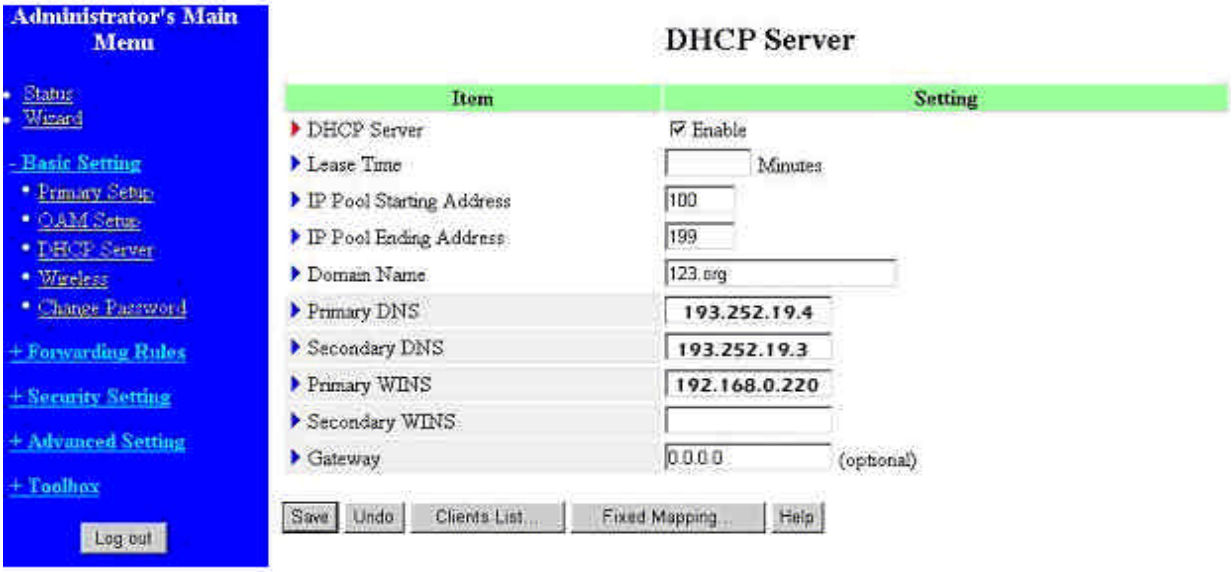
Option. Certains FAI le demandent. Dès que vous avez fini, cliquez sur le bouton **Save** pour sauvegarder les changements dans la mémoire Flash du routeur. Puis redémarrez le routeur.

4.4.2 OAM Server: Serveur OAM



Depuis cette page, vous pouvez paramétrer la fonction OAM pour le canal virtuel. Cliquez sur la case **Enable** pour activer la fonction désirée ou décochez pour la désactiver. Puis cliquez sur le bouton **Save** pour sauvegarder les changements. Cliquez sur le bouton Refresh AD/FM State pour visualiser l'état du canal.

4.4.2 DHCP Server



Les paramètres d'un environnement TCP/IP inclus la configuration de l'adresse IP de l'hôte, son masque de sous réseau, l'adresse de la passerelle et le DNS. C'est assez difficile et surtout assez long pour configurer manuellement tous les ordinateurs du réseau. Heureusement que le serveur DHCP permet de configurer automatiquement les ordinateurs du réseau. Si vous activez le serveur DHCP du routeur, paramétrez vos ordinateurs pour que ces derniers obtiennent une adresse IP automatiquement via un serveur DHCP, alors tous les ordinateurs de votre réseau, au démarrage du système, chargeront automatiquement les bons paramètres TCP/IP. En général, par défaut, les paramètres TCP/IP de chaque ordinateur sont déjà configurés de cette manière. Les paramètres du serveur DHCP inclus les points suivants :

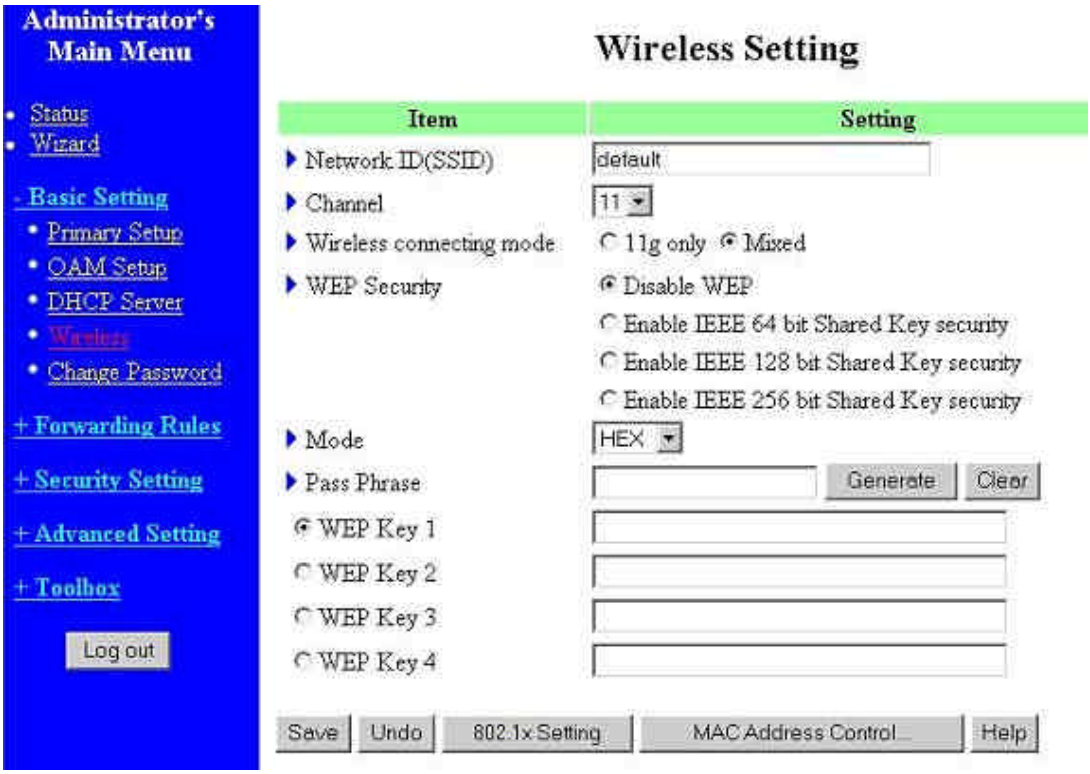
1. **DHCP Server**: Sélectionnez **"Disable"**(désactiver) ou **"Enable."**(activer)
2. **Lease Time:** durée de vie du bail (le même ordinateur gardera la même adresse IP durant cette période)

   IP Pool Starting Address/ IP Pool Ending Address: Quand une requête d'obtention d'adresse IP est demandée par un ordinateur, le serveur DHCP envoi une adresse IP libre compris entre la valeur saisie dans **IP Pool Starting Address** et la valeur saisie dans **IP Pool Ending Address.**
3. **Domain Name**: valeur optionnelle, sera transférer au poste client.
4. **Primary DNS/Secondary DNS**: Adresses IP DNS fournies par votre FAI.
5. **Primary WINS/Secondary WINS**: Adresses IP de serveurs WINS (si vous en avez).
6. **Gateway**: L'adresse de passerelle devrait être l'adresse de IP d'une autre passerelle. A utiliser seulement si ce routeur sert de passerelle, et n'est pas le routeur principal pour se

connecter à internet.

Cette fonction permet de configurer une autre passerelle à votre ordinateur.

4.4.3 Paramètres sans fil et 802.1X



Les paramètres sans fil vous permettent de configurer les points suivants:

1. **Network ID (SSID)**: Le nom de réseau est utilisé pour identifier votre réseau sans fil (WLAN). Les stations clients peuvent se connecter librement à ce produit ou un à autre point d'accès ayant le même **Network ID**. (par défaut, ce Network ID est **default**).
2. **Channel**: numéro du canal radio. Le numéro de canal par défaut est **11**.
3. **WEP Security**: Sélectionnez le type d'algorithme désiré. Activer la sécurité permet de protéger vos données quand ils sont transférés d'une machine vers une autre. Le standard IEEE 802.11 WEP (256, 128 ou 64 bits) est utilisé.
4. **WEP Key 1, 2, 3 & 4**: Quand vous activez une clé de sécurité 64, 128 ou 256 bits, sélectionnez une clé WEP à utiliser puis entrez 58, 26 ou 10 digits au format hexadécimal (0, 1, 2…8,9, A, B, …F).
5. **Pass-phrase Generator**: Etant donné qu'une suite de caractères en hexadécimal est difficilement mémorisable, le routeur propose un outil pour convertir un mot ou une phrase en valeur hexadécimal.

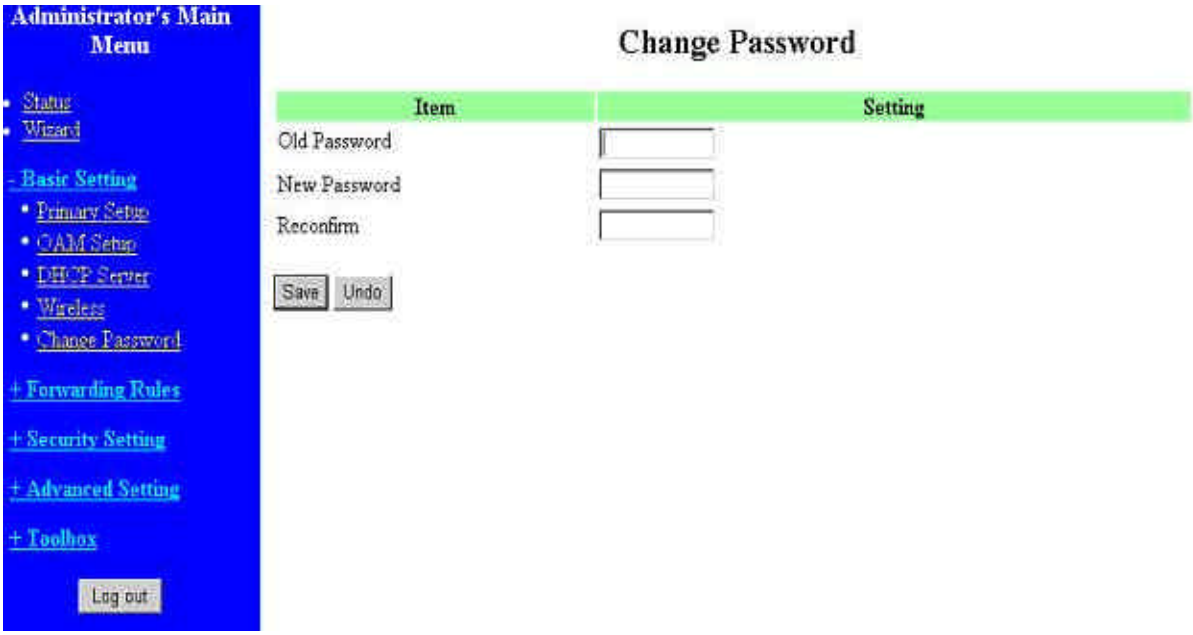
6. **802.1X Setting**

802.1X: Cliquez sur la case **Enable** pour activer cette fonction. Quand cette fonction est activée, l'utilisateur sans fil doit s'authentifier en premier avant de pouvoir utiliser les services du réseau

RADIUS Server: Adresse IP du serveur 82.1X ou nom de domaine

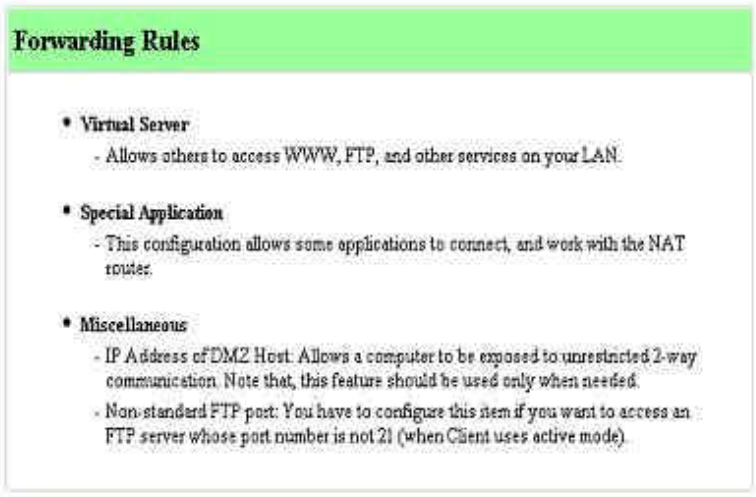
RADIUS Shared Key: valeur de la clé partagée par le serveur Radius et ce routeur.

4.4.4 Change Password: Changement du mot de passe

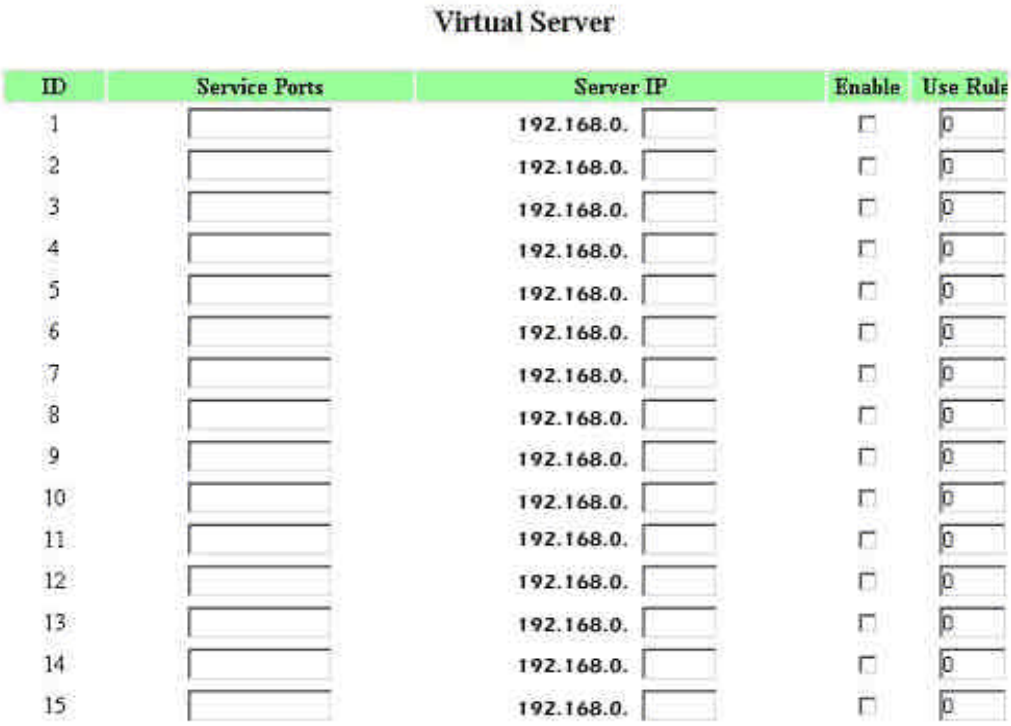


Le mot de passe peut être modifié à cet endroit. Nous vous recommandons de changer le mot de passe pour des raisons de sécurité.

4.5 Forwarding Rules / Règles de filtrage



4.5.1 Virtual Server: Serveur Virtuel



Le firewall de ce produit filtre tous les paquets inconnus pour protéger votre réseau Intranet.

Comme cela les machines de votre réseau local sont inaccessibles depuis internet. Si vous le désirez, vous pouvez rendre accessible une de vos machines en activant la fonction **Virtual Server**.

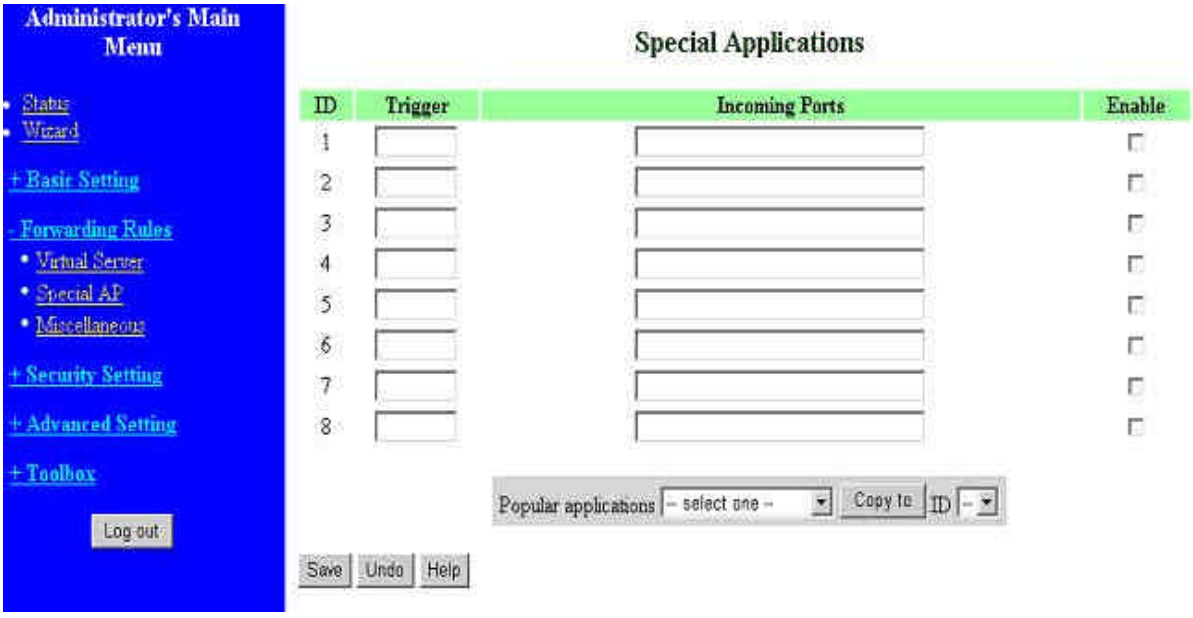
Un serveur virtuel est défini par un numéro de port (**Service port**). Toutes requêtes vers ce port seront redirigées vers l'ordinateur spécifié par son adresse IP (**Server IP**).

Le serveur virtuel peut fonctionner avec les règles de plages de connexions (**Scheduling Rules**), donnant ainsi une flexibilité au niveau du contrôle d'accès. Pour plus de d détails, voir **Scheduling Rules.**

Par exemple, si vous avez un serveur FTP (port 21 par défaut) dont l'adresse IP est 192.168.0.10, un serveur web (port 80 par défaut) à l'adresse 192.168.0.20, et un serveur VPN (port 1723 par défaut) à l'adresse 192.168.0.60, alors vous devez définir vos serveurs virtuels de la manière suivante :

Service Port	Server IP	Enable
21	192.168.0.10	V
80	192.168.0.20	V
1723	192.168.0.60	V

4.5.2 Special AP: Applications spéciales



Certaines applications nécessitent de multiple connexions, comme les jeux en lignes, la visioconférence, la téléphonie par Internet, etc….à cause de la fonction Firewall, ces applications ne peuvent fonctionner avec un routeur qui fait du pure NAT. La fonction **Special Applications** permet à

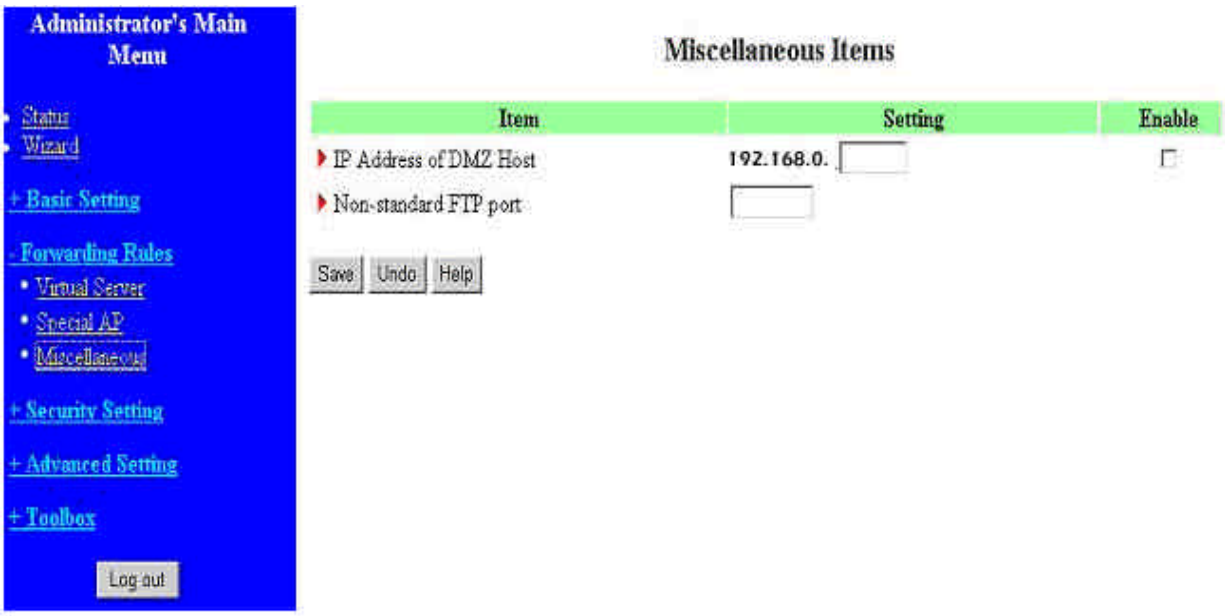
ces applications de fonctionner avec ce produit. Si malgré cela, vos applications ne fonctionnent toujours pas, alors il faut utiliser la fonction DMZ.

1. **Trigger**: numéro du port sortant utilisé par l'application.
2. **Incoming Ports**: quand le paquet défini par le **Trigger** est détecté, alors les paquets entrant envoyés vers les ports spécifiés sont autorisés à passer à travers le firewall.

Certaines applications sont déjà prédéfinis, sélectionnez votre application, cliquez sur le bouton **Copy to**, ajoute l'application prédéfini à la liste.

Note! Une seule machine à la fois peut utiliser l'application spéciale.

4.5.3 Miscellaneous Items: Divers



IP Address of DMZ Host

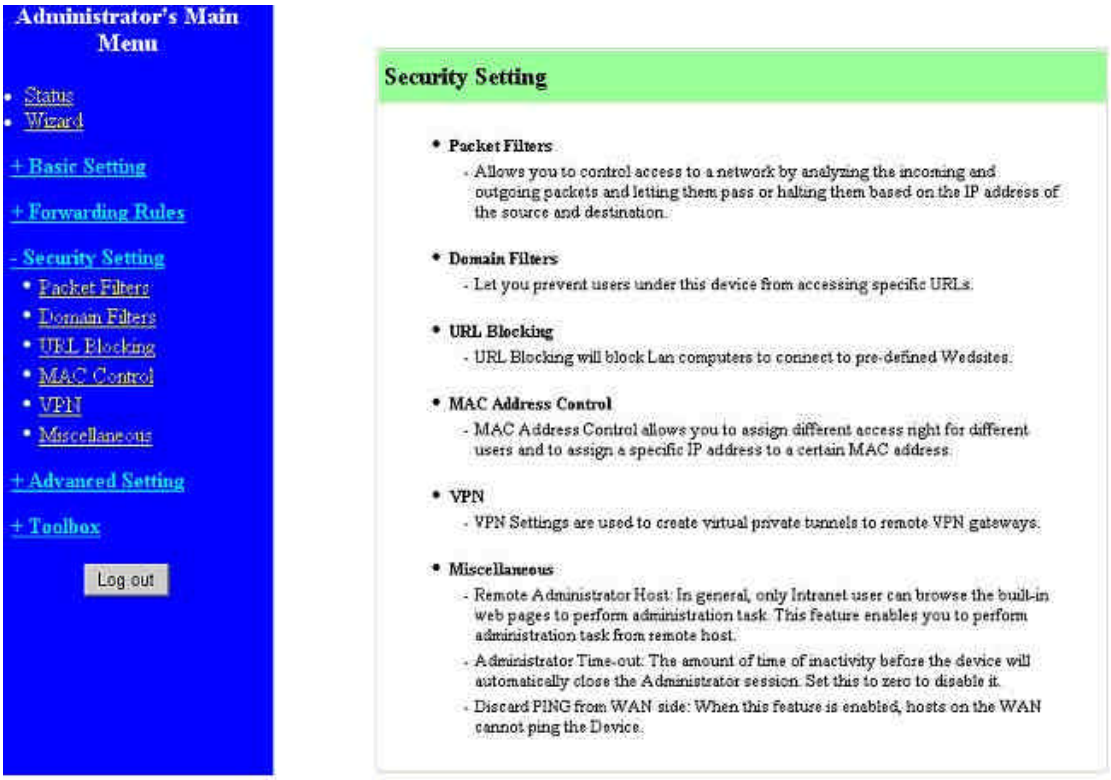
Une machine DMZ (DeMilitarized Zone), est une machine qui n'est pas protégée par le firewall. Permet à une machine d'être exposée à Internet pour les jeux en réseau, la visioconférence, de la téléphonie par Internet et d'autres applications spéciales.

NOTE: Cette fonction est à utiliser seulement en cas de besoin.

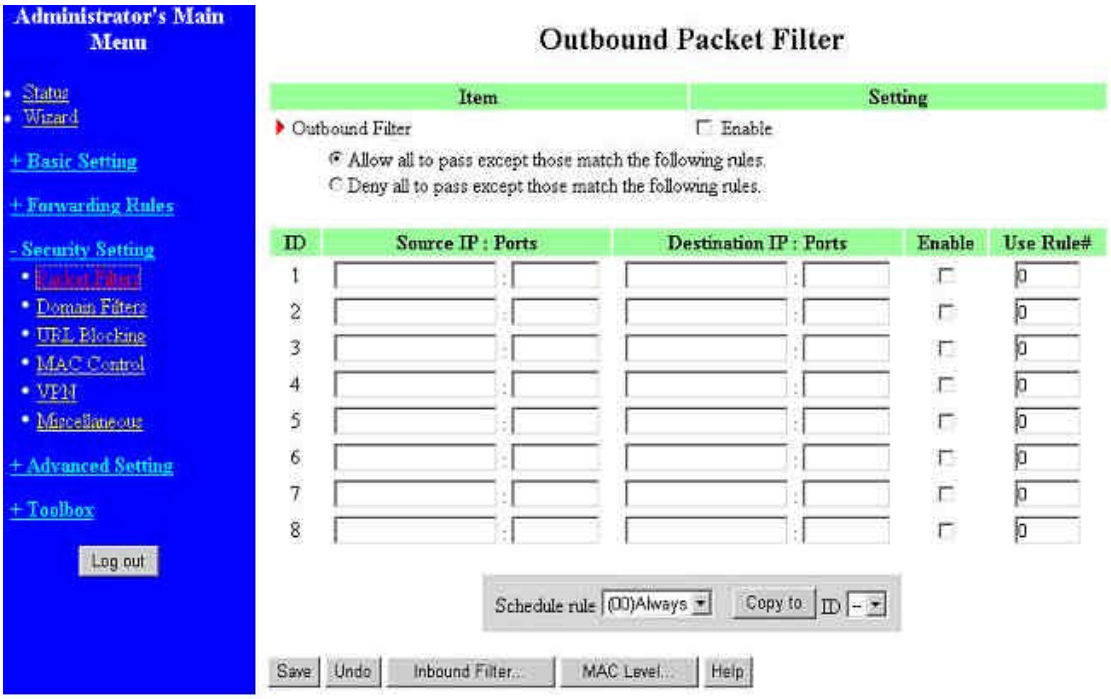
Non-standard FTP port

Configurez ce paramètre, si vous désirez accéder à un serveur FTP dont le port est différent de 21. Cette valeur sera perdue au redémarrage du routeur.

4.6 Security Settings: Paramètres de sécurité



4.6.1 Packet Filter: Filtrage par paquets



Le filtrage de paquets vous permet de définir quels paquets sont autorisés à passer à travers le routeur. **Outbound filter** ne s'applique qu'aux paquets sortants. Cependant, **Inbound Filter**, ne s'applique seulement qu'aux paquets en destination des serveurs virtuels ou des machines en DMZ. Vous pouvez sélectionner un des deux règles de filtrage suivantes:

1. **Allow all to pass except those match the specified rules** (autorise tout le monde sauf les machines correspondant aux règles spécifiées)
2. **Deny all to pass except those match the specified rules** (bloque tout le monde sauf les machines correspondant aux règles spécifiées)

Vous pouvez spécifier jusqu'à 8 règles pour chaque direction: sortante ou entrante. Pour chaque règle, vous devez spécifier les points suivants:

- **Source IP**: l'adresse IP source
- **Source port**: le numéro du port source
- **Destination IP**: l'adresse IP de destination
- **Destination port**: le numéro du port de destination
- **Protocol**: protocole à utiliser - TCP, UDP ou les deux en même temps.
- **Use Rule#:** le numéro de la règle

Pour l'adresse IP source ou de destination, vous pouvez spécifier une adresse IP unique (4.3.2.1), ou un bloc d'adresse IP (4.3.2.1-4.3.2.254). Une entrée vide, signifie toutes adresses IP.
Pour le numéro de port source ou de destination, vous pouvez définir un port unique (80) ou un bloc de ports (1000-1999). Ajoutez le préfixe "T" ou "U" pour spécifier le type de protocole TCP ou UDP. Par exemple, T80, U53, U2000-2999. Si aucun préfixe n'est défini, cela signifie les 2 protocoles TCP et UDP en même temps. Une entrée vide, signifie tous les ports. Le filtrage de paquets **Packet Filter** peut fonctionner avec les règles de connexions **Scheduling Rules**, rendant ainsi le contrôle d'accès plus flexible. Pour plus de détails, voir le chapitre **Scheduling Rule**.

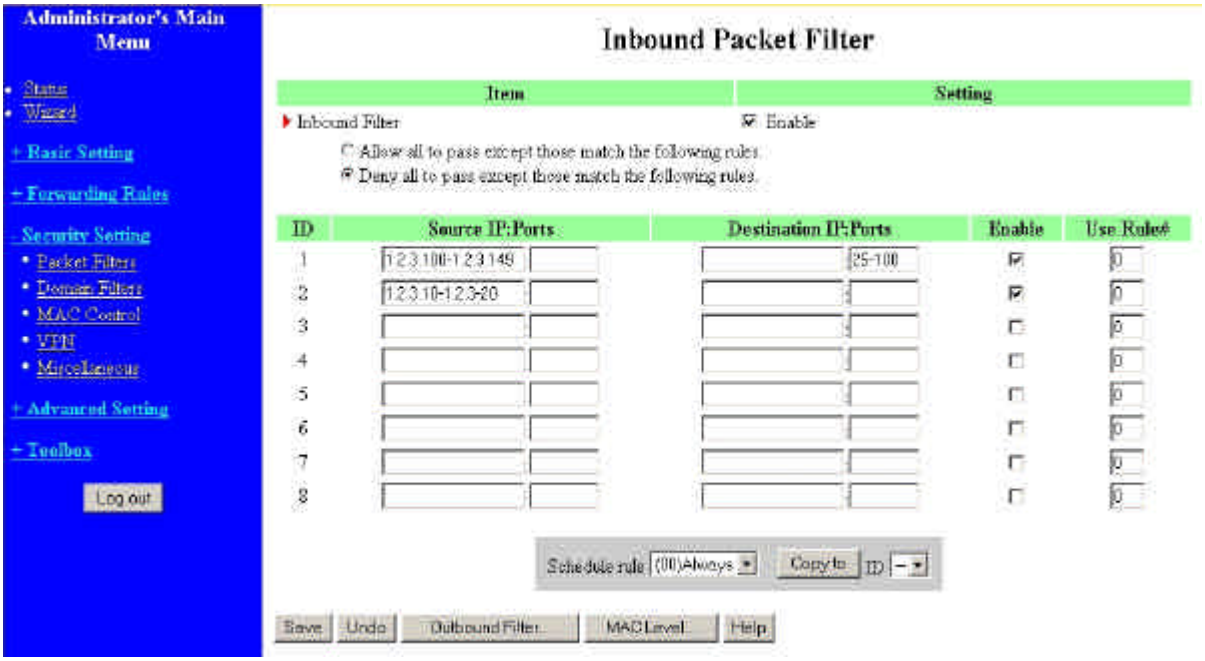
Chaque règle peut-être activée ou désactivée individuellement.

Inbound Filter:

Pour activer le filtre de paquets entrant, **Inbound Packet Filter** , cliquez sur le bouton **Inbound Filter**. Puis cochez la case **Enable**.

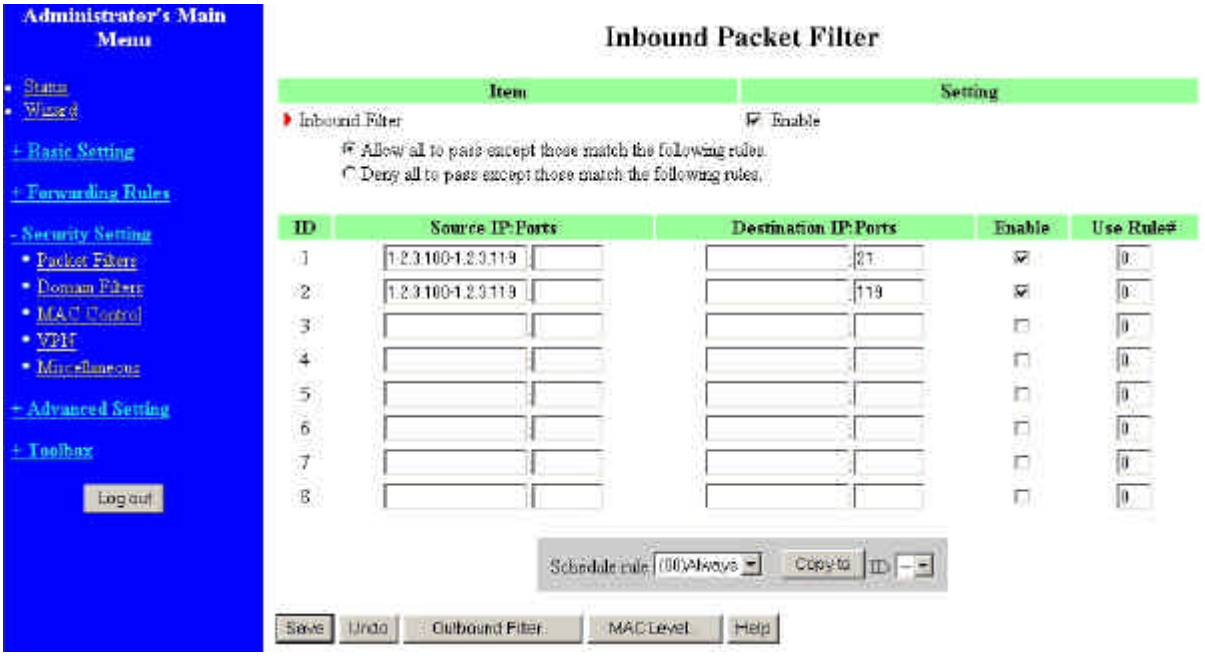
En supposant que vous avez un serveur SMTP (25), un serveur POP (110), un serveur web (110) un serveur FTP (21) et un serveur de news (119), définis comme serveur virtuel ou en DMZ.

Exemple 1:



- (1.2.3.100-1.2.3.149) Il s sont autorisés à envoyer des mail (25), recevoir des mails (110) et à accéder au serveur web (80).
- (1.2.3.10-1.2.3.20) Ils ont tous les droits d'accès (rien ne les bloque).
- Le reste est bloqué

Exemple 2:



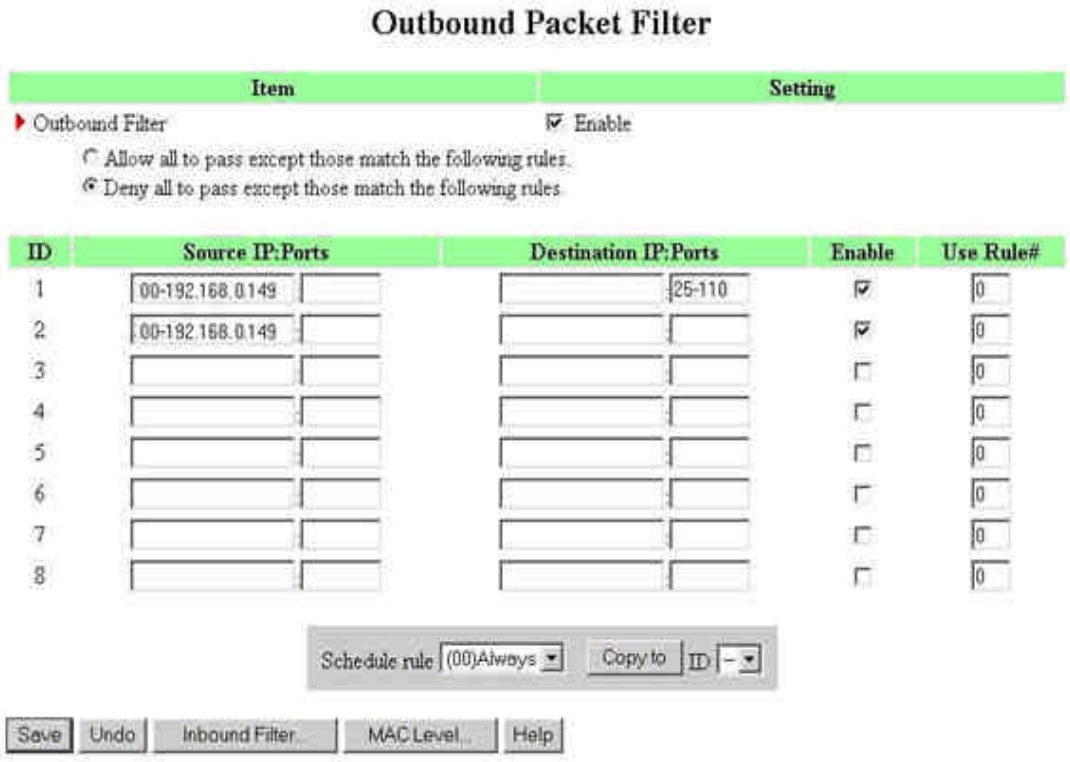
- (1.2.3.100-1.2.3.119) Ils peuvent tout faire sauf lire les news (port 119) et envoyer des fichiers par FTP (port 21).
- Le reste est autorisé.

Cliquez sur le bouton **Save** à la fin de la configuration.

Outbound Filter:

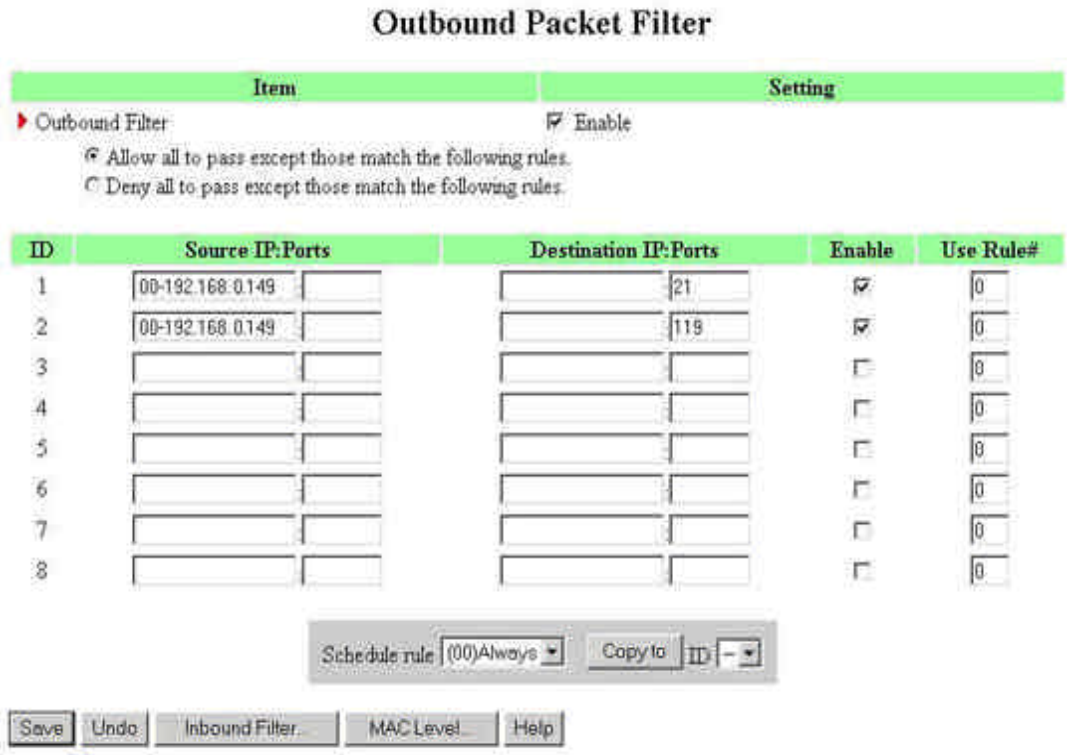
Pour activer le filtrage de paquets sortant **Outbound Packet Filter**, cliquez sur le bouton **Outbound Filter** puis cocher la case **Enable**.

Exemple 1:



- (192.168.0.100-192.168.0.149) Ils sont autorisés à envoyer des mail (port 25), recevoir des mails (port 110), surfer sur Internet (port 80). Le port 53 (DNS) est aussi nécessaire pour résoudre les noms de domaine.
- (192.168.0.10-192.168.0.20) Ils peuvent tout faire (rien n'est bloqué pour eux.
- Le reste est bloqué.

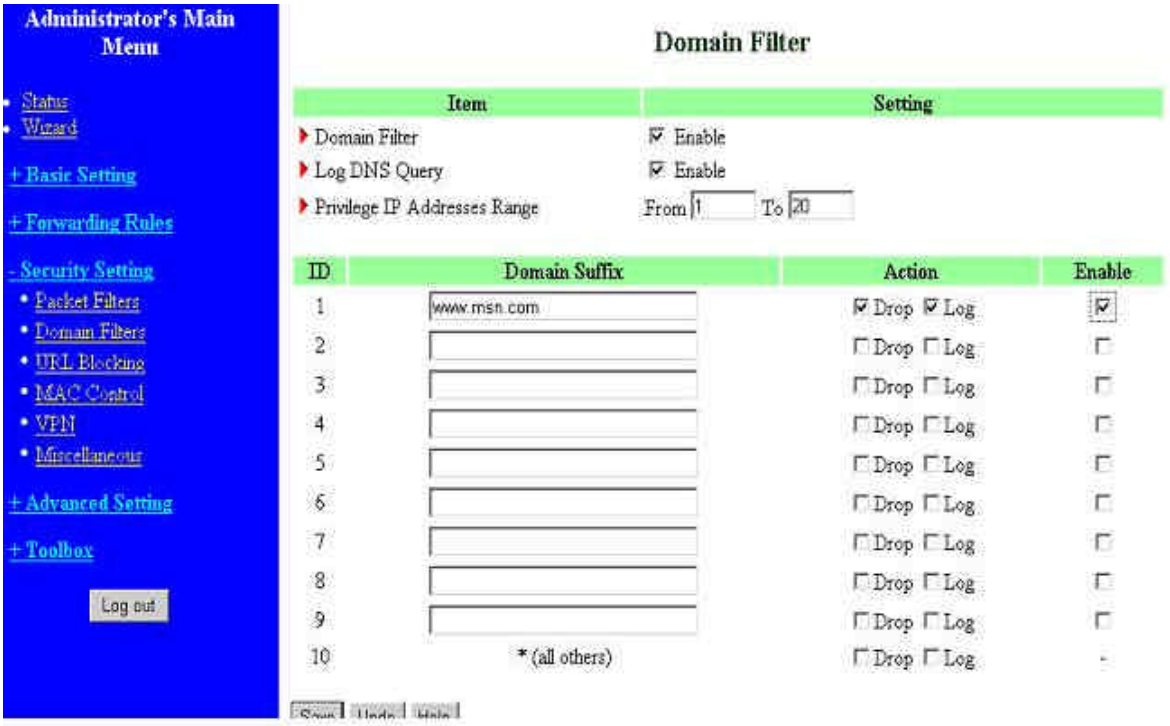
Exemple 2:



- (192.168.0.100-192.168.0.119) Ils peuvent tout faire sauf lire les news (port 119) et effectuer des transferts de fichiers en FTP (port 21).
- Le reste est autorisé.

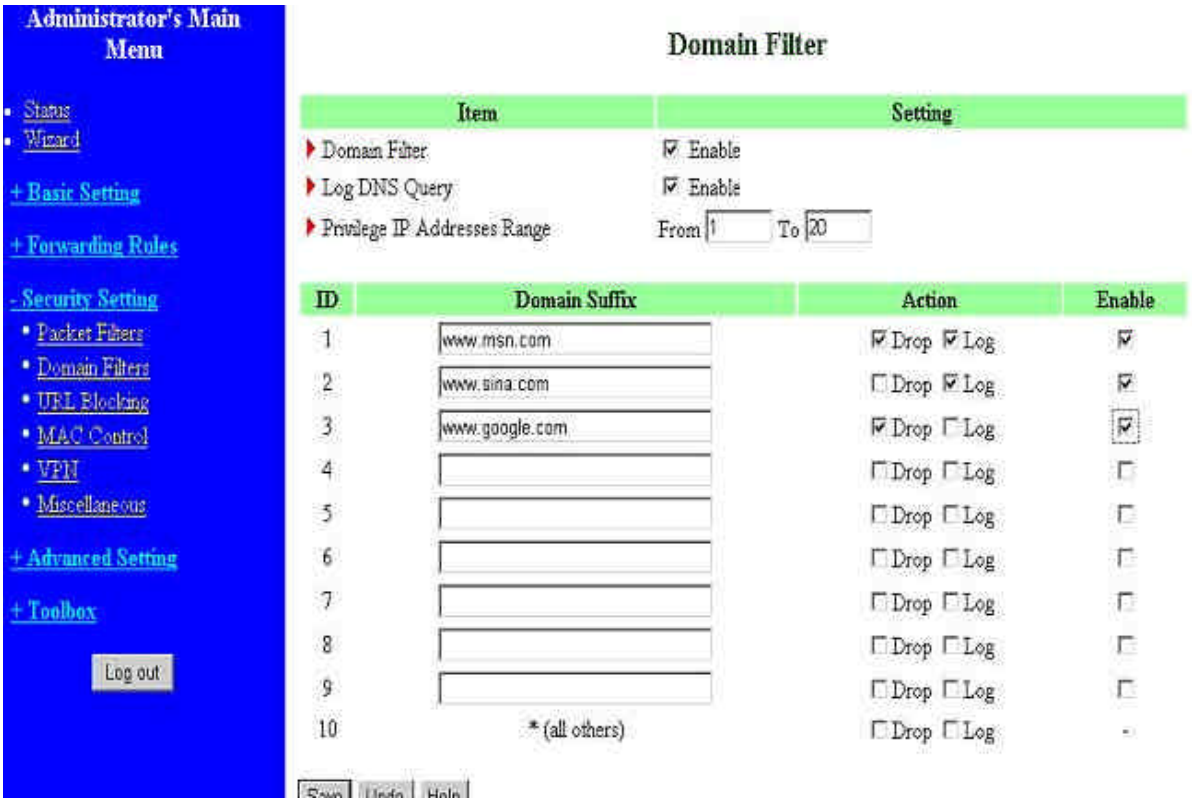
Cliquez sur le bouton **Save** à la fin de la configuration.

4.6.2 Domain Filter: Filtrage par nom de domaine



- **Domain Filter**
  Le filtrage par domaine permet de bloquer des sites web spécifiques.
- **Domain Filter Enable**
  Cochez la case **Enable** pour activer le filtrage par domaine.
- **Log DNS Query**
  Cochez la case **Enable** si vous désirez créer un historique quand une personne accède à cette adresse web spécifique.
- **Privilège IP Addresses Range**
  Permet de créer un groupe d'adresse IP qui peut accéder au réseau sans restriction.
- **Domain Suffix**
  Suffixe ou adresse web à surveiller. Par exemple ".com", "xxx.com".
- **Action**
  Quand une personne accède au site web correspondant, vous pouvez définir une action à apporter.
  Cliquez sur **Drop** pour bloquer l'accès. Cliquez sur **Log** pour enregistrer cet accès dans un fichier journal, mais l'accès n'est pas bloqué.
- **Enable**
  Cochez cette case pour activer la règle correspondante.

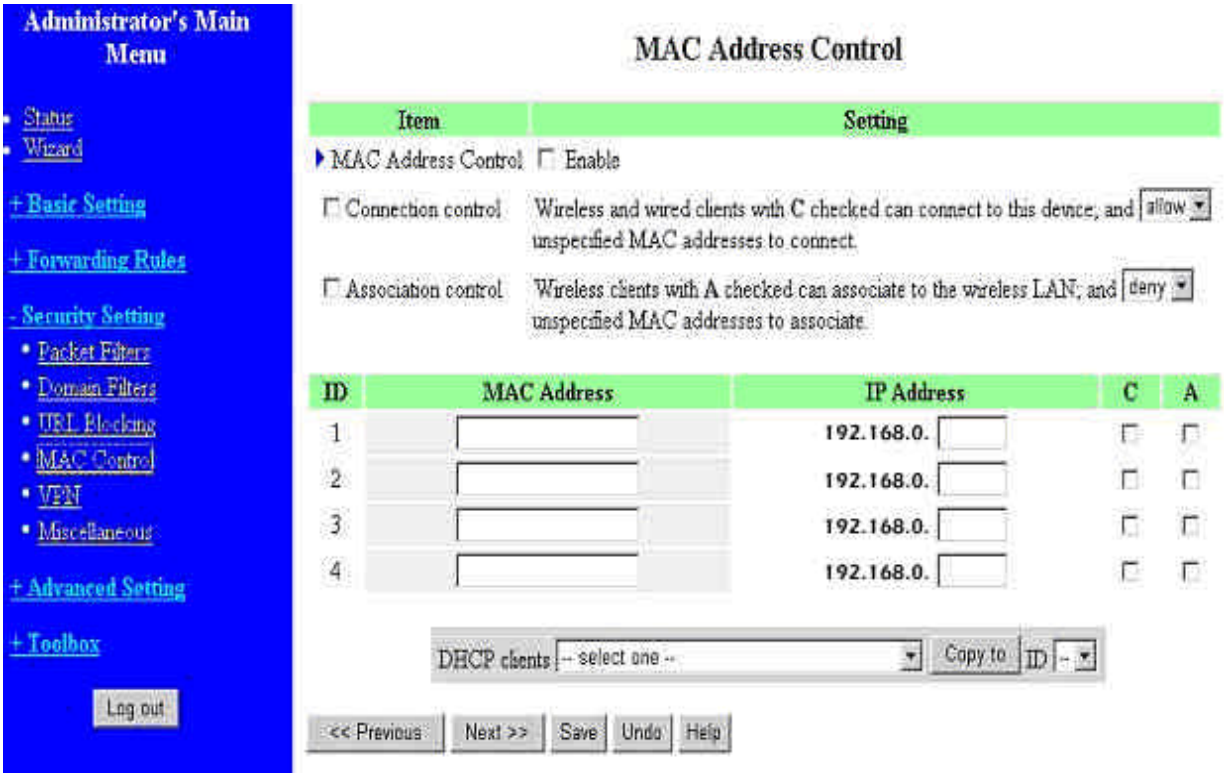
Exemple:



Dans cet exemple:

1. L'adresse URL "www.msn.com" sera bloquée, puis l'action sera enregistrée dans un fichier journal.
2. L'adresse URL "www.sina.com" ne sera pas bloquée, mais l'action sera enregistrée dans un fichier journal.
3. L'adresse URL "www.google.com" sera bloquée, mais l'action ne sera pas enregistrée dans un fichier journal.
4. Les adresses IP X.X.X.1 à X.X.X.20 ne sont pas concernées par ces règles de filtrage, donc ils peuvent surfer sur n'importe quel site web.

4.6.4 MAC Address Control: Contrôle par adresse MAC



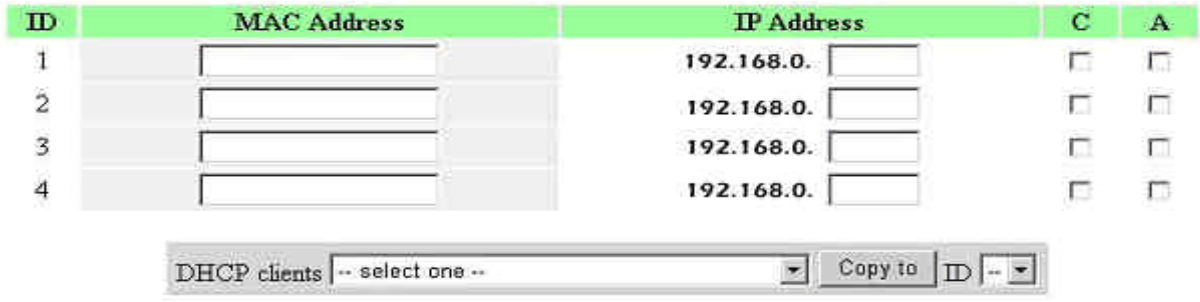
Le contrôle par adresse MAC permet de définir plusieurs droits d'accès pour les différents utilisateurs et d'attribuer une adresse IP à certaines adresses MAC.

MAC Address Control Cochez la case **Enable** pour activer le contrôle par adresse MAC. Les paramètres définis ici ne prennent effet que lorsque la case **Enable** est cochée.

Connection control Cochez la case **Connection Control** pour activer cette règle. Cette règle définit qui a le droit de se connecter à ce routeur. Cela concerne autant les ordinateurs sans fil que les ordinateurs connecté avec un câble réseau. Si un client n'a pas l'autorisation de se connecter, alors il ne pourra pas se connecter au routeur, donc ne pourra pas aller sur internet. Sélectionnez **Allow** (autorisé) ou **Deny** (interdit) pour autoriser ou interdire les machines dont l'adresse MAC se ne trouve pas dans ce tableau.

Association control Sélectionnez **Associate control** pour activer les règles entre les machines sans fil et les autres machines du réseau LAN. Si on interdit une machine du réseau LAN de s'associer avec une machine sans fil, alors tout échange entre ces 2 machines sera bloqués. Sélectionnez **Allow** (autorisé) ou **Deny** (interdit) pour autoriser ou interdire les machines dont l'adresse MAC ne se trouve pas dans ce tableau.

Control table



La table de contrôle **Control Table** est ce tableau se trouvant en bas de la page **MAC Address Control**. Chaque rangée de cette table indique l'adresse MAC et l'adresse IP correspondant à la machine. Vous pouvez distinguer 4 colonnes :

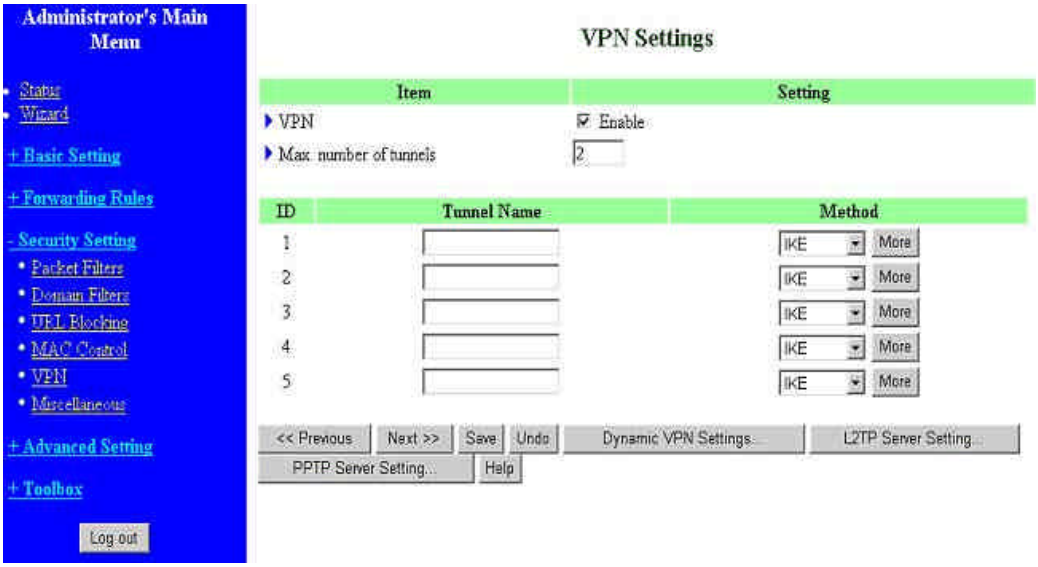
MAC Address	Adresse MAC de la machine
IP Address	L'adresse IP de la machine. Laissez en blanc si vous ne tenez pas compte de son adresse IP.
C	Quand **Connection Control** est activé, cochez la case **C** permet à la machine spécifiée de se connecter à ce routeur.
A	Quand **Associate control** est activé, cochez la case **A** permet d'associer la machine spécifiée avec les machines sans fil.

Sur cette page, cette petite fenêtre vous aide à saisir les adresses MAC.

Vous pouvez sélectionner une machine spécifique dans la zone **DHCP clients**, sélectionnez un numéro ID dans la partie **ID**, puis cliquez sur le bouton **Copy to** pour ajouter l'adresse MAC de cette machine.

Previous page and Next Page Boutons **Previous page** (page précédente) et **Next Page** (page suivante). Pour simplifier cette page de configuration, cette fenêtre **Control Page** est divisée en plusieurs pages. Vous pouvez utiliser ces boutons pour passer d'une page à une autre.

4.6.5 VPN setting: Paramètres VPN

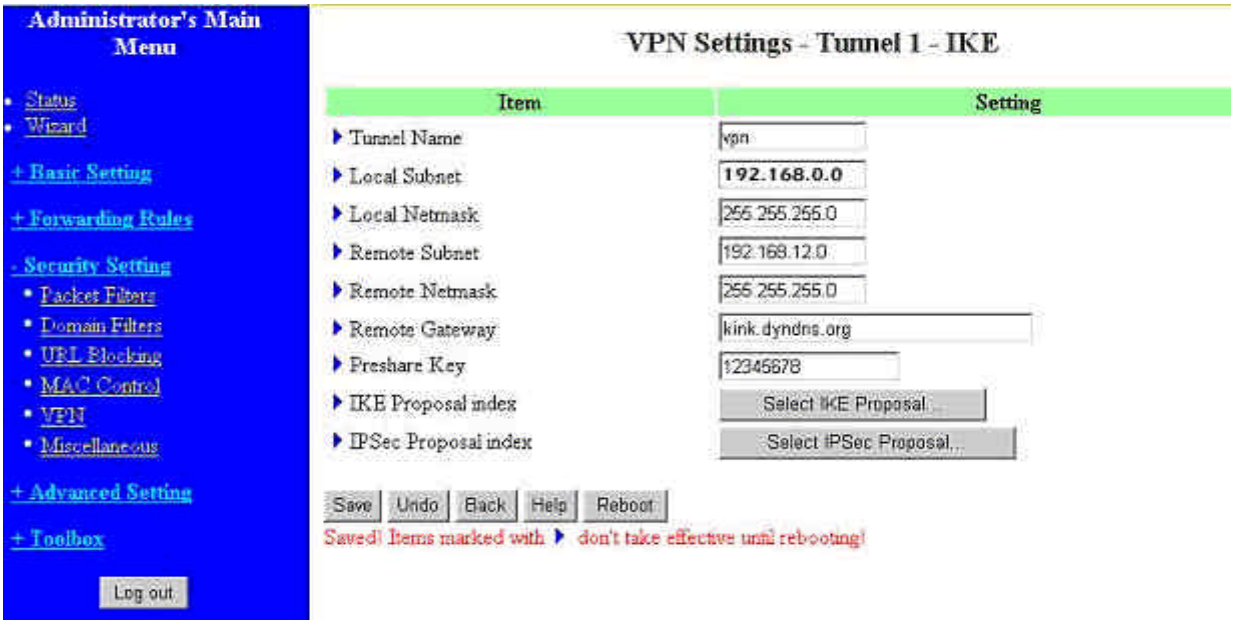


Permet de créer un réseau virtuel privé (Virtual Private Network) à travers la connexion internet. Cette technologie est très sécurisée, supporte la confidentialité des données, en utilisant des protocoles d'encapsulation, des algorithmes d'encryptions et de brouillage.

- **VPN enable**
  L'activation du VPN permet de créer un tunnel sécurisé à travers Internet, mais dégrade les performances de votre réseau. Donc activez le VPN si vous avez réellement besoin d'une connexion VPN. Par défaut le VPN est désactivé.
- **Max. number of tunnels**
  Comme le VPN dégrade les performances du réseau, le nombre de tunnel VPN est donc limité. Définissez soigneusement le nombre de tunnel que le routeur doit créer. Cette valeur va de 1 à 5.
- **Tunnel name**
  Le nom de votre tunnel VPN.
- **Method**
  VPN IPSEc supporte deux types de méthodes pour obtenir des clés: clé manuelle ou échange de clé automatique. Avec une clé manuelle, l'administrateur système saisi manuellement une clé d'encryption et d'authentification à chaque extrémité du tunnel VPN. Cependant avec la méthode IKE (Internet Key Exchange), les clés d'échange par Internet sont créées automatiquement. Il suffit donc de saisir juste une clé partagée prédéfinie (pre-shared key) à chaque bout du tunnel.
- **Fonctions des boutons**

Pour afficher la configuration détaillée de votre tunnel **IKE** ou **Manual**, cliquez sur le bouton **More**.

4.6.5.1 VPN Settings – IPSEC



VPN Settings – IKE

Le tunnel VPN se crée en 3 temps (3 parties séparées): la partie basique (adresse IP, etc.…), IKE proposal, et IPSec proposal.

La partie basique est défini par: le **Local Subnet** (sous-réseau local), le **Local Netmask** (masque de sous réseau local), le **Remote Subnet** (le sous-réseau distant), le **Remote Netmask** (le masque de sous réseau distant), la **Remote Gateway** (la passerelle distante) et enfin la **Preshared Key** (la clé partagée prédéfinie). **Tunnel Name**: Le nom du tunnel que vous avez nommé.

Paramètres de base:

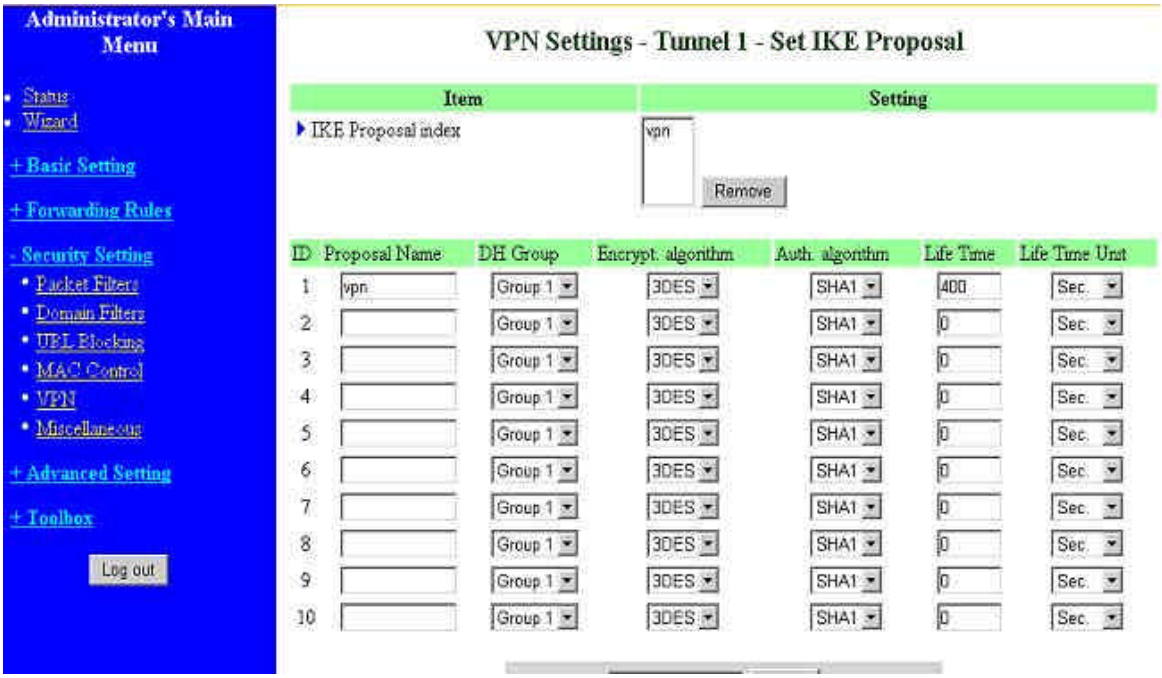
- **Local subnet:**
  Adresse du réseau local, peut-être l'adresse d'une machine, une partie du réseau ou le réseau entier.
- **Local netmask :**
  Masque de sous réseau du réseau local.
- **Remote subnet**
  Adresse du réseau à distance, peut-être l'adresse d'une machine, une partie du réseau ou le réseau entier.
- **Remote netmask**
  Masque de sous réseau du réseau à distance.

- **Remote gateway**
  L'adresse IP de la passerelle VPN distante.
- **Pre-shared key**
  La première clé partagée et prédéfinie qui démarre le mécanisme IKE des deux passerelles VPN pour négocier une clé sécurisée. La **Pre-shared key** doit être la même de chaque côté du tunnel VPN.

Fonctions des boutons:

- **Select IKE proposal:** Cliquez sur ce bouton pour paramétrer les valeurs IKE les plus fréquemment utilisées.
- **Select IPSec proposal:** Cliquez sur ce bouton pour paramétrer les valeurs IPSec les plus fréquemment utilisées.

VPN Settings - Set IKE Proposal



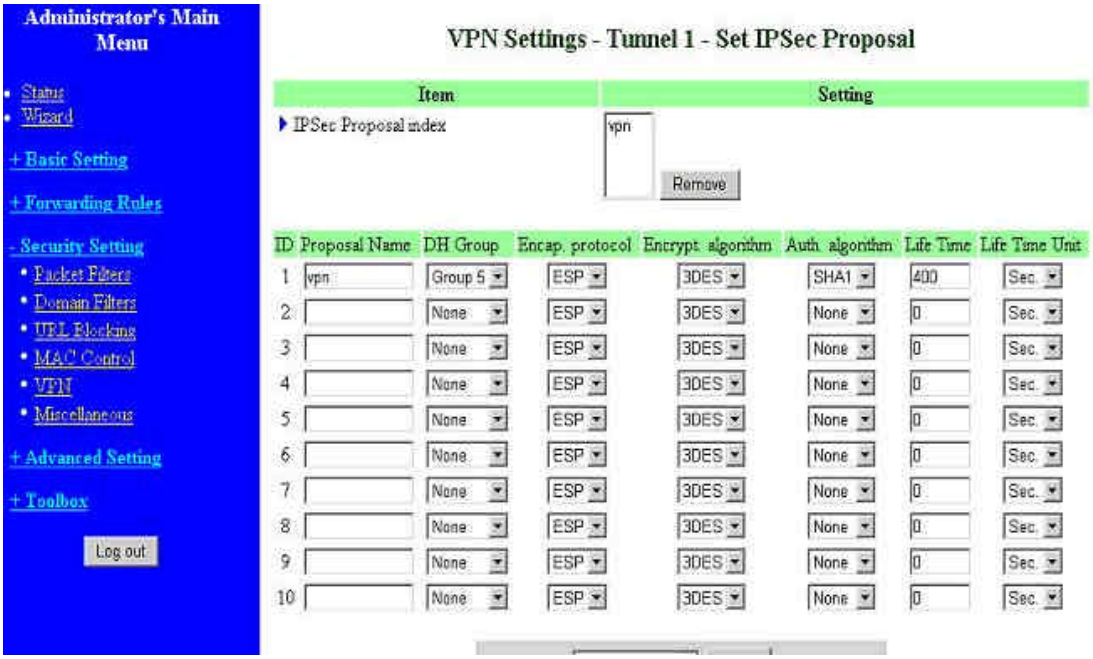
- **IKE Proposal index :**
  Une liste de proposition est indexée depuis la liste de proposition IKE ci-dessous. Sélectionnez un numéro d'ID depuis **Proposal ID**, puis cliquez sur le bouton **Add to**, ajoute cette proposition à la liste. Vous ne pouvez choisir que 4 propositions par mis la liste pour le tunnel dédié. Le bouton **Remove** se trouvant à côté de la liste **IKE Proposal index**, permet d'enlever une proposition de l'index.
- **Proposal name:**
  Nom de la proposition IKE, donnez un nom explicite.

- **DH group:**
  Vous pouvez sélectionner jusqu'à 3 groupes: groupe 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).
- **Encryption algorithm:**
  Vous pouvez sélectionner 2 algorithmes différents d'encryption: 3DES (Codage 168 bits) ou DES (56 bits).
- **Authentication algorithm:**
  Vous pouvez sélectionner jusqu'à 2 algorithmes d'authentification: SHA1 ou MD5.
- **Life time:**
  L'unité du Life Time (temps de vie) dépend de la valeur Life Time Unit. Si la valeur de l'unité est la seconde, la durée de vie du tunnel doit être choisi entre 300 et 172 800 secondes. Si la valeur de l'unité est en KB (Kilo-octets), la durée de vie du tunnel est calculée par rapport au nombre de KB maximum transmis dans le tunnel. Cette valeur va de 20 480 KBs à 2 147 483 647 KBs.
- **Life time unit**
  Unité de mesure du temps de vie: en secondes ou en KB.
- **Proposal ID**
  L'identifiant **IKE proposal** peut être sélectionné pour ajouter la proposition correspondante au tunnel dédié. Vous pouvez, au total avoir 10 propositions IKE. Au plus, seulement 4 propositions peuvent être appliquées à un tunnel dédié.

Fonctions des boutons:

- **Add to :** Cliquez sur ce bouton pour ajouter la proposition sélectionnée à la liste **IKE Proposal index**. Les propositions de la liste d'index seront utilisées en mode phase 1 pour la négociation IKE pour obtenir la valeur IKSAMP SA pour le tunnel dédié.

VPN Settings -Set IPSec Proposal



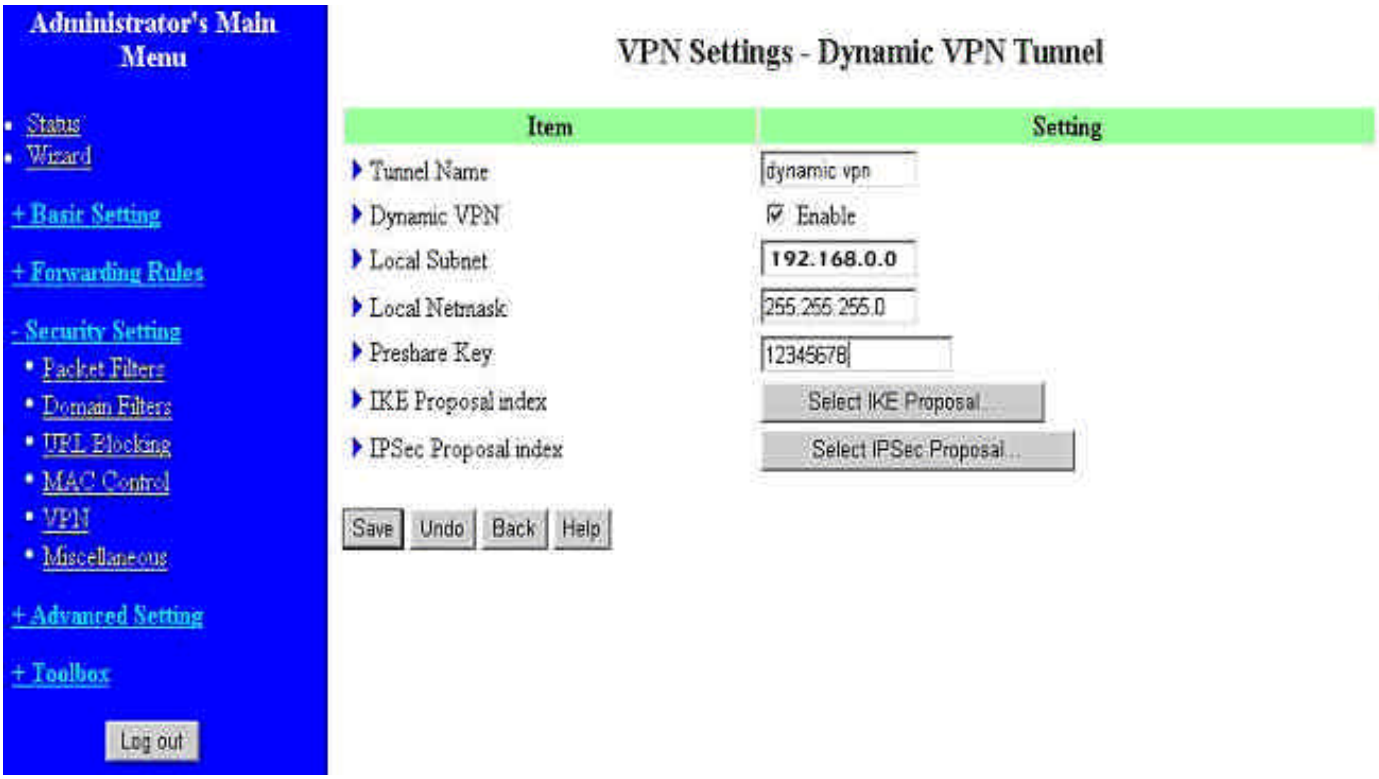
- **IPSec Proposal index**:
  Une liste de proposition est indexée depuis la liste de proposition IPSec ci-dessous. Sélectionnez un numéro d'ID depuis **Proposal ID**, puis cliquez sur le bouton **Add to**, ajoute cette proposition à la liste. Vous ne pouvez choisir que 4 propositions par mis la liste pour le tunnel dédié. Le bouton **Remove** se trouvant à côté de la liste **IPSec Proposal index**, permet d'enlever une proposition de l'index.
- **Proposal name:**
  Nom de la proposition IPSec, donnez un nom explicite.
- **DH group:**
  Vous pouvez sélectionner jusqu'à 3 groupes: groupe 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).
- **Encapsulation protocol:**
  Vous pouvez sélectionner jusqu'à 2 protocoles d'encapsulation: ESP ou AH.
- **Encryption algorithm:**
  Vous pouvez sélectionner jusqu'à 2 algorithmes d'encryption: 3DES ou DES. Mais si le protocole d'encapsulation est AH, alors l'algorithme d'encryption est inutile.
- **Authentication algorithm:**
  Vous pouvez sélectionner jusqu'à 2 algorithmes d'authentification: SHA1 ou MD5. Mais vous pouvez sélectionner **None** (aucun) pour la proposition IPSec.
- **Life time:**
  L'unité du Life Time (temps de vie) dépend de la valeur Life Time Unit. Si la valeur de l'unité est la seconde, la durée de vie du tunnel doit être choisi entre 300 et 172 800 secondes. Si la valeur de l'unité est en KB, la durée de vie du tunnel est calculée par rapport au nombre de KB maximum transmis dans le tunnel. Cette valeur va de 20 480 KBs à 2 147 483 647 KBs.

- **Life time unit:**
  Unité de mesure du temps de vie: en secondes ou en KB.
- **Proposal ID:**
  L'identifiant **IPSec proposal** peut être sélectionné pour ajouter la proposition correspondante au tunnel dédié. Vous pouvez, au total avoir 10 propositions IKE. Au plus, seulement 4 propositions peuvent être appliquées au tunnel dédié.

Fonction des boutons:

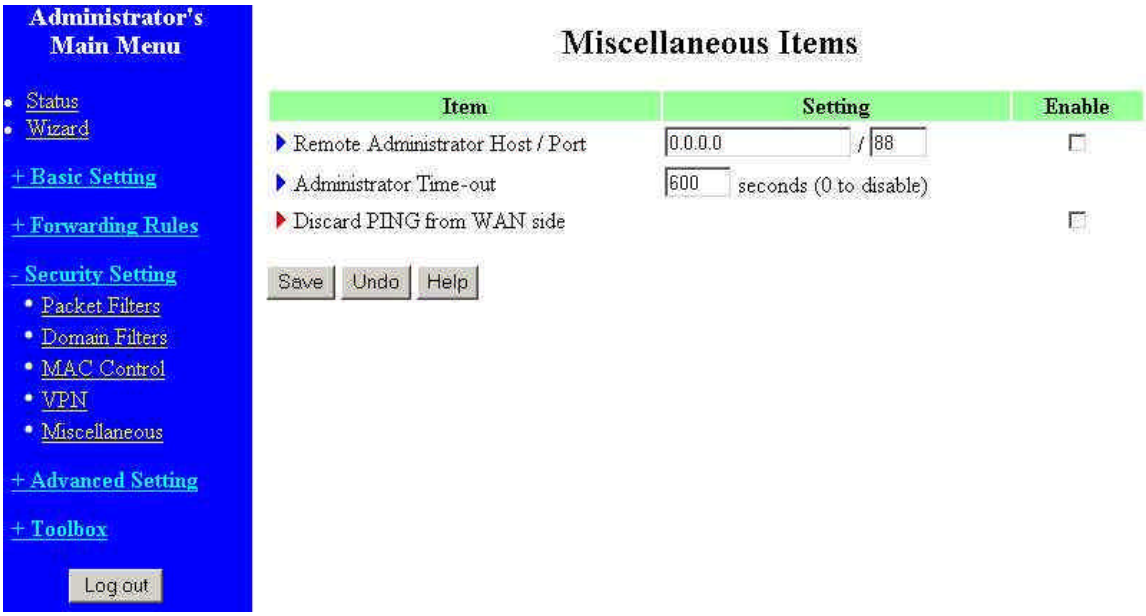
- **Add to :** Cliquez sur ce bouton pour ajouter la proposition sélectionnée à la liste **IPSec Proposal index**. Les propositions de la liste d'index seront utilisées en mode phase 2 pour la négociation IKE pour obtenir la valeur IPSec SA pour le tunnel dédié.

4.6.5.2 VPN Settings - Dynamic VPN Tunnel



Quand vous utilisez le **VPN Dynamic IP Settings**, le routeur fonctionnera en tant que serveur VPN dynamique. Le serveur VPN dynamique ne vérifiera pas les informations IP du client. Dans ce cas, les utilisateurs peuvent construire un tunnel VPN avec la passerelle VPN depuis n'importe quelle machine distante sans se soucier de son adresse IP.

4.6.6 Miscellaneous Items / Autres fonctionnalités



Remote Administrator Host/Port:

En général, il n'y a que les utilisateurs locaux qui peuvent accéder au routeur pour exécuter les tâches administratives. Cette fonction vous permet d'exécuter les tâches administratives depuis des machines distantes. Si cette fonction est activée, seule l'adresse IP spécifiée peut exécuter les tâches administratives à distance. Si l'adresse IP est 0.0.0.0, n'importe quelle machine peut exécuter les tâches administratives à distance. Vous pouvez utiliser le masque de sous réseau pour spécifier un groupe d'adresse IP avec l'annotation «/nn». Par exemple: "10.1.2.0/24".

NOTE: Quand l'administration à distance est activée, le port du serveur web d'administration à utiliser est le 88 par défaut. Vous pouvez changer ce numéro de port si vous le désirez.

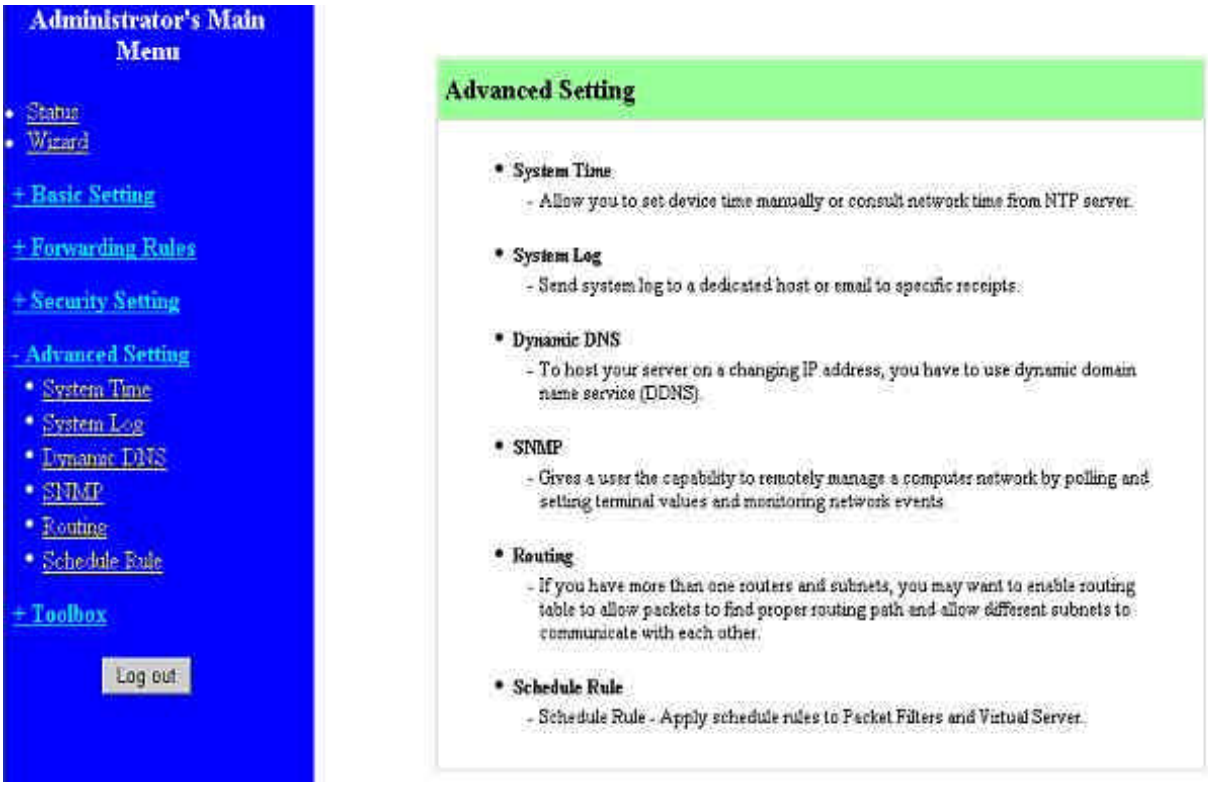
Administrator Time-out

Temps d'inactivité avant la déconnexion automatique. Mettez la valeur zéro pour désactiver cette fonction.

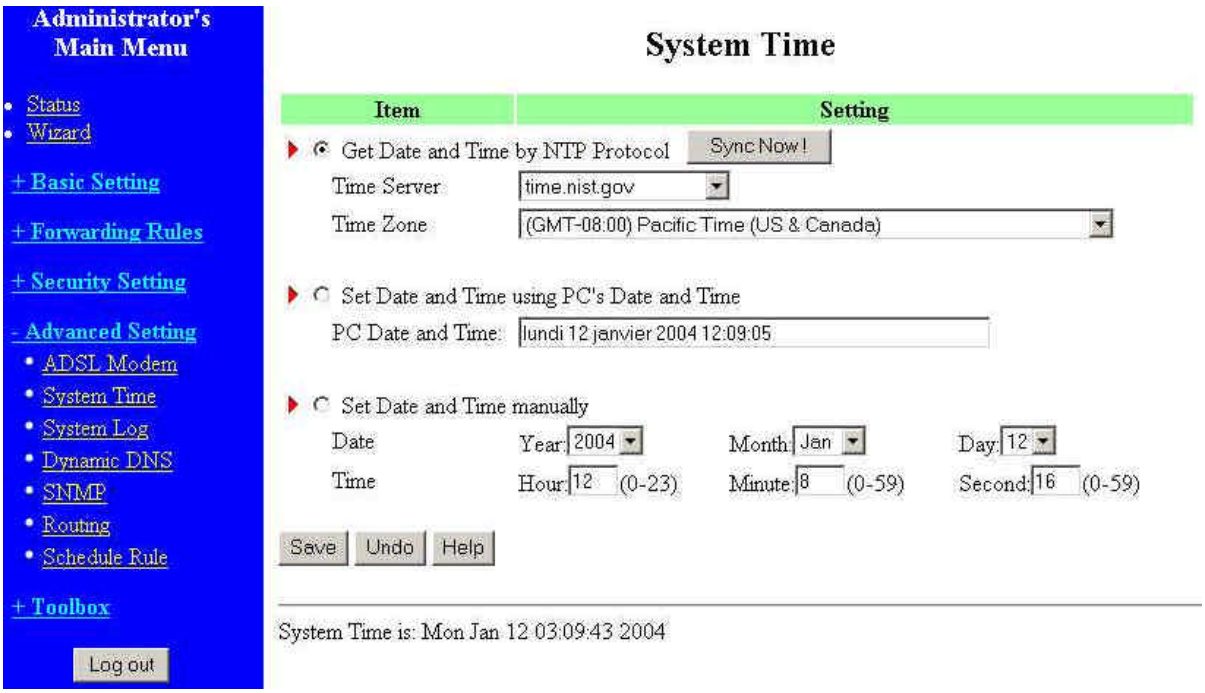
Discard PING from WAN side

Quand cette fonction est activée, aucune réponse à une commande PING ne sera renvoyée par le routeur.

4.7 Advanced Settings / Fonctions évoluées

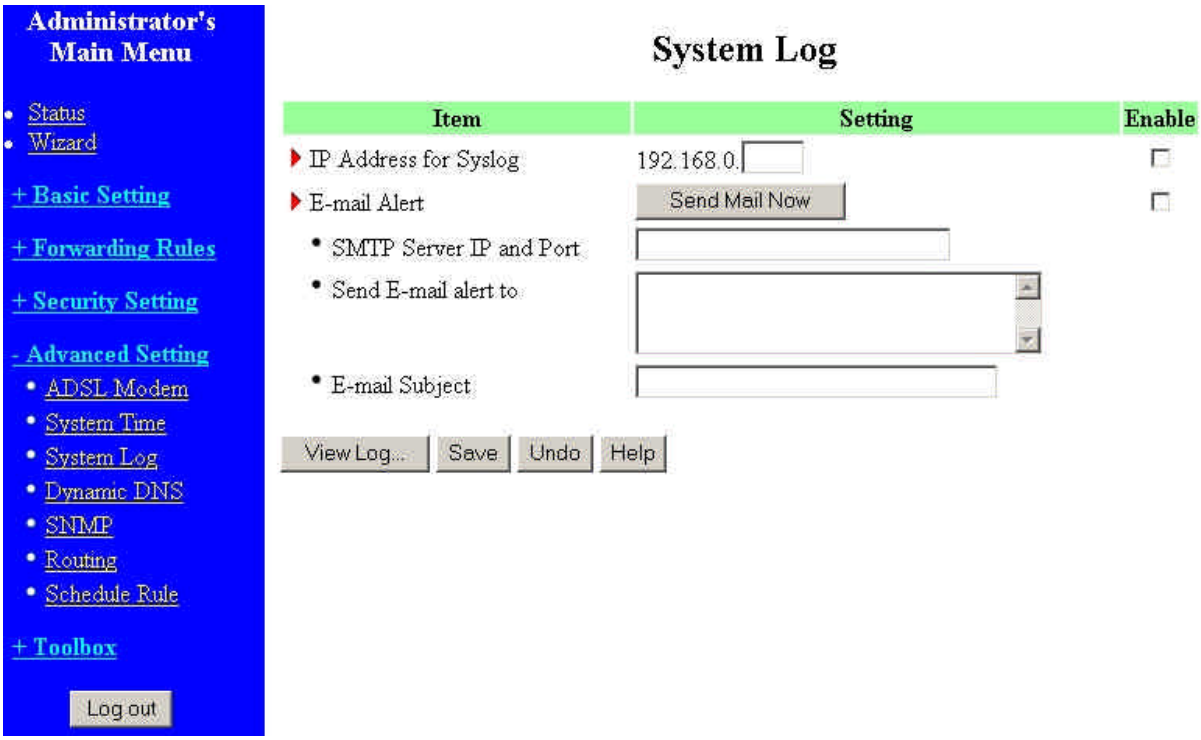


4.7.1 System Time



- **Get Date and Time by NTP Protocol:**
  Sélectionnez, si vous désirez obtenir la date et l'heure via le protocole NTP. Le routeur va se connecter à un serveur de temps sur Internet pour synchroniser son horloge.
- **Time Server:**
  Sélectionnez un serveur de temps.
- **Time Zone:**
  Sélectionnez votre fuseau horaire.
- **Set Date and Time using PC's Date and Time:**
  Sélectionnez si vous désirez utiliser la date et l'heure de votre ordinateur comme horloge du routeur.
- **Set Date and Time manually:**
  Sélectionnez si vous désirez saisir la date et l'heure manuellement.
- **Fonctions des boutons:**
  Sync Now: Synchronise l'horloge système avec un serveur de temps réseau

4.7.2 System Log



Vous avez 2 méthodes pour exporter le journal système: via un serveur Syslog (UDP) ou via un envoie d'email par le protocole SMTP (TCP).

IP Address for Syslog:

Adresse IP de votre serveur Syslog. Cochez la case **Enable** pour activer cette fonction.

E-mail Alert Enable

Cochez la case Enable pour activer les alertes par email (envoie du syslog par email).

SMTP Server IP and Port:

Saisissez l'adresse IP et le port du serveur SMTP à contacter. Si vous ne spécifiez pas de numéro de port, par défaut le port est le 25.

Par exemple, "mail.masociete.com" ou "192.168.1.100:26".

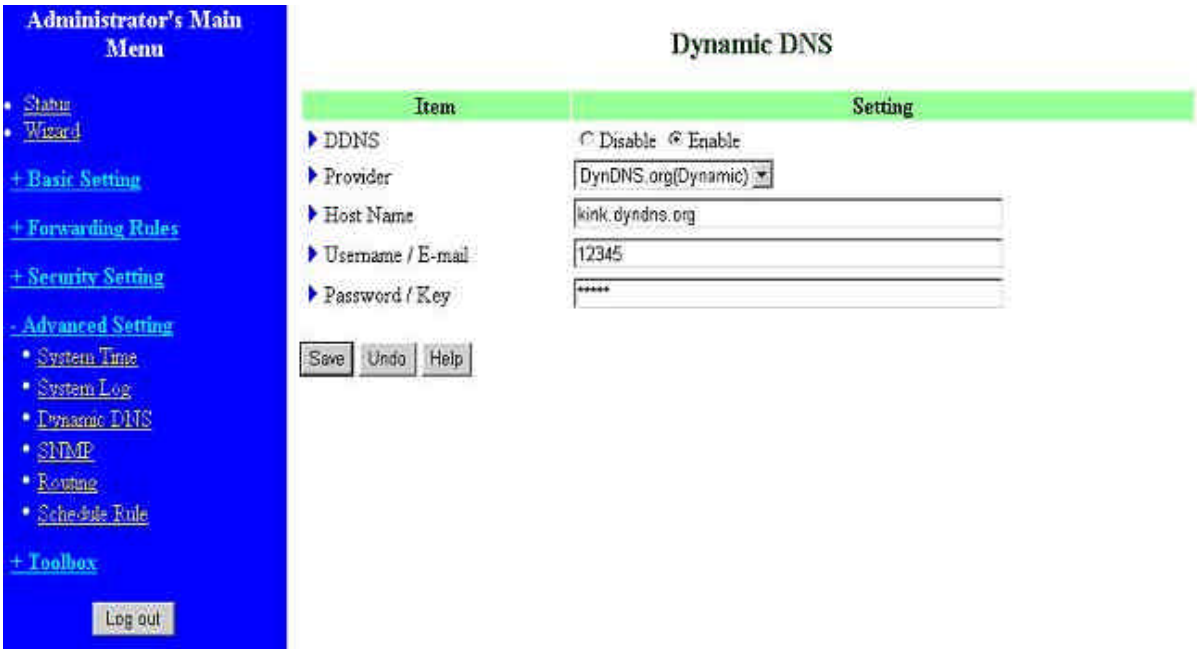
Send E-mail alert to

L'adresse email qui va recevoir le message. Vous pouvez spécifier plusieurs adresses email en les séparant par un point virgule ou une virgule (';' ou ',').

E-mail Subject

Le sujet de votre message. Ce paramètre est optionnel.

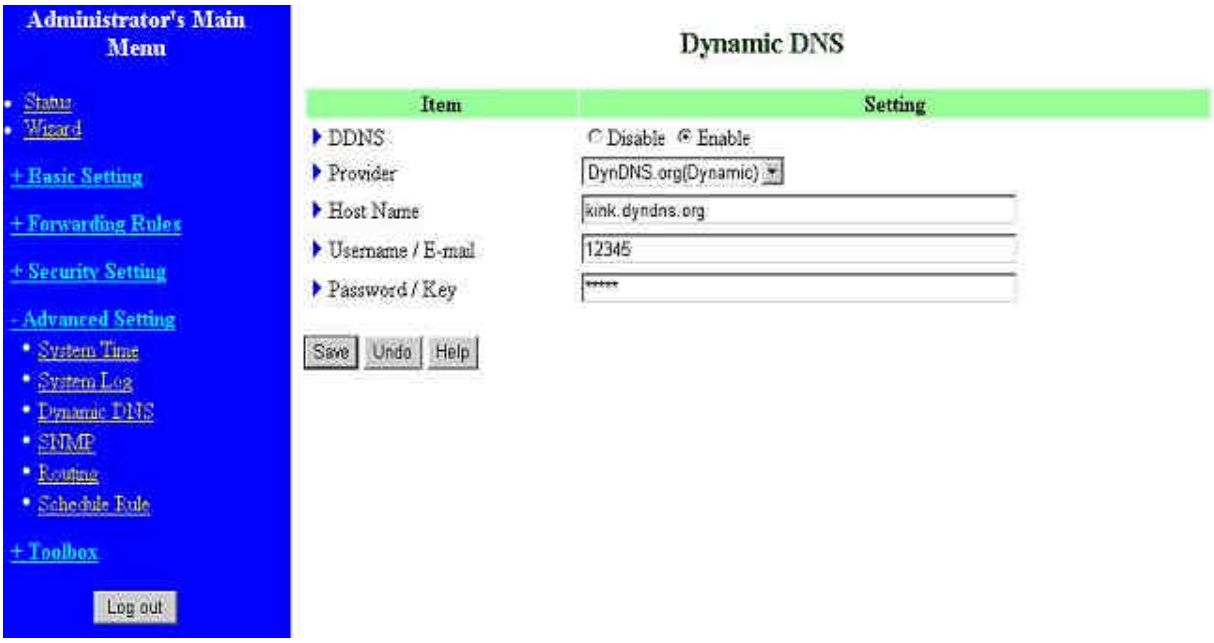
4.7.3 Dynamic DNS



Pour accéder à votre serveur intranet avec une adresse IP dynamique, vous devez utiliser un service de nom de domaine dynamique (DDNS).
Dans ce cas, les utilisateurs qui veulent se connecter à votre serveur, n'ont besoin de connaître que votre nom de serveur. Le Dynamic DNS va automatiquement lier le nom de votre machine à votre adresse IP courante, qui change à chaque fois que vous vous connectez à votre FAI (Fournisseur d'Accès Internet).
Avant d'activer le **Dynamic DNS**, vous devez créer un compte sur un des serveurs DNS Dynamique listé dans la zone **Provider**.
Pour activer le **Dynamic DNS**, cliquez sur la case à cocher **Enable** se trouvant en face du champ **DDNS**.
Puis vous devez saisir les informations appropriées concernant votre serveur DNS Dynamique.
Vous devez définir les points suivants:
- **Provider**
- **Host Name**
- **Username/E-mail**
- **Password/Key**

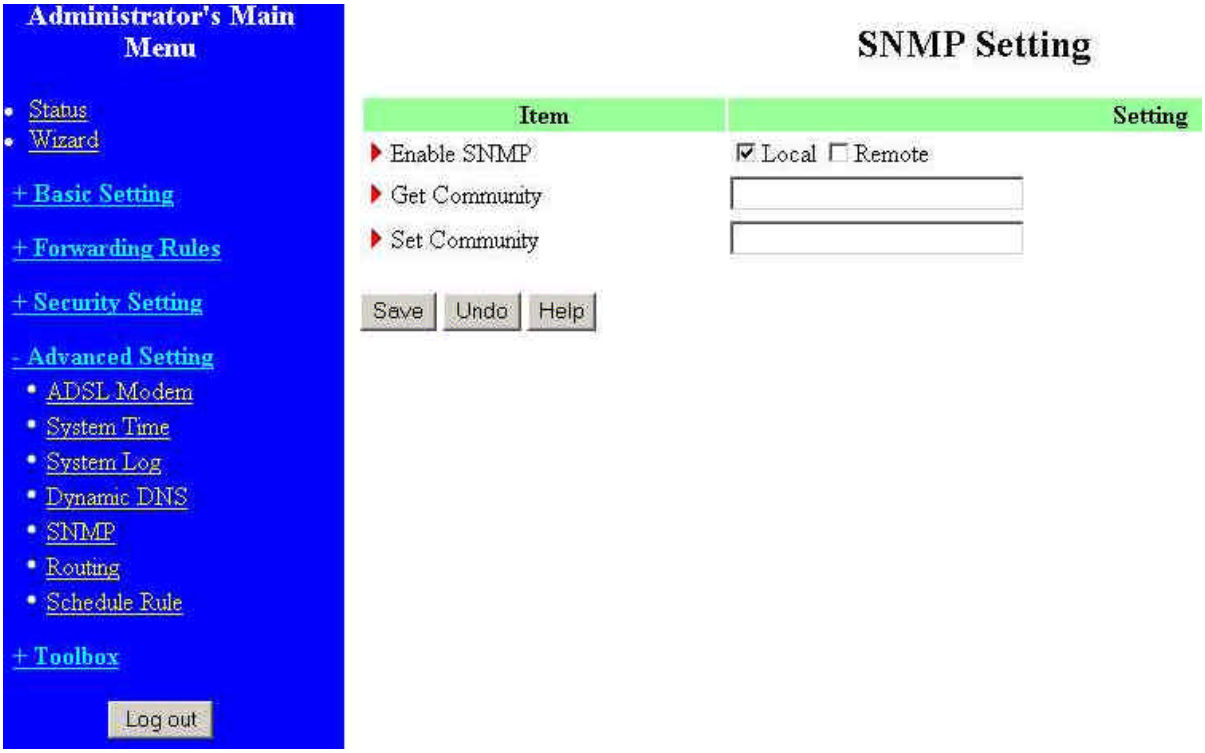
Ces informations vous sont communiquées à l'enregistrement de votre nom de domaine auprès d'un des serveurs DNS Dynamique que vous avez choisi.

Exemple:



Cliquez sur le bouton **Save** dès que la configuration du DynDNS est finie.

4.7.4 SNMP Setting / Paramétrage SNMP



En bref, **SNMP** - **Simple Network Management Protocol** - est un protocole conçu pour donner à un utilisateur la capacité de gérer à distance un ordinateur du réseau en surveillant les évènements du réseau.

Enable SNMP

Vous devez cocher la case **Local** ou **Remote** ou les deux, pour activer la fonction **SNMP**. Si la case **Local** est cochée, ce périphérique va répondre à toutes requêtes du réseau LAN. Si la case **Remote** est cochée, ce périphérique va répondre à toutes requêtes en provenance du port WAN.

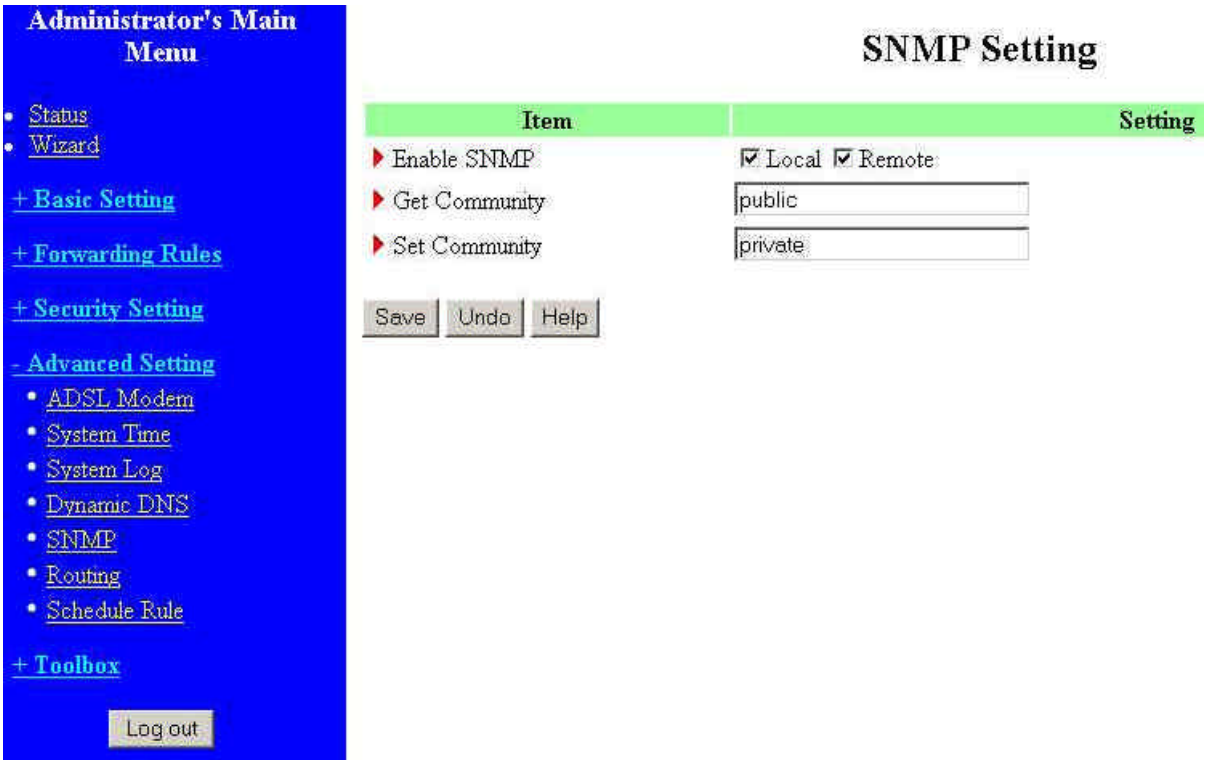
Get Community

Saisissez la communauté **GetRequest** à laquelle le routeur doit répondre.

Set Community

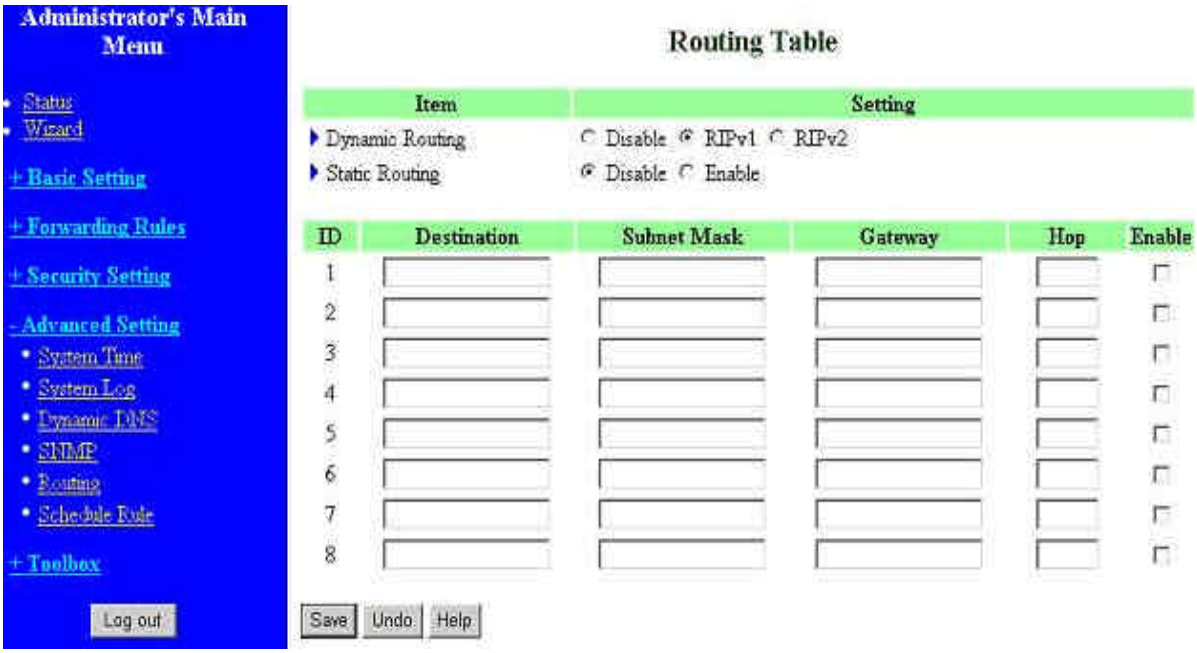
Saisissez la communauté **SetRequest** qui sera acceptée par le routeur.

Exemple:



1. Ce périphérique va répondre à tous clients SNMP dont la valeur **GetCommunity** est paramétrée comme **"public"**.
2. Ce périphérique va répondre à tous clients SNMP dont la valeur **SetCommunity** est paramétrée comme «**private**».
3. Ce périphérique répondra à toutes requêtes provenant du port **LAN** ou du port **WAN**.

4.7.5 Routing Table / Table de routage



Les tables de routages vous permettent d'établir des chemins de transferts des paquets entre les interfaces physiques des routeurs. Si vous avez plus d'un routeur et plus d'un réseau, vous devez activer la table de routage pour permettre aux paquets de trouver leur chemin et permettre aux différents sous réseau de communiquer ensemble.

Routing Table: pour paramétrer les tables de routages Statiques et Dynamiques.

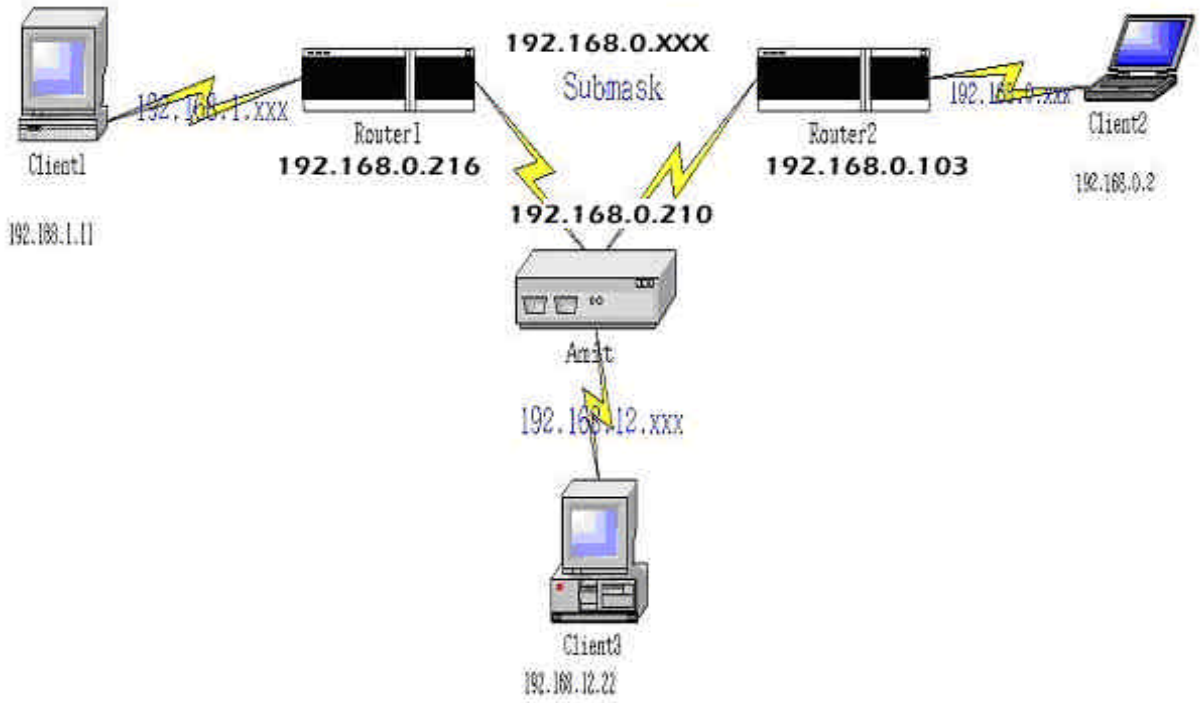
- **Dynamic Routing:**

  RIP - **Routing Information Protocol** - échange les informations de routes pour les ordinateurs du réseau entre routeurs. Sélectionnez **RIPv2** si vous avez plusieurs sous réseau dans votre réseau local. Sinon sélectionnez **RIPv1** si vous avez besoin de ce protocole.

- **Static Routing**:

  Vous pouvez créer jusqu'à 8 routes statiques. Vous pouvez entrer **l'adresse IP de destination**, le **masque de sous réseau**, la **passerelle**, le **nombre de saut** puis activer ou désactiver la règle en cochant ou décochant la case **Enable**.

Exemple:



Configuration du routeur qui fait office de NAT:

Destination	Subnet Mask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.0.216	1	?
192.168.0.0	255.255.255.0	192.168.0.103	1	?

Si par exemple, **Client3** (192.168.12.22) veut envoyer un paquet vers **Client2** (192.168.0.2), il va utiliser la table de routage pour déterminer son chemin, il passera donc par l'adresse IP 192.168.0.103 (**Router2**).
Et s'il veut communiquer avec **Client1** (192.168.1.11), il passera par **Router1** qui est en 192.168.0.216.
Chaque règle peut-être activée ou désactivée individuellement.
A la fin de la configuration, cliquez sur le bouton **Save** pour sauvegarder les changements.

4.7.6 Schedule Rule / Règles horaires

Vous pouvez paramétrer des règles pour activer ou désactiver certains services à des heures spécifiques. Pour cela, cochez la case **Enable** se trouvant en face de **Schedule**.

Puis cliquez sur le bouton **"Add New Rule"**

Vous pouvez définir une règle puis paramétrer la date et l'heure de connexion et de déconnexion du service. L'exemple ci-dessous montre que le service ftp-time s'active tous les jours à 14h10 puis s'arrête à 16h20. Donc chaque jour en dehors de cette plage le serveur ftp ne sera pas disponible.

Après la configuration de la règle1 (Rule1):

Schedule Enable

Sélectionnez la case **Enable** si vous voulez activer les règles de programmation.

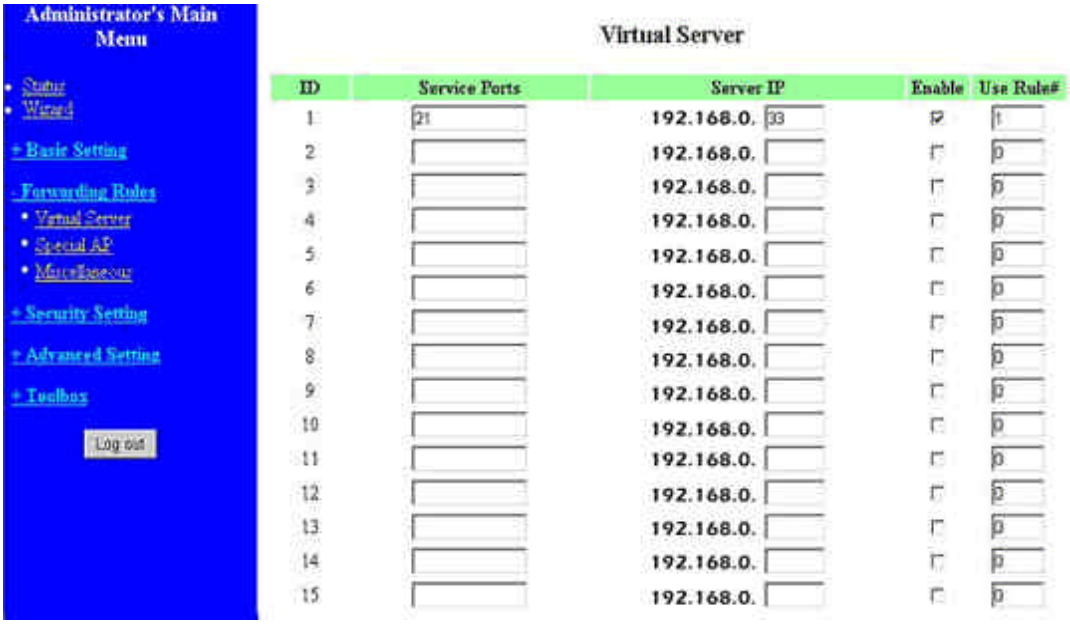
Edit

Pour éditer les règles de programmation.

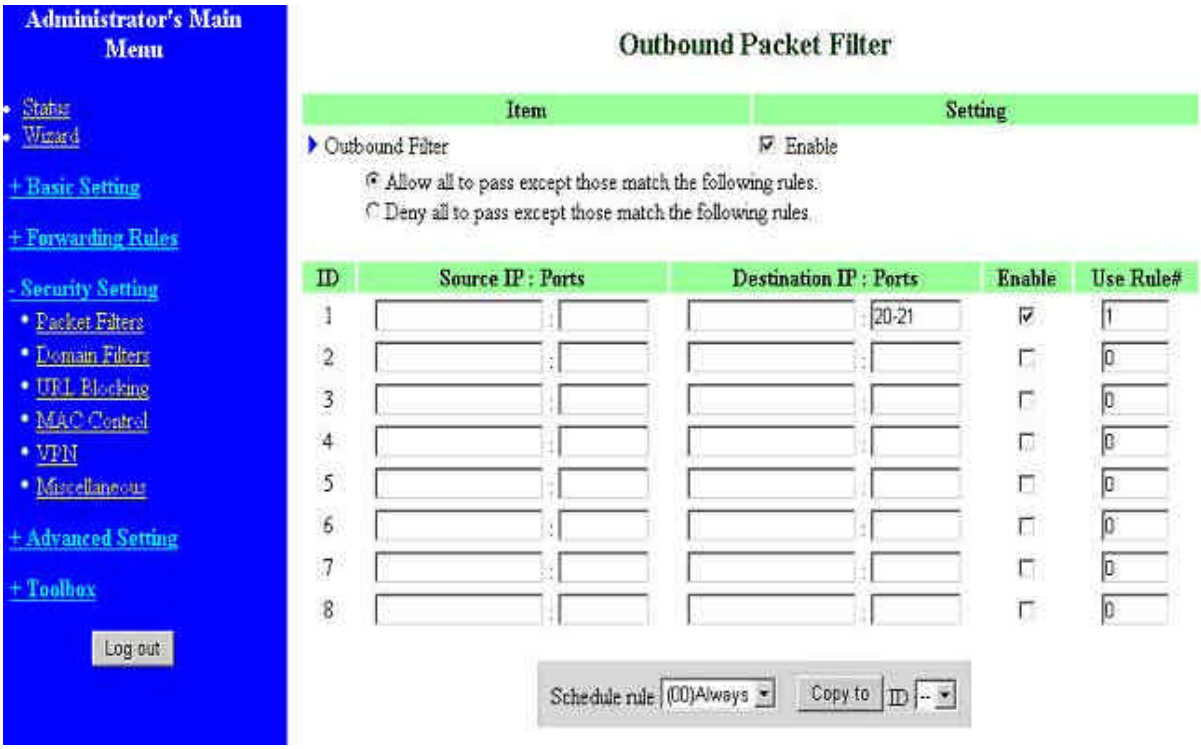
Delete

Pour supprimer les règles programmées. Vous pouvez associer ces règles avec les fonctions **Virtual Server** et **Packets Filter**, par exemple:

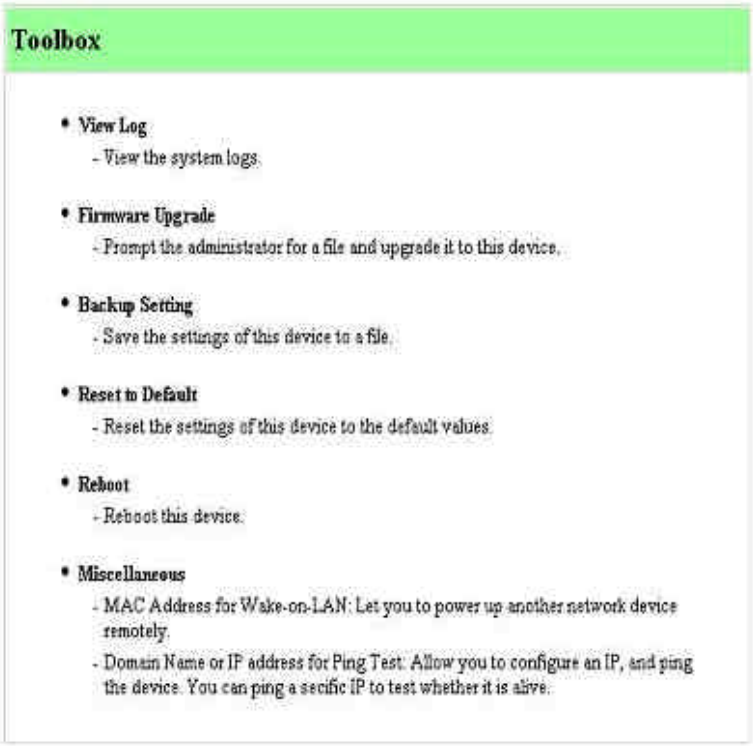
Exemple1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)



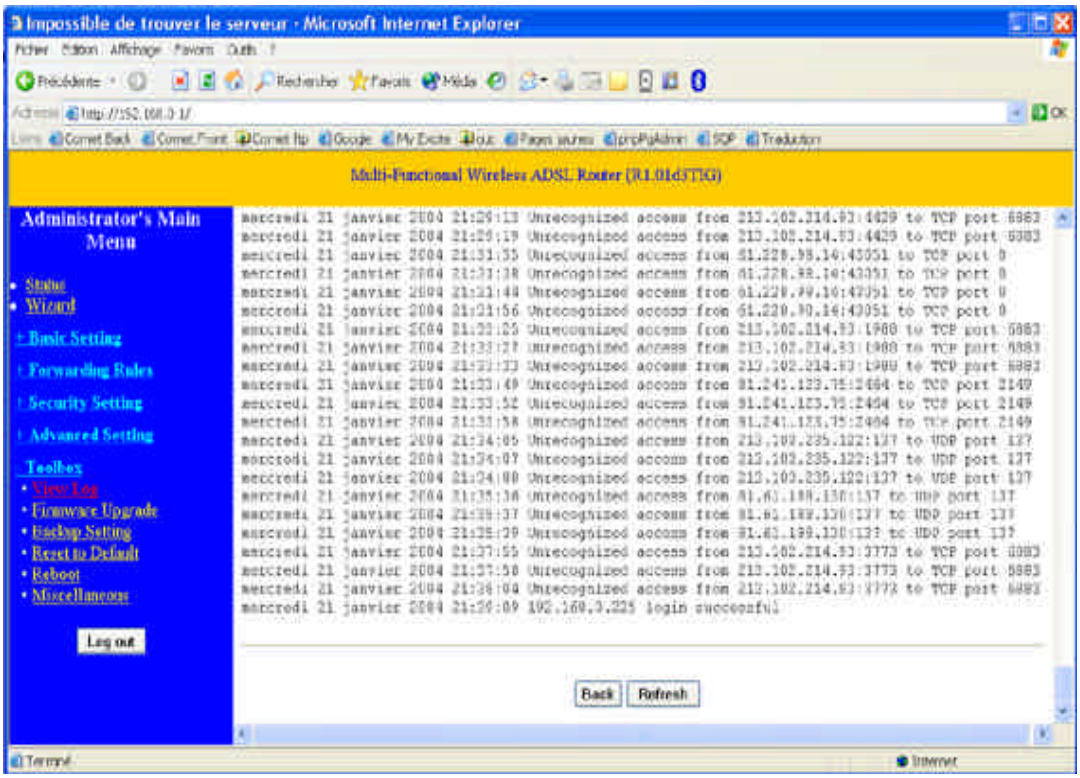
Exanple2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).



4.8 Toolbox / Utilitaires

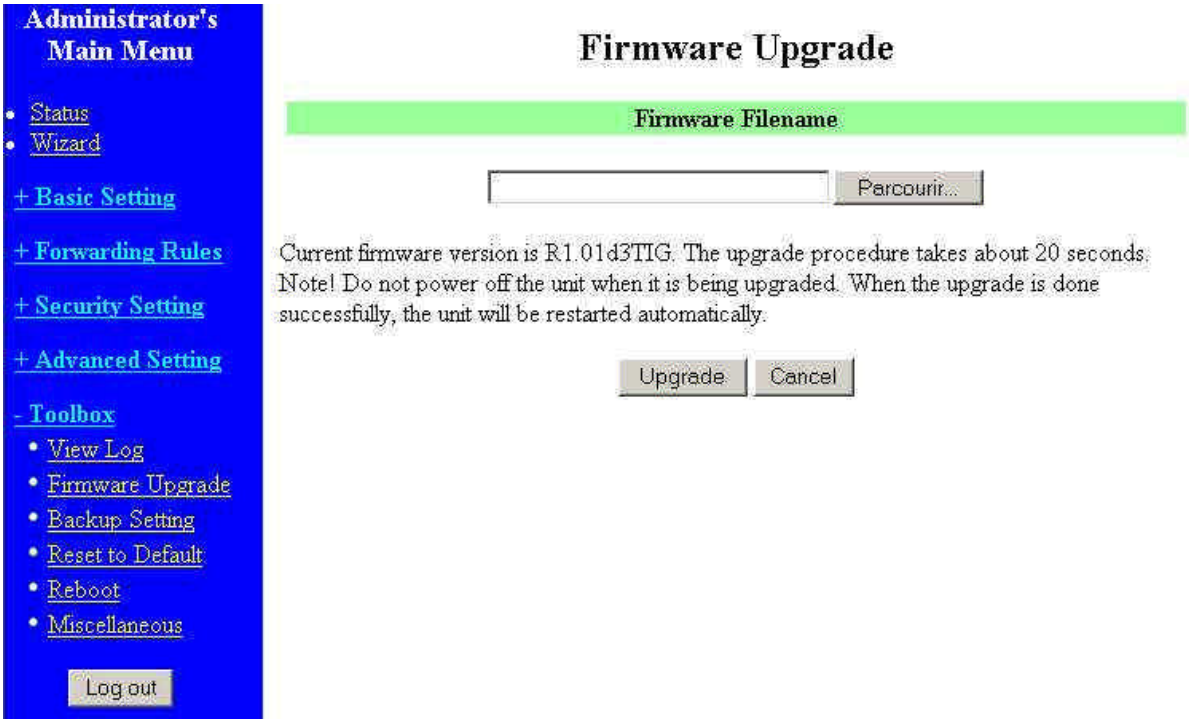


4.8.1 View Log (System Log)



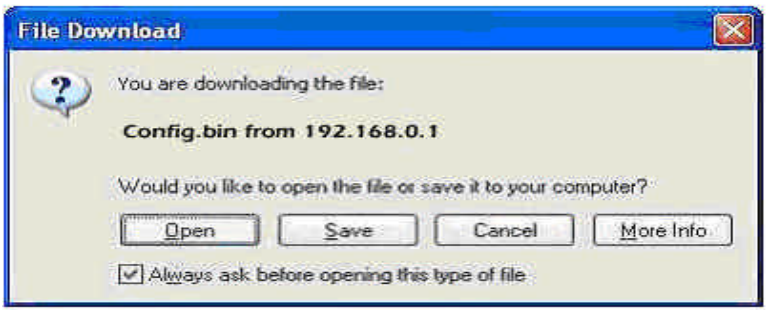
Vous pouvez visualiser le journal des évènements – Log – en cliquant sur le bouton **View Log**.

4.8.2 Firmware Upgrade / Mise à jour firmware



Vous pouvez mettre à jour le firmware du routeur en cliquant sur le bouton **Firmware Upgrade**.
Cliquez sur le bouton **Parcourir**, sélectionnez le fichier firmware puis cliquez sur le bouton **Upgrade**.
La procédure de mise à jour prend à peu près 20 secondes. Pendant cette période, ne pas éteindre le routeur.
Quand la mise à jour est terminée, le routeur redémarrera tout seul.

4.8.3 Backup Setting / Sauvegarde des paramètres



Vous pouvez sauvegarder les paramètres du routeur vers un fichier binaire en cliquant sur **Backup**

Setting. Quand vous voulez restaurer vos paramètres, il suffit de cliquer sur **Firmware Upgrade** puis sélectionnez votre fichier.

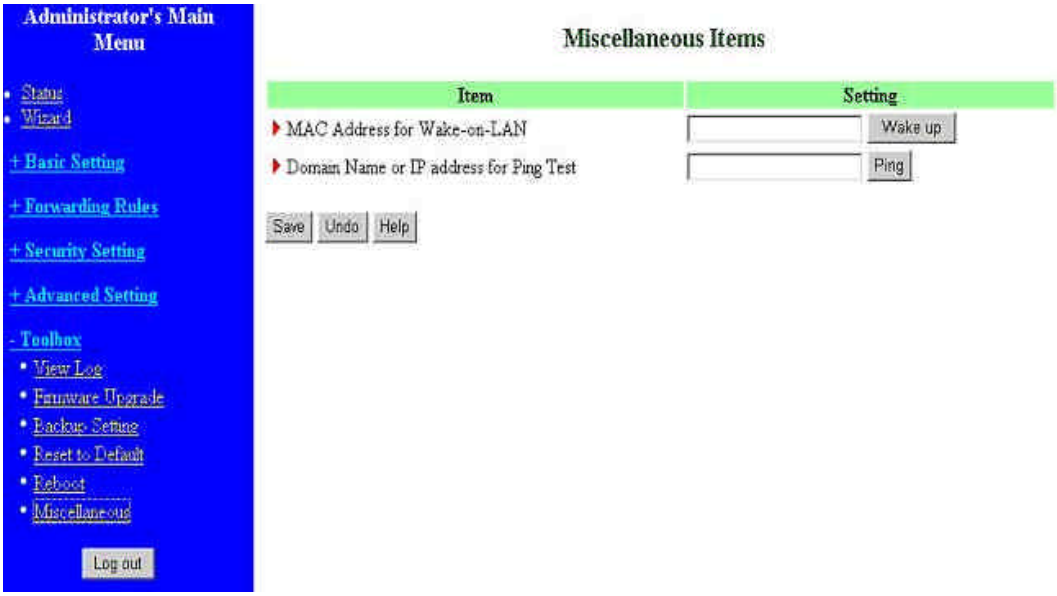
4.8.4 Reset to default / Réinitialisation des paramètres à leurs valeurs par défaut

Vous pouvez effacer tous les paramètres pour que le routeur reprenne ses valeurs d'usine en cliquant sur **Reset default**.

4.8.5 Reboot / Redémarrer

Vous pouvez redémarrer le routeur en cliquant sur **Reboot**.

4.8.6 Miscellaneous Items



MAC Address for Wake-on-LAN

Wake-on-LAN est une technologie permettant de démarrer une machine du réseau à distance. Pour utiliser cette fonction, la machine cible doit supportée le Wake-On-Lan, cette fonction doit être activée et vous devez connaître la MAC adresse de cette dernière. Saisissez sa MAC adresse puis cliquez sur le bouton Wake up, fera démarrer immédiatement la machine cible.

Domain Name or IP address for Ping Te st

Vous permet de spécifier une adresse IP puis d'exécuter la commande PING (ECHO) à destination du périphérique. Vous pouvez pinguer une adresse IP spécifique pour vérifier si elle est fonctionnelle.

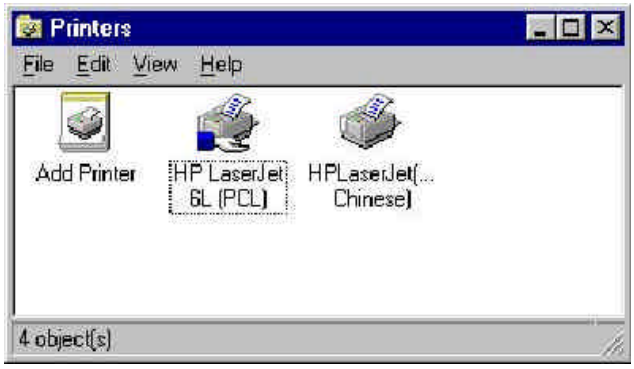
Chapitre 5 Serveur d'impression

Ce produit fournit la fonction de serveur d'impression pour les systèmes d'exploitation Microsoft Windows 95/98/Me/NT/2000/XP et les plates-formes basés sur UNIX (comme Linux)

5.1 Windows 95/98

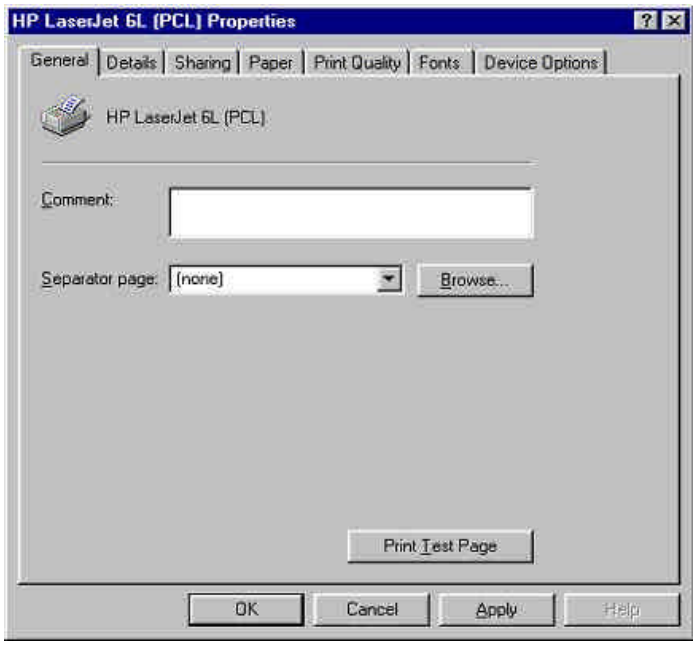
Dès que vous avez fini d'installer le logiciel décrit au chapitre3, votre ordinateur est capable d'imprimer vers l'imprimante connectée sur le routeur. Dans la suite de ce chapitre, nous utiliserons le terme **Serveur d'impression**, l'imprimante connectée au routeur.

Sur Windows 95/98, cliquez sur **Démarrer**, **Paramètres**, **Imprimantes**.

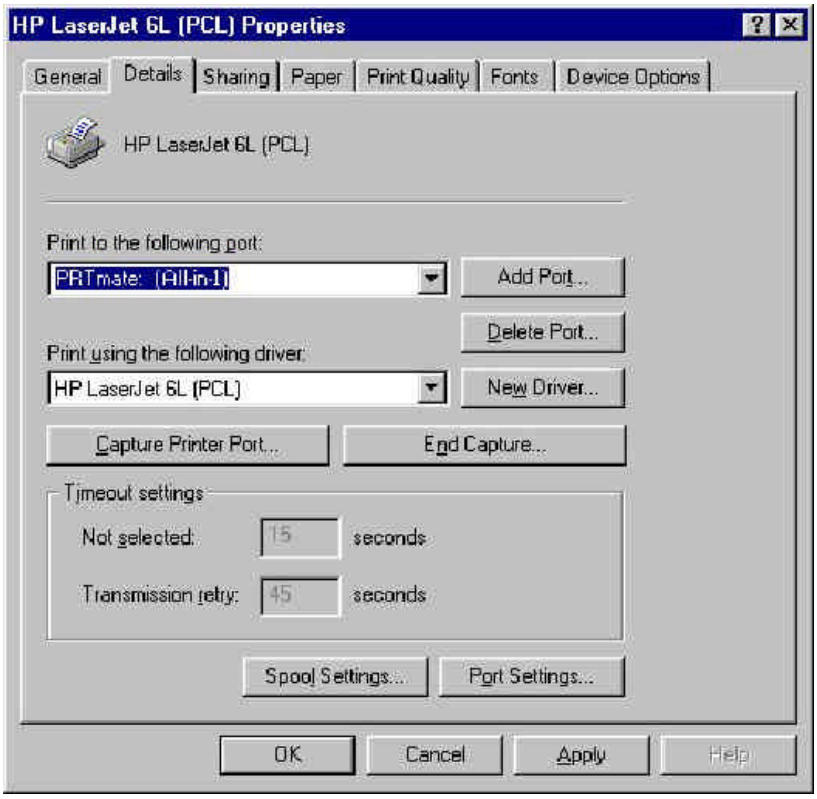


Vous pouvez maintenant configurer le serveur d'impression de ce produit.

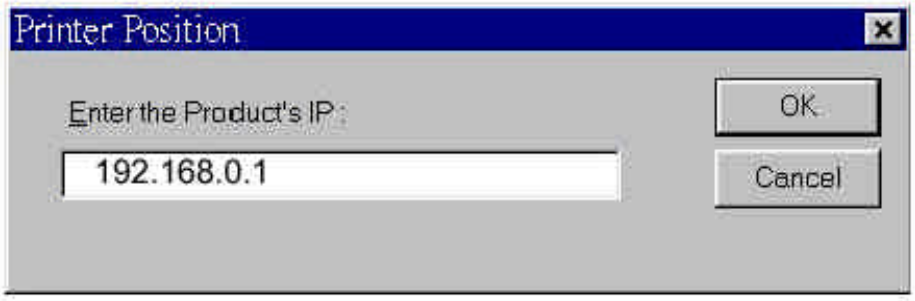
1. Sélectionnez l'icône de votre imprimante, par exemple **HP LaserJet6L**. Effectuez un click droit sur cet icône puis sélectionnez **Propriétés**.



2. Sélectionnez l'onglet **Détails**:



3. Dans la zone **Imprimer vers**, sélectionnez **PRTmate: (All-in-1)**. Vérifiez que vous avez bien installé le driver correspondant à votre imprimante.
4. Cliquez sur le bouton **Paramètres du port**.

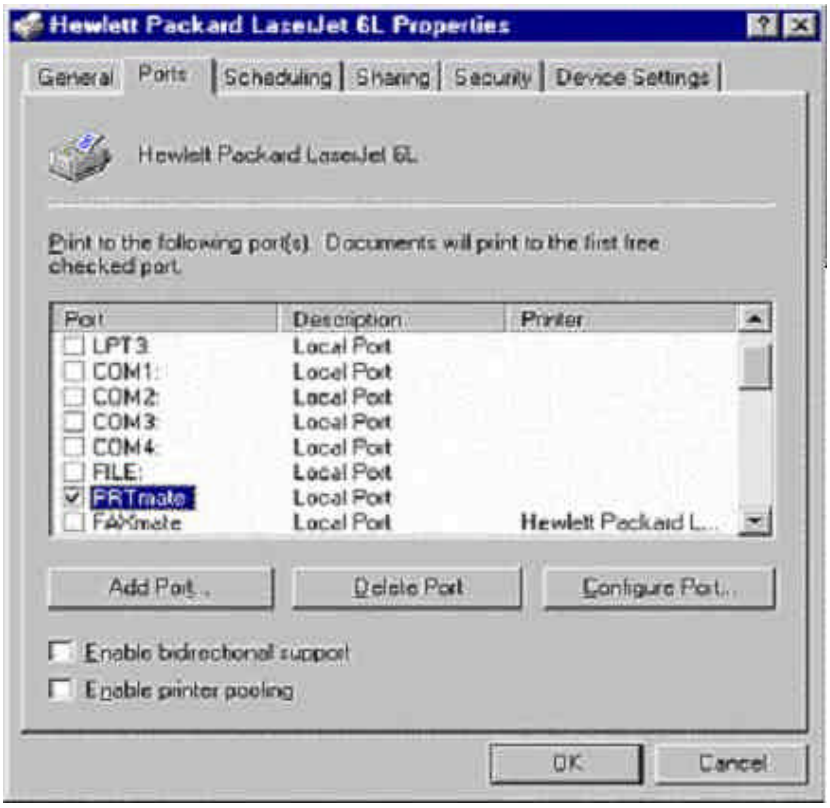


Saisissez l'adresse IP du routeur puis cliquez sur le bouton **OK**.

6. Vérifiez que tous les paramètres mentionnés plus haut sont corrects puis cliquez sur le bouton **OK**.

5.2 Windows NT

La procédure de configuration pour Windows NT est similaire à la configuration sous Windows 95/98 exceptée la fenêtre **Propriété de l'imprimante**.



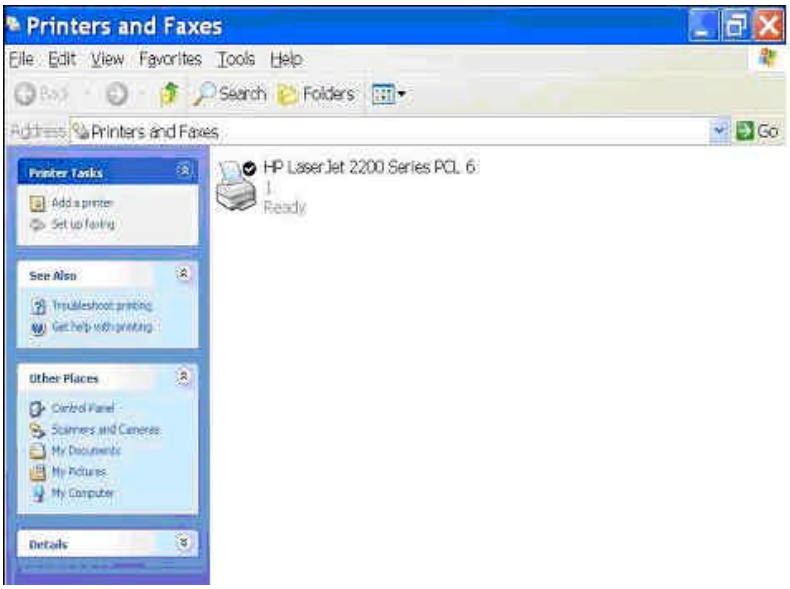
Par rapport à la configuration sous Windows 95/98, l'onglet **Détails** devient **Ports** sous Windows NT, et **Paramètres du port** devient **Configurer le port**.

5.3 Windows 2000 et XP

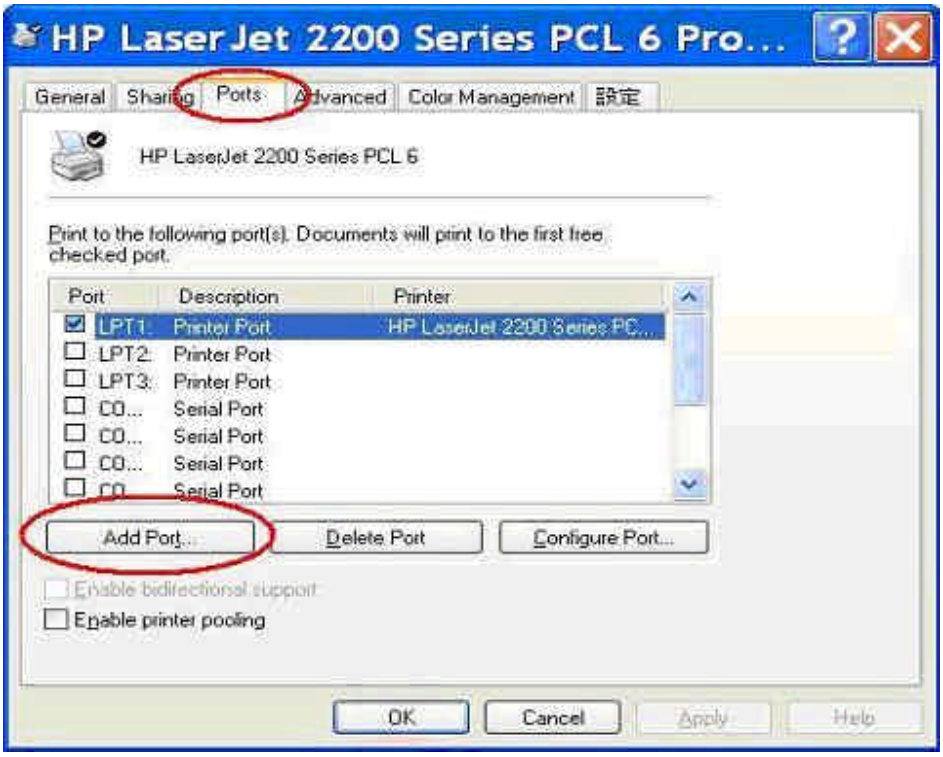
Sous Windows 2000 et XP, vous n'avez pas besoin d'installer le logiciel livré en standard. Windows 2000 et XP ont le client LPR intégré, les utilisateurs peuvent utiliser cette fonctionnalité pour imprimer.

Vous devez installer l'imprimante sur le port local LPT1 ou autres ports avant de poursuivre les instructions ci-dessous.

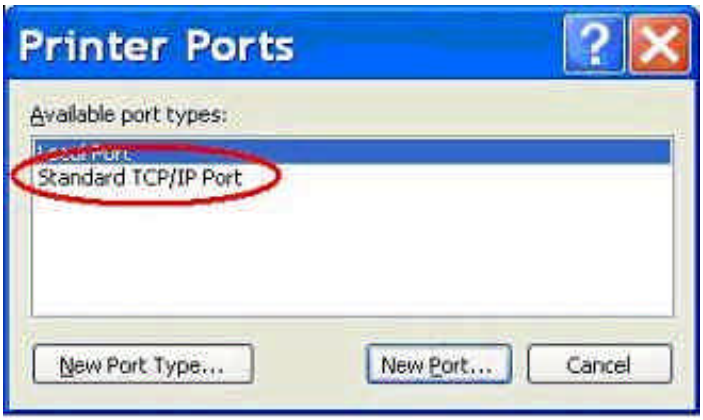
1. Ouvrez **Imprimantes et télécopieurs.**



2. Clic droit sur l'icône de l'imprimante, sélectionnez l'onglet **Ports** puis cliquez sur le bouton **Ajouter port**.

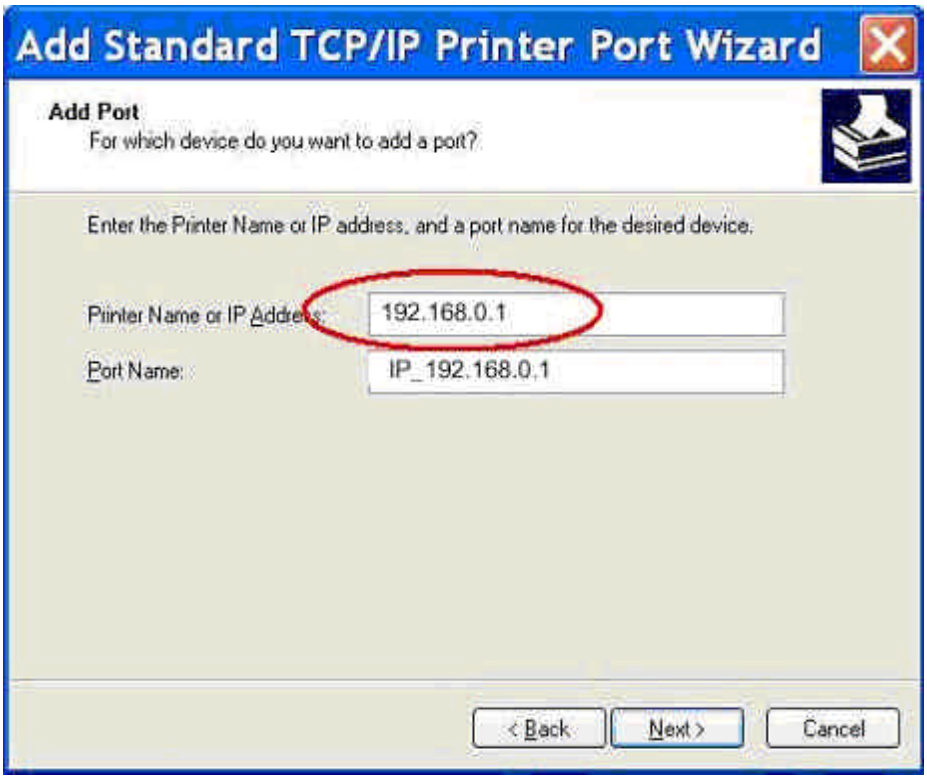


3. Sélectionnez **“Standard TCP/IP Port”**, puis cliquez sur le bouton **Ajouter un Port**.



4. Cliquez sur le bouton **Suivant** puis fournissez les informations suivantes:

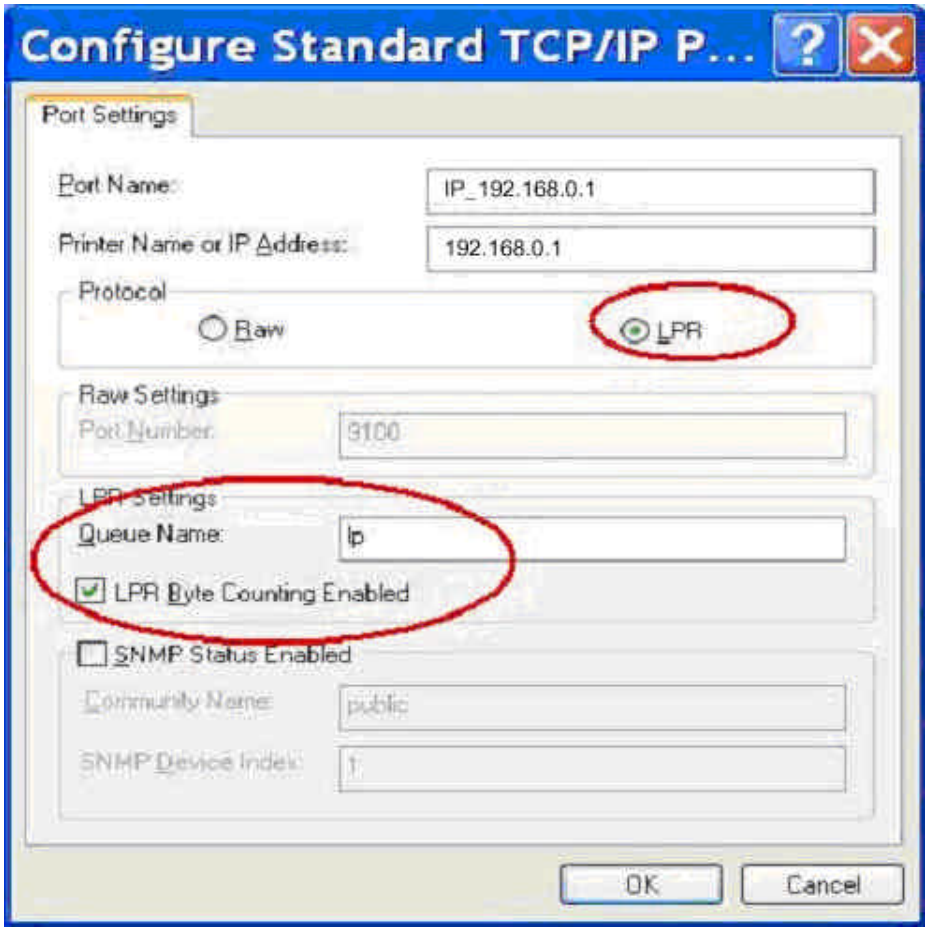
Tapez l’adresse IP du routeur puis cliquez sur le bouton **Suivant**.



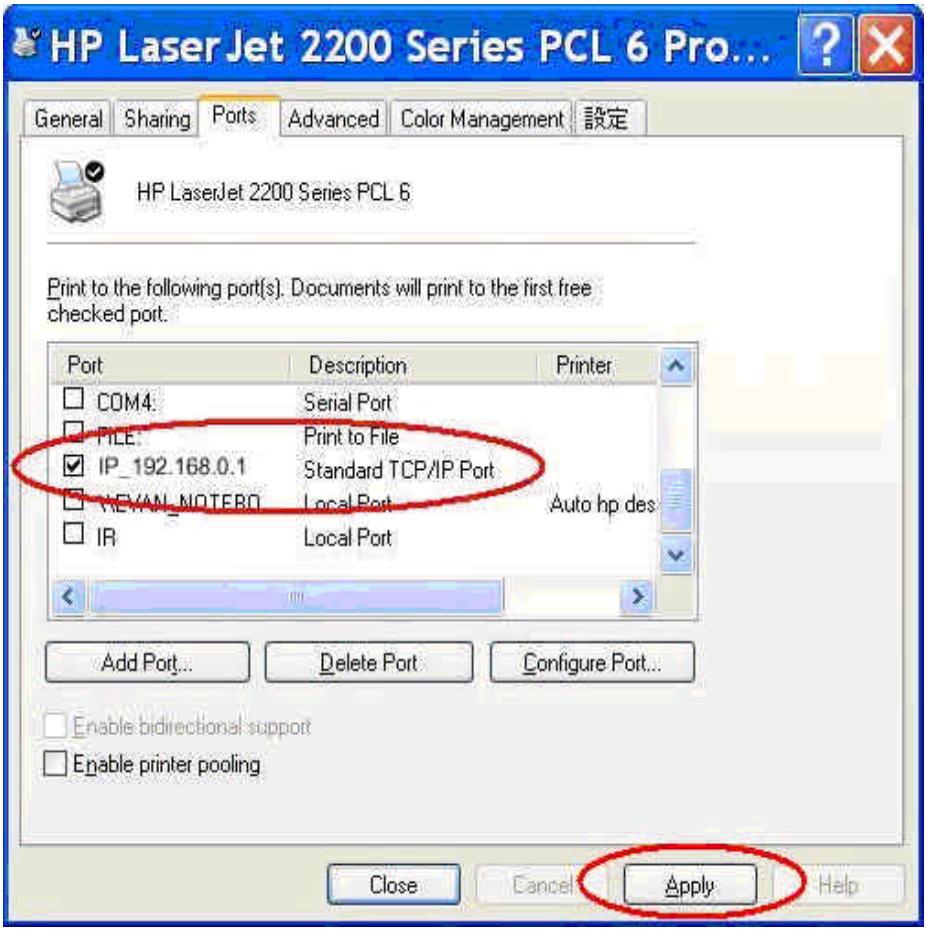
4. Sélectionnez le bouton **Personnalisé** puis cliquez sur le bouton **Paramètres**.

6. Dans la zone **Protocole**, sélectionnez **LPR**. Dans la zone **Paramètres LPR**, **Nom de la file d'attente**, tapez **lp** en minuscule (l comme lima et p comme papa).

Puis cochez la case **Comptage des octets LPR activé**.



7. Cliquez sur le bouton **OK** pour activer les changements.



5.4 Linux (exemple avec Red Hat)

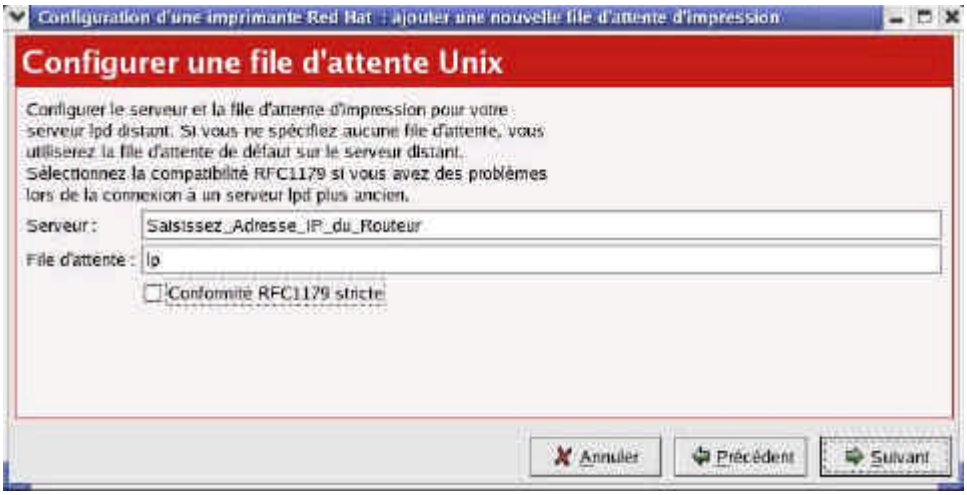
Veuillez suivre la procédure de configuration traditionnelle sous Linux pour ajouter une imprimante. Le nom de l'imprimante est «**lp**».

1. Cliquez sur le chapeau rouge, sélectionnez **Paramètres de système**, **Printing**.

2. Cliquez sur **Nouveau**, une nouvelle fenêtre s'affiche, cliquez sur **Suivant**.

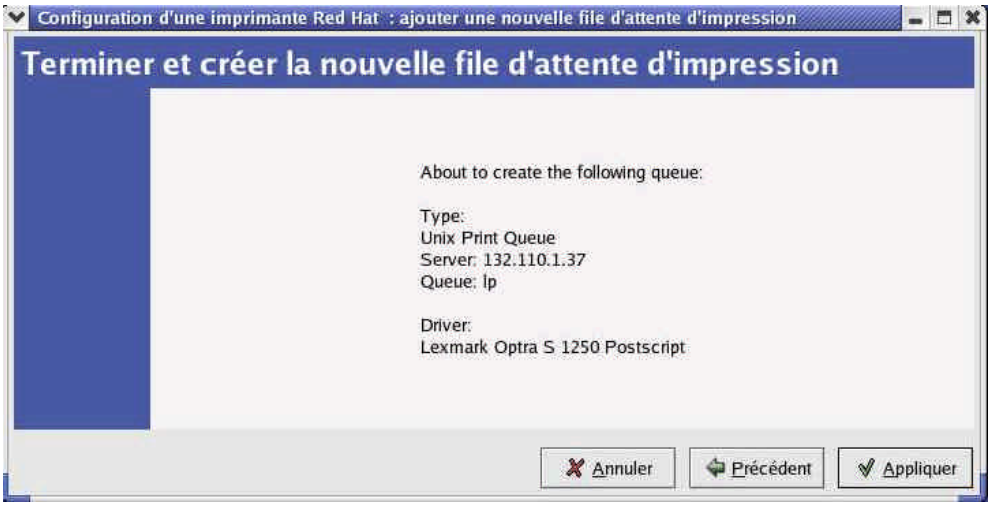
3. Saisissez le nom de votre imprimante, cochez le bouton **Imprimante Unix** (LPD), puis cliquez sur le bouton **Suivant**.

4. Saisissez **l'adresse IP du routeur** dans la zone **Serveur**, et **lp** (l comme lima et p comme papa) dans le champ **File d'attente**, puis cliquez sur le bouton **Suivant**.



5. Sélectionnez la marque et le modèle de votre imprimante puis cliquez sur le bouton **Suivant**.

6. Cliquez sur le bouton **Appliquer** pour finir l'installation de votre imprimante.



7. Enfin cliquez sur le bouton **Appliquer** pour terminer l'installation définitive.

8. Une dernière fenêtre apparaît, cliquez sur le bouton **Valider**.

Vous pouvez aussi installer l'imprimante en ligne de commande (pour les utilisateurs avancés seulement):

Linux a un client LPR intégré, vous pouvez l'utiliser pour imprimer.

Vous pouvez le paramétrer manuellement ou via l'utilitaire **printtool** depuis **Xwindows**.

PS: Le nom du spool est **lp** (lp en minuscule, l comme lima et p comme papa)

Exemple:

/etc/printcap

---

lp:\

:sd=/var/spool/lpd/lp:\

:mx#0:\

:sh:\

:rm=192.168.0.1:\

:rp=lp:\ ---------->key point

:if=/var/spool/lpd/lp/filter:

Then add the corresponding directory

#mkdir /var/spool/lpd/lp

Too see the detail, please refer to the online manual in linux.

#man printcap

5.5 Apple MACOS

Note: Avec le système Apple MACOS, il faut que l'imprimante connectée au routeur soit Postscript.

1. Démarrer le **centre d'impression** ou **Configuration de l'imprimante**. Pour cela, parcourir votre le disque système, généralement il s'appelle **Macintosh HD**, allez dans le dossier **Applications** puis **Utilitaires**.

2. Sélectionnez **Impression via IP**, saisissez l'adresse IP du routeur dans la zone **Adresse de l'imprimante**.

3. Dans la zone **File d'attente**, saisissez **lp** en minuscule (l comme lima et p comme papa).

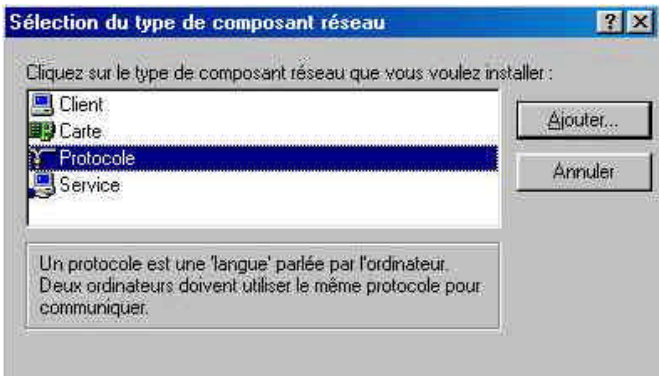
4. Dans **Modèle de l'imprimante**, sélectionnez **Générique** ou le modèle de votre imprimante. Attention il faut absolument que votre imprimante soit au format Postscript.

Annexe A Configuration TCP/IP sous Windows 95/98

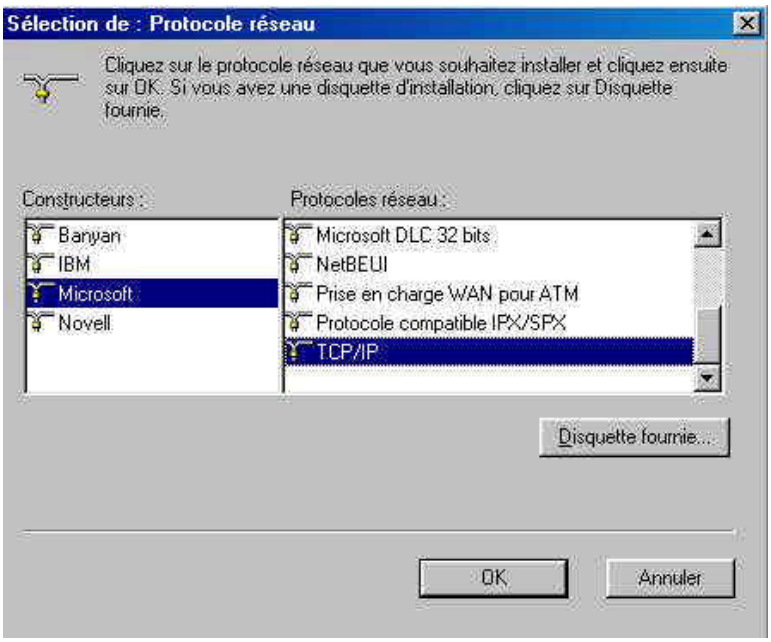
Cette section vous montre comment installer le protocole TCP/IP sur votre ordinateur. Bien sur, votre carte réseau est sensée être correctement installée dans votre ordinateur. Si ce n'est pas le cas, veuillez faire référence au manuel d'installation de votre carte avant de continuer. D'ailleurs, la section B2 vous explique comment paramétrer les valeurs TCP/IP pour fonctionner correctement avec le routeur.

A.1 Installation du protocole TCP/IP:

1. Cliquez sur le bouton **Démarrer**, sélectionnez **Paramètres** puis cliquez sur **Panneau de Configuration**.
2. Double cliquez sur l'icône **Réseau** puis sélectionnez l'onglet **Configuration**.
3. Cliquez sur le bouton **Ajouter**.
4. Double cliquez sur **Protocole** pour ajouter le protocole TCP/IP.



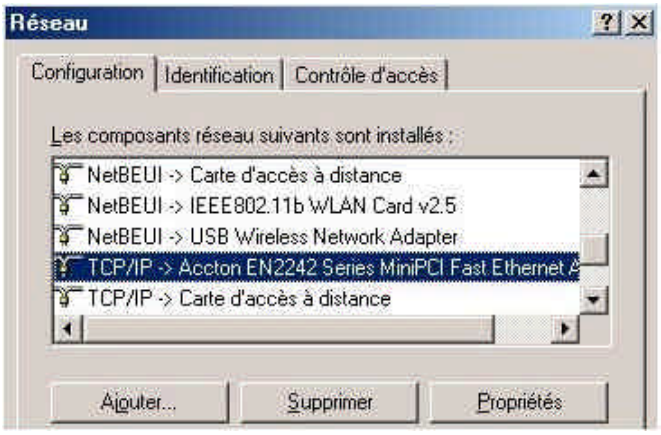
5. Sélectionnez **Microsoft** dans la partie **Constructeurs**. Sélectionnez **TCP/IP** dans la zone **Protocoles réseau**. Puis cliquez sur le bouton **OK**.



5. Le système vous demandera sûrement le CDROM système de Windows. Insérerez le CDROM dès qu'il vous le demande puis suivez les instructions jusqu'au redémarrage de votre ordinateur.

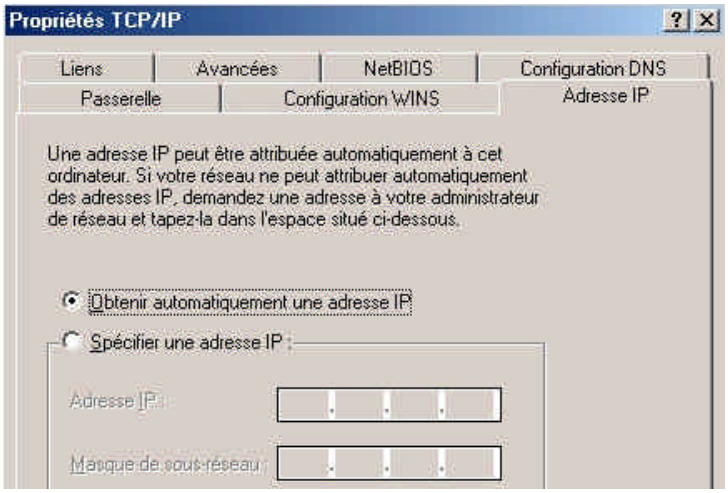
A.2 Paramétrage du protocole TCP/IP pour fonctionner avec le routeur:

1. Cliquez sur le bouton **Démarrer**, sélectionnez **Paramètres** puis cliquez sur **Panneau de Configuration**
2. Double cliquez sur l'icône **Réseau** puis sélectionnez l'onglet **Configuration**. Sélectionnez le protocole **TCP/IP** qui est affecté à votre carte réseau.

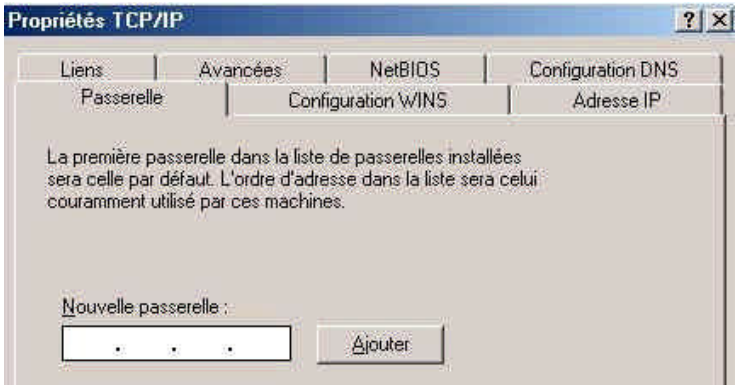


3. Cliquez sur le bouton **Propriétés** pour paramétrer le protocole TCP/IP.
4. Vous avez 2 méthodes de paramétrage:
   AConfiguration automatique:

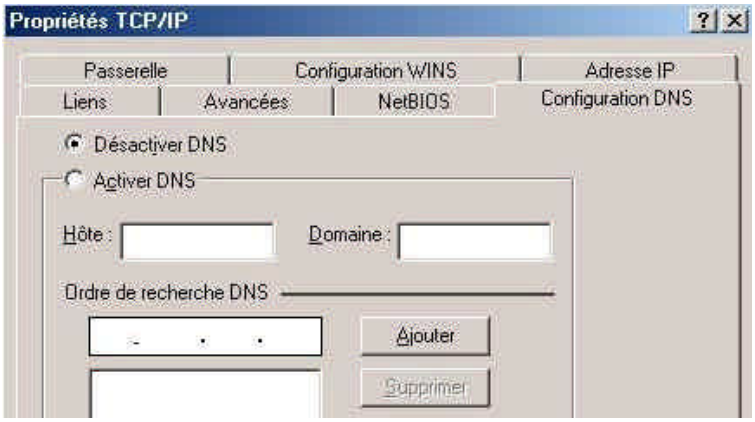
a. Sélectionnez **Obtenir automatiquement une adresse IP** depuis l'onglet **Adresse IP**.



b. Ne rien saisir dans l'onglet **Passerelle**.



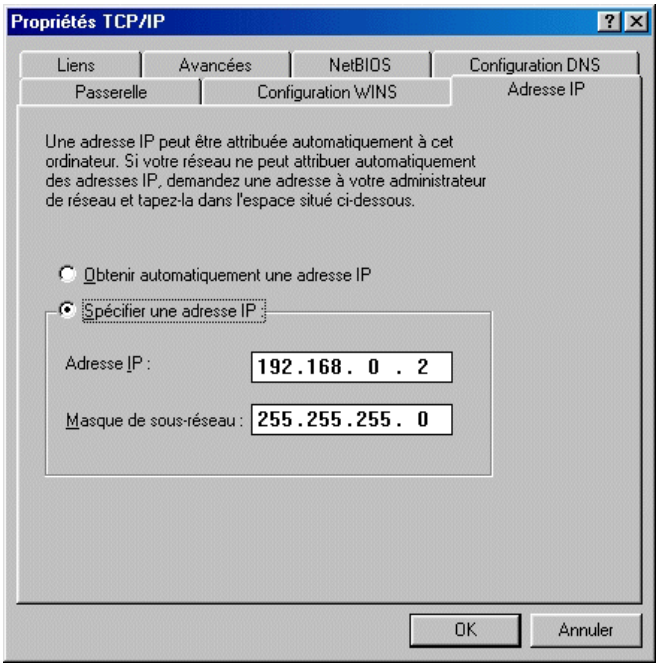
c. Dans l'onglet **Configuration DNS**, sélectionnez **Désactiver DNS**.



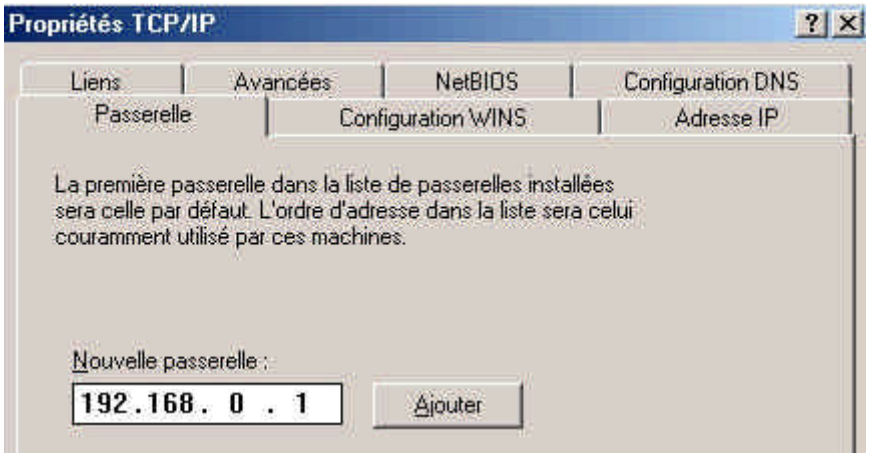
B. Configuration de l'adresse IP manuellement.

a. Sélectionnez **Spécifier une adresse IP**. L'adresse IP du routeur étant 192.168.0.1,

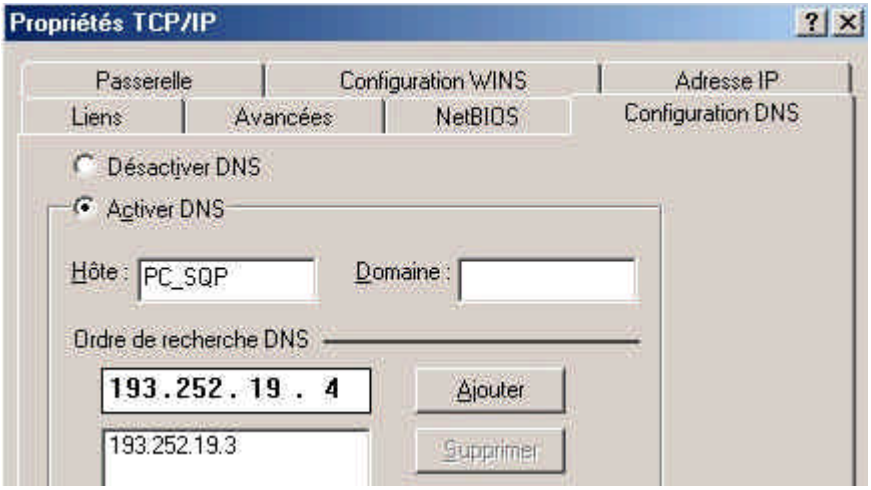
choisissez donc une adresse IP du même genre, comme par exemple 192.168.0.xxx (xxx compris entre 2 et 254). Ici nous allons choisir **192.168.0.2**, puis l'adresse de sous réseau sera **255.255.255.0**.



b. Sélectionnez l'onglet **Passerelle**, saisissez l'adresse IP du routeur, dans notre exemple ce sera **192.168.0.1**, car l'adresse du routeur est 192.168.0.1, puis cliquez sur le bouton **Ajouter**.



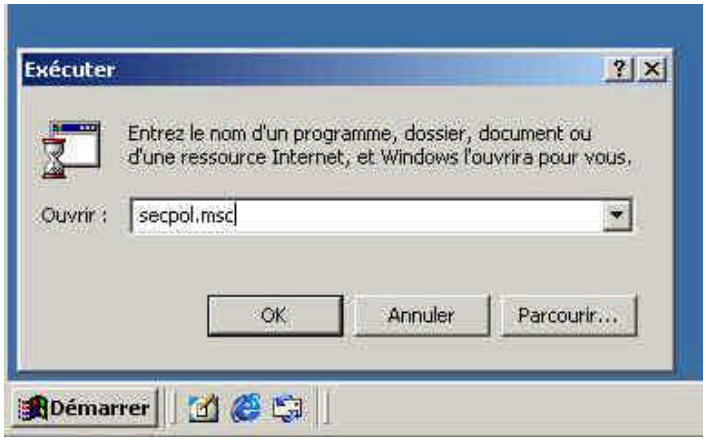
c. Sélectionnez l'onglet **Configuration DNS**, cochez le bouton **Activer DNS**, saisissez un nom dans la zone **Hôte**, saisissez l'adresse IP DNS que votre FAI vous a communiquée puis cliquez sur le bouton **Ajouter**. Dans notre exemple, nous avons saisi les 2 adresses IP DNS de Wanadoo.


Propriétés TCP/IP
Passerelle
Configuration WINS
Adresse IP
Liens
Avancées
NetBIOS
Configuration DNS
Désactiver DNS
Activer DNS
Hôte : PC_SQP
Domaine :
Ordre de recherche DNS
193.252.19 . 4
Ajouter
193.252.19.3
Supprimer

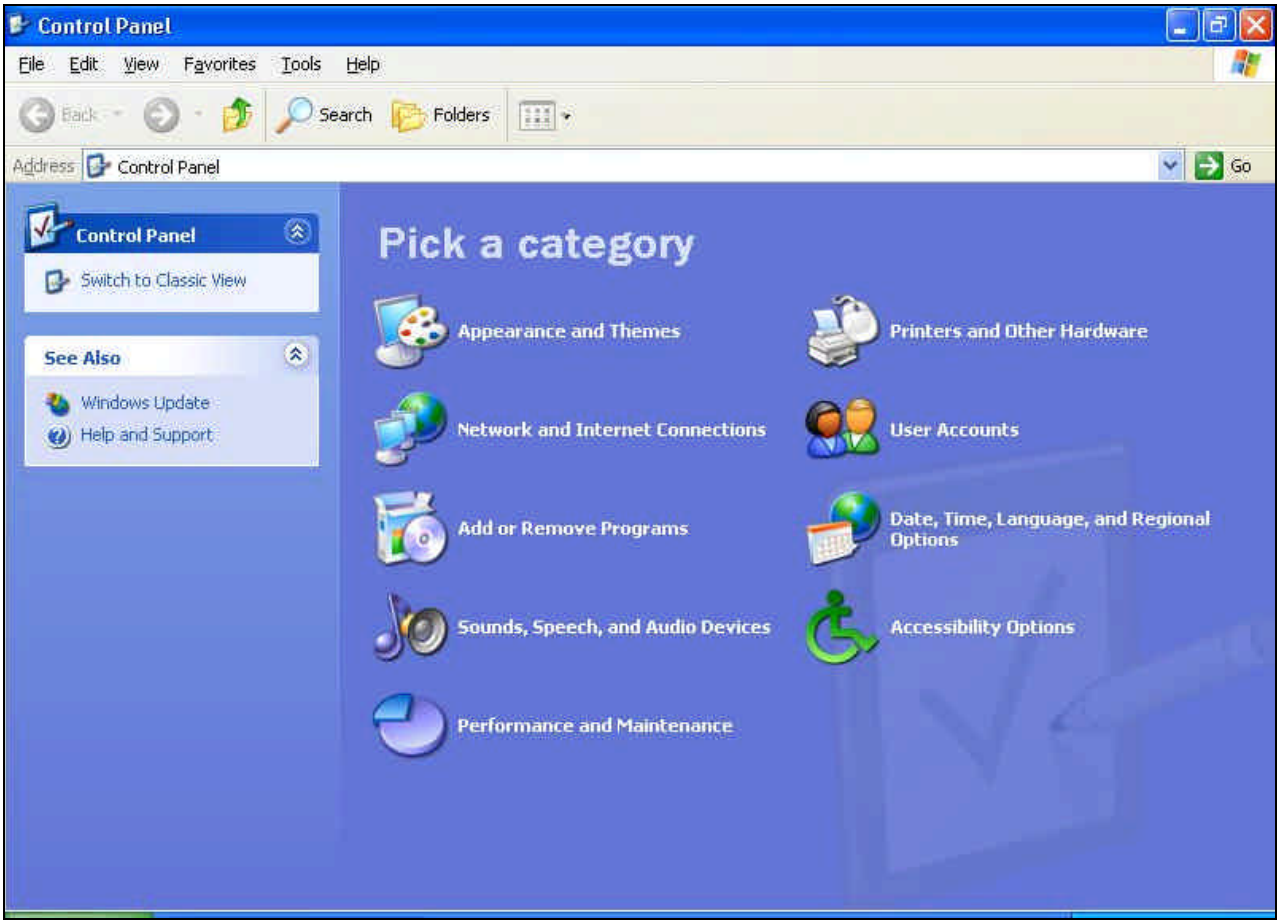
Annexe B Guide d'installation IPSec sous Win 2000/XP

Exemple: Connexion d'un client Win XP/2000 vers le Routeur VPN
(La configuration sous Windows 2000 est similaire que sous Windows XP)

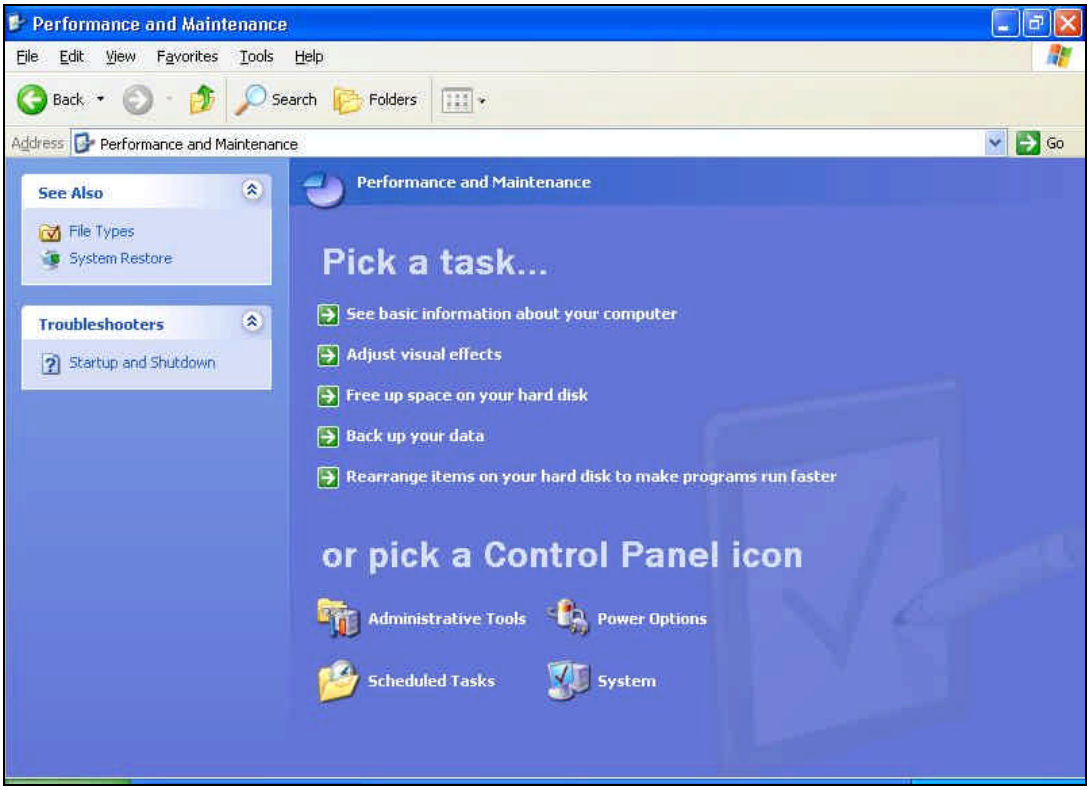
1. Sur **Windows 2000/XP**, cliquez sur **Démarrer**, **Exécuter**. Dans la zone **Ouvrir**, tapez **secpol.msc** puis cliquez sur le bouton **OK**. Sélectionnez le dossier **Stratégies locales**.



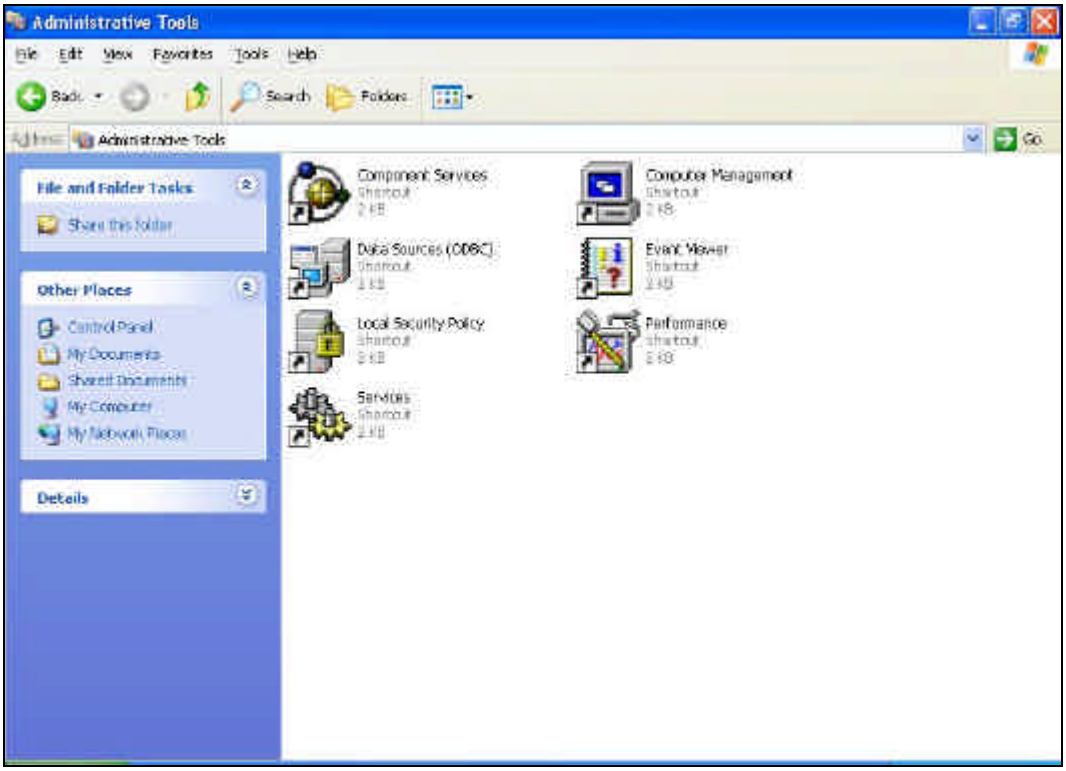
2. Ou sous Windows XP, cliquez sur **Démarrer, Paramètres, Panneau de configuration**



Double cliquez sur l'icône **Performances et maintenance**.

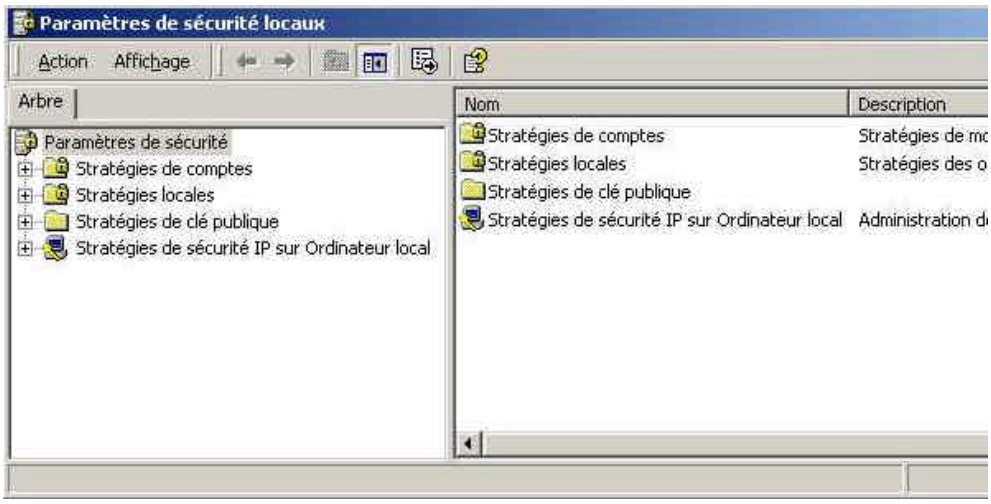


Double cliquez sur l'icône **Outils d'administration**.



stratégie de sécurité locale

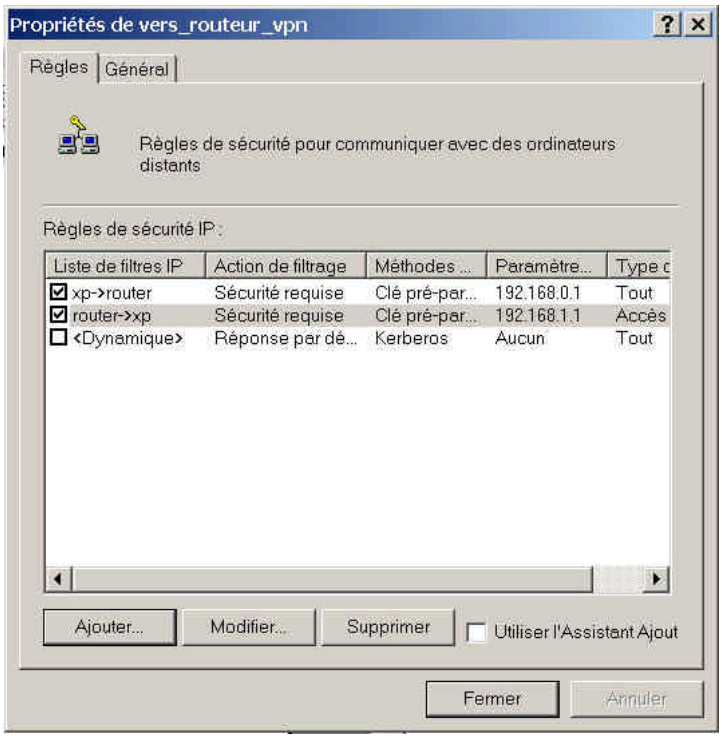
Double cliquez sur l'icône **Stratégie de sécurité locale**.



Effectuez un clic droit sur **Stratégies de sécurité IP sur Ordinateur local** puis sélectionnez **Créer une stratégie de sécurité IP**.

La fenêtre de l'assistant s'ouvre, cliquez sur le bouton **Suivant**, entrez un nom pour cette connexion (**vers_routeur_vpn** par exemple), puis cliquez sur le bouton **Suivant**.

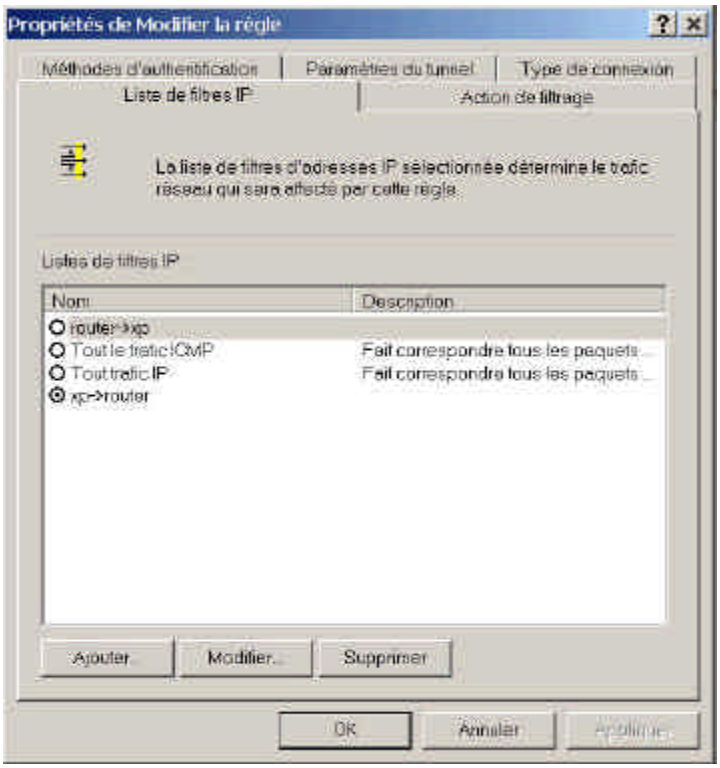
Décochez la case **Activer la règle de réponse par défaut** puis cliquez sur le bouton **Suivant**.
Vérifiez que la case **Modifier les propriétés** est cochée puis cliquez sur le bouton **Terminer**.



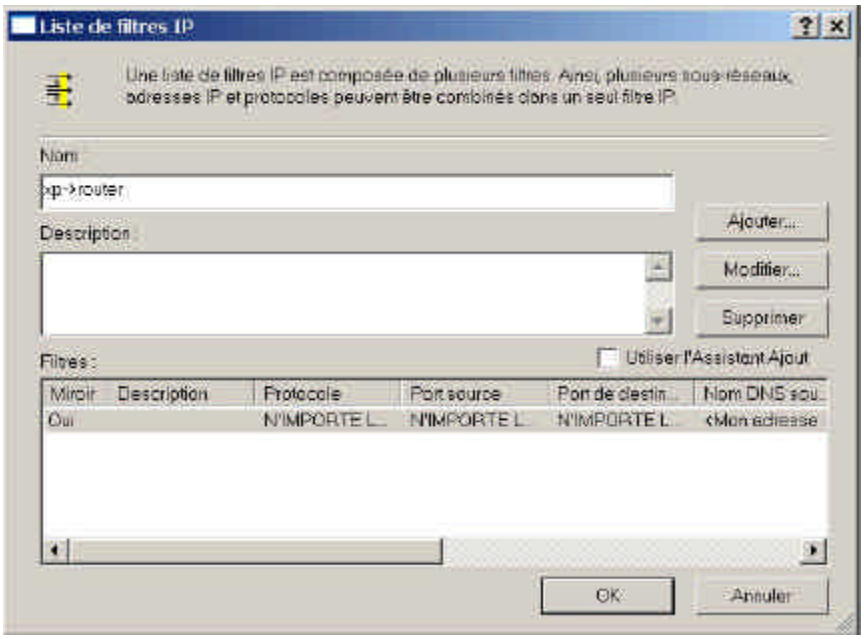
Créez 2 listes de filtre: "xp→router" et "router→xp" par exemple.

Liste de filtre 1: xp→routeur

Depuis la fenêtre **Propriétés de nouvelles règles**, désélectionnez la case **Utiliser l'Assistant Ajout** puis cliquez sur le bouton **Ajouter** pour créer une nouvelle règle.

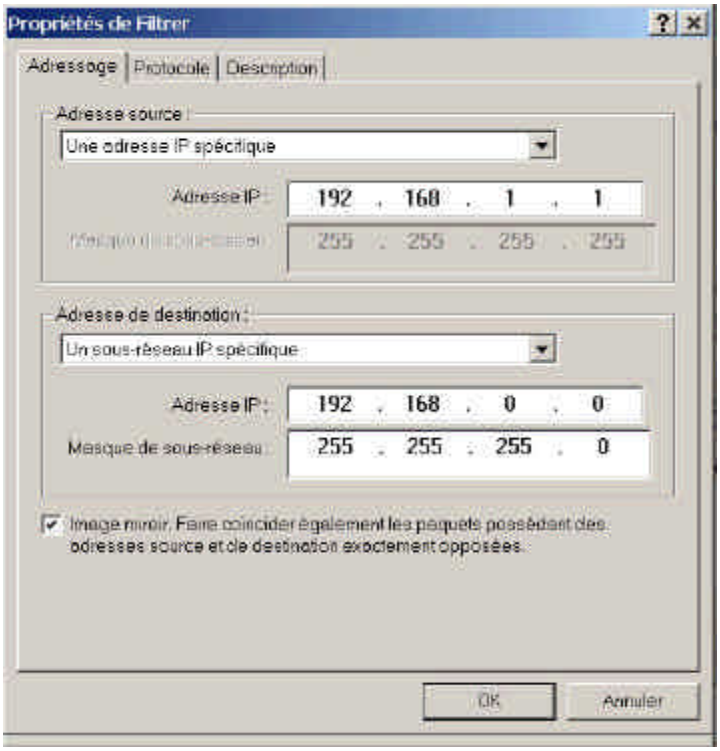


Cliquez sur le bouton **Ajouter.**



Entrez un nom, par exemple: **xp→router** puis désélectionnez la case **Utiliser l'assistant Ajout.**

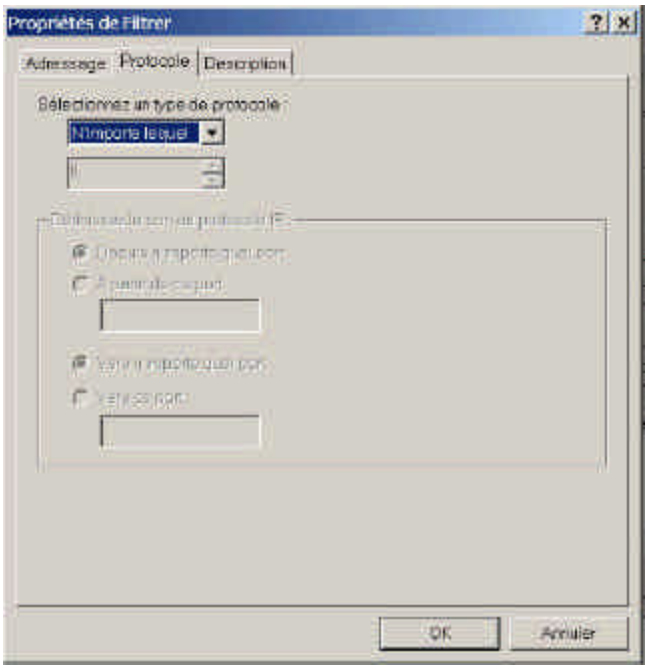
Cliquez sur le bouton **Ajouter.**



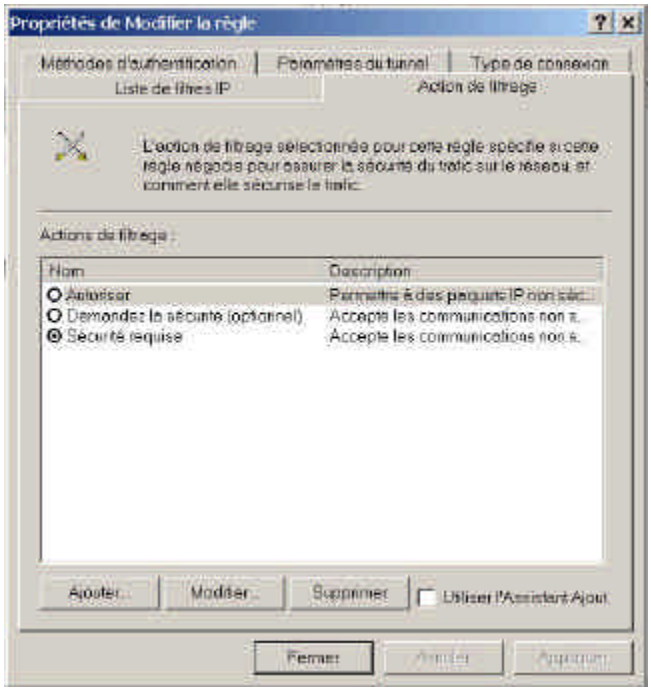
Dans le champ **Adresse source**, sélectionnez **Une adresse IP spécifique** puis saisissez l'adresse **192.168.1.1**.

Dans le champ **Adresse de destination**, sélectionnez **Un sous réseau IP spécifique**, saisissez l'adresse IP: **192.168.0.0** et un masque de sous réseau: **255.255.255.0**

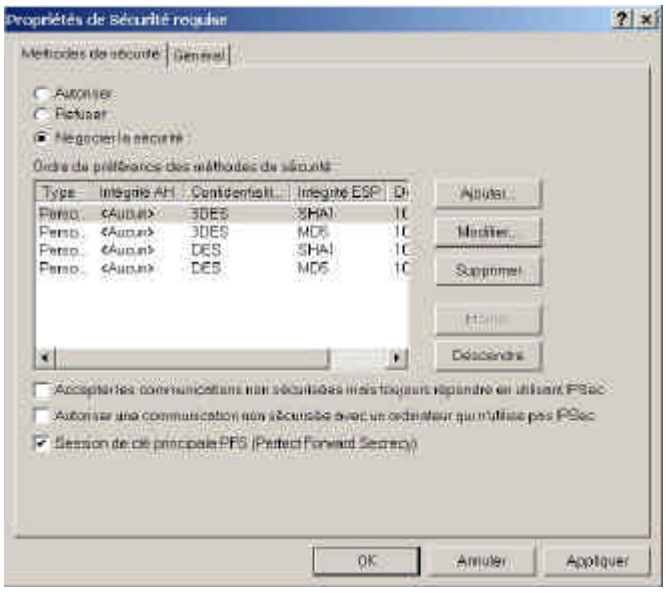
Si vous désirez un protocole pour votre filtre, cliquez sur l'onglet **Protocole**.



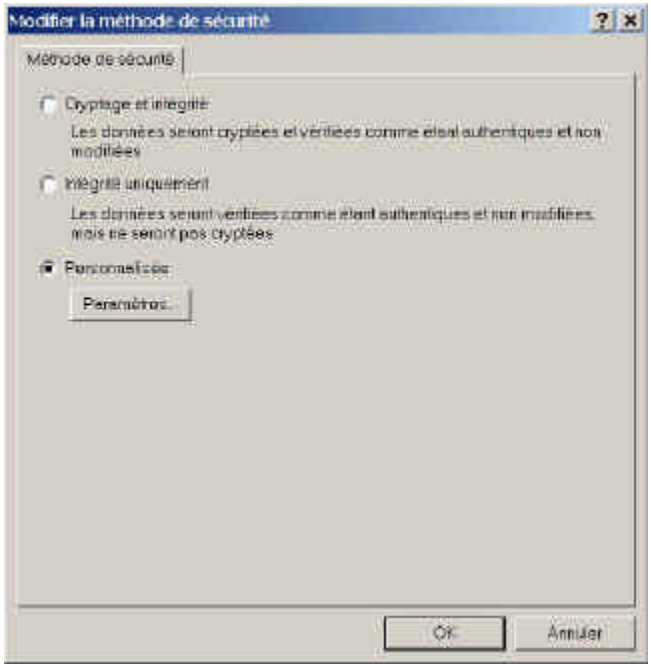
Cliquez sur le bouton **OK**. Puis cliquez sur le bouton **OK** de la fenêtre **Liste de filtre IP**



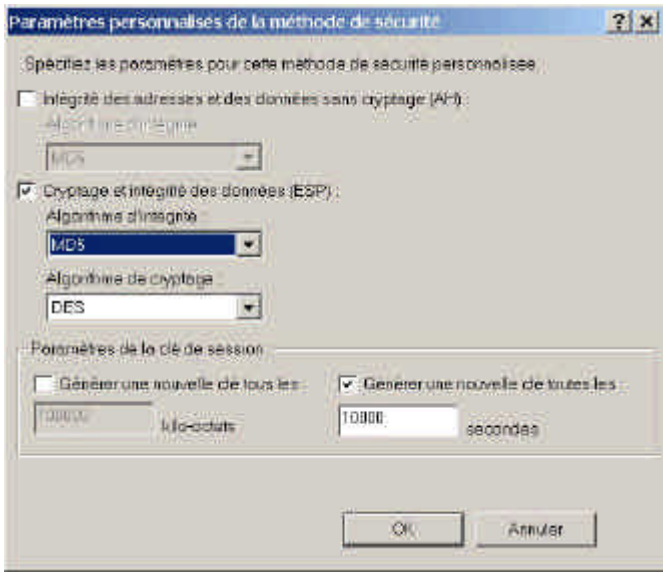
Sélectionnez l'onglet **Action de filtrage**, cochez le bouton **Sécurité requise** puis cliquez sur le bouton **Modifier**.



Cochez le bouton **Négocier la sécurité**, cochez la case **Session de clé protocole PFS (Perfect Forward Secrecy)** puis cliquez sur le bouton **Modifier**.



Cochez le bouton **Personnalisée (pour les utilisateurs expérimentés)** puis cliquez sur le bouton **Paramètres**.



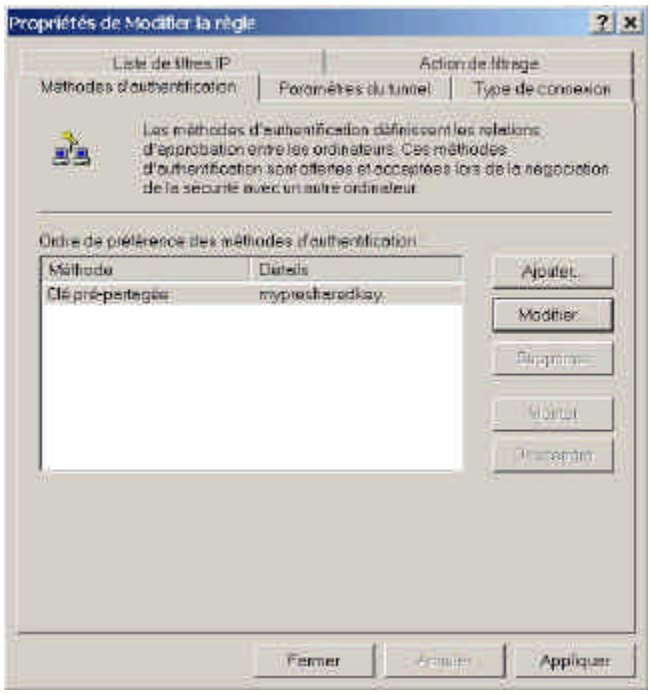
Sélectionnez **Cryptage et intégrité des données (ESP)**

Configurez **l'Algorithme d'intégrité** sur **MD5**

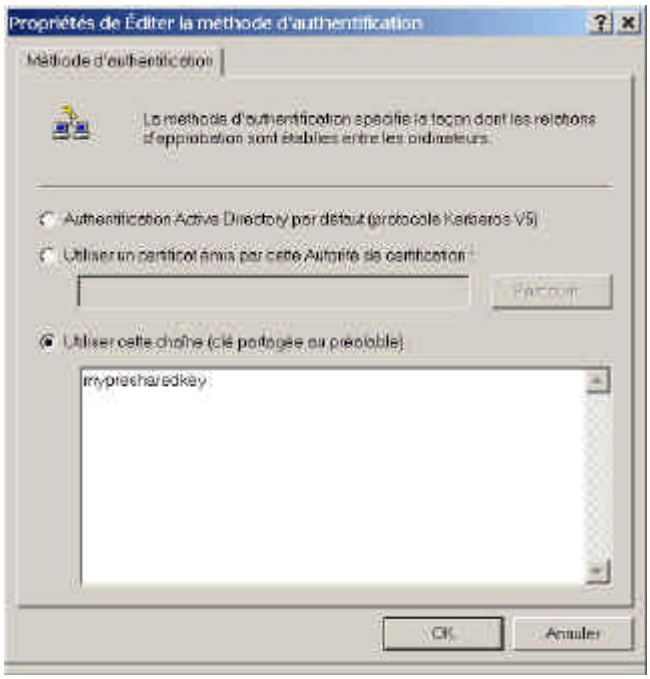
Configurez **l'Algorithme de cryptage** sur **DES**

Configurez **Générer une nouvelle clé tous les:** sur **10000** secondes

Cliquez sur le bouton **OK** jusqu'à revenir sur la fenêtre **Propriétés de nouvelle règle.**

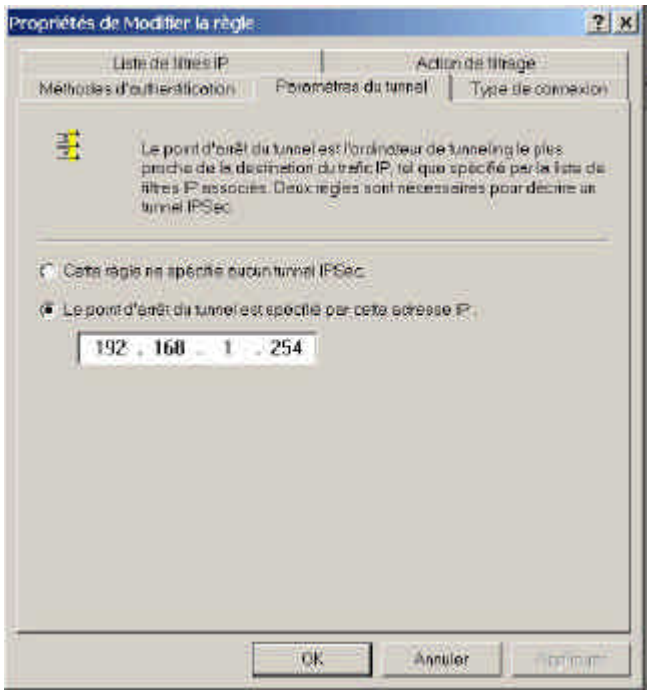


Sélectionnez **Méthodes d'authentification**, cliquez sur le bouton **Ajouter**.



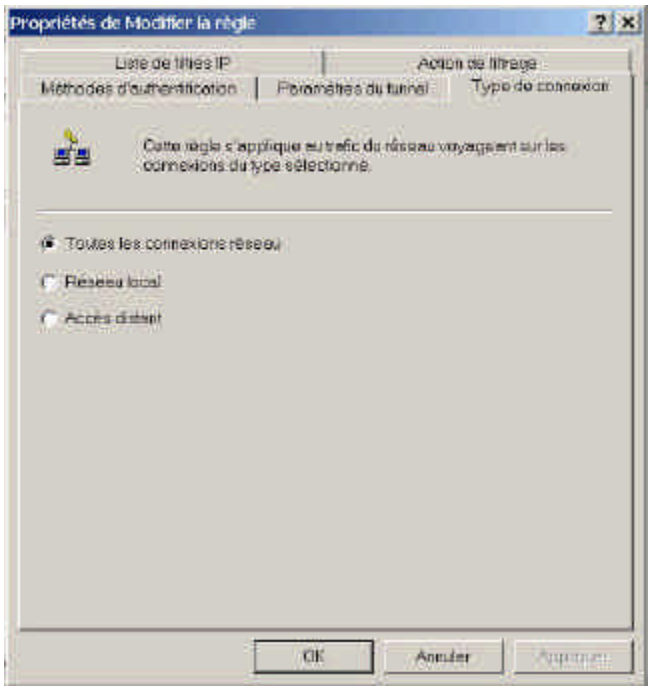
Sélectionnez le bouton **Utiliser cette chaîne (clé partagée au préalable)**, puis saisissez votre clé partagée comme par exemple **mypresharedkey**, puis cliquez sur le bouton **OK**.
Cliquez sur le bouton **OK** depuis l'onglet **Méthodes d'authentification**.

Sélectionnez l'onglet **Paramètres du tunnel**.



Configurez Le point d'arrêt du tunnel est spécifié par cette adresse IP sur 192.168.1.254.

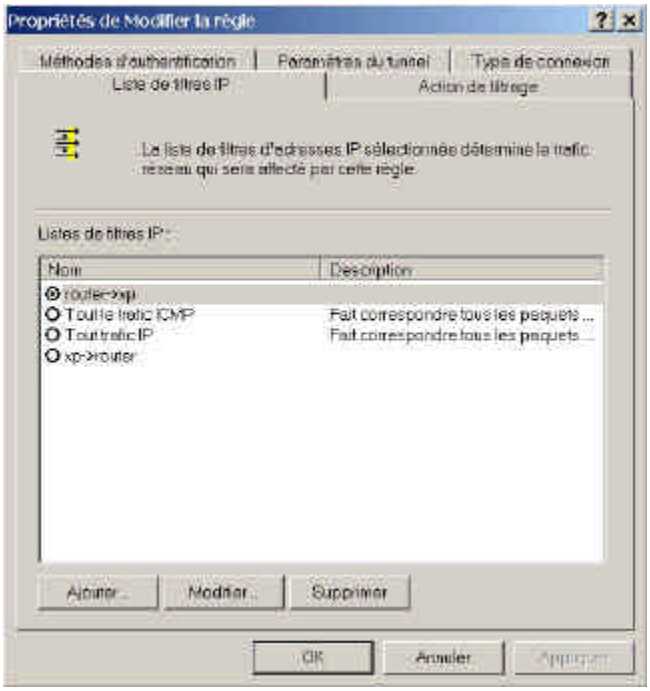
Sélectionnez l'onglet **Type de connexion**.



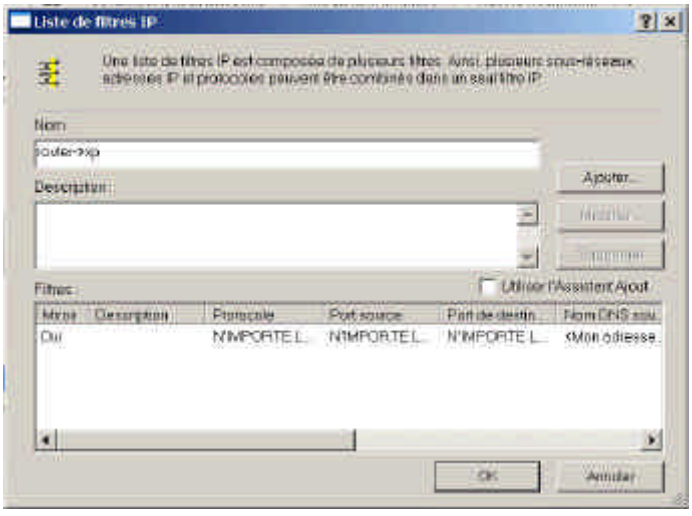
Sélectionnez **Toutes les connexions réseau**.

Tunnel 2: router->xp

Depuis la fenêtre **Propriétés de nouvelles règles**, désélectionnez la case **Utiliser l'Assistant Ajout** puis cliquez sur le bouton **Ajouter** pour créer une nouvelle règle.

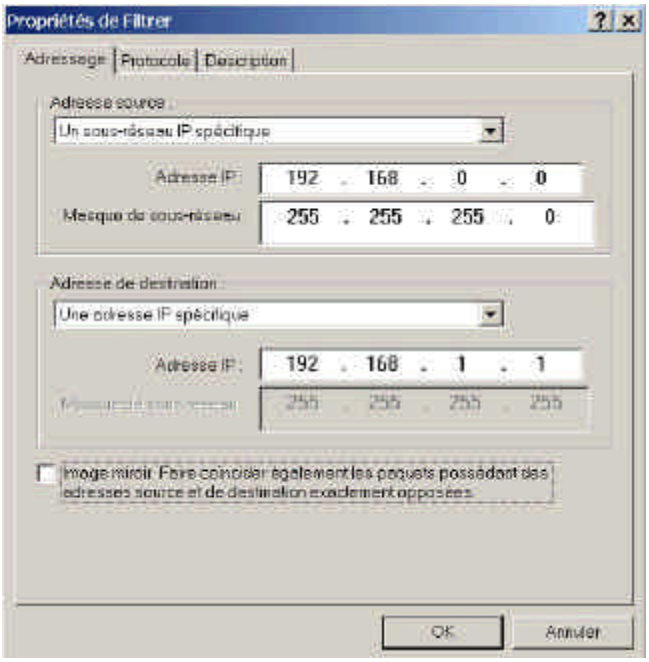


Cliquez sur le bouton **Ajouter**



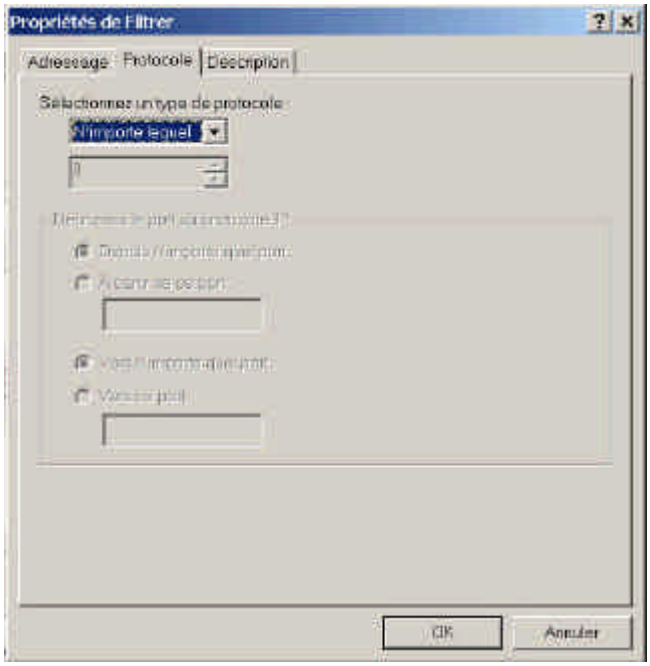
Entrez un nom dans la zone **Nom**, par exemple **routeur→xp**.

Désélectionnez la case **Utiliser l'Assistant Ajout** puis cliquez sur le bouton **Ajouter**.

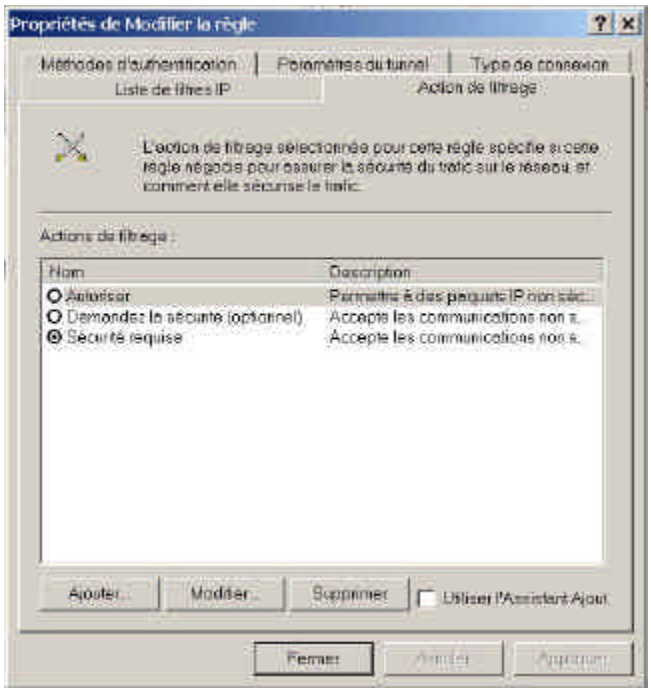


Dans la zone **Adresse source**, sélectionnez **Un sous réseau IP spécifique**, saisir dans **Adresse IP 192.168.0.0** et dans **masque de sous réseau 255.255.255.0**
Dans la zone **Adresse de destination**, sélectionnez **Une adresse IP spécifique**, saisir dans **Adresse IP 192.168.1.1.**

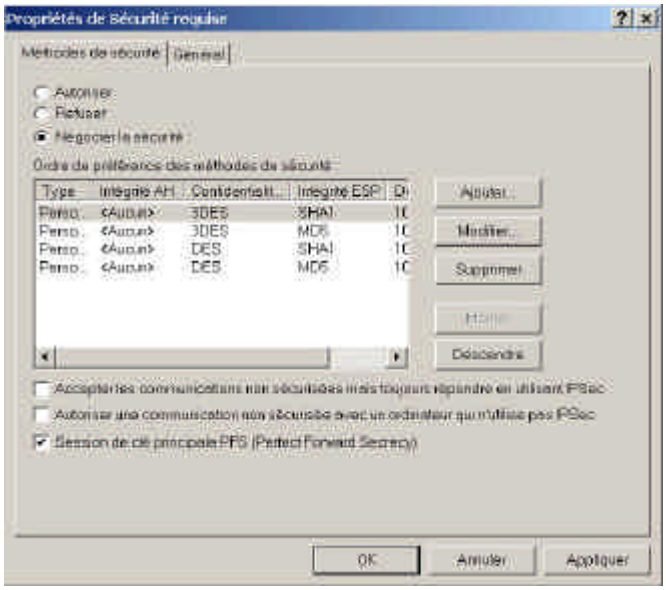
Si vous désirez sélectionner un protocole, cliquez sur l'onglet **Protocole**.



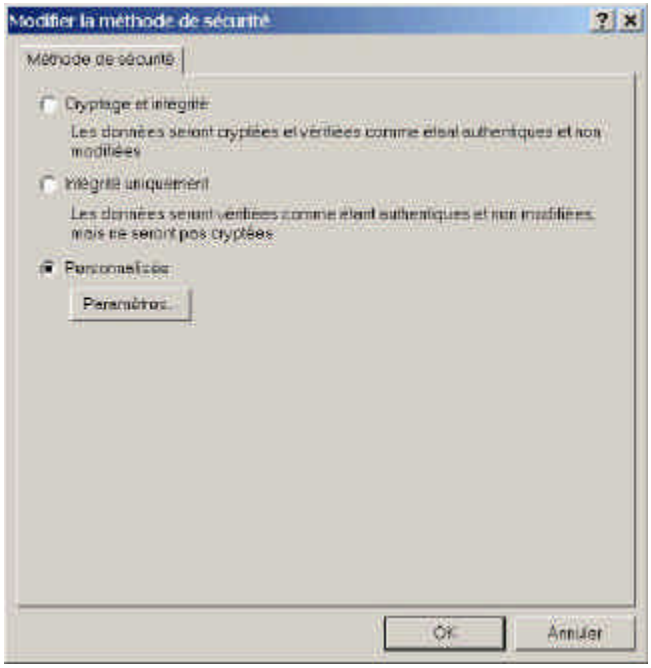
Cliquez sur le bouton **OK**, puis de nouveau sur le bouton **OK** de la fenêtre **Liste de filtres IP**.



Sélectionnez l'onglet **Action de filtrage**, sélectionnez le bouton **Exiger la sécurité** puis cliquez sur le bouton **Modifier**.

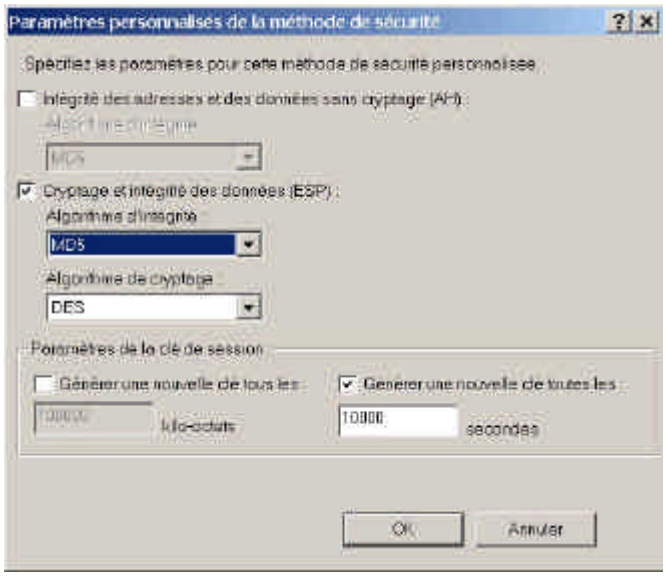


Sélectionnez **Negociate security**, Sélectionnez **Session Clé principale PFS (Perfect Forward Secrecy)** puis cliquez sur le bouton **Modifier**.



Sélectionnez **Personnalisée (pour les utilisateurs expérimentés)**

Cliquez sur le bouton **Paramètres.**



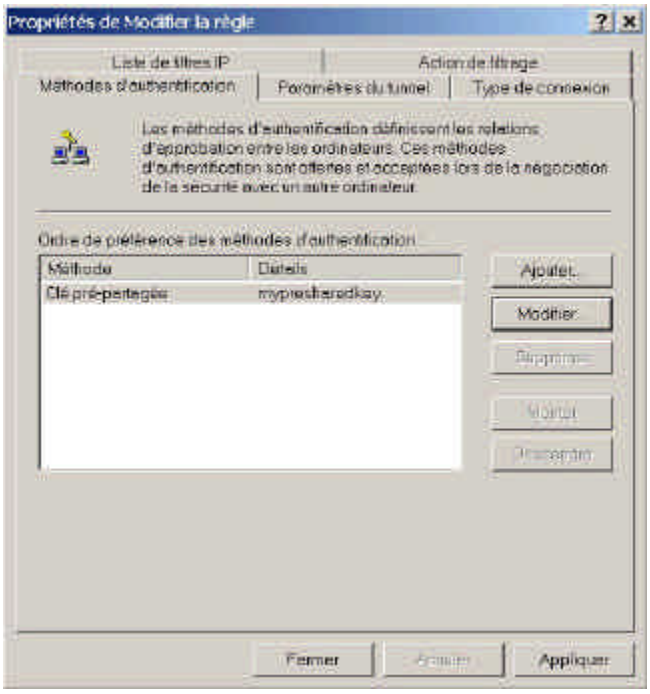
Sélectionnez **Cryptage et intégrité des données (ESP)**

Configurez **l'Algorithme d'intégrité** sur **MD5**

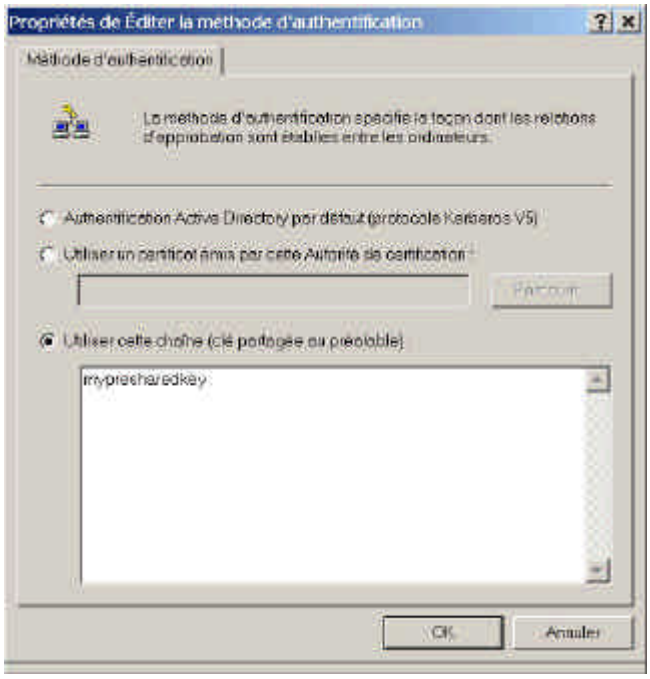
Configurez **l'Algorithme de cryptage** sur **DES**

Configurez **Générer une nouvelle clé tous les:** sur **10000** secondes

Cliquez sur le bouton **OK** jusqu'à revenir sur la fenêtre **Propriétés de nouvelle règle.**



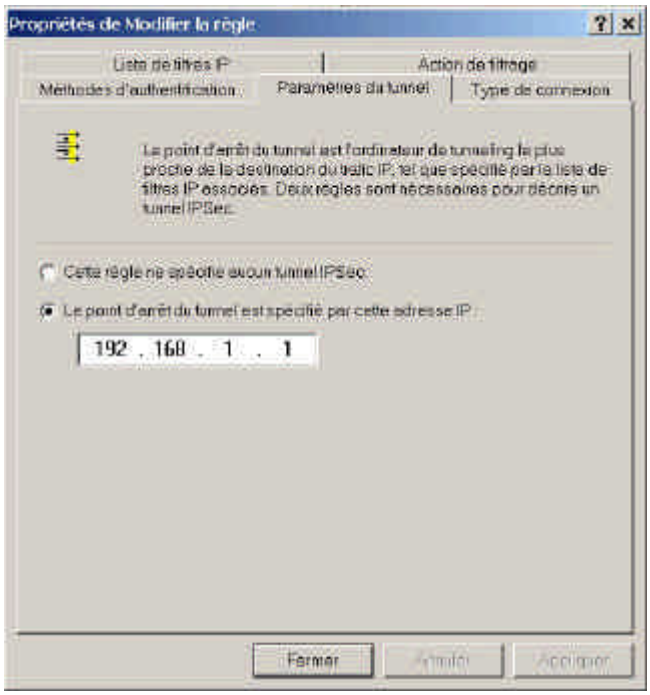
Sélectionnez l'onglet **Méthodes d'authentification** puis cliquez sur le bouton **Modifier**.



Sélectionnez le bouton **Utiliser cette chaîne pour protéger l'échange de clés (clé partagée prédéfinie)**, puis saisissez votre clé pré-chargée comme par exemple **mypresharedkey**, puis cliquez sur le bouton **OK**.

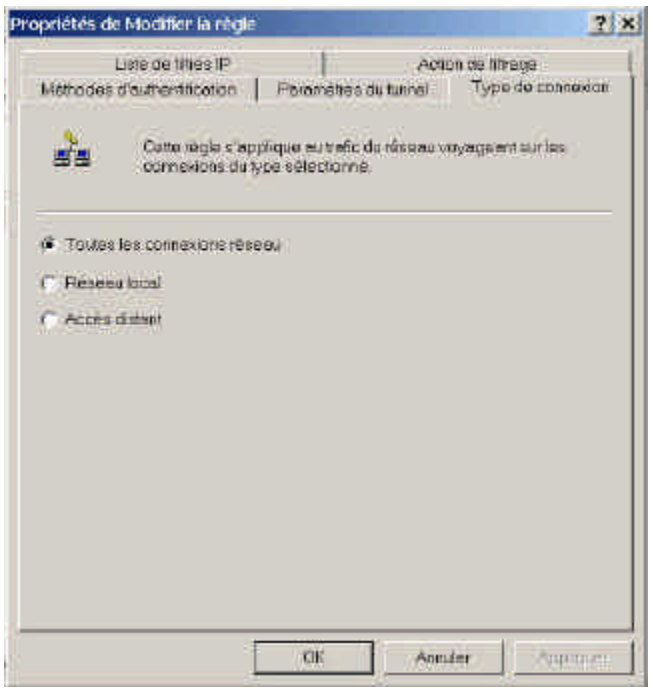
Cliquez sur le bouton **OK** depuis l'onglet **Méthodes d'authentification**.

Sélectionnez l'onglet **Paramètres du tunnel.**



Sélectionnez **Le point d'arrêt du tunnel est spécifiée par cette adresse IP**, puis saisir l'adresse IP: **192.168.1.1**.

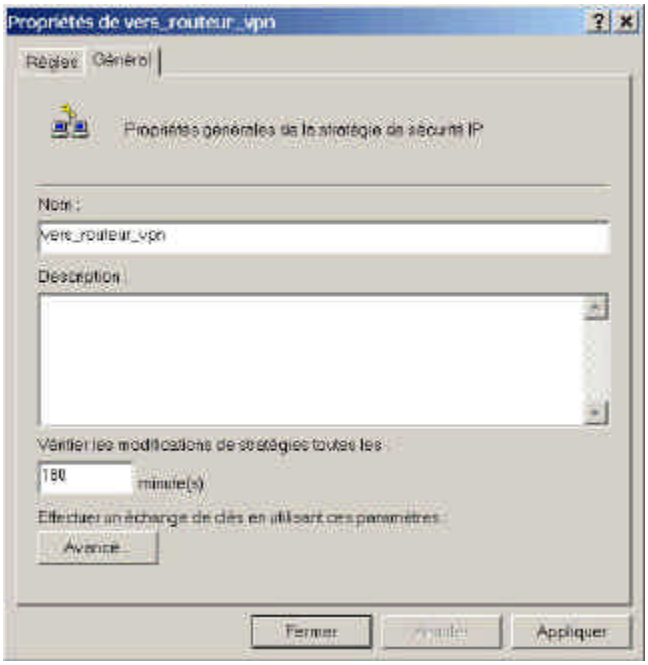
Sélectionnez l'onglet **Type de connexion.**



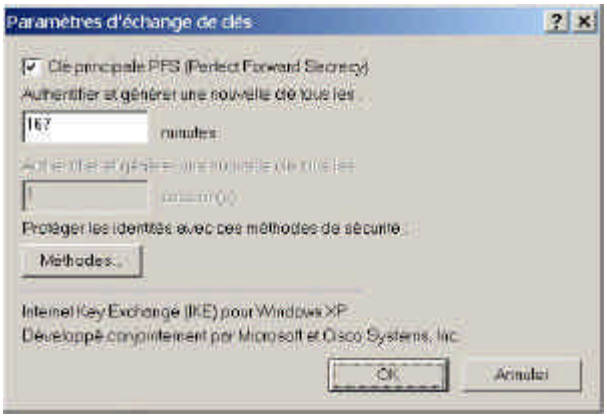
Sélectionnez **Toutes les connexions réseau.**

Configurez les propriétés IKE

Sélectionnez l'onglet **Général**



Cliquez sur le bouton **Avancé.**

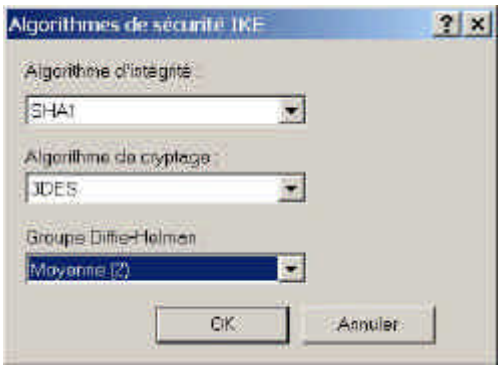


Activer la case **Clé principale PFS (Perfect Forward Secrecy)** .

Configurez **Authentifier et générer une nouvelle clé tous les** en mettant 10000 secondes, ce qui fait 167 minutes.

Cliquez sur le bouton **Méthodes**.

Si cette méthode n'existe pas déjà, Cliquez sur le bouton **Ajouter**.



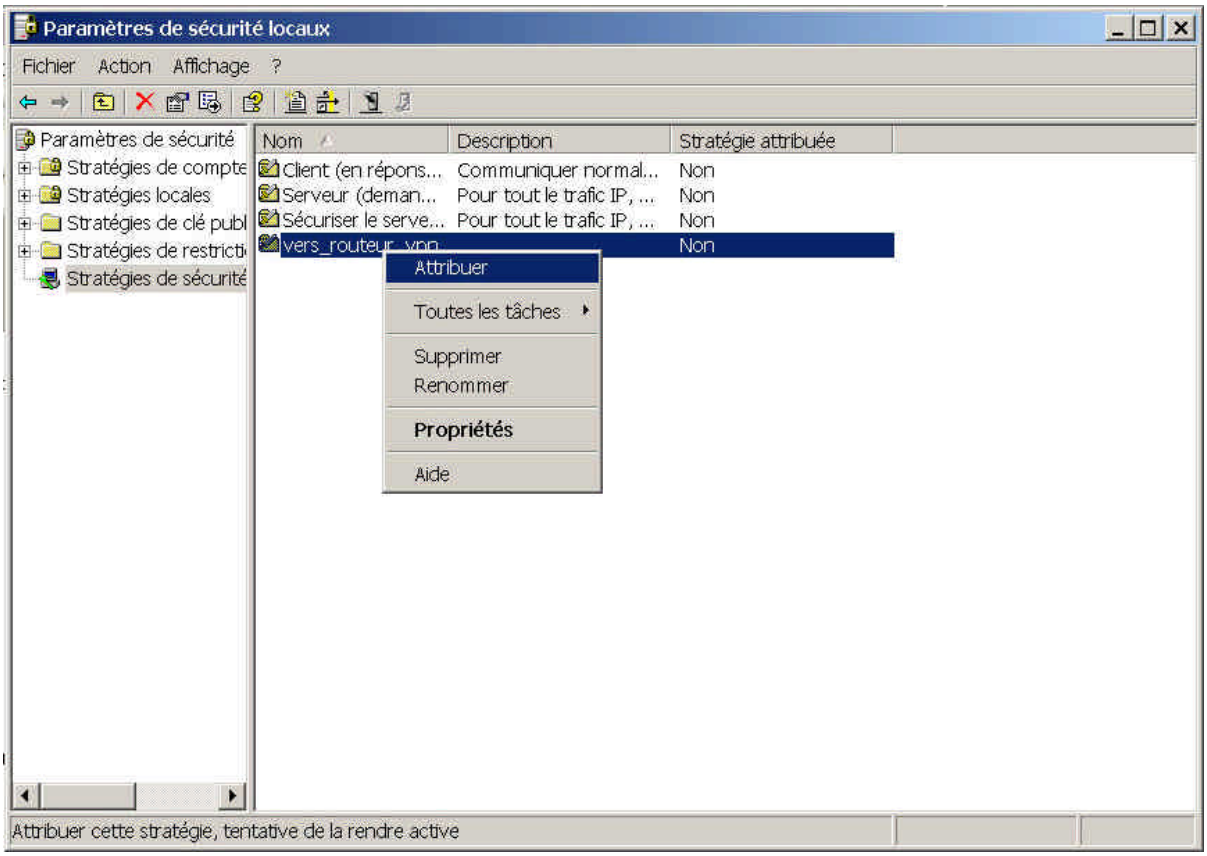
Configurez **Algorithme d'intégrité** sur **SHA1**

Configurez **Algorithme de cryptage** sur **3DES**

Configurez **Groupe Diffie-Helman** sur **Moyenne (2)**

Cliquez sur le bouton **OK**.

Revenez ensuite au paramètres de sécurité locaux et effectuer l'attribution de votre nouvelle stratégie de sécurité IP sur l'ordinateur local nommé **vers_routeur_vpn** par un clic droit.

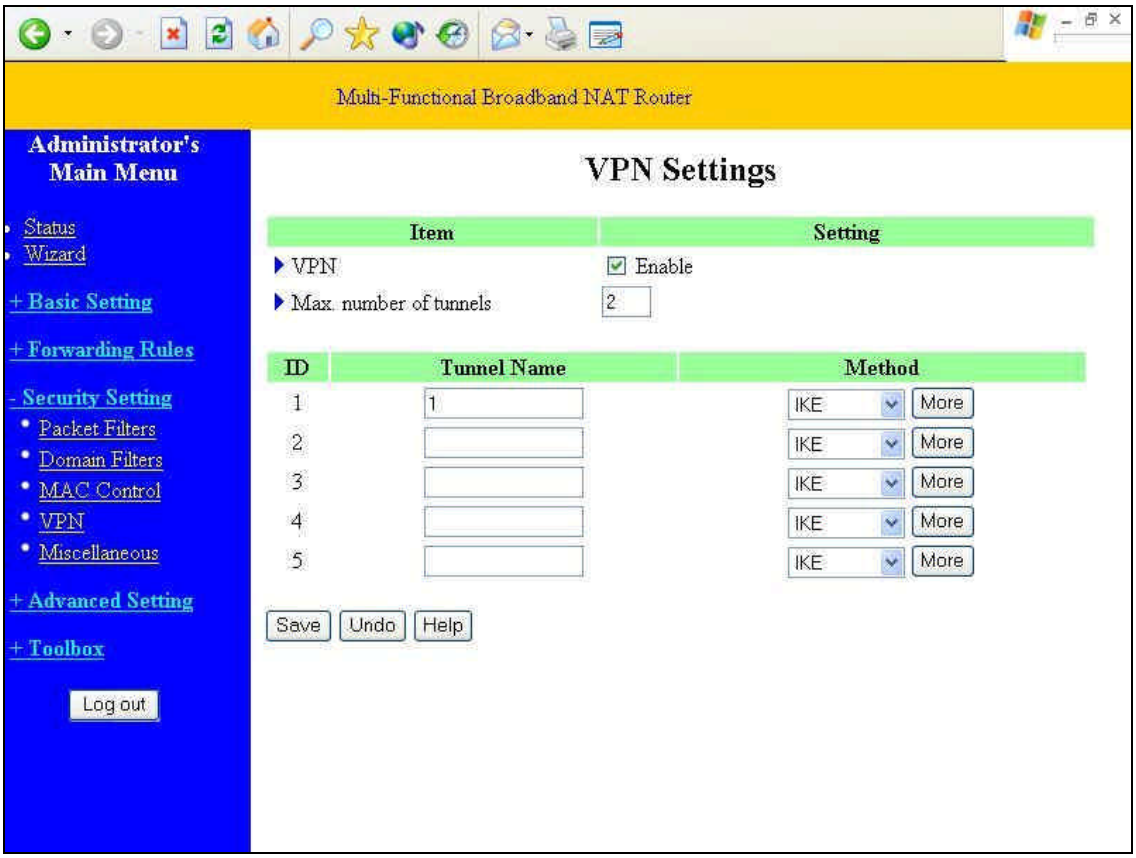


Paramétrage du routeur

Routeur VPN: Adresse IP WAN:192.168.1.254

Adresse IP LAN:192.168.0.1

PC: 192.168.0.123



VPN Settings:

Cochez la case **Enable** en face de VPN

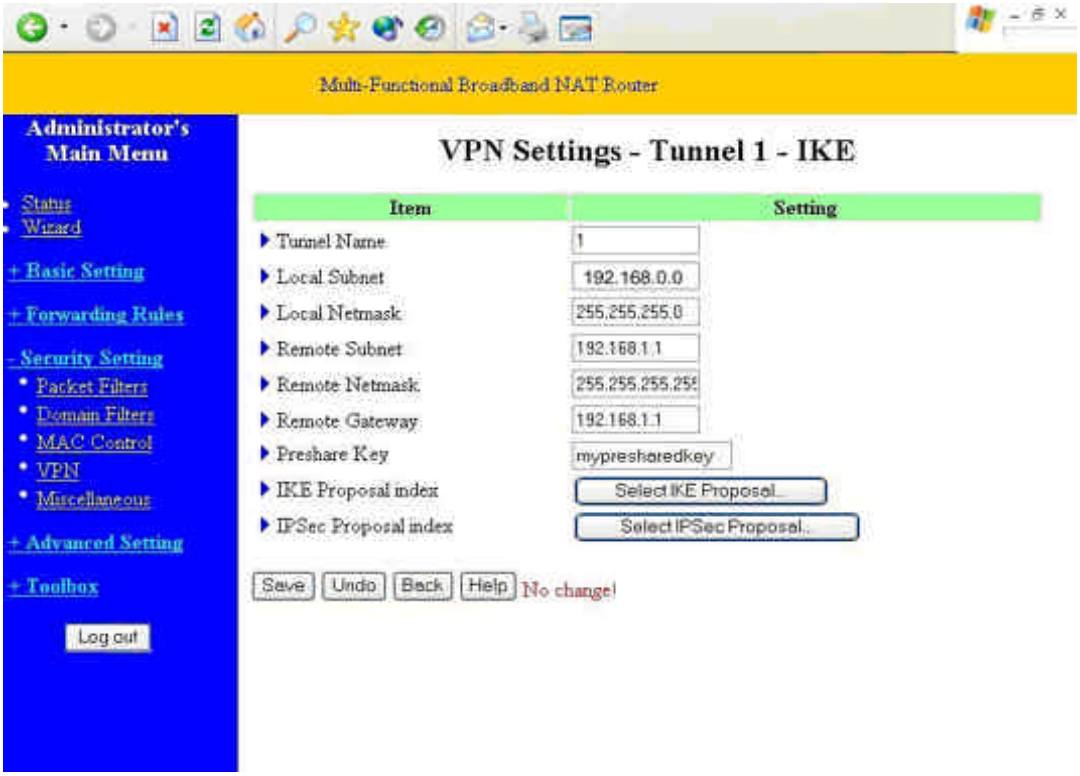
Max. number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Cliquez sur le bouton **More.**→



VPN Settings - Tunnel 1 - IKE

Tunnel:1

Local Subnet:192.168.0.0

Local Netmask:255.255.255.0

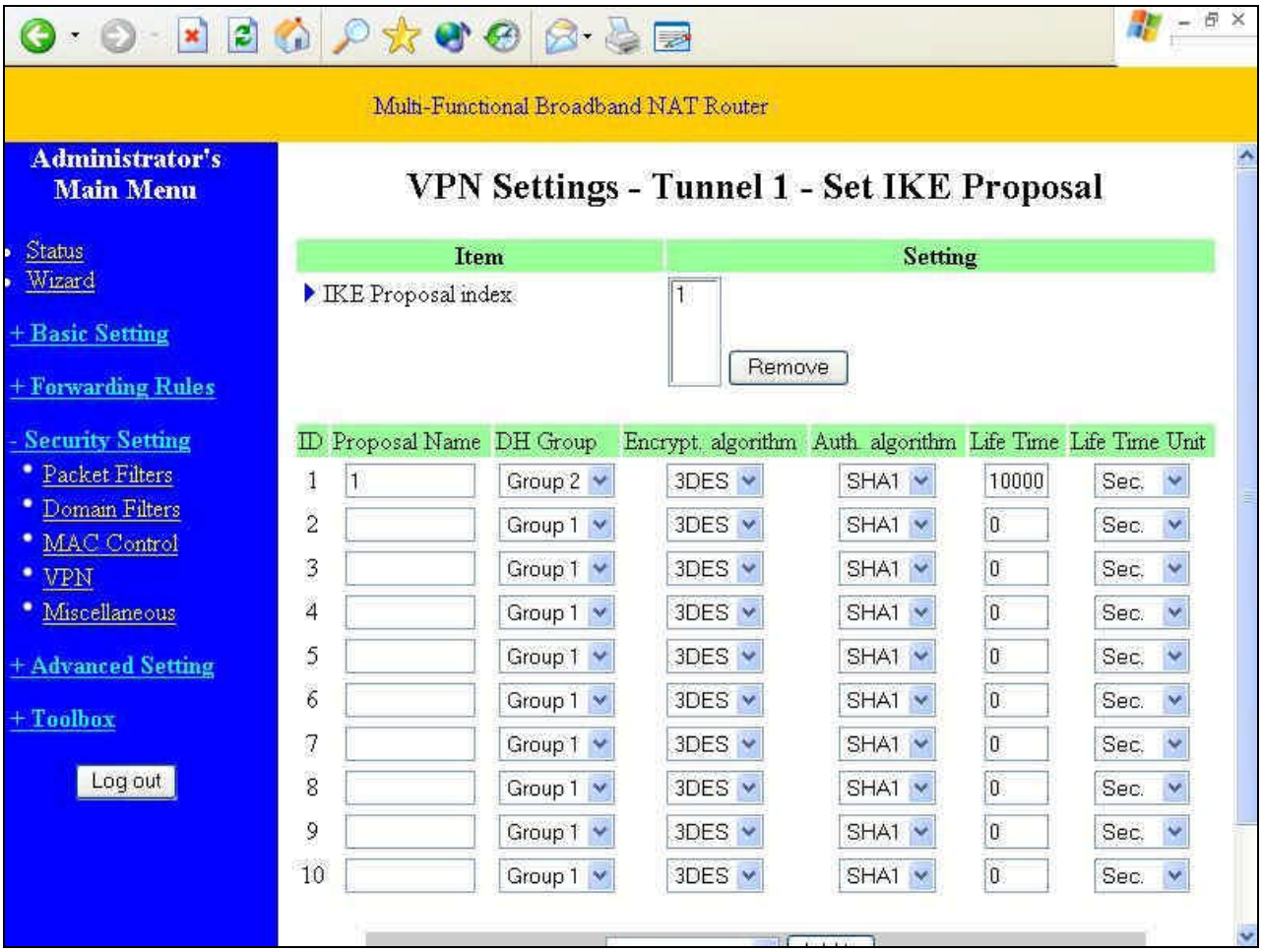
Remote Subnet:192.168.1.1

Remote Netmask:255.255.255.255

Remote Gateway:192.168.1.1

Pre-shared Key: mypresharekey

Cliquez sur le bouton **Select IKE Proposal.**



VPN Settings - Tunnel 1 - Set IKE Proposal

ID: 1

Proposal Name: 1

DH Group: Group2

Encrypt. Algorithm: 3DES

Auth. Algorithm: SHA1

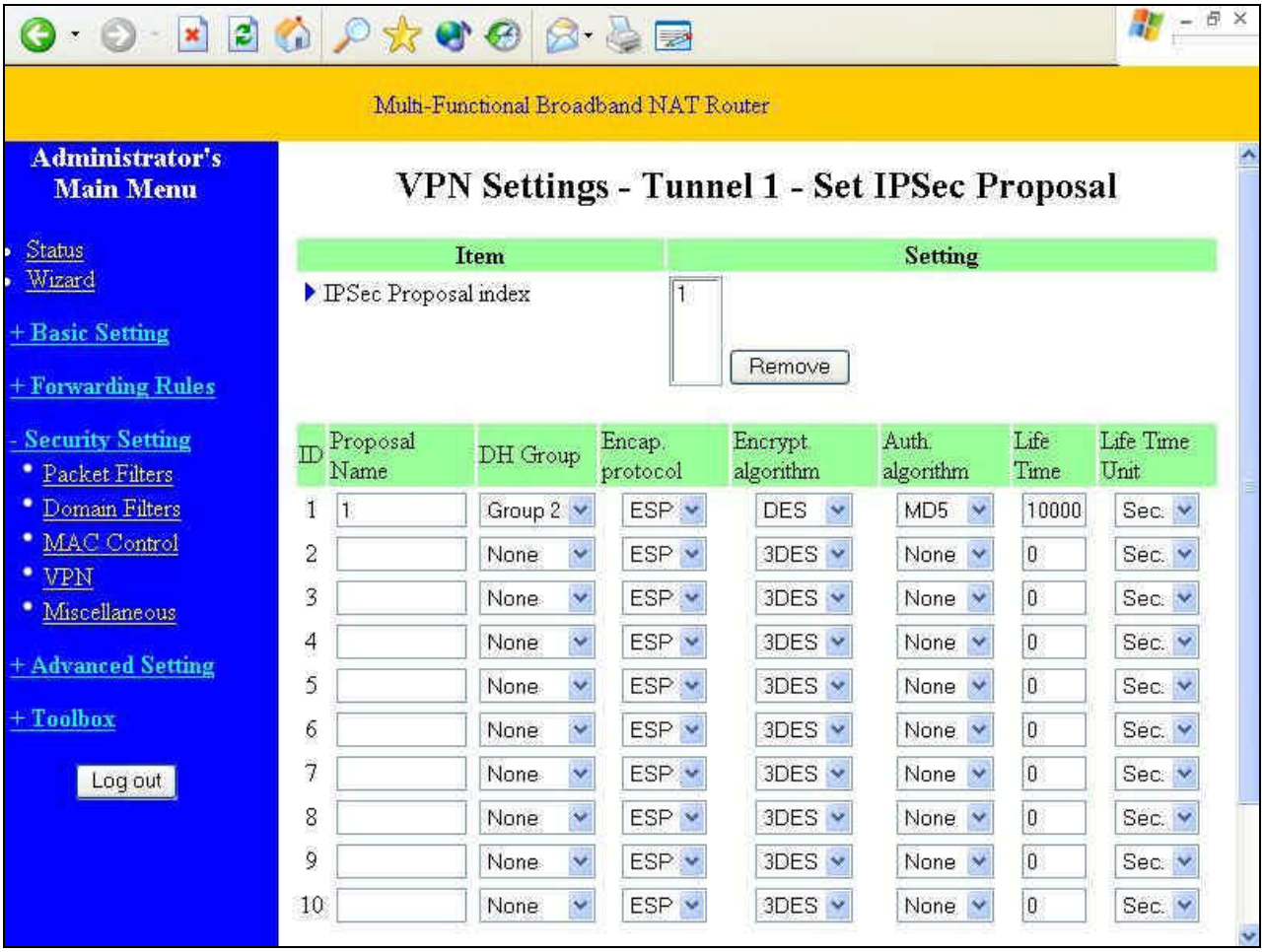
Life Time: 10000

Life Time Unit: Sec.

Dans **Proposal ID**, sélectionnez **1** puis cliquez sur le bouton **Add to**

Cliquez sur le bouton **Save.**

Cliquez sur le bouton **Select IPSec proposal.**



VPN Settings - Tunnel 1 - Set IPSec Proposal

ID: 1

Proposal Name: proposal1

DH Group: Group2

Encaps. Protocol: ESP

Encrypt. Algorithm: DES

Auth. Algorithm:MD5

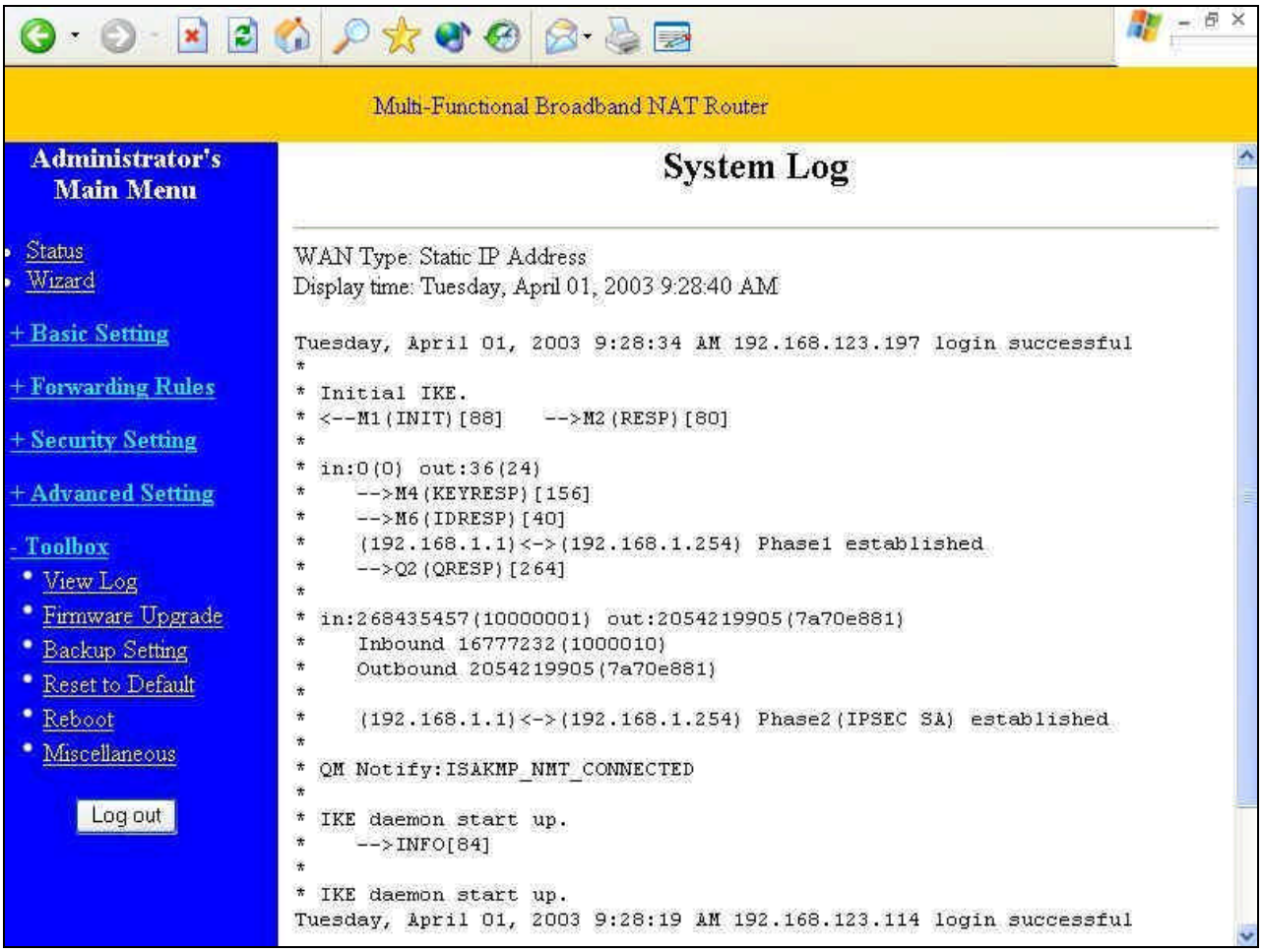
Life Time: 10000

Life Time Unit: Sec.

Dans **Proposal ID**, sélectionnez **1** puis cliquez sur le bouton **Add to**

Cliquez sur le bouton **Save.**

Vous pouvez visualiser votre connexion VPN depuis la page **System Log**, et corriger les paramètres si nécessaire. **Phase1** est lié aux paramètres **IKE**, et **Phase2** est lié aux paramètres **IPSEC**.



Annexe C Paramètres 802.1x

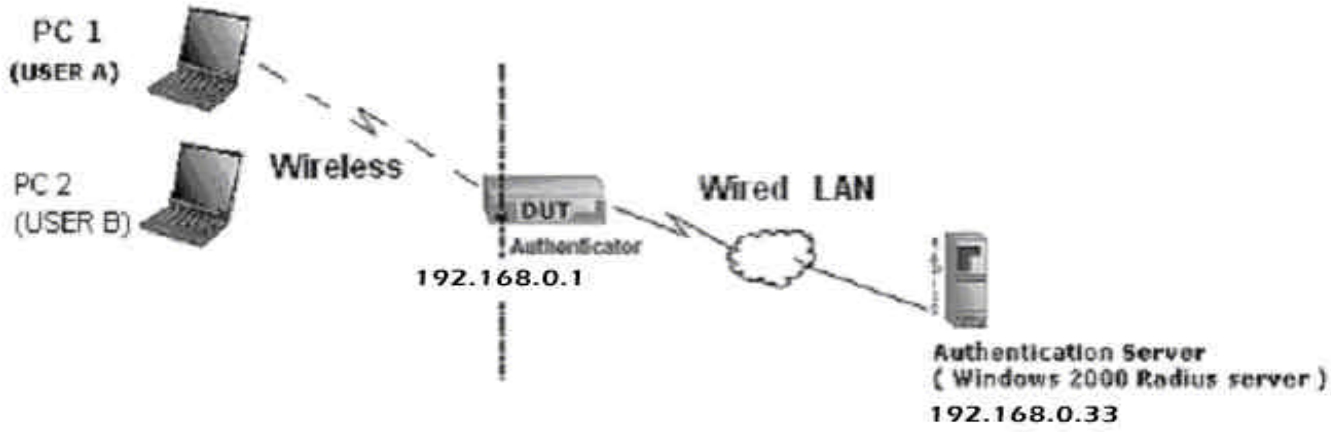


Figure 1: Environnement de test (Serveur Radius sous Windows 2000)

1 Détails des équipements

PC1:

Microsoft Windows XP Professionnel sans le Service Pack 1.

Comet Labs WN561 : adaptateur sans fil

PC2:

Microsoft Windows XP Professionnel avec le Service Pack 1a.

Comet Labs WN591 : adaptateur sans fil USB.

Serveur d'authentification: Serveur RADIUS Windows 2000 avec Service Pack 3 et Hot Fix Q313664 installés.

Note. Le serveur Radius sous Windows 2000 ne supporte que PEAP après la mise à jour Service Pack 3 et Hot Fix Q313664. *(Plus de détails:http://support.microsoft.com/default.aspx?scid=kb; en-us;313664)*

2 DUT

Configuration:

1.Serveur DHCP activé.

2.Adresse IP WAN statique.

3.Adresse IP LAN: 192.168.0.254/24.

4.Adresse IP du serveur RADIUS à saisir.

5.Clé partagée du serveur RADIUS à saisir.

6.Clé WEP et paramètres 802.1X à configurer.

Le test suivant utilise les méthodes d'authentification intégrées telles que: EAP_TLS, PEAP_CHAPv2 (Windows XP avec SP1 seulement), et PEAP_TLS (Windows XP avec SP1 seulement) utilisant la Smart Card ou un autre Certificat de Windows XP Professionnel.

3. Paramètres du DUT et du Serveur Radius Windows 2000

3-1-1. Paramétrage du serveur RADIUS Windows 2000

Nous avons du changer la méthode d'authentification sur MD5_Challenge, utiliser une Smart Card ou un autre certificat sur le serveur RADIUS par rapport aux conditions de test.

3-1-2. Paramétrage du DUT

1.Activer 802.1X (cochez la case Enable de la section 802.1X)

2.Saisissez l'adresse IP du serveur RADIUS.

3.Saisissez la clé partagée (clé partagée par le DUT et le serveur RADIUS)

4.Nous serons amené à changer la longueur de la clé d'encryption pour être confirme avec les conditions de test.

3-1-3. Paramétrage des cartes réseaux sur les PCs

1. Sélectionnez IEEE802.1X comme méthode d'authentification (fig.2)

Note. La figure 2 montre une capture d'écran d'un système Windows XP sans le Service Pack 1 installé. Si l'utilisateur a installé le Service Pack 1, alors il ne verra pas l'option MD5-Challenge de la fenêtre EAP Type, mais il aura une nouvelle option PEAP (Protected EAP)

2.Sélectionnez MD5-Challenge, Smart Card ou un autre Certificat.

3. Dans cet exemple, nous allons choisir d'utiliser un Certificat (voir fig.3).

4. Nous changerons le type EAP si besoin.

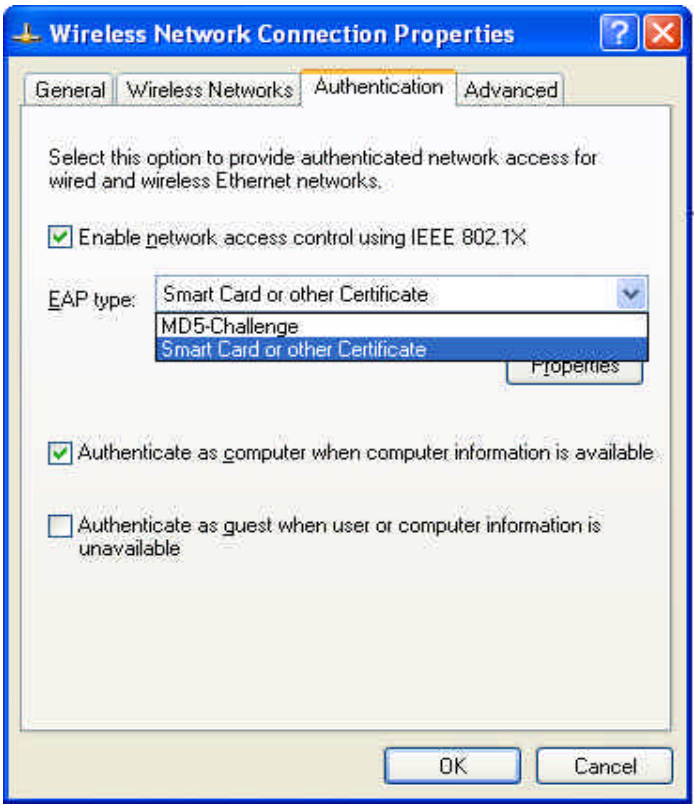


Figure 2: Activé le contrôle d'accès IEEE802.1X

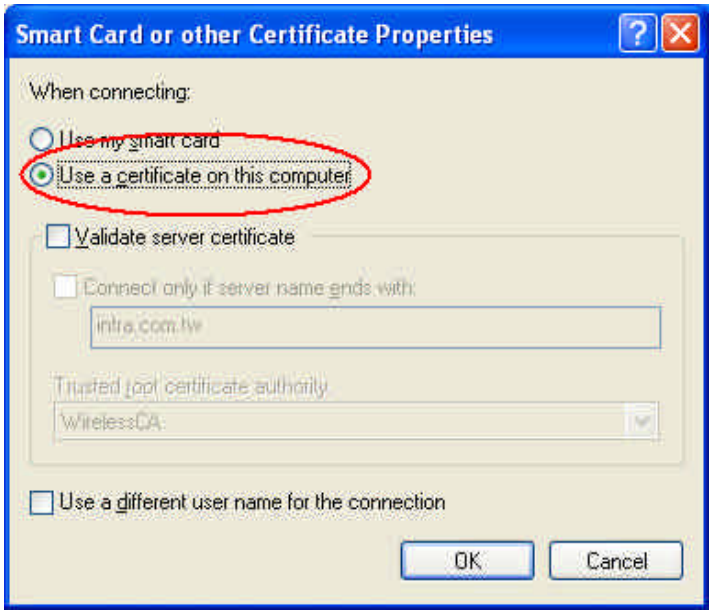


Figure 3: Smart card or certificate properties

4. Test de l'authentification du serveur RADIUS Windows 2000:

4.1.DUT authentifie PC1 à l'aide d'un certificat (PC2 fonctionne de la même manière).

1. Téléchargez puis installez le certificat sur PC1 (Fig.4).

2. PC1 choisit le SSID du DUT comme Point d'accès.

3. Configurez le type d'authentification des clients sans fil et du serveur RADIUS sur EAP_TLS.

4. Désactivez la connexion sans fil puis réactivez-la.

5. Le DUT va envoyer le certificat de l'utilisateur au serveur RADIUS qui renvoie le résultat du message d'authentification vers PC1 (Fig.5).

6. Windows XP vous dira si l'authentification a réussi ou a échoué, puis finit la procédure d'authentification (Fig.6).

7. Terminez le test dès que PC1 obtient une adresse IP dynamique et peut pinguer une autre machine avec succès.

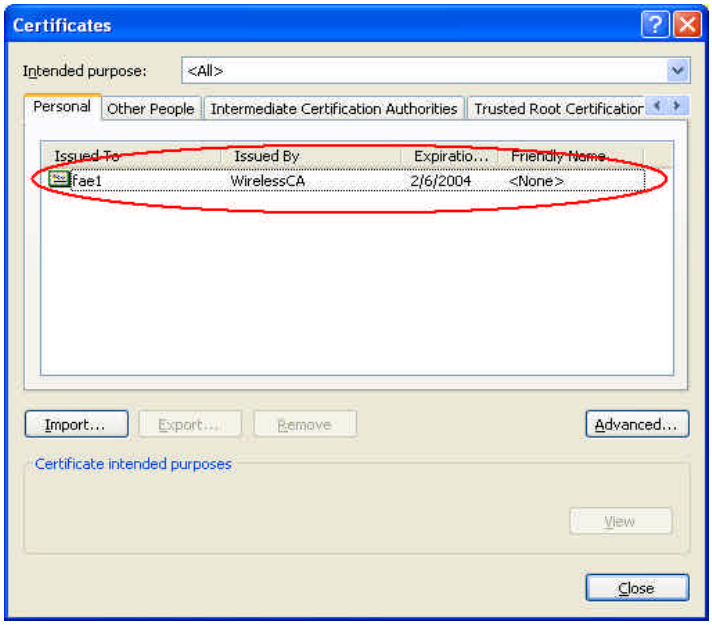


Figure 4: Information de Certificat sur PC1

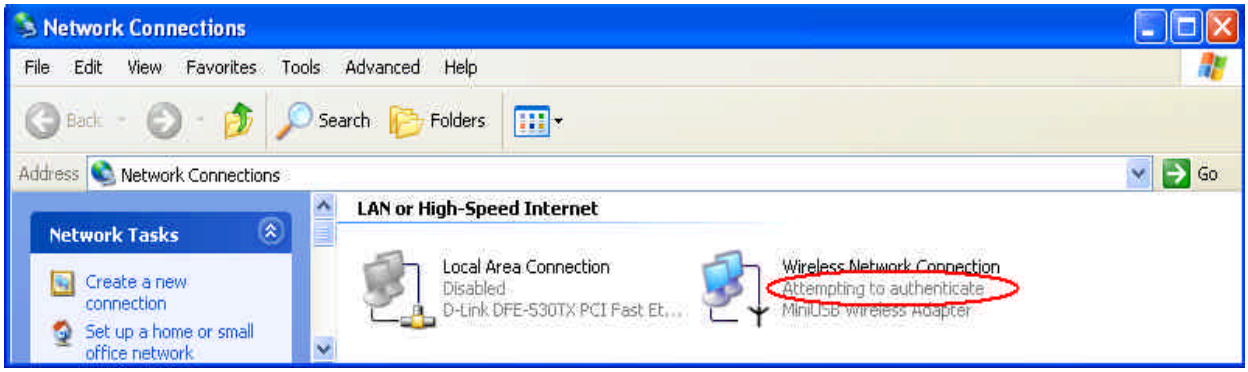


Figure 5: Authentification en cours

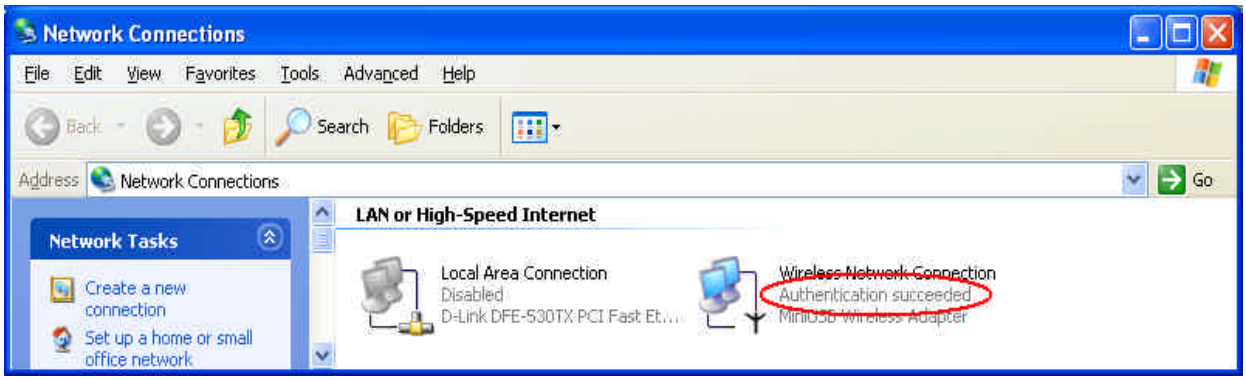


Figure 6: Authentification avec succès

4.2 DUT authentifie PC2 en utilisant le PEAP_TLS.

1. PC2 choisit le SSID du DUT comme Point d'accès.

2. Configurez le type d'authentification des clients sans fil et du serveur RADIUS sur:

PEAP_TLS.

3. Désactivez la connexion sans fil puis réactivez-la.

4. Le DUT va envoyer le certificat de l'utilisateur au serveur RADIUS qui renvoie le résultat du message d'authentification vers PC2.

5. Windows XP vous dira si l'authentification a réussi ou a échoué, puis finit la procédure d'authentification

6. Terminez le test dès que PC2 obtient une adresse IP dynamique et peut pinguer une autre machine avec succès.

Type Supporté : Comet Labs supporte le type d'authentification 802.1X suivant:

PEAP-CHAPv2 et PEAP-TLS.

Note.

1.PC1 fonctionne sous Windows XP Service Pack 1.

2.PC2 fonctionne sous Windows XP Service Pack 1a.

3.PEAP n'est supporté que sous Windows XP Service Pack 1a. seulement.

4.Windows XP Service Pack1 autorise l'authentification 802.1X seulement si les fonctions d'encryptions de données sont activées.

Annexe D FAQ

Remise des paramètres à leurs valeurs par défaut

A l'aide d'une pointe fine, appuyez sur le bouton **RESET** jusqu'à ce que la LED **SYS** clignote très rapidement. Il faut compter 6 à 7 secondes avant que la LED **SYS** ne clignote rapidement

Le routeur a de nouveau ses paramètres d'usine.

Paramètres de connexion des quelques Fournisseurs d'accès Internet français:

La plupart des Fournisseurs d'Accès à Internet utilisent les mêmes paramètres que Wanadoo.

- **Wanadoo, 9Online, Club-Internet, Free non dégroupé, Télé2, Tiscali…**
  WAN Type: PPP over Ethernet (RFC 2516)
  Data Encapsulation: LLC
  VPI Number: 8
  VCI Number: 35
  Schedule type: UBR

- **Free dégroupé:**
  WAN Type: IP over ATM (RFC 1483 Routed) Static IP ou Dynamic IP. Généralement Dynamic IP est utilsé
  Data Encapsulation: VC-Mux
  VPI Number: 8
  VCI Number: 36
  Schedule type: UBR

Nous contacter

Adresse de la société Comet Labs: http://www.cometlabs.com et http://france.cometlabs.com

FAQ support: support@cometlabs.com

Assistance téléphonique en France : 0826 880 880