

Kabel-/DSL-Breitband-Router

4-Port 10/100 Mbit/s Switch integriert

Benutzerhandbuch

SMC7004VBR V.2



Kabel-/DSL-Breitband-Router 4-Port 10/100 Mbit/s Switch integriert Benutzerhandbuch

Ein Breitband-Router der SMC Barricade™-Serie

INHALTSVERZEICHNIS

Einführung	1
Merkmale und Vorteile	2
Packungsinhalt	3
Minimalanforderungen	4
Kennenlernen des Barricade™	5
LED-Anzeigen	6
Anschließen	7
Grundlegende Vorgehensweise bei der Installation	7
Konfiguration des Computers	9
Konfiguration unter Windows 95/98/Me	9
Konfiguration von Windows 2000	12
Konfiguration von Windows XP	13
Konfigurieren eines Macintosh-Computers	15
Konfiguration des Barricade™	17
Konfiguration des Browsers	18
Deaktivieren der Proxy-Verbindung	18
Zugriff auf das Geräte-Management des Barricade™	20
Arbeiten in der web-basierenden Verwaltungsschnittstelle	21
Vornehmen von Konfigurationsänderungen	21
Installationsassistent	23
Schritt 1: Time Zone (Zeitzone)	23
Schritt 2: Broadband Type (Breitbandtyp)	24
Schritt 3: Finish configuration (Abschließen der Konfiguration)	25
Erweiterte Konfiguration	26
System	26
WAN	30
LAN	37
NAT	38

Inhaltsverzeichnis

Firewall	41
DDNS Settings (Dynamische DNS-Einstellungen)	47
UPnP	47
Tools (Extras)	48
Status	49
Fehlerbehebung	51
Technical Specifications	57
Compliances	i
Legal Information and Contacts	v

EINFÜHRUNG

Herzlichen Glückwunsch zum Kauf Ihres Barricade™ Kabel-/DSL-Breitband-Routers (SMC7004VBR). Wir freuen uns, Ihnen ein leistungsstarkes und doch einfaches Kommunikationsgerät zur Verbindung Ihres lokalen Netzwerks (LAN) mit dem Internet bereitstellen zu können.

Wichtige Information!

Diese Informationen sind für DSL-Benutzer ohne Internet-Pauschalgebühr („Flat Rate“) gedacht **.

Mit Ihrem SMC DSL-Router haben Sie ein hochwertiges Gerät erworben, welches Ihnen den schnellen und problemlosen Zugriff auf das Internet ermöglicht. Die Werkseinstellung dieses Routers ist auf einen möglichst unterbrechungsfreien Zugriff auf die Internetdaten ausgelegt. Damit empfiehlt sich aus Kostengründen in jedem Fall der Anschluß einer sog. „flat rate“.

Warum?

Bitte bedenken Sie, daß der Router nicht automatisch abschaltet, wenn Sie Ihren PC herunterfahren! Sie können zwar ein automatisches Abschalten auslösen, indem Sie eine sog. „Idle Time“ Einstellung vornehmen. (siehe dazu die Betriebsanleitung: PPPoE oder PPTP WAN-Access Configuration). Je nach eingestellter Zeitdauer (1-5 Min.) trennt der Router die DSL/Internet-Verbindung. Dies bietet aber noch keine 100% Sicherheit.

Deshalb Achtung! Dies geschieht nur, wenn für den Router keine offenen Anfragen aus dem LAN-oder WAN-Bereich (= Anfragen die aus dem Internet z. B. bei der Nutzung von File Sharing Programmen wie eMule, eDonkey, usw.) eingehen, die den Router aktiv halten. Um diesen unabwägbaren Möglichkeiten zu begegnen und sich damit gegen unliebsame Leitungsnutzungs-

Einführung

kosten abzusichern, empfehlen wir für Ihren DSL-Anschluss in jedem Fall den Abschluß einer „flat rate“.

Die einzige Alternative: Ziehen Sie nach Beendigung Ihrer Internet-Session den Netzstecker des Routers! Im Zweifelsfall fragen Sie Ihre SMC Hotline-Mitarbeiter.

** „flat-rate“ ist ein Tarifangebot Ihres DSL-Leitungsanbieters, welches eine zeitlich unbegrenzte Nutzung Ihres Internet-zuganges zu einem Pauschaltarif ermöglicht.

Merkmale und Vorteile

- Internet-Verbindung per DSL- oder Kabelmodem über einen 10/100 Mbit/s-WAN-Port.
- Lokale Netzwerkverbindung über 10/100-Mbit/s-Ethernet-Switch-Ports.
- DHCP für dynamische IP-Konfiguration und DNS für Domänen-namenzuordnung.
- Firewall mit SPI (Stateful Packet Inspection), Clientrechten, Erkennung von Eindringversuchen, DoS und NAT.
- Mehrbenutzer-Zugriff über ein Einzelbenutzerkonto und Funktio-nalität eines virtuellen Servers (für geschützten Zugriff auf Inter-netdienste wie WWW, FTP, E-Mail und Telnet) durch NAT.
- Unterstützung für Virtual Private Network mit PPTP, L2TP oder IPSec-Pass-through.
- Benutzerdefinierbarer Tunnel mit Erkennung für Anwendungen, die mehrere Verbindungen benötigen.
- Zugangskontrolle, mit der der Benutzer das Aufrufen bestimmter Websites verhindern kann.

- E-Mail-Warnungen, wenn die Sicherheit des Netzwerks des Benutzers beeinträchtigt ist.
- Einfache Einrichtung über einen Web-Browser auf jedem Betriebssystem, das TCP/IP unterstützt.
- Kompatibel zu allen gängigen Internet-Anwendungen.

Packungsinhalt

Vor dem Installieren des Barricade™ Kabel-DSL-Breitband-Routers sollten Sie sicherstellen, dass alle im Lieferumfang enthaltenen Teile vorhanden sind. Außerdem müssen Sie dafür sorgen, dass Sie über die erforderliche Verkabelung verfügen. Wenn der Packungsinhalt nicht vollständig ist oder Teile beschädigt sind, wenden Sie sich sofort an Ihren Händler.

- Barricade™ Breitband-Router.
- Netzteil.
- Ein Ethernet-Kabel (Kat. 5).
- Vier Gummifüße.
- Ein CD-ROM.

Heben Sie nach Möglichkeit den Karton und das Verpackungsmaterial auf. Sie benötigen diese, wenn Sie das Produkt zurücksenden.

Minimalanforderungen

- Kabel- oder DSL-Modem mit Ethernet-Anschluss und Internet Zugang. Internet-Zugang über Ihre lokale Telefongesellschaft oder Ihren Internet-Provider (ISP) über ein DSL- oder Kabelmodem.
- Ein mit einer Fast-Ethernet-Karte (10 Mbit/s, 100 Mbit/s oder 10/100 Mbit/s) oder einem USB-to-Ethernet-Konverter ausgestatteter Computer.
- Netzwerkadapter mit Ethernet-Verkabelung (UTP CAT 5) und auf dem PC installierten Protokoll TCP/IP.
- Internet Explorer 4.0 (oder höher) oder Netscape Navigator 4.7 (oder höher) für die web-basierende Konfiguration des Barricade™.

KENNENLERNEN DES BARRICADE™

Der SMC7004VBR Barricade™ Kabel-/DSL-Breitband-Router ist die perfekte Lösung für Heiminstallationen und kleine Büros. Dieser komplett ausgestattete Router bietet Folgendes:

- 4 – LAN-Ports mit automatischer 10/100-Mbit/s-Erkennung und automatischer MDI/MDIX-Umschaltung.
- 1 – WAN-Port (10/100 Mbit/s) mit automatischer MDI/MDIX-Umschaltung.
- LEDs für Netzwerkstatus und Fehlerbehebung.
- [Reset]-schalter.



LED-Anzeigen

Der Barricade™ verfügt über LED-Anzeigen auf der Vorderseite, die Installation und Fehlerbehebung im Netzwerk vereinfachen.

LED	EIN	AUS	BLINKT
PWR	Das Gerät wird mit Netzspannung versorgt	Das Gerät wird nicht mit Netzspannung versorgt	-
WAN	Es wurde eine gute WAN-Verbindung erkannt	Es wurde keine WAN-Verbindung erkannt	Daten werden gesendet oder empfangen
LINK/ACT	Es wurde eine gute LAN-Verbindung erkannt	Es wurde keine LAN-Verbindung erkannt	Daten werden gesendet oder empfangen
10/100 Mbps	LAN-Port wird mit 100 Mbit/s betrieben	LAN-Port wird mit 10 Mbit/s betrieben	-

Zurücksetzen des Barricade™

Der [Reset]-schalter befindet sich auf der Rückseite des Barricade™ Breitband-Routers. Verwenden Sie eine Büroklammer oder eine Kugelschreiberspitze, um den [Reset]-schalter zu betätigen.

Reset (Zurücksetzen)

Falls der Router Probleme beim Verbindungsaufbau mit dem Internet hat, trennen Sie ihn 3 Sekunden lang vom Netz und stecken Sie ihn dann wieder ein.

Wiederherstellen der Werkseinstellungen

Falls das Problem durch das Zurücksetzen des Routers nicht behoben wird, gehen Sie folgendermaßen vor:

1. Lassen Sie das Stromkabel des Routers eingesteckt.
2. Suchen Sie den [Reset]-Schalter auf der Rückseite des Geräts und halten Sie ihn gedrückt, bis die WAN-LED ausgeht.
3. Lassen Sie den [Reset]-Schalter wieder los.

ANSCHLIEßEN

Der SMC7004VBR Barricade™ Kabel-/DSL Breitband-Router wird zwischen dem Kabel-/DSL-Breitbandmodem und Ihren Computern angeschlossen. Wenn Sie weitere Computer verbinden wollen, schließen Sie sie einfach an die LAN-Ports an der Rückseite des Routers an.



Grundlegende Vorgehensweise bei der Installation

1. Anschließen des LAN

Führen Sie ein Ethernet-Kabel von einem der LAN-Ports an der Rückseite des Barricade™ zum Netzwerkadapter Ihres Computers.

2. Anschließen des WAN:

Führen Sie ein Ethernet-Kabel von Ihrem Kabel- oder DSL-Modem zum WAN-Port an der Rückseite des Routers.

3. Einschalten

Verbinden Sie das Netzkabel mit dem Barricade™.

Wenn Sie alle Hardwarekomponenten miteinander verbunden haben, legen Sie die Barricade™-CD-ROM ein. Hierauf stellt der EZ 3-Click Installationsassistent automatisch eine Verbindung mit dem Internet her.

Hinweise zur Konfiguration der PCs siehe das Kapitel Konfiguration des Computers.

Die erweiterte Konfiguration des Barricade™ Broadband Routers wird im Kapitel Konfiguration des Barricade™ beschrieben.

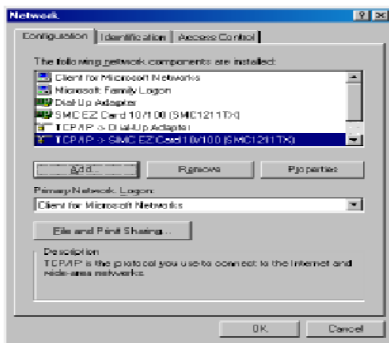
KONFIGURATION DES COMPUTERS

Die Information in diesem Kapitel beschreiben die Konfiguration unter den folgenden Betriebssystemen:

- Windows 95/98
- Windows Me
- Windows 2000
- Windows XP
- Apple Macintosh

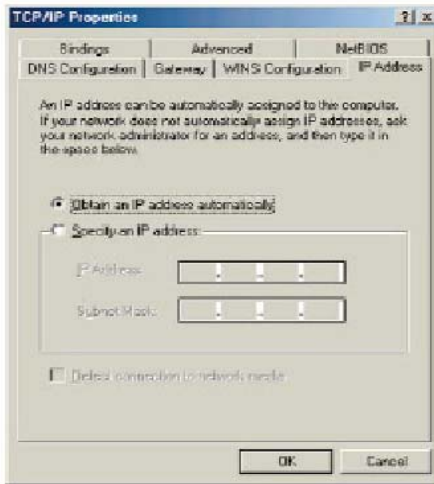
Konfiguration unter Windows 95/98/Me

1. Rufen Sie die Netzwerkeinstellungen auf, indem Sie auf [Start] klicken, [Settings] (Einstellungen) wählen und auf [Control Panel] (Systemsteuerung) klicken.
2. Doppelklicken Sie in der Systemsteuerung auf das Symbol [Network] (Netzwerk).



Konfiguration des Computers

3. Markieren Sie die TCP/IP-Zeile, die Ihrer Netzwerkkarte in der Registerkarte [Configuration] (Konfiguration) des Fensters [Network] zugewiesen wurde.
4. Klicken Sie dann auf [Properties] (Eigenschaften), um die TCP/IP-Einstellungen des Adapters anzuzeigen.



5. Klicken Sie im Dialogfeld [TCP/IP Properties] (Eigenschaften von TCP/IP) auf die Option [Obtain an IP address] (IP-Adresse automatisch beziehen).
6. Klicken Sie auf die Registerkarte [Gateway] und vergewissern Sie sich, dass das Gateway-Feld leer ist. Falls sich dort IP-Adressen befinden, markieren Sie diese und klicken Sie auf [Remove] (Entfernen), bis der Bereich leer ist.
7. Klicken Sie auf [OK], um das Fenster [TCP/IP Properties] zu schließen.

Konfiguration unter Windows 95/98/Me

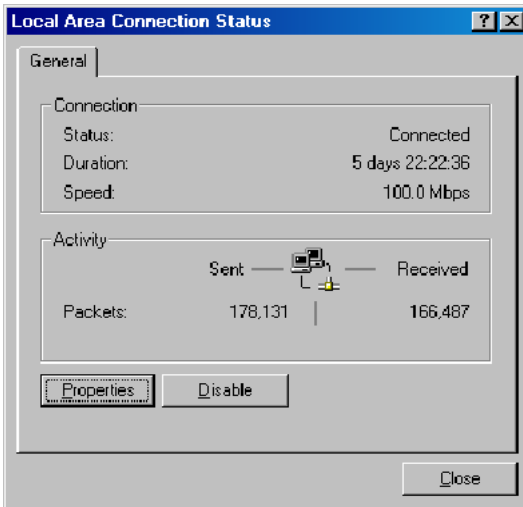
8. Klicken Sie im Fenster [Network Properties] (Netzeigenschaften) auf die Schaltfläche [OK], um die Änderungen zu speichern.

Hinweis: Windows fordert Sie in bestimmten Fällen auf, die Installations-CD von Windows einzulegen oder weitere Dateien bereitzustellen. Suchen Sie diese Dateien im Ordner `c:\windows\options\cabs` oder legen Sie die Windows-CD in das CD-ROM-Laufwerk ein und suchen Sie am entsprechenden Speicherort, wie „D:\win98“, „D:\win9x“ usw. (hierbei ist „D“ die Bezeichnung Ihres CD-ROM-Laufwerks).

9. Windows fordert Sie eventuell auf, den PC neu zu starten. Klicken Sie in diesem Fall auf [Yes] (Ja). Falls Windows Sie nicht zu einem Neustart auffordert, starten Sie den Computer trotzdem neu, um zu gewährleisten, dass die neuen Einstellungen übernommen werden.

Konfiguration von Windows 2000

1. Rufen Sie die Netzwerkeinstellungen auf, indem Sie auf [Start] klicken, [Settings] (Einstellungen) wählen und auf [Control Panel] (Systemsteuerung) klicken.
2. Doppelklicken Sie in der Systemsteuerung auf das Symbol [Network and Dial-up Connections] (Netzwerk- und DFÜ-Verbindungen).
3. Doppelklicken Sie auf das Symbol [Local Area Connection] (LAN-Verbindung) für den Ethernet-Adapter, der an den Barricade™ angeschlossen ist. Wenn das Dialogfeld [Status] geöffnet wird, klicken Sie auf [Properties] (Eigenschaften).



4. Vergewissern Sie sich, dass im Dialogfeld [Local Area Connection Properties] (Eigenschaften von LAN-Verbindung) das Kontrollkästchen neben [Internet Protocol (TCP/IP)] (Internetprotokoll (TCP/IP)) aktiviert ist. Markieren Sie dann den Eintrag [Internet Protocol (TCP/IP)] und klicken Sie auf [Properties] (Eigenschaften).

5. Wählen Sie [Obtain an IP address automatically] (IP-Adresse automatisch beziehen), um den Computer für DHCP zu konfigurieren. Klicken Sie auf [OK], um diese Änderung zu speichern und das Fenster [Properties] (Eigenschaften) zu schließen.
6. Klicken Sie erneut auf [OK], um die Änderungen zu speichern.
7. Starten Sie Ihren PC neu.

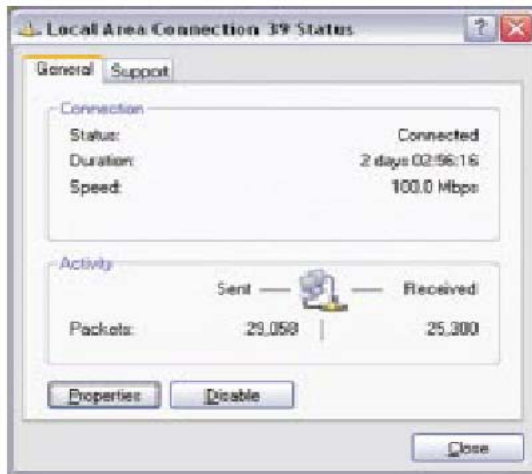
Konfiguration von Windows XP

Bei den folgenden Anleitungen wird davon ausgegangen, dass Sie Windows XP mit der Standardschnittstelle ausführen. Wenn Sie die Classic-Schnittstelle verwenden (in der die Symbole und Menüs wie bei früheren Windows-Versionen aussehen), gehen Sie bitte nach der vorangegangenen Anleitung für Windows 2000 vor.

1. Klicken Sie auf [Start] (Start), wählen Sie [Control Panel] (Systemsteuerung), wählen Sie [Network and Internet Connections] (Netzwerk- und Internetverbindungen) und klicken Sie auf das Symbol [Network Connections] (Netzwerkverbindungen).

Konfiguration des Computers

2. Doppelklicken Sie auf das Symbol [Local Area Connection] (LAN-Verbindung) für den Ethernet-Adapter, der an den Barricade™ angeschlossen ist. Klicken Sie auf [Properties] (Eigenschaften).



3. Vergewissern Sie sich, dass im Dialogfeld [Local Area Connection Properties] (Eigenschaften von LAN-Verbindung) das Kontrollkästchen neben [Internet Protocol (TCP/IP)] aktiviert ist. Markieren Sie den Eintrag [Internet Protocol (TCP/IP)] (Internetprotokoll (TCP/IP)) und klicken Sie auf [Properties].
4. Wählen Sie [Obtain an IP address automatically] (IP-Adresse automatisch beziehen), um den Computer für DHCP zu konfigurieren. Klicken Sie auf [OK], um diese Änderung zu speichern und das Fenster [Properties] (Eigenschaften) zu schließen.
5. Klicken Sie erneut auf [OK], um die Änderungen zu speichern.
6. Starten Sie Ihren PC neu.

Konfigurieren eines Macintosh-Computers

Eventuell entsprechen die hier aufgeführten Schritte nicht genau den Schritten, die für Ihr Betriebssystem erforderlich sind, da diese Anweisungen und Abbildungen mit OS 8.5 erstellt wurden, Mac OS 7.x und höher jedoch zwar ähnlich, aber unter Umständen nicht identisch mit Mac OS 8.5 sind.

1. Öffnen Sie das Menü [Apple]. Klicken Sie auf [Control Panel] (Kontrollfelder) und wählen Sie [TCP/IP] aus.
2. Vergewissern Sie sich, dass im Dialogfenster [TCP/IP] die Option [Ethernet] im Feld [Connect Via] (Verbindung) ausgewählt ist.

Wenn die Option [Using DHCP Server] (DHCP Server) bereits im Feld [Configure] (Konfigurationsmethode) ausgewählt ist, ist Ihr Computer bereits für DHCP konfiguriert. Schließen Sie in diesem Fall das Dialogfeld [TCP/IP] und fahren Sie mit Abschnitt Deaktivieren der Proxy-Verbindung.

3. Alle erforderlichen Informationen finden Sie im Dialogfeld [TCP/IP]. Notieren Sie die Werte in den entsprechenden Feldern unten.
4. Wählen Sie [Using DHCP Server] (DHCP Server) im Feld [Configure] (Konfigurationsmethode) aus und schließen Sie das Fenster.
5. Ein weiteres Fenster wird geöffnet, in dem Sie gefragt werden, ob Ihre TCP/IP-Einstellungen gespeichert werden sollen. Klicken Sie auf [Save] (Sichern).

KONFIGURATION DES BARRICADE™

Nachdem Sie TCP/IP auf einem Client-Computer konfiguriert haben, konfigurieren Sie den Barricade™ Breitband-Router mit einem Web-Browser. Der Barricade™ kann über jeden Java-fähigen Browser konfiguriert werden, z. B. Internet Explorer 4.0 oder höher oder Netscape Navigator 4.7 oder höher. Über die Web-Verwaltungsschnittstelle können Sie den Barricade™ konfigurieren und Statistiken zur Überwachung der Netzwerkaktivität anzeigen.

Hinweis: Bevor Sie versuchen, den Router zu konfigurieren, sollten Sie unter www.smc.de oder www.smc-europe.com die letzte Firmware-aktualisierung herunterladen.

Führen Sie die folgenden Schritte aus, bevor Sie sich beim web-basierenden Verwaltungs-Hilfsprogramm des Barricade™ Routers anmelden:

1. Vergewissern Sie sich, dass der Browser korrekt konfiguriert ist (siehe unten).
2. Deaktivieren Sie alle Firewall- und Sicherheitsprogramme.
3. Vergewissern Sie sich, dass die Verbindungs-LED („Link“) des Ports leuchtet, über den Ihr Computer an den Barricade™ angeschlossen ist. Falls die Verbindungs-LED nicht leuchtet, schließen Sie den Computer an ein anderes Kabel an, bis Sie eine gute Verbindung erhalten.

Konfiguration des Browsers

Vergewissern Sie sich, dass der Browser für eine direkte Verbindung zum Internet über die Ethernet-Verbindung des Computers konfiguriert ist. Die Einstellungen hierfür können Sie im Bereich mit den Optionen/Voreinstellungen des Browsers vornehmen.

Deaktivieren der Proxy-Verbindung

Darüber hinaus müssen Sie sich vergewissern, dass die HTTP-Proxy-Funktion Ihres Web-Browsers deaktiviert ist, damit Ihr Web-Browser die Konfigurationsseiten des Barricade™ anzeigen kann. Im Folgenden sind die Vorgehensweisen für Internet Explorer und für Netscape aufgeführt. Führen Sie die entsprechenden Schritte für Ihren Browser aus.

Internet Explorer (5 oder höher)

1. Öffnen Sie den Internet Explorer. Klicken Sie auf [Tools] (Extras) und anschließend auf [Internet Options] (Internetoptionen).
2. Klicken Sie im Fenster [Internet Options] auf die Registerkarte [Connections] (Verbindungen).
3. Klicken Sie dann auf [LAN Settings] (LAN-Einstellungen).
4. Deaktivieren Sie alle Kontrollkästchen und klicken Sie auf [OK], um die geänderten LAN-Einstellungen zu speichern.
5. Klicken Sie erneut auf [OK], um das Fenster Internet Options] zu schließen.

Deaktivieren der Proxy-Verbindung

Netscape (4 oder höher)

1. Öffnen Sie den Netscape-Browser. Klicken Sie auf [Edit] (Bearbeiten) und anschließend auf [Preferences] (Einstellungen).
2. Doppelklicken Sie im Fenster [Preferences] unter [Category] (Kategorie) auf [Advanced] (Erweitert) und anschließend auf [Proxies].
3. Wählen Sie [Direct connection to the Internet] (Direkte Verbindung zum Internet) aus.
4. Klicken Sie auf [OK], um die Änderungen zu speichern.

Zugriff auf das Geräte-Management des Barricade™

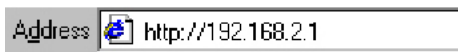
Gehen Sie wie folgt vor, um auf die web-basierende Management-Funktionen des Barricade zuzugreifen:

1. Starten Sie Ihren Web-Browser.

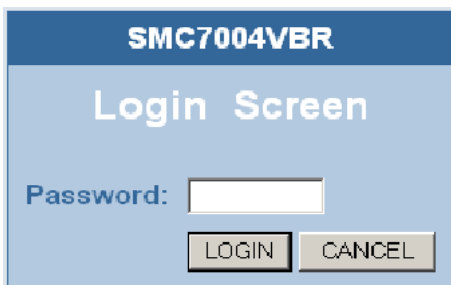
Hinweis: Ihr Computer muss nicht ONLINE sein, wenn Sie den Barricade™ Router konfigurieren wollen.

2. Geben Sie Folgendes in die Adresszeile ein:

<http://192.168.2.1>



3. Wenn der Anmeldebildschirm des Barricade™ erscheint, geben Sie das Standardkennwort ein und klicken Sie auf [Login] (Anmelden), um auf den Router zuzugreifen.



Hinweis: Das Standardkennwort des Barricade™ lautet "smcadmin". Beim Kennwort wird Groß-Kleinschreibung unterschieden.

4. Wenn Sie sich bei der web-basierenden Verwaltungsschnittstelle für den Barricade™ angemeldet haben, haben Sie zwei Möglichkeiten, die im Kapitel Arbeiten in der web-basierenden Verwaltungs- schnittstelle beschrieben werden.

ARBEITEN IN DER WEB-BASIERENDEN VERWALTUNGS- SCHNITTSTELLE

Die Verwaltungsschnittstelle des Barricade™ besteht aus einem Installationsassistenten, dem Setup Wizard, und einem Bereich [Advanced Setup] (Erweiterte Konfiguration). Mit dem Setup Wizard können Sie den Barricade™ sehr schnell für die Verwendung mit einem Kabelmodem oder DSL-Modem einrichten. Das [Advanced Setup] (Erweiterte Konfiguration) unterstützt erweiterte Funktionen wie Erkennung von Hackerangriffen, IP- und MAC-Address Filtering, Entdeckung von Eindringversuchen, Einrichtung virtueller Server, virtuelle DMZ-Hosts sowie weitere Funktionen.

Vornehmen von Konfigurationsänderungen

Konfigurierbare Parameter haben ein Dialogfeld oder eine Dropdown-Liste. Nach dem Vornehmen einer Konfigurationsänderung müssen Sie unten auf der Seite auf [Apply] (Übernehmen) oder [Next] (Weiter) klicken, um die neue Einstellung zu aktivieren.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Hinweis: Damit die Anzeige nach der Eingabe eines Befehls korrekt aktualisiert wird, muss der Internet Explorer 5.0 folgendermaßen konfiguriert sein: Unter [Tools/ Internet Options/General/Temporary Internet Files/ Settings] (Extras/Internetoptionen/Allgemein/ Temporäre Internetdateien/Einstellungen) muss die Option [Check for newer versions of stored pages] (Neuere Versionen der gespeicherten Seiten suchen) auf [Every visit to the page] (Bei jedem Zugriff auf die Seite) eingestellt sein.

SMC[®]
Networks

Setup Wizard

The Barricade setup will allow you to configure your Barricade for use with an external Cable or DSL modem. Click on the navigation menu on the left to change individual settings.

Advanced Setup

The Barricade supports advanced functions like Intrusion Detection, IP and MAC address filtering, parental control, virtual servers, and special applications. We recommend you keep the default settings.

Overview

Thank you for purchasing the SMC EX Connect Barricade Broadband Router. The Barricade is a secure device ideal for home networking and small business users alike. Its easy setup will allow you to enjoy risk-free Internet access within minutes.

Installationsassistent

Nachfolgend werden die im Bereich des Installationsassistenten zur Verfügung stehenden Optionen beschrieben. Mit diesem Assistenten müssen Sie 3 Schritte ausführen, um einen ISP zu konfigurieren.

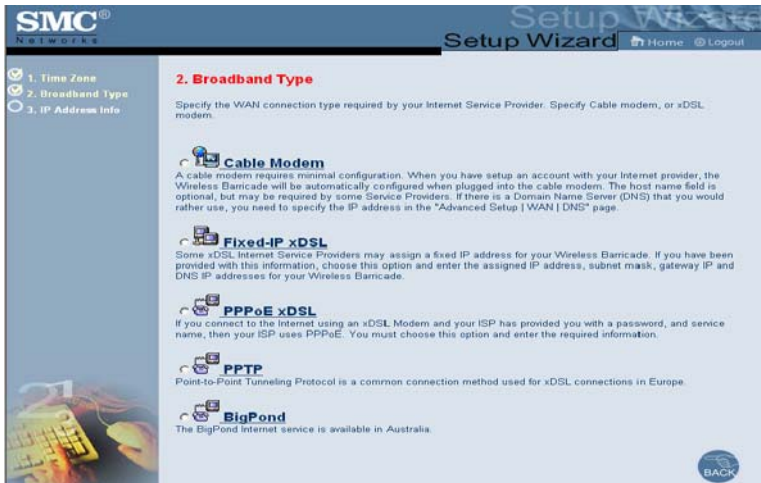
Schritt 1: Time Zone (Zeitzone)

Im ersten Schritt konfigurieren Sie die Zeitzone, in der Sie sich befinden. Diese Einstellung wird benötigt, damit die Zeitstempel für Client-Filterung und Protokolleinträge korrekt sind.



Schritt 2: Broadband Type (Breitbandtyp)

Wählen Sie den Typ der verwendeten Breitbandverbindung aus.



- **[Cable Modem]** (Kabelmodem)
Ihr ISP hat Ihnen möglicherweise eine Host-Namen gegeben. Geben Sie in diesem Fall den Namen in das Feld ein.
- **[Fixed-IP xDSL]** (xDSL-Verbindung mit fester IP-Adresse)
Einige xDSL-Internetanbieter ordnen möglicherweise eine feste (statische) IP-Adresse für Ihr Gateway zu. Wenn Sie diese Informationen erhalten haben, wählen Sie die betreffende Option und geben Sie die zugewiesene IP-Adresse, Subnetzmaske, Gateway-IP-Adresse und DNS-IP-Adresse für den Barricade™ ein.

- **[PPPoE]**

Geben Sie den PPPoE-Benutzernamen und das entsprechende Kennwort ein, die Sie von Ihrem Provider erhalten haben. Der Servicename ist normalerweise optional, kann aber bei einigen Internet-Anbietern erforderlich sein. Belassen Sie die [Maximum Transmission Unit] (maximale Übertragungseinheit, MTU) auf dem Standardwert (1492), wenn Sie keine triftigen Gründe haben, die Angabe zu ändern. Geben Sie einen Wert in Minuten für die maximale Wartezeit ein, während der die Internet-Verbindung bei fehlender Aktivität gehalten wird. Wenn die Verbindung länger als diese Zeit inaktiv ist, wird sie abgebrochen. Aktivieren Sie die Option [Auto-reconnect] (Automatische Wiederherstellung der Verbindung), falls die Verbindung automatisch wiederhergestellt werden soll, wenn erneut versucht wird, auf das Internet zuzugreifen.

- **[PPTP]**

Point-to-Point Tunneling Protocol ist eine verbreitete Verbindungsmethode, die in Europa bei xDSL-Verbindungen Verwendung findet.

- **[BigPond[®]]**

Der Internet-Service BigPond[®] wird in Australien angeboten.

Schritt 3: Finish configuration (Abschließen der Konfiguration)

Wenn Sie die Verbindung zum ISP konfiguriert haben, klicken Sie auf [Finish] (Fertig stellen). Der Barricade™ konfiguriert nun automatisch die Internet-Verbindung.

Erweiterte Konfiguration

Nachfolgend wird der Bereich [Advanced Setup] (Erweiterte Konfiguration) beschrieben. Dieser Abschnitt wird zur manuellen Konfiguration der ISP-Verbindung, zum Definieren der erweiterten Systemparameter sowie zur Verwaltung und Steuerung des Barricade™ und seiner Ports und zur Überwachung der Netzwerkbedingungen verwendet.

System

In diesem Abschnitt können Sie die örtliche Zeitzone, das Kennwort für den Administratorzugang und die IP-Adresse eines PC für die Fernverwaltung des Barricade™ konfigurieren.

- **[Time Zone]** (Zeitzone)

Geben Sie hiermit die Zeitzone für den Barricade™ an. Diese Angabe ist für Protokolleinträge und zur Client-Zugangssteuerung erforderlich.

Es gibt 3 Optionen zur Konfiguration des internen Zeitgebers des Routers:

- Verwendung voreingestellter oder benutzerdefinierter NTP-Server.
- Verwendung der Systemuhr Ihres Computers.

- Manuelle Angabe der Uhrzeit und des Datums.

SMC
Advanced Setup

System
Time Zone
Password Settings
Remote Management
WAN
LAN
NAT
Firewall
DDNS
UPnP
Tools
Status

Time Zone

Use the section below to configure the Barricade's system time. Select your timezone and configure the daylight savings option based on your location. This information is used for the time/date parental rules you can configure with the Barricade's Advanced Firewall. This information is also used for your network logging.

Once you set your time zone, you can automatically update the Barricade's internal clock by synchronizing with a public time server over the Internet. To configure this setting, choose one of the options below - each option allows a different method of updating.

Get Date and Time by online Time Servers (NTP)

Time Zone: (GMT-08:00)Pacific Time (US & Canada), Tijuana

Pre-set Servers: time.nist.gov

Custom Server: Sync Now!

Set Date and Time using PC's Date and Time

Computer Time/Date: Thursday, June 19, 2003 11:18:06 PM

Set Date and Time manually

Date: Year 2003, Month Jun, Day 19

Time: Hour 22 (D-23), Minute 35 (D-59), Second 44 (D-59)

HELP APPLY CANCEL

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

- **[Password Settings]** (Kennworteinstellungen)

In diesem Menü können Sie den Zugriff durch ein Kennwort einschränken. Das Standardkennwort des Barricade™ lautet smcadmin.

Hinweis: Kennwörter können bis zu 9 alphanumerische Zeichen enthalten und unterscheiden Groß-/Kleinschreibung.

The screenshot shows the SMC Networks Advanced Setup web interface. The page title is "Advanced Setup" and "Password Settings". The left sidebar shows a navigation menu with "System" expanded, including "Time Zone", "Password Settings", and "Remote Management". The main content area has a heading "Password Settings" and a sub-heading "Password Options" with three input fields for "Current Password", "New Password", and "Confirm New Password". Below that is the "Idle Time Out Settings" section with an "Idle Time Out" field set to "0 Mins" and a note "(Idle Time = 0 : NO Time Out)". At the bottom right are "HELP", "APPLY", and "CANCEL" buttons.

- **[Remote Management]** (Fernverwaltung)

Die Fernverwaltungsfunktion ermöglicht einem fernen PC, den Barricade™ über einen Standard-Web-Browser zu konfigurieren, zu verwalten und zu überwachen.

1. Wählen Sie [Enable] (Aktivieren).
2. Wählen Sie unter [Allow Access to] (Zulassen von Zugriff auf) eine der beiden Optionen:

[Any IP Address] (Beliebige IP-Adresse)

Sie können den Barricade™ von jeder IP-Adresse WAN-seitig verwalten.

[Single IP] (Einzelne IP-Adresse)

Sie können den Barricade™ nur von dieser IP-Adresse WAN-seitig verwalten.

[IP Range] (IP-Adressbereich)

Sie können den Barricade™ von jeder IP-Adresse in diesem Bereich fern verwalten.

3. Legen Sie den Port für die Fernverwaltung auf den Port, über den Sie fern auf den Barricade™ zugreifen wollen.

Hinweis: Es darf kein Port angegeben werden, der bereits verwendet wird. Wenn Sie z. B. einen Web-Server auf Port 80 betreiben, dürfen Sie den Port für die Fernverwaltung nicht auf 80 setzen.

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System (expanded), Time Zone, Password Settings, Remote Management (highlighted), WAN, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Remote Management" and includes the following text: "Set the remote management of the Wireless Barricade. If you want to manage the Wireless Barricade from a remote location (outside of the local network), you must also specify the IP address of the remote PC." Below this text is a configuration form with the following fields: "Remote Management" with radio buttons for "Enable" and "Disable" (selected); "Allow Access to:" with radio buttons for "Any IP Address" (selected), "Single IP:" (with an empty text input), and "IP Range:" (with two empty text inputs separated by a tilde); and "Remote Management Port:" with a text input containing "88". At the bottom right of the form are three circular buttons: "HELP", "APPLY", and "CANCEL".

WAN

Geben Sie den von Ihrem Internet-Anbieter angegebenen WAN-Verbindungstyp ein und klicken Sie dann auf [More Configuration] (Weitere Konfigurationsangaben), um detaillierte Konfigurationsparameter für den ausgewählten Verbindungstyp festzulegen.

- **[Dynamic IP]** (Dynamische IP)

Der Host-Name ist normalerweise optional, kann aber bei einigen Internet-Anbietern erforderlich sein. Die Standard-MAC-Adresse wird auf die physische WAN-Schnittstelle auf dem Barricade™ gesetzt. Verwenden Sie diese Adresse, wenn Sie sich für den Internet-Service registrieren lassen, und ändern Sie sie nicht, außer wenn Ihr Internet-Anbieter Sie dazu auffordert. Wenn Ihr Provider die MAC-Adresse einer Ethernet-Karte beim Einrichten Ihres Breitband-Kontos als Kennung verwendete, schließen Sie nur den PC mit der registrierten MAC-Adresse an den Barricade™ an und klicken Sie auf [Clone MAC Address] (MAC-Adresse kopieren) an. Hierdurch wird die aktuelle Barricade™-MAC-Adresse durch die bereits registrierte MAC-Adresse der Ethernet-Karte ersetzt.

Wenn Sie sich nicht sicher sind, wie die registrierte MAC-Adresse lautet, wenden Sie sich an Ihren ISP und lassen Sie eine neue MAC-Adresse für Ihr Konto registrieren. Führen Sie die Registrierung mit der MAC-Adresse des Barricade™ durch.

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

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

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

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

Below the text is a form with the following fields and buttons:

Host Name	<input type="text"/>	<input type="button" value="Clone MAC Address"/>
MAC Address	<input type="text" value="00-50-18-1A-11-1B"/>	<input type="button" value="Clone MAC Address"/>

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

- **[PPPoE]**

Geben Sie den PPPoE-Benutzernamen und das entsprechende Kennwort ein, die Sie von Ihrem Provider erhalten haben. Der Servicename ist normalerweise optional, kann aber bei einigen Internet-Anbietern erforderlich sein. Der MTU-Wert (Maximum Transmission Unit, maximale Übertragungseinheit) steuert die maximale Größe der Datenpakete. Belassen Sie den Wert auf dem Standardwert (1492), wenn Sie keine triftigen Gründe haben, ihn zu ändern.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Geben Sie einen Wert in Minuten für die [Maximum Idle Time (in minutes)] (Maximale Wartezeit (in Minuten)) ein, während der die Internet-Verbindung bei fehlender Aktivität gehalten wird. Wenn die Verbindung länger als diese Zeit inaktiv ist, wird sie abgebrochen. Aktivieren Sie die Option [Auto-reconnect] (automatische Wiederherstellung der Verbindung), falls die Verbindung automatisch wiederhergestellt werden soll, wenn eine Anwendung erneut versucht, auf das Internet zuzugreifen.

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN, Dynamic IP, PPPoE (highlighted), Static IP, BigPond®, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "PPPoE" and contains the following text: "Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet Service Provider requires the use of PPPoE, enter the information below."

User Name	<input type="text"/>
Password	<input type="password"/>
Please retype your password	<input type="password"/>
Service Name	<input type="text"/>
MTU	1492 (1440<=MTU Value<=1492)
Maximum Idle Time (0-60)	10 (minutes)
	<input checked="" type="checkbox"/> Auto-reconnect

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

- **[PPTP]**

Point-to-Point Tunneling Protocol (PPTP) ermöglicht den sicheren Fernzugriff über das Internet durch einfaches Einwählen an einem lokalen Punkt, den der Provider zur Verfügung stellt. Der obige Bildschirm ermöglicht Client-PCs das Einrichten einer normalen PPTP-Sitzung und erlaubt die problemlose Konfiguration des PPTP-Clients auf jedem Client-PC.

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE, PPTP (highlighted), Static IP, BigPond, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'PPTP' and includes a descriptive text: 'Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.' Below this is a configuration form with the following fields and values:

PPTP Account:	<input type="text"/>
PPTP Password:	<input type="password"/>
Please retype your password:	<input type="password"/>
Service IP Address:	<input type="text" value="0.0.0.0"/>
My IP Address:	<input type="text" value="0.0.0.0"/>
My Subnet Mask:	<input type="text" value="255.255.255.0"/>
Connection ID:	<input type="text"/>
MTU:	<input type="text" value="1492"/> (1400-1460)
Maximum Idle Time (0-60):	<input type="text" value="10"/> (minutes)
	<input checked="" type="checkbox"/> Auto-reconnect

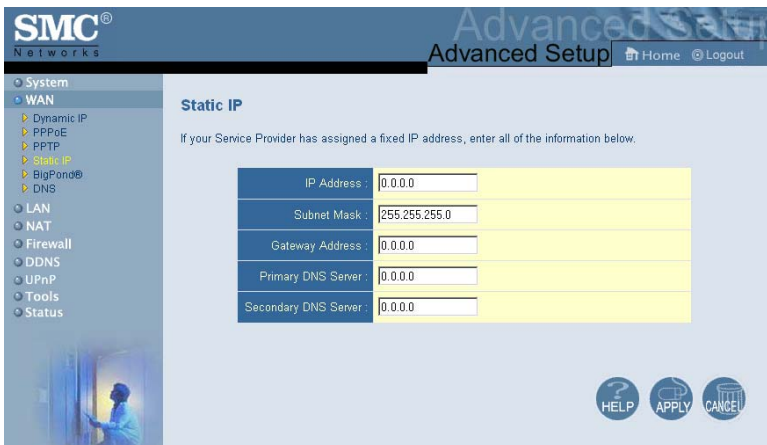
At the bottom right of the interface are three circular buttons: HELP, APPLY, and CANCEL.

Hinweis: Das Setzen von [Maximum Idle Time] (maximale Wartezeit) auf [0] und/oder die Aktivierung der Option [Auto-Reconnect] (automatische Wiederherstellung der Verbindung) kann eine Erhöhung Ihrer Telefonrechnung bewirken, wenn Sie keine „Flatrate“ (Pauschalzugang zum Internet) haben.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

- **[Static IP]** (Statische IP)

Wenn Ihr Internet-Provider Ihnen eine feste IP-Adresse zugewiesen hat, geben Sie diese IP-Adresse sowie die vom Provider bereitgestellte Subnetzmaske für den Barricade™ und die Gateway-Adresse Ihres ISP ein. Sie brauchen möglicherweise eine feste Adresse, wenn Sie Internet-Dienste wie einen Web-Server oder einen FTP-Server bereitstellen wollen.



The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP (highlighted), BigPond®, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Static IP" and includes the instruction: "If your Service Provider has assigned a fixed IP address, enter all of the information below." Below this instruction is a form with five rows, each with a label and a text input field:

IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Address :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>

At the bottom right of the interface, there are three circular buttons: HELP (with a question mark icon), APPLY (with a checkmark icon), and CANCEL (with a trash can icon).

- **[BigPond®]**

In diesem Abschnitt können Sie den integrierten Client konfigurieren.

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

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text"/> (optional)

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

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

- **[DNS]**

Domänennamensserver (DNS-Server) stellen die Verbindung zwischen numerischen IP-Adressen und den entsprechenden Domänen-Namen (z. B. www.smc.de oder www.smc-europe.com) her. Ihr Internet-Anbieter sollte Ihnen die IP-Adresse eines oder mehrerer Domänennamensserver mitteilen. Geben Sie diese Adressen auf dieser Anzeige ein.

The screenshot shows the SMC Networks Advanced Setup web interface. The top navigation bar includes the SMC logo, the text "Advanced Setup", and links for "Home" and "Logout". A left sidebar menu lists various system settings: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP, BigPond®, DNS (highlighted), LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "DNS" and contains a descriptive paragraph: "A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 202.42.118.222. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here." Below the text are two input fields: "Primary DNS Server:" and "Secondary DNS Server:", both containing the placeholder "0.0.0.0". At the bottom right of the interface are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

LAN

Von diesem Abschnitt aus können Sie die TCP/IP-Einstellungen für die Barricade™-LAN-Schnittstelle und DHCP-Clients konfigurieren.

- **LAN IP**

Verwenden Sie das Menü [LAN], um die LAN-IP-Adresse für den Barricade™ zu konfigurieren und dem DHCP-Server die dynamische Client-Adressenzuordnung zu ermöglichen. Geben Sie einen Zeitraum für das Ausleihen von IP-Adressen an, falls dies erforderlich ist. Für privat eingesetzte Netzwerke kann diese auf [Forever] (Unbegrenzt) gesetzt werden; dies bedeutet, dass für das Ausleihen von IP-Adressen keine zeitliche Beschränkung gilt.

- **IP-Adresspool**

Vom Benutzer kann eine dynamische Start-IP-Adresse angegeben werden, z. B. 192.168.2.100 (Standardwert). In diesem Beispiel gehen die IP-Adressen von 192.168.2.100 bis 192.168.2.199 und gehen dadurch in den Pool für die dynamischen IP-Adressen über. Die IP-Adressen von 192.168.2.2 bis 192.168.2.99 und von 192.168.2.200 bis 192.168.2.254 stehen als statische IP-Adressen zur Verfügung.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Hinweis: Die Adresse des Barricade™ darf nicht für den Pool der DHCP-Client-Adressen angegeben werden.

The screenshot shows the 'LAN Settings' page in the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with options: System, WAN, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'LAN Settings' and includes a descriptive paragraph: 'You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Wireless Barricade must have an IP address for the local network.' Below this are two configuration sections: 'LAN IP Settings' and 'DHCP Server Settings'. The 'LAN IP Settings' section has fields for IP Address (192.168.2.1), Subnet Mask (255.255.255.0), and a DHCP Server checkbox (checked 'Enable'). The 'DHCP Server Settings' section has a Lease Time dropdown (set to 'One Week'), a Start IP Address pool (192.168.2.100), and an End IP Address pool (192.168.2.199). At the bottom right, there are three buttons: HELP, APPLY, and CANCEL.

NAT

In diesem Abschnitt können Sie die Funktionen für [Virtual Server] (Virtueller Server) und [Special Application] (Spezielle Anwendung), mit denen die Port-Öffnungen in der Firewall des Routers gesteuert werden, konfigurieren. In diesem Abschnitt kann Unterstützung für verschiedene Internet-basierte Anwendungen, wie z. B. VPN-Verbindungen, konfiguriert werden.

- **[Virtual Server]** (Virtueller Server)

Sie können den Barricade™ als virtuellen Server konfigurieren. Ferne Benutzer, die über öffentliche IP-Adressen auf Dienste wie WWW oder FTP auf Ihrer lokalen Site zugreifen, können automatisch auf lokale, mit privaten IP-Adressen konfigurierte Server umgeleitet werden. Für maximale Flexibilität kann der Barricade™ einen einzelnen Port (80) oder einen Bereich von Ports (80-100) unterstützen. Der Datentyp kann als TCP, UDP oder beides (UDP und TCP) definiert werden.

Zu den häufiger genutzten Ports gehören: HTTP: 80, FTP: 21, Telnet: 23 und POP3: 110.

Virtual Server

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

Wait known services:

ID	IP Address	Ports	Data Type	Enable
1	192.168.2.1		TCP	<input checked="" type="checkbox"/>
2	192.168.2.1		TCP	<input checked="" type="checkbox"/>
3	192.168.2.1		TCP	<input checked="" type="checkbox"/>
4	192.168.2.1		TCP	<input checked="" type="checkbox"/>
5	192.168.2.1		TCP	<input checked="" type="checkbox"/>
6	192.168.2.1		TCP	<input checked="" type="checkbox"/>
7	192.168.2.1		TCP	<input checked="" type="checkbox"/>
8	192.168.2.1		TCP	<input checked="" type="checkbox"/>
9	192.168.2.1		TCP	<input checked="" type="checkbox"/>
10	192.168.2.1		TCP	<input checked="" type="checkbox"/>
11	192.168.2.1		TCP	<input checked="" type="checkbox"/>
12	192.168.2.1		TCP	<input checked="" type="checkbox"/>
13	192.168.2.1		TCP	<input checked="" type="checkbox"/>
14	192.168.2.1		TCP	<input checked="" type="checkbox"/>
15	192.168.2.1		TCP	<input checked="" type="checkbox"/>
16	192.168.2.1		TCP	<input checked="" type="checkbox"/>
17	192.168.2.1		TCP	<input checked="" type="checkbox"/>
18	192.168.2.1		TCP	<input checked="" type="checkbox"/>
19	192.168.2.1		TCP	<input checked="" type="checkbox"/>
20	192.168.2.1		TCP	<input checked="" type="checkbox"/>

- **[Special Applications]** (Spezialanwendungen)

Einige Anwendungen, z. B. Internetspiele, Videokonferenzen, Internet-Telefonie u. a, benötigen mehrere Verbindungen. Diese Anwendungen funktionieren nicht, wenn Network Address Translation (NAT, Netzwerkadressumsetzung) aktiv ist. Wenn Sie Anwendungen ausführen müssen, die mehrere Verbindungen benötigen, geben Sie in der folgenden Anzeige die weiteren öffentlichen Ports an, die für jede Anwendung geöffnet werden sollen.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Geben Sie den Port oder Port-Bereich, der normalerweise der Anwendung zugewiesen ist, im Feld [Trigger Port] (Auslöser-Port) an, wählen Sie als Protokolltyp TCP oder UDP aus und geben Sie dann die öffentlichen Ports und den Datentyp an, die dem Auslöser-Port zugewiesen sind, um sie für den eingehenden Datenverkehr zu öffnen.

Der maximale Bereich, der für alle NAT-Ports angegeben werden kann, ist 0 bis 65535.

Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Popular applications:

ID	Trigger Ports	Trigger Type	Incoming Port's	Data Type	Enable
1	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
2	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
3	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
4	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
5	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
6	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
7	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
8	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
9	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
10	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>

HELP APPLY CANCEL

Firewall

Die Firewall wirkt sich kaum auf die Systemleistung aus. Es empfiehlt sich, sie zum Schutz Ihrer Netzwerkbenutzer aktiviert zu lassen. Wenn Sie die SPI-Firewall (Stateful Packet Inspection) aktivieren wollen, klicken Sie auf [Advanced] (Erweitert) im Abschnitt [Firewall], wählen Sie [Enable] (Aktivieren) aus und klicken Sie auf [Apply] (Übernehmen).

Die SPI-Firewall des Barricade™ ermöglicht die Zugangskontrolle angeschlossener Client-PCs und blockt übliche Hackerangriffe ab, darunter IP-Spoofing, Land-Angriff, Ping-of-Death, IP-Pakete mit der Länge Null, Smurf-Angriff, UDP-Port-Loopback, Snork-Angriff, TCP-Nullscan und TCP-SYN-Flooding.

- **[Parental Control:]** (Zugangskontrolle:)

Mit dieser Option können Sie verschiedene Rechte für die Client-PCs festlegen. Die Funktion erlaubt das Kontrollieren des Zugangs von Kindern und Jugendlichen zu bestimmten Inhalten und/oder zum Internet allgemein an bestimmten Tagen und zu bestimmten Uhrzeiten.

Folgendermaßen definieren Sie eine Regel für die Zugangskontrolle: Klicken Sie auf [Click here to configure a new Parental Control Rule] (Hier klicken, um eine Regel für die Zugangskontrolle zu definieren). Hierdurch gelangen Sie zum Abschnitt [Rule Setup] (Definition der Regel).



Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Rule Description :	<input type="text"/>	
DHCP menu option :	<input type="radio"/> Computer Name : <input type="text" value="DHCP client list"/>	
	<input checked="" type="radio"/> Single IP : 192.168.2. <input type="text" value="0"/>	
	<input type="radio"/> IP Range : 192.168.2. <input type="text"/> - <input type="text"/>	
Schedule for Rule :	<input checked="" type="radio"/> Rule is Active all the time <input type="radio"/> Set Time and Date Rule is Active	

Pre-Defined Blocking Options		
Block	Block Information	Enable
..Any Internet Access	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input type="checkbox"/>
..Specific Web Sites	Set Web Sites and Keywords you want to block	<input type="checkbox"/>
..Secure Web Sites	HTTPS, TCP Port 443	<input type="checkbox"/>
..E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
..E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
..Newsgroup Access	NNTP, TCP Port 119	<input type="checkbox"/>
..FTP Access	FTP, TCP Port 20,21	<input type="checkbox"/>

Custom Blocking Options		
Block	Port Types	Enable
Ports: <input type="text"/> - <input type="text"/>	<input type="text" value="TCP"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text" value="TCP"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text" value="TCP"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text" value="TCP"/> Traffic	<input type="checkbox"/>

- **[Rule Description:]** (Beschreibung der Regel:)

Geben Sie eine Beschreibung der Regel ein.
Beispiel: „Veras Internet-Zugang“.

- **[DHCP menu option:]** (DHCP-Menüoption:)

Wenden Sie diese Regel auf eine bestimmte IP-Adresse oder einen bestimmten Bereich von IP-Adressen in Ihrem LAN an. Sie können über die DHCP-Client-Liste schnell IP-Adressen hinzufügen, die durch DHCP-Verbindungen bereitgestellt wurden.

- **[Schedule for Rule:]** (Zeitplan für Regel:)

Geben Sie Datum und Uhrzeit für die Gültigkeit dieser Regel an. Sie können angeben, dass die Regel immer gültig ist, oder einen bestimmten Gültigkeitszeitraum angeben.

Sie können angeben, in welchem Zeitraum diese Regel gültig sein soll, indem Sie das Feld neben dem Datum markieren.

Als Zeitangabe legen Sie fest, ab welcher Uhrzeit und wie lange die Regel gelten soll.

Schedule for Rule :	<input type="radio"/> Rule is Active all the time <input checked="" type="radio"/> Set Time and Date Rule is Active
Rule is Active on :	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday
Rule Starts at :	<input type="text"/> : <input type="text"/> AM
Rule is Active for :	<input type="text"/> hours <input type="text"/> minutes

- **[MAC Filtering Table:]** (MAC-Filterung:)

Mit der MAC-Filterungsfunktion des Barricade™ können Sie den Zugriff auf Ihr Netzwerk auf Grundlage der MAC-Adresse (Media Access Control, Medienzugriffssteuerung) des Clients steuern. Diese ID ist für jeden Netzwerkadapter spezifisch.

Sie können festlegen, dass die MAC-Adresse Zugang zu Ihrem Netzwerk erhält, oder ihr den Zugang zum Netz verweigern.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Mit dieser Funktion können DHCP-IP-Adressen auch auf bestimmte MAC-Adressen abgebildet werden. Sie ermöglicht zusammen mit den Zugangskontrollregeln eine optimale Steuerung.

The screenshot shows the 'MAC Filtering Table' configuration page in the SMC Advanced Setup interface. The page includes a navigation menu on the left, a main title 'MAC Filtering Table', and a sub-header 'Advanced Setup'. Below the title, there is a description: 'This section helps promote MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.' The configuration area contains a 'MAC Address Control' section with 'Enable' selected and a 'DHCP Client List' dropdown menu. Below this is a table with 8 rows for configuring MAC filtering rules. The table has columns for ID, Computer Name, IP Address, MAC Address, Action, and Deny. At the bottom right, there are buttons for 'HELP', 'APPLY', and 'CANCEL'.

ID	Computer Name	IP Address	MAC Address	Action	Deny
1		192.168.2			
2		192.168.2			
3		192.168.2			
4		192.168.2			
5		192.168.2			
6		192.168.2			
7		192.168.2			
8		192.168.2			

- **[Website Blocking] (Website-Blockierung)**

Die Funktion [Website Blocking] (Website-Blockierung) des Barricade™ blockiert den Zugriff auf Website-Domänen (z. B. www.somesite.com) oder auf Websites, die ein angegebenes Schlüsselwort im URL haben. Auf diese Weise können Sie Personen vor problematischen Inhalten im Internet schützen.

The screenshot shows the 'Website Blocking' configuration page in the SMC Advanced Setup interface. The page includes a navigation menu on the left, a main title 'Website Blocking', and a sub-header 'Advanced Setup'. Below the title, there is a description: 'You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site. To specify the PCs that you want to block these websites to, go to the "Parental Control" page and check the box for "Block Specific Web Sites" in the "Pre-Defined Blocking Options" section.' The configuration area contains a table with 23 rows for configuring website blocking rules. The table has columns for Site Number, URL / Keyword, and Rule Number. At the bottom, there is a 'Clear All URLs and Keywords' button. At the bottom right, there are buttons for 'HELP', 'APPLY', and 'CANCEL'.

Site Number	URL / Keyword	Rule Number
Site 1		Site 2
Site 3		Site 4
Site 5		Site 6
Site 7		Site 8
Site 9		Site 10
Site 11		Site 12
Site 13		Site 14
Site 15		Site 16
Site 17		Site 18
Site 19		Site 20
Site 21		Site 22
Site 23		Site 24

- **[Advanced Firewall Settings]**
(Erweiterte Firewall-Einstellungen)

In diesem Abschnitt können Sie verschiedene erweiterte Funktionen für die Firewall des Barricade™ konfigurieren.

The screenshot shows the 'Advanced Firewall Settings' page in the SMC Networks Advanced Setup utility. The interface includes a left-hand navigation menu with categories like System, WAN, LAN, NAT, and Firewall. The Firewall section is expanded, showing sub-options such as Firewall Control, MAC Filter, Website Blocking, Advanced, DMZ, DDNS, UPnP, Tools, and Status. The main content area is titled 'Advanced Firewall Settings' and contains a descriptive paragraph, an email alert configuration section, and three main configuration sections: FIREWALL Options, VPN Passthrough, and EMAIL Settings. Each section contains a table of settings with radio buttons for 'Enable' and 'Disable' and input fields for email-related settings. At the bottom right, there are buttons for HELP, APPLY, and CANCEL.

SMC® NETWORKS Advanced Setup Home Logout

Advanced Firewall Settings

Use this section to configure the advanced settings of your Barricade Firewall. You can enable/disable each option depending on your requirements. If you want to be alerted via email for hacker attacks, please configure the email alert option.

Email Alerts require you to set an SMTP (outgoing) mail server to send the email. Your username and password are also required as most ESPs are using outgoing authentication to cut down on SPAM.

FIREWALL Options	
Advanced Firewall Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Discard Ping From WAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

VPN Passthrough	
PPTP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPSec	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

EMAIL Settings	
Your Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
User name	<input type="text"/>
Password	<input type="text"/>

HELP APPLY CANCEL

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

Folgende Funktionen können festgelegt werden:

[Advanced Firewall Protection]

(Erweiterter Firewall-Schutz)

Aktivieren/Deaktivieren des SPI-Abschnitts der Firewall.

[Discard Ping from WAN]

(Ping aus dem WAN verwerfen)

Wenn diese Funktion aktiviert ist, kann kein Host im WAN einen Ping für das Produkt ausführen. Dies verhindert Angriffe aus dem WAN, weil die Verbindung unsichtbar ist. Das Aktivieren dieser Option wird aus Sicherheitsgründen empfohlen.

[VPN Pass-through]

Aktivieren Sie diese Option, wenn Sie eine PPTP-, L2TP- oder IPsec-VPN-Verbindung verwenden.

[Email Settings] (E-Mail-Einstellungen)

Konfigurieren Sie diese Option, wenn Sie vom Barricade™ per E-Mail benachrichtigt werden möchten, wenn Hacker versuchen, das Netzwerk anzugreifen. Sie müssen Ihre E-Mail-Adresse, den Benutzernamen und das Kennwort sowie einen SMTP-Server, über den die Mail gesendet werden soll, angeben.

- **[DMZ] (Demilitarized Zone) (Entmilitarisierte Zone)**

Wenn Sie einen Client-PC haben, der eine Internet-Anwendung hinter der Firewall nicht korrekt ausführen kann, können Sie den Client-PC für uneingeschränkten Internetzugang in beide Richtungen öffnen. Sie können die LAN-IP-Adresse eines DMZ-Hosts eingeben und auf [Enable] (Aktivieren) klicken.

Hinweis: Das Hinzufügen eines Clients zur DMZ kann Ihr lokales Netzwerk für eine Reihe von Sicherheitsrisiken anfällig machen. Diese Option sollte deshalb nur verwendet werden, wenn es absolut erforderlich ist.

DDNS Settings (Dynamische DNS-Einstellungen)

Der Barricade™ verfügt über eine integrierte Funktion für dynamische DNS-Zuweisung, mit der Benutzer im Internet ihre(n) Domännennamen an bestimmte Computer oder Server binden können. Mit DDNS folgt Ihr Domänenname automatisch Ihrer IP-Adresse, indem Ihre DNS-Einträge geändert werden, wenn sich Ihre IP-Adresse ändert.

In diesem Bereich befindet sich auch ein Abschnitt [Server Configuration] (Serverkonfiguration), der automatisch die Port-Optionen öffnet, die im Abschnitt [Virtual Server] (Virtueller Server) markiert wurden. Geben Sie einfach die IP-Adresse Ihres Servers, z. B. des Web-Servers, ein und klicken Sie dann auf die Port-Option [HTTP Port 80], damit Benutzer über die WAN-Verbindung (Internet) auf den Server zugreifen können.

The screenshot shows the 'Advanced Setup' interface for SMC Networks. The left sidebar contains a navigation menu with options: System, WAN, LAN, NAT, Firewall, DDNS (selected), UPnP, Tools, and Status. The main content area is titled 'DDNS (Dynamic DNS) Settings'. It includes a description: 'Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.' Below this is a 'Dynamic DNS' section with a radio button for 'Enable' (selected) and a 'Disable' option. The 'Service Configuration' section contains fields for 'DNS Service' (set to 'DynDNS.org(Dynamic)'), 'Domain Name', 'Username / E-mail', and 'Password / Key'. The 'Server Configuration' section shows 'Server IP' as '192.168.2.' and 'Server Type' with checkboxes for 'Web Server: (HTTP) Port 80', 'Port 8000', 'FTP Server: Port 20', 'Port 21', and 'Email Server:(POP3) Port 110', 'SMTP: Port 25'. At the bottom right are 'HELP', 'APPLY', and 'CANCEL' buttons.

UPnP

Der Barricade™ unterstützt UPnP (Universal Plug and Play), eine Netzwerkarchitektur, die die Kompatibilität verschiedener Netzwerkkomponenten ermöglicht. Mithilfe dieser Funktion kann ein UPnP-basiertes Betriebssystem wie Windows XP automatisch mit dem Barricade™ kommunizieren und die erforderlichen Services bei Bedarf öffnen.

Tools (Extras)

Mit dem Menü [Tools] können Sie die aktuelle Konfiguration sichern, eine zuvor gespeicherte Konfiguration wiederherstellen, die Werkseinstellungen wiederherstellen, die Firmware aufrüsten und den Barricade™ zurücksetzen.

- **[Configuration Tools]** (Konfigurationswerkzeuge)

[Backup Router Settings] (Router-Einstellungen sichern)

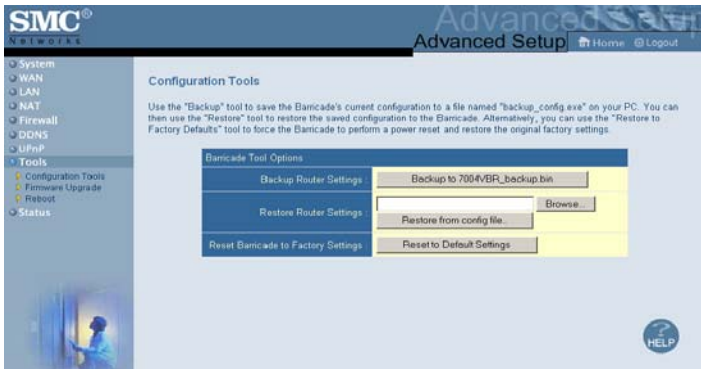
Mit dieser Funktion wird die Konfiguration des Barricade™ in einer Datei gespeichert.

[Restore Router Settings] (Router-Einstellungen wiederherstellen)

Mit dieser Funktion können Sie Einstellungen mithilfe einer gespeicherten Sicherungskopie der Konfigurationsdatei wiederherstellen.

[Reset Barricade to Factory Settings] (Barricade auf Werkseinstellungen zurücksetzen)

Aktiviert beim Wireless Barricade™ wieder die ursprünglichen Werkseinstellungen.



- **[Firmware Upgrade]** (Firmware-Aufrüstung)
Diese Funktion erlaubt das problemlose Herunterladen der aktuellsten Firmware. Laden Sie die Aktualisierungsdatei von der SMC-Website (www.smc.de oder www.smc-europe.com) und speichern Sie sie auf Ihrer Festplatte. Wählen Sie die Datei aus und klicken Sie dann auf [Apply] (Übernehmen). Vergewissern Sie sich im Abschnitt [Status page Information] (Information über Statusseite), dass die Aktualisierung erfolgreich war.
- **[Reboot]** (Neustart)
Klicken Sie auf [Apply] (Anwenden), um den Barricade™ neu zu starten. Die Zurücksetzung ist beendet, wenn die Netz-LED nicht mehr blinkt.

Hinweis: Nach der Aktivierung einiger Optionen muss der Router zurückgesetzt werden. Mit dieser Option kann diese Funktion ausgeführt werden.

Status

Das Fenster [Status] zeigt den WAN/LAN-Verbindungsstatus, die Firmware- und Hardwareversionsnummern, unerlaubte Versuche zum Zugriff auf Ihr Netzwerk sowie Informationen zu mit Ihrem Netzwerk verbundenen DHCP-Clients an.

Dieses Fenster enthält die folgenden Elemente:

- **INTERNET**
Zeigt den Typ und den Status der WAN-Verbindung an.
- **GATEWAY**
Zeigt die IP-Einstellungen des Systems sowie den DHCP- und Firewall-Status an.

Arbeiten in der web-basierenden Verwaltungs- schnittstelle

- **INFORMATION**

Zeigt die Anzahl angeschlossener Clients, die Firmwareversionen, die physische MAC-Adresse für jede Medienschnittstelle und die Hardwareversion und Seriennummer an.

- **Sicherheitsprotokoll**

Zeigt unzulässige Zugriffsversuche auf Ihr Netzwerk an.

- [Save] (Speichern): Klicken Sie auf diese Schaltfläche, um eine Datei mit einem Sicherheitsprotokoll zu speichern.
- [Clear] (Löschen): Klicken Sie auf diese Schaltfläche, um das Zugriffsprotokoll zu löschen.
- [Refresh] (Aktualisieren): Klicken Sie auf diese Schaltfläche, um die Anzeige zu aktualisieren.

- **DHCP-Clientprotokoll**

Zeigt Informationen zu allen DHCP-Clients in Ihrem Netzwerk an.

Weitere Informationen über den Router 7004VBR V.2 finden Sie unter www.smc.de oder www.smc-europe.com.

FEHLERBEHEBUNG

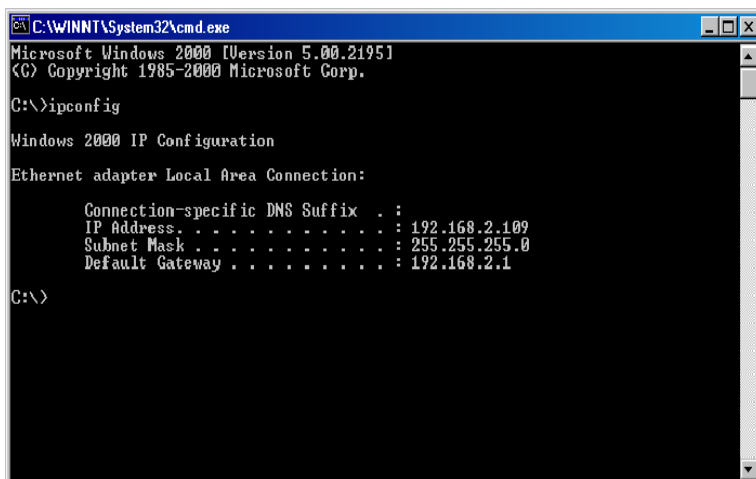
Dieser Abschnitt enthält einige nützliche Hinweise dazu, wie Sie Ihren Computer und den Barricade™-Router online bekommen.

1. Vergewissern Sie sich, dass eine Verbindung zum Barricade™ Router besteht

Wenn Sie nicht auf die web-basierende Funktion zur Verwaltung des Barricade™ zugreifen können, ist möglicherweise die Verbindung oder Konfiguration nicht korrekt. Die Abbildungen in diesem Abschnitt wurden auf einem Windows 2000-Computer erstellt, aber die Vorgehensweisen gelten ebenso für Windows 95/98/Me/XP.

Gehen Sie wie folgt vor, um den Status der TCP/IP-Konfiguration zu ermitteln:

1. Klicken Sie auf [Start] und wählen Sie [Run] (Ausführen).
2. Geben Sie cmd oder command ein (ohne Anführungszeichen), um eine DOS-Eingabeaufforderung zu öffnen.
3. Geben Sie im DOS-Fenster ipconfig ein und überprüfen Sie die angezeigten Informationen.
4. Wenn Ihr Computer für DHCP eingerichtet ist, sollte Ihre TCP/IP-Konfiguration ähnlich wie folgt aussehen:
 - [IP Address] (IP-Adresse) 192.168.2.X
(x ist eine Zahl von 100 bis 199).
 - [Subnet] (Subnetz): 255.255.255.0.
 - [Gateway]: 192.168.2.1.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\>
```

Wenn die IP-Adresse mit 169.254.XXX.XXX beginnt, lesen Sie Abschnitt 2. Es wird eine andere IP-Adresse angezeigt.

Falls Sie eine andere IP-Adresse konfiguriert haben, lesen Sie Abschnitt 3.

2. Die IP-Adresse beginnt mit 169.254.XXX.XXX

Wenn eine solche IP-Adresse angezeigt wird, müssen Sie überprüfen, ob eine einwandfreie Verbindung zum Barricade™ Router besteht.

Vergewissern Sie sich, dass die Verbindungs-LED des Barricade™ Routers für den Port leuchtet, an den dieser Computer angeschlossen ist. Wenn dies nicht der Fall ist, versuchen Sie, ein anderes Kabel zu verwenden.

Wenn die LED leuchtet, öffnen Sie ein DOS-Fenster, wie in Abschnitt 1 beschrieben, und geben Sie `ipconfig/renew` ein.

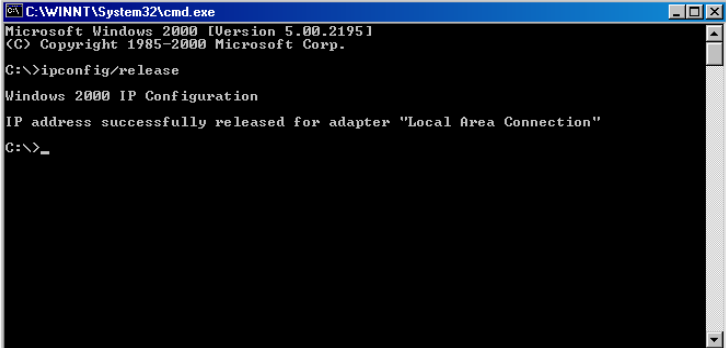
Wenn Sie noch immer keine IP-Adresse vom Barricade™ erhalten, müssen Sie Ihren Netzwerkadapter neu installieren. Entnehmen Sie die hierzu erforderlichen Informationen der Dokumentation des Adapters.

3. Es wird eine andere IP-Adresse angezeigt

Wenn eine andere IP-Adresse angezeigt wird, ist der PC möglicherweise nicht für eine DHCP-Verbindung konfiguriert. Siehe das Kapitel Konfiguration des Computers.

Wenn Sie sich vergewissert haben, dass der Computer für DHCP onfiguriert ist, gehen Sie wie nachfolgend beschrieben vor.

1. Öffnen Sie ein DOS-Fenster wie oben beschrieben.
2. Geben Sie `ipconfig/release` ein.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

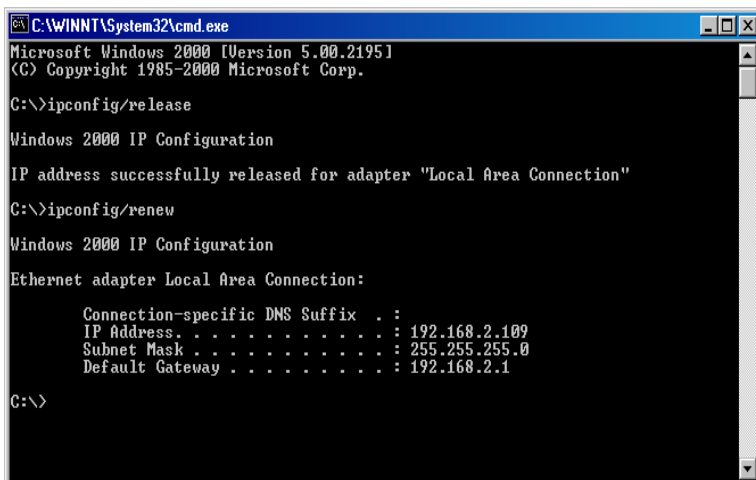
C:\>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>_
```

3. Geben Sie anschließend ipconfig/renew ein.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\>
```

Sobald Sie eine gültige IP-Adresse vom Barricade™ erhalten, können Sie auf die web-basierende Funktion zur Verwaltung zugreifen.

Wenn Sie noch immer keine IP-Adresse vom Barricade™ erhalten, setzen Sie den Router wie im Kapitel Kennenlernen des Barricade™ beschrieben zurück und führen Sie die in diesem Anhang beschriebenen Schritte erneut aus.

Wenn Sie nach dem Zurücksetzen immer noch nicht auf den Router zugreifen können, müssen Sie sich an den Technischen Support von SMC wenden.

4. Es wird eine Verbindung mit dynamischer IP verwendet und das System geht nicht online

Die meisten Kabelgesellschaften verwenden eine Konfiguration mit dynamischer IP-Adresse, um den Zugriff auf das Internet zu ermöglichen. Falls auch Sie eine solche Verbindung verwenden und keine Verbindung aufbauen können, gehen Sie wie folgt vor:

1. Trennen Sie das Kabel- oder DSL-Modem für 2 Minuten von der Stromversorgung.
2. Vergewissern Sie sich, dass der Barricade™ Router für die Verwendung einer dynamischen IP-Adresse eingerichtet ist.
3. Verbinden Sie das Modem wieder mit der Stromversorgung.
4. Warten Sie, bis das Modem wieder eine Verbindung mit dem Netzwerk hergestellt hat, und klicken Sie dann auf die Statusseite des Routers, um sich zu vergewissern, dass Sie online sind.

Diese Vorgehensweise ist sinnvoll, da bestimmte Breitbandverbindungen eine MAC-Adresse benötigen, damit ein Zugriff auf das Netzwerk hergestellt werden kann. Diese MAC-Adresse kann durch den oben beschriebenen Vorgang geändert werden, bei dem die zugelassene MAC-Adresse in die MAC-Adresse des Barricade™ Routers geändert wird.

TECHNICAL SPECIFICATIONS

Below is an outline of the Technical Specifications for the Barricade™ 4-Port Cable/DSL Broadband Router. (SMC7004VBR V.2)

Standards

802.3, 802.3u

WAN Port

1 – 10/100Mbps RJ45, with Auto MDI/MDIX

LAN Port

4 – 10/100Mbps RJ45, with Auto MDI/MDIX

Supported WAN type

Static IP

Dynamic IP

PPP over Ethernet

PPTP

Big Pond

NAT

Maximum 253 Users

Protocol

IP Protocol

TCP/IP v4

DHCP server

Proxy DNS server

Management and Configuration

Web-based

Firewall

NAT firewall and SPI firewall

Technical Specifications

VPN

VPN pass-through including PPTP/L2TP/IPsec

User Authentication

Password protected browser-based UI PAP/CHAP/MSCHAP
Authentication protocol supported

Upgrade method

Web-based

LEDs

Power
WAN
Link
Activity

Input Power

DC 5V 2A

Operating Temperature

0°~40°C

Humidity

10%~90% non-condensing

Storage Temperature

-20°~70°C

Humidity

0~95% non-condensing

Compliance

FCC
CE
UL

Dimensions

13.2 x 8.7 x 3.3 cm

Weight

200g

COMPLIANCES

FCC Interference Statement

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

Industry Canada – Class B

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

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

EC Conformance Declaration – Class B

SMC contact for these products in Europe is:
SMC Networks Europe,
Edificio Conata II,
Calle Frutuós Gelabert 6-8, 2o, 4a,
08970 - Sant Joan Despí,
Barcelona, Spain.

This product complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the

Compliances

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:

Emission:

EN 5022: 1998+A1:2000

EN 61000-3-2: 2000, EN 61000-3-3: 1995+A1:2000

Immunity

EN 55024:1998+A1:2001,

EN 61000-4-2, 61000-4-3, 61000-4-4, 61000-4-5

EN 61000-4-6, 61000-4-11

Safety Test:

EN 60950

Safety Compliance

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlußsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.

9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8V, 50-60Hz nicht über- oder unterschreiten sowie den minimalen Strom von 1A nicht unterschreiten. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

LEGAL INFORMATION AND CONTACTS

SMC's Limited Warranty Statement

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

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

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries, either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned

Legal Information and Contacts

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.

Legal Information and Contacts

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.

