

**Router Barricade[™] g haut débit
Wireless Câble/DSL 2.4GHz 54Mps**

Manuel d'utilisation

SMC2804WBR



Routeur Barricade™ g haut débit Wireless Câble/DSL 2.4GHz 54Mbps

Un produit de la gamme des routeurs Barricade™ haut débit de SMC

TABLE DES MATIÈRES

À propos du routeur Barricade™ g sans fil	1
Témoins lumineux	3
Points forts	4
Installation du routeur Barricade™ g sans fil . . .	6
Contenu de l'emballage	6
Description du matériel	7
Configuration requise	10
Connexion du système	11
Procédure d'installation de base	11
Configuration de TCP/IP client	16
Installation de TCP/IP	16
Windows 95, Windows 98 ou ME	16
Windows 2000	17
Configuration de TCP/IP	19
Configuration de votre ordinateur	
sous Windows 95/98/Me	20
Configuration de votre ordinateur sous Windows NT 4.0	23
Configuration de votre ordinateur sous Windows 2000	26
Configuration de votre ordinateur sous Windows XP . . .	27
Configuration d'un ordinateur Macintosh	28
Configuration IP manuelle	29
Vérification de la connexion TCP/IP	31
Configuration du routeur Barricade™ g sans fil	33
Configuration du navigateur	34
Désactivation de la connexion du proxy	34
Exploration de l'interface Web	35
Modification de la configuration	37
Assistant de configuration Setup Wizard	38
Time Zone (Fuseau horaire)	38
Broadband Type (Type de connexion haut débit)	39

Table des Matières

Configuration avancée	43
System (Système)	45
WAN (Réseau étendu)	48
LAN (Réseau local)	56
Wireless (Sans fil)	57
Translation d'adresses réseau (NAT)	64
Firewall	67
Paramètres DDNS (DNS dynamique)	79
Paramétrage UPnP (Universal Plug and Play)	80
Tools (Outils)	81
Dépannage	86
Specifications	90
Compliances	i
Legal Information and Contacts	v
SMC's Limited Warranty Statement	v
Full Installation Manual	vii
Firmware and Drivers	vii
Contact SMC	vii
Statement of Conditions	vii
Limitation of Liability	viii
Trademarks	viii

À PROPOS DU ROUTEUR BARRICADE™ G SANS FIL

Félicitations pour votre achat du routeur Barricade™ g haut débit sans fil. SMC est fier de vous proposer ce périphérique de communication puissant, mais simple pour la connexion de votre réseau local (LAN) à Internet.

Information Importante !

Cette information est destinée aux utilisateurs DSL ne bénéficiant pas d'un contrat à tarif forfaitaire.**

Le routeur DSL que vous venez de recevoir est un appareil de haute qualité qui vous permet d'accéder rapidement et facilement à Internet.

Les paramètres par défaut de ce routeur ont été définis pour vous permettre d'utiliser Internet en continu. C'est la raison pour laquelle, pour des problèmes de coût, nous vous recommandons de souscrire un contrat de type « forfaitaire » auprès de votre fournisseur de ligne DSL.

Pourquoi ?

N'oubliez pas qu'un routeur est un appareil entièrement indépendant, qui ne s'éteint pas automatiquement lorsque vous arrêtez votre PC.

Vous pouvez déclencher un arrêt automatique en définissant un « délai d'inactivité » (pour plus de détails, consultez votre manuel à la section traitant de la configuration de l'accès WAN PPPoE ou PPTP). Une fois le délai défini (1 à 5 min) dépassé, le routeur coupe la liaison DSL si celle-ci n'est plus active. Mais cela ne suffit pas à assurer une sécurité totale.

À propos du routeur Barricade™ g sans fil

Cette déconnexion a lieu uniquement si aucune requête ouverte ne provient du réseau local ou réseau étendu (il peut s'agir ici de requêtes en provenance d'Internet, c'est-à-dire établies grâce à des programmes de partage de fichiers comme eMule, eDonkey, etc.) qui maintiennent le routeur actif.

Pour contourner ce problème lié à une activité imprévisible et vous éviter des coûts de connexion plus élevés que prévu, nous vous recommandons à nouveau de souscrire un contrat de type forfaitaire pour votre connexion DSL.

La seule autre solution sûre : **débrancher la prise de courant !**

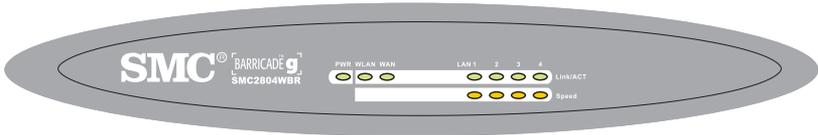
C'est-à-dire déconnecter votre routeur du secteur.

N'hésitez pas à contacter le support téléphonique SMC si vous avez d'autres questions.

** Le tarif forfaitaire est une offre de votre fournisseur de ligne DSL qui vous permet de bénéficier d'un accès illimité dans le temps à Internet à un tarif (forfaitaire) fixe.

Témoins lumineux

Le routeur Barricade™ g sans fil comporte des témoins lumineux. Ces témoins sont décrits dans l'illustration et le tableau qui suivent.



Témoin	État	Description
PWR (Alimentation, vert)	Allumé	Le routeur Barricade™ g sans fil est sous tension.
WLAN (Vert)	Allumé	Le routeur Barricade™ g sans fil a établi une connexion sans fil.
WAN (Vert)	Allumé	La connexion du port WAN au réseau est établie.
Link/ACT (Liaison/Activité) (Vert)	Allumé	Le port LAN indiqué a établi une connexion réseau.
	Clignotant	Le port LAN indiqué transmet ou reçoit des données.
Vitesse (Orange)	Éteint	La connexion 10 Mbps au réseau du port LAN (réseau local) indiqué est établie.
	Allumé	La connexion 100 Mbps au réseau du port LAN (réseau local) indiqué est établie.

Points forts

- Connexion Internet avec un modem DSL ou Câble via un port WAN 10/100 Mbps.
- Connexion de réseau local via des ports Ethernet 10/100 Mbps ou une interface sans fil 54 Mbps (supportant jusqu'à 253 utilisateurs mobiles).
- Compatibilité 802.11g draft, interopérabilité avec plusieurs fournisseurs.
- Sécurité avancée grâce à un cryptage WEP 64/128 bits, à l'identificateur de propriété 802.1x, à la désactivation de la fonction SSID Broadcast (Diffusion SSID) et au filtrage d'adresses MAC pour protéger vos données à caractère critique et authentifier uniquement les utilisateurs autorisés sur votre réseau.
- Accès itinérant transparent dans un environnement WLAN 802.11g draft.
- Protocole DHCP permettant une configuration IP dynamique et serveur DNS assurant le mappage des noms de domaine.
- Firewall doté de fonctions SPI (Stateful Packet Inspection), de droits d'accès client et de fonctions de protection contre les attaques extérieures, de refus de service et de translation d'adresses réseau (NAT).
- La fonction de translation d'adresses réseau autorise également l'accès de plusieurs utilisateurs à l'aide d'un compte utilisateur unique et la fonction de serveur virtuel (pour l'accès protégé aux services Internet, tels que le Web, la messagerie électronique, les services FTP et Telnet).

Points forts

- Support de réseau privé virtuel utilisant le mode Pass Through PPTP, L2TP ou IPSec.
- Tunnel de détection d'application personnalisable supportant les applications qui nécessitent plusieurs connexions.
- Contrôle parental permettant à l'utilisateur de limiter la navigation sur le Web.
- Alertes automatiques par courrier électronique lorsque le réseau est attaqué.
- Configuration aisée via un navigateur Web installé sur les systèmes d'exploitation qui supportent TCP/IP.
- Compatible avec les applications Internet les plus courantes.

INSTALLATION DU ROUTEUR BARRICADE™ G SANS FIL

Avant d'installer le routeur Barricade™ g haut débit sans fil, assurez-vous de disposer de tous les éléments répertoriés dans la section « Contenu de l'emballage ». Si l'un de ces éléments est absent ou endommagé, contactez votre revendeur SMC local. Assurez-vous également de disposer de tous les câbles nécessaires avant de démarrer l'installation du routeur.

Une fois cette installation effectuée, reportez-vous au programme de configuration Web à la section « Configuration du routeur Barricade™ g sans fil » à la page 33 pour obtenir des informations relatives à la configuration du routeur.

Contenu de l'emballage

Après avoir déballé le routeur Barricade™ g haut débit sans fil, vérifiez le contenu de l'emballage afin de vous assurer de la présence des composants suivants :

- Routeur Barricade™ g haut débit sans fil.
- Cordon d'alimentation.
- Un câble Ethernet de catégorie 5.
- Quatre patins en caoutchouc.
- CD-ROM d'installation contenant ce manuel d'utilisation et l'assistant d'installation EZ 3-Click Installation Wizard.
- Guide d'installation rapide.

Si l'un de ces éléments est absent ou endommagé, contactez immédiatement votre revendeur. Si possible, conservez le carton et les emballages d'origine dans le cas d'un éventuel retour du produit.

Enregistrez votre produit sur le site Web de SMC www.smc.com ou www.smc-europe.com. Le routeur Barricade™ g sans fil bénéficie d'une garantie de cinq ans.

Description du matériel

Le routeur peut être connecté à Internet ou à un site distant par l'intermédiaire de son port WAN RJ-45. Il peut être connecté directement à votre ordinateur ou à un réseau local à l'aide de l'un des ports réseau Fast Ethernet.

La vitesse d'accès à Internet est fonction de votre type de service. Le débit de la connexion ADSL à pleine vitesse peut s'élever à 8 Mbps en réception et à 640 Kbps en émission. Celui de la connexion ADSL G.lite (ou Splitterless) s'élève à 1,5 Mbps en réception et à 512 Kbps en émission. Les modems Câble peuvent assurer un débit maximal de 36 Mbps en réception et de 2 Mbps en émission. Le réseau RNIS fournit jusqu'à 128 Kbps lors de l'utilisation de deux canaux de support. Les connexions analogiques RTPC peuvent désormais fonctionner jusqu'à 56 Kbps. Cependant, il se peut que le débit réel offert par les fournisseurs de services varie considérablement par rapport à ces limites maximales.

Même si la vitesse d'accès à Internet est déterminée par le type de modem connecté au routeur, le transfert de données entre les périphériques connectés au réseau local peut s'effectuer jusqu'à 100 Mbps via les ports Fast Ethernet.

Installation du routeur Barricade™ g sans fil

Le routeur est équipé, sur le panneau avant, de témoins de contrôle de l'état du système et des ports, simplifiant l'installation et le dépannage du réseau. Il est également doté de quatre ports LAN RJ-45 et d'un port WAN RJ-45 sur le panneau arrière.

- Quatre ports RJ-45 pour la connexion à un réseau local Ethernet 10BASE-T/100BASE-TX. Ces ports permettent la négociation automatique du débit de transmission à 10/100 Mbps, du mode Half/Full-duplex et des signaux de reconnaissance MDI/MDI-X (c'est-à-dire la possibilité de connecter ces ports à n'importe quel périphérique réseau au moyen d'un câble direct). Ces ports peuvent être connectés directement à un poste de travail ou à un serveur équipé d'une carte d'interface réseau Ethernet, ou encore à un périphérique de réseau tel qu'un concentrateur ou un commutateur Ethernet.
- Un port RJ-45 pour les connexions à un modem DSL ou Câble (WAN). Ce port permet aussi la négociation automatique de la vitesse à 10/100 Mbps, du mode Half/Full-duplex et des signaux de reconnaissance MDI/MDI-X.

Description du matériel

La figure ci-dessous présente les composants du routeur.

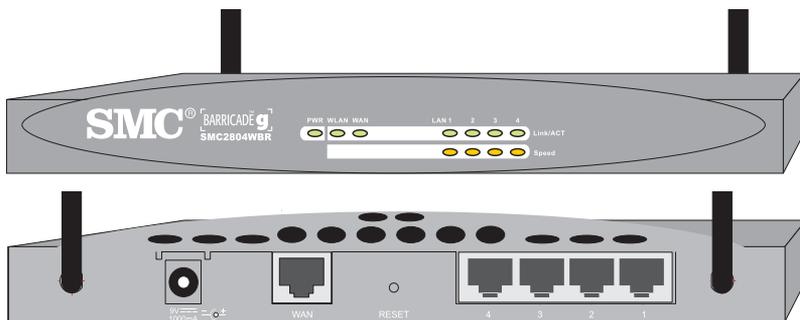


Figure 1. Panneaux avant et arrière

Élément	Description
Bouton Reset (Réinitialiser)	Ce bouton permet de réinitialiser le système ou de restaurer les paramètres par défaut.
Témoins	Ces indicateurs contrôlent l'état de l'alimentation et des ports WLAN, WAN et LAN. (Reportez-vous à la section « Témoins lumineux » à la page 3.)
Ports de réseau local	Ports Fast Ethernet (RJ-45). Connectez des périphériques de votre réseau local à ces ports (par exemple, un ordinateur, un concentrateur ou un commutateur).
Port WAN	Port WAN (RJ-45). Connectez votre modem Câble, votre modem DSL ou un routeur Ethernet à ce port.
Prise d'alimentation	Branchez sur cette prise le cordon d'alimentation fourni. Avertissement : l'utilisation d'un cordon d'alimentation inapproprié peut endommager l'appareil.

Configuration requise

Vous devez disposer de la configuration minimale suivante :

- Un accès à Internet, acquis auprès de votre opérateur téléphonique ou Fournisseur d'Accès Internet (FAI), à l'aide d'un modem DSL ou Câble.
- Un ordinateur configuré pour une attribution d'adresse IP statique ou dynamique via DHCP, une adresse de serveur Passerelle et une adresse de serveur DNS attribuée par votre fournisseur de services.
- Un ordinateur équipé d'une carte 10 Mbps, 100 Mbps ou 10/100 Mbps Fast Ethernet, ou d'un convertisseur USB-Ethernet.
- Le protocole réseau TCP/IP installé sur chaque ordinateur nécessitant un accès à Internet.
- Un navigateur Web supportant Java, tel que Microsoft Internet Explorer version 5.0 ou ultérieure ou Netscape Communicator version 4.0 ou ultérieure, installé sur un ordinateur de votre site pour la configuration du routeur.

Connexion du système

Le routeur peut être installé à n'importe quel emplacement pratique au bureau ou au domicile. Aucune configuration spéciale de câblage ou de refroidissement n'est requise. Cependant, vous devez respecter les recommandations suivantes :

- N'installez pas le routeur à proximité d'appareils de chauffage.
- N'installez pas le routeur dans un environnement poussiéreux ou humide.

Veillez également à mettre le système hors tension, à retirer le cordon d'alimentation de la prise secteur et à sécher vos mains lors de l'installation du routeur.

Procédure d'installation de base

1. **Connectez le réseau local** : connectez le routeur à votre ordinateur ou à un concentrateur ou un commutateur. Connectez le câble Ethernet à partir de l'un des ports LAN situés à l'arrière du routeur à la carte réseau de votre ordinateur ou à un autre périphérique réseau.

Vous pouvez aussi connecter le routeur à votre ordinateur (en utilisant un adaptateur client sans fil) par l'intermédiaire de signaux radio. Positionnez les deux antennes à l'arrière du routeur dans les positions voulues. Pour une meilleure couverture, positionnez une antenne verticalement et l'autre horizontalement. **(Les antennes émettent des signaux dans le plan toroïdal et offrent donc une meilleure couverture lorsqu'elles sont placées sur deux axes différents.)**

Installation du routeur Barricade™ g sans fil

- 2. Connectez le WAN :** préparez un câble Ethernet pour la connexion du routeur à un modem Câble/xDSL ou à un routeur Ethernet.
- 3. Mettez le routeur sous tension :** branchez le cordon d'alimentation au routeur.

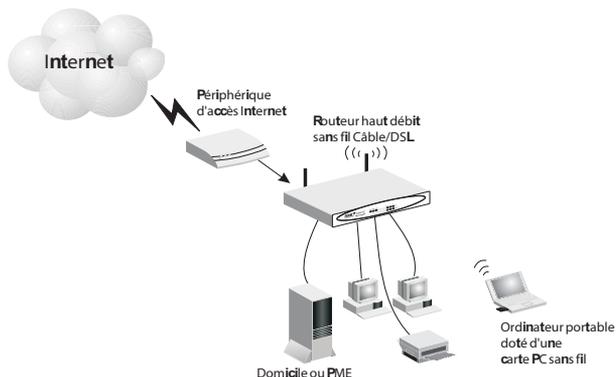


Figure 2. Connexion du routeur Barricade™ g sans fil

Connexion au réseau à l'aide d'un câblage Ethernet

Les quatre ports LAN du routeur négocient automatiquement le débit Ethernet 10 Mbps ou Fast Ethernet 100 Mbps, ainsi que le mode de transmission (Half/Full-duplex).

Utilisez un câble à paire torsadée pour connecter l'un des quatre ports LAN du routeur à un adaptateur Ethernet de votre ordinateur. Vous pouvez également relier en cascade l'un des ports LAN du routeur à un concentrateur ou un commutateur Ethernet, puis connecter votre ordinateur ou un autre équipement réseau au concentrateur ou au commutateur. Lors du branchement sur la prise RJ-45, vérifiez que les clips de fixation sont bien enclenchés pour assurer la connexion.

Avertissement : ne raccordez pas de prise téléphonique à un port RJ-45. Cela peut endommager le routeur. En revanche, utilisez uniquement des câbles à paire torsadée dotés de connecteurs RJ-45 conformes aux normes FCC.

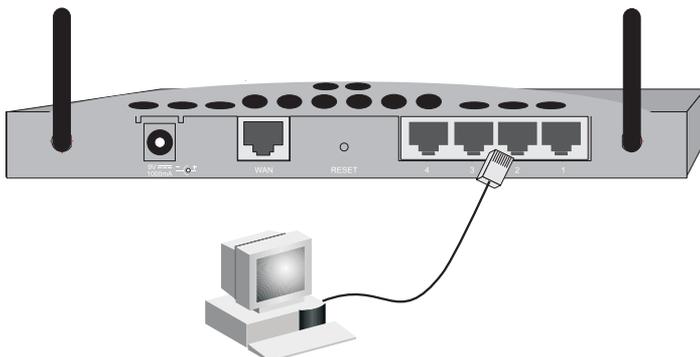


Figure 3. Établissement des connexions de réseau local

Connexion au réseau à l'aide de signaux radio

Installez une carte réseau sans fil dans chaque ordinateur destiné à être connecté à Internet ou à votre réseau local par l'intermédiaire de signaux radio. SMC propose actuellement plusieurs cartes réseau sans fil, telles que les cartes SMC2802W et SMC2835W.

Faites pivoter les deux antennes situées à l'arrière du routeur vers la position voulue. Pour une meilleure couverture, positionnez une antenne verticalement et l'autre horizontalement. Essayez de placer le routeur au centre de votre réseau sans fil. Normalement, plus l'antenne est haute, meilleures sont les performances. Assurez-vous que l'emplacement du routeur offre une réception optimale partout dans votre bureau ou votre domicile.

Installation du routeur Barricade™ g sans fil

Les ordinateurs équipés d'une carte sans fil peuvent communiquer les uns avec les autres au sein d'un réseau local sans fil indépendant ; il suffit pour cela de les configurer sur le même canal radio. Toutefois, le routeur peut offrir un accès à votre réseau local filaire/sans fil ou un accès à Internet pour tous les postes sans fil. Chaque PC sans fil de cette infrastructure réseau peut communiquer avec n'importe quel ordinateur du groupe sans fil via une liaison radio, ou accéder à d'autres ordinateurs ou à d'autres ressources réseau dans l'infrastructure de réseau local filaire ou sur Internet via le routeur.

L'infrastructure sans fil ne se limite pas à étendre l'accessibilité des PC sans fil au réseau local filaire, mais elle double aussi la portée de transmission sans fil efficace des PC sans fil en retransmettant les signaux radio entrants par l'intermédiaire du routeur.

Une infrastructure sans fil peut être utilisée pour l'accès à une base de données centrale ou pour la connexion entre des travailleurs mobiles, comme illustré à la figure ci-dessous :

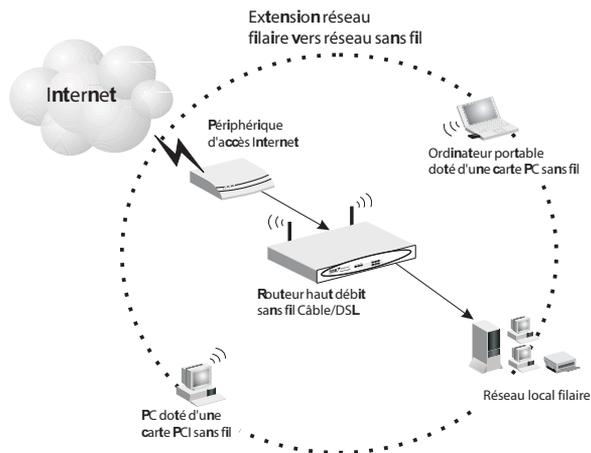


Figure 4. Établissement des connexions WLAN

Connexion du routeur Barricade™ g sans fil à Internet

Si les services Internet sont fournis via un modem Câble/xDSL, utilisez un câble Ethernet à paire torsadée blindé ou non (catégorie 3 ou supérieure), doté de prises RJ-45, pour connecter le modem haut débit directement au port WAN du routeur.

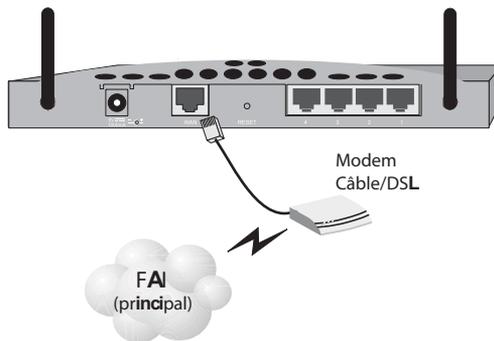


Figure 5. Établissement de la connexion WAN

Remarque : lors de la connexion du modem au port WAN, utilisez un câble 100 ohms à paire torsadée, blindé ou non, de catégorie 3, 4 ou 5 et doté de connecteurs RJ-45 aux deux extrémités.

Raccordement du cordon d'alimentation

Branchez l'une des extrémités du cordon à la prise située sur le routeur et l'autre extrémité à une prise secteur. Assurez-vous que le témoin d'alimentation PWR situé sur le panneau avant est allumé. S'il n'est pas allumé, reportez-vous à la section « Dépannage » à la page 86.

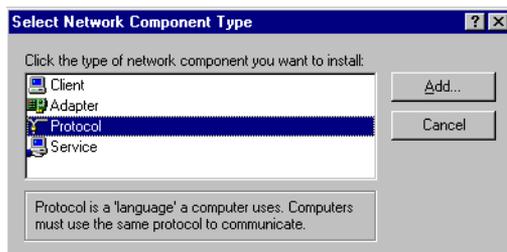
CONFIGURATION DE TCP/IP CLIENT

Si vous n'avez pas déjà configuré le protocole TCP/IP sur vos postes clients, reportez-vous à la section ci-après. Pour plus de détails sur la procédure de configuration d'une adresse TCP/IP sur un poste, reportez-vous à la section « Configuration de TCP/IP » à la page 19.

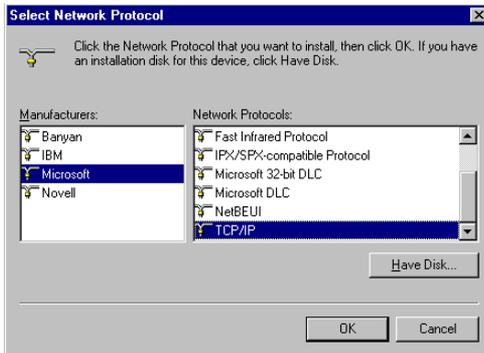
Installation de TCP/IP

Windows 95, Windows 98 ou ME

1. Cliquez sur [Start/Settings/Control Panel] (Démarrer/Paramètres/Panneau de configuration).
2. Double-cliquez sur l'icône [Network] (Réseau) et sélectionnez l'onglet [Configuration] de la fenêtre [Network] (Réseau).
3. Cliquez sur le bouton [Add] (Ajouter).
4. Double-cliquez sur [Protocol] (Protocole).



5. Sélectionnez [Microsoft] dans la liste des constructeurs. Choisissez [TCP/IP] dans la liste [Network Protocols] (Protocoles réseau). Cliquez sur [OK] pour revenir à la fenêtre [Network] (Réseau).



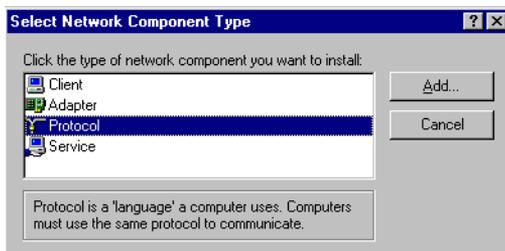
6. Le protocole TCP/IP s'affiche dans cette fenêtre. Cliquez sur [OK]. Il se peut que le système d'exploitation vous invite à redémarrer votre ordinateur. Cliquez sur [Yes] (Oui) ; l'ordinateur redémarre.

Windows 2000

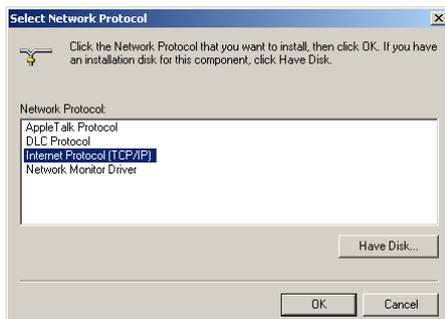
1. Cliquez sur le bouton [Start] (Démarrer) et choisissez [Settings] (Paramètres), puis cliquez sur l'icône [Network and Dial-up Connections] (Connexions réseau et accès à distance).
2. Double-cliquez sur l'icône [Local Area Connection] (Connexion au réseau local), puis cliquez sur le bouton [Properties] (Propriétés) dans l'onglet [General] (Général).
3. Cliquez sur le bouton [Install...] (Installer).

Configuration de TCP/IP client

4. Double-cliquez sur [Protocol] (Protocole).



5. Choisissez [Internet Protocol (TCP/IP)] (Protocole Internet (TCP/IP)). Cliquez sur [OK] pour revenir à la fenêtre [Network] (Réseau).



6. Le protocole TCP/IP s'affiche dans cette fenêtre. Cliquez sur [OK] pour terminer la procédure d'installation.

Configuration de TCP/IP

Pour accéder à Internet via le routeur, vous devez configurer les paramètres réseau des ordinateurs de votre réseau local afin d'utiliser le même sous-réseau IP que celui du routeur.

Les paramètres réseau par défaut du routeur sont les suivants :

Adresse IP de passerelle : 192.168.2.1

Subnet Mask (Masque de sous-réseau) : 255.255.255.0

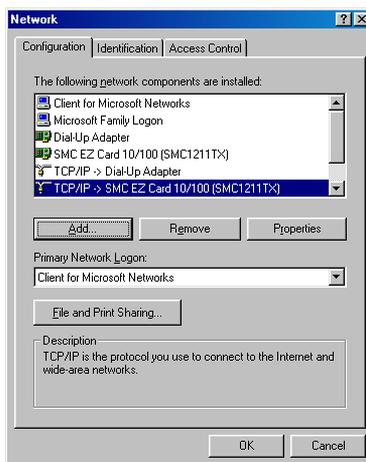
Remarque : vous pouvez modifier ces paramètres afin de répondre aux besoins spécifiques de votre réseau, mais vous devez auparavant configurer au moins un ordinateur selon la procédure décrite dans ce chapitre afin d'accéder à l'interface de configuration Web du routeur. Voir « Configuration du routeur Barricade™ g sans fil » à la page 33 pour plus d'informations sur la configuration du routeur.

Si vous n'avez pas déjà configuré TCP/IP pour votre ordinateur, reportez-vous à « Configuration de TCP/IP client » à la page 16. L'adresse IP de l'ordinateur client connecté doit être 192.168.2.x (où x est compris entre 2 et 254). Vous pouvez définir l'adresse IP des postes clients en vous la procurant automatiquement auprès du service DHCP du routeur ou au moyen d'une configuration manuelle.

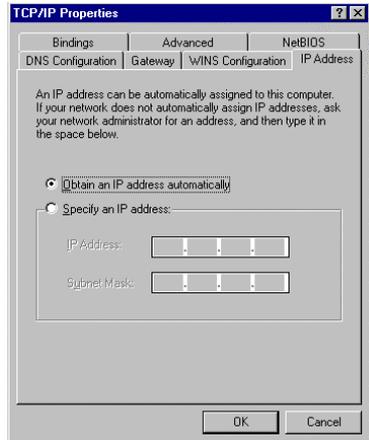
Configuration de votre ordinateur sous Windows 95/98/Me

Il se peut que les instructions communiquées dans le présent document ne correspondent pas exactement à votre version de Windows. Cela est dû au fait que ces instructions et ces écrans sont basés sur Windows 98. Windows 95 et Windows Millenium Edition sont très similaires, mais pas totalement identiques à Windows 98.

1. Depuis le Bureau Windows, cliquez sur [Start/Settings/Control Panel] (Démarrer/Paramètres/Panneau de configuration).
2. Dans le Panneau de configuration, localisez l'icône [Network] (Réseau) et double-cliquez dessus.
3. Dans la fenêtre [Network] (Réseau), sous l'onglet [Configuration], double-cliquez sur l'entrée [TCP/ IP] affichée pour votre carte réseau.



4. Cliquez sur l'onglet [IP Address] (Adresse IP).



5. Cliquez sur l'option [Obtain an IP address] (Obtenir une adresse IP).
6. Cliquez ensuite sur l'onglet [Gateway] (Passerelle) et vérifiez que la zone [Gateway] est vide. Si des adresses IP sont présentes dans la section [Gateway], mettez chacune d'elles en surbrillance et cliquez sur [Remove] (Supprimer) jusqu'à ce que la section soit vide.
7. Cliquez sur le bouton [OK] pour fermer la fenêtre des propriétés TCP/IP.
8. Dans la fenêtre [Network Properties] (Propriétés du réseau), cliquez sur le bouton [OK] pour enregistrer ces nouveaux paramètres.

Remarque : il est possible que Windows vous demande le disque d'installation de Windows ou des fichiers supplémentaires. Recherchez les fichiers dans c:\windows\options\cabs, ou insérez votre CD-ROM Windows dans le lecteur de CD-ROM puis spécifiez l'emplacement des fichiers, par exemple D:\win98 ou D:\win9x (si D est la lettre de votre lecteur de CD-ROM).

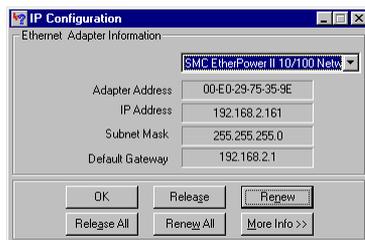
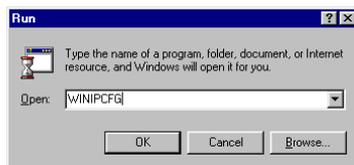
Configuration de TCP/IP client

- Il est possible que Windows vous invite à redémarrer votre PC. Si tel est le cas, cliquez sur le bouton [Yes] (Oui).
Si Windows ne vous invite pas à redémarrer votre ordinateur, faites-le quand même pour enregistrer vos paramètres.

Lecture des paramètres IP de votre routeur Barricade™ g sans fil

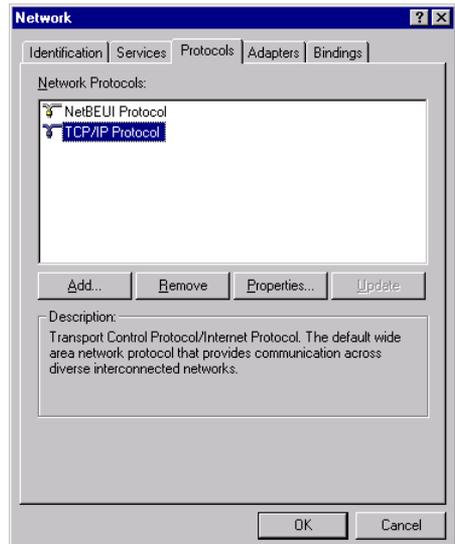
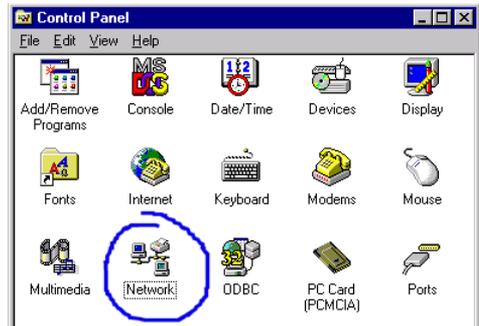
Maintenant que vous avez configuré votre ordinateur pour la connexion à votre routeur, il est nécessaire de lui indiquer les nouveaux paramètres réseau. En libérant les anciens paramètres IP et en les remplaçant par ceux de votre routeur, vous pouvez également vérifier que vous avez correctement configuré votre ordinateur.

- Cliquez sur [Start/Run] (Démarrer/Exécuter).
- Tapez WINIPCFG puis cliquez sur [OK].
- Dans la liste déroulante, sélectionnez votre carte réseau, cliquez sur [Release] (Libérer), puis sur [Renew] (Renouveler). Vérifiez que votre adresse IP est maintenant 192.168.2.xxx, votre masque de sous-réseau 255.255.255.0 et votre passerelle par défaut 192.168. 2.1. Ces valeurs attestent du fonctionnement du routeur. Cliquez sur [OK] pour fermer la fenêtre [IP Configuration] (Configuration IP).



Configuration de votre ordinateur sous Windows NT 4.0

1. Depuis le Bureau Windows, cliquez sur [Start/Settings/Control Panel] (Démarrer/Paramètres/Panneau de configuration).
2. Double-cliquez sur l'icône [Network] (Réseau).
3. Cliquez sur l'onglet [Protocols] (Protocoles).
4. Double-cliquez sur [TCP/IP Protocol] (Protocole TCP/IP).



Configuration de TCP/IP client

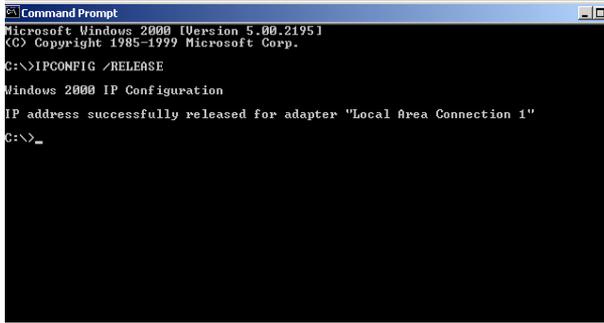
5. Cliquez sur l'onglet [IP Address] (Adresse IP).
6. Dans la liste déroulante des cartes, assurez-vous que votre carte Ethernet est sélectionnée.
7. Cliquez sur l'option [Obtain an IP address from a DHCP server] (Obtenir une adresse IP à partir d'un serveur DHCP).
8. Cliquez sur [OK] pour la fermer.
9. Windows peut alors copier des fichiers et vous demander de redémarrer votre système. Cliquez sur [Yes] (Oui) ; votre ordinateur redémarre.

Lecture des paramètres IP depuis votre routeur Barricade™ g sans fil

Maintenant que vous avez configuré votre ordinateur pour la connexion au routeur, il est nécessaire de lui indiquer les nouveaux paramètres réseau. En libérant les anciens paramètres IP et en les remplaçant par ceux du routeur, vous pouvez également vérifier que vous avez correctement configuré votre ordinateur.

1. Depuis le Bureau Windows, cliquez sur [Start/Programs/Command Prompt] (Démarrer/Programmes/Invite de commandes).

2. Dans la fenêtre qui s'affiche, tapez IPCONFIG/RELEASE et appuyez sur la touche <ENTRÉE>.

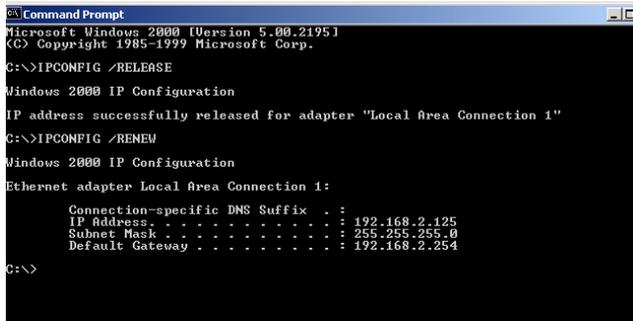


```
Command Prompt
Microsoft Windows [Version 5.00.21951]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"
C:\>_
```

3. Tapez IPCONFIG /RENEW et appuyez sur la touche <ENTRÉE>. Vérifiez que votre adresse IP est maintenant 192.168.2.xxx, votre masque de sous-réseau 255.255.255.0 et votre passerelle par défaut 192.168.2.1. Ces valeurs attestent du fonctionnement du routeur.



```
Command Prompt
Microsoft Windows [Version 5.00.21951]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"
C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

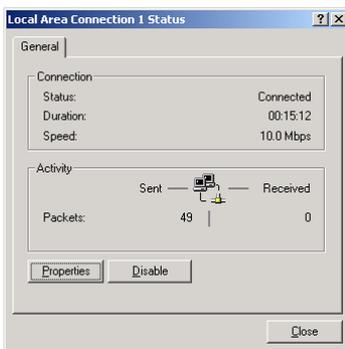
Ethernet adapter Local Area Connection 1:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254
C:\>
```

4. Tapez EXIT et appuyez sur <ENTRÉE> pour fermer la fenêtre [Command Prompt] (Invite de commandes).

Configuration de votre ordinateur sous Windows 2000

1. Accédez à vos paramètres réseau en cliquant sur le bouton [Start] (Démarrer) et en sélectionnant [Settings] (Paramètres), puis [Control Panel] (Panneau de configuration).
2. Dans le Panneau de configuration, localisez l'icône [Network and Dial-up Connections] (Connexions réseau et accès à distance) et double-cliquez dessus.
3. Localisez l'icône [Local Area Connection] (Connexion au réseau local) pour la carte Ethernet connectée au routeur, et double-cliquez dessus. Lorsque la boîte de dialogue [Status] (État) s'ouvre, cliquez sur le bouton [Properties] (Propriétés).
4. Dans la boîte de dialogue [Local Area Connection Properties] (Propriétés de Connexion au réseau local), vérifiez que la case à cocher située à côté du protocole Internet (TCP/IP) est activée. Mettez ensuite en surbrillance le protocole Internet (TCP/IP) et cliquez sur le bouton [Properties] (Propriétés).
5. Sélectionnez l'option [Obtain an IP address automatically] (Obtenir une adresse IP automatiquement) afin de configurer votre ordinateur pour DHCP. Cliquez sur le bouton [OK] pour enregistrer cette modification et fermer la fenêtre [Properties] (Propriétés).
6. Cliquez de nouveau sur [OK] pour enregistrer ces nouvelles modifications.

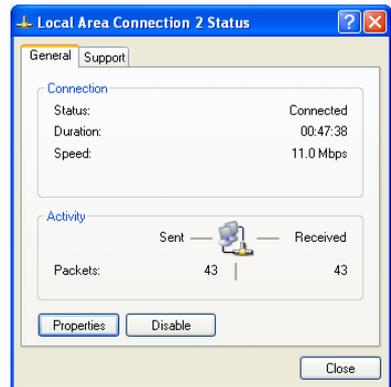


7. Redémarrez votre PC.
8. Pour obtenir de nouveaux paramètres réseau, consultez « Lecture des paramètres IP de votre routeur Barricade™ g sans fil » à la page 22.

Configuration de votre ordinateur sous Windows XP

Les instructions suivantes supposent que vous exécutez Windows XP avec l'interface par défaut. Si vous utilisez l'interface classique (dans laquelle les icônes et les menus ressemblent à ceux des versions précédentes de Windows), suivez les instructions pour Windows 2000 présentées plus haut.

1. Pour accéder à vos paramètres réseau, cliquez sur [Start] (Démarrer), sur [Control Panel] (Panneau de configuration) puis sur [Network and Internet Connections] (Connexions réseau et Internet), puis cliquez sur l'icône [Network Connections] (Connexions réseau).
2. Localisez l'icône [Local Area Connection] (Connexion au réseau local) pour la carte Ethernet connectée au routeur, et double-cliquez dessus. Cliquez ensuite sur le bouton [Properties] (Propriétés).



Configuration de TCP/IP client

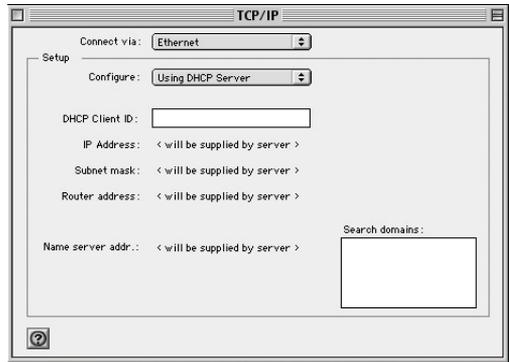
3. Dans la boîte de dialogue [Local Area Connection Properties] (Propriétés de Connexion au réseau local), vérifiez que la case à cocher située à côté du protocole Internet (TCP/IP) est activée. Mettez ensuite en surbrillance le protocole Internet (TCP/IP) et cliquez sur le bouton [Properties] (Propriétés).
4. Sélectionnez l'option [Obtain an IP address automatically] (Obtenir une adresse IP automatiquement) afin de configurer votre ordinateur pour DHCP. Cliquez sur le bouton [OK] pour enregistrer cette modification et fermer la fenêtre [Properties] (Propriétés).
5. Cliquez de nouveau sur [OK] pour enregistrer ces nouvelles modifications.
6. Redémarrez votre PC.

Configuration d'un ordinateur Macintosh

Vous noterez peut-être que les instructions de ce manuel ne correspondent pas exactement à votre écran. En effet, ces étapes et les captures d'écrans ont été effectuées sous Mac OS 8.5. Mac OS 7.x et les systèmes ultérieurs sont tous très similaires, mais peuvent ne pas être identiques à Mac OS 8.5.

1. Déroulez le menu [Apple]. Cliquez sur [Control Panel] (Tableau de bord) et sélectionnez TCP/IP.

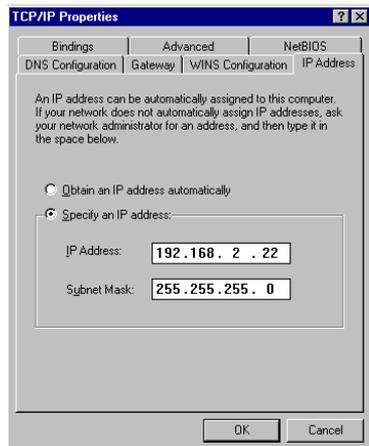
2. Dans la boîte de dialogue qui s'affiche, vérifiez que l'option [Ethernet] est sélectionnée dans la zone [Connect via:] (Se connecter via).



3. Sélectionnez [Using DHCP Server] (Utiliser un serveur DHCP) dans la zone [Configure] (Configuration).
4. Fermez la boîte de dialogue TCP/IP.

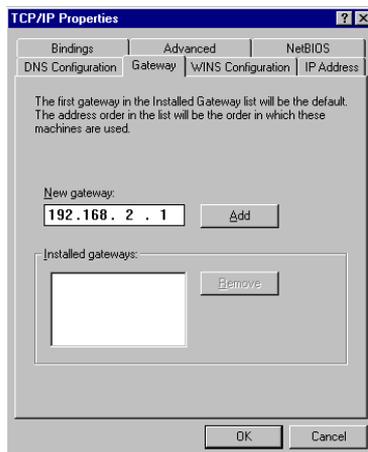
Configuration IP manuelle

1. Activez l'option [Specify an IP address] (Spécifier une adresse IP) sous l'onglet [IP Address] (Adresse IP). Entrez une adresse IP en fonction du réseau par défaut 192.168.2.x (où x est compris entre 2 et 254), puis utilisez 255.255.255.0 pour le masque de sous-réseau.

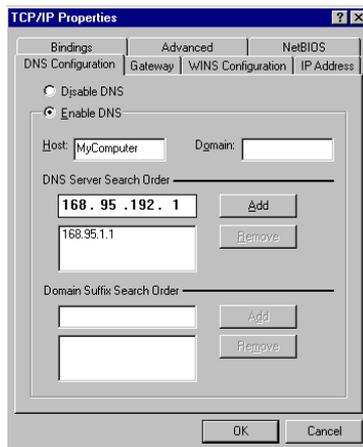


Configuration de TCP/IP client

2. Dans l'onglet [Gateway] (Passerelle), ajoutez l'adresse IP du routeur (par défaut : 192.168.2.1) dans la zone [New gateway] (Nouvelle passerelle) et cliquez sur [Add] (Ajouter).



3. Sous l'onglet [DNS Configuration] (Configuration DNS), ajoutez l'adresse IP du routeur et cliquez sur [Add] (Ajouter). Les requêtes DNS sont automatiquement relayées au(x) serveur(s) DNS offert(s) par votre Fournisseur d'Accès Internet. Sinon, ajoutez des serveurs DNS spécifiques dans la zone [DNS Server Search Order] (Ordre de recherche DNS) et cliquez sur [Add] (Ajouter).



4. Une fois la configuration TCP/IP terminée, cliquez sur [OK], puis redémarrez l'ordinateur. Configurez ensuite d'autres postes du réseau local en suivant les procédures décrites ci-dessus.

Vérification de la connexion TCP/IP

Après avoir installé le protocole de communication TCP/IP puis configuré une adresse IP sur le même réseau que le routeur, utilisez la commande Ping pour vérifier si votre ordinateur s'est correctement connecté au routeur. L'exemple ci-après indique comment la procédure Ping peut être exécutée dans une fenêtre MS-DOS. En premier lieu, exécutez la commande Ping suivante :

```
ping 192.168.2.1
```

Si un message similaire au suivant s'affiche :

```
Pinging 192.168.2.1 with 32 bytes of data  
(Envoi d'une requête " ping " sur 192.168.2.1  
avec 32 octets de données) :  
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64  
(Réponse de 192.168.2.1 : octets=32 temps=2 ms  
TTL=64)
```

une liaison entre votre ordinateur et le routeur a été établie.

Si le message suivant apparaît :

```
Pinging 192.168.2.1 with 32 bytes of data (Envoi  
d'une requête " ping " sur 192.168.2.1 avec 32  
octets de données) :  
Request timed out (Délai d'attente de la demande  
dépassé),
```

Configuration de TCP/IP client

il se peut qu'un incident se soit produit lors de la procédure d'installation. Vérifiez les éléments suivants dans l'ordre indiqué :

1. Le câble Ethernet est-il correctement connecté entre le routeur et l'ordinateur ?

Le témoin lumineux LAN (Réseau local) du routeur et le témoin Link (Liaison) de la carte réseau de votre ordinateur doivent être allumés.

2. Le protocole TCP/IP est-il correctement configuré sur votre ordinateur ?

Si l'adresse IP du routeur est 192.168.2.1, celle de votre ordinateur doit être comprise entre 192.168.2.2 et 192.168.2.254 et celle de la passerelle par défaut doit être 192.168.2.1.

Si la commande Ping du routeur aboutit, vous êtes prêt à vous connecter à Internet !

CONFIGURATION DU ROUTEUR BARRICADE™ G SANS FIL

Ce routeur peut être configuré par tous les navigateurs supportant Java, y compris Internet Explorer version 4.0 ou ultérieure ou bien Netscape Navigator version 4.0 ou ultérieure. Grâce à l'interface d'administration Web, vous pouvez configurer le routeur et afficher des statistiques pour surveiller l'activité du réseau.

Remarque : avant d'essayer de configurer votre routeur, si vous avez accès à Internet visitez www.smc.com ou www.smc-europe.com et téléchargez la dernière mise à jour du logiciel pour garantir que votre routeur utilisera le logiciel le plus récent.

Avant de vous connecter à l'administration Web, vérifiez les points suivants :

1. Votre navigateur doit être correctement configuré (voir ci-dessous).
2. Désactivez tout firewall ou logiciel de sécurité en cours d'exécution.
3. Vérifiez que le témoin de liaison correspondant à la connexion de votre ordinateur au routeur est correct. Si ce témoin est éteint, essayez un autre câble jusqu'à ce que la liaison soit correcte.

Configuration du navigateur

Vérifiez que votre navigateur est configuré pour une connexion directe à Internet au moyen du câble Ethernet installé dans l'ordinateur. Cette configuration s'effectue dans la section options/préférences de votre navigateur.

Désactivation de la connexion du proxy

Vous devez également vérifier que la fonctionnalité Proxy HTTP de votre navigateur Web est désactivée. Cela est nécessaire pour que votre navigateur Web puisse afficher les pages de configuration du routeur. Les étapes ci-dessous concernent Internet Explorer et Netscape. Déterminez le navigateur utilisé et suivez les étapes appropriées.

Internet Explorer version 5 ou ultérieure (pour Windows)

1. Ouvrez Internet Explorer. Cliquez sur [Tools] (Outils), puis sur [Internet Options] (Options Internet).
2. Dans la fenêtre qui s'affiche, cliquez sur l'onglet [Connections] (Connexions).
3. Cliquez sur le bouton [LAN Settings] (Paramètres LAN).
4. Désactivez toutes les cases à cocher puis cliquez sur [OK] pour enregistrer les modifications de ces paramètres.
5. Cliquez de nouveau sur [OK] pour fermer la fenêtre [Internet Options] (Options Internet).

Internet Explorer (pour Macintosh)

1. Ouvrez Internet Explorer. Cliquez sur [Edit/Preferences] (Edition/Préférences).
2. Dans la boîte de dialogue qui s'affiche, sous [Network] (Réseau), sélectionnez [Proxies] (Serveur proxy).
3. Désactivez toutes les cases à cocher et cliquez sur [OK].

Netscape (version 4 ou ultérieure)

1. Ouvrez Netscape. Cliquez sur [Edit] (Edition), puis sur [Preferences] (Préférences).
2. Dans la fenêtre qui s'affiche, sous [Category] (Catégorie), double-cliquez sur [Advanced] (Avancé), puis cliquez sur [Proxies] (Serveur proxy).
3. Activez l'option [Direct connection to the Internet] (Connexion directe à Internet).
4. Cliquez sur [OK] pour enregistrer ces modifications.

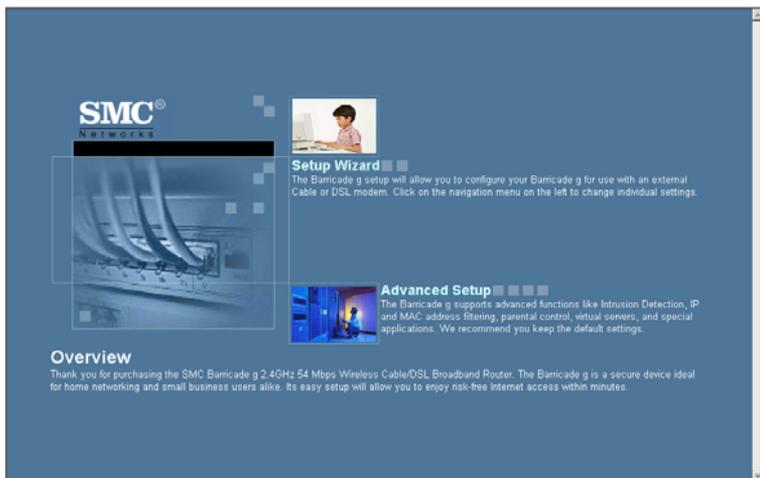
Exploration de l'interface Web

Pour accéder à l'interface d'administration du routeur, entrez l'adresse IP du routeur dans votre navigateur Web : <http://192.168.2.1>. Cliquez ensuite sur [LOGIN] (Se connecter). (Par défaut, aucun mot de passe n'est défini.)



Configuration du routeur Barricade™ g sans fil

La page d'accueil affiche les options [Setup Wizard] (Assistant de configuration) et [Advanced Setup] (Configuration avancée).



L'interface d'administration du routeur comporte un Assistant de configuration [Setup Wizard] et une section de configuration avancée [Advanced Setup]. Servez-vous de l'Assistant de configuration pour configurer rapidement le routeur afin de l'utiliser avec un modem Câble ou DSL.

La section [Advanced Setup] supporte des fonctions plus avancées, parmi lesquelles la détection d'attaques extérieures, le filtrage d'adresses IP et MAC, la détection d'intrusion, la configuration de serveur virtuel, les hôtes DMZ virtuels et d'autres fonctions avancées.

Modification de la configuration

Les paramètres configurables sont dotés d'une boîte de dialogue ou d'une liste déroulante. Lorsqu'une modification de configuration a été apportée à une page, n'oubliez pas de cliquer sur le bouton [APPLY] (Appliquer) ou [NEXT] (Suivant) au bas de la page pour valider le nouveau paramètre.

Remarque : pour garantir l'actualisation correcte de l'écran à la suite d'une entrée de commande, assurez-vous qu'Internet Explorer 5.0 est configuré comme suit : dans [Tools/Internet Options/General/Temporary Internet Files/Settings] (Outils/Options Internet/Général/Fichiers Internet temporaires/Paramètres), le paramètre [Check for newer versions of stored pages] (Vérifier s'il existe une version plus récente des pages enregistrées) doit avoir pour valeur [Every visit to the page] (À chaque visite de la page).

Assistant de configuration Setup Wizard

Time Zone (Fuseau horaire)

Cliquez sur l'image de l'assistant Setup Wizard. La première des étapes de l'Assistant est la configuration du fuseau horaire.

Pour la précision horaire du filtrage de poste client et des événements de journal, vous devez définir le fuseau horaire. Sélectionnez votre fuseau horaire et votre serveur horaire dans la liste déroulante, puis cliquez sur [NEXT] (SUIVANT).

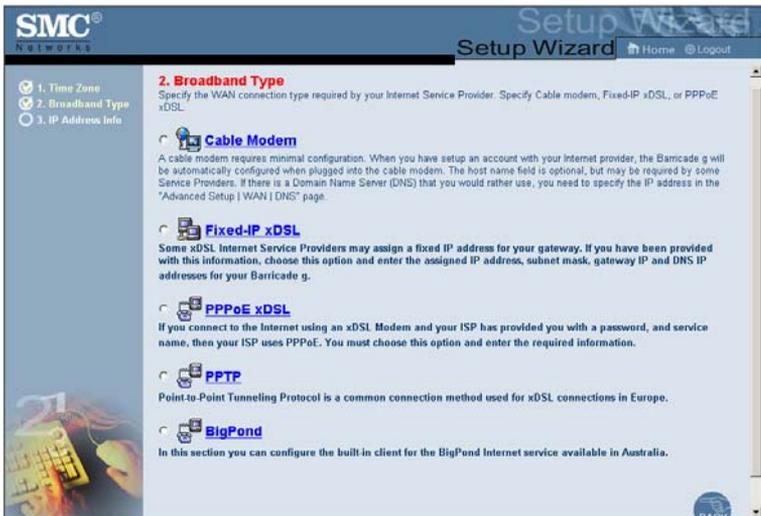


The screenshot shows the '1. Time Zone' configuration page of the SMC Networks Setup Wizard. The page has a blue header with the SMC Networks logo and the text 'Setup Wizard' and 'Setup Wizard' with 'Home' and 'Logout' links. On the left, there is a sidebar with three steps: '1. Time Zone' (selected), '2. Broadband Type', and '3. IP Address Info'. The main content area is titled '1. Time Zone' and contains the following text: 'Set the time zone for the Barricade g. This information is used for log entries and client filtering.' Below this is a 'Set Time Zone' section with a dropdown menu showing '(GMT-08:00)Pacific Time (US & Canada), Tijuana'. The next section is 'Configure Time Server (NTP):' with the text 'You can automatically maintain the system time on your SMC Barricade by synchronizing with a public time server over the Internet.' Below this is a checkbox labeled 'Enable Automatic Time Server Maintenance'. The text below the checkbox says 'When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:'. There are two dropdown menus for 'Primary Server:' and 'Secondary Server:', both showing '132.163.4.102 - North America' and '192.5.41.41 - North America' respectively. A 'NEXT' button is located in the bottom right corner of the page.

Broadband Type (Type de connexion haut débit)

Sélectionnez le type de connexion haut débit dont vous disposez.

Pour une connexion par modem Câble, consultez la page suivante. Pour une connexion xDSL avec adresse IP fixe, reportez-vous à la section « Fixed-IP xDSL (Connexion xDSL via une adresse IP statique) » à la page 40, pour une connexion xDSL via le protocole PPP sur Ethernet, à la section « PPPoE (Point-to-point over Ethernet) » à la page 41 et pour une connexion BigPond, à la section « BigPond » à la page 43.



The screenshot shows the SMC Networks Setup Wizard interface. The title bar includes the SMC logo and the text 'Setup Wizard' with 'Home' and 'Logout' links. The main content area is titled '2. Broadband Type' and instructs the user to 'Specify the WAN connection type required by your Internet Service Provider. Specify Cable modem, Fixed-IP xDSL, or PPPoE xDSL.' There are five radio button options: 'Cable Modem', 'Fixed-IP xDSL', 'PPPoE xDSL', 'PPTP', and 'BigPond'. Each option has a brief description of its requirements. A sidebar on the left shows the progress of the wizard with three steps: '1. Time Zone', '2. Broadband Type' (which is selected), and '3. IP Address Info'. A 'BACK' button is visible in the bottom right corner.

SMC
NETWORKS

Setup Wizard
Home Logout

2. Broadband Type
Specify the WAN connection type required by your Internet Service Provider. Specify Cable modem, Fixed-IP xDSL, or PPPoE xDSL.

Cable Modem
A cable modem requires minimal configuration. When you have setup an account with your Internet provider, the Barricade g will be automatically configured when plugged into the cable modem. The host name field is optional, but may be required by some Service Providers. If there is a Domain Name Server (DNS) that you would rather use, you need to specify the IP address in the "Advanced Setup | WAN | DNS" page.

Fixed-IP xDSL
Some xDSL Internet Service Providers may assign a fixed IP address for your gateway. If you have been provided with this information, choose this option and enter the assigned IP address, subnet mask, gateway IP and DNS IP addresses for your Barricade g.

PPPoE xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a password, and service name, then your ISP uses PPPoE. You must choose this option and enter the required information.

PPTP
Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.

BigPond
In this section you can configure the built-in client for the BigPond Internet service available in Australia.

1. Time Zone
2. Broadband Type
3. IP Address Info

BACK

Configuration du routeur Barricade™ g sans fil

Cable Modem (Modem Câble)

Après la sélection de [Cable Modem] (Modem Câble) pour [Broadband Type] (Type haut débit), un message apparaît pour indiquer que les données ont été enregistrées avec succès.

Remarque : sélectionnez [Home] (Accueil) pour revenir à la page d'accueil, puis sélectionnez [Advanced Settings/WAN] (Paramètres avancés/WAN) pour configurer les paramètres nécessaires. (Voir la section « WAN (Réseau étendu) » à la page 48.)

Fixed-IP xDSL (Connexion xDSL via une adresse IP statique)



The screenshot shows a web interface for configuring Fixed-IP xDSL. It features a title bar with a small icon and the text 'Fixed-IP xDSL'. Below the title bar, there are four rows of input fields, each with a label on the left and four numeric input boxes on the right. The labels are 'IP Address', 'Gateway IP Address', 'DNS IP Address', and 'Subnet Mask'. The numeric input boxes are arranged in a 4x4 grid, with each row corresponding to one of the labels.

Field	Digit 1	Digit 2	Digit 3	Digit 4
IP Address	0	0	0	0
Gateway IP Address	0	0	0	0
DNS IP Address	0	0	0	0
Subnet Mask	0	0	0	0

Certains Fournisseurs d'Accès Internet xDSL peuvent attribuer une adresse IP statique. Si tel est le cas, sélectionnez cette option et entrez l'adresse IP qui vous a été attribuée, l'adresse IP de la passerelle, les adresses IP DNS et le masque du sous-réseau. Cliquez sur [FINISH] (Terminer) pour terminer la configuration.

PPPoE (Point-to-point over Ethernet)



The screenshot shows a web-based configuration interface for PPPoE. At the top left, there is a logo with the text 'PPPoE'. Below it, a blue header bar contains the text 'Use PPPoE Authentication'. The main form area is yellow and contains several input fields: 'User Name', 'Password', 'Please retype your password', and 'Service Name'. Below these are 'MTU' (set to 1454 with a note '(1440<=MTU Value<=1492)') and 'Maximum Idle Time' (set to 10). At the bottom, there is a checkbox labeled 'Auto-reconnect' which is checked.

Entrez le nom d'utilisateur PPPoE et le mot de passe attribués par votre Fournisseur d'Accès Internet. Le nom de service est généralement facultatif ; cependant, il peut être requis par certains fournisseurs.

Conservez la valeur par défaut (1454) attribuée à la zone [MTU] (Maximum Transmission Unit), à moins d'avoir une raison particulière de la modifier.

Entrez la durée maximale d'inactivité (en minutes) dans la zone [Maximum Idle Time]. Cette durée correspond à l'intervalle de temps maximal pendant lequel la connexion à Internet doit être maintenue en période d'inactivité. Si le temps d'inactivité de la connexion dépasse la valeur attribuée à la zone [Maximum Idle Time], la connexion est interrompue. (Par défaut : 10)

Activez l'option [Auto-reconnect] (Reconnexion automatique) afin que la connexion soit automatiquement rétablie dès que vous tentez de nouveau d'accéder à Internet. Cliquez sur [FINISH] (Terminer) pour terminer la configuration.

Configuration du routeur Barricade™ g sans fil

PPTP (Point-to-Point Tunneling Protocol)

IP Address:	0	0	0	0
Subnet Mask:	0	0	0	0
Default Gateway:	0	0	0	0
User ID:	<input type="text"/>			
Password:	<input type="text"/>			
PPTP Gateway:	0	0	0	0
Idle Time Out:	10	(min)		

La méthode de connexion PPTP est une méthode couramment utilisée en Europe pour les connexions xDSL. Elle peut être utilisée pour relier différents réseaux physiques en utilisant Internet comme intermédiaire.

Si vous avez reçu les informations indiquées à l'écran, entrez l'adresse IP, le masque de sous-réseau, l'adresse IP de la passerelle par défaut, l'identifiant et le mot de passe et la passerelle PPTP.

Entrez la durée maximale d'inactivité (en minutes) dans la zone [Maximum Idle Time]. Cette durée correspond à l'intervalle de temps maximal pendant lequel la connexion à Internet doit être maintenue en période d'inactivité. Si le temps d'inactivité de la connexion dépasse la valeur attribuée à la zone [Maximum Idle Time], la connexion est interrompue. (Par défaut : 10)

Cliquez sur [FINISH] (Terminer) pour terminer la configuration. (Reportez-vous à « Protocole PPTP (Point-to-Point Tunneling Protocol) » à la page 51 pour plus de détails.)

Remarque : si vous ne bénéficiez pas d'un tarif forfaitaire, sachez que l'attribution de la valeur 0 au paramètre [Maximum Idle Time] (Durée maximale d'inactivité) et/ou l'activation de l'option [Auto-Reconnect] (Reconnexion automatique) peut augmenter le montant de votre facture téléphonique.

BigPond

In this section you can configure the built-in client for the BigPond Internet service available in Australia.

BigPond Authentication Client	
User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	login-server

Si vous utilisez le service Internet BigPond disponible en Australie, vous devez saisir votre nom d'utilisateur, mot de passe et nom de service pour l'authentification BigPond. Cliquez sur [FINISH] (Terminer) pour terminer la configuration.

Configuration avancée

Utilisez l'interface Web d'administration pour définir les paramètres du système, gérer et contrôler le routeur et ses ports, ou surveiller l'état du réseau. Le tableau suivant présente les options disponibles dans ce programme :

Menu	Description
System (Système)	Sert à définir le fuseau horaire, le mot de passe d'accès en tant qu'administrateur et l'adresse IP d'un ordinateur autorisé à gérer le routeur à distance.
WAN (Réseau étendu)	Indique le type de connexion Internet : <ul style="list-style-type: none">• Configuration hôte avec adresse IP dynamique et l'adresse MAC physique de chaque interface de support• Configuration PPPoE• PPTP• Adresse IP statique et adresse de passerelle du FAI• BigPond (service Internet disponible en Australie)• Serveurs DNS à utiliser pour la résolution des noms de domaines
LAN (Réseau local)	Définit la configuration TCP/IP associée à l'interface LAN du routeur et à tous les clients DHCP.

Configuration du routeur Barricade™ g sans fil

Menu	Description
NAT (Translation d'adresses réseau)	Permet de partager un compte de Fournisseur d'Accès Internet unique entre plusieurs utilisateurs et de configurer des serveurs virtuels.
Wireless (Sans fil)	Configure la fréquence radio, le SSID, le cryptage et l'identificateur de priorité 802.1x pour les communications sans fil.
Firewall	Permet la configuration d'un grand nombre de fonctions de sécurité et de fonctions spécialisées, comprenant : contrôle d'accès, prévention du piratage et DMZ.
DDNS	La fonctionnalité DNS dynamique intégrée fournit aux utilisateurs sur Internet une méthode pour lier leurs noms de domaines à des ordinateurs ou des serveurs.
UPnP	Avec Universal Plug and Play, un périphérique peut joindre automatiquement et de façon dynamique un réseau, obtenir une adresse IP, communiquer ses capacités et obtenir des informations sur la présence et les capacités des autres périphériques. Les périphériques peuvent ensuite communiquer directement les uns avec les autres. Cela facilite le réseau de poste à poste.
Tools (Outils)	Contient les options permettant de sauvegarder et de restaurer la configuration actuelle, de restaurer tous les paramètres de configuration par défaut, de mettre à niveau le logiciel du système ou de réinitialiser ce dernier.
Status (État)	Indique le type et l'état de la connexion WAN, les numéros de version du logiciel et du matériel, les paramètres IP du système, ainsi que des informations DHCP, NAT et de firewall. Affiche le nombre de postes clients connectés, les versions du logiciel, l'adresse MAC physique de chaque interface de support, ainsi que le numéro de version et de série du matériel. Affiche le journal de sécurité et des clients DHCP.

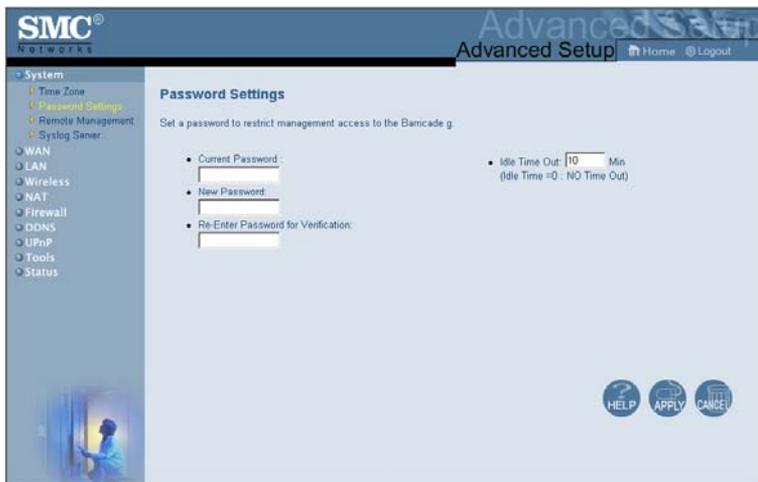
System (Système)

Time Zone (Fuseau horaire)

The screenshot shows the 'Advanced Setup' page for 'Time Zone' in the SMC Networks management interface. The page title is 'Time Zone' and it includes a sub-header 'Set the time zone of the Barricade g. This information is used for log entries and client filtering.' Below this, there is a 'Set Time Zone' section with a dropdown menu currently set to '(GMT-08:00)Pacific Time (US & Canada); Tijuana'. The 'Configure Time Server (NTP)' section explains that the system can automatically maintain time by synchronizing with a public time server over the Internet. There is a checked checkbox for 'Enable Automatic Time Server Maintenance'. Below this, instructions state that when this option is enabled, two different time servers should be configured. The 'Primary Server' is set to '132.163.4.102 - North America' and the 'Secondary Server' is set to '192.5.41.41 - North America'. At the bottom right, there are three circular buttons: 'HELP', 'APPLY', and 'CANCEL'. A navigation menu on the left lists various system settings like 'Time Zone', 'Password Settings', 'Remote Management', 'Syslog Server', 'WAN', 'LAN', 'Wireless', 'NAT', 'Firewall', 'DNS', 'UPnP', 'Tools', and 'Status'.

Permet de définir le fuseau horaire et le serveur horaire du routeur. Cette information est utilisée pour les entrées de journal et le contrôle des accès clients.

Password Settings (Paramètres de mot de passe)



Ce menu sert à limiter les accès au moyen d'un mot de passe. Par défaut, aucun mot de passe n'est défini. Pour des raisons de sécurité, il est conseillé de définir un mot de passe avant de relier le routeur à Internet.

Les mots de passe peuvent comporter 3 à 12 caractères alphanumériques et ne font pas de distinction entre les majuscules et les minuscules.

Remarque : si vous oubliez votre mot de passe ou que vous ne pouvez pas accéder à l'interface utilisateur, appuyez sur le bouton [Reset] (Réinitialiser) sur le panneau arrière (en le maintenant enfoncé pendant au moins cinq secondes), afin de restaurer les valeurs par défaut. (Par défaut, aucun mot de passe n'est défini.)

Entrez la durée maximale d'inactivité (en minutes) dans la zone [Maximum Idle Time] (Durée maximale d'inactivité). Cette durée correspond à l'intervalle de temps maximal pendant lequel la session de connexion doit être maintenue en période d'inactivité. Si la connexion reste inactive pendant un temps supérieur au délai maximal d'inactivité, la session système est fermée et vous devez ouvrir une nouvelle session d'administration Web. (Par défaut : 10 minutes)

Remote Management (Administration à distance)



La fonctionnalité [Remote Management] (Administration à distance) permet à un ordinateur distant de configurer, de gérer et de contrôler le routeur à l'aide d'un navigateur Web standard. Activez la case à cocher [Enable] (Activer), puis entrez l'adresse IP du système hôte distant. Cliquez sur [APPLY] (Appliquer).

Remarque : si vous spécifiez 0.0.0.0 pour cette adresse IP, n'importe quel système hôte pourra gérer le routeur.

Syslog Server (Serveur Syslog)



Le serveur Syslog permet de télécharger le fichier journal du routeur et de le transmettre à l'adresse IP du serveur que vous spécifiez dans cet écran. (Par défaut : désactivé)

WAN (Réseau étendu)

Spécifiez le type de connexion WAN indiqué par votre Fournisseur d'Accès Internet, puis cliquez sur [More Configuration] (Suite de la configuration) afin d'entrer des paramètres de configuration détaillés pour le type de connexion sélectionné.

Dynamic IP (IP dynamique)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under the WAN category, the following options are listed: Dynamic IP (selected), PPPoE, PPTP, Static IP, BigPond, and DNS. The main content area is titled "Dynamic IP" and contains the following text:

The Host name is optional, but may be required by some Service Providers. The default MAC address is set to the WAN's physical interface on the Danicade g

If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.

If necessary, you can use the "Release" and "Renew" buttons on the Status page to release and renew the WAN IP address.

The configuration form includes:

- Host Name:
- MAC Address: - - - - -
- Clone MAC Address:

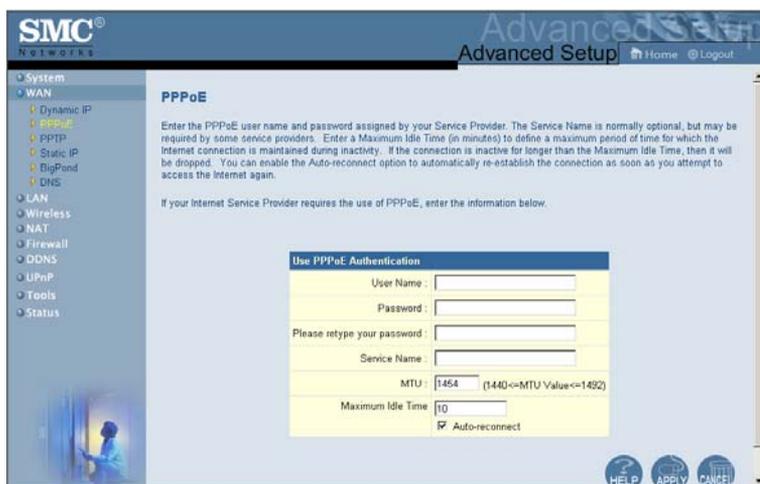
At the bottom right of the form area, there are three circular buttons: HELP, APPLY, and CANCEL.

Le nom d'hôte est facultatif ; cependant, il peut être requis par certains Fournisseurs d'Accès Internet. L'adresse MAC par défaut correspond à l'interface physique du réseau WAN sur le routeur. Utilisez cette adresse lors de l'inscription pour le service Internet ; elle ne doit être modifiée que si elle est requise par votre Fournisseur d'Accès Internet. Si ce dernier a utilisé l'adresse MAC d'une carte Ethernet comme identificateur lors de la configuration initiale de votre compte de connexion haut débit, connectez uniquement l'ordinateur comportant l'adresse MAC enregistrée au routeur, puis cliquez sur le bouton [Clone MAC Address] (Cloner l'adresse MAC). Cela aura pour effet de remplacer l'adresse IP MAC actuelle du routeur par celle de la carte Ethernet déjà enregistrée.

Configuration du routeur Barricade™ g sans fil

Si vous ne savez pas avec certitude quel ordinateur a été configuré à l'origine par le technicien haut débit, contactez votre Fournisseur d'Accès Internet et demandez-lui d'enregistrer une nouvelle adresse MAC pour votre compte. Enregistrez l'adresse MAC par défaut du routeur.

PPPoE (Point-to-Point Over Ethernet)



The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with options like System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'PPPoE' and contains the following text: 'Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.' Below this text is a form titled 'Use PPPoE Authentication' with the following fields: 'User Name', 'Password', 'Please retype your password', 'Service Name', 'MTU' (with a value of 1454 and a range of 1440 to 1492), 'Maximum Idle Time' (with a value of 10), and a checked 'Auto-reconnect' checkbox. At the bottom right of the form are buttons for 'HELP', 'APPLY', and 'CANCEL'.

Entrez le nom d'utilisateur PPPoE et le mot de passe attribués par votre Fournisseur d'Accès Internet. Le nom de service est généralement facultatif ; cependant, il peut être requis par certains fournisseurs.

La zone MTU (Maximum Transmission Unit) sert à définir la taille maximale des paquets de données. Conservez la valeur par défaut (1454) à moins d'avoir une raison particulière de la modifier.

Entrez la durée maximale d'inactivité (en minutes) dans la zone [Maximum Idle Time]. Cette durée correspond à l'intervalle de temps maximal pendant lequel la connexion à Internet doit être maintenue en période d'inactivité. Si le temps d'inactivité de la connexion dépasse la valeur attribuée à la zone [Maximum Idle Time], la connexion est interrompue. (Par défaut : 10 minutes)

Activez l'option [Auto-reconnect] (Reconnexion automatique) afin que la connexion soit automatiquement rétablie dès que vous tentez de nouveau d'accéder à Internet.

Remarque : si vous ne bénéficiez pas d'un tarif forfaitaire, sachez que l'attribution de la valeur 0 au paramètre [Maximum Idle Time] (Durée maximale d'inactivité) et/ou l'activation de l'option [Auto-Reconnect] (Reconnexion automatique) peut augmenter le montant de votre facture téléphonique.

Protocole PPTP (Point-to-Point Tunneling Protocol)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under WAN, the following options are listed: Dynamic IP, PPPoE, PPTP (highlighted in yellow), Static IP, BigPond, and DNS. The main content area is titled 'PPTP' and includes a descriptive text: 'Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.' Below this is a configuration form with the following fields: IP Address (0 0 0 0), Subnet Mask (0 0 0 0), Default Gateway (0 0 0 0), User ID (text input), Password (text input), PPTP Gateway (0 0 0 0), and Idle Time Out (10 (min)). A red asterisk note at the bottom states: '* If you have an ISP that charges by the time, change your idle time out value to 1 minute.' At the bottom right, there are three buttons: HELP, APPLY, and CANCEL.

Configuration du routeur Barricade™ g sans fil

Le protocole PPTP (Point-to-Point Tunneling Protocol) peut être utilisé pour relier différents réseaux physiques en utilisant Internet comme intermédiaire. L'utilisation de l'écran ci-dessus permet aux ordinateurs clients d'établir une session PPTP normale et simplifie la configuration du client PPTP sur chacune de ces machines.

Entrez l'adresse IP, le masque de sous-réseau et l'adresse IP de passerelle par défaut qui vous ont été attribués (ces informations sont généralement fournies par votre FAI), puis l'identificateur d'utilisateur PPTP, le mot de passe et l'adresse IP de la passerelle PPTP.

Entrez la durée maximale d'inactivité (en minutes) dans la zone [Maximum Idle Time] (Durée maximale d'inactivité). Cette durée correspond à l'intervalle de temps maximal pendant lequel la connexion PPTP doit être maintenue en période d'inactivité. Si le temps d'inactivité de la connexion dépasse la valeur attribuée à la zone [Maximum Idle Time], la connexion est interrompue. (Par défaut : 10 minutes)

Remarque : si vous ne bénéficiez pas d'un tarif forfaitaire, sachez que l'attribution de la valeur 0 au paramètre [Maximum Idle Time] (Durée maximale d'inactivité) et/ou l'activation de l'option [Auto-Reconnect] (Reconnexion automatique) peut augmenter le montant de votre facture téléphonique.

Static IP Address (Adresse IP statique)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP (highlighted), BigPond, DNS, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Static IP" and contains the following text: "If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided." and "Has your Service Provider given you an IP address and Gateway address?". Below this text are three input fields: "IP address assigned by your Service Provider", "Subnet Mask", and "Service Provider Gateway Address". Each field is a four-digit box with a dropdown arrow. At the bottom right of the main area are three buttons: HELP, APPLY, and CANCEL.

Si votre Fournisseur d'Accès Internet a attribué une adresse IP statique, entrez cette adresse et le masque de sous-réseau du routeur, puis entrez l'adresse de passerelle de votre Fournisseur d'Accès Internet.

Il se peut que vous ayez besoin d'une adresse statique si vous souhaitez fournir des services Internet, tels qu'un serveur Web ou un serveur FTP.

Configuration du routeur Barricade™ g sans fil

BigPond



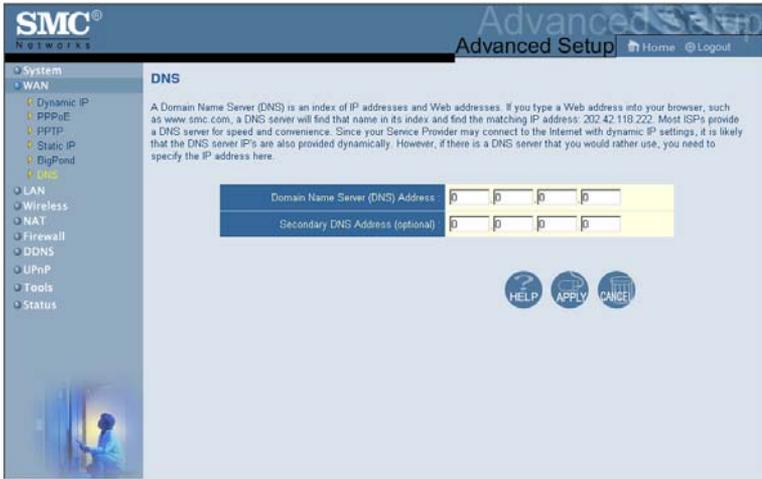
The screenshot shows the SMC Advanced Setup web interface. The top navigation bar includes the SMC logo, the text "Advanced Setup", and links for "Home" and "Logout". A left sidebar menu lists various configuration categories: System, WAN (with sub-items: Dynamic IP, PPPoE, PPTP, Static IP, BigPond), DNS, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "BigPond" and contains the following text: "In this section you can configure the built-in client for the BigPond Internet service available in Australia." Below this text is a form titled "BigPond Authentication Client" with the following fields:

BigPond Authentication Client	
User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text" value="login-server"/>

At the bottom right of the form area, there are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

BigPond est un Fournisseur d'Accès Internet australien qui utilise un système basé sur les pulsations pour maintenir les connexions Internet. Pour configurer le client intégré, indiquez vos nom d'utilisateur, mot de passe et nom de service afin de pouvoir vous connecter. Dans la zone [Authentication Service Name] (Nom de service d'authentification) conservez la mention « login-server » (serveur de connexion) pour autoriser tous les types de configuration.

DNS



Les serveurs DNS mettent en correspondance des adresses IP numériques avec les noms de domaine équivalents (par exemple, www.smc.com). Votre Fournisseur d'Accès Internet doit indiquer l'adresse IP d'un ou de plusieurs serveurs DNS. Entrez ces adresses dans cet écran.

LAN (Réseau local)

The screenshot shows the 'Advanced Setup' page for LAN settings. On the left is a navigation menu with options: System, WAN, LAN (selected), Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'LAN Settings' and includes a sub-section 'LAN IP'. Below this, there are three rows of input fields: 'IP Address' (192, 168, 2, 1), 'IP Subnet Mask' (255, 255, 255, 0), and 'DHCP Server' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected). A 'Lease Time' dropdown menu is set to 'One Week'. Below that is the 'IP Address Pool' section with 'Start IP' (192, 168, 2, 100), 'End IP' (192, 168, 2, 199), and a 'Domain Name' text box. At the top right of the interface are links for 'Home' and 'Logout'.

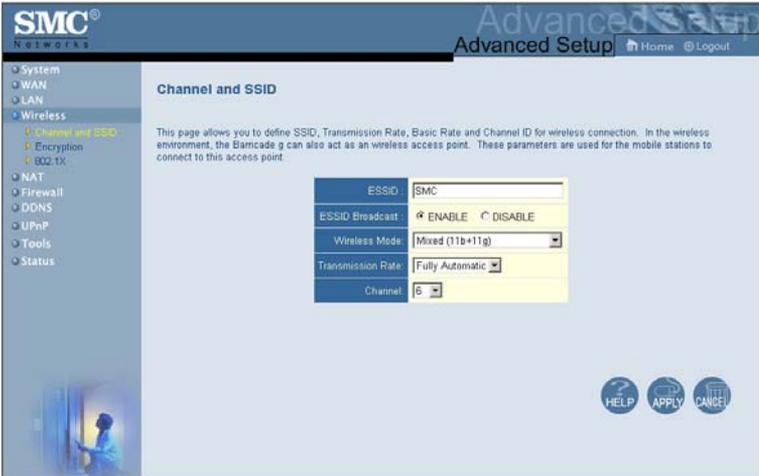
- [LAN IP] (Adresse IP du réseau local)
Utilisez le menu [LAN] (Réseau local) pour configurer l'adresse IP de réseau local associée au routeur et pour activer le serveur DHCP pour l'attribution dynamique des adresses aux postes clients.
- Si nécessaire, définissez la durée de bail dans la zone [Lease Time]. Dans le cas d'un réseau domestique, vous pouvez attribuer la valeur [Forever] (Toujours) à ce paramètre. Cela signifie que le bail d'adresse IP n'est pas limité dans le temps.
- [IP Address Pool] (Pool d'adresses IP)
L'utilisateur peut spécifier une adresse IP de début dynamique, telle que 192.168.2.100 (valeur par défaut). Une fois cette adresse définie, le pool d'adresses IP dynamiques sera constitué d'adresses IP allant de 192.168.2.100 à 192.168.2.199.
Les adresses IP allant de 192.168.2.2 à 192.168.2.99 et de 192.168.2.200 à 192.168.2.254 seront disponibles en tant qu'adresses IP statiques.

Assurez-vous de ne pas inclure l'adresse du routeur dans le pool d'adresses de postes clients. Veillez également à configurer vos postes clients aux fins d'attribution d'adresses IP dynamiques.

Wireless (Sans fil)

Pour configurer le routeur comme point d'accès sans fil pour les clients sans fil (fixes ou itinérants), il vous suffit de définir le canal radio, l'identificateur SSID et les options de cryptage.

Channel and SSID (Canal et SSID)



The screenshot shows the 'Channel and SSID' configuration page in the SMC Networks Advanced Setup interface. The page title is 'Channel and SSID'. Below the title, there is a descriptive paragraph: 'This page allows you to define SSID, Transmission Rate, Basic Rate and Channel ID for wireless connection. In the wireless environment, the Barracade g can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.' The configuration fields are as follows:

ESSID	SMC
ESSID Broadcast	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode	Mixed (11b+11g)
Transmission Rate	Fully Automatic
Channel	6

At the bottom right of the page, there are three buttons: HELP, APPLY, and CANCEL.

Vous devez spécifier un canal radio et un SSID à utiliser par le routeur et tous vos clients sans fil. Assurez-vous de configurer tous vos clients aux mêmes valeurs.

[ESSID] : l'identificateur Service Set ID. Il doit avoir la même valeur que pour les autres périphériques sans fil de votre réseau.

Configuration du routeur Barricade™ g sans fil

[SSID Broadcast] : Diffusion du SSID sur le réseau sans fil pour faciliter les connexions aux ordinateurs clients.

Pour des raisons de sécurité, il est conseillé de désactiver cette fonction. (Par défaut : activé)

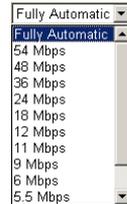
Remarque : le SSID respecte la distinction entre les majuscules et les minuscules et peut comporter au maximum 32 caractères alphanumériques.

[Wireless Mode] (Mode sans fil) : sélectionnez le mode de communication du routeur.

La valeur par défaut est Mixte (11b+11g).



[Transmission Rate] (Vitesse de transmission) : définit la vitesse de transmission des données à partir du routeur. Plus cette vitesse est faible, plus la distance de transmission est grande. La valeur par défaut est [Fully Automatic] (Entièrement automatique).



[Channel] (Canal) : le canal radio au travers duquel le routeur communique avec les ordinateurs de son BSS. La valeur par défaut est 6.



Remarque : les canaux disponibles sont limités par les réglementations locales.

Encryption (Cryptage)



Pour transmettre des données sensibles par l'intermédiaire de canaux sans fil, il est recommandé d'activer le cryptage WEP (Wired Equivalent Privacy). Ce cryptage vous impose d'utiliser le même ensemble de clés de cryptage et de décryptage pour le routeur et tous vos clients sans fil. Vous pouvez choisir entre un cryptage standard sur 64 bits et un cryptage plus robuste sur 128 bits.



Configuration du routeur Barricade™ g sans fil

Vous pouvez générer automatiquement les clés de cryptage ou les saisir manuellement. Pour la sécurité 64 bits automatique, entrez une phrase mot de passe et cliquez sur [Generate] (Générer). Quatre clés seront générées (comme indiqué ci-dessous). Choisissez une clé dans la liste déroulante ou acceptez la clé par défaut. La sécurité 128 bits automatique génère une clé unique.

The screenshot shows the 'Advanced Setup' page for WEP encryption. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless (selected), NAT, Firewall, DDNS, UPnP, Tools, and Status. Under 'Wireless', the sub-menu items are 'Channel and SSID', 'Encryption' (selected), and 'WDS'. The main content area is titled 'Encryption' and includes a description: 'Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Barricade g and wireless client devices to use encryption. Do you want to use encryption?'. A 'WEP Mode' dropdown menu is set to '64-bit WEP'. Below this, a text box for a 'Passphrase' is followed by a 'Generate' button. A table for keys is shown with four rows labeled 'Key 1' through 'Key 4'. Each row has five input fields for key characters and a 'Default Key' dropdown menu. A 'Clear All Keys' button is located below the table. At the bottom right, there are three circular buttons: 'HELP', 'APPLY', and 'CANCEL'.

SMC® Networks Advanced Setup Home Logout

Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Barricade g and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode: 64-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase:	<input type="text"/>	Generate
Key 1:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	Default Key: 1
Key 2:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	
Key 3:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	
Key 4:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	

Clear All Keys

HELP APPLY CANCEL

The screenshot shows the 'Advanced Setup' page for SMC Networks. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, Wireless (selected), Channel and SSID, Encryption (selected), 802.1X, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Encryption' and includes the following text: 'Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Baricade g and wireless client devices to use encryption. Do you want to use encryption?'. Below this text is a 'WEP Mode' dropdown menu set to '128-bit WEP'. A note states: 'Enter a passphrase and click the Generate button, or manually enter a key into the table.' The interface features a 'Passphrase' input field with a 'Generate' button, and a 'Key' section with a table for manual entry. The table has three rows and five columns, each containing a masked key field. A 'Clear Key' button is located below the table. At the bottom right, there are three circular buttons: 'HELP', 'APPLY', and 'CANCEL'.

Si vous utilisez le cryptage, configurez pour le routeur les mêmes clés que celles utilisées sur chacun de vos clients sans fil. Notez que le cryptage WEP protège les données échangées entre les nœuds sans fil mais ne protège pas les transmissions effectuées sur votre réseau filaire ou sur Internet.

Configuration du routeur Barricade™ g sans fil

802.1X

The screenshot shows the 'Advanced Setup' page for '802.1X' configuration on an SMC router. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless (selected), Channel and SSID, Encryption, 802.1X, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled '802.1X' and includes a description: 'This page allows you to set the 802.1X, a method for performing authentication to wireless connection. These parameters are used for this access point to connect to the Authentication Server.' Below this, there are two sections: 'General Parameters' and 'RADIUS Server Parameters'. The 'General Parameters' section includes: 'Enable 802.1X' (radio buttons for Yes and No, with No selected), 'Session Idle Timeout' (300 seconds), 'Re-Authentication Period' (3600 seconds), 'Quiet Period' (60 seconds), and 'Server Type' (RADIUS dropdown). The 'RADIUS Server Parameters' section includes: 'Server IP' (192.168.1.1), 'Server Port' (1812), 'Secret Key' (empty), and 'NAS ID' (empty).

Les accès pour les tâches d'administration sont contrôlés dans la base de données d'authentification stockée sur le routeur. Si un serveur RADIUS d'authentification est utilisé, vous devez spécifier la séquence d'authentification et les paramètres correspondants pour le protocole d'authentification à distance.

- Paramètres généraux

Zone	Valeur par défaut	Description
Enable 802.1X (Activer 802.1x)	Yes (Oui)	Active l'utilisation du contrôle de sécurité 802.1x.
Session Idle Timeout (Délai d'inactivité de la session)	300 (durée exprimée en secondes)	Cette durée correspond à l'intervalle de temps maximal pendant lequel la connexion doit être maintenue en période d'inactivité.
Re-Authentication Period (Délai de réauthentification)	3600 (durée exprimée en secondes)	Cette durée correspond à l'intervalle de temps maximal pendant lequel le serveur RADIUS réaffecte dynamiquement une clé de session à une station cliente connectée.
Quiet Period (Délai d'attente)	60 (durée exprimée en secondes)	Cette durée correspond à l'intervalle de temps maximal pendant lequel le routeur attend entre chaque échec de l'authentification.
Server Type (Type de serveur)	RADIUS	Permet de sélectionner le type de serveur d'authentification.

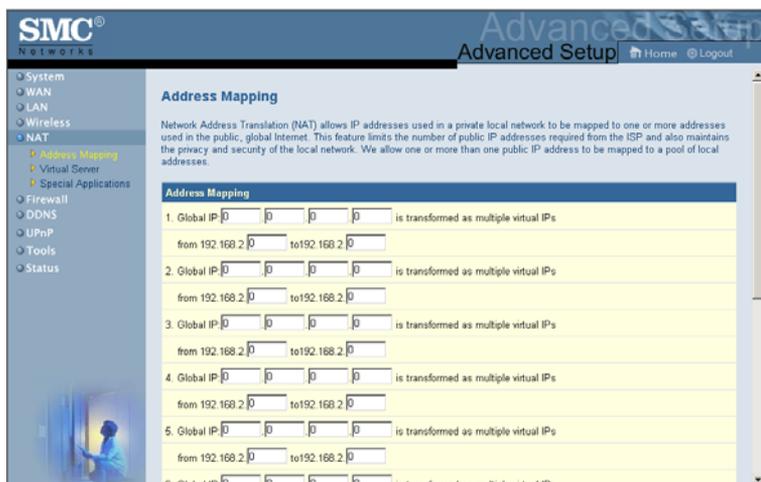
- Paramètres du serveur RADIUS

Zone	Valeur par défaut	Description
Server IP (Adresse IP du serveur)	192.168.1.1	Adresse IP du serveur RADIUS
Server Port (Port du serveur)	1812	Le Port UDP 1812 est utilisé pour les messages d'authentification du serveur RADIUS.
Secret Key (Clé secrète)	(NIL)	Permet de définir une chaîne de texte à la fois sur le client et sur le serveur RADIUS pour sécuriser le trafic RADIUS.
NAS-ID (ID NAS)	(NIL)	Permet de définir l'identificateur de requête sur le serveur d'accès réseau (NAS, Network Access Server).

Translation d'adresses réseau (NAT)

Cette section vous permet de configurer le mappage d'adresses, le serveur virtuel et les fonctionnalités d'applications spéciales permettant de contrôler les ouvertures de ports sur le firewall du routeur. Elle peut être utilisée pour supporter plusieurs applications basées sur Internet telles que les réseaux privés virtuels.

Address Mapping (Mappage d'adresses)



Cette fonctionnalité permet le partage d'une ou plusieurs adresses IP publiques entre plusieurs utilisateurs internes. Entrez l'adresse IP publique à partager dans la zone [Global IP] (Adresse IP globale). Entrez la plage des adresses IP internes qui se partageront l'adresse IP globale.

Virtual Server (Serveur virtuel)

Virtual Server

You can configure the Baramcade g as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Baramcade g redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- Port Ranges: ex. 100-150
- Multiple Ports: ex. 25,110,80
- Combination: ex. 25-100,80

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	Add	Clean
1	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
2	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
3	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
4	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
5	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
6	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
7	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean
8	192.168.2.	TCP			<input type="checkbox"/>	Add	Clean

Si vous configurez le routeur en tant que serveur virtuel, les utilisateurs distants accédant aux services Web ou FTP de votre site local via des adresses IP publiques pourront être automatiquement redirigés vers des serveurs locaux configurés à l'aide d'adresses IP privées. En d'autres termes, en fonction du service demandé (numéro de port TCP/UDP), le routeur redirigera la demande de service externe vers le serveur approprié (situé à une autre adresse IP interne).

Par exemple, si vous attribuez au paramètre Type/Public Port la valeur TCP/80 (HTTP ou Web) et au paramètre Private IP/Port la valeur 192.168.2.2/80, toutes les requêtes HTTP provenant d'utilisateurs externes seront transférées vers l'adresse 192.168.2.2 sur le port 80. Par conséquent, en entrant simplement l'adresse IP attribuée par le Fournisseur d'Accès Internet, les utilisateurs Internet peuvent accéder au service dont ils ont besoin à l'adresse locale vers laquelle vous les redirigez.

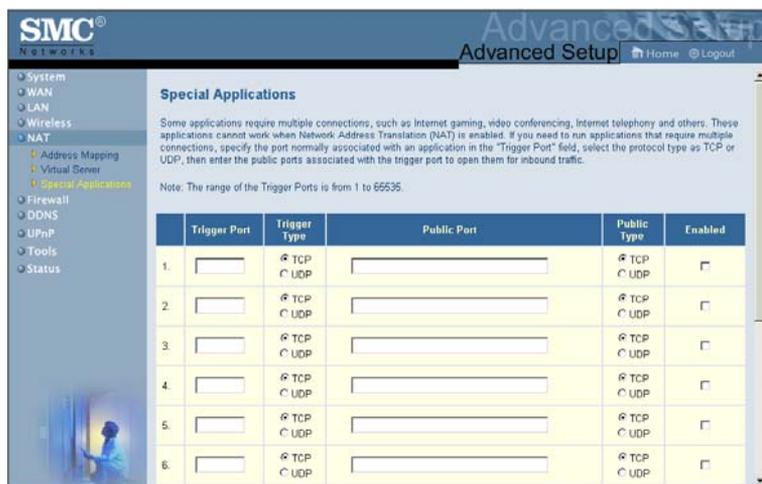
Configuration du routeur Barricade™ g sans fil

Voici quelques-uns des ports de service TCP les plus courants :

HTTP : 80, FTP : 21, Telnet : 23 et POP3 : 110.

Special Applications (Applications spéciales)

Certaines applications, telles que les jeux Internet ainsi que les applications de téléconférence et de téléphonie Internet, requièrent plusieurs connexions. Ces applications ne peuvent pas fonctionner lorsque la fonction de translation d'adresses réseau (NAT) est activée. Pour lancer des applications qui requièrent plusieurs connexions, utilisez l'écran ci-après afin d'indiquer les ports publics supplémentaires à ouvrir pour chaque application.



The screenshot shows the SMC Networks Advanced Setup interface. The sidebar menu includes System, WAN, LAN, Wireless, NAT, Address Mapping, Virtual Server, Special Applications (highlighted), Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Special Applications" and contains a note: "Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the 'Trigger Port' field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic." Below the note is a table with 6 rows and 5 columns: Trigger Port, Trigger Type, Public Port, Public Type, and Enabled.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

Dans la zone [Trigger Port] (Port de déclenchement), spécifiez le numéro de port public normalement associé à une application. Définissez le type de protocole TCP ou UDP, puis entrez les ports nécessaires à l'application. Les ports peuvent être au format 7, 11, 57, sous forme d'intervalle, par exemple 72-96, ou une combinaison des deux, comme 7, 11, 57, 72-96.

Les applications courantes nécessitant plusieurs ports sont énumérées dans la zone [Popular Applications] (applications courantes). Dans cette liste déroulante, sélectionnez l'application, puis sélectionnez un numéro de ligne pour y copier ces données.

Remarque : si vous sélectionnez une ligne qui contient déjà des données, les valeurs en cours sont écrasées.

Pour obtenir la liste complète des ports et des services qui s'exécutent sur ces ports, consultez www.iana.org/assignments/port-numbers.

Firewall

Le firewall du routeur permet le contrôle d'accès des ordinateurs clients connectés et bloque les attaques extérieures les plus courantes : usurpation d'adresse IP (IP Spoofing), Land Attack, Ping of Death, IP de taille nulle (IP with zero length), Smurf Attack, bouclage de port UDP (UDP port loopback), Snork Attack, scannage nul TCP (TCP null scan) et inondation SYN TCP (TCP SYN flooding). Le firewall n'a que peu d'impact sur les performances du système ; il est donc conseillé de le laisser activé, afin de protéger les utilisateurs du réseau.

Access Control (Contrôle d'accès)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall (expanded), DDNS, UPnP, Tools, and Status. Under Firewall, the following options are listed: Access Control (selected), MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, and DMZ. The main content area is titled "Access Control" and includes a description: "Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering." Below the description, there are two main sections: "Enable Filtering Function" with radio buttons for "Yes" (selected) and "No", and "Normal Filtering Table (up to 10 computers)". The table below contains one entry:

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Normal	192.168.2.101 - 125	WWW, WWW with URL Blocking, FTP, AIM	Always Blocking	Edit Delete

Below the table is a link labeled "Add PC". At the bottom right of the interface are three circular buttons: "HELP", "APPLY", and "CANCEL".

Cette option vous permet d'attribuer aux ordinateurs clients différents droits d'accès basés sur des adresses IP.

Remarque : cliquez sur [Add PC] (Ajouter un ordinateur), puis définissez les paramètres associés aux services d'ordinateur client, comme indiqué sur l'écran ci-après.

The screenshot shows the 'Access Control Add PC' configuration page in the SMC Advanced Setup interface. The page title is 'Access Control Add PC' and it includes a descriptive paragraph: 'This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.'

Configuration fields include:

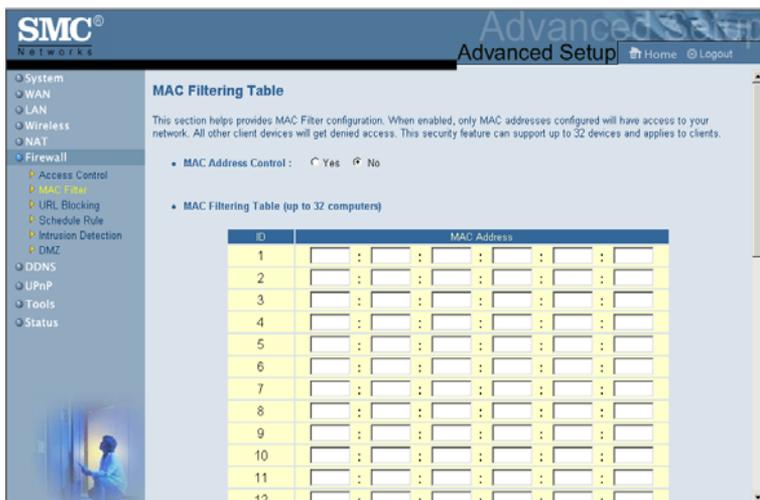
- Client PC Description: [Text Input]
- Client PC IP Address: 192.168.2. [IP Input] - [IP Input]
- Client PC Service: [List of services with checkboxes for blocking]

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Teinat Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN/PPTP	TCP Port 1723	<input type="checkbox"/>
VPN/L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

Below the table is a 'User Define Service' section with fields for Protocol (TCP/UDP), Port Range, and Scheduling Rule (Ref. Schedule Rule Page): Always Blocking.

Buttons: OK, Cancel

MAC Filtering Table (Table de filtrage des adresses MAC)



The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall (selected), DMZ, DDNS, UPnP, Tools, and Status. The Firewall section is expanded to show sub-items: Access Control, MAC Filter (selected), URL Blocking, Schedule Rule, and Intrusion Detection.

The main content area is titled "MAC Filtering Table". It includes a description: "This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients." Below the description are two configuration options:

- MAC Address Control : Yes No
- MAC Filtering Table (up to 32 computers)

The MAC Filtering Table is a table with 12 rows and 13 columns. The first column is labeled "ID" and contains numbers 1 through 12. The remaining 12 columns are grouped under the header "MAC Address". Each cell in the MAC Address columns contains a small input field with a colon separator, representing the hexadecimal MAC address format (XX:XX:XX:XX:XX:XX).

ID	MAC Address												
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													

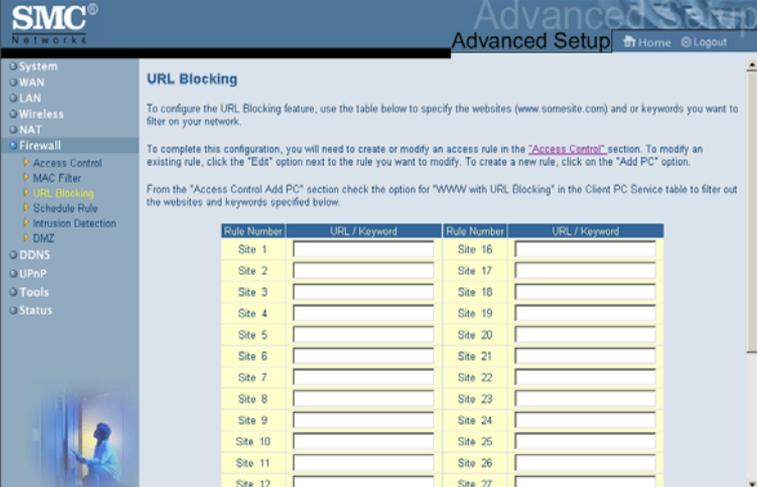
La fonctionnalité de filtrage d'adresses du routeur vous permet de contrôler l'accès à votre réseau de 32 clients au maximum, sur la base de l'adresse MAC (Media Access Control) de la machine cliente. Cet identificateur est unique pour chaque carte réseau. Si l'adresse MAC apparaît dans le tableau, la machine cliente correspondante aura accès au réseau.

URL Blocking (Blocage d'URL)

Pour configurer la fonctionnalité de blocage d'URL, utilisez le tableau ci-dessous afin de spécifier les sites Web (www.site.com) et/ou les mots clés que vous souhaitez filtrer sur votre réseau.

Pour terminer cette configuration, vous aurez besoin de modifier ou de créer une règle d'accès, voir la section « Access Control (Contrôle d'accès) » à la page 68. Pour modifier une règle existante, cliquez sur l'option [Edit] (Modifier) en regard de la règle à modifier. Pour créer une nouvelle règle, cliquez sur l'option [Add PC] (Ajouter un ordinateur).

Dans la section [Add PC] de [Access Control] (Contrôle d'accès), activez l'option [WWW with URL Blocking] (WWW avec blocage d'URL) dans le tableau [Client PC Service] (Service PC client) afin d'éliminer les sites Web et les mots clés spécifiés dessous.



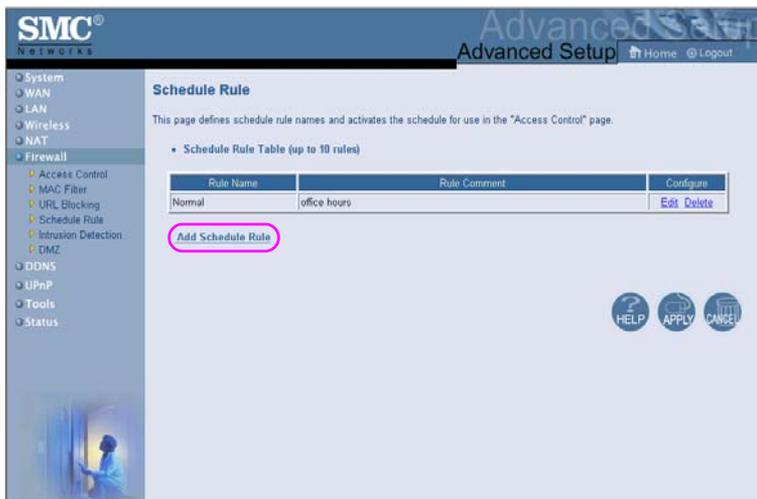
The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with options like System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'URL Blocking' and contains instructions on how to configure this feature. Below the instructions is a table for specifying sites and keywords to be blocked.

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	

Utilisez l'écran ci-dessus pour bloquer l'accès aux sites ou aux URL Web contenant le mot clé spécifié dans le tableau.

Schedule Rule (Règle de planification)

La fonctionnalité de règle de planification vous permet de configurer des règles particulières basées sur la date et sur l'heure. Ces règles peuvent être ensuite utilisées pour configurer des règles de contrôle d'accès plus spécifiques.



Active le contrôle d'accès Internet basé sur les horaires.

1. Cliquez sur [Add Schedule Rule] (Ajouter une règle de planification).
2. Définissez les paramètres associés à la règle de planification (comme indiqué sur l'écran ci-après).
3. Cliquez sur [OK] puis sur le bouton [APPLY] (Appliquer) pour enregistrer vos paramètres.

SMC Networks Advanced Setup

Home Logout

System
WAN
LAN
Wireless
NAT
Firewall
Access Control
MAC Filter
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
DDNS
UPnP
Tools
Status

Edit Schedule Rule

Name:

Comment:

Activate Time Period

Week Day	Start Time (h:mm)	End Time (h:mm)
Every Day	00 : 00	00 : 00
Sunday	00 : 00	00 : 00
Monday	08 : 00	18 : 00
Tuesday	08 : 00	18 : 00
Wednesday	00 : 00	18 : 00
Thursday	00 : 00	18 : 00
Friday	00 : 00	18 : 00
Saturday	00 : 00	00 : 00

OK Cancel

Intrusion Detection (Détection d'intrusion)

SMC Networks Advanced Setup

Home Logout

System
WAN
LAN
Wireless
NAT
Firewall
Access Control
MAC Filter
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
DDNS
UPnP
Tools
Status

Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Barricade g will support full operation as initiated from the local LAN.

The Barricade g firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- Intrusion Detection Feature**

SPI and Anti-DoS firewall protection	<input checked="" type="checkbox"/>
RIP detect	<input checked="" type="checkbox"/>
Discard Ping To WAN	<input type="checkbox"/>
- Stateful Packet Inspection**

Packet Fragmentation	<input checked="" type="checkbox"/>
TCP Connection	<input checked="" type="checkbox"/>
UDP Session	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>

Configuration du routeur Barricade™ g sans fil

The screenshot shows the 'Advanced Setup' page for SMC Networks. The left sidebar contains a navigation menu with 'Firewall' selected. The main content area is titled 'Advanced Setup' and includes a 'Home' link and a 'Logout' button. The configuration is divided into several sections:

- When hackers attempt to enter your network, we can alert you by e-mail:** Fields for 'Your E-mail Address', 'SMTP Server Address', 'POP3 Server Address', 'User name', and 'Password'.
- Connection Policy:** Fields for 'Fragmentation half-open wait' (10 sec), 'TCP SYN wait' (30 sec), 'TCP FIN wait' (5 sec), 'TCP connection idle timeout' (3600 sec), 'UDP session idle timeout' (30 sec), and 'H.323 data channel idle timeout' (180 sec).
- DoS Detect Criteria:** Fields for 'Total incomplete TCP/UDP sessions HIGH' (300 session), 'Total incomplete TCP/UDP sessions LOW' (250 session), 'Incomplete TCP/UDP sessions (per min) HIGH' (250 session), 'Incomplete TCP/UDP sessions (per min) LOW' (200 session), 'Maximum incomplete TCP/UDP sessions number from same host' (10), 'Incomplete TCP/UDP sessions detect sensitive time period' (300 msec), 'Maximum half-open fragmentation packet number from same host' (30), 'Half-open fragmentation detect sensitive time period' (10000 msec), and 'Flooding cracker block time' (300 sec).

- **[SPI and Anti-DoS firewall protection] (Protection SPI et anti-refus de service par firewall) (par défaut : activé)**
La fonction de détection d'intrusion du routeur limite l'accès du trafic entrant via le port WAN. Lorsque la fonction SPI est activée, tous les paquets entrants sont bloqués, à l'exception des types pour lesquels l'option Stateful Packet Inspection est activée.
- **[RIP Defect] (Défaut RIP) (par défaut : activé)**
Si le routeur ne répond pas à un paquet de requête RIP, celui-ci reste dans la file d'entrée et n'est pas libéré. L'accumulation des paquets peut provoquer le remplissage de la file d'entrée et causer ainsi des problèmes importants pour tous les protocoles. L'activation de cette fonction empêche l'accumulation des paquets.
- **[Discard Ping from WAN] (Rejeter les Ping à partir du réseau étendu) (par défaut : désactivé)**
Empêche l'acheminement vers le réseau d'un PING sur le port WAN du routeur.

- **[Stateful Packet Inspection] (Inspection des paquets avec état)**

Cette inspection de paquets est dite [stateful] (avec état) car elle examine le contenu du paquet pour déterminer l'état de la communication.

En d'autres termes, elle vérifie que l'ordinateur de destination indiqué a préalablement demandé la communication en cours. Cela permet de s'assurer que toutes les communications sont déclenchées par l'ordinateur destinataire et qu'elles n'ont lieu qu'avec des sources connues et approuvées à partir d'interactions précédentes. Non seulement les firewalls d'inspection avec état font preuve d'une plus grande rigueur dans leur inspection des paquets, mais ils ferment également les ports jusqu'à ce qu'une connexion avec le port spécifique soit demandée.

Lorsque des types de trafic particuliers sont contrôlés, seul le type de trafic déclenché à partir du réseau local interne est autorisé. Par exemple, si l'utilisateur sélectionne uniquement l'option [FTP Service] (Service FTP) dans l'écran [Stateful Packet Inspection], tout le trafic entrant est bloqué, à l'exception des connexions FTP établies à partir du réseau local.

[Stateful Packet Inspection] (Inspection des paquets avec état) vous permet de sélectionner différents types d'applications faisant appel à des numéros de ports dynamiques. Si vous souhaitez utiliser la fonction SPI pour bloquer des paquets, cliquez sur la case d'option [Yes] (Oui) dans la zone [Enable SPI and Anti-DoS firewall protection] (Activer la protection SPI et anti-refus de service par firewall), puis sélectionnez le type d'inspection souhaité, tel que la fragmentation des paquets, la connexion TCP, la session UDP, le service FTP, le service H.323 ou le service TFTP.

Configuration du routeur Barricade™ g sans fil

- **[When hackers attempt to enter your network, we can alert you by e-mail] (Lorsque des pirates tentent de s'introduire dans votre réseau, nous pouvons vous avertir par courrier électronique)**
Entrez votre adresse pour être averti des intrusions de pirates. Spécifiez vos serveurs SMTP et POP3, votre nom d'utilisateur et votre mot de passe.
- **[Connection Policy] (Stratégie de connexion)**
Entrez les valeurs appropriées pour les sessions TCP/UDP comme décrit dans le tableau suivant.

Paramètre	Valeur par défaut	Description
Fragmentation half-open wait (Attente de fragmentation d'ouverture)	10 sec	Indique le nombre de secondes pendant lesquelles une structure d'état de paquet reste active. Lorsque ce délai expire, le routeur abandonne le paquet non assemblé, en libérant cette structure pour qu'elle puisse être utilisée par un autre paquet.
TCP SYN wait (Attente de synchronisation TCP)	30 sec	Définit le temps pendant lequel le logiciel attend une session TCP à synchroniser avant de l'abandonner.
TCP FIN wait (Attente TCP FIN)	5 sec	Indique le temps pendant lequel une session TCP est maintenue après la détection d'un paquet FIN par le firewall.
TCP connection idle timeout (Délai d'inactivité de connexion TCP)	3600 secondes (1 heure)	Temps pendant lequel une session TCP est maintenue en l'absence d'activité.
UDP session idle timeout (Délai d'inactivité de session UDP)	30 sec	Temps pendant lequel une session UDP est maintenue en l'absence d'activité.
H.323 data channel idle timeout (Délai d'inactivité de canal de données H.323)	180 sec	Temps pendant lequel une session H.323 est maintenue en l'absence d'activité.

Critères de refus de service et d'analyse de port

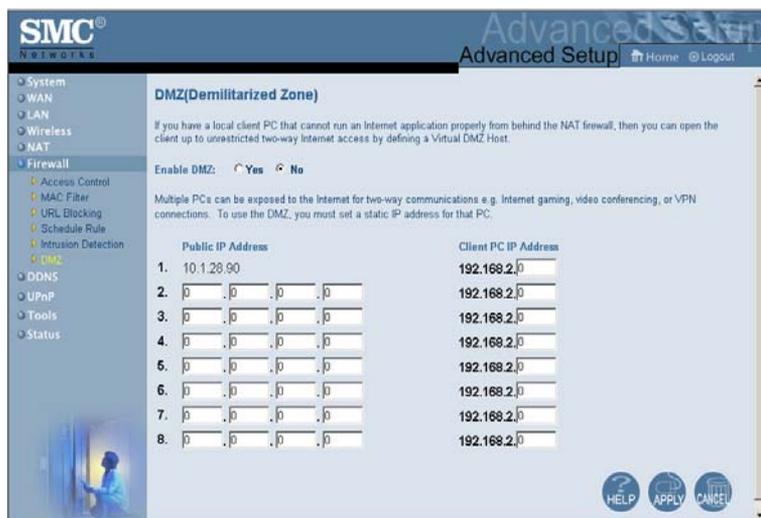
Définissez les critères de refus de service et d'analyse de port dans les zones prévues à cet effet (comme indiqué ci-dessous).

Paramètre	Valeur par défaut	Description
Total incomplete TCP/UDP sessions HIGH (Nombre total de sessions TCP/UDP incomplètes SEUIL HAUT)	300 sessions	Définit le nombre de sessions nouvellement non établies qui conduira le logiciel à <i>commencer</i> à supprimer les sessions à moitié ouvertes.
Total incomplete TCP/UDP sessions LOW (Nombre total de sessions TCP/UDP incomplètes SEUIL BAS)	250 sessions	Définit le nombre de sessions nouvellement non établies qui conduira le logiciel à <i>arrêter</i> de supprimer les sessions à moitié ouvertes.
Incomplete TCP/UDP sessions (per min.) HIGH (Sessions TCP/UDP incomplètes par minute SEUIL HAUT)	250 sessions	Nombre maximal de sessions TCP/UDP incomplètes autorisées par minute.
Incomplete TCP/UDP sessions (per min.) LOW (Sessions TCP/UDP incomplètes par minute SEUIL BAS)	200 sessions	Nombre minimal de sessions TCP/UDP incomplètes autorisées par minute. Spécifiez la valeur 0 si aucune valeur minimale n'est requise.
Maximum incomplete TCP/UDP sessions number from same host (Nombre maximal de sessions TCP/UDP incomplètes à partir du même hôte)	10 sessions	Nombre maximal de sessions TCP/UDP incomplètes à partir du même hôte.
Incomplete TCP/UDP sessions detect sensitive time period (Temps de détection des sessions TCP/UDP incomplètes)	300 msec	Temps nécessaire avant qu'une session TCP/UDP incomplète ne soit détectée comme telle.
Maximum half-open fragmentation packet number from same host (Nombre maximal de paquets de fragmentation à moitié ouverts à partir du même hôte)	30	Nombre maximal de paquets de fragmentation à moitié ouverts à partir du même hôte.
Half-open fragmentation detect sensitive time period (Temps de détection de fragmentation à moitié ouverte)	1 sec	Temps nécessaire avant qu'une session de fragmentation à moitié ouverte ne soit détectée comme telle.

Configuration du routeur Barricade™ g sans fil

Paramètre	Valeur par défaut	Description
Flooding cracker block time (Délai du craquement d'inondation)	300 sec	Délai entre la détection d'une attaque de type inondation et le blocage de cette attaque.

DMZ



The screenshot shows the 'DMZ(Demilitarized Zone)' configuration page in the SMC Networks Advanced Setup interface. The page includes a navigation menu on the left with options like System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'DMZ(Demilitarized Zone)' and contains the following text: 'If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.' Below this, there is a section 'Enable DMZ:' with radio buttons for 'Yes' and 'No', where 'No' is selected. A descriptive paragraph states: 'Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.' There are two columns of IP address input fields: 'Public IP Address' and 'Client PC IP Address'. The first row is pre-filled with '10.1.28.90' and '192.168.2.0'. The remaining seven rows are empty, each with a number from 2 to 8. At the bottom right, there are three circular buttons: 'HELP', 'APPLY', and 'CANCEL'.

Si votre poste client ne parvient pas à exécuter correctement une application Internet derrière le firewall, vous pouvez l'ouvrir à un accès Internet bidirectionnel illimité. Dans cet écran, entrez l'adresse IP d'un hôte DMZ. L'ajout d'un poste client à l'hôte DMZ (Demilitarized can be Zone, Zone démilitarisée) peut présenter de nombreux risques de sécurité pour le réseau local. Par conséquent, cette option ne doit être utilisée qu'en dernier recours.

Paramètres DDNS (DNS dynamique)

SMC[®] NETWORKS Advanced Setup Home Logout

DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

This DNS feature is powered by TZO.com. With a DDNS connection you can host your own web site, email server, FTP site and more at your own location even if you have a dynamic IP address. To sign-up for a free 30-day trial click [here](#)

Dynamic DNS: Enabled Disabled

TZO Configuration

Domain Name:

E-mail:

Key: [Get free 30-day trial key!](#)

Control Panel: [Click here to login to your TZO control panel!](#)

Server Configuration

Server IP:

Server Type:

Web Server: (HTTP)	Port 80 <input type="checkbox"/>	Port 8000 <input type="checkbox"/>
FTP Server:	Port 20 <input type="checkbox"/>	Port 21 <input type="checkbox"/>
Email Server: (POP3)	Port 110 <input type="checkbox"/>	(SMTP) Port 25 <input type="checkbox"/>

[Domain Name] (Nom de domaine)

Série de chaînes alphanumériques séparées par des points, qui constitue l'adresse de la connexion réseau du routeur et identifie le propriétaire de cette adresse.

La fonctionnalité DNS dynamique intégrée fournit aux utilisateurs sur Internet une méthode pour lier leurs noms de domaines à des ordinateurs ou des serveurs. DDNS permet à votre nom de domaine de suivre automatiquement votre adresse IP : vos enregistrements DNS changent ainsi lorsque votre adresse IP change.

Configuration du routeur Barricade™ g sans fil

Cette section est également dotée d'une section [Server Configuration] (Configuration du serveur) qui permet d'ouvrir automatiquement les options de port activées dans la section [Virtual Server] (Serveur virtuel). Entrez simplement l'adresse IP de votre serveur (par exemple, votre serveur Web), puis cliquez sur l'option de port [HTTP Port 80] afin que les utilisateurs puissent accéder à ce serveur à partir de la connexion WAN (Internet).

Cette fonctionnalité DNS est fournie par TZO.com. Avec une connexion DDNS, vous pouvez héberger votre propre site Web, un serveur de messagerie, un site FTP et bien plus encore, même si vous possédez une adresse IP dynamique. (Par défaut : désactivé.)

Paramétrage UPnP (Universal Plug and Play)

SMC®
Networks

Advanced Setup | Home | Logout

System
WAN
LAN
Wireless
NAT
Firewall
DDNS
UPnP
Tools
Status

UPnP[Universal Plug and Play] Setting

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity networking in addition to control and data transfer among networked devices in the home, office and everywhere in between.

UPnP: ON OFF

HELP APPLY CANCEL

Activez UPnP en cochant ON sur l'écran ci-dessus.

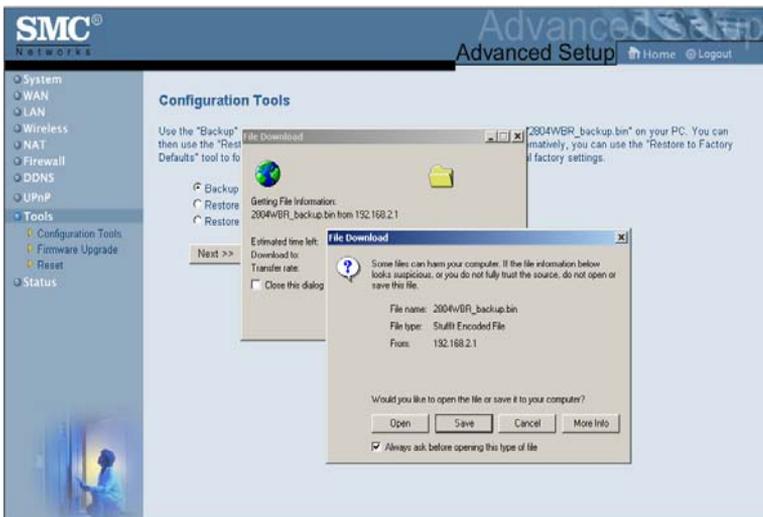
UPnP permet au périphérique d'effectuer automatiquement les opérations suivantes :

- se connecter dynamiquement à un réseau,
- obtenir une adresse IP,
- communiquer ses capacités et obtenir des informations sur la présence et les capacités des autres périphériques.
(Par défaut : OFF.)

Tools (Outils)

Utilisez le menu [Tools] (Outils) pour sauvegarder la configuration actuelle, restaurer une configuration précédemment enregistrée, restaurer les paramètres par défaut, mettre à jour le logiciel et réinitialiser le routeur.

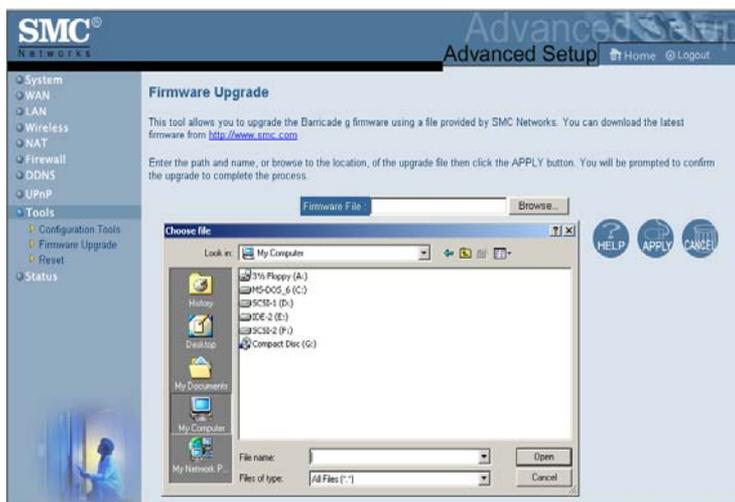
Tools - Configuration Tools (Outils - Outils de configuration)



Configuration du routeur Barricade™ g sans fil

- [Backup] (Sauvegarder)
Enregistre la configuration du routeur dans un fichier.
- [Restore] (Restaurer)
Restaure les paramètres à partir d'un fichier de configuration précédemment enregistré.
- [Restore to factory defaults] (Restaurer les paramètres par défaut)
Restaure les paramètres d'origine du routeur.

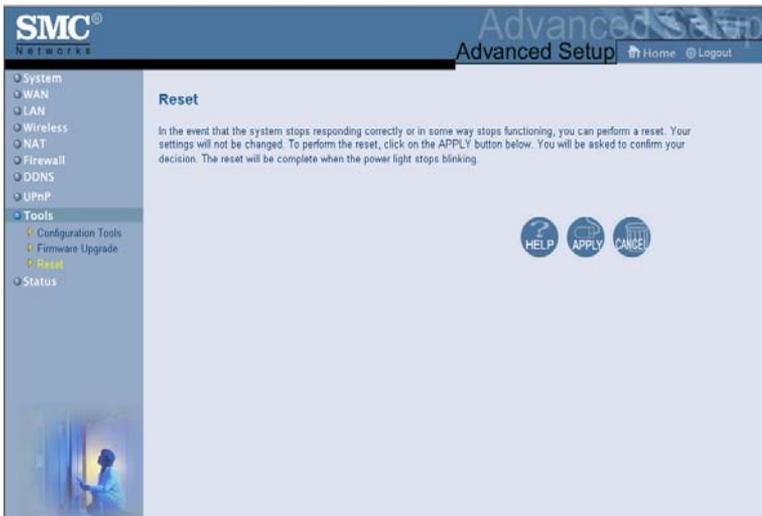
Tools - Firmware Upgrade (Outils - Mise à niveau du logiciel)



Utilisez cet écran pour mettre à jour la dernière version du logiciel ou de l'interface utilisateur. Téléchargez le fichier de mise à niveau à partir du site Web de SMC (www.smc.com ou www.smc-europe.com) et enregistrez-le sur votre disque dur.

Dans la zone [Upgrade Target] (Mettre à niveau la cible), choisissez [Firmware] (Logiciel). Cliquez ensuite sur [Browse] (Parcourir) pour localiser le fichier préalablement téléchargé. Cliquez sur [APPLY] (Appliquer). Contrôlez la section Information de l'écran [Status] (État) pour vous assurer que la mise à niveau a été effectuée correctement.

Tools - Reset (Outils - Réinitialiser)



Cliquez sur [APPLY] (Appliquer) pour réinitialiser le routeur. La réinitialisation est terminée lorsque le témoin d'alimentation cesse de clignoter.

Remarque : si vous utilisez le bouton [Reset] du panneau avant, le routeur réinitialise l'alimentation. Si vous maintenez ce bouton enfoncé pendant plus de cinq secondes, tous les témoins lumineux s'allument et les paramètres par défaut sont restaurés.

Configuration du routeur Barricade™ g sans fil

Status (État)

L'écran [Status] (État) affiche l'état des connexions WAN/LAN, les numéros de version du matériel et du logiciel, les tentatives non autorisées d'accès au réseau, ainsi que des informations relatives à tous les postes clients DHCP connectés au réseau.

SMC Networks Advanced Setup Home Logout

Status

You can use the Status screen to see the connection status for Barricade g's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 04/29/2003 02:28:09 am

INTERNET	GATEWAY	INFORMATION
Cable/DSL: CONNECTED	IP Address: 192.168.2.1	Numbers of DHCP Clients: 1
WAN IP: 10.1.28.90	Subnet Mask: 255.255.255.0	Runtime Code Version:
Subnet Mask: 255.255.252.0	DHCP Server: Enabled	1.03 (Apr 26 2003 14:23:39)
Gateway: 10.1.28.254	Firewall: Enabled	Boot Code Version: V1.272
Primary DNS: 10.1.3.5	UPnP: Disabled	LAN MAC Address:
Secondary DNS: 10.2.3.4	Wireless: Enabled	00:04-E2-78-A6-D6

Security Log
View any attempts that have been made to gain access to your network.

04/29/2003	02:07:134	192.168.2.1	
04/29/2003	01:55:47	192.168.2.1	
04/29/2003	01:55:45	Denier From 1	
04/29/2003	01:25:32	Begin 10 qn	
04/29/2003	00:56:51	192.168.2.1	
04/29/2003	00:56:49	Denier From 1	
04/29/2003	00:43:55	NTP Date/Ts	
04/29/2003	00:39:43	NTP Date/Ts	
04/29/2003	00:35:08	NTP Date/Ts	

DHCP Client Log
View information on LAN DHCP clients currently linked to the Barricade g.

192.168.2.100	mac=00-E0-29-
---------------	---------------

Configuration avancée

Cet écran comporte les éléments suivants :

Section	Description
INTERNET	Affiche le type et l'état de connexion WAN.
GATEWAY (Passerelle)	Affiche les paramètres IP du système ainsi que l'état du service DHCP et du firewall.
INFORMATION	Affiche le nombre de postes clients connectés, les versions du logiciel, l'adresse MAC physique de chaque interface de support, ainsi que le numéro de version et de série du matériel.
Security Log (Journal de sécurité)	Affiche les tentatives non autorisées d'accès à votre réseau.
Save (Enregistrer)	Cliquez sur ce bouton pour enregistrer le fichier journal de sécurité.
Clear (Effacer)	Cliquez sur ce bouton pour supprimer le journal d'accès.
Refresh (Actualiser)	Cliquez sur ce bouton pour actualiser l'affichage de l'écran.
DHCP Client Log (Journal des clients DHCP)	Affiche des informations concernant l'ensemble des clients DHCP présents sur votre réseau.

DÉPANNAGE

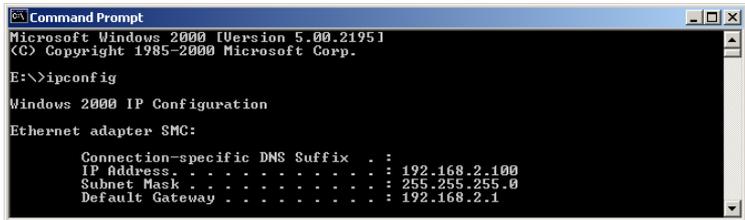
Cette section contient des informations utiles pour vous permettre de connecter votre imprimante et votre routeur.

A. Vérification de la connexion à votre routeur

S'il vous est impossible d'accéder aux pages Web d'administration du routeur, il se peut que vous ne soyez pas connecté ou configuré correctement. Les captures d'écrans de cette section ont été réalisées sur une machine Windows 2000, mais les mêmes étapes s'appliquent à Windows 95/98/Me/XP.

Pour déterminer l'état de votre configuration TCP/IP, procédez comme suit :

1. Cliquez sur [Start] (Démarrer) puis choisissez [Run] (Exécuter).
2. Tapez « cmd » ou « command » pour ouvrir une fenêtre DOS.
3. Dans la fenêtre DOS, tapez « ipconfig » et vérifiez les informations affichées.
4. Si votre ordinateur est configuré pour DHCP, votre configuration TCP/IP devrait présenter des informations similaires aux informations suivantes :
 - [IP Address] (Adresse IP) : 192.168.2.X (x étant un nombre compris entre 100 et 199)
 - [Subnet] (Sous-réseau) : 255.255.255.0
 - [Gateway] (Passerelle) : 192.168.2.1



```
Command Prompt
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter SMC:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

Si votre adresse IP commence par 169.254.XXX.XXX, reportez-vous à la section suivante.

Si vous avez une autre adresse IP, reportez-vous à la section C.

B. J'obtiens une adresse IP commençant par 169.254.XXX.XXX

Si vous obtenez cette adresse IP, vous devez vérifier que vous êtes correctement connecté au routeur.

Vérifiez que le témoin de liaison correspondant au port auquel cet ordinateur est connecté est bien allumé sur le routeur. Si ce n'est pas le cas, essayez un autre câble.

Si le témoin de liaison est allumé, ouvrez une fenêtre DOS selon les instructions de la section précédente et tapez « ipconfig/renew ».

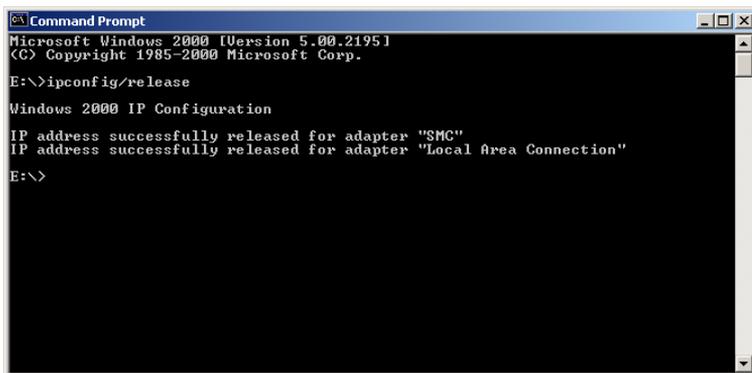
Si vous ne parvenez toujours pas à obtenir une adresse IP du routeur, réinstallez votre carte réseau. Reportez-vous au manuel de votre carte pour plus d'informations sur la manière de procéder.

C. Une autre adresse IP s'est affichée

Si une autre adresse IP s'est affichée, il est possible que le PC ne soit pas configuré pour une connexion DHCP. Reportez-vous à la section « Configuration de TCP/IP client » à la page 16 pour plus d'informations.

Après avoir vérifié que votre ordinateur était configuré pour DHCP, effectuez les étapes suivantes.

1. Ouvrez une fenêtre DOS comme décrit plus haut.
2. Tapez « ipconfig/release »



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

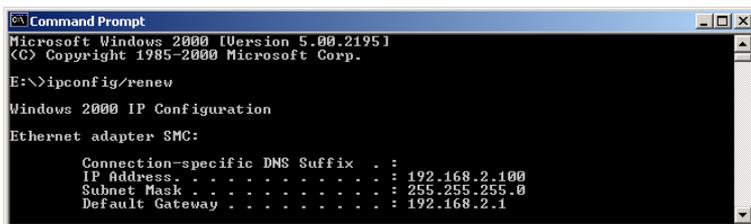
E:\>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "SMC"
IP address successfully released for adapter "Local Area Connection"

E:\>
```

3. puis « ipconfig/renew ».



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter SMC:

    Connection-specific DNS Suffix . . : 
    IP Address . . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

D. Le témoin 10/100 n'est pas allumé lorsqu'une connexion est établie.

1. Vérifiez que l'ordinateur hôte et le concentrateur sont sous tension.
2. Vérifiez que le câble réseau est connecté aux deux appareils.
3. Vérifiez que le cordon de catégorie 5 fonctionne à 100 Mbps et que la longueur des cordons ne dépasse pas 100 mètres.
4. Vérifiez les connexions de la carte réseau.
5. Le port du concentrateur/commutateur 10BASE-T/100BASE-TX, la carte réseau ou le câble peut être défectueux.

SPECIFICATIONS

Below is an outline of the Technical Specifications for the SMC2804WBR.

Standards

IEEE 802.3 10BASE-T Ethernet

IEEE 802.3u 100BASE-TX FastEthernet

IEEE 802.11b

IEEE 802.11g draft

WAN Interface

10BASE-T/100BASE-TX

LAN Interfaces

10BASE-T/100BASE-TX

4 RJ-45 ports: LAN data transfer rate is up to 10/20Mbps (10BASE-T half/full duplex) or 100/200Mbps (100BASE-TX with half/full duplex)

Antenna

2 Detachable Antennas with Reversed SMA Connectors

Management

Browser-based management

Both DHCP Server and Client provided

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Wireless Security – 64/128-bit WEP encryption, 802.1x, SSID broadcast disabled, MAC address filtering

Firewall – Access Control, hacker prevention, logging

Virtual Server via NAT & NAPT

Virtual Private Network – PPTP, L2TP, IPSec pass-through

Intrusion Detection, Email Alerts, Parental Control

Indicator Panel

Power, WLAN, WAN (Link, Activity), LAN (Link/Activity, Speed - 10/100 Mbps)

Dimensions

130 x 85 x 32 mm (5.12 x 3.35 x 1.26 in.)

Weight

370 g (13.05 oz)

Input Power

9 V, 1 A

Maximum Current

0.04 A RMS max. @ 110V/240V

Power Consumption

5 Watts max. @ 100-240 VAC

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 854-859 TELNET, RFC 1321 MD5, RFC 1497 BOOTP Extension, RFC 1570 PPP LCP Extension, RFC 1631 NAT, RFC1661 PPP, RFC 1700 Assigned Numbers, RFC 1866 HTML, RFC 1945 HTTP, RFC 1994 CHAP, RFC 2131 DHCP, RFC 2637 PPTP

Temperature

Operating 0 to 40 °C (32 to 104 °F)

Storage -40 to 70 °C (-40 to 158 °F)

Humidity

5% to 95% (noncondensing)

Specifications

Compliances

CE Mark

Emissions

FCC Class B

VCCI Class B

Industry Canada Class B

EN55022 (CISPR 22) Class B

C-Tick - AS/NZS 3548 (1995) Class B

Immunity

EN 61000-3-2/3

EN 61000-4-2/3/4/5/6/8/11

EN 300 328-2 V.1.2.1 (11-2001)

Safety

CSA/NRTL (UL1950, CSA 22.2.950)

GS (EN60950)

CB (IEC60950)

COMPLIANCES

FCC - Class B

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 harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2^o, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. This equipment is also compatible with R&TTE Directive 1999/5/EC for Electromagnetic compatibility and radio spectrum matters (ERM) Wideband Transmission systems; Data Transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques, covering essential requirements under Article 3(2) of the R&TTE Directive. For the evaluation of the compliance with these Directives, the following standards were applied:

- RFI
- * Limit class B according to EN 55022:1998
- Emission:
- * Limit class A for harmonic current emission according to EN 61000-3-2/1995
 - * Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995
- Immunity:
- * Product family standard according to EN 55024:1998
 - * Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ± 4 kV, Air Discharge: ± 8 kV)
 - * Radio-frequency electromagnetic field according to EN 61000-4-3:1996 (80 - 1000MHz with 1kHz AM 80% Modulation: 3V/m)
 - * Electrical fast transient/burst according to EN 61000-4-4:1995(AC/DC power supply: ± 1 kV, Data/Signal lines: ± 0.5 kV)
 - * Surge immunity test according to EN 61000-4-5:1995(AC/DC Line to Line: ± 1 kV, AC/DC Line to Earth: ± 2 kV)
 - * Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996(0.15 - 80MHz with 1kHz AM 80% Modulation: 3V/m)
 - * Power frequency magnetic field immunity test according to EN 61000-4-8:1993(1A/m at frequency 50Hz)
 - * Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994(>95% Reduction @10ms, 30% Reduction @500ms, >95% Reduction @500ms)
- LVD:
- * EN60950(A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)
- ERM:
- * EN 300 328 V1.2.1 (11-2001)

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: « Appareils Numériques », NMB-003 édictée par le ministère des Communications.

Australia AS/NZS 3548 (1995) - Class B



ACN 069 351 613

SMC contact for products in Australia is:

SMC Communications Pty. Ltd.
Suite 18, 12 Tryon Road,
Lindfield NSW2070,
Phone: 61-2-8875-7887
Fax: 61-2-8875-7777

Safety Compliance

Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Operating Voltage	Cord Set Specifications
120 Volts	UL Listed/CSA Certified Cord Set
	Minimum 18 AWG
	Type SVT or SJT three conductor cord
	Maximum length of 15 feet
	Parallel blade, grounding type attachment plug rated 15A, 125V
240 Volts (Europe only)	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm ²
	IEC-320 receptacle
	Male plug rated 10A, 250V

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

LEGAL INFORMATION AND CONTACTS

SMC's Limited Warranty Statement

SMC Networks Europe ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 2 year limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavour to repair or replace any product returned under warranty within 30 days of receipt of the product. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies

The standard limited warranty can be upgraded to a 5 year Limited Lifetime * warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as a period of 5 years from the date of purchase of the product from SMC or its authorized reseller.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries, either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Legal Information and Contacts

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF A SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM COUNTRY TO COUNTRY. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

Full Installation Manual

Full installation manuals are provided on the Installation CD-Rom. Manuals in other languages than those included on the CD-Rom are provided on www.smc-europe.com (section support).

Firmware and Drivers

For latest driver, technical information and bug-fixes please visit www.smc-europe.com (section support).

Contact SMC

Contact details for your relevant countries are available on www.smc-europe.com and www.smc.com.

Statement of Conditions

In line with our continued efforts to improve internal design, operational function, and/or reliability, SMC reserves the right to make changes to the product(s) described in this document without notice. SMC does not assume any liability that may occur due to the use or application of the product(s) described herein. In order to obtain the most accurate knowledge of installation, bug-fixes and other product related information we advise to visit the relevant product support page at www.smc-europe.com before you start installing the equipment. All information is subject to change without notice.

Limitation of Liability

In no event, whether based in contract or tort (including negligence), shall SMC be liable for incidental, consequential, indirect, special or punitive damages of any kind, or for loss of revenue, loss of business or other financial loss arising out of or in connection with the sale, installation, maintenance, use, performance, failure or interruption of its products, even if SMC or its authorized reseller has been advised of the possibility of such damages.

Copyright Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Trademarks

SMC is a registered trademark and EZ Connect is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.



Référence produit : SMC2804WBR