

Routeur Barricade ADSL

Routeur haut débit avec modem ADSL intégré

- ◆ Compatible avec les principaux DSLAM
- ◆ Firewall (journaux d'attaques extérieures, refus de service et filtrage de poste client)
- ◆ Supporte la modulation de ligne DMT
- ◆ Quatre ports Ethernet 10/100 à négociation automatique
- ◆ Serveur d'impression intégré
- ◆ Pass Through PPTP, L2TP et IPSec
- ◆ Accès Internet multi-utilisateurs avec un compte utilisateur unique
- ◆ Supporte PPPoE (PPP sur Ethernet) et PPPoA (PPP sur ATM)
- ◆ Installation Plug & Play
- ◆ Administration basée sur le Web



Routeur haut débit avec modem ADSL intégré

Un produit de la gamme des solutions de connectivité Barricade primées
de SMC

SMC[®]
Networks

Décembre 2002
Réf. : 750.9701, UK 750.9735
Pub. : 150000035400A

TABLE DES MATIÈRES

1	Introduction	1-1
	À propos du routeur Barricade	1-1
	Points forts	1-1
	Contextes d'utilisation	1-3
2	Installation	2-1
	Contenu de l'emballage	2-1
	Configuration requise	2-2
	Description du matériel	2-3
	Témoins	2-4
	Connexion du système	2-5
	Connexion de la ligne ADSL	2-5
	Configuration de la ligne téléphonique	2-6
	Raccordement du cordon d'alimentation	2-9
3	Configuration des ordinateurs clients	3-1
	Configuration TCP/IP	3-1
4	Configuration du routeur Barricade	4-1
	Exploration de l'interface Web	4-2
	Modification de la configuration	4-2
	Assistant de configuration	4-3
	Time Zone (Fuseau horaire)	4-3
	Internet Sharing (Partage Internet)	4-4
	Parameter Setting (Paramétrage)	4-5
	Finish (Terminer)	4-6
	PPPoE & PPPoA	4-7
	Finish (Terminer)	4-9
	Protocoles multiples sur mode ATM	4-11
	Finish (Terminer)	4-13
	Advanced Setup (Configuration avancée)	4-15
	Exploration de l'interface Web	4-15
	Modification de la configuration	4-17

TABLE DES MATIÈRES

Paramètres système	4-18
Time Zone (Fuseau horaire)	4-18
Password Settings (Paramètres de mot de passe)	4-19
Remote Management (Administration à distance)	4-20
DNS	4-21
WAN (Réseau étendu)	4-22
PPPoE (PPP over Ethernet, PPP sur Ethernet)	4-22
ATM	4-24
ISP (FAI)	4-26
LAN (Réseau local)	4-27
NAT (Translation d'adresses réseau)	4-28
Address Mapping (Mappage d'adresses)	4-29
Virtual Server (Serveur virtuel)	4-30
Routing System (Système de routage)	4-31
Static Route (Route statique)	4-32
RIP	4-33
Routing Table (Table de routage)	4-35
Firewall	4-36
Access Control (Contrôle d'accès)	4-38
Access Control (Contrôle d'accès) : Add PC (Ajouter un ordinateur)	4-40
URL Blocking (Blocage d'URL)	4-41
Schedule Rule (Règle de planification)	4-42
Intrusion Detection (Détection d'intrusion)	4-44
DMZ	4-51
SNMP	4-52
Community (Communauté)	4-52
Trap (Interception)	4-53
ADSL	4-54
Parameters (Paramètres ADSL)	4-54
Status (État)	4-55
Tools (Outils)	4-59
Configuration Tools (Outils de configuration)	4-59
Firmware Upgrade (Mise à niveau du logiciel)	4-60
Reset (Réinitialisation)	4-61
Status (État)	4-62

5	Configuration de TCP/IP client	5-1
	Windows 95/98/Me	5-2
	Désactivation du proxy HTTP	5-5
	Lecture des paramètres IP depuis votre routeur ADSL	5-8
	Windows NT 4.0	5-9
	Désactivation du proxy HTTP	5-12
	Lecture des paramètres IP depuis votre routeur	
	Barricade	5-12
	Windows 2000	5-14
	Désactivation du proxy HTTP	5-16
	Lecture des paramètres IP depuis votre routeur	
	Barricade	5-16
	Windows XP	5-19
	Désactivation du proxy HTTP	5-22
	Lecture des paramètres IP depuis votre routeur	
	Barricade	5-22
	Configuration de votre ordinateur Macintosh	5-24
	Désactivation du proxy HTTP	5-26
	Lecture des paramètres IP depuis votre routeur	
	Barricade	5-28
6	Configuration des services d'impression	6-1
	Installation du moniteur de port d'imprimante	6-1
	Configuration du serveur d'impression	6-4
	Configuration de l'imprimante réseau sous	
	Windows 95/98/Me/2000	6-4
	Configuration de l'imprimante réseau sous	
	Windows NT	6-6
	Configuration de l'imprimante réseau sous Unix	6-8
A	Dépannage	A-1
B	Câbles	B-1
	Câble Ethernet	B-1
	Spécifications	B-1
	Conventions de câblage	B-1

TABLE DES MATIÈRES

Connexion au port Ethernet RJ-45	B-2
Brochages	B-2
Câble ADSL	B-4
Spécifications	B-4
Conventions de câblage	B-4
C Specifications	C-1
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
Index	I-1

CHAPITRE 1

INTRODUCTION

Félicitations pour votre achat du routeur Barricade haut débit avec modem ADSL intégré (SMC7404BRA EU). SMC est fier de vous proposer ce périphérique de communication puissant mais simple, pour la connexion de votre réseau local (LAN) à Internet. Ce routeur offre une solution pratique et puissante pour les utilisateurs qui souhaitent surfer sur Internet de la manière la plus sûre.

À propos du routeur Barricade

Le routeur Barricade offre un accès Internet à plusieurs utilisateurs via le partage d'un compte utilisateur unique. Cette nouvelle technologie offre de nombreuses fonctions sécurisées et économiques. Il est simple à configurer et peut être opérationnel en quelques minutes.

Points forts

- Connexion Internet par l'intermédiaire d'un port WAN RJ-11.
- Connexion au réseau local via quatre ports Ethernet 10/100Mbps.
- Protocole DHCP permettant une configuration IP dynamique et serveur DNS assurant le mappage des noms de domaine.

INTRODUCTION

- Firewall doté de fonctions SPI (Stateful Packet Inspection), de droits d'accès client, de détection d'intrusion et de translation d'adresses réseau (NAT).
- La fonction de translation d'adresses réseau autorise également l'accès Internet 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).
- Connexion VPN Pass-Through (mode tunnel IPSec-ESP, L2TP, PPTP).
- Tunnel de détection d'application personnalisable supportant les applications qui nécessitent plusieurs connexions.
- Configuration aisée via un navigateur Web installé sur les systèmes d'exploitation qui supportent TCP/IP.
- Compatible avec les applications Internet les plus courantes.

Contextes d'utilisation

Le routeur Barricade offre de nombreuses applications avancées, telles que :

- **Réseau local filaire**

Le routeur Barricade offre une connectivité aux périphériques 10/100Mbps filaires, ce qui facilite la création d'un réseau destiné au grand public ou aux PME.

- **Accès à Internet**

Cet appareil supporte les accès à Internet via une connexion DSL. Dans la mesure où de nombreux fournisseurs DSL utilisent PPPoE ou PPPoA pour établir des communications avec les utilisateurs finals, le routeur Barricade comprend des clients intégrés correspondant à ces protocoles, de sorte qu'il n'est plus nécessaire d'installer ces services sur l'ordinateur.

- **Adresse IP partagée**

Le routeur Barricade permet à 253 utilisateurs d'accéder simultanément à Internet à l'aide d'une adresse IP partagée. Grâce à un seul compte de FAI, plusieurs utilisateurs du réseau peuvent naviguer simultanément sur le Web.

- **Serveur virtuel**

Si vous disposez d'une adresse IP statique, vous pouvez configurer le routeur Barricade de façon à ce qu'il serve d'hôte virtuel pour la translation d'adresses réseau. Les utilisateurs distants peuvent accéder aux divers services de votre site à l'aide d'une adresse IP constante. En fonction du service demandé (ou du numéro de port), le routeur Barricade peut ensuite acheminer la requête vers le serveur approprié (situé à une autre adresse IP interne). Votre réseau est ainsi sécurisé

contre les attaques extérieures directes de pirates et vous pouvez, grâce à une administration plus souple, modifier les adresses IP internes sans que cela ait une incidence sur les tentatives externes d'accès au réseau.

- **Support d'hôte DMZ**

Cette fonction garantit l'entière transparence, vis-à-vis d'Internet, d'un ordinateur connecté en réseau. Elle est utilisée lorsque la fonction de translation d'adresses réseau (NAT) et la sécurité de firewall empêchent une application Internet de fonctionner correctement.

- **Sécurité**

Le routeur Barricade prend en charge les fonctions de sécurité qui interdisent l'accès Internet à des utilisateurs spécifiés ou qui filtrent toutes les demandes de services particuliers que l'administrateur ne souhaite pas gérer. Le firewall du routeur Barricade bloque également 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).

- **Réseau privé virtuel (VPN) Pass-Through**

Le routeur Barricade supporte trois des protocoles de réseau privé virtuel les plus fréquemment utilisés : PPTP, L2TP et IPSec. Ces protocoles permettent aux utilisateurs distants d'établir une connexion sécurisée à leur réseau d'entreprise. Si votre Fournisseur d'Accès Internet supporte les réseaux privés virtuels, ces protocoles peuvent être utilisés pour créer un tunnel authentifié et chiffré permettant le transfert de données sécurisées via Internet (c'est-à-dire, un réseau de données

partagé de façon classique). Les protocoles VPN supportés par le routeur Barricade sont décrits brièvement ci-après.

- PPTP (Point-to-Point Tunneling Protocol) – Ce protocole fournit un tunnel sécurisé pour l'accès distant des postes clients à une passerelle de sécurité PPTP. PPTP comprend des dispositions d'émission d'appel et de contrôle de flux requises par les Fournisseurs d'Accès Internet.
- L2TP fusionne les meilleures fonctionnalités de PPTP et L2F. Comme PPTP, L2TP requiert que les routeurs du FAI supportent le protocole.
- IPSec (IP Security) – Ce protocole assure le chiffrement de couche réseau IP. IPSec peut supporter des réseaux de chiffrement de grande envergure (tels qu'Internet) à l'aide de certificats numériques permettant l'authentification des périphériques.

CHAPITRE 2

INSTALLATION

Avant d'installer le Routeur haut débit Barricade avec modem ADSL intégré, 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 local. Assurez-vous également de disposer de tous les câbles nécessaires avant de démarrer l'installation du routeur Barricade. Après avoir installé le routeur Barricade, reportez-vous à la section « Configuration du routeur Barricade » à la page 4-1.

Contenu de l'emballage

Après avoir défait l'emballage du routeur Barricade, vérifiez le contenu du coffret dans lequel vous devez trouver les éléments ci-dessous.

- Routeur Barricade ADSL (SMC7404BRA EU).
- Cordon d'alimentation.
- Un câble Ethernet de catégorie 5.
- Câble téléphonique de raccordement.
- CD-ROM contenant la documentation.
- Le présent manuel d'utilisation.
- Guide de commande du service ADSL.

Contactez immédiatement votre revendeur si vous constatez que l'un de ces éléments ne convient pas, est absent ou endommagé. Si possible, conservez le carton et les emballages d'origine dans le cas d'un éventuel retour du produit.

Configuration requise

Vous devez disposer de la configuration minimale suivante :

- Un accès à Internet, obtenu auprès de votre Fournisseur d'Accès Internet, à l'aide d'un modem DSL.
- 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 d'Accès Internet.
- Un ordinateur équipé d'une carte Fast Ethernet 10Mbps, 100Mbps ou 10/100Mbps, 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 4.0 ou ultérieure ou Netscape Communicator version 4.0 ou ultérieure, installé sur un ordinateur de votre site pour la configuration du routeur Barricade.

Description du matériel

Le routeur Barricade contient un modem DSL intégré et peut être connecté à Internet ou à un site distant par l'intermédiaire de son port WAN RJ-11. Il peut être connecté directement à votre ordinateur ou à un réseau local à l'aide de l'un des quatre ports réseau Fast Ethernet RJ-45.

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. Cependant, il se peut que le débit réel offert par les fournisseurs d'accès varie considérablement par rapport à ces limites maximales.

Les données échangées entre des périphériques connectés à votre réseau local peuvent circuler à une vitesse pouvant atteindre 100 Mbps via les ports Fast Ethernet.

Le routeur Barricade 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. Le panneau arrière est doté des ports suivants :

Élément	Description
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 d'imprimante parallèle	Un port parallèle pouvant être connecté à une imprimante. Cette dernière peut ensuite être partagée par tous les utilisateurs du réseau local.

Bouton Reset (Réinitialiser)	Ce bouton permet de réinitialiser le système ou de restaurer les paramètres par défaut. Pour effectuer une réinitialisation sans perte des paramètres de configuration, consultez « Reset (Réinitialisation) » à la page 4-62.
Prise d'alimentation	Branchez sur cette prise le cordon d'alimentation fourni. Avvertissement : l'utilisation d'un cordon d'alimentation inapproprié peut endommager le routeur Barricade.
Port WAN	Port WAN (RJ-11) Branchez sur ce port votre ligne DSL.

Témoins

Vérification de l'état

Contrôlent l'état de l'alimentation et des ports.

Témoin (LED)	Apparence	État
Power (Alimentation)	Allumé	Le routeur Barricade est sous tension. Fonctionnement normal.
	Éteint	L'appareil n'est plus alimenté en électricité ou défaillant.
Ethernet (4 témoins)	Allumé	Liaison Ethernet.
	Clignotant	Émission/réception de données.
	Éteint	Pas de liaison.
ADSL Syn (Synchronisation ADSL)	Allumé	La connexion ADSL fonctionne correctement.
	Clignotant	Démarrage.
	Éteint	La connexion ADSL n'est pas établie.
ADSL Data (Données ADSL)	Clignotant	Émission/réception de données.
	Éteint	Pas de transfert de données.

Connexion du système

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

- N'installez pas le routeur Barricade à proximité d'appareils de chauffage.
- N'installez pas le routeur Barricade 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 Barricade.

Connexion de la ligne ADSL

Reliez au moyen d'un câble téléphonique standard la prise murale fournissant le service ADSL au port WAN de votre routeur Barricade. Lors du branchement sur la prise RJ-11 ADSL, vérifiez que les clips de fixation sont bien enclenchés pour assurer la connexion. Si vous utilisez un service ADSL sans périphérique de répartition (splitterless), ajoutez des filtres passe-bas entre la prise murale ADSL et vos téléphones. (Ces filtres laissent passer les signaux vocaux mais éliminent les signaux de données.)

Configuration de la ligne téléphonique

Installation d'une connexion à pleine vitesse

Si vous utilisez une connexion à pleine vitesse (G.dmt), votre fournisseur de services raccordera la ligne ADSL extérieure à un périphérique de répartition données/voix. Dans ce cas, vous pourrez raccorder vos téléphones et votre ordinateur directement au périphérique de répartition comme indiqué ci-dessous :

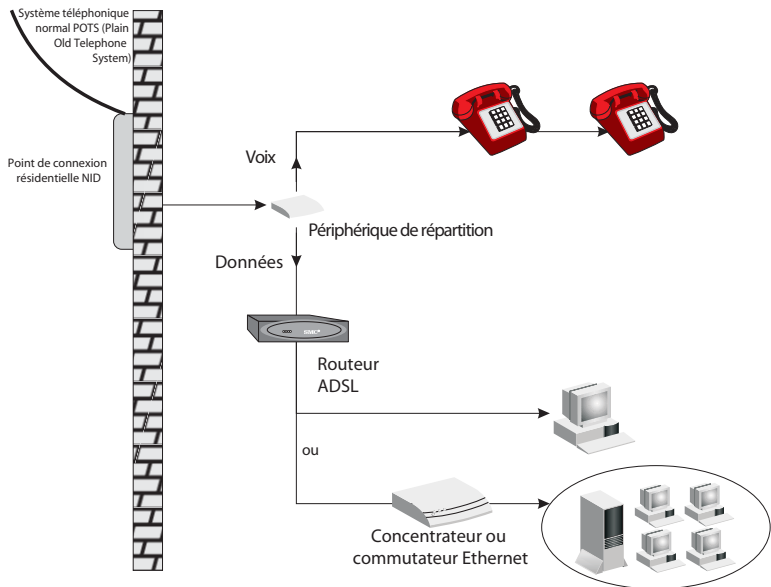


Figure 2-1. Installation avec un périphérique de répartition

Installation d'une connexion sans périphérique de répartition (Splitterless)

Si vous utilisez une connexion Splitterless (G.lite), votre fournisseur de services raccordera directement la ligne ADSL extérieure à votre système téléphonique. Dans ce cas, vous pourrez connecter vos téléphones et votre ordinateur directement à la ligne ADSL entrante, mais vous devrez ajouter des filtres passe-bas à vos téléphones comme illustré ci-dessous :

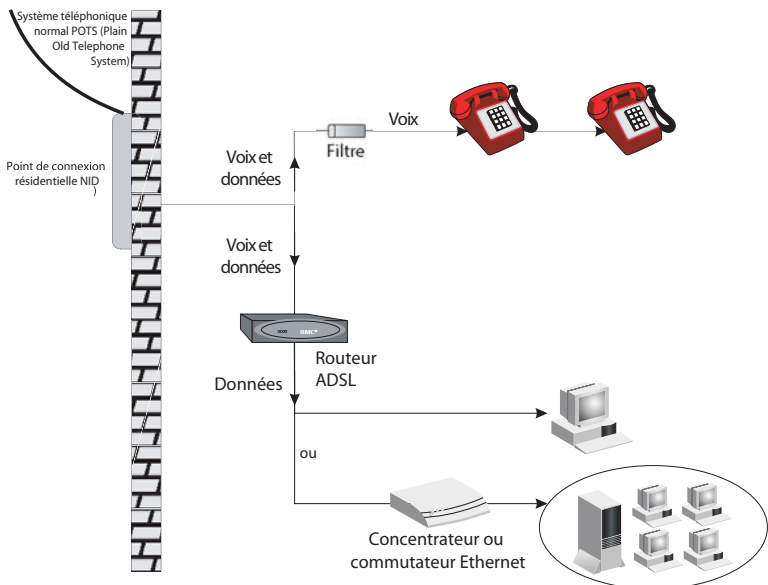


Figure 2-2. Installation sans périphérique de répartition

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

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

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

Avvertissement : ne raccordez pas de prise téléphonique à un port RJ-45. Cela peut endommager le routeur Barricade.

- Remarques :**
- 1.** utilisez un câble à paire torsadée 100 ohms blindé ou non blindé avec des connecteurs RJ-45 pour tous les ports Ethernet. Utilisez un câble de catégorie 3, 4 ou 5 pour les connexions 10 Mbps et de catégorie 5 pour les connexions 100 Mbps.
 - 2.** chaque câble à paire torsadée ne doit pas dépasser 100 mètres de long.

Raccordement du cordon d'alimentation

Branchez l'une des extrémités du cordon d'alimentation à la prise située à l'arrière du routeur Barricade et l'autre extrémité à une prise secteur.

Vérifiez que le témoin d'alimentation situé sur le panneau avant est allumé. S'il n'est pas allumé, reportez-vous à la section « Dépannage » à la page A-1.

En cas de rupture de l'alimentation électrique, le routeur Barricade redémarre automatiquement et reprend son fonctionnement dès que l'alimentation est rétablie.

Si le routeur Barricade est correctement configuré, il lui faut environ 30 secondes pour établir une connexion avec le fournisseur de services ADSL après sa mise sous tension. Pendant ce temps, le témoin Sync clignote. Une fois la connexion ADSL établie, le témoin ADSL Sync reste allumé en continu.

CHAPITRE 3

CONFIGURATION DES ORDINATEURS CLIENTS

Configuration TCP/IP

Pour accéder à Internet via le routeur Barricade, 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 Barricade sont les suivants :

Adresse IP : 192.168.2.1

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 la section « Configuration de TCP/IP client » à la page 5-1 afin d'accéder à l'interface de configuration Web du routeur Barricade pour effectuer les modifications nécessaires. (Pour plus de détails sur la configuration du routeur Barricade, reportez-vous à la section « Configuration du routeur Barricade » à la page 4-1.)

CHAPITRE 4

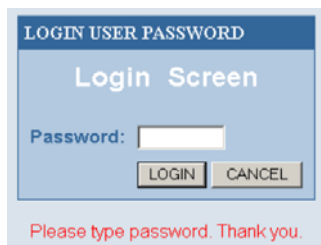
CONFIGURATION DU ROUTEUR BARRICADE

Après avoir configuré TCP/IP sur un poste client, utilisez un navigateur Web pour configurer le routeur Barricade. Ce dernier peut être configuré par tous les navigateurs supportant Java, y compris Internet Explorer version 4.0 ou ultérieure ou Netscape Navigator version 4.0 ou ultérieure. Grâce à l'interface d'administration Web, vous pouvez configurer le routeur Barricade et afficher des statistiques afin de surveiller l'activité du réseau.

Pour accéder à l'interface d'administration du routeur Barricade, entrez l'adresse IP du routeur dans le navigateur Web :

`http://192.168.2.1`

(le routeur Barricade est automatiquement commuté sur le port 88 qui permet l'accès aux fonctions d'administration). Cliquez ensuite sur « LOGIN » (Se connecter). Aucun mot de passe n'est défini par défaut.



Remarque : dans certains navigateurs, il peut être nécessaire d'ajouter « :88 » après l'adresse IP d'administration.
Exemple : `http://192.168.2.1:88`

Exploration de l'interface Web

L'interface d'administration du routeur Barricade comporte un Assistant de configuration (Setup Wizard) et une section de configuration avancée (Advanced Setup).

Setup Wizard (Assistant de configuration) : Utilisez l'Assistant de configuration pour installer rapidement le routeur Barricade. Consultez la section « Assistant de configuration » à la page 4-3.

Advanced Setup (Configuration avancée) : La section Advanced Setup supporte des fonctions plus avancées, parmi lesquelles la détection d'attaques extérieures, le filtrage d'adresses IP et MAC, la configuration de serveur virtuel, les hôtes DMZ virtuels, etc. Consultez la section « Advanced Setup (Configuration avancée) » à la page 4-16.

Modification de la configuration

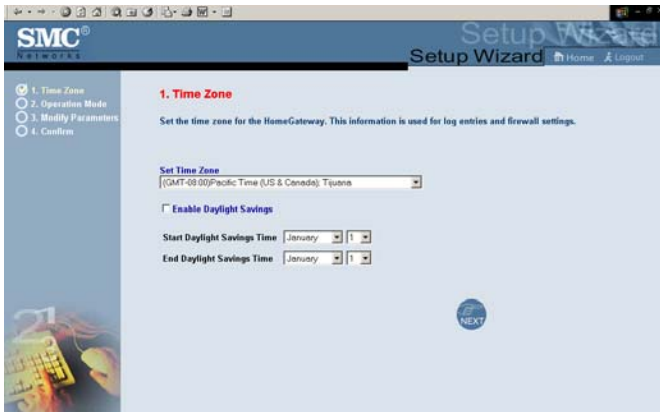
Les paramètres configurables sont dotés d'une boîte de dialogue ou d'une liste déroulante. Lorsqu'une modification de configuration a été apportée dans une page, veillez à cliquer sur le bouton « Apply » (Appliquer) ou « Next » (Suivant) au bas de la page pour valider le nouveau paramètre.

Remarque : pour garantir la régénération 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

Time Zone (Fuseau horaire)

Cliquez sur « Setup Wizard » (Assistant de configuration). La première des étapes de l'Assistant est la configuration du fuseau horaire.

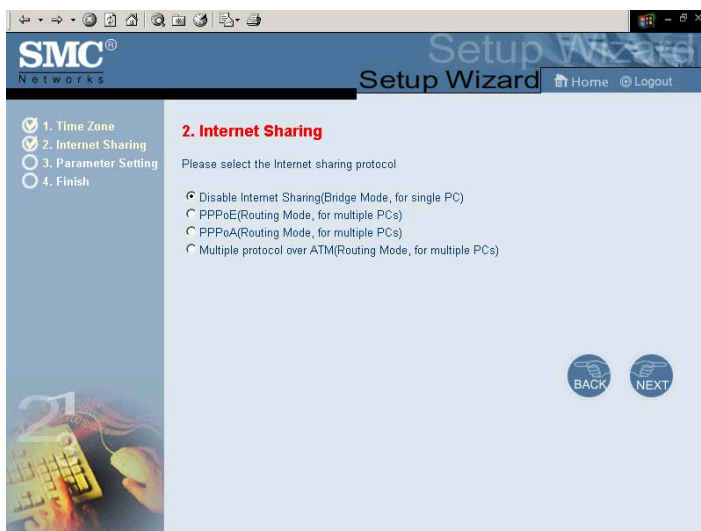


Pour la précision horaire des entrées de journal et des événements système, vous devez définir le fuseau horaire. Sélectionnez votre fuseau horaire dans la liste déroulante affichée.

S'il y a lieu, cochez pour activer la gestion de l'heure d'été, et entrez les dates de début et de fin de la période d'heure d'été pour l'endroit où vous vous trouvez.

Internet Sharing (Partage Internet)

Sélectionnez le mode de fonctionnement. Reportez-vous à la section « PPPoE & PPPoA » à la page 4-7 si vous envisagez d'utiliser l'un de ces modes et à la section « Protocoles multiples sur mode ATM » à la page 4-11 si vous envisagez d'utiliser le protocole de routage multiprotocole.

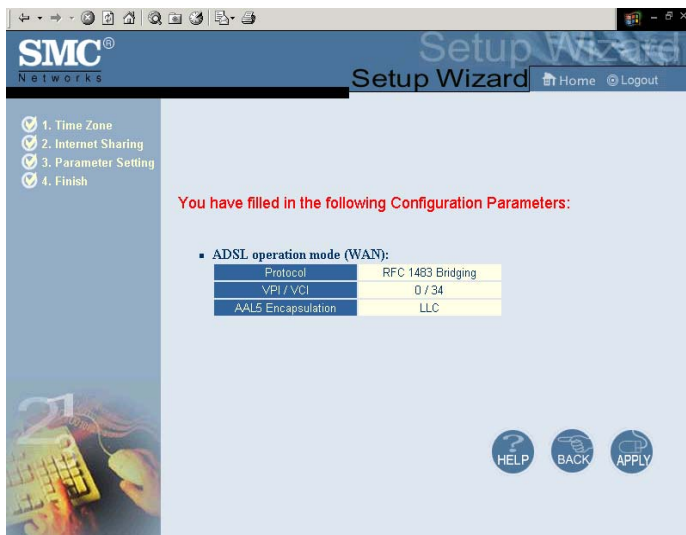


Parameter Setting (Paramétrage)



Paramètre	Description
VPI/VCI	Les flux de données sont scindés en cellules de longueur fixe, contenant chacune un identificateur VPI (Virtual Path Identifier) qui identifie le chemin entre deux nœuds et un identificateur VCI (Virtual Circuit Identifier) qui identifie le chemin de données au sein de ce chemin virtuel. Chaque circuit virtuel maintient un flux constant de cellules entre les deux points extrêmes. Lorsqu'il n'y a pas de données à transmettre, des cellules vides sont envoyées. Et lorsqu'il est nécessaire de transmettre des données, elles sont immédiatement insérées dans les flux de cellules.

Finish (Terminer)



Paramètre	Description
Protocole (Protocole)	Indique le protocole employé.
VPI/VCI	Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).
AAL5 Encapsulation (Encapsulation AAL5)	Montre le type d'encapsulation de paquet.

Votre routeur Barricade est maintenant installé. Reportez-vous à la section « Dépannage » à la page A-1 si vous ne parvenez pas à établir de connexion à Internet.

PPPoE & PPPoA

SMC[®] Networks Setup Wizard

Home Logout

1. Time Zone
2. Internet Sharing
3. Parameter Setting
4. Finish

3. Parameter Setting

Username:

Password:

Retype Password:

DNS:

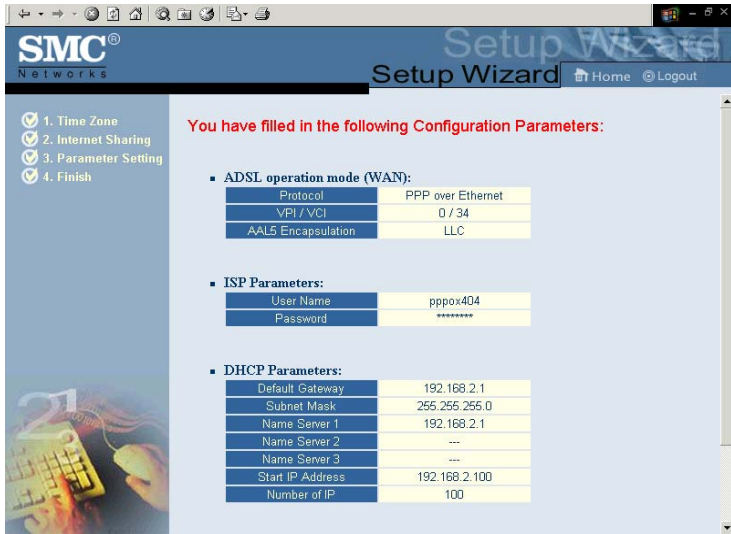
VPI/VCI: /

HELP BACK NEXT

Paramètre	Description
Username (Nom d'utilisateur)	Entrez le nom d'utilisateur affecté par le FAI.
Password (Mot de passe)	Entrez votre mot de passe.
Retype Password (Retapez le mot de passe)	Confirmez le mot de passe.

Paramètre	Description
DNS	Entrez une adresse IP de serveur de noms de domaine.
VPI/VCI	Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier). Les flux de données sont scindés en cellules de longueur fixe, contenant chacune un identificateur VPI (Virtual Path Identifier) qui identifie le chemin entre deux nœuds et un identificateur VCI (Virtual Circuit Identifier) qui identifie le chemin de données au sein de ce chemin virtuel. Chaque circuit virtuel maintient un flux constant de cellules entre les deux points extrêmes. Lorsqu'il n'y a pas de données à transmettre, des cellules vides sont envoyées. Et lorsqu'il est nécessaire de transmettre des données, elles sont immédiatement insérées dans les flux de cellules.

Finish (Terminer)



Paramètre	Description
ADSL Operation Mode (WAN) (Mode de fonctionnement ADSL (WAN))	
Protocol (Protocole)	Indique le protocole utilisé.
VPI/VCI	Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).
AAL5 Encapsulation (Encapsulation AAL5)	Montre le type d'encapsulation de paquet.
ISP Parameters (Paramètres FAI)	
Username (Nom d'utilisateur)	Nom affecté par le FAI.
Password (Mot de passe)	Mot de passe (caché).

Paramètre	Description
DHCP Parameters (Paramètres DHCP)	
Default Gateway (Passerelle par défaut)	Adresse IP de passerelle par défaut. Si le routeur Barricade ne parvient pas à trouver l'adresse de destination dans son réseau local, il achemine les paquets vers la passerelle par défaut (son adresse vous sera généralement transmise par votre FAD).
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau.
Name Server 1 (Serveur de noms 1)	Adresse IP du serveur de noms principal.
Name Server 2 (Serveur de noms 2)	Adresse IP d'un serveur de noms auxiliaire.
Name Server 3 (Serveur de noms 3)	Adresse IP d'un serveur de noms auxiliaire.
Start IP Address (Adresse IP de début)	Adresse IP de début des adresses IP affectées par DHCP.
Number of IP (Nombre d'IP)	Nombre d'adresses IP disponibles pour une affectation par le serveur DHCP.

Votre routeur Barricade est maintenant installé. Reportez-vous à la section « Dépannage » à la page A-1 si vous ne parvenez pas à établir de connexion à Internet.

Protocoles multiples sur mode ATM

The screenshot shows the SMC Networks Setup Wizard at the '3. Parameter Setting' stage. The progress bar on the left indicates that steps 1 (Time Zone), 2 (Internet Sharing), and 3 (Parameter Setting) are completed, while step 4 (Finish) is not. The main area contains the following configuration fields:

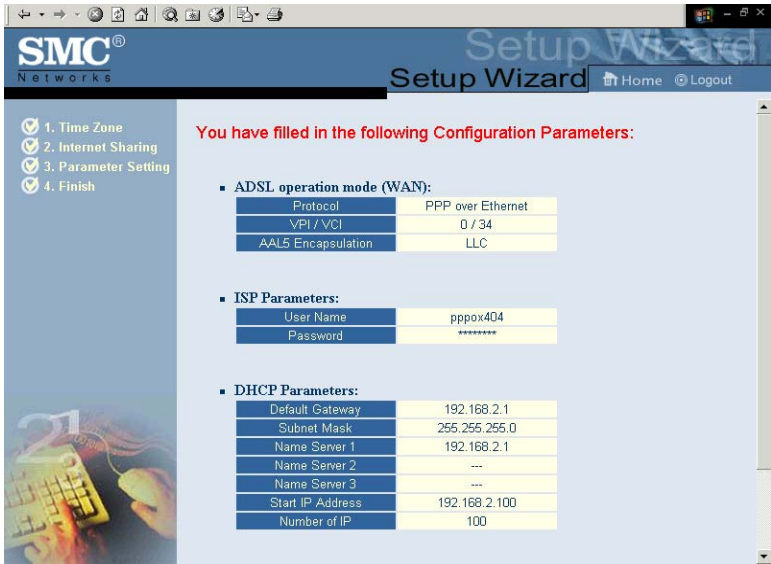
- DNS:** 200 | 0 | 10 | 254
- WAN IP:** 0 | 0 | 0 | 0
- Subnet Mask:** 0 | 0 | 0 | 0
- VPI/VCI:** 0 / 34
- Default Gateway:** 0 | 0 | 0 | 0

Navigation buttons for HELP, BACK, and NEXT are located at the bottom right of the wizard window.

Paramètre	Description
DNS	Entrez une adresse IP de serveur de noms de domaine.
WAN IP (IP WAN)	Entrez une adresse IP pour l'interface WAN du routeur Barricade.
Subnet Mask (Masque de sous-réseau)	Entrez un masque de sous-réseau.

Paramètre	Description
VPI/VCI	<p>Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).</p> <p>Les flux de données sont scindés en cellules de longueur fixe, contenant chacune un identificateur VPI (Virtual Path Identifier) qui identifie le chemin entre deux nœuds et un identificateur VCI (Virtual Circuit Identifier) qui identifie le chemin de données au sein de ce chemin virtuel. Chaque circuit virtuel maintient un flux constant de cellules entre les deux points extrêmes. Lorsqu'il n'y a pas de données à transmettre, des cellules vides sont envoyées. Et lorsqu'il est nécessaire de transmettre des données, elles sont immédiatement insérées dans les flux de cellules.</p>
Default Gateway (Passerelle par défaut)	<p>Entrez une adresse IP de passerelle par défaut. Si le routeur Barricade ne parvient pas à trouver l'adresse de destination dans son réseau local, il achemine les paquets vers la passerelle par défaut (dont l'adresse vous est généralement fournie par votre FAI).</p>

Finish (Terminer)



Paramètre	Description
ADSL Operation Mode (WAN)	
(Mode de fonctionnement ADSL)	
(WAN)	
Protocol (Protocole)	Indique le protocole utilisé.
VPI/VCI	Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).
AAL5 Encapsulation (Encapsulation AAL5)	Montre le type d'encapsulation de paquet.

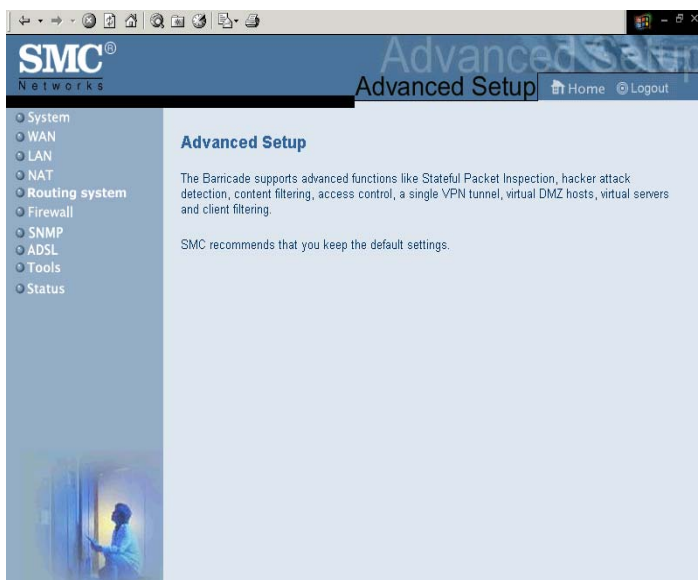
Paramètre	Description
<hr/>	
Network Layer Parameters (WAN) (Paramètres de la couche réseau (WAN))	
IP Address (Adresse IP)	Montre l'adresse IP WAN.
Subnet Mask (Masque de sous-réseau)	Montre le masque de sous-réseau WAN.
Default Gateway (Passerelle par défaut)	Montre la passerelle par défaut WAN.
DHCP Parameters (Paramètres DHCP)	
Default Gateway (Passerelle par défaut)	Adresse IP de passerelle par défaut. Si le routeur Barricade ne parvient pas à trouver l'adresse de destination dans son réseau local, il achemine les paquets vers la passerelle par défaut (dont l'adresse vous est généralement fournie par votre FAI).
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau.
Name Server 1 (Serveur de noms 1)	Adresse IP du serveur de noms principal.
Name Server 2 (Serveur de noms 2)	Adresse IP d'un serveur de noms auxiliaire.
Name Server 3 (Serveur de noms 3)	Adresse IP d'un serveur de noms auxiliaire.
Start IP Address (Adresse IP de début)	Adresse IP de début des adresses IP affectées par DHCP.
Number of IP (Nombre d'IP)	Nombre d'adresses IP disponibles pour une affectation par le serveur DHCP.

Votre routeur Barricade est maintenant installé. Reportez-vous à la section « Dépannage » à la page A-1 si vous ne parvenez pas à

établir de connexion à Internet.

Advanced Setup (Configuration avancée)

Le choix de l'option « Advanced Setup » (Configuration avancée) affiche le menu principal dans la partie gauche de l'écran et des informations descriptives dans la partie droite. Les liens du menu principal servent à naviguer vers d'autres menus qui affichent des paramètres de configuration et des statistiques.



Exploration de l'interface Web

L'interface d'administration avancée du routeur Barricade comprend les dix menus clés suivants – System (Système), WAN (Réseau étendu), LAN (Réseau local), NAT, Routing system (Système de routage), Firewall, SNMP, ADSL, Tools (Outils) et Status (État).

Le tableau suivant décrit brièvement les options disponibles dans la fonction « Advanced Setup » (Configuration avancée).

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 Barricade à distance, ainsi que l'adresse IP d'un serveur de noms de domaine.
WAN (Réseau étendu)	Indique les paramètres de connexion Internet.
LAN (Réseau local)	Définit la configuration TCP/IP associée à l'interface LAN du routeur Barricade et aux clients DHCP.
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.
Routing system (Système de routage)	Définit les paramètres de routage et affiche la table de routage en cours.
Firewall (Pare-feu)	Permet la configuration d'un grand nombre de fonctions de sécurité et de fonctions spécialisées, comprenant : Access Control (Contrôle d'accès), URL blocking (Blocage d'URL), Internet access control scheduling (Planification du contrôle d'accès à Internet), Intruder detection (Détection d'intrusion) et DMZ.
SNMP	Chaîne de communauté et paramétrage de serveur d'interception.
ADSL	Définit le type d'opération ADSL et montre l'état de la connexion ADSL.

Menu	Description
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.

Modification de la configuration

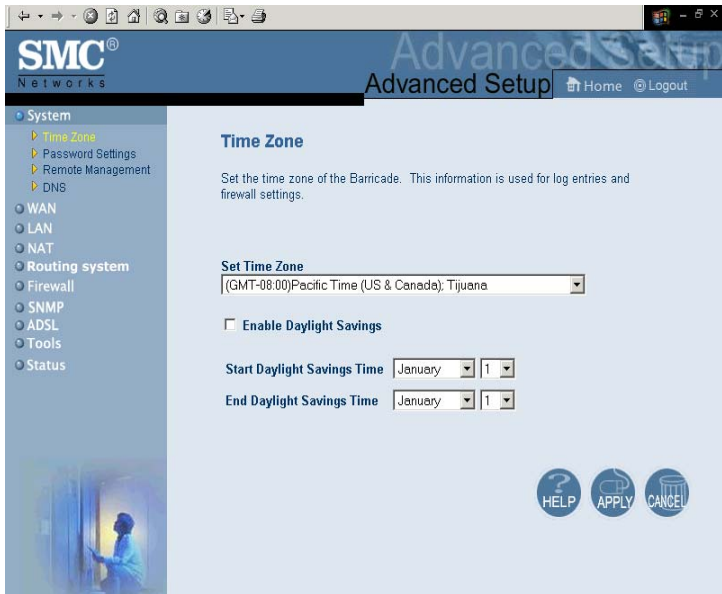
Les paramètres configurables sont dotés d'une boîte de dialogue ou d'une liste déroulante. Une fois qu'une modification de configuration a été apportée dans une page, veillez à cliquer sur le bouton « APPLY » (Appliquer) ou « NEXT » (Suivant) au bas de la page pour valider le nouveau paramètre.



Remarque : pour garantir la régénération 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).

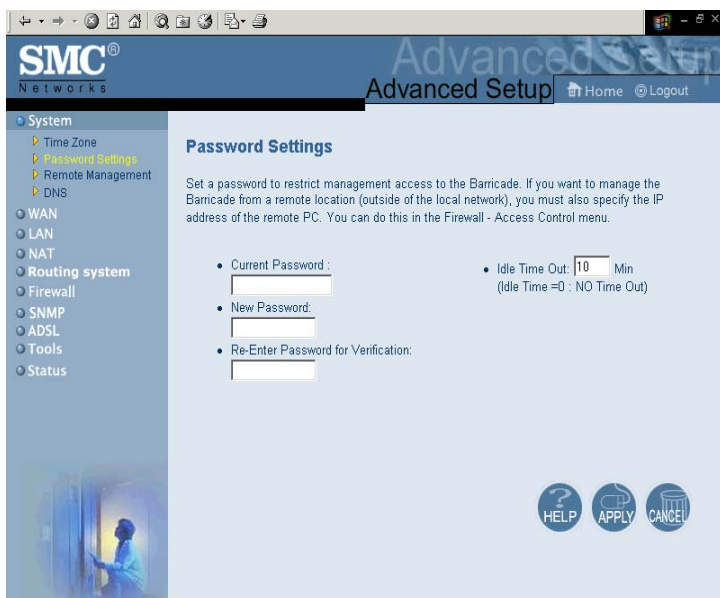
Paramètres système

Time Zone (Fuseau horaire)



Définissez votre fuseau horaire local. Cette information est utilisée pour les entrées de journal et le filtrage des postes clients.

Password Settings (Paramètres de mot de passe)

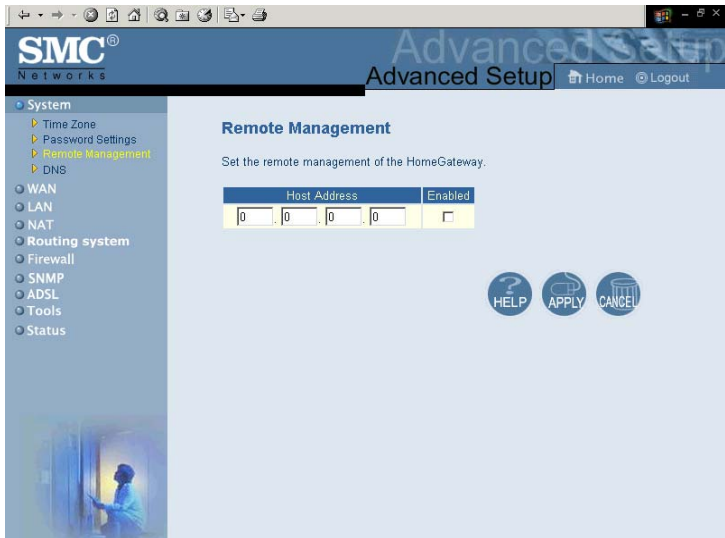


Cette page sert à limiter les accès au moyen d'un mot de passe. Par défaut, aucun mot de passe n'est défini. Pour des raisons de sécurité, il est conseillé de définir un mot de passe avant de relier le routeur Barricade à Internet.

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 (de couleur bleue) 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.)

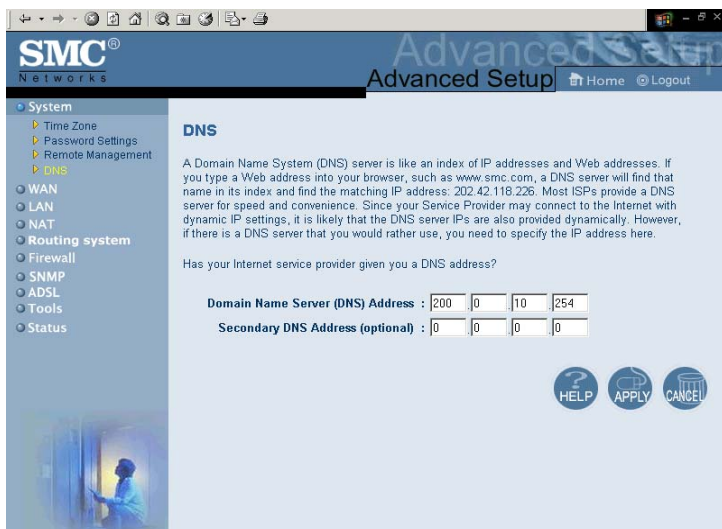
Remote Management (Administration à distance)



Par défaut, l'accès d'administration n'est disponible que pour les utilisateurs de votre réseau local. Cependant, vous pouvez également gérer le routeur Barricade à partir d'un hôte distant en entrant l'adresse IP d'un ordinateur distant dans cet écran. Activez la case à cocher « Enabled » (Activée) pour activer cette fonction.

Remarque : si vous activez cette case à cocher et spécifiez l'adresse IP 0.0.0.0, n'importe quel système hôte pourra gérer le routeur Barricade.

DNS



Les serveurs DNS permettent de mapper un nom de domaine (par exemple, `www.smc.com`) avec l'adresse IP numérique équivalente (par exemple, `64.147.25.20`). Votre Fournisseur d'Accès Internet doit indiquer l'adresse IP d'un ou de plusieurs serveurs DNS. Entrez ces adresses sur cette page.

WAN (Réseau étendu)

PPPoE (PPP over Ethernet, PPP sur Ethernet)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), PPPoE (selected), ATM, ISP, LAN, NAT, Routing system, Firewall, SNMP, ADSL, Tools, and Status. The main content area is titled 'PPPoE Interface Parameter' and contains a configuration table for the PPPoE interface. The table has the following fields: Enable/Disable (set to 'Disable'), IP Address (set to '0.0.0.0'), Subnet Mask (set to '0.0.0.0'), VPI/VCI (set to '0 / 34'), Encapsulation (set to 'LLC'), Idle Time (Minute) (set to '0'), and ISP Name (set to '1.ISP'). At the bottom right of the configuration area, there are three circular buttons: HELP, APPLY, and CANCEL.

Paramètre	Description
Enable/Disable (Activer, désactiver)	Active/désactive l'interface PPPoE.
IP Address (Adresse IP)	Si votre adresse IP est affectée par le FAI chaque fois que vous vous connectez, laissez ce champ entièrement à zéro. Sinon, entrez ici l'adresse IP statique fournie par votre FAI.
Subnet Mask (Masque de sous-réseau)	Si votre masque de sous-réseau est affecté par le FAI chaque fois que vous vous connectez, laissez ce champ entièrement à zéro. Sinon, entrez ici votre masque de sous-réseau.

Paramètre	Description
VPI/VCI	<p>Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).</p> <p>Les flux de données sont scindés en cellules de longueur fixe, contenant chacune un identificateur VPI (Virtual Path Identifier) qui identifie le chemin entre deux nœuds et un identificateur VCI (Virtual Circuit Identifier) qui identifie le chemin de données au sein de ce chemin virtuel. Chaque circuit virtuel maintient un flux constant de cellules entre les deux points extrêmes. Lorsqu'il n'y a pas de données à transmettre, des cellules vides sont envoyées. Lorsque des données doivent être transmises, elles sont immédiatement insérées dans les flux de cellules.</p>
Encapsulation	<p>Indique comment gérer plusieurs protocoles dans la couche de transport ATM.</p> <ul style="list-style-type: none"> • VC-MUX. Point to Point Protocol over ATM Virtual Circuit Multiplexer (Protocole point à point sur multiplexeur de circuits virtuels ATM) (encapsulation nulle) n'autorise qu'un seul protocole par circuit virtuel (temps système moindre). • LLC. Point to Point Protocol over ATM Logical Link Control (Protocole point à point sur contrôle de liaison logique ATM) autorise plusieurs protocoles par circuit virtuel (temps système légèrement plus important).
Idle Time (Minute) (Délai d'inactivité en minutes)	<p>Saisissez la durée maximale d'inactivité pour la connexion Internet. Lorsque ce délai est dépassé, il est mis fin à la connexion.</p>
ISP Name (Nom du FAI)	<p>Choisissez le FAI à qui la connexion doit s'appliquer.</p>

ATM

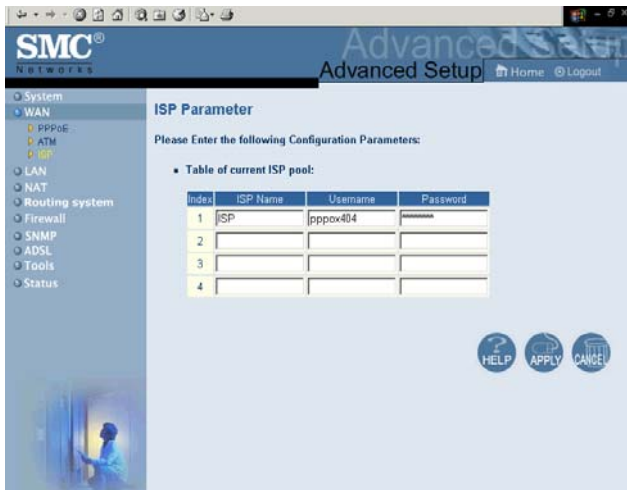
**Paramètre****Description**

Protocol
(Protocole)

- Disable (Désactiver) : désactive la connexion.
- 1483 Bridging (Pontage 1483) : Le pontage est une technologie normalisée de la couche 2. Elle est généralement utilisée dans les réseaux d'entreprise pour étendre la portée physique d'un segment de réseau local unique et accroître le nombre de stations dans un réseau local sans nuire aux performances. Les données pontées sont encapsulées à l'aide du protocole RFC1483 pour permettre leur transport.
- PPPoA : Point-to-Point Protocol over ATM (Protocole point à point sur ATM) est une méthode d'encapsulation des données pour la transmission vers un point distant.

Paramètre	Description
Protocol (Protocole)	<ul style="list-style-type: none"> 1483 Routing (Routage 1483) : Permet une connexion simple et économique à Internet par l'intermédiaire d'un port 10BASE-T standard. Le routeur recherche l'adresse réseau de chaque paquet rencontré sur le port du réseau local. Si cette adresse est signalée comme locale dans la table de routage, elle est filtrée. Si l'adresse est destinée au port ADSL, elle est transmise. Si l'adresse n'est pas trouvée, elle est automatiquement transmise au routeur par défaut (c'est-à-dire au routeur ADSL en tête de réseau).
IP Address (Adresse IP)	Adresse IP de l'interface ATM.
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau de l'interface ATM.
VPI/VCI	<p>Virtual Path Indicator (Indicateur de chemin virtuel) : chaque connexion doit avoir une paire unique de paramètres VPI/VCI.</p> <p>Virtual Channel Indicator (Indicateur de canal virtuel) : chaque connexion doit avoir une paire unique de paramètres VPI/VCI.</p>
Encapsulation	<p>Indique comment gérer plusieurs protocoles dans la couche de transport ATM.</p> <ul style="list-style-type: none"> VC-MUX. Point to Point Protocol over ATM Virtual Circuit Multiplexer (Protocole point à point sur multiplexeur de circuits virtuels ATM) (encapsulation nulle) n'autorise qu'un seul protocole par circuit virtuel (temps système moindre). LLC. Point to Point Protocol over ATM Logical Link Control (Protocole point à point sur contrôle de liaison logique ATM) autorise plusieurs protocoles par circuit virtuel avec un temps système légèrement plus important.

ISP (FAI)

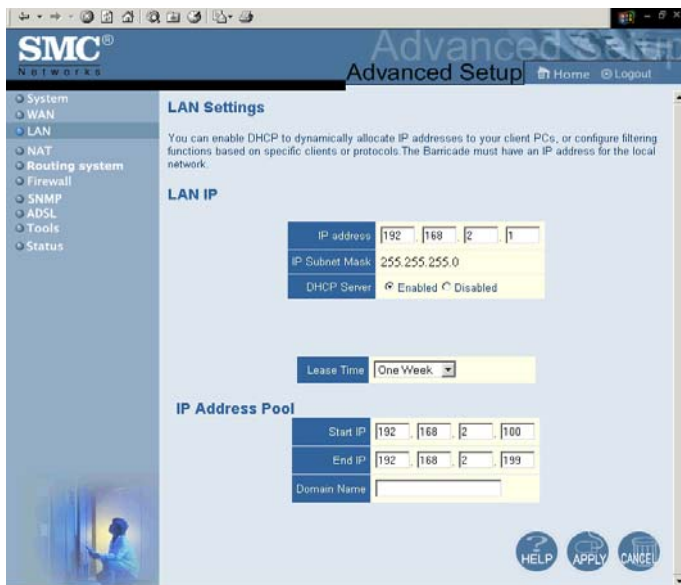


The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), PPPoE, ATM, ISP, LAN, NAT, Routing system, Firewall, SNMP, ADSL, Tools, and Status. The main content area is titled "ISP Parameter" and includes the instruction "Please Enter the following Configuration Parameters:". Below this is a section labeled "Table of current ISP pool:" which contains a table with four columns: Index, ISP Name, Username, and Password. The first row is pre-filled with the values "1", "ISP", "pppox404", and "XXXXXXXX". The second, third, and fourth rows are empty. At the bottom right of the interface are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

Index	ISP Name	Username	Password
1	ISP	pppox404	XXXXXXXX
2			
3			
4			

Entrez le nom du Fournisseur d'Accès Internet, le nom d'utilisateur et le mot de passe pour chacune de vos connexions de FAI.

LAN (Réseau local)



Paramètre	Description
LAN IP (Adresse IP du réseau local)	
IP Address (Adresse IP)	Adresse IP du routeur Barricade.
IP Subnet Mask (Masque de sous-réseau IP)	Identificateur VPI (Virtual Path Identifier) et identificateur VCI (Virtual Circuit Identifier).
DHCP Server (Serveur DHCP)	Pour affecter dynamiquement une adresse IP à des ordinateurs clients, activez le serveur DHCP (Dynamic Host Configuration Protocol).
Lease Time (Durée du bail)	Définit la durée du bail DHCP.

Paramètre	Description
IP Address Pool (Pool d'adresses IP)	
Start IP Address (Adresse IP de début)	Spécifiez l'adresse IP de début du pool DHCP. N'incluez pas l'adresse de passerelle du routeur Barricade dans le pool d'adresses de poste client. Si vous modifiez la plage du pool, assurez-vous que les trois premiers octets correspondent à l'adresse IP de la passerelle, c'est-à-dire, 192.168.2.xxx.
End IP Address (Adresse IP de fin)	Spécifiez l'adresse IP de fin du pool DHCP.
Domain Name (Nom de domaine)	Si votre réseau utilise un nom de domaine, entrez-le ici. Sinon, laissez ce champ vide.

Veillez également à configurer vos postes clients aux fins d'attribution d'adresses IP dynamiques (voir la section « Configuration des ordinateurs clients » à la page 3-1 pour les détails).

NAT (Translation d'adresses réseau)

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

Address Mapping (Mappage d'adresses)



Utilisez le mappage d'adresses pour permettre la conversion d'un nombre limité d'adresses IP publiques en plusieurs adresses IP privées en vue d'une utilisation dans le réseau local interne. Cette opération dissimule aussi le réseau interne pour une confidentialité et une sécurité plus grandes.

Virtual Server (Serveur virtuel)

Virtual Server

You can configure the Barricade 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 Barricade redirects the external service request to the appropriate server (located at another internal IP address).

	Private IP	Private Port	Type	Public Port
1.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
2.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
3.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
4.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
5.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
6.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
7.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
8.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
9.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
10.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
11.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
12.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
13.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
14.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
15.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
16.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
17.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
18.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
19.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
20.	192.168.2. <input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

HELP APPLY CANCEL

Si vous configurez le routeur Barricade en tant que serveur virtuel, les utilisateurs distants accédant aux services Web ou FTP de votre site local via des adresses IP publiques peuvent automatiquement

être 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 Barricade 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.

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

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

Remarque : pour utiliser correctement cette fonction, l'interface WAN doit comporter une adresse IP statique. Si votre FAI ne propose que des adresses IP dynamiques, recherchez l'expression « libérer IP dynamique » dans n'importe quel moteur de recherche courant pour trouver les outils qui permettent d'utiliser un même nom de domaine même si votre adresse IP change chaque fois que vous vous connectez au FAI.

Routing System (Système de routage)

Ces pages définissent les paramètres liés au routage, notamment les paramètres de routes statiques et RIP (Routing Information Protocol).

Static Route (Route statique)

SMC® Networks Advanced Setup | Home | Logout

Static Route Parameter

Please Enter the Following Configuration Parameters:

- Table of current static route entries:
click <add> button to add new entry, or click <delete> or <modify> button to change the selected entry.

Index	Network Address	Subnet Mask	Gateway
<input checked="" type="radio"/> 1	192.168.4.1	255.255.255.0	64.147.25.20
<input type="radio"/> 2	192.168.44.1	255.255.0.0	64.147.25.21
<input type="radio"/> 3	192.168.33.1	255.255.0.0	64.147.25.22

Buttons: Add | Delete | Modify

Buttons: APPLY | CANCEL

Paramètre

Description

Index
(Indice)

Activez la case correspondant à la route à supprimer ou à modifier.

Network Address
(Adresse réseau)

Entrez l'adresse IP de l'ordinateur distant avec lequel vous souhaitez établir une route statique.

Subnet Mask
(Masque de sous-réseau)

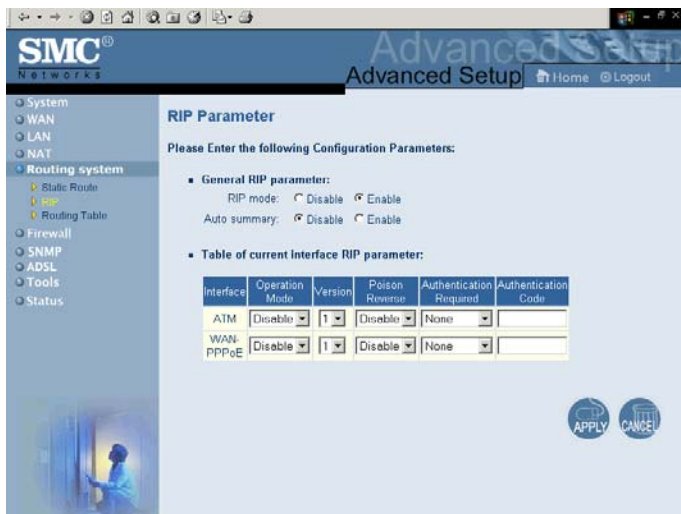
Entrez le masque de sous-réseau de l'ordinateur distant avec lequel vous souhaitez établir une route statique.

Gateway
(Passerelle)

Entrez l'adresse IP WAN de la passerelle vers le réseau distant.

Cliquez sur « Add » (Ajouter) pour ajouter une nouvelle route statique à la liste ou activez une case correspondant à une route déjà entrée et cliquez sur « Modify » (Modifier). Pour supprimer une entrée de la liste, cliquez sur « Delete » (Supprimer).

RIP



Paramètre	Description
Interface	L'interface WAN à configurer.
Operation Mode (Mode de fonctionnement)	Disable (Désactiver) : RIP est désactivé sur cette interface. Enable (Activer) : RIP est activé sur cette interface.
Version	Silent (Silencieux) : écoute les diffusions de route et met à jour sa table de routes. Il ne participe pas à l'envoi de diffusions de routes. Définit la version RIP (Routing Information Protocol) à utiliser sur cette interface.
Poison Reverse	Méthode par laquelle un routeur signale à son voisinage qu'un des routeurs n'est plus connecté.

Paramètre	Description
Authentication Required (Authentication nécessaire)	<ul style="list-style-type: none">• None (Aucune) : pas d'authentification.• Password (Mot de passe) : une clé d'authentification de mot de passe est incluse dans le paquet. Si elle ne correspond pas à celle attendue, le paquet est écarté. Cette méthode n'offre qu'une sécurité très faible, car il est possible de connaître les clés d'authentification en examinant les paquets RIP. <p>MD5 : MD5 est un algorithme permettant de vérifier l'intégrité des données grâce à la création d'un condensé de message sur 128 bits à partir des données d'origine (qui peuvent être un message d'une longueur quelconque) ; ce condensé est censé être propre à ces données particulières de la même façon qu'une empreinte digitale est propre à un individu.</p>
Authentication Code (Code d'authentification)	Mot de passe ou clé d'authentification MD5.

RIP envoie des messages de mise à jour du routage à intervalles réguliers ainsi que lors des changements de la topologie du réseau. Lorsqu'un routeur reçoit une mise à jour du routage qui inclut des modifications d'une entrée, il met à jour sa table de routage pour refléter la nouvelle route. Les routeurs RIP ne conservent que la meilleure route pour une destination. Après avoir mis à jour sa table de routage, le routeur commence immédiatement à transmettre les mises à jour du routage pour informer les autres routeurs du réseau de la modification.

Routing Table (Table de routage)

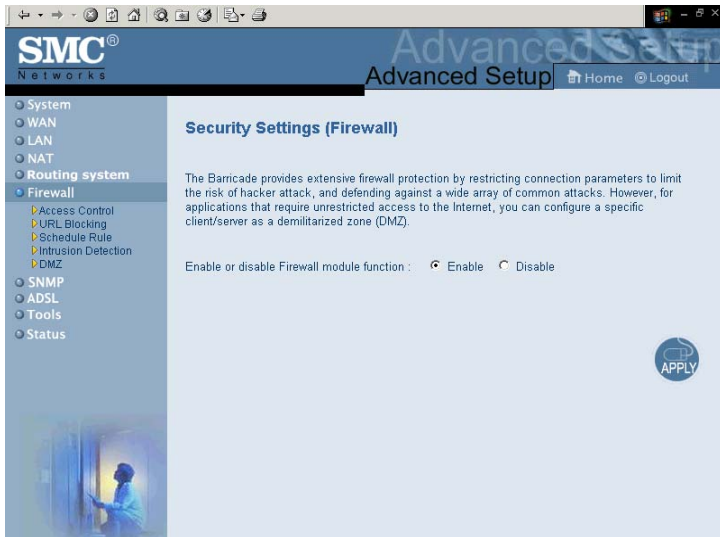


Paramètre	Description
Flags (Indicateurs)	Indique l'état de la route : C = Connexion directe dans le même sous-réseau. S = Route statique. R = Route affectée par RIP (Routing Information Protocol). I = Route de redirection ICMP (Internet Control Message Protocol).
Network Address (Adresse réseau)	Adresse IP de destination.
Netmask (Masque de réseau)	Sous-réseau associé à la destination. Il s'agit d'un modèle qui identifie dans l'adresse de destination les bits d'adresse utilisés pour le routage vers des sous-réseaux particuliers. Chaque bit correspondant à un « 1 » fait partie du numéro de réseau/sous-réseau ; chaque bit correspondant à « 0 » fait partie du numéro d'hôte.
Gateway (Passerelle)	Adresse IP du routeur au tronçon suivant, vers lequel les trames correspondantes sont acheminées.
Interface	Interface locale à travers laquelle le tronçon suivant de cette route est atteint.

Paramètre	Description
Metric (Mesure)	Lorsqu'un routeur reçoit une mise à jour du routage qui contient une entrée réseau de destination nouvelle ou modifiée, il ajoute 1 à la valeur de mesure indiquée dans la mise à jour et entre le réseau dans la table de routage.

Remarque : la plupart des routeurs modernes supportent RIP-2, de sorte qu'une table de routage statique n'est habituellement pas nécessaire.

Firewall



Le firewall du routeur Barricade permet le contrôle d'accès des ordinateurs clients 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 le réseau.

Remarque : lorsque vous sélectionnez une case d'option de la zone « Enable or disable Firewall module function » (Activation ou désactivation des fonctions de firewall), assurez-vous de cliquer sur le bouton « APPLY » (Appliquer).

Access Control (Contrôle d'accès)

SMC Advanced Setup Home Logout

System
WAN
LAN
NAT
Routing system
Firewall
Access Control
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
SNMP
ADSL
Tools
Status

Access Control

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.

- Enable Filtering Function : Yes No
- Normal Filtering Table (up to 10 computers)

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure

Add PC

- MAC Filtering Table (up to 32 computers)

Rule Number	Client PC MAC Address										
	00	:	00	:	03	:	F1	:	F3	:	03
1	00	:	00	:	03	:	F1	:	F3	:	03
2	00	:	00	:	01	:	01	:	50	:	E7
3	00	:	00	:	00	:	00	:	00	:	00
4	00	:	00	:	00	:	00	:	00	:	00
5	00	:	00	:	00	:	00	:	00	:	00
6	00	:	00	:	00	:	00	:	00	:	00
7	00	:	00	:	00	:	00	:	00	:	00
8	00	:	00	:	00	:	00	:	00	:	00
9	00	:	00	:	00	:	00	:	00	:	00
10	00	:	00	:	00	:	00	:	00	:	00
11	00	:	00	:	00	:	00	:	00	:	00
12	00	:	00	:	00	:	00	:	00	:	00
13	00	:	00	:	00	:	00	:	00	:	00
14	00	:	00	:	00	:	00	:	00	:	00
15	00	:	00	:	00	:	00	:	00	:	00
16	00	:	00	:	00	:	00	:	00	:	00
17	00	:	00	:	00	:	00	:	00	:	00
18	00	:	00	:	00	:	00	:	00	:	00
19	00	:	00	:	00	:	00	:	00	:	00
20	00	:	00	:	00	:	00	:	00	:	00
21	00	:	00	:	00	:	00	:	00	:	00
22	00	:	00	:	00	:	00	:	00	:	00
23	00	:	00	:	00	:	00	:	00	:	00
24	00	:	00	:	00	:	00	:	00	:	00
25	00	:	00	:	00	:	00	:	00	:	00
26	00	:	00	:	00	:	00	:	00	:	00
26	00	:	00	:	00	:	00	:	00	:	00
27	00	:	00	:	00	:	00	:	00	:	00
28	00	:	00	:	00	:	00	:	00	:	00
29	00	:	00	:	00	:	00	:	00	:	00
30	00	:	00	:	00	:	00	:	00	:	00
31	00	:	00	:	00	:	00	:	00	:	00
32	00	:	00	:	00	:	00	:	00	:	00

HELP APPLY CANCEL

Cette fonction permet aux utilisateurs de définir le trafic sortant autorisé ou non autorisé par l'intermédiaire de l'interface WAN. Par défaut, tout le trafic sortant est autorisé. (Voir ci-après pour plus d'informations.)

Le routeur Barricade peut aussi limiter l'accès des systèmes hôtes dans le réseau local. La table de filtrage des adresses MAC (MAC Filtering Table) permet d'indiquer au routeur Barricade jusqu'à 32 adresses MAC dont l'accès au port WAN n'est pas autorisé.

L'écran « Access Control » (Contrôle d'accès) comporte les éléments suivants :

Paramètre	Description
Normal Filtering Table (Table de filtrage normal)	Affiche la table de filtrage des adresses IP (ou des gammes d'adresses IP).
MAC Filtering Table (Table de filtrage des adresses MAC)	Affiche la table de filtrage des adresses MAC (Media Access Control).

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).

Access Control (Contrôle d'accès) : Add PC (Ajouter un ordinateur)

The screenshot shows the 'Access Control Add PC' configuration page in the SMC Networks Advanced Setup. The page includes a navigation menu on the left, a main content area with configuration fields, a table of services, and a 'User Define Service' section.

Access Control Add PC

This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need config URL address first in "URL Blocking Site" page. For scheduling function, you also need config schedule rule first in "Schedule Rule" page.

- Client PC Description:
- Client PC IP Address: 192.168.2. -

Client PC Services:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3120, 8000, 8000, 8081	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input checked="" type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input checked="" type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	ADL Instant Messenger, TCP Port 5190	<input checked="" type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input checked="" type="checkbox"/>
SNMP	UDP Port 161, 162	<input checked="" 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"/>

User Define Service

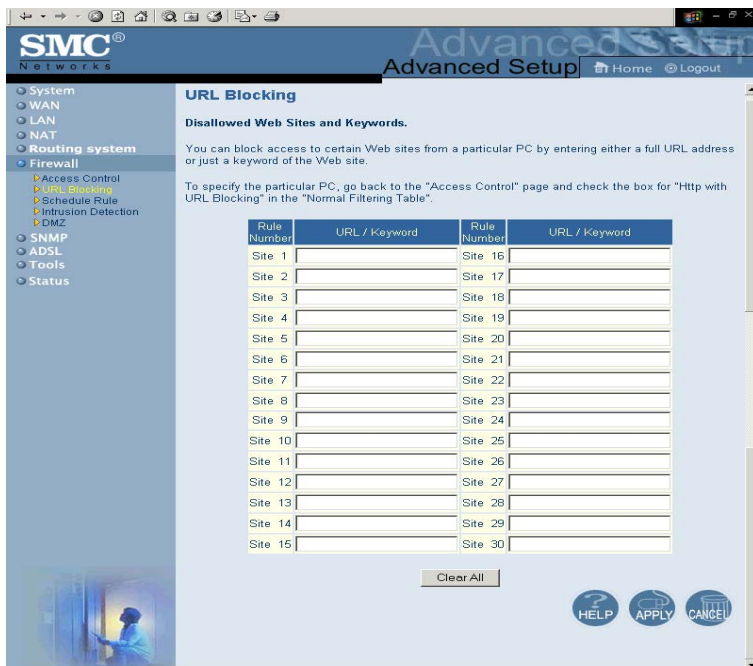
Protocol: TCP UDP

Port Range: - , - , - , -

Scheduling Rule (Ref. Schedule Rule Page):

Buttons:

URL Blocking (Blocage d'URL)



Le routeur Barricade permet à l'utilisateur de bloquer l'accès à des sites Web à partir d'un ordinateur particulier en entrant soit une adresse URL complète, soit seulement un mot-clé. Cette fonctionnalité peut être utilisée pour empêcher les enfants d'accéder à des sites Web violents ou à caractère pornographique.

Schedule Rule (Règle de planification)

SMC Networks Advanced Setup Home Logout

System
WAN
LAN
NAT
Routing system
Firewall
Access Control
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
SNMP
ADSL
Tools
Status

Schedule Rule

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

- Schedule Rule Table (up to 10 rules)

Rule Name	Rule Comment	Configure
Jim	temp	Edit Delete
Betty	consult Part time	Edit Delete

[Add Schedule Rule](#)

HELP APPLY CANCEL

Vous pouvez filtrer l'accès Internet pour des clients locaux en vous basant sur des règles.

Chaque règle de contrôle d'accès peut être activée à une heure planifiée. Définissez la planification sur la page « Schedule Rule » (Règle de planification) et appliquez la règle sur la page « Access Control » (Contrôle d'accès).

1. Cliquez sur « Add Schedule Rule » (Ajouter une règle de planification).
2. Définissez les paramètres appropriés pour une règle de planification (comme indiqué sur l'écran ci-après).

3. Cliquez sur « OK » puis sur « APPLY » (Appliquer) pour enregistrer vos paramètres.

Edit Schedule Rule

Name:

Comment:

Activate Time Period:

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

Intrusion Detection (Détection d'intrusion)

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, NAT, Routing system, Firewall (selected), Access Control, URL Blocking, Schedule Rule, Intrusion Detection (selected), DMZ, SNMP, ADSL, Tools, and Status. The main content area is titled "Intrusion Detection" and contains the following sections:

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 will support full operation as initiated from the local LAN.

The Barricade 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.

- **Enable SPI and Anti-DoS firewall protection:** Yes No
- **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"/>
- **Hacker Prevention Feature**

Discard Ping From WAN	<input type="checkbox"/>
RIP defect	<input checked="" type="checkbox"/>
- **When hackers attempt to enter your network, we can alert you by e-mail**

Your E-mail Address:

SMTP Server Address:

POP3 Server Address:

User name:

Password:
- **Connection Policy**

Fragmentation half-open wait: sec.

TCP SYN wait: sec.

TCP FIN wait: sec.

TCP connection idle timeout: sec.

UDP session idle timeout: sec.

H.323 data channel idle timeout: sec.
- **DoS Detect Criteria:**

Total incomplete TCP/UDP sessions HIGH: session

Total incomplete TCP/UDP sessions LOW: session

Incomplete TCP/UDP sessions (per min) HIGH: session

Incomplete TCP/UDP sessions (per min) LOW: session

Maximum incomplete TCP/UDP sessions number from same host:

Incomplete TCP/UDP sessions detect sensitive time period: msec.

Maximum half-open fragmentation packet number from same host:

Half-open fragmentation detect sensitive time period: msec.

Flooding cracker block time: sec.

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

Le firewall du routeur Barricade inspecte les paquets au niveau de la couche Application et enregistre des informations concernant les sessions TCP et UDP, parmi lesquelles les délais d'attente et le nombre de sessions actives. Il permet également de détecter et d'empêcher certains types d'attaques réseau, tels que les attaques par refus de service.

Les attaques réseau qui refusent l'accès à un périphérique réseau sont appelées « attaques par refus de service ». Les attaques de ce type visent les périphériques et les réseaux connectés à Internet. Leur objectif n'est pas de dérober des informations, mais de désactiver un périphérique ou un réseau afin d'empêcher les utilisateurs d'accéder à des ressources réseau.

Le routeur Barricade vous protège contre les attaques par refus de service suivantes : Ping of Death (inondation Ping), inondation SYN (SYN flooding), fragment IP (Teardrop Attack), Brute-force Attack, Land Attack, usurpation d'adresse IP (IP Spoofing), IP de taille nulle (IP with zero length), scannage nul TCP (TCP null scan), bouclage de port UDP (UDP port loopback), Snork Attack, etc.

Remarque : le firewall n'a que peu d'impact sur les performances du système ; il est donc conseillé d'activer les fonctions de prévention afin de protéger votre réseau.

Paramètre	Valeur par défaut	Description
Enable SPI and Anti-DoS firewall protection (Activer la protection SPI et anti-refus de service par firewall)	Yes (Oui)	La fonction de détection d'intrusion du routeur Barricade 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 en haut de l'écran.

Paramètre	Valeur par défaut	Description
Stateful Packet Inspection		<p>Cette option vous permet de sélectionner différents types d'application faisant appel à des numéros de port dynamiques. Si vous souhaitez utiliser la fonction SPI (Stateful Packet Inspection) 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 de paquet, la connexion TCP, la session UDP, le service FTP, le service H.323 ou le service TFTP.</p> <p>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 de la 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.</p> <p>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.</p>

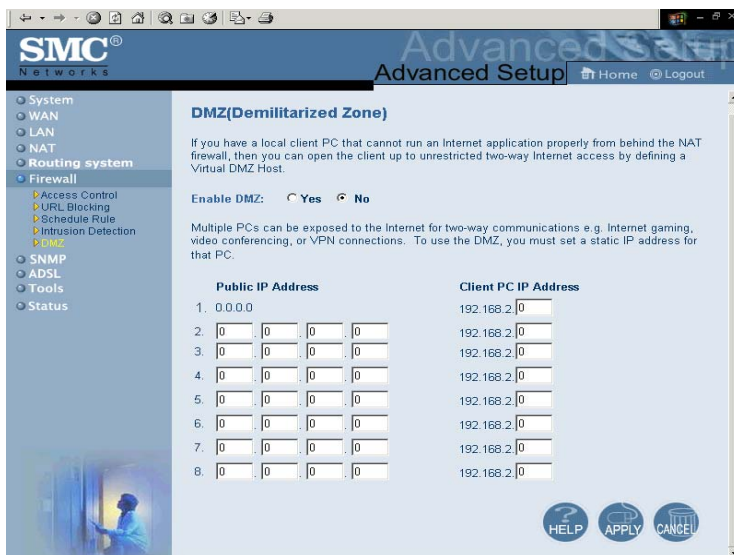
Paramètre	Valeur par défaut	Description
Fonction de protection contre les attaques extérieures		
Discard Ping from WAN (Rejeter les Ping à partir du réseau étendu)	Discard (Rejeter)	Empêche l'acheminement vers le réseau d'un PING sur le port WAN de la passerelle.
RIP Defect (Défaut RIP)	Enabled (Activé)	Si le routeur ne répond pas à un paquet de requête IPX 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.
Lorsque des pirates tentent de s'introduire dans votre réseau, nous pouvons vous avertir par e-mail		
Your E-Mail Address (Votre adresse e-mail)		Entrez votre adresse e-mail.
SMTP Server Address (Adresse du serveur SMTP)		Entrez l'adresse de votre serveur SMTP (il s'agit généralement de la partie de l'adresse e-mail qui suit le symbole « @ »).
POP3 Server Address (Adresse du serveur POP3)		Entrez l'adresse de votre serveur POP3 (il s'agit généralement de la partie de l'adresse e-mail qui suit le symbole « @ »).
User Name (Nom d'utilisateur)		Entrez le nom d'utilisateur de votre compte de messagerie électronique.
Password (Mot de passe)		Entrez le mot de passe de votre compte de messagerie électronique.

Paramètre	Valeur par défaut	Description
Politique de connexion		
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 qu'une session TCP atteigne un état stable avant de l'abandonner.
TCP FIN wait (Attente TCP FIN)	5 sec	Indique le temps pendant lequel une session TCP est gérée après la détection d'un échange 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 gérée en l'absence d'activité.
UDP session idle timeout (Délai d'inactivité de session UDP)	30 sec	Temps pendant lequel une session UDP est gérée 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 gérée en l'absence d'activité.

Paramètre	Valeur par défaut	Description
DoS Detect Criteria (Critères de détection de refus de service)		
Total incomplete TCP/UDP sessions HIGH (Nombre total de sessions TCP/UDP incomplètes SEUIL HAUT)	300 sessions	Définit le nombre de nouvelles sessions 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 nouvelles sessions 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	Affectez à ce paramètre la valeur 0, car aucune valeur minimale n'est obligatoire et l'affectation d'une valeur plus élevée aurait un impact négatif sur les performances.
Maximum incomplete TCP/UDP sessions number from same host (Nombre maximal de sessions TCP/UDP incomplètes à partir du même hôte)	10	Nombre maximal de sessions TCP/UDP incomplètes à partir du même hôte.

Paramètre	Valeur par défaut	Description
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)	10 000 msec	Temps nécessaire avant qu'une session de fragmentation à moitié ouverte ne soit détectée comme telle.
Flooding cracker block time (Délai du craquage d'inondation)	300 sec	Délai entre la détection d'une attaque de type inondation et le blocage de cette attaque.

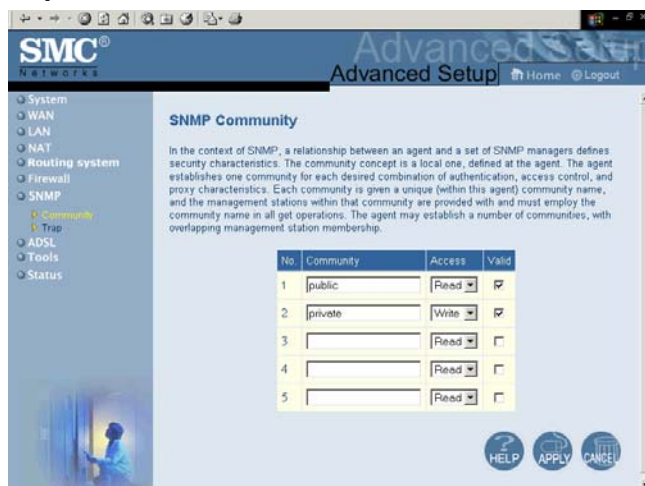
DMZ



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

SNMP

Community (Communauté)

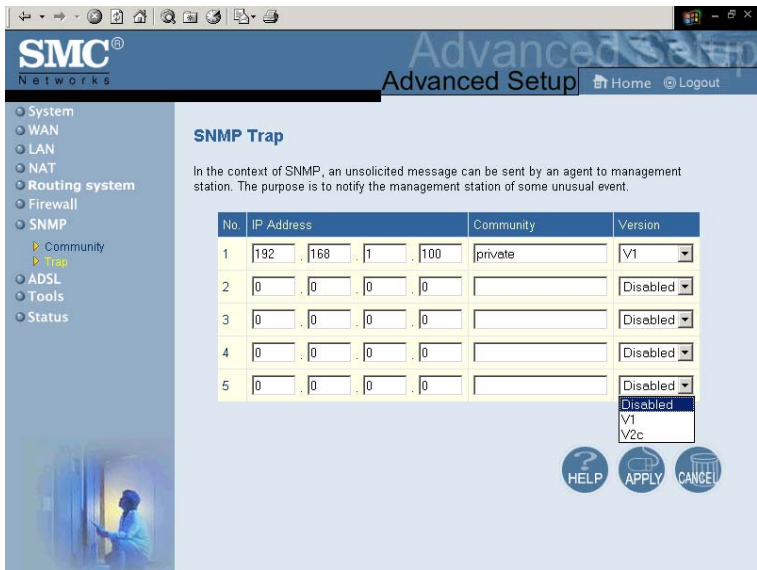


Utilisez l'écran de configuration SNMP pour afficher et modifier les paramètres du protocole SNMP (Simple Network Management Protocol). Pour accéder à ces informations, il est possible d'utiliser un ordinateur connecté au réseau, appelé NMS (Network Management Station). Les droits d'accès à l'agent sont contrôlés par les chaînes de communauté. Pour communiquer avec le routeur Barricade, le NMS doit d'abord soumettre une chaîne de communauté valide pour authentification.

Paramètre	Description
Community (Communauté)	Un nom de communauté autorisé pour l'accès aux fonctions d'administration.
Access (Accès)	L'accès aux fonctions d'administration est limité à Read only (Lecture seule) ou Read/ Write (Lecture/écriture).
Valid (Valide)	Active ou désactive l'entrée.

Remarque : il est possible d'indiquer jusqu'à 5 noms de communauté.

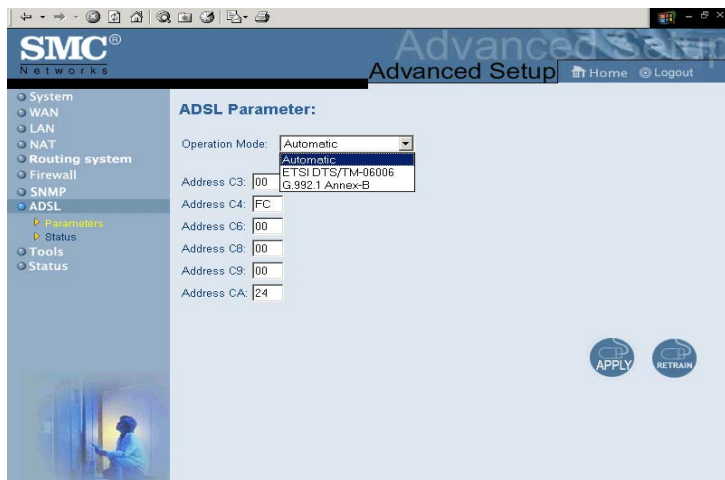
Trap (Interception)



Paramètre	Description
IP Address (Adresse IP)	Les interceptions sont envoyées à cette adresse lorsque des erreurs ou des événements particuliers se produisent dans le réseau.
Community (Communauté)	Chaîne de communauté (mot de passe) spécifiée pour la gestion des interceptions. Entrez un mot, autre que public ou private, pour empêcher des personnes non autorisées de lire des informations dans votre système.
Version	Définit l'état d'interception de l'entrée à « Disabled » (Désactivée) ou « Enabled » (Activée) avec V1 ou V2c. Le protocole v2c a été introduit fin 1995 et inclut des améliorations de la v1 qui sont universellement acceptées. Parmi ces améliorations figurent une commande de rapatriement en bloc pour réduire le trafic d'administration réseau lors de la lecture d'une séquence de variables MIB, et un ensemble plus élaboré de codes d'erreur pour une meilleure génération d'états sur une station d'administration réseau.

ADSL

Parameters (Paramètres ADSL)



Paramètre	Description
Operation Mode (Mode de fonctionnement)	<ul style="list-style-type: none"> Automatic (Automatique) ETSI DTS/TM-06006 standard (Norme ETSI DTS/TM-06006) G.992.1 standard (Norme G.992.1)
Address 3C (Adresse 3C), etc.	Réservés.

Status (État)

SMC®
NETWORKS

Advanced Setup Home Logout

- System
- WAN
- LAN
- NAT
- Routing system
- Firewall
- SNMP
- ADSL
 - Parameters
 - Status
- Tools
- Status

Monitoring Index:

- ADSL Status Information:
 - Status.
 - Data Rate Information.
 - Defect/Failure Indication.
 - Statistics.

ADSL Status Information:

- Status:

Line Status	Configured	Current
---	---	Activating

 - [Go Top]
- Data Rate:

Stream Type	Interleaved Channel Data Rate	Fast Channel Data Rate
Up Stream	0 (Kbps.)	0 (Kbps.)
Down Stream	0 (Kbps.)	0 (Kbps.)

 - [Go Top]
- Operation Data / Defect Indication:

Operation Data	Upstream	Downstream
Noise Margin	-0.5 dB	-0.5 dB
Output Power	-0.5 dBm	-0.5 dBm
Attenuation	-0.5 dB	-0.5 dB

Indicator Name	Near End Indicator	Far End Indicator
Fast Path FEC Correction	65535	65535
Interleaved Path FEC Correction	65535	65535
Fast Path CRC Error	65535	65535
Interleaved Path CRC Error	65535	65535
Loss of Signal Defect	---	---
Loss of Frame Defect	---	---
Loss of Power Defect	---	---
Fast Path HEC Error	65535	65535
Interleaved Path HEC Error	65535	65535

 - [Go Top]
- Statistics:

Received Superframes Interleaved	0
Transmitted Superframes Interleaved	0
Received Superframes Fast	0
Transmitted Superframes Fast	0

 - [Go Top]

HELP

Paramètre	Description
Status (État)	
Line Status (État de la ligne)	Montre l'état en cours de la ligne ADSL.
Débit	
Upstream (Émission)	Débit réel et maximal en émission.
Downstream (Réception)	Débit réel et maximal en réception.
Operation Data/Defect Indication (Données de fonctionnement/indication de défaut)	
Noise Margin (Marge de bruit)	
	Émission : Marge de bruit minimale en émission.
	Downstream (Réception) : Marge de bruit minimale en réception.
Output Power (Puissance de sortie)	Fluctuation maximale de la puissance de sortie.
Attenuation (Atténuation)	
	Émission : Réduction maximale de la puissance du signal d'émission.
	Downstream (Réception) : Réduction maximale de la puissance du signal de réception.
Fast Path FEC Correction (Correction FEC rapide)	Vous pouvez utiliser deux voies d'attente : fast (rapide) et interleaved (entrelacée). Pour chaque voie, un système de correction d'erreur direct (Forward Error Correction, FEC) est employé pour garantir une meilleure intégrité des données. Pour une immunité maximale contre le bruit, le système FEC peut être complété par un entrelaceur.

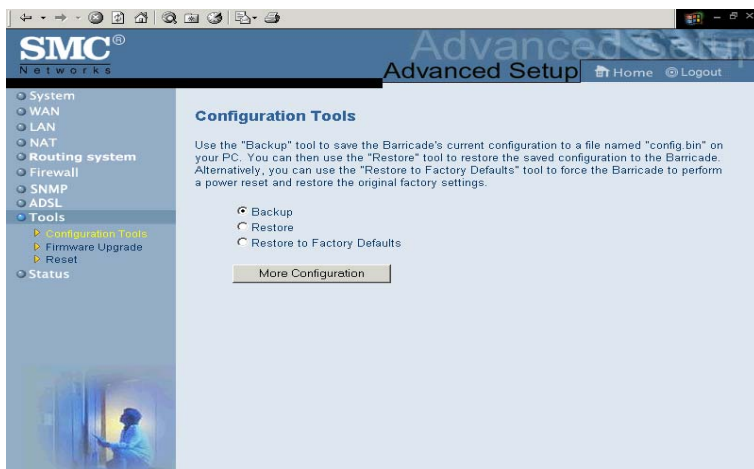
Paramètre	Description
Interleaved Path FEC Correction (Correction FEC entrelacée)	Un entrelaceur est essentiellement un tampon utilisé pour introduire un retard, afin de permettre à des techniques de correction d'erreurs supplémentaires de gérer le bruit. L'entrelacement ralentit le flux des données et peut ne pas être optimal pour les signaux temps réel tels que la transmission vidéo.
Fast Path CRC Error (Erreur de CRC rapide)	Indique le nombre d'erreurs de contrôle de redondance cyclique rapides.
Interleaved Path CRC Error (Erreur de CRC entrelacée)	Indique le nombre d'erreurs de contrôle de redondance cyclique entrelacées.
Loss of Signal Defect (Défaut de perte du signal)	Discontinuités momentanées du signal.
Loss of Frame Defect (Défaut de perte de trames)	Défaillances dues à des pertes de trames.
Loss of Power Defect (Défaut de perte d'alimentation)	Défaillances dues à une perte d'alimentation.
Fast Path HEC Error (Erreur HEC rapide)	Erreur de dissimulation d'erreurs d'en-têtes rapides.
Interleaved Path HEC Error (Erreur HEC entrelacée)	Erreur de dissimulation d'erreurs d'en-têtes entrelacées.
Statistics (Statistiques)	Les supertrames représentent le niveau le plus haut de la présentation des données. Chaque supertrame contient des trames ADSL normales, et l'une d'elles est utilisée pour fournir la synchronisation de la supertrame, identifiant le début d'une supertrame. Certaines autres trames sont également utilisées pour des fonctions spéciales.

Paramètre	Description
Received Superframes Interleaved (Superframes reçues entrelacées)	Nombre de supertrames entrelacées reçues.
Transmitted Superframes Interleaved (Superframes émises entrelacées)	Nombre de supertrames entrelacées émises.
Received Superframes Fast (Superframes reçues rapides)	Nombre de supertrames rapides reçues.
Transmitted Superframes Fast (Superframes émises rapides)	Nombre de supertrames rapides émises.

Tools (Outils)

Utilisez le menu « Tools » (Outils) pour sauvegarder la configuration actuelle, restaurer une configuration précédemment enregistrée ou restaurer les paramètres par défaut.

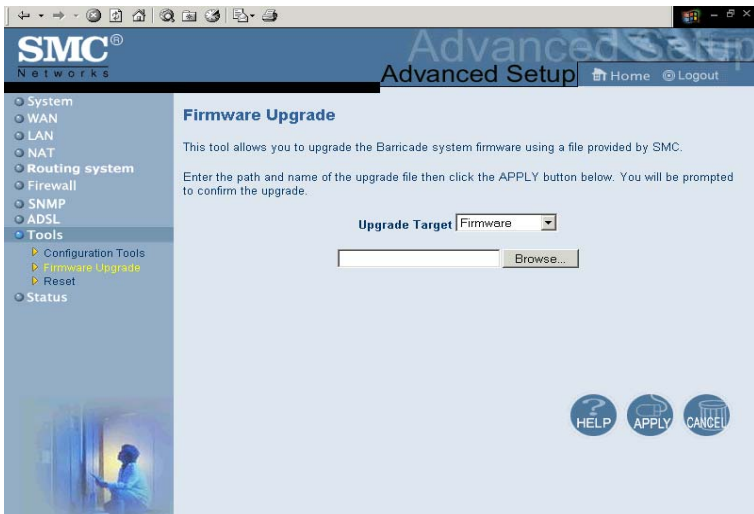
Configuration Tools (Outils de configuration)



Activez la case à cocher « Backup » (Sauvegarde) et cliquez sur « More Configuration » (Configuration supplémentaire) pour sauvegarder la configuration de votre routeur Barricade dans un fichier nommé config.bin sur votre ordinateur. Vous pouvez ensuite cliquer sur la case d'option « Restore » (Restaurer) puis sur « More Configuration » pour restaurer ce fichier.

Pour restaurer les paramètres par défaut, activez « Restore to Factory Defaults » (Restaurer les valeurs par défaut) puis cliquez sur « More Configuration » (Configuration supplémentaire). Un message vous demandera de confirmer votre décision.

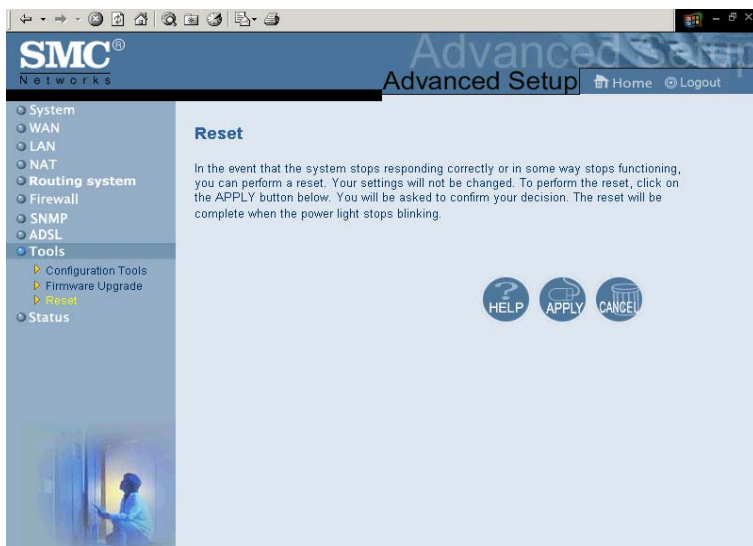
Firmware Upgrade (Mise à niveau du logiciel)



Utilisez cet écran pour mettre à jour le logiciel ou l'interface utilisateur. Dans la zone « Upgrade Target » (Mettre à jour la cible), choisissez « Firmware » (Logiciel) ou « User Interface » (Interface utilisateur) en fonction de ce que vous voulez mettre à jour. Cliquez ensuite sur « Browse » (Parcourir) pour localiser le fichier préalablement téléchargé.

Remarque : pour obtenir des informations sur la dernière version du logiciel ou de l'interface utilisateur et la télécharger, visitez le site Web de SMC à l'adresse www.smc.com ou www.smc-europe.com.

Reset (Réinitialisation)



Cette page permet d'effectuer une réinitialisation. Les paramètres de configuration ne sont pas rétablis à leurs valeurs par défaut.

Remarque : lorsque vous appuyez sur le bouton de réinitialisation sur le panneau arrière, le routeur Barricade effectue une réinitialisation au niveau de l'alimentation et les valeurs par défaut sont restaurées.

Status (État)

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

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, NAT, Routing system, Firewall, SNMP, ADSL, Tools, and Status (selected). The main content area is titled 'Status' and includes the following information:

Current Time: 01/01/1970 01:29:26

INTERNET	GATEWAY	INFORMATION
Cable/DSL: CONNECTED	IP Address: 192.168.2.1	Numbers of DHCP Clients: 1
WAN IP: 192.168.3.2	Subnet Mask: 255.255.255.0	Runtime Code Version: 0.52 (Apr 15 2002 10:53:20)
Subnet Mask: 255.255.255.0	DHCP Server: Enabled	Boot Code Version: V1.12
Gateway: 0.0.0.0	Firewall: Enabled	LAN MAC Address: 00-70-46-00-00-01
Primary DNS: 168.95.1.1		WAN MAC Address: 00-70-46-00-00-02
Secondary DNS: 0.0.0.0		Hardware Version: 01
		Serial Num: A00000001

Below the status information, there are two log sections:

- Security Log:** View any attempts that have been made to gain access to your network. The log table shows the following entries:

Date	Time	IP
01/01/1970	03:10:02	192.168.2.1
01/01/1970	02:37:41	192.168.2.1
01/01/1970	01:09:02	192.168.2.1
01/01/1970	00:48:39	192.168.2.1
01/01/1970	00:01:58	192.168.2.1
- DHCP Client Log:** View information on LAN DHCP clients currently linked to the HomeGateway. The log table shows the following entry:

IP	MAC
ip=192.168.2.101	mac=00-10-B5-

At the bottom of the logs, there are 'Save', 'Clear', and 'Refresh' buttons. The bottom right corner of the page features 'HELP', 'BACK', and 'CANCEL' buttons.

Vous pouvez enregistrer le journal de sécurité dans un fichier en cliquant sur « Save » (Enregistrer) puis en choisissant un emplacement.

Cet écran comporte les éléments suivants :

Paramètre	Description
INTERNET	Affiche le type et l'état de la connexion WAN.
GATEWAY	Affiche les paramètres IP du système ainsi que l'état du serveur 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 et du routeur Barricade, ainsi que les numéros de version et de série du matériel.
Security Log (Journal de sécurité)	Affiche les tentatives non autorisées d'accès à votre réseau.
DHCP Client Log (Journal des clients DHCP)	Affiche des informations concernant les clients DHCP présents dans votre réseau.

CHAPITRE 5

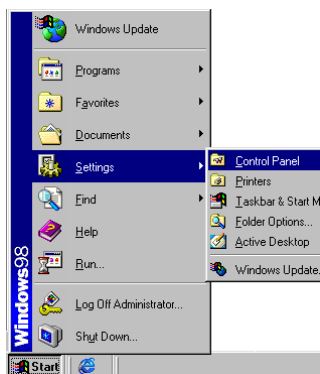
CONFIGURATION DE TCP/IP

CLIENT

Après avoir procédé à l'installation matérielle en connectant tous vos périphériques réseau, vous devez configurer votre ordinateur pour la connexion au routeur Barricade. Déterminez d'abord de quelle manière votre Fournisseur d'Accès Internet vous fournit votre adresse IP. De nombreux Fournisseurs d'Accès Internet définissent ces numéros automatiquement en se servant du protocole DHCP (*Dynamic Host Configuration Protocol*). D'autres fournissent une adresse IP statique et des numéros associés, que vous devez entrer manuellement. La manière dont votre Fournisseur d'Accès Internet affecte votre adresse IP déterminera comment vous devrez configurer votre ordinateur. Consultez la section ci-après pour la configuration sous Windows 95/98/Me. Consultez la section « Windows NT 4.0 » à la page 5-9, « Windows 2000 » à la page 5-14, « Windows XP » à la page 5-19, ou « Configuration de votre ordinateur Macintosh » à la page 5-24, selon votre système d'exploitation.

Windows 95/98/Me

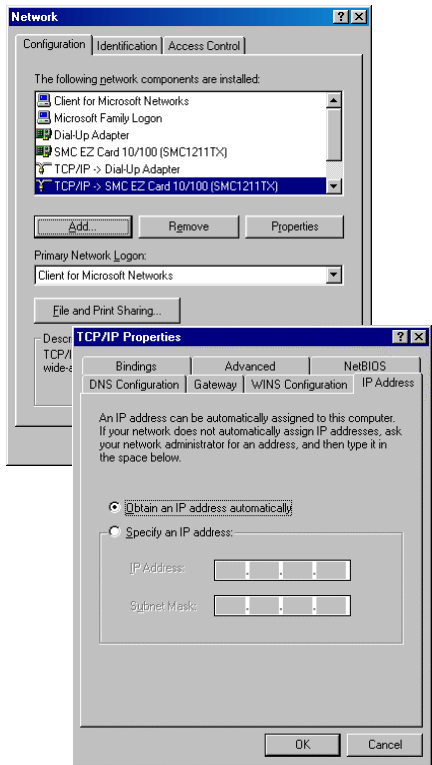
Il se peut que les instructions communiquées dans la présente section ne correspondent pas exactement à votre version de Windows. Cela est dû au fait que les instructions et les écrans sont basés sur Windows 98. Windows 95 et Windows Millenium Edition sont très similaires, mais pas totalement identiques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



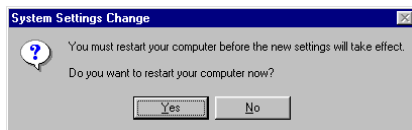
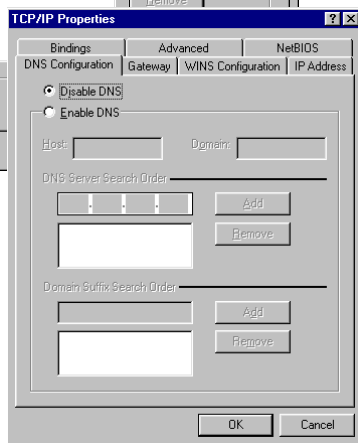
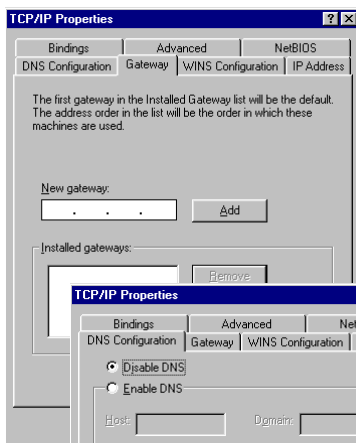
1. Depuis le Bureau Windows, cliquez sur le bouton « Start » (Démarrer). Choisissez « Settings » (Paramètres), puis cliquez sur « Control Panel » (Panneau de configuration).
2. Dans le Panneau de configuration, double-cliquez sur l'icône « Network » (Réseau).



3. Dans la fenêtre « Network » (Réseau), sous l'onglet « Configuration », double-cliquez sur l'élément « TCP/IP » affiché pour votre carte réseau.
4. Activez l'onglet « IP Address » (Adresse IP).
5. Si l'option « Obtain an IP address automatically » (Obtenir automatiquement une adresse IP) est sélectionnée, votre ordinateur est déjà configuré pour DHCP. Cliquez sur « Cancel » (Annuler) pour fermer chaque fenêtre et passez à la section « Désactivation du proxy HTTP » à la page 5-5. Sinon, recherchez votre adresse IP et votre masque de sous-réseau. Notez ces valeurs sur les lignes ci-après.



6. Cliquez sur l'onglet « Gateway » (Passerelle) et notez les numéros affichés sous « Installed gateways » (Passerelles installées).
7. Cliquez sur l'onglet « DNS Configuration » (Configuration DNS). Consultez les serveurs DNS présents dans la liste « DNS Server Search Order » (Ordre de recherche DNS). Notez les éventuelles adresses présentes.
8. Après avoir noté vos paramètres, contrôlez-les une fois de plus pour vous assurer que vos notes sont correctes. Cliquez sur l'onglet « IP Address » (Adresse IP), puis sur « Obtain an IP address automatically » (Obtenir automatiquement une adresse IP). Cliquez sur « OK ».



9. Il est possible que votre système Windows ait besoin du CD-ROM de Windows 95/98/Me pour copier certains fichiers. Une fois la copie effectuée, vous êtes invité à redémarrer votre système. Cliquez sur « Yes » (Oui) ; votre ordinateur redémarre.

Paramètres de configuration TCP/IP

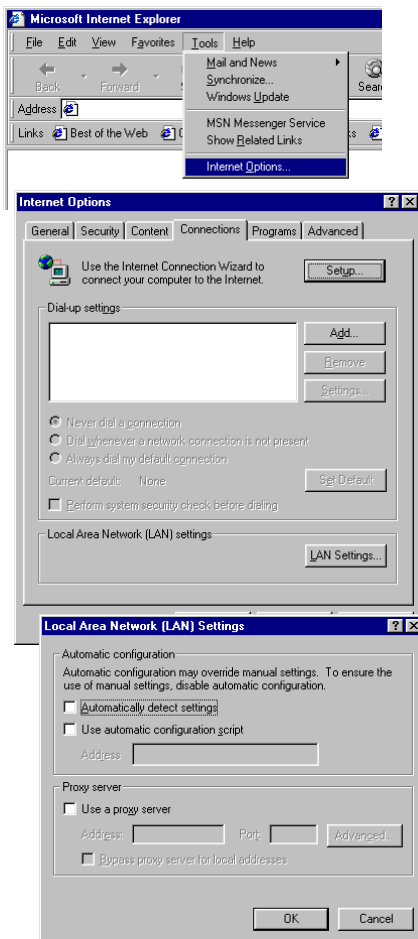
Adresse IP _____.____.____.____
Masque de sous-réseau _____.____.____.____
Serveur DNS principal _____.____.____.____
Serveur DNS secondaire _____.____.____.____
Passerelle par défaut _____.____.____.____
Nom de système hôte _____.____.____.____

Désactivation du proxy HTTP

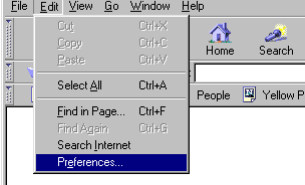
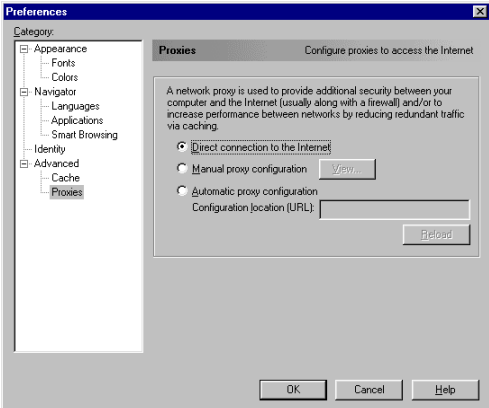
Vous devez vérifier que la fonctionnalité « Proxy HTTP » de votre serveur Web est désactivée pour que votre navigateur puisse afficher les pages de configuration HTML du routeur Barricade. Les étapes suivantes concernent Internet Explorer et Netscape. Déterminez le navigateur utilisé et suivez les étapes appropriées.

Internet Explorer

1. Ouvrez Internet Explorer et cliquez sur le bouton « Stop » (Arrêter). Cliquez sur « Tools » (Outils), puis sur « Internet Options » (Options Internet).
2. Dans la fenêtre qui s'affiche, cliquez sur l'onglet « Connections » (Connexions). Cliquez ensuite sur le bouton « LAN Settings... » (Paramètres LAN).
3. Désactivez toutes les cases à cocher.
4. Cliquez sur « OK », puis de nouveau sur « OK » pour fermer la fenêtre « Internet Options » (Options Internet).



Netscape

1. Ouvrez Netscape et cliquez sur le bouton « Stop » (Arrêter). Cliquez sur « Edit » (Edition), puis sur « Preferences... » (Préférences).
- 
- The screenshot shows the Netscape application window with the menu bar open. The 'Edit' menu is selected, and 'Preferences...' is highlighted at the bottom of the menu. Other visible options include Cut, Copy, Paste, Select All, Find in Page..., Find Again, Search Internet, Home, Search, People, and Yellow P.
2. Dans la fenêtre qui s'affiche, sous « Category », double-cliquez sur « Advanced » (Avancées), puis cliquez sur « Proxies » (Proxy). Sélectionnez « Direct connection to the Internet » (Connexion directe à Internet). Cliquez sur « OK ».
- 
- The screenshot shows the 'Preferences' dialog box with the 'Proxies' tab selected. The 'Category' list on the left shows 'Advanced' and 'Proxies' selected. The 'Proxies' section has three radio buttons: 'Direct connection to the Internet' (selected), 'Manual proxy configuration', and 'Automatic proxy configuration'. There is a 'View...' button next to 'Manual proxy configuration' and a 'Reload' button below the 'Automatic proxy configuration' section. The 'Configuration location (URL):' field is empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.
3. Répétez ces étapes pour tous les ordinateurs Windows 95/98/Me connectés à votre routeur Barricade.

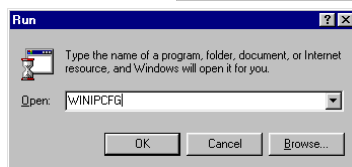
Lecture des paramètres IP depuis votre routeur ADSL

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

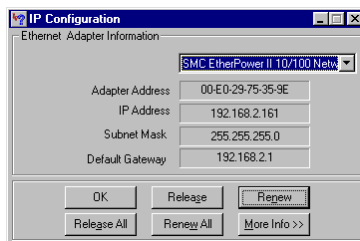
1. Cliquez sur « Start » (Démarrer), puis sur « Run » (Exécuter).



2. Tapez « WINIPCFG », puis cliquez sur « OK ». L'affichage de la fenêtre « IP Configuration » (Configuration IP) peut nécessiter de une à deux secondes.



3. 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**



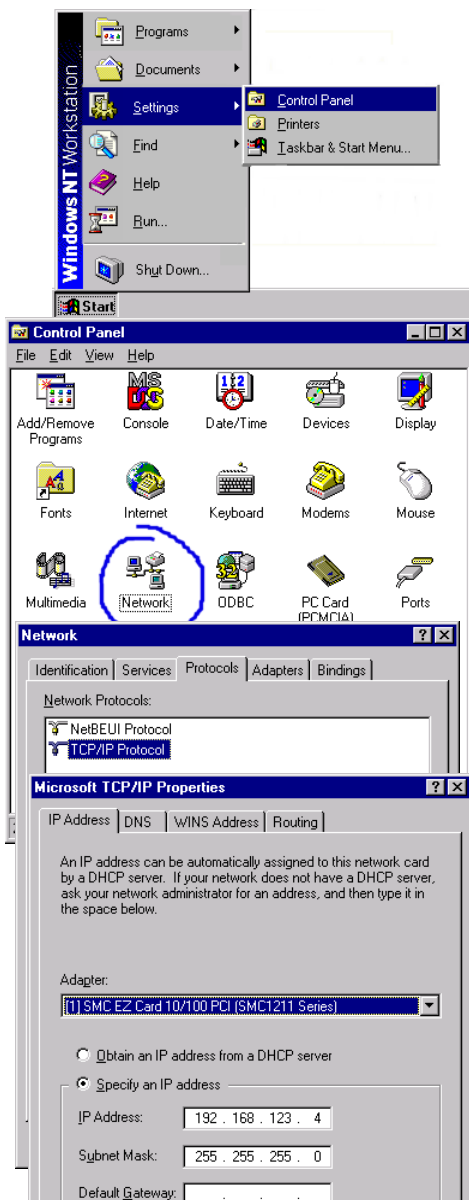
et votre passerelle par défaut **192.168.2.1**. Ces valeurs attestent du fonctionnement de votre routeur Barricade. Cliquez sur « OK » pour fermer la fenêtre « IP Configuration » (Configuration IP).

Windows NT 4.0

Après avoir procédé à l'installation matérielle en connectant vos périphériques réseau, vous devez configurer votre ordinateur pour la connexion au routeur Barricade. Déterminez d'abord de quelle manière votre Fournisseur d'Accès Internet vous fournit votre adresse IP. De nombreux Fournisseurs d'Accès Internet définissent ces numéros automatiquement en se servant du protocole DHCP (*Dynamic Host Configuration Protocol*). D'autres fournissent une adresse IP statique et des numéros associés, que vous devez entrer manuellement. La manière dont votre Fournisseur d'Accès Internet affecte votre adresse IP déterminera comment vous devrez configurer votre ordinateur.

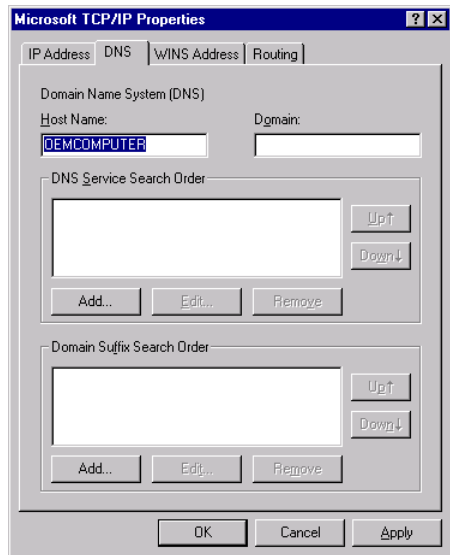
Procédez comme suit :

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. Sélectionnez l'onglet « Protocols » (Protocoles).
4. Double-cliquez sur « TCP/IP Protocol » (Protocole TCP/IP).
5. Activez l'onglet « IP Address » (Adresse IP).
6. Dans la liste déroulante des cartes, assurez-vous que votre carte Ethernet est sélectionnée.
7. Si l'option « Obtain an IP address automatically »



(Obtenir automatiquement une adresse IP) est sélectionnée, votre ordinateur est déjà configuré pour DHCP. Cliquez sur « Cancel » (Annuler) pour fermer chaque fenêtre et passez à la section « Désactivation du proxy HTTP » à la page 5-12.

8. Dans la boîte de dialogue « TCP/IP Properties » (Propriétés TCP/IP), sous l'onglet « IP address » (Adresse IP), repérez votre adresse IP, votre masque de sous-réseau et votre passerelle par défaut. Notez ces valeurs sur les lignes ci-après.
9. Cliquez sur l'onglet « DNS » pour voir quels sont les serveurs DNS principal et secondaire. Notez ces valeurs sur les lignes ci-après.
10. Après avoir noté vos paramètres IP, cliquez sur l'onglet « IP address » (Adresse IP). Sélectionnez « Obtain IP address automatically » (Obtenir automatiquement une adresse IP), puis cliquez sur « OK ». Cliquez de nouveau sur « OK » pour fermer la fenêtre « Network » (Réseau).



11. Windows peut alors copier certains fichiers et vous demander de redémarrer votre système. Cliquez sur « Yes » (Oui) ; votre ordinateur redémarre.

Paramètres de configuration TCP/IP

Adresse IP _____.____.____.____
Masque de sous-réseau _____.____.____.____
Passerelle par défaut _____.____.____.____
Serveur DNS principal _____.____.____.____
Serveur DNS secondaire _____.____.____.____
Nom de système hôte _____.____.____.____

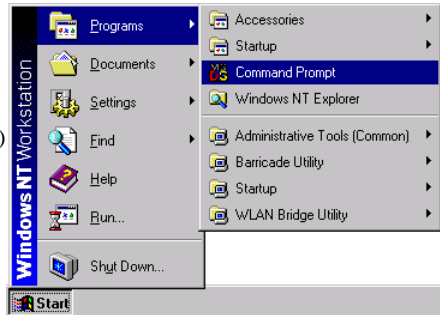
Désactivation du proxy HTTP

Vous devez vérifier que la fonctionnalité « Proxy HTTP » de votre serveur Web est désactivée pour que votre navigateur puisse afficher les pages de configuration HTML du routeur Barricade. Déterminez quel est le navigateur utilisé et reportez-vous à la section « Internet Explorer » à la page 5-6 ou « Netscape » à la page 5-7.

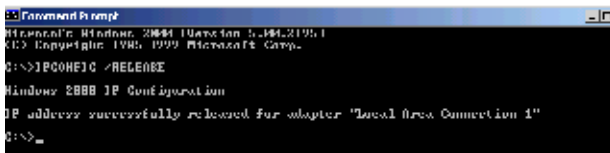
Lecture des paramètres IP depuis votre routeur Barricade

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

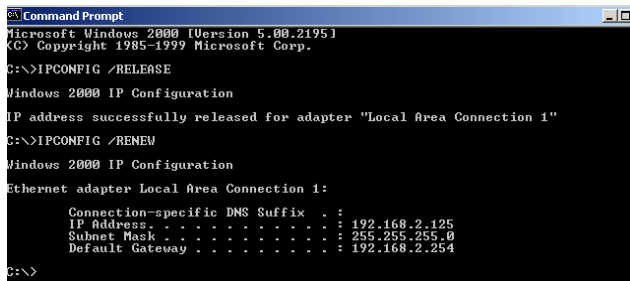
1. Depuis le Bureau Windows, cliquez sur « Start/Programs/ » (Démarrer/Programmes/) puis sur « Command Prompt » (Invite de commandes).



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



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 de votre routeur Barricade.

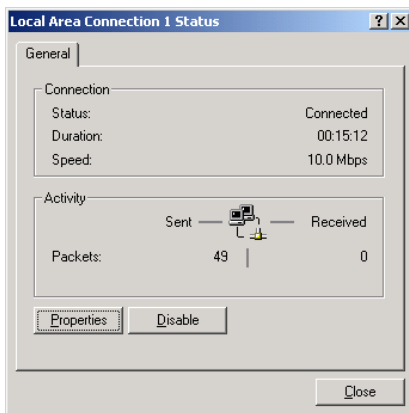
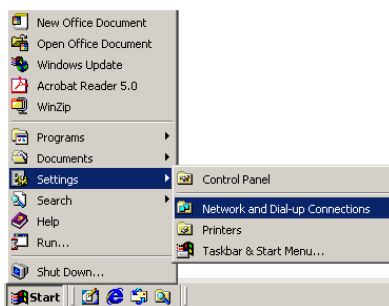


4. Tapez « EXIT » et appuyez sur <ENTRÉE> pour fermer la fenêtre « Command Prompt » (Invite de commandes).

Votre ordinateur est maintenant configuré pour la connexion au routeur Barricade.

Windows 2000

1. Depuis le Bureau Windows, cliquez sur « Start/Settings/Network and Dial-Up Connections » (Démarrer/Paramètres/Connexions réseau et accès à distance).
2. Cliquez sur l'icône correspondant à la connexion à votre routeur Barricade.
3. L'écran d'état de la connexion s'ouvre. Cliquez sur « Properties » (Propriétés).

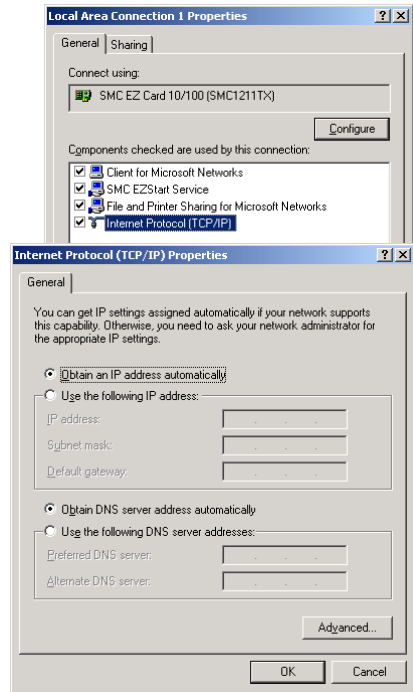


4. Double-cliquez sur « Internet Protocol (TCP/IP) » (Protocole Internet (TCP/IP)).

5. S'il existe des informations d'adresse IP dans la boîte de dialogue « Internet Protocol (TCP/IP) Properties » (Propriétés de Protocole Internet (TCP/IP)), elles doivent être notées. Utilisez pour cela les lignes ci-après.

6. Si les options « Obtain an IP address automatically » (Obtenir une adresse IP automatiquement) et « Obtain DNS server address automatically »

(Obtenir les adresses des serveurs DNS automatiquement) sont sélectionnées, votre ordinateur est déjà configuré pour DHCP. Cliquez sur « Cancel » (Annuler) pour fermer chaque fenêtre et passez à la section « Désactivation du proxy HTTP » à la page 5-16.



7. Activez l'option « Obtain an IP address automatically » (Obtenir une adresse IP automatiquement), puis « Obtain DNS server address automatically » (Obtenir les adresses des serveurs DNS automatiquement). Cliquez sur « OK » ou « Close » (Fermer) pour fermer chaque fenêtre.

Paramètres de configuration TCP/IP

Adresse IP _____
Masque de sous-réseau _____
Passerelle par défaut _____
Serveur DNS préféré _____
Serveur DNS auxiliaire _____

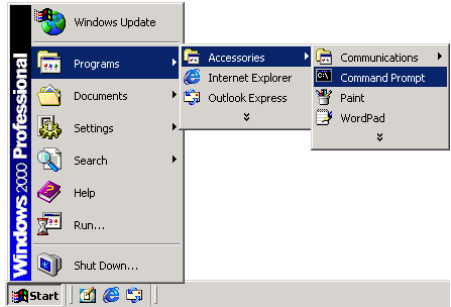
Désactivation du proxy HTTP

Vous devez vérifier que la fonctionnalité « Proxy HTTP » de votre serveur Web est désactivée pour que votre navigateur puisse afficher les pages de configuration HTML du routeur Barricade. Déterminez quel est le navigateur utilisé et reportez-vous à la section « Internet Explorer » à la page 5-6 ou « Netscape » à la page 5-7.

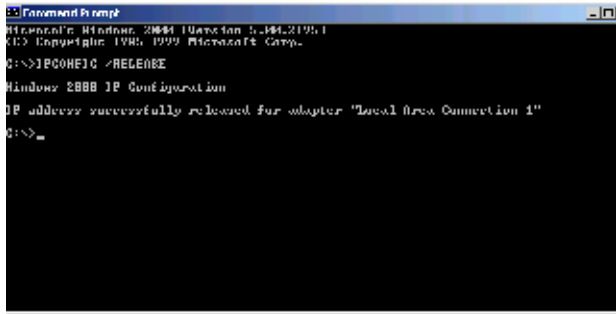
Lecture des paramètres IP depuis votre routeur Barricade

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

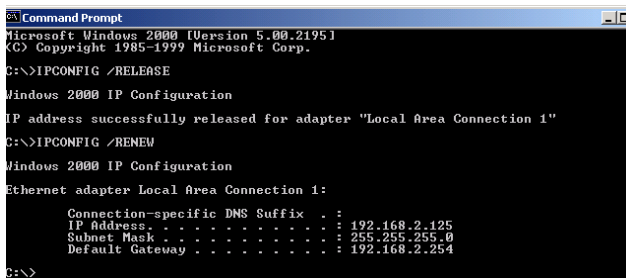
1. Depuis le Bureau Windows, cliquez sur « Start/Programs/ Accessoires » (Démarrer/ Programmes/ Accessoires) puis sur « Command Prompt » (Invite de commandes).



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



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 de votre routeur ADSL.



```
Command Prompt
Microsoft Windows [Version 5.00.2195]
(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

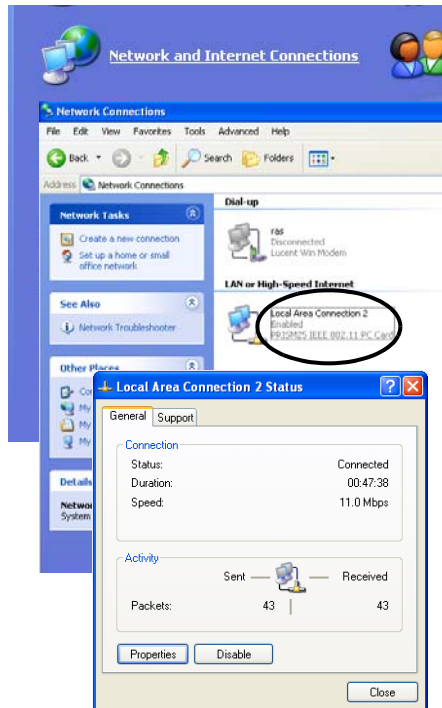
C:\>
```

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

Votre ordinateur est maintenant configuré pour la connexion au routeur Barricade.

Windows XP

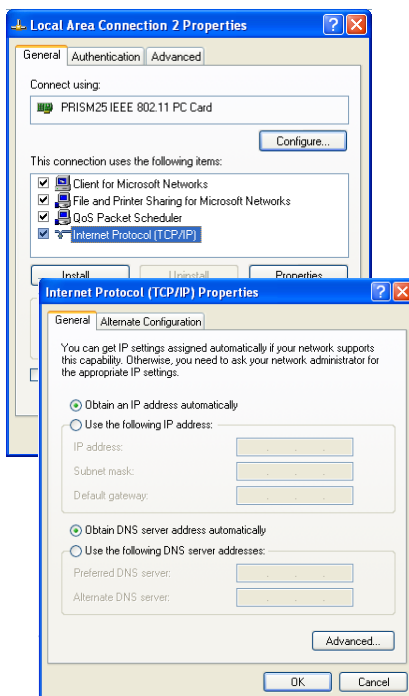
1. Cliquez sur « Start/ Control Panel »
(Démarrer/Panneau de configuration).
2. Dans la fenêtre qui s'affiche, cliquez sur « Network and Internet Connections »
(Connexions réseau et Internet).
3. L'écran « Network Connections »
(Connexions réseau) s'ouvre. Double-cliquez sur la connexion de ce périphérique.
4. Sur l'écran d'état de la connexion, cliquez sur « Properties »
(Propriétés).



5. Double-cliquez sur « Internet Protocol (TCP/IP) » (Protocole Internet (TCP/IP)).

6. S'il existe des informations d'adresse IP dans la boîte de dialogue « Internet Protocol (TCP/IP) Properties » (Propriétés de Protocole Internet (TCP/IP)), elles doivent être notées. Utilisez pour cela les lignes ci-après.

7. Si les options « Obtain an IP address automatically » (Obtenir une adresse IP automatiquement) et « Obtain DNS server address automatically » (Obtenir les adresses des serveurs DNS automatiquement) sont sélectionnées, votre ordinateur est déjà configuré pour DHCP. Cliquez sur « Cancel » (Annuler) pour fermer chaque fenêtre et passez à la section « Désactivation du proxy HTTP » à la page 5-22.



8. Activez l'option « Obtain an IP address automatically » (Obtenir une adresse IP automatiquement), puis « Obtain DNS server address automatically » (Obtenir les adresses des serveurs DNS automatiquement). Cliquez sur « OK » ou « Close » (Fermer) pour fermer chaque fenêtre.

Paramètres de configuration TCP/IP

Adresse IP _____._____._____._____
Masque de sous-réseau _____._____._____._____
Passerelle par défaut _____._____._____._____
Serveur DNS préféré _____._____._____._____
Serveur DNS auxiliaire _____._____._____._____

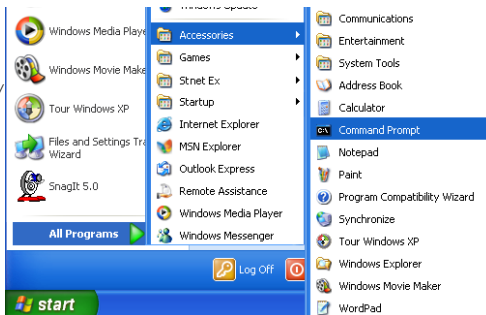
Désactivation du proxy HTTP

Vous devez vérifier que la fonctionnalité « Proxy HTTP » de votre serveur Web est désactivée pour que votre navigateur puisse afficher les pages de configuration HTML du routeur Barricade. Déterminez quel est le navigateur utilisé et reportez-vous à la section « Internet Explorer » à la page 5-6 ou « Netscape » à la page 5-7.

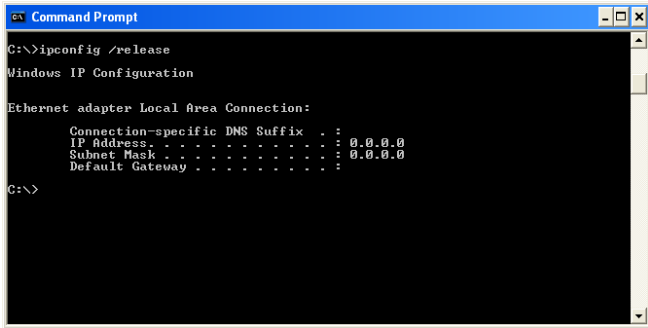
Lecture des paramètres IP depuis votre routeur Barricade

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

1. Depuis le Bureau Windows, cliquez sur « Start/Programmes/ Accessoires/ Command Prompt » (Démarrer/ Programmes/ Accessoires/Invite de commandes).



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



```

C:\>ipconfig /release

Windows IP Configuration

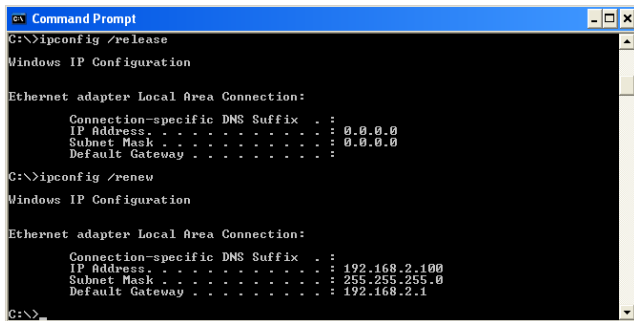
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

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 de votre routeur ADSL.



```

C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>

```

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

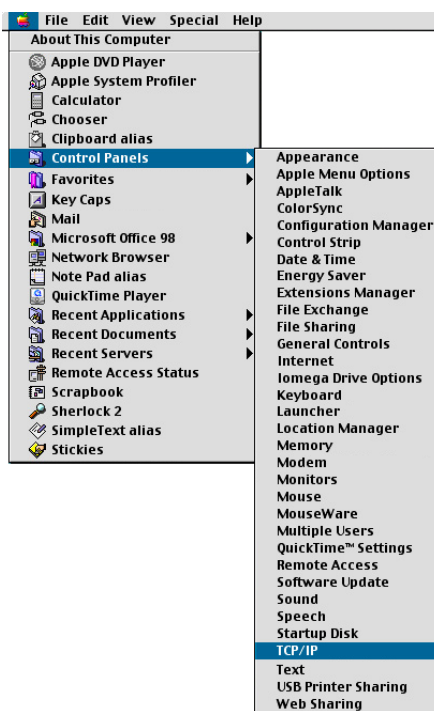
Votre ordinateur est maintenant configuré pour la connexion au routeur Barricade.

Configuration de votre ordinateur Macintosh

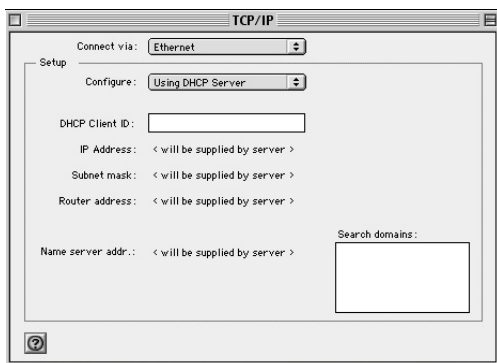
Vous noterez peut-être que les instructions de ce manuel ne correspondent pas exactement à votre système d'exploitation. En effet, ces étapes et les captures d'écrans ont été effectuées sous Mac OS 8.5. Mac OS 7.x et les systèmes ultérieurs sont similaires, mais pas identiques à Mac OS 8.5.

Procédez comme suit :

1. Déroulez le menu Apple. Cliquez sur « Control Panels » (Tableaux de bord), puis 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).

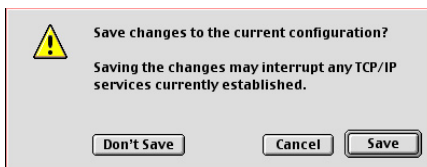


- Si l'option « Using DHCP Server » (Utiliser un serveur DHCP) est sélectionnée dans la zone « Configure » (Configuration), votre ordinateur est déjà configuré pour DHCP.



Fermez la boîte de dialogue TCP/IP et passez à la section « Désactivation du proxy HTTP » à la page 5-26.

- S'il existe des informations d'adresse IP dans l'écran « TCP/IP », elles doivent être notées. Utilisez pour cela les lignes ci-après.
- Après avoir noté vos paramètres IP, sélectionnez l'option « Using DHCP Server » (Utiliser un serveur DHCP) dans la zone « Configure » (Configuration), puis fermez la fenêtre.
- Un message apparaît et vous êtes invité à enregistrer vos paramètres. Cliquez sur « Save » (Enregistrer).



Paramètres de configuration TCP/IP

Adresse IP _____

Masque de sous-réseau _____

Adresse du routeur _____

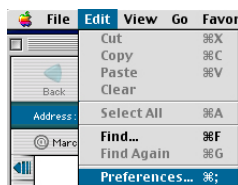
Adresse du serveur de noms _____

Désactivation du proxy HTTP

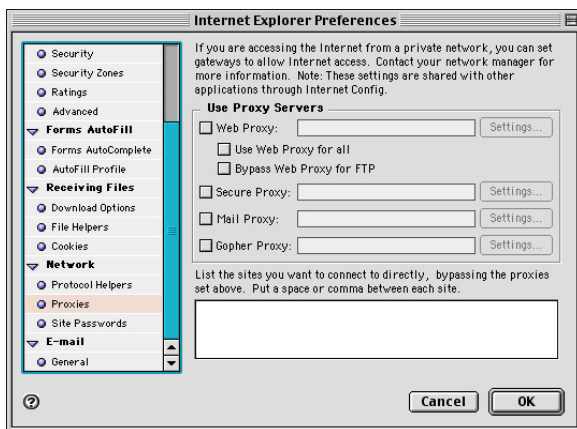
Vous devez vérifier que la fonctionnalité « Proxy HTTP » de votre serveur Web est désactivée pour que votre navigateur puisse afficher les pages de configuration HTML du routeur Barricade. Les étapes suivantes concernent Internet Explorer et Netscape. Déterminez le navigateur utilisé et suivez les étapes appropriées.

Internet Explorer

1. Ouvrez Internet Explorer et cliquez sur le bouton « Stop » (Arrêter). Cliquez sur « Edit » (Edition), puis sur « Preferences » (Préférences).

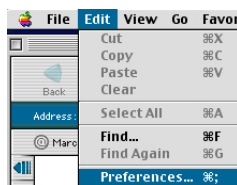


2. Dans la boîte de dialogue qui s'affiche, sous Network (Réseau), sélectionnez « Proxies » (Serveur proxy).
3. Désactivez toutes les cases à cocher, puis cliquez sur « OK ».



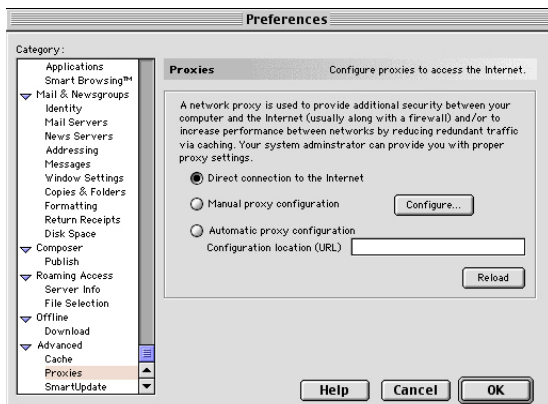
Netscape

1. Ouvrez Netscape et cliquez sur le bouton « Stop » (Arrêter). Cliquez sur « Edit » (Edition), puis sur « Preferences » (Préférences).



2. Dans la boîte de dialogue qui s'affiche, dans la colonne de gauche « Category » (Catégories), sélectionnez « Advanced » (Avancées). Dans la zone « Advanced » (Avancées), sélectionnez « Proxies » (Serveur proxy).

3. Activez l'option « Direct Connection to the Internet » (Connexion directe à Internet), puis cliquez sur « OK ».

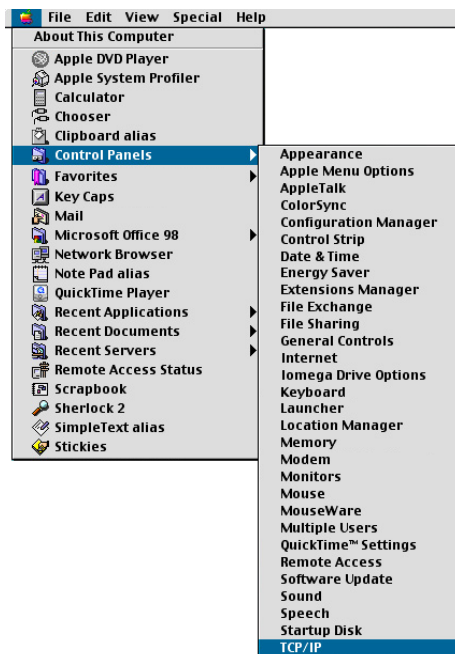


Lecture des paramètres IP depuis votre routeur Barricade

Barricade

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

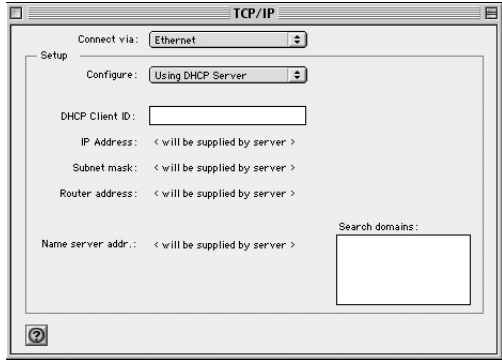
1. Déroulez le menu Apple. Cliquez sur « Control Panels » (Tableaux de bord), puis sélectionnez TCP/IP.



2. Vos nouveaux paramètres apparaissent dans la fenêtre TCP/IP. 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 de votre routeur Barricade.

3. Fermez la fenêtre TCP/IP.

Votre ordinateur est maintenant configuré pour la connexion au routeur Barricade.



CHAPITRE 6

CONFIGURATION DES SERVICES D'IMPRESSION

Pour utiliser le serveur d'impression intégré au routeur Barricade, vous devez d'abord installer le moniteur de port selon la procédure décrite dans la section ci-après pour Windows 95/98/Me/NT/2000/XP.

Pour configurer le serveur d'impression du routeur Barricade pour Windows 95/98/Me/NT/2000/XP ou Unix, consultez la section « Configuration du serveur d'impression » à la page 6-4.

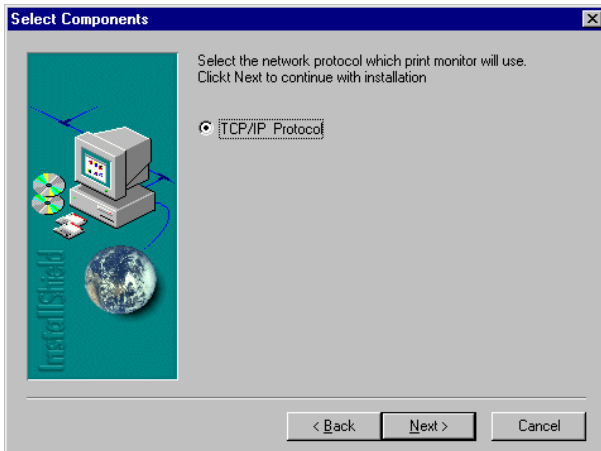
Installation du moniteur de port d'imprimante

Ignorez cette section si vous utilisez Unix.

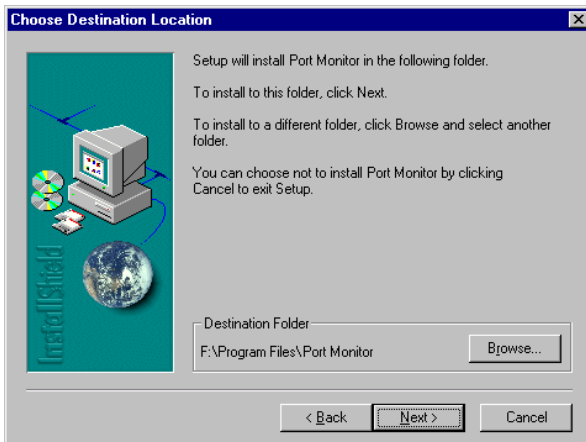
Pour les postes clients Windows 95/98/Me/NT/2000/XP, il est nécessaire d'installer le moniteur de port selon la procédure décrite dans cette section.

1. Insérez le CD-ROM d'installation dans votre lecteur de CD-ROM. Dans le répertoire PrintSvr, exécutez le programme « setup.exe ». Le programme d'installation du moniteur de port vous conseille de fermer tous les autres programmes Windows en cours d'exécution sur votre ordinateur. Cliquez sur « Next » (Suivant) pour continuer.

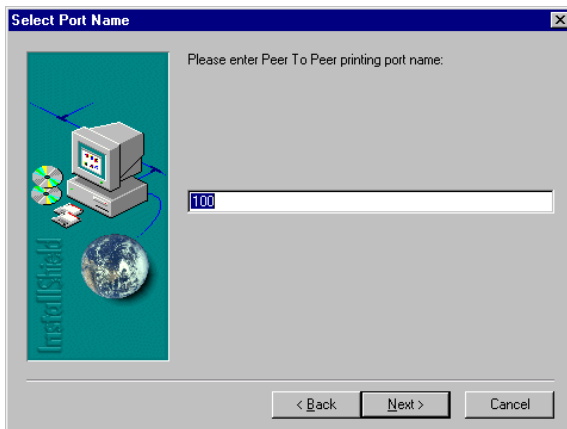
2. L'écran qui s'affiche ensuite indique que le poste client d'impression utilise le protocole réseau TCP/IP pour surveiller les demandes d'impression. Cliquez sur « Next » (Suivant).



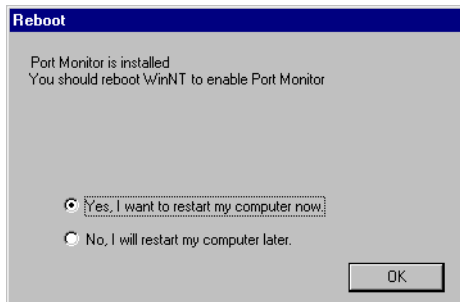
3. Sélectionnez le dossier de destination et cliquez sur le bouton « Next » (Suivant). Le programme d'installation lance l'installation des programmes dans le dossier de destination.



4. Sélectionnez le dossier programme qui va contenir l'icône du programme pour la désinstallation du moniteur de port, puis cliquez sur « Next ».
5. Entrez le nom du port d'imprimante qui sert à identifier le moniteur de port sur votre système et cliquez sur « Next » (Suivant).



6. Une fois l'installation du moniteur de port terminée, activez l'option « Yes, I want to restart my computer now » (Oui, je veux redémarrer mon ordinateur maintenant), puis cliquez sur « OK ».



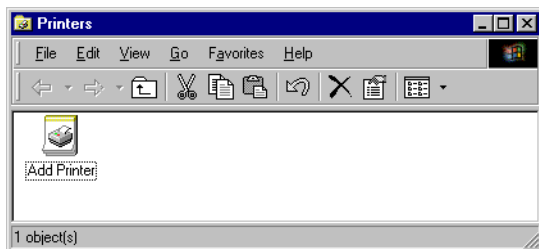
7. Après avoir redémarré l'ordinateur, ajoutez le serveur d'impression Barricade à votre système selon la procédure décrite dans la section suivante.

Configuration du serveur d'impression

Le serveur d'impression du routeur Barricade prend en charge Microsoft Windows 95/98/Me/NT/2000/XP et Unix. Sous Windows 95/98/Me/NT/2000/XP, vous devez installer le moniteur de port, selon la procédure décrite dans la section précédente, avant d'ajouter le serveur d'impression du routeur Barricade à votre système d'exploitation.

Configuration de l'imprimante réseau sous Windows 95/98/Me/2000

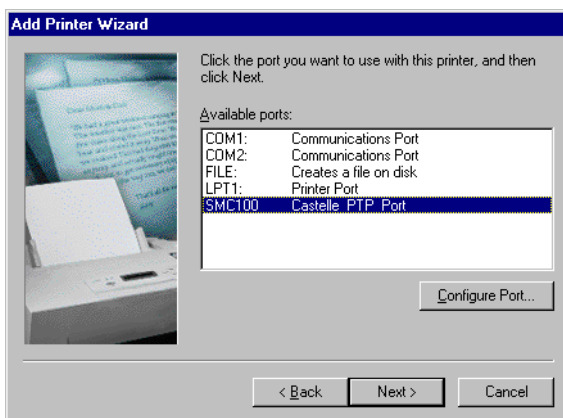
1. Sous Windows 95/98/Me/2000/XP, ouvrez la fenêtre Printers (Imprimantes) à partir de My Computer (Poste de travail) et double-cliquez sur l'icône Add Printer (Ajout d'imprimante).



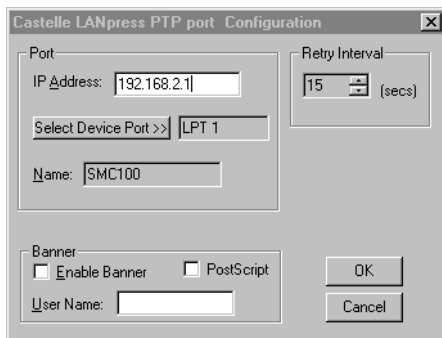
2. Suivez les messages vous invitant à ajouter une imprimante locale à votre système.



3. Indiquez le type d'imprimante connecté au routeur Barricade.
4. Sélectionnez le port contrôlé. Le nom de port par défaut est « SMC100 ». Cliquez sur le bouton « Configure Port » (Configurer un port).



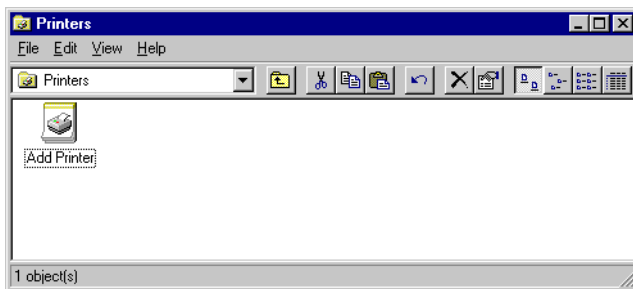
5. Entrez l'adresse IP du routeur Barricade et cliquez sur « OK ». Cliquez ensuite sur « Next » (Suivant) dans la boîte de dialogue Add Printer Wizard (Assistant Ajout d'imprimante).



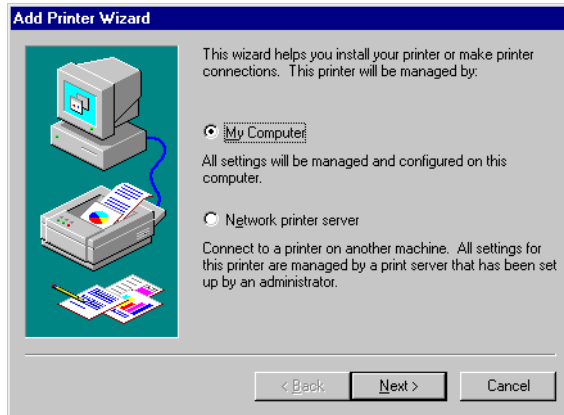
6. Continuez à suivre les invites pour terminer l'installation du serveur d'impression Barricade. L'imprimante est alors ajoutée à votre menu Printers (Imprimantes).

Configuration de l'imprimante réseau sous Windows NT

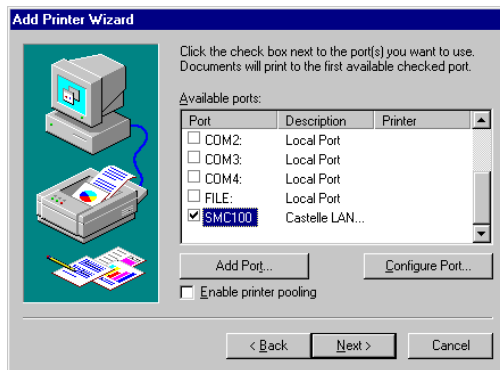
1. Sous Windows NT, ouvrez la fenêtre Printers (Imprimantes) à partir de My Computer (Poste de travail) et double-cliquez sur l'icône « Add Printer » (Ajout d'imprimante).



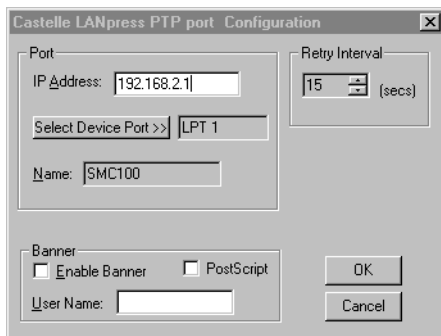
2. Suivez les messages vous invitant à ajouter une imprimante locale à votre système.



3. Sélectionnez le port contrôlé. Le nom de port par défaut est « SMC100 ». Cliquez ensuite sur le bouton « Configure Port » (Configurer le port).



- Entrez l'adresse IP du routeur Barricade et cliquez sur « OK ». Cliquez sur « Next » (Suivant) dans la boîte de dialogue Add Printer Wizard (Assistant Ajout d'imprimante).



- Indiquez le type d'imprimante connecté au routeur Barricade.
- Continuez à suivre les invites pour terminer l'installation du serveur d'impression Barricade. Le type d'imprimante spécifié est alors ajouté à votre menu Printers (Imprimantes).

Configuration de l'imprimante réseau sous Unix

Suivez la procédure de configuration classique sous Unix pour configurer le serveur d'impression Barricade. Le nom de l'imprimante est « lpt1 ».

ANNEXE A

DÉPANNAGE

La présente section décrit les incidents les plus courants que vous pouvez rencontrer, ainsi que les solutions possibles. Le routeur Barricade peut aisément être contrôlé via les témoins lumineux de son panneau avant pour l'identification des incidents.

Tableau de dépannage	
Symptôme	Action
Témoins lumineux	
Témoin d'alimentation éteint	<ul style="list-style-type: none">• Vérifiez les connexions entre le routeur Barricade, l'alimentation externe et la prise murale.• Si le témoin d'alimentation ne s'allume pas lorsque le cordon d'alimentation est branché, il se peut qu'un incident se soit produit au niveau de la prise secteur, du cordon d'alimentation ou de l'alimentation externe. Cependant, si l'appareil s'arrête en cours de fonctionnement, vérifiez l'état des connexions, ainsi que l'absence de perte d'énergie ou de surtension au niveau de la prise secteur. Si l'incident ne peut toujours pas être isolé, il se peut que l'alimentation externe soit défectueuse. Dans ce cas, prenez contact avec le service d'assistance technique.

Tableau de dépannage	
Symptôme	Action
Témoins lumineux	
Témoin Link (Liaison) éteint	<ul style="list-style-type: none"> • Vérifiez que le routeur Barricade et le périphérique relié sont sous tension. • Assurez-vous que le câble est branché au routeur et au périphérique correspondant. • Vérifiez que le type de câble approprié est utilisé et que sa longueur n'excède pas les limites indiquées. • Assurez-vous que l'interface réseau du périphérique connecté est configurée pour la vitesse de communication et pour le mode Duplex appropriés. • Vérifiez que l'adaptateur du périphérique raccordé et les branchements ne sont pas défectueux. Si nécessaire, remplacez les adaptateurs ou les câbles défectueux.
Problèmes de connexion réseau	
Il est impossible d'atteindre le routeur Barricade avec la commande ping à partir du réseau local connecté, ou le routeur ne parvient à atteindre aucun périphérique du réseau local connecté avec la commande ping.	<ul style="list-style-type: none"> • Vérifiez que les adresses IP sont correctement configurées. Pour la plupart des applications, vous devez utiliser la fonction DHCP du routeur Barricade pour affecter dynamiquement des adresses IP aux systèmes hôtes du réseau local connecté. Toutefois, si vous configurez manuellement des adresses IP sur le réseau local, vérifiez que la même adresse réseau (composant réseau de l'adresse IP) et le même masque de sous-réseau sont utilisés pour le routeur Barricade et les périphériques connectés du réseau local. • Assurez-vous que le périphérique auquel vous souhaitez appliquer la commande Ping (ou à partir duquel vous exécutez cette commande) a été configuré pour TCP/IP.

Tableau de dépannage	
Symptôme	Action
Incidents d'administration	
Impossibilité de se connecter à l'aide du navigateur Web	<ul style="list-style-type: none"> • Vérifiez que vous avez configuré le routeur Barricade avec une adresse IP, un masque de sous-réseau et une passerelle par défaut corrects. • Vérifiez que vous disposez d'une connexion réseau valide avec le routeur Barricade et que le port que vous utilisez n'a pas été désactivé. • Contrôlez le câblage réseau entre la station d'administration et le routeur Barricade.
Oubli ou perte du mot de passe	<ul style="list-style-type: none"> • Appuyez sur le bouton Reset (Réinitialiser) du panneau arrière (en le maintenant enfoncé pendant au moins cinq secondes) pour restaurer les paramètres par défaut.

ANNEXE B

CÂBLES

Câble Ethernet

Attention : ne raccordez pas de prise téléphonique à un port RJ-45. Pour les connexions Ethernet, utilisez uniquement des câbles à paire torsadée dotés de connecteurs RJ-45 conformes aux normes FCC.

Spécifications

Types de câble et spécifications			
Câble	Type	Longueur max.	Connecteur
10BASE-T	UTP cat. 3, 4 ou 5 100 ohms	100 m	RJ-45
100BASE-TX	UTP cat. 5 100 ohms	100 m	RJ-45

Conventions de câblage

Pour les connexions Ethernet, un câble à paire torsadée doit avoir deux paires de fils. Chaque fil est identifié par deux couleurs différentes. Par exemple, un fil peut être rouge, tandis que l'autre sera rouge avec des bandes blanches. Un connecteur RJ-45 doit également être présent aux deux extrémités du câble.

Chaque paire doit être reliée aux connecteurs RJ-45 selon une orientation particulière. La figure suivante illustre la numérotation des broches du connecteur RJ-45 Ethernet.

Veillez à maintenir les connecteurs dans le même sens lorsque vous connectez les fils aux broches.

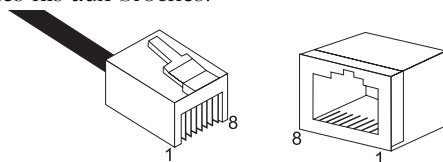


Figure B-1. Numéros des broches du connecteur Ethernet RJ-45

Connexion au port Ethernet RJ-45

Utilisez le câble Ethernet de catégorie 5 direct fourni dans le coffret pour connecter le routeur Barricade à votre PC. Pour la connexion à d'autres périphériques réseau tels qu'un commutateur Ethernet, utilisez le type de câble indiqué dans le tableau suivant.

Type de port de périphérique connecté	Type de câble de connexion
MDI-X	Direct
MDI	Croisé

Brochages

Sur les câbles 10BASE-T/100BASE-TX, les broches 1 et 2 servent à transmettre les données et les broches 3 et 6 à les recevoir.

Brochage RJ-45	
Numéro de broche	Signal*
1	Tx+ (Émission+)
2	Tx- (Émission-)
3	Rx+ (Réception+)
6	Rx- (Réception-)

* Les signes « + » et « - » représentent la polarité des fils composant chaque paire.

Câblage direct

Si le port sur le périphérique connecté est doté d'un câblage croisé interne (MDI-X), utilisez un câble direct.

Brochage d'un câble direct	
Extrémité 1	Extrémité 2
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

Câblage croisé

Si le port sur le périphérique connecté est doté d'un câblage direct (MDI), utilisez un câble croisé.

Brochage d'un câble croisé	
Extrémité 1	Extrémité 2
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

Câble ADSL

Utilisez un câble téléphonique standard pour relier la prise téléphonique murale RJ-11 au port ADSL RJ-11 du routeur ADSL.

Attention : ne raccordez pas de prise téléphonique à un port RJ-45.

Spécifications

Types de câble et spécifications		
Câble	Type	Connecteur
Ligne ADSL	Câble téléphonique standard	RJ-11

Conventions de câblage

Pour les connexions ADSL, un câble doit comporter une paire de fils. Chaque fil est identifié par une couleur particulière. Par exemple, un fil peut être rouge, tandis que l'autre sera rouge avec des bandes blanches. Un connecteur RJ-11 doit également être présent aux deux extrémités du câble.

Chaque paire doit être reliée aux connecteurs RJ-11 selon une orientation particulière. La figure suivante illustre la numérotation des broches du connecteur RJ-11. Veillez à maintenir les connecteurs dans le même sens lorsque vous connectez les fils aux broches.

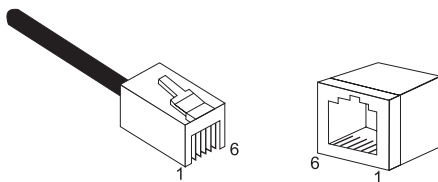
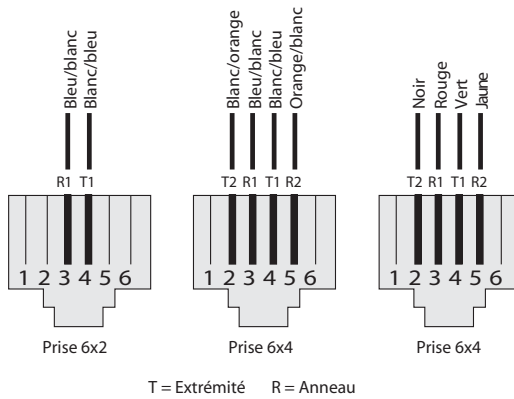


Figure B-2. Numéros des broches du connecteur RJ-11



Broche	Nom du signal	Couleurs des câbles
1	<i>Non utilisé</i>	
2	Extrémité ligne 2	Noir ou blanc/orange
3	Anneau ligne 1	Rouge ou bleu/blanc
4	Extrémité ligne 1	Vert ou blanc/bleu
5	Anneau ligne 2	Jaune ou orange/blanc
6	<i>Non utilisé</i>	

Figure B-3. Sorties RJ-11

APPENDIX C

SPECIFICATIONS

Standards Compliance

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

Safety

UL 1950

EN60950 (TÜV)

CSA 22.2 No. 950

IEEE 802.3 10 BASE-T Ethernet

IEEE 802.3u 100 BASE-TX Fast Ethernet

Modem Standards

ITU G.992.1 (G.dmt)

ITU G.992.2 (G.Lite)

ITU G.994.1 (G.handshake)

ITU T.413 issue 2 - ADSL full rate

LAN Interface

4 RJ-45 10 BASE-T/100 BASE-TX ports

Auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half-duplex or full-duplex.

SPECIFICATIONS

WAN Interface

1 ADSL RJ-11 port

Indicator Panel

Power, Ethernet, ADSL Syn, ADSL Data

Dimensions

220 x 132.8 x 30.5 mm (8.66 x 5.23 x 1.20 in)

Weight

0.6 kg (1.32 lbs)

Input Power

12 V 1 A

Power Consumption

12 Watts max.

Management

Web management

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Firewall – Client privileges, hacker prevention and logging, Stateful
Packet Inspection

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

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793
TCP, RFC 783 TFTP, RFC 1483 AAL5 Encapsulation, RFC 1661 PPP,
RFC 1866 HTML, RFC 2068 HTTP, RFC 2364 PPP over ATM

Temperature

Operating 0 to 40°C (32 to 104°F)

Storage -40 to 70°C (-40 to 158°F)

Humidity

5% to 95% (noncondensing)

Warranty

Limited Lifetime

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

Note: In order to maintain compliance with the limits for a Class B digital device, you are required to use a quality interface cable when connecting to this device. Changes or modifications not expressly approved by our company could void the user's authority to operate this equipment.

FCC - Part 68

This equipment complies with Part 68 of the FCC rules. This equipment comes with a label attached to it that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11C.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0.) To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact our company at the numbers shown on back of this manual for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

No repairs may be done by the customer.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

When programming and/or making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in off-peak hours such as early morning or late evenings.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone facsimile machine unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or such business, other entity, or individual.

In order to program this information into your facsimile, refer to your communications software user manual.

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 Industry Canada.

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 l'Industrie.

Australia AS/NZS 3548 (1995) - Class B



ACN 069 351 613

EC Conformance Declaration - Class B

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. For the evaluation of the compliance with these Directives, the following standards were applied:

- RFI Emission:
- Limit class B according to EN 55022:1998
 - Limit class B 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 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/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 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
 - Power frequency magnetic field immunity test according to EN 61000-4-8:1993 (1 A/m at frequency 50 Hz)
 - Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994 (>95% Reduction @10 ms, 30% Reduction @500 ms, >95% Reduction @5000 ms)
- LVD:
- EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

LEGAL INFORMATION AND CONTACTS

SMC's Limited Warranty Statement

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.

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.

INDEX

A

ADSL

- connexion de ligne 2-5
- spécifications pour le câblage B-4
- splitterless 2-5

ADSL splitterless 2-5

B

brochages

- port RJ-45 B-2

C

câble

- brochages RJ-45 B-2
- spécifications ADSL B-4
- spécifications Ethernet B-1

CE Mark 1-iii

client, configuration 5-1

connexion

- ligne ADSL 2-9
- port de console 2-9
- port Ethernet 2-8

D

- dépannage A-1
 - incidents d'administration A-3
 - témoins lumineux A-1
- DHCP 2-2

E

- EC conformance 1-iii
- Ethernet
 - connexion de ligne 2-8
 - spécifications pour le câblage B-1
- Ethernet LAN
 - specifications C-2
 - standards conformance C-2

F

- filtre 2-5, 2-7

G

- G.lite 2-5

I

- installation 2-1
 - filtre 2-5, 2-7
 - G.dmt : 2-6
 - G.lite 2-7
 - périphérique de répartition 2-6
- Internet Explorer
 - utilisation de la version 5.0 4-2, 4-17

P

- passerelle
 - serveur 2-2
- périphérique de répartition 2-6
- ping A-2
- port
 - RJ-11 2-5
 - RJ-45, brochages B-2

S

- specifications*
 - advanced features* C-2
 - Ethernet LAN C-2
 - management C-2

T

- témoin
 - alimentation A-1
 - Link (Liaison) A-2
- témoin (LED) 2-4
 - Ethernet 2-4
 - synchronisation 2-4
- témoins lumineux A-1

W

- Web
 - interface
 - boutons de configuration 4-2, 4-17
 - menu principal 4-3



Référence produit : SMC7404BRA EU
Publication : 150000035400A
Révision : E092002-R01