LINKSYS®

A Division of Cisco Systems, Inc.

ADSL2-Gateway

mit 4-Port-Switch

Benutzerhandbuch

VERDRAHTET

Modell-Nr. **AG241**

Cisco Systems

Copyright und Marken

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum ADSL2-Gateway mit 4-Port-Switch ist es, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. "Beachten Sie folgende Symbole:"

Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.

Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.

Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

Wort: *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

Abbildung 0-1: Kurzbeschreibung der Abbildung

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhalt unter "Abbildungsverzeichnis".

Table of Contents

List of Figures

Kapitel 1: Einführung

Willkommen

Das Linksys ADSL2-Gateway mit 4-Port-Switch ist die kompakte Internetverbindungslösung für zu Hause. Die ADSL-Modemfunktion ermöglicht eine extrem schnelle Internetverbindung, die um einiges schneller ist als Einwählverbindungen - ganz ohne Beanspruchen der Telefonleitung.

Schließen Sie Ihre Computer über den integrierten 10/100 Ethernet-Switch mit 4 Ports zum schnellen Hochfahren Ihres Netzwerks an das Gateway an. Sie können Dateien, Drucker, Festplattenspeicher und andere Ressourcen gemeinsam verwenden oder per Computerspiele gegen Spielegegner antreten. Verbinden Sie vier Computer direkt miteinander, oder hängen Sie weitere Hubs und Switches an, um die Größe des Netzwerks Ihren Bedürfnissen gemäß zu gestalten. In diesem Gateway werden all diese Vorteile vereinigt, sodass das gesamte Netzwerk von der High Speed-Internetverbindung profitieren kann.

Zum Schutz Ihrer Daten und Privatsphäre verfügt das ADSL2-Gateway mit 4-Port-Switch über eine erweiterte Firewall, mit der Eindringlinge und Angriffe über das Internet abgewehrt werden. Wireless-Datenübertragungen können durch leistungsstarke Datenverschlüsselung geschützt werden. Schützen Sie Ihre Familie mit Kinderschutzfunktionen wie die Beschränkung von Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern. Die Konfiguration ist mit jedem beliebigen Web-Browser kinderleicht.

Mit dem Linksys ADSL2-Gateway mit 4-Port-Switch im Zentrum Ihres Netzwerks sind Sie auf dem besten Weg in die Zukunft.

Der Inhalt dieses Handbuchs

In diesem Benutzerhandbuch sind die zur Einrichtung und Verwendung des ADSL2-Gateways mit 4-Port-Switch erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden das ADSL2-Gateway mit 4-Port Switch, die Anwendungen und das vorliegende Benutzerhandbuch beschrieben.

- Kapitel 2: Planen Ihres Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.

- Kapitel 3: Beschreibung des ADSL2-Gateways mit 4-Port-Switch
  In diesem Kapitel werden die physischen Funktionen des Gateways beschrieben.

- Kapitel 4: Anschließen des ADSL2-Gateways mit 4-Port-Switch
  In diesem Kapitel finden Sie Anweisungen zum Verbinden des Gateways mit dem Netzwerk.

- Kapitel 5: Konfigurieren des Gateways
  In diesem Kapitel wird erläutert, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des ADSL2-Gateways mit 4-Port-Switch erörtert.

- Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem Gateway
  In diesem Anhang finden Sie Anleitungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden.

- Anhang C: Aktualisieren der Firmware
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Firmware des Gateways, sollte dies einmal erforderlich sein.

- Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

- Anhang E: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang F: Zulassungsinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.

- Anhang G: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.

- Anhang H: Garantieinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.

- Anhang I: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressourcen, darunter auch zum technischen Support.

Kapitel 2: Planen Ihres Netzwerks

Die Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway Ihr lokales Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird Ihr Computernetzwerk geschützt, sodass Ihre Computer für andere Benutzer im Internet nicht "sichtbar" sind. Somit wird der private Charakter Ihres Netzwerks bewahrt. Das Gateway schützt Ihr Netzwerk, indem es alle über den Internet-Port eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internetanschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, sofern zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass Sie über die Ports des Gateways eine Verbindung zu zwei verschiedenen Netzwerken herstellen können. Mit den LAN-Ports können Sie eine Verbindung zum LAN und mit dem ADSL-Port eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 Mbit/s.

Abbildung 2-1: Netzwerk

***LAN**: Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.*

IP-Adressen

Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein "Standort" bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, Ihren Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das entsprechende Gerät stets dieselbe IP-Adresse hat, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, wie z. B. Server-Computern oder Druckservern, verwendet.

HINWEIS: Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzerhandbuch wird auf "Internet-IP-Adressen" und "LAN-IP-Adressen" verwiesen.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, sodass Gateway und Netzwerk unsichtbar für das Internet sind; weitere Informationen hierzu finden Sie in "Kapitel 5: Konfigurieren des Gateways" unter "Sicherheit" in der Beschreibung zum Blockieren von WAN-Anfragen.

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, wie z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als "dynamisch" bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät, wie z. B. das Gateway, fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehr als ein DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler, wie z. B. IP-Adresskonflikte, auf. Informationen zum Deaktivieren der DHCP-Funktion beim Gateway erhalten Sie in "Kapitel 5: Konfigurieren des Gateways".

Was ist ein VPN?

Ein VPN (*Virtual Private Network*) ist eine Verbindung zwischen zwei Endpunkten (z. B. ein VPN-Gateway) in verschiedenen Netzwerken, mit deren Hilfe private Daten sicher über ein gemeinsam genutztes oder öffentliches Netzwerk, wie z. B. das Internet, gesendet werden können. Dadurch wird ein privates Netzwerk aufgebaut, über das Daten sicher zwischen diesen beiden Standorten bzw. Netzwerken gesendet werden können.

Dies geschieht mithilfe eines "Tunnels". Die beiden Computer oder Netzwerke werden über einen VPN-Tunnel verbunden, durch den Daten über das Internet so übertragen werden können, als ob die Übertragung innerhalb dieser beiden Netzwerke ausgeführt würde. Dabei handelt es sich nicht um einen tatsächlichen Tunnel, sondern um eine Verbindung, die durch die Verschlüsselung der zwischen den Netzwerken gesendeten Daten gesichert wird.

VPN wurde als kostengünstige Alternative zu einer privaten, speziellen, gemieteten Leitung für ein privates Netzwerk entwickelt. Mit Verschlüsselungs- und Authentifizierungstechnologie, die den Industriestandards

entspricht (IPSec, Kurzform für *IP Security*, IP-Sicherheit), stellt das VPN eine sichere Verbindung her, die praktisch genauso funktioniert, als ob Sie direkt mit Ihrem lokalen Netzwerk verbunden wären. VPNs können zum Aufbau sicherer Netzwerke verwendet werden, durch die ein Zentralbüro mit Zweigniederlassungen, Telearbeitern und/oder Mitarbeitern im Außendienst verbunden werden kann (Reisende können eine Verbindung zu einem VPN-Gateway von jedem beliebigen Computer mit VPN-Client-Software, die IPSec, wie z. B. SSH Sentinel, unterstützt, herstellen).

Es gibt zwei grundlegende Möglichkeiten, eine VPN-Verbindung herzustellen:

- VPN-Gateway - VPN-Gateway
- Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Das VPN-Gateway erstellt einen "Tunnel" bzw. Kanal zwischen zwei Endpunkten, sodass die Datenübertragungen dazwischen sicher sind. Ein Computer mit VPN-Client-Software, die IPSec unterstützt, kann als einer der beiden Endpunkte verwendet werden. Das VPN-Gateway kann von jedem beliebigen Computer mit integriertem IPSec Security Manager (Microsoft 2000 und XP) einen VPN-Tunnel mithilfe von IPSec herstellen (weitere Informationen finden Sie in "Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem VPN-Gateway". Für andere Betriebssystemversionen von Microsoft müssen zusätzliche VPN-Client-Softwareanwendungen von Drittanbietern installiert werden, die IPSec unterstützen.

Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Im folgenden Beispiel wird ein VPN zwischen einem Computer und einem VPN-Gateway beschrieben (siehe Abb. 2-2). Eine Geschäftsfrau auf Dienstreise stellt in ihrem Hotelzimmer eine Verbindung mit ihrem ISP her. Auf ihrem Notebook-Computer ist VPN-Client-Software installiert, die mit den VPN-Einstellungen ihres Büros konfiguriert ist. Sie ruft die VPN-Client-Software auf, die IPSec unterstützt, und stellt eine Verbindung zum VPN-Gateway im Zentralbüro her. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt die Geschäftsfrau nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob sie physisch damit verbunden wäre.

VPN-Gateway - VPN-Gateway

Ein Beispiel für ein VPN zwischen zwei VPN-Gateways kann folgendermaßen beschrieben werden (siehe Abb. 2-3). Ein Telearbeiter verwendet sein VPN-Gateway zu Hause für seine stets aktive Internetverbindung. Sein Gateway ist mit den VPN-Einstellungen seines Büros konfiguriert. Wenn er eine Verbindung zum Gateway seines Büros herstellt, erstellen die zwei Gateways einen Tunnel, indem Sie die Daten ver- und entschlüsseln. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt der Telearbeiter nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob er physisch damit verbunden wäre.

Zusätzliche Informationen und Anweisungen zum Erstellen Ihres eigenen VPNs finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international oder in "Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem VPN-Gateway".

Abbildung 2-2: Computer - VPN-Gateway

WICHTIG: Sie müssen mindestens ein VPN Gateway an ein Ende des VPN-Tunnels schalten. Am anderen Ende des VPN-Tunnels muss sich ein anderes VPN-Gateway oder ein Computer mit sd VPN-Client-Software befinden, die IPSec unterstützt.

Wozu benötige ich ein VPN?

Ein Computernetzwerk bietet hochgradige Flexibilität, die bei einem auf Papier basierenden Schriftverkehr nicht gegeben ist. Mit dieser Flexibilität geht jedoch auch ein erhöhtes Sicherheitsrisiko einher. Aus diesem Grund wurden Firewalls entwickelt. Mit Firewalls werden Daten innerhalb eines lokalen Netzwerks geschützt. Aber wie wird dieser Schutz gewährleistet, sobald Informationen an ein Ziel außerhalb Ihres lokalen Netzwerks gesendet werden, wenn E-Mails gesendet werden, oder wenn Sie eine Verbindung zum Netzwerk Ihres Unternehmens herstellen müssen, während Sie unterwegs sind? Wie werden Ihre Daten geschützt?

Hier kann sich ein VPN als nützlich erweisen. VPNs sichern die Daten, die an ein Ziel außerhalb Ihres Netzwerks gesendet werden, so als ob sie sich immer noch innerhalb des Netzwerks befänden.

Wenn von Ihrem Computer Daten über das Internet gesendet werden, sind sie stets Angriffen ausgesetzt. Möglicherweise verfügen Sie bereits über eine Firewall, mit der die Daten, die verschoben oder an Ziele innerhalb Ihres Netzwerks gesendet werden, vor Angriffen und Beschädigungen von Einheiten außerhalb Ihres Netzwerks geschützt werden. Sobald jedoch Daten an Ziele außerhalb Ihres Netzwerks gesendet werden, d. h. wenn Sie Daten per E-Mail versenden oder mit jemandem über das Internet kommunizieren, werden die Daten nicht mehr durch die Firewall geschützt.

Ihre Daten sind nun Hackern ausgesetzt, die mit einer Reihe von Methoden nicht nur die übertragenen Daten, sondern auch Ihre Netzwerkanmelde- und Sicherheitsdaten stehlen können. Dies sind einige der gängigsten Methoden:

1) MAC-Adressen-Spoofing

Paketen, die über ein Netzwerk, entweder Ihr lokales Netzwerk oder das Internet, übertragen werden, wird eine Paket-Kopfzeile vorangestellt. Diese Paket-Kopfzeilen enthalten sowohl Quell- als auch Zielinformationen, damit das Paket zügig übertragen wird. Ein Hacker kann diese Informationen zum Spoofing (Fälschen) einer auf dem Netzwerk zugelassenen MAC-Adresse verwenden. Mit dieser gefälschten MAC-Adresse kann der Hacker außerdem Informationen für einen anderen Benutzer abfangen.

2) Daten-Sniffing

"Daten-Sniffing" bezeichnet eine Methode, die von Hackern zum Abrufen von Netzwerkdaten verwendet wird, wenn die Daten sich in unsicheren Netzwerken, wie z. B. dem Internet, befinden. Werkzeuge für diese Aktivitäten, wie z. B. Programme zur Protokollanalyse und Netzwerkdiagnose, sind in vielen Fällen im Betriebssystem integriert und ermöglichen die Anzeige der Daten im Textformat.

3) Man-in-the-Middle-Angriffe

Sobald der Hacker entweder durch Spoofing oder Sniffing genug Informationen gesammelt hat, kann er einen "Man-in-the-Middle-Angriff" starten. Dieser Angriff wirkt sich so aus, dass Daten, die von einem Netzwerk an ein anderes Netzwerk übertragen werden, an ein neues Ziel umgeleitet werden. Obwohl die Daten von dem vorgesehenen Empfänger nicht empfangen werden, wird dem Absender genau dies angezeigt.

Dies sind nur einige der von Hackern verwendeten Methoden, und es werden stets neue Methoden entwickelt. Ohne die Sicherheit Ihres VPNs sind Ihre Daten ständig solchen Angriffen ausgesetzt, wenn sie über das Internet

Abbildung 2-3: VPN-Gateway - VPN-Gateway

übertragen werden. Daten, die über das Internet übertragen werden, durchlaufen oftmals viele verschiedene Server in aller Welt, bevor Sie ihr Ziel erreichen. Für nicht geschützte Daten ist dies ein langer Weg; hier erfüllt jedoch ein VPN seinen Zweck.

Kapitel 3: Beschreibung des ADSL2-Gateways mit 4-Port-Switch

Rückseite

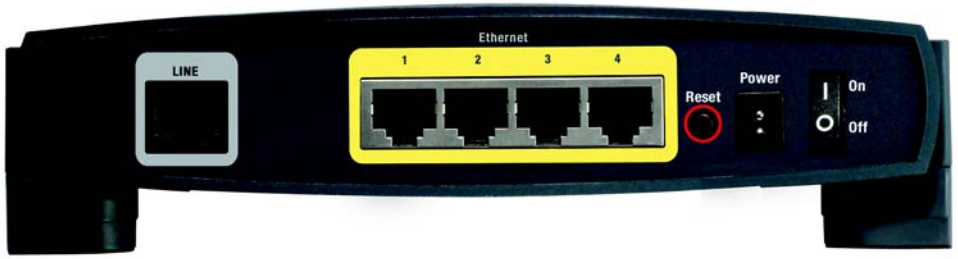

Abbildung 3-1: Rückseite

Die Ports des Gateways für den Anschluss eines Netzwerkkabels befinden sich auf der Rückseite des Geräts. Die Tasten des Gateways befinden sich ebenfalls auf der Rückseite.

LINE (Verbindung) Der **LINE**-Port dient zum Anschließen an die ADSL-Verbindung.

Ethernet (1-4) Die **Ethernet**-Ports dienen zum Anschließen an den Computer und andere Netzwerkgeräte.

Reset-Taste Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie entweder die **Reset**-Taste ungefähr zehn Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) unter **Factory Defaults** (Werkseinstellungen) zurück.

Power (Netzstrom) Der Netzstrom-Port dient zum Anschließen des Netzstromadapters.

On/Off (Ein/Aus) Mit diesem Schalter wird das Gateway ein- und ausgeschaltet.

Mit diesen Produkten, wie mit vielen weiteren Linksys Produkten auch, stehen Ihnen grenzenlose Netzwerkbetriebsoptionen offen. Weitere Informationen dazu, welche Produkte mit dem Gateway verwendet werden können, finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international.

Wichtig: Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen (WEP-Verschlüsselung, Wireless- und LAN-Einstellungen usw.) gelöscht und durch die Werkseinstellungen ersetzt. Wenn Sie diese Einstellungen beibehalten möchten, sollten Sie das Gateway nicht zurücksetzen.

Vorderseite

Die LEDs des Gateways, mit denen Informationen zur Netzwerkaktivität angezeigt werden, befinden sich auf der Vorderseite.

Abbildung 3-2: Vorderseite

Power (Netzstrom) Grün. Die Netzstrom-LED leuchtet auf, wenn das Gateway eingeschaltet wird.

Ethernet (1-4) Grün. Die **LAN**-LED hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den LAN-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt.

DSL Grün. Die **DSL-**LED leuchtet bei jeder erfolgreichen DSL-Verbindung auf. Die LED blinkt, während die ADSL-Verbindung hergestellt wird.

Internet Grün. Die **Internet**-LED leuchtet grün auf, wenn eine Internetverbindung zur Sitzung des Internetdienstanbieters (ISP) hergestellt wurde. Die **Internet**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist.

Kapitel 4: Anschließen des ADSL2-Gateways mit 4-Port-Switch

Übersicht

Die Einrichtung des Gateways umfasst mehr als das bloße Anschließen der Hardware. Sie müssen Ihre vernetzten Computer so konfigurieren, dass sie die vom Gateway zugewiesenen IP-Adressen annehmen (falls zutreffend); darüber hinaus müssen Sie das Gateway mithilfe von Einstellungen konfigurieren, die Sie von Ihrem ISP (*Internet Service Provider*) erhalten.

Sie haben möglicherweise nach der Installation Ihrer Breitbandverbindung die Informationen zur Einrichtung Ihres Modems vom Installationstechniker Ihres ISP erhalten. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und der Einrichtung des Gateways beginnen.

Verbindung mit einem Computer

1. Bevor Sie beginnen, stellen Sie sicher, dass all Ihre Hardwaregeräte, einschließlich des Gateways und der Computer, ausgeschaltet sind.

2. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1 bis 4 beschriftet) auf der Rückseite des Gateways (siehe Abb. 4-1) und das andere Ende am Ethernet-Port des Computers an.

3. Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.

Abbildung 4-1: Ethernet-Verbindung

4. Schließen Sie ein Ende des zweites Netzwerkkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an den NTBA an.

Abbildung 4-2: ADSL-Verbindung

5. Schließen Sie den Netzstromadapter an den Netzstrom-Port des Gateways an (siehe Abb. 4-3), und stecken Sie den Netzstromadapter anschließend in eine Netzsteckdose. Stellen Sie den On-/Off-Schalter auf **On** (Ein).

   - Sobald das Netzgerät richtig angeschlossen und der Schalter auf **On** (Ein) gestellt ist, sollte die Netzstrom-LED auf der Vorderseite grün leuchten. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen ist. Wenn die LED eine Minute oder länger blinkt, finden Sie Informationen zur Fehlerbehebung in "Anhang A: Fehlerbehebung".

6. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

HINWEIS: Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Abbildung 4-3: Netzstromverbindung

Die Installation der Gateway-Hardware ist jetzt abgeschlossen.

Wechseln Sie zu "Kapitel 5: Konfigurieren des Gateways".

HINWEIS: Sie sollten stets die Standardeinstellung der SSID, **linksys**, ändern und die WEP-Verschlüsselung aktivieren.

Kapitel 5: Konfigurieren des Gateways

Übersicht

Folgen Sie zum Konfigurieren des Gateways den in diesem Kapitel aufgeführten Schritten, und verwenden Sie das webbasierte Dienstprogramm des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm mit einem an das Gateway angeschlossenen Computer über Ihren Web-Browser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer nur die folgenden Fenster des Dienstprogramms:

- **Grundlegende Einrichtung**: Geben Sie im Fenster *Grundlegende Einrichtung* die von Ihrem ISP bereitgestellten Einstellungen ein.
- **Verwaltungsfunktionen**: Klicken Sie auf die Registerkarte *Verwaltung* und anschließend auf die Registerkarte **Verwaltungsfunktionen**. Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie das Standardpasswort, um das Gateway zu schützen.

Es gibt sechs Hauptregisterkarten: **Einrichtung**, **Sicherheit**, **Zugriffsbeschränkungen**, **Anwendungen & Spiele**, **Verwaltung** und **Status**. Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

Einrichtung

- **Grundlegende Einrichtung**: Geben Sie in dieses Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (*Dynamic Domain Name System*) des Gateways zu aktivieren.
- **Erweitertes Routing**: Sie können in diesem Fenster die Konfigurationseinstellungen für dynamisches und statisches Routing ändern.

Sicherheit

- **Firewall**: Dieses Fenster enthält Filter und geblockte WAN-Anfragen. Durch die Verwendung von Filtern kann der Internetzugriff bestimmter interner Benutzer und anonyme Internet-Anfragen geblockt werden.
- **VPN**: Verwenden Sie dieses Fenster, um die Option **IPSec Passthrough** und/oder **PPTP Passthrough** zu aktivieren oder deaktivieren, und richten Sie VPN-Tunnel ein.

Haben Sie: TCP/IP auf Ihren Computern aktiviert? Computer tauschen über das Netzwerk mit diesem Protokoll Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.

Hinweis: Für zusätzliche Sicherheit sollten Sie das Passwort über die Registerkarte **Verwaltung** ändern.

Zugriffsbeschränkungen

- **Internetzugriff**: Mithilfe dieses Fensters können Sie bestimmten Benutzern den Zugriff auf Ihr Netzwerk erlauben bzw. deren Zugriff verhindern.

Anwendungen & Spiele

- **Einfaches Port-Forwarding**: Verwenden Sie dieses Fenster, um die gängigsten Dienste und Anwendungen auf Ihrem Netzwerk einzurichten.
- **Weiterleitung an einen Anschlussbereich**: Klicken Sie auf diese Registerkarte, um öffentliche Dienste oder weitere spezielle Internetanwendungen auf Ihrem Netzwerk einzurichten.
- **Port Triggering**: Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internetanwendungen festzulegen.
- **DMZ**: Verwenden Sie dieses Fenster, um für einen Benutzer die Internetverbindung zur Verwendung von speziellen Diensten einzurichten.
- **QoS:** QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

Verwaltung

- **Verwaltungsfunktionen**: In diesem Fenster können Sie Zugriffsrechte für das Gateway sowie SNMP-, UPnP- und WT-82-Einstellungen ändern.
- **Berichtaufzeichnung**: Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnose**: Verwenden Sie dieses Fenster, um einen Ping-Test durchzuführen.
- **Sichern & Wiederherstellen**: Mit der Registerkarte **Sichern & Wiederherstellen** können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.
- **Werkseinstellungen**: Verwenden Sie dieses Fenster, wenn Sie das Gateway of die Werkseinstellungen zurücksetzen möchten.
- **Firmware aktualisieren**: Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.
- **Neustart**: Über diese Registerkarte können Sie für Ihr Gateway einen Warm- oder Kaltstart ausführen.

Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Lokales Netzwerk**: In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **DSL-Verbindung**: In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Um auf das webbasierte Dienstprogramm zuzugreifen, starten Sie Internet Explorer oder Netscape Navigator, und geben Sie im Adressenfeld die Standard-IP-Adresse des Gateways (192.168.1.1) ein. Drücken Sie anschließend die Eingabetaste.

Das in Abbildung 5-1 angezeigte Fenster zur Eingabe des Passworts wird angezeigt. (Unter anderen Betriebssystemen als Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (als Standardbenutzername) in das Feld **Benutzername** sowie **admin** (als Standardkennwort) in das Feld **Kennwort** ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

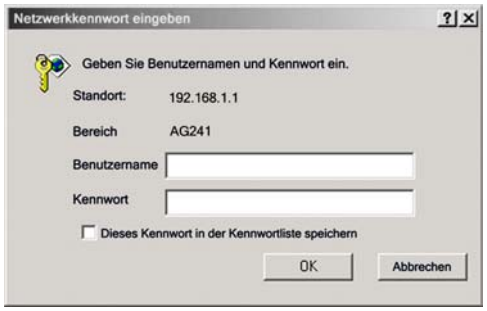

Abbildung 5-1: Fenster für die Passworteingabe

Registerkarte Einrichtung

Registerkarte Grundlegende Einrichtung

Im ersten dargestellten Fenster wird die Registerkarte **Grundlegende Einrichtung** angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Einstellungen speichern**, um Ihre Änderungen zu übernehmen, oder auf die Schaltfläche **Änderungen verwerfen**, um Ihre Änderungen zu verwerfen.

Interneteinrichtung

- **PVC-Verbindung**: Wählen Sie im Dropdown-Menü **PVC-Verbindung** eine Nummer aus. Aktivieren Sie anschließend **Jetzt aktivieren**, um die Verbindung zu aktivieren.
- **VC-Einstellungen**: **Virtuelle Verbindung, VPI und VCI**: Für diese Felder gibt es zwei Optionen: **VPI** (*Virtual Path Identifier*; Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.
  - **Multiplexing**: Wählen Sie entsprechend dem verwendeten ISP für diese Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
  - **QoS-Typ**: Wählen Sie im Dropdown-Menü aus den folgenden Optionen aus: **CBR** (*Continuous Bit Rate;* Konstante Bitrate), um eine feste Bandbreite für Sprach- oder Datenverkehr festzulegen, **UBR** (*Unspecific Bit Rate*; Unbestimmte Bitrate) für Anwendungen, die zeitunabhängig sind (z. B. E-Mail), oder **VBR** (*Variable Bite Rate*; Variable Bitrate) für diskontinuierlichen Verkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam genutzt werden.

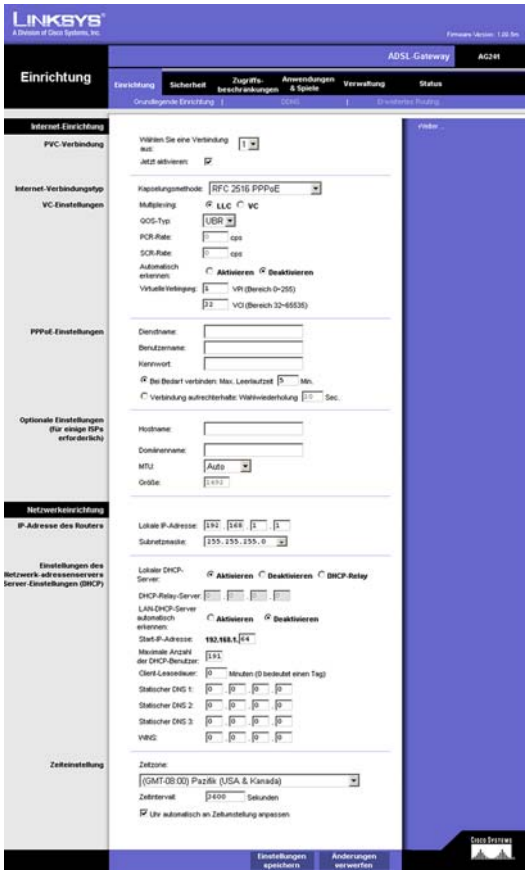

Abbildung 5-2: Registerkarte Grundlegende Einrichtung

- **PCR-Rate**: (*Peak Cell Rate*; Spitzenzellrate): Wenn Sie die Rate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate, anhand der Sie die maximale Rate, mit der der Absender Zellen senden kann, feststellen können. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **SCR-Rate**: (*Sustain Cell Rate*; Dauerzellrate): Bestimmt den Mittelwert der Zellrate, die übertragen werden kann. Die Dauerzellrate ist gewöhnlich niedriger als die Spitzenzellrate. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **Automatisch erkennen**: Wählen Sie **Aktivieren** aus, um die Einstellungen automatisch anzuzeigen, bzw. **Deaktivieren**, um die Werte manuell einzugeben.

- **Virtueller Verbindung**: Geben Sie die Bereiche für VPI und VCi in das jeweilige Feld ein.

- **Internet-Verbindungstyp**: Das Gateway unterstützt fünf Kapselungstypen: **RFC 1483-Überbrückung**, **RFC 1483-Weiterleitung**, **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Nur Überbrückungsmodus**. Das jeweilige Fenster *Grundlegende Einrichtung* und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

RFC 1483-Überbrückung

Dynamische IP-Adresse

IP-Einstellungen: Wählen Sie **IP-Adresse automatisch beziehen**, wenn Sie laut Angaben Ihres ISP die Verbindung über eine dynamische IP-Adresse herstellen.

Statische IP-Adresse

Wenn Sie für die Internetverbindung eine permanente (statische) IP-Adresse verwenden, wählen Sie **Folgende IP-Adresse verwenden** aus.

- **Internet-IP-Adresse**: Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnetzmaske**: Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primärer DNS** (erforderliche Einstellung) und **Sekundärer DNS** (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

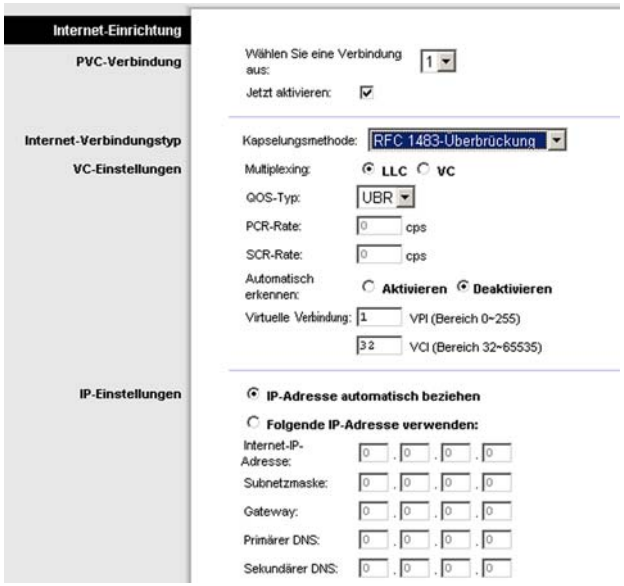

Abbildung 5-3: Dynamische IP-Adresse

Abbildung 5-4: Statische IP-Adresse

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

IPoA

Wenn Sie Classical IP über ATM verwenden müssen, wählen Sie **IPoA**.

- **IP-Adresse**: Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnetzmaske**: Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Standard-Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primärer DNS** (erforderliche Einstellung) und **Sekundärer DNS** (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

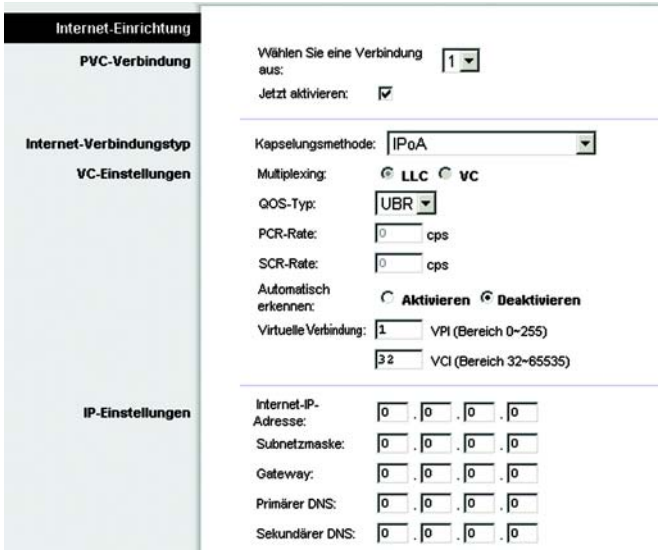

Abbildung 5-5: IPoA

RFC 2516 PPPoE

Einige ISPs auf DSL-Basis verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **Dienstname**: Geben Sie den Namen Ihres PPPoE-Diensts in das Feld ein.
- **Benutzername/Passwort**: Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Bei Bedarf verbinden: Max. Leerlaufzeit**: Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Bei Bedarf verbinden** Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Bei Bedarf verbinden** zu aktivieren. Geben Sie im Feld **Max. Leerlaufzeit** die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Verbindung aufrechterhalten: Wahlwiederholung**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche neben **Verbindung aufrechterhalten**. Im Feld **Wahlwiederholung** legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

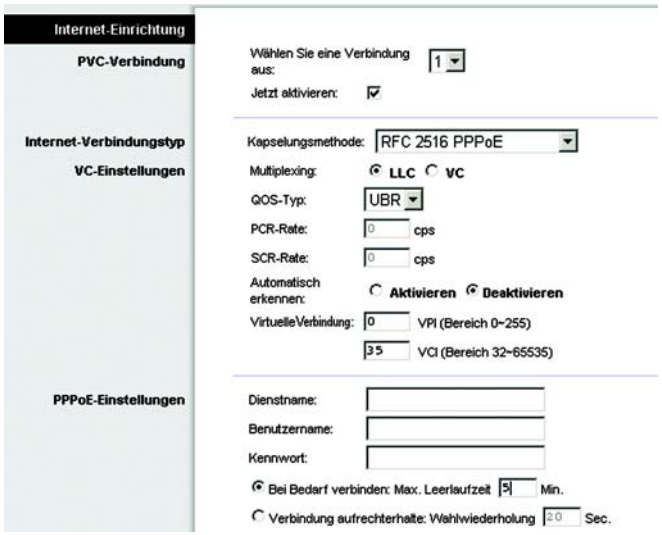

Abbildung 5-6: RFC 2516 PPPoE

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

RFC 2364 PPPoA

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Leitung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **Benutzername/Passwort**: Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Bei Bedarf verbinden: Max. Leerlaufzeit**: Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Bei Bedarf verbinden** Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Bei Bedarf verbinden** zu aktivieren. Geben Sie im Feld **Max. Leerlaufzeit** die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Verbindung aufrechterhalten: Wahlwiederholung**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche neben **Verbindung aufrechterhalten**. Im Feld **Wahlwiederholung** legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

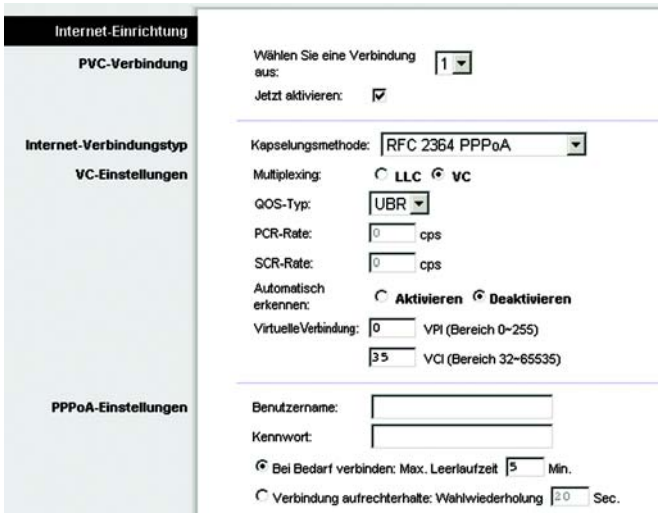

Abbildung 5-7: RFC 2364 PPPoA

Nur Überbrückungsmodus

Wenn Sie Ihr Gateway als Bridge verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Nur Überbrückungsmodus** aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen.**

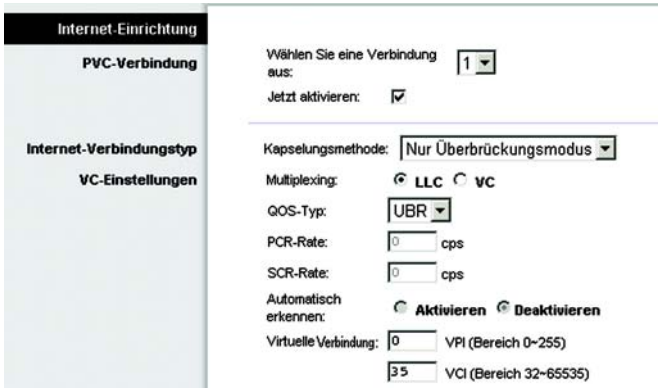

Abbildung 5-8: Nur Überbrückungsmodus

Optionale Einstellungen (für einige ISPs erforderlich)

- **Hostname/Domänenname**: In diese Felder können Sie einen Hostnamen bzw. Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Erfragen Sie bei Ihrem ISP, ob Ihr Breitband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU:** Mit der MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manuell** aus, und geben Sie den gewünschten Wert in das Feld *Size* (Größe) ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch festgelegt.

Netzwerkeinrichtung

- **IP-Adresse des Routers**: Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
  - **Lokale IP-Adresse**: Der Standardwert ist 192.168.1.1.
  - **Subnetzmaske**: Der Standardwert ist 255.255.255.0.
- **Einstellungen des Netzwerkadressenservers (DHCP)**: Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen.
  - **DHCP-Relay-Server**: Wenn Sie den lokalen DHCP-Server oder das DHCP-Relay für den lokalen DHCP-Server aktivieren, geben Sie die IP-Adresse für den DHCP-Server in die Felder ein.
  - **LAN-DHCP-Server automatisch erkennen**.
  - **Start-IP-Adresse**: Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.1.2 betragen, da die Standard-IP-Adresse für das Gateway 192.168.1.1 ist.
  - **Maximale Anzahl der DHCP-Benutzer**: Geben Sie die maximale Anzahl von Benutzern bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab.
  - **Client-Leasedauer**: Bei der Client-Leasedauer handelt es sich um den Zeitraum, über den ein Netzwerkbenutzer mithilfe seiner aktuellen dynamischen IP-Adresse eine Verbindung mit dem Gateway herstellen darf. Geben Sie den Zeitraum in Minuten ein, über den dem Benutzer diese dynamische IP-Adresse gewährt wird.
  - **Statisches DNS 1-3**: Mit dem DNS (*Domain Name System*) übersetzt das Internet Domänen- oder Website-Namen in Internetadressen oder URLs. Sie erhalten von Ihrem ISP mindestens eine IP-Adresse

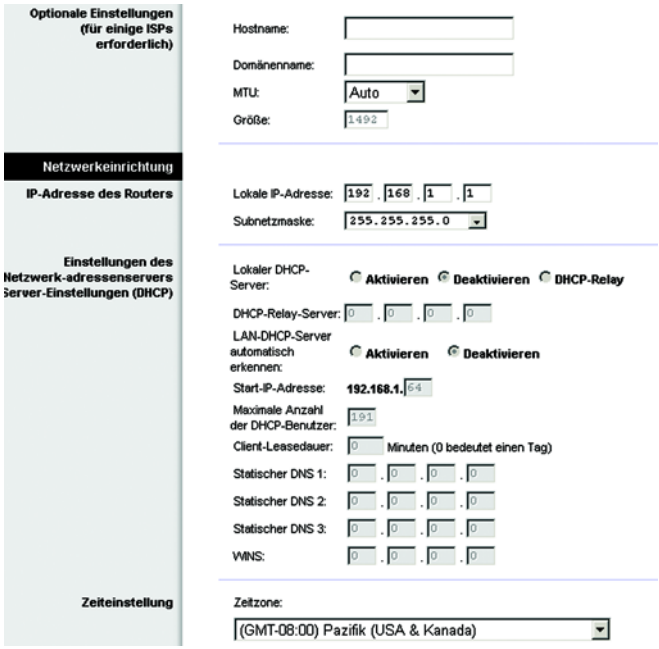

Abbildung 5-9: Optionale Einstellungen

für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für den DNS-Server eingeben. Der Router verwendet diese für einen schnelleren Zugriff auf laufende DNS-Server.

- **WINS**: Mithilfe von WINS (*Windows Internet Naming Service*) werden NetBIOS-Namen in IP-Adressen umgewandelt. Wenn Sie einen WINS-Server verwenden, geben Sie hier die IP-Adresse des Servers ein. Andernfalls lassen Sie dieses Feld leer.
- **Zeiteinstellung**: Mit dieser Option legen Sie die Zeitzone für Ihr Gateway fest. Wählen Sie Ihre Zeitzone aus dem Dropdown-Menü aus. Aktivieren Sie gegebenenfalls die Option **Uhr automatisch an Zeitumstellung anpassen**.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Registerkarte **DDNS**

Das Gateway verfügt über die Funktion **DDNS** (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich bei den DDNS-Dienstanbietern unter www.dyndns.org anmelden.

DDNS

DDNS-Dienst: Wenn der von Ihnen verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **DynDNS.org** aus (siehe Abbildung 5-10). Um den DDNS-Dienst zu deaktivieren, wählen Sie die Option **Deaktiviert** aus.

Abbildung 5-10: DynDNS.org

DynDNS.org

- **Benutzername**, **Passwort** und **Hostname**: Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet-IP-Adresse**: Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

TZO.com

- **E-Mail-Adresse**, **Passwort** und **Domänenname**: Geben Sie die E-Mail-Adresse, das TZO-Passwort und den Domänenname des Dienstes ein, den Sie mit TZO eingerichtet haben.
- **Internet-IP-Adresse**: Hier ist die aktuelle IP-Adresse des Routers aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

Abbildung 5-11: TZO.com

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Registerkarte Erweitertes Routing

Über das Fenster *Erweitertes Routing* können Sie die Einstellungen für dynamisches und statisches Routing konfigurieren

Erweitertes Routing

- **Betriebsmodus**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann dank dieser Funktion IP-Adressen Ihres lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktiviert**.
- **Dynamisches Routing**: Mit der Option **Dynamisches Routing** kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Das Gateway legt unter Verwendung des RIP-Protokolls die Route der Netzwerkpakete auf der Grundlage der geringsten Anzahl an Sprüngen zwischen Quelle und Ziel fest. Das RIP-Protokoll sendet in regelmäßigen Abständen Routing-Informationen an andere Gateways im Netzwerk. Klicken Sie zum Aktivieren des RIP-Protokolls auf **Aktiviert**. Klicken Sie zum Deaktivieren des RIP-Protokolls auf **Deaktiviert**.
  - **RIP-Version übertragen**: Wählen Sie für die Übertragung von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1**, **RIP1-kompatibel** oder **RIP2**.
  - **RIP-Version empfangen**: Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**.
- **Statisches Routing**: Wenn das Gateway an mehr als einem Netzwerk angeschlossen ist, muss u. U. zwischen den Gateways eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:
  - **Set-Nummer auswählen**: Wählen Sie die Anzahl der statischen Routen aus dem Dropdown-Menü aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routeneinträge. Wenn Sie nach Auswahl eines Eintrags eine Route löschen möchten, klicken Sie auf die Schaltfläche **Diesen Eintrag löschen**.
  - **Ziel-IP-Adresse**: Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert **0** festgelegt ist.
  - **Subnetzmaske**: Mithilfe der Subnetzmaske (auch Netzwerkmaske genannt) wird festgelegt, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.
  - **Gateway**: Bei dieser IP-Adresse handelt es sich um die IP-Adresse des Gateway-Geräts, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.
  - **Anzahl der Gateways**: Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie diese Zahl in das Feld ein.

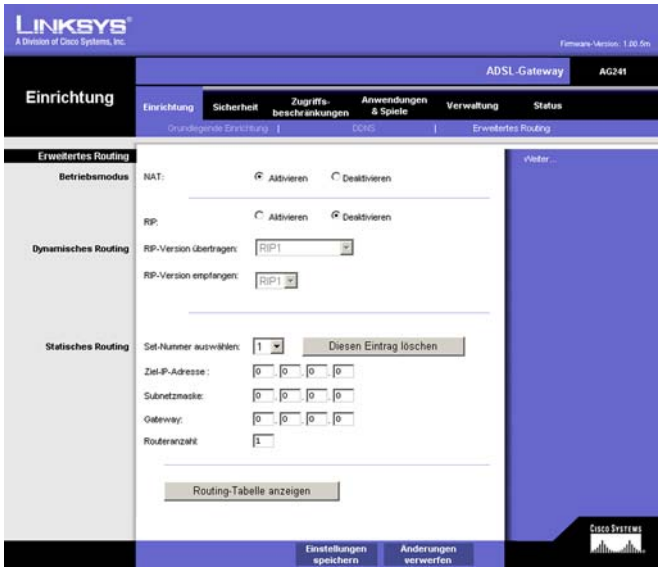

Abbildung 5-12: Erweitertes Routing

- **Routing-Tabelle anzeigen**: Klicken Sie auf die Schaltfläche **Routing-Tabelle anzeigen**, um ein Fenster mit den durch das LAN übertragenen Daten zu öffnen. Für jede Route wird die Ziel-IP-Adresse, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Schließen**, um zum vorherigen Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-13: Erweiterte Wireless-Einstellungen

Registerkarte Sicherheit

Firewall

Wenn Sie auf die Registerkarte **Sicherheit** klicken, wird das Fenster *Firewall* angezeigt. Dieses Fenster enthält Filter und die Option zum Blockieren von WAN-Anfragen. Durch die Verwendung von Filtern können spezielle Internetdatentypen und anonyme Internet-Anfragen geblockt werden. Klicken Sie zum Hinzufügen des Firewall-Schutzes auf **Aktivieren**. Klicken Sie zum Deaktivieren des Firewall-Schutzes auf **Deaktivieren**.

Abbildung 5-14: Firewall

Zusätzliche Filter

- **Filterproxy**: Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie den Filterproxy ablehnen, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Um die Proxy-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **Cookies filtern**: Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Um die Cookie-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **Java-Applets filtern**: Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Um die Java Applet-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **ActiveX filtern**: Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Um die ActiveX-Filterung zu aktivieren, klicken Sie auf die Option **Aktivieren**.

Blockieren von WAN-Anfragen

- **Anonyme Internet-Anfragen blockieren**: Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit Ihres Netzwerks erhöhen, indem Ihre Netzwerk-Ports nicht angezeigt werden und Ihr Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Anonyme Internet-Anfragen blockieren**, um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

VPN

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Über dieses Fenster können Sie Ihre VPN-Einstellungen konfigurieren und damit die Sicherheit Ihres Netzwerks erhöhen.

VPN-Passthrough

- **IPSec-Passthrough**: IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zur Implementierung eines sicheren Paketaustauschs auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Aktivieren**. Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.
- **PPTP-Passthrough**: PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf einem Windows NT 4.0- oder Windows 2000-Server. Um PPTP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Aktivieren**. Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.
- **L2TP-Passthrough**: Bei L2TP-Passthrough (*Layering 2 Tunneling Protocol Passthrough*) handelt es sich um eine Erweiterung von PPTP (*Point-to-Point Tunneling Protocol*), mit der der Betrieb eines VPN über das Internet ermöglicht wird. Um P2TP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Aktivieren**. Um P2TP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Deaktivieren**.

IPSec VPN-Tunnel

Das VPN-Gateway erstellt einen Tunnel bzw. Kanal zwischen zwei Endpunkten, sodass die Datenübertragungen zwischen diesen beiden Endpunkten sicher sind.

- Um den Tunnel festzulegen, wählen Sie den Tunnel, den Sie erstellen möchten, aus dem Dropdown-Menü **Tunneleintrag auswählen** aus. Es können bis zu 5 gleichzeitig aktive Tunnel erstellt werden. Klicken Sie anschließend auf **Enabled** (Aktiviert), um den IPSec VPN-Tunnel zu aktivieren. Wenn der Tunnel aktiviert ist, geben Sie den Namen des Tunnels in das Feld **Tunnelname** ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird. Um einen Tunneleintrag zu löschen, wählen Sie den entsprechenden Tunnel aus, und klicken Sie auf **Löschen**. Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung der Einstellungen anzuzeigen.
- **Lokale sichere Gruppe** und **Entfernte sichere Gruppe**: **Lokale sichere Gruppe** umfasst die Computer in Ihrem LAN, die auf den Tunnel zugreifen können. **Entfernte sichere Gruppe** umfasst die Computer am entfernten Ende des Tunnels, die auf den Tunnel zugreifen können. Diese Computer können durch ein Subnetz, eine spezielle IP-Adresse oder einen Bereich festgelegt werden.
- **Lokales Sicherheits-Gateway**.

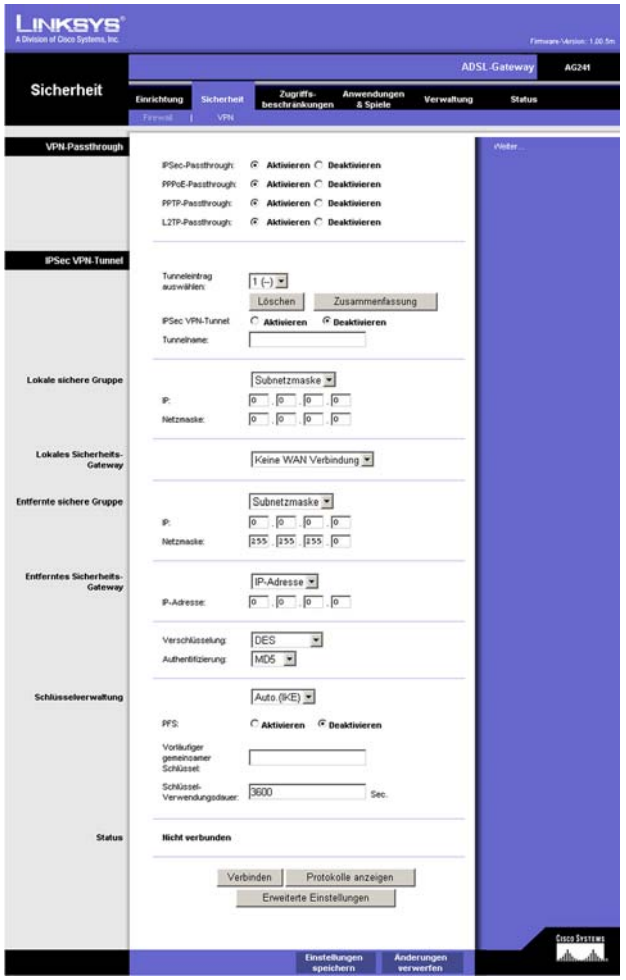

Abbildung 5-15: VPN

Abbildung 5-16: Zusammenfassung der VPN-Einstellungen

- **Entferntes Sicherheits-Gateway**: Bei dem **Entferntes Sicherheits-Gateway** handelt es sich um das VPN-Gerät (beispielsweise ein zweites VPN-Gateway) am entfernten Ende des VPN-Tunnels. Geben Sie die IP-Adresse oder Domäne des VPN-Geräts am anderen Ende des Tunnels ein. Bei dem entfernten VPN-Gerät kann es sich um ein anderes VPN-Gateway, einen VPN-Server oder einen Computer mit VPN-Client-Software handeln, der IPSec unterstützt. Bei der IP-Adresse kann es sich je nach den Einstellungen des entfernten VPN-Geräts um eine statische (permanente) Adresse oder um eine dynamische (sich ändernde) Adresse handeln. Vergewissern Sie sich, dass Sie die korrekte IP-Adresse eingegeben haben; anderenfalls kann keine Verbindung hergestellt werden. Denken Sie daran, dass dies NICHT die IP-Adresse des lokalen VPN-Gateways ist, sondern die IP-Adresse des entfernten VPN-Gateways bzw. -Geräts, mit dem kommuniziert werden soll. Wenn Sie eine IP-Adresse eingeben, kann nur mit der angegebenen IP-Adresse auf den Tunnel zugegriffen werden. Wenn Sie **Alle** auswählen, kann mit jeder IP-Adresse auf den Tunnel zugegriffen werden.
- **Verschlüsselung**: Mit **Verschlüsselung** machen Sie die Verbindung noch sicherer. Es stehen zwei Verschlüsselungstypen zur Verfügung: **DES** und **3DES** (empfohlen wird **3DES**, da dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Deaktivieren** auswählen. In Abbildung 5-22 wurde DES ausgewählt (Standardeinstellung).
- **Authentifizierung**: Die Authentifizierung stellt eine weitere Sicherheitsstufe dar. Es stehen zwei Authentifizierungstypen zur Verfügung: **MD5** und **SHA** (empfohlen wird **SHA**, da dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit **Deaktivieren** an beiden Enden des Tunnels deaktiviert werden. Im Fenster *Manual Key Management* (Manuelle Schlüsselverwaltung) wurde der Standardwert **MD5** ausgewählt.
- **Schlüsselverwaltung**: Wählen Sie aus dem Dropdown-Menü **Auto (IKE)** oder **Manuell** aus. Die beiden Methoden werden im Folgenden beschrieben.

  Auto (IKE)
  Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Pre-shared Key** (Vorläufiger gemeinsamer Schlüssel) ein. Wenn dieses Verfahren verwendet wird, MUSS das Wort an beiden Enden des Tunnels eingegeben werden. Auf der Grundlage dieses Worts wird ein Schlüssel erstellt, mit dem die über den Tunnel versendeten Daten verschlüsselt und entschlüsselt werden. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden. Im Feld **Schlüssel-Verwendungsdauer** können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, sodass der Schlüssel unbegrenzt lange zur Verfügung steht. Markieren Sie das Kontrollkästchen neben PFS (Perfect Forward Secrecy) [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind.

Manuell
Wählen Sie **Manuell** und anschließend den Verschlüsselungsalgorithmus aus dem Dropdown-Menü aus. Geben Sie den Codierschlüssel in das dafür vorgesehene Feld ein (wenn Sie **DES** als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 16 hexadezimale Zeichen ein, wenn Sie **3DES** ausgewählt haben, geben Sie 48 hexadezimale Zeichen ein). Wählen Sie den Authentifizierungsalgorithmus aus dem Dropdown-Menü aus. Geben Sie den Authentifizierungsschlüssel in das dafür vorgesehene Feld ein (wenn Sie **MD5** als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 32 hexadezimale Zeichen ein, wenn Sie **SHA1** ausgewählt haben, geben Sie 40 hexadezimale Zeichen ein). Geben Sie in die entsprechenden Felder **Inbound SPI** (Eingangs-SPI) und **Outbound SPI** (Ausgangs-SPI) ein.

- **Status**: In dieser Zeile wird der Status der Verbindung angezeigt.

Klicken Sie auf die Schaltfläche **Verbinden**, um Ihren VPN-Tunnel zu verbinden. Klicken Sie auf **Protokolle anzeigen**, um die System-, UPnP-, VPN-, Firewall-, Zugriffs- oder alle Protokolle anzuzeigen. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**, um das Fenster *Advanced IPSec VPN Tunnel Setup* (Erweiterte IPSec VPN-Tunnel-Einrichtung) anzuzeigen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

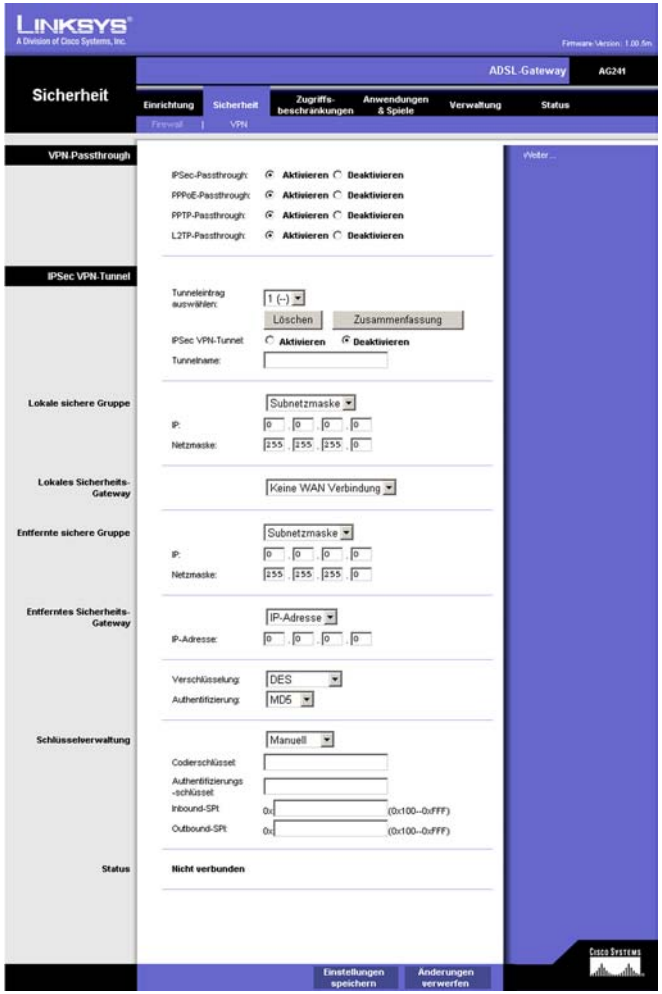

Abbildung 5-17: Manuelle Schlüsselverwaltung

Abbildung 5-18: Systemprotokoll

Erweiterte IPSec VPN-Tunnel-Einrichtung

Sie können über das Fenster *Erweiterte IPSec VPN-Tunnel-Einrichtung* die Einstellungen für bestimmte VPN-Tunnel anpassen.

Phase 1

- **Phase 1** wird zur Erstellung einer Sicherheitsverknüpfung (SA), auch "IKE SA" (*Internet Key Exchange, Security Association*) genannt, verwendet. Nach Abschluss von Phase 1 wird in Phase 2 mindestens eine "IPSec SA" erstellt und für IPSec-Sitzungen verwendet.
- **Betriebsmodus**: Es gibt zwei Modi: **Hauptmodus** und **Aggressiver Modus**, die die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen austauschen. Der Hauptmodus wird häufiger verwendet, wobei einige Anwender jedoch den schnelleren aggressiven Modus vorziehen. Der Hauptmodus kann zur durchschnittlichen Verwendung eingesetzt werden und enthält mehr Authentifizierungserfordernisse als der aggressive Modus. Die Verwendung des Hauptmodus wird empfohlen, da dieser Modus sicherer ist. Bei beiden Modi werden vom VPN-Gateway Anfragen sowohl im Haupt- als auch im aggressiven Modus vom standortfernen VPN-Gerät akzeptiert.
- **Verschlüsselung**: Wählen Sie die Länge des Schlüssels aus, der zum Verschlüsseln/Entschlüsseln von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: **DES** und **3DES**. Die Verwendung von **3DES** wird empfohlen, da diese Verschlüsselungsart sicherer ist.
- **Authentifizierung**: Wählen Sie die Methode aus, die zur Authentifizierung von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: **MD5** und **SHA**. Die Verwendung von **SHA** wird empfohlen, da diese sicherer ist.
- **Gruppe**: Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.
- **Schlüssel-Verwendungsdauer**: Im Feld **Schlüssel-Verwendungsdauer** können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Phase 2

- **Verschlüsselung**: Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.
- **Authentifizierung**: Die in Phase 1 ausgewählte Authentifizierungsmethode wird angezeigt.
- **PFS** (PFS, *Perfect Forward Secrecy*): In dieser Zeile wird der PFS-Status angezeigt.
- **Gruppe**: Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

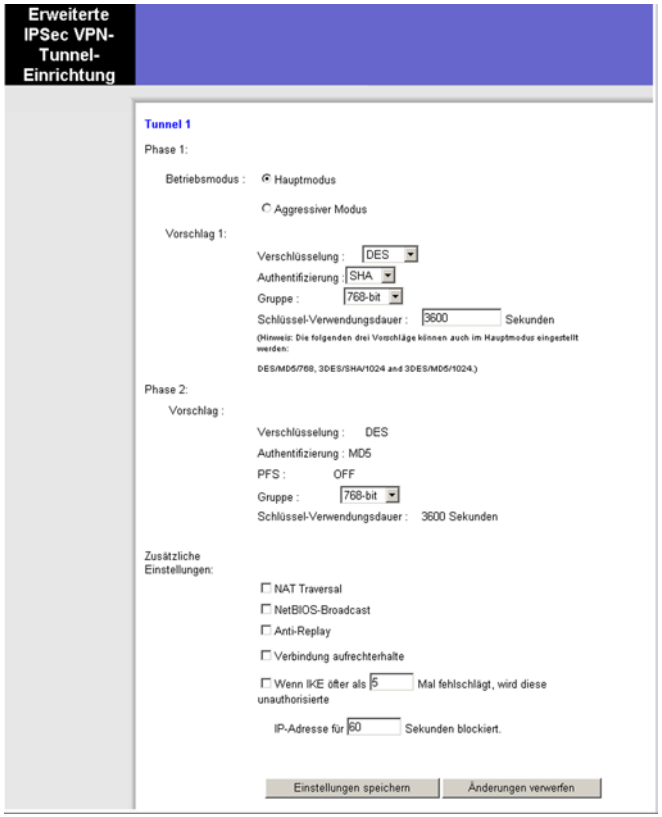

Abbildung 5-19: Erweiterte IPSec VPN-Tunnel-Einrichtung

- **Schlüssel-Verwendungsdauer**: Im Feld **Schlüssel-Verwendungsdauer** können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Zusätzliche Einstellung

- **NetBIOS-Broadcast**: Aktivieren Sie das Kontrollkästchen neben **NetBIOS-Broadcast**, um den NetBIOS-Datenverkehr durch den VPN-Tunnel zu leiten.
- **Anti-Replay**: Aktivieren Sie das Kontrollkästchen neben **Anti-Replay**, um den Anti-Replay-Schutz zu aktivieren. Mithilfe dieser Funktion werden die Sequenznummern der eingehenden Datenpakete aufgezeichnet, wodurch die Sicherheit auf IP-Paketebene gewährleistet wird.
- **Verbindung aufrechterhalten**: Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her.
- Aktivieren Sie dieses Kontrollkästchen, um unberechtigte IP-Adressen zu blockieren. Füllen Sie dieses Feld aus, um die Anzahl der fehlgeschlagenen IKE festzulegen, bevor die unberechtigte IP-Adresse blockiert wird. Geben Sie den Zeitraum in Sekunden in dieses Feld ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**. Klicken Sie auf die Schaltfläche **Nehr Information**, um weitere Informationen zu dieser Registerkarte zu erhalten.

Registerkarte Zugriffsbeschränkungen

Internetzugriff

Mit der Registerkarte **Zugriffsbeschränkungen** können Sie bestimmte Arten der Internetverwendung blockieren bzw. zulassen. Sie können für bestimmte Computer Sicherheitsrichtlinien für den Internetzugriff und Filter mithilfe von Netzwerk-Anschlussnummern einrichten.

- **Richtlinien für Internetzugriff**: Mehrfache Filter können als Sicherheitsrichtlinien für den Internetzugriff gespeichert werden. Wählen zur Bearbeitung einer Richtlinie die entsprechende Nummer aus dem Dropdown-Menü aus. Die Anzeige der Registerkarte ändert sich, um die Änderungen an den Einstellungen an dieser Richtlinie anzuzeigen. Klicken Sie zum Löschen dieser Richtlinie auf die Schaltfläche **Löschen**. Klicken Sie zur Anzeige einer Zusammenfassung aller Richtiglinien auf die Schaltfläche **Zusammenfassung**.

  Die Zusammenfassung wird in einem Fenster mit dem entsprechenden Namen und den entsprechenden Einstellungen angezeigt. Um zur Registerkarte **Filter** zurückzukehren, klicken Sie auf die Schaltfläche **Schließen**.
- **Richtliniennamen eingeben**: Richtlinien werden auf Grundlage der hier aufgeführten Felder erstellt.

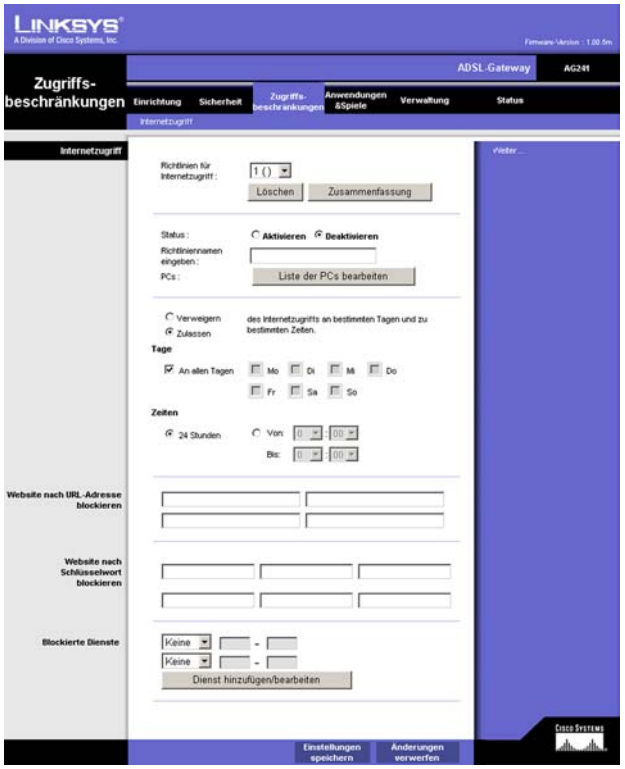

Abbildung 5-20: Internetzugriff

Abbildung 5-21: Internet-Richtlinien - Zusammenfassung

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Geben Sie im Feld **Richtlinienname** einen Namen für die Richtlinie ein. Wählen Sie **Internetzugriff** als Richtlinientyp aus.
2. Klicken Sie auf die Schaltfläche **PC-Liste bearbeiten**. Das Fenster *PC-Liste* wird geöffnet. In diesem Fenster können Sie die IP-Adresse bzw. MAC-Adresse der Computer angeben, auf die die Richtlinie angewendet werden soll. Sie können auch über die IP-Adresse Computerbereiche eingeben. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um Ihre Einstellungen zu speichern, oder klicken Sie auf die Schaltfläche **Änderungen verwerfen**, um Ihre Änderungen zu verwerfen und zur Registerkarte **Filter** zurückzukehren.
3. Klicken Sie auf die entsprechende Option (**Verweigern** oder **Zulassen**), um den Internetzugriff für die PCs, die im Fenster *PC-Liste* aufgeführt sind, zu blockieren oder zuzulassen.
4. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet zugegriffen werden kann, wie z. B. FTP oder Telnet, indem Sie diese Dienste in den Dropdown-Menüs neben **Blockierte Dienste** auswählen. Wenn ein Dienst nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Dienst hinzufügen/bearbeiten**, um das Fenster *Anschlussdienste* zu öffnen und der Liste einen Dienst hinzuzufügen. Sie müssen einen Dienstnamen und das von diesem Dienst verwendete Protokoll sowie den Anschlussbereich eingeben.
5. Durch Auswahl der entsprechenden Zeit- und Datumseinstellung legen Sie den Zeitpunkt fest, zu dem der Internetzugriff gefiltert wird.
6. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um die Richtlinie zu aktivieren.

   Der Internetzugriff kann auch über die URL-Adresse gefiltert werden, die Sie für den Zugriff auf Internetadressen eingeben. Geben Sie hierfür die Adresse in eines der Felder für 'Website nach URL-Adresse blockieren' ein. Wenn Ihnen die URL-Adresse nicht bekannt ist, können Sie das Filtern mithilfe bestimmter Stichwörter vornehmen. Geben Sie hierfür ein Stichwort in eines der Felder für das Blockieren von Websites nach Schlüsselwort ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

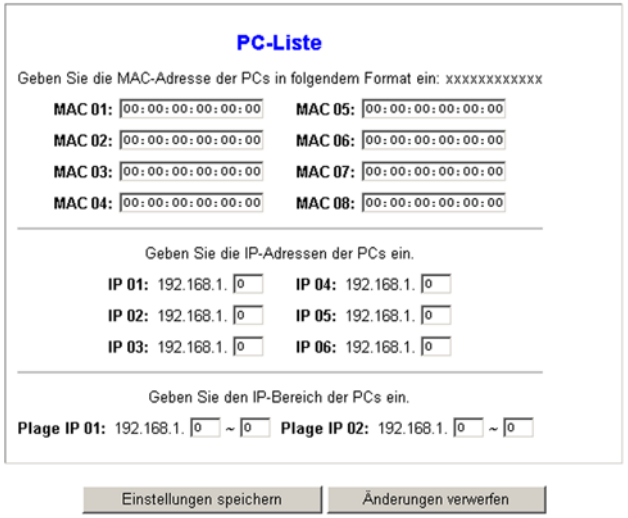

Abbildung 5-22: PC-Liste

Abbildung 5-23: Anschlussdienste

Registerkarte Anwendungen und Spiele

Einfaches Port-Forwarding

Das Fenster *Einfaches Port-Forwarding* bietet Optionen zur Anpassung der Anschlussdienste der gängigsten Anwendungen.

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

Wählen Sie in diesem Feld eine Anwendung aus, oder geben Sie eine Anwendung ein. Geben Sie in diese Felder anschließend die Anschlussnummern der externen und internen Anschlüsse an. Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP** oder **UDP**. Geben Sie in das Feld die IP-Adresse ein. Klicken Sie auf **Aktivieren**, um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-24: Einfaches Port-Forwarding

Weiterleitung an einen Anschlussbereich

Im Fenster *Port-Forwarding* können Sie öffentliche Dienste auf Ihrem Netzwerk, wie z. B. Web-, FTP-, E-Mail-Server oder spezielle Internetanwendungen, festlegen. (Unter speziellen Internetanwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internetspiele ausführen. Bei einigen Internetanwendungen ist keine Weiterleitung erforderlich.)

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Anwendung**: Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Von** und **Bis**: Geben Sie die Anfangs- und Endnummern der Ports ein, die weitergeleitet werden sollen.
- **TCP** und **UDP**: Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP**, **UDP** oder **Beide**.
- **IP-Adresse**: Geben Sie die IP-Adresse ein, und klicken Sie auf **Aktivieren**.

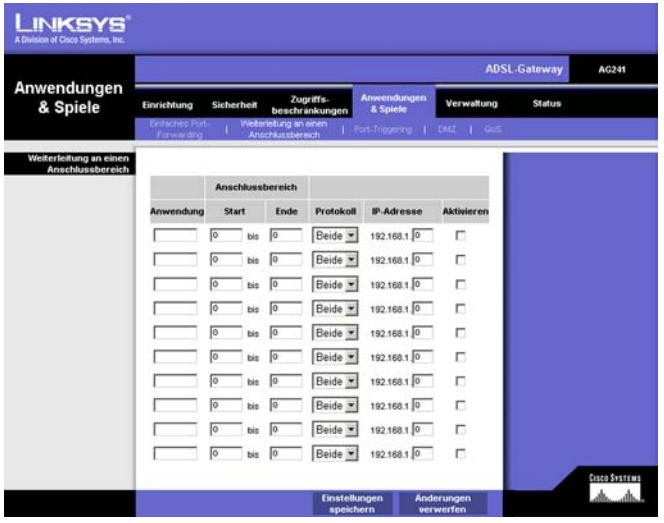

Abbildung 5-25: Weiterleitung an einen Anschlussbereich

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Port-Triggering

Port-Triggering wird bei speziellen Anwendungen verwendet, über die ein Anschluss auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Anschlussnummern. Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln zum richtigen Computer weitergeleitet.

- **Anwendung**: Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start-Port** und **End-Port**: Geben Sie Anfang und Ende der Bereichsnummern für Port-Triggering sowie die Bereichsnummern für Port-Forwarding der Anschlüsse ein, die Sie weiterleiten möchten.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

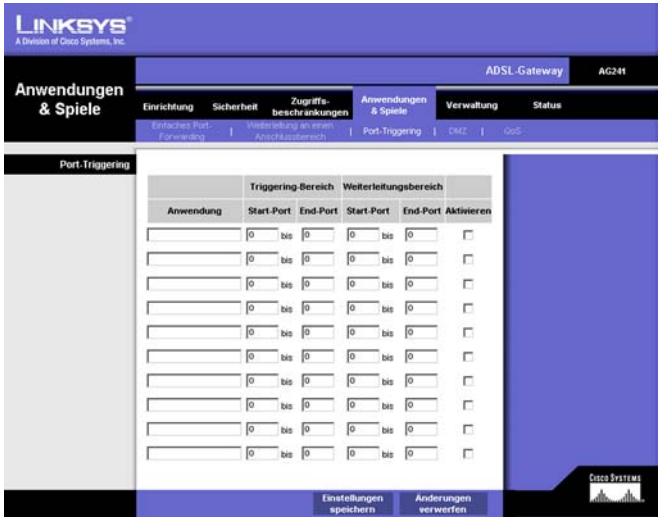

Abbildung 5-26: Port-Triggering

DMZ

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen Netzwerkbenutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste, wie Internetspiele oder Videokonferenzen, nutzen kann. Mit DMZ-Hosting werden alle Anschlüsse gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Weiterleitung an einen Anschlussbereich**, bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

- **DMZ-Hosting**: Mit der DMZ-Funktion (*Demilitarized Zone*; Entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internetspiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Aktivieren**, um diese Funktion zu verwenden. Klicken Sie auf **Deaktivieren**, um die DMZ-Funktion zu deaktivieren.
- **DMZ Host IP Address** (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln einer IP-Adresse finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-27: DMZ

QOS

QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

Anwendungsbasierte QoS

Über **Anwendungsbasierte QoS** werden Informationen beim Übertragen und Empfangen verwaltet. Je nachdem, welche Einstellungen im Fenster *QoS* festgelegt sind, weist diese Funktion Informationen eine hohe oder niedrige Priorität für die fünf voreingestellten Anwendungen und drei zusätzliche Anwendungen zu, die Sie bestimmen.

Aktivieren/Deaktivieren: Wählen Sie zur Verwendung der anwendungsbasierten QoS die Option **Aktivieren**. Behalten Sie andernfalls die Standardeinstellung **Deaktivieren** bei.

Hohe/mittlere/niedrige Priorität: Wählen Sie für jede der Anwendungen **Hohe Priorität** (Datenverkehr in dieser Warteschlange belegt 60 % der gesamten Bandbreite), **Mittlere Priorität** (Datenverkehr in dieser Warteschlange belegt 18 % der gesamten Bandbreite) oder **Niedrige Priorität** (Datenverkehr in dieser Warteschlange belegt 1 % der gesamten Bandbreite).

FTP (*File Transfer Protocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk (Internet, UNIX usw.). Nachdem HTML-Seiten für eine Website auf einem lokalen System gestaltet wurden, werden sie üblicherweise über FTP auf den Webserver geladen.

HTTP (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird. Seine Hauptfunktion besteht darin, eine Verbindung mit einem Webserver herzustellen und HTML-Seiten an den Webbrowser des Clients zu übertragen.

Telnet: Ein Protokoll zur Terminal-Emulation, das häufig in Internet- und TCP/IP-basierten Netzwerken verwendet wird. Dadurch wird einem Benutzer an einem Terminal oder Computer ermöglicht, sich bei einem entfernten Gerät anzumelden und ein Programm auszuführen.

SMTP (*Simple Mail Transfer Protocol*): **Das standardmäßige E-Mail-Protokoll im Internet.** Ein TCP/IP-Protokoll, mit dem das Meldungsformat sowie der MTA (*Message Transfer Agent*; Meldungsübertragungsagent) festgelegt werden, der die Mail speichert und weiterleitet.

POP3 (*Post Office Protocol 3*): Ein im Internet verbreitet eingesetzter Standard-Mailserver. Er bietet einen Meldungsspeicher, in dem eingehende Mails gespeichert werden, bis sich der entsprechende Empfänger anmeldet und die Mails herunterlädt. POP3 ist ein einfaches System mit wenig Auswahlmöglichkeiten. Alle ausstehenden Meldungen und Anhänge werden zur selben Zeit heruntergeladen. POP3 verwendet das SMTP-Meldungsprotokoll.

Spezielle Anschlussnummer: Sie können drei zusätzliche Anwendungen hinzufügen, indem Sie deren jeweilige Anschlussnummern in die Felder *Spezielle Anschlussnummer* eingeben.

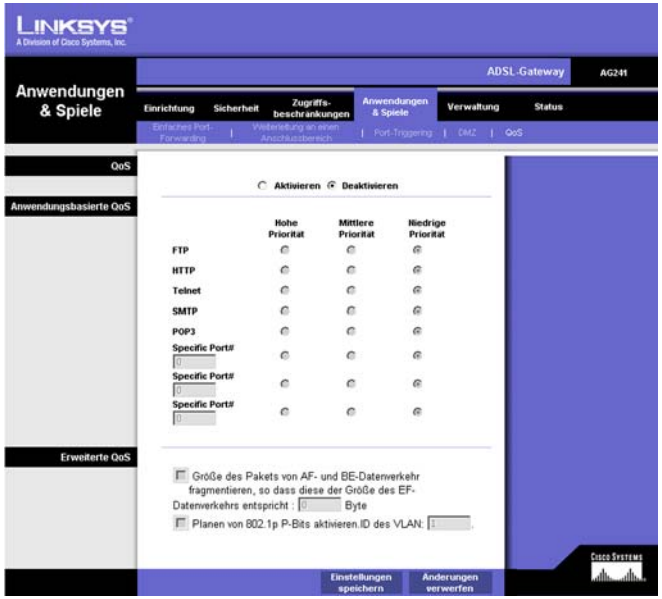

Abbildung 5-28: QOS

Erweiterte QoS

Mit dieser Einstellung können Sie Prioritäten für die Datenverkehrswarteschlange festlegen.

Fragment packet's size of AF and BE traffic to be equal to the size of EF traffic (Größe des Pakets von AF- und BE-Datenverkehr fragmentieren, sodass diese der Größe des EF-Datenverkehrs entspricht): Wählen Sie diese Option aus, um die Paketgrößen von Warteschlangen der Art AF (*Assured Forwarding*; Garantierte Weiterleitung) und BE (*Best Effort*; Beste Bemühung) zu fragmentieren, sodass die Effizienz zum Übertragen von Warteschlangen der Art EF (*Expedited Forwarding*; Express-Weiterleitung) erhöht wird. Geben Sie einen Bereich zwischen 68 und 1492 Byte ein.

Enable 802.1p P bits scheduling. VLAN's VID. (Planen von 802.1p P-Bits aktivieren. ID des VLAN): Wählen Sie diese Option aus, um das Planen von 802.1p P-Bits-Klassifikationen für das entsprechende VLAN basierend auf der IEEE 802.1Q VLAN-Identifikation zu aktivieren. Geben Sie die VLAN-ID in das Feld ein.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Einstellungen speichern**, oder klicken Sie auf die Schaltfläche **Änderungen verwerfen**, um die Änderungen rückgängig zu machen.

Registerkarte Verwaltung

Verwaltungsfunktionen

Über das Fenster *Verwaltungsfunktionen* können Sie die Einstellungen für den Gateway-Zugriff sowie die Einstellungen für **SNMP** (*Simple Network Management Protocol*) und **UPnP** (*Universal Plug and Play*) ändern.

Gateway-Zugriff

Lokaler Gateway-Zugriff: Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Passworts aufgefordert. Der Standardbenutzername und das Standardpasswort sind **admin**.

- **Gateway-Benutzername**: Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway-Passwort**: Es wird empfohlen, dass Sie Ihr Standardpasswort in ein persönliches Passwort ändern.
- **Zur Bestätigung erneut eingeben**: Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.
- **Entfernter Gateway-Zugriff**: Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

Abbildung 5-29: Verwaltungsfunktionen

WICHTIG: Durch Aktivieren der Funktion **Entfernte Verwaltung** ist es jedem Benutzer, der auf Ihr Passwort zugreifen kann, möglich, das Gateway von jedem beliebigen Standort im Internet aus zu konfigurieren.

- **Entfernte Verwaltung**: Mit dieser Funktion können Sie das Gateway von einem entfernten Standort aus über das Internet verwalten. Um **Entfernte Verwaltung** zu aktivieren, klicken Sie auf die Option **Aktivieren**.
- **Verwaltungsanschluss**: Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.

SNMP

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung.

Identifikation: Um **SNMP** zu verwenden, klicken Sie auf **Aktiviert**. Um **SNMP** zu deaktivieren, klicken Sie auf **Deaktiviert**.

UPnP

Mit UPnP kann unter Windows XP das Gateway automatisch für verschiedene Internetanwendungen, wie z. B. Internetspiele oder Videokonferenzen, konfiguriert werden.

UPnP: Um **UPnP** zu verwenden, klicken Sie auf **Aktivieren**.

Wählen Sie eine PVC-Verbindung aus. Wählen Sie im Dropdown-Menü eine Nummer aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Berichtaufzeichnung

Über die Registerkarte **Berichtaufzeichnung** steht ein Protokoll zur Verfügung, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für Ihre Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.

- **Protokoll**: Um die Berichtaufzeichnung zu verwenden, klicken Sie auf **Aktivieren**.
- **Logviewer-IP-Adresse**: Geben Sie in dieses Feld die IP-Adresse ein, über die die Protokolle empfangen werden sollen.

E-Mail-Warnungen

E-Mail-Warnungen: Um E-Mail-Warnungen zu verwenden, klicken Sie auf die Option **Aktivieren**.

- **DoS-Schwellwerte**: Geben Sie die Schwellwerte der Ereignisse an, die Sie empfangen möchten.
- **SMTP Mail-Server**: Geben Sie in dieses Feld die IP-Adresse des SMTP-Servers ein.
- **E-Mail-Adresse für Warnungsprotokolle**: Geben Sie in dieses Feld die E-Mail-Adresse für die Warnungsprotokolle ein.
- **E-Mail-Antwortadresse**: Geben Sie die E-Mail-Adresse für Antwort-E-Mails ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **Protokolle anzeigen**.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Einstellungen speichern**, um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Änderungen verwerfen**.

Abbildung 5-30: Berichtaufzeichnung

Abbildung 5-31: Systemprotokoll

Diagnose

Ping-Test

Ping-Test-Parameter

- **Ping-Ziel-IP-Adresse**: Geben Sie in dieses Feld die IP-Adresse ein, die Sie für den Ping-Befehl verwenden möchten. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping-Größe**: Geben Sie die Größe des Ping-Pakets an.
- **Anzahl der Pings**: Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping-Intervall**: Geben Sie das Ping-Intervall in Millisekunden an.
- **Ping-Wartezeit**: Geben Sie die Wartezeit in Millisekunden an.
- **Ping-Ergebnisse**: In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Klicken Sie auf die Schaltfläche **Test starten**, um den Ping-Test zu starten.

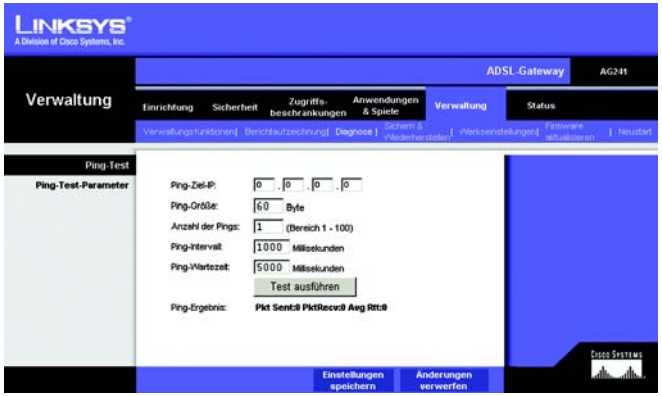

Abbildung 5-32: Ping-Test

Sichern & Wiederherstellen

Mit der Registerkarte **Sichern & Wiederherstellen** können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Routers auf die Schaltfläche **Sichern**. Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Routers auf die Schaltfläche **Browse** (Durchsuchen), um nach der Datei zu suchen, und befolgen Sie dann die Anweisungen auf dem Bildschirm. Wenn Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche **Wiederherstellen**.

Abbildung 5-33: Sichern & Wiederherstellen

Werkseinstellungen

Werkseinstellungen wiederherstellen: Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Ja**.

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, kicken Sie auf die Schaltfläche **Einstellungen speichern** bzw. klicken Sie auf **Änderungen verwerfe**), um Ihre Änderungen zu verwerfen.

Abbildung 5-34: Werkseinstellungen

Aktualisieren der Firmware

Mit dem ADSL Gateway können Sie Firmware für die LAN-Seite (Netzwerkseite) des Gateways aktualisieren.

Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der Linksys Website heruntergeladen und extrahiert haben.
2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Aktualisieren**, und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung 5-35: Firmware aktualisieren

Neustart

Über diese Registerkarte können Sie für Ihr Gateway einen Warm- oder Kaltstart ausführen.

Neustart-Modus: Um Ihr Gateway neu zu starten, wählen Sie **Kaltstart** oder **Warmstart** aus. Um das Gateway aus- und wieder einzuschalten, wählen Sie die Option **Kaltstart**. Um das Gateway neu zu starten, ohne es auszuschalten, wählen Sie die Option **Warmstart**.

Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um den Neustart zu starten. Ein Fenster wird angezeigt, in dem Sie gefragt werden, ob das Gerät neu gestartet werden soll. Klicken Sie auf **OK**.

Klicken Sie auf die Schaltfläche **Änderungen verwerfen**, wenn Sie Ihre Änderungen rückgängig machen möchten.

Abbildung 5-36: Neustart

Registerkarte

Gateway

In diesem Fenster werden Informationen zu Ihrem Gateway und den WAN-Internetverbindungen angezeigt.

Gateway-Informationen

Im Bereich der Gateway-Informationen sind Angaben zur Software-Version, MAC-Adresse und zur derzeitigen Zeit enthalten.

Internetverbindungen

Nachdem Sie die Nummer der Internetverbindung aus dem Dropdown-Menü ausgewählt haben, werden die Optionen der Internetverbindungen angezeigt. Dabei handelt es sich um **Anmeldetyp**, **Schnittstelle**, **IP-Adresse**, **Subnetzmaske**, **Standard-Gateway** und die Server **DNS 1**, **2** und **3**.

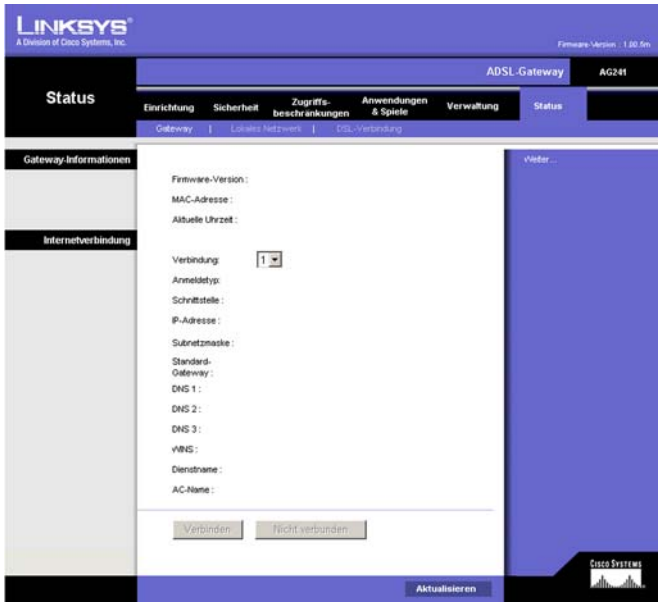

Abbildung 5-37: Status

DHCP erneuern: Klicken Sie auf die Schaltfläche **DHCP erneuern**, um die aktuelle IP-Adresse Ihres Gateways durch eine neue IP-Adresse zu ersetzen.

DHCP löschen: Klicken Sie auf die Schaltfläche **DHCP löschen**, um die aktuelle IP-Adresse Ihres Gateways zu löschen.

Klicken Sie auf die Schaltfläche Aktualisieren, um die Anzeige zu aktualisieren.

Lokales Netzwerk

Im Bereich der Angaben zum lokalen Netzwerk sind Informationen zur lokalen Mac-Adresse, IP-Adresse, Subnetzmaske, DHCP-Server und zur End-IP-Adresse aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP-Client-Tabelle**.

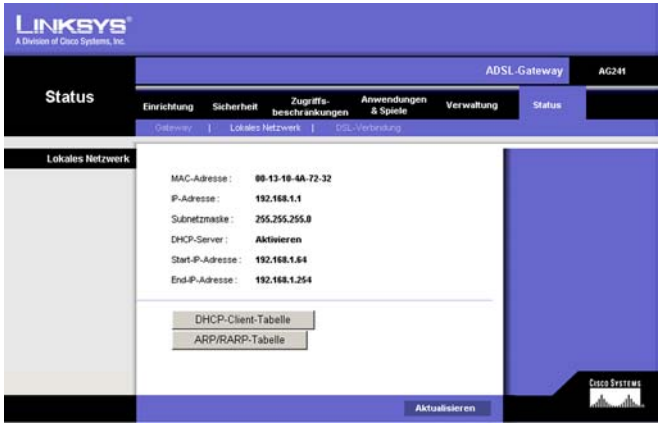

Abbildung 5-38: Lokales Netzwerk

DHCP-Client-Tabelle: Klicken Sie auf die Schaltfläche **DHCP-Client-Tabelle**, um die aktuellen DHCP-Client-Daten aufzurufen. In diesem Bereich sind MAC-Adresse, Computername sowie IP-Adresse der Netzwerk-Clients, die den DHCP-Server verwenden, aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus, und klicken Sie anschließend auf die Schaltfläche **Löschen**.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Anzeige zu aktualisieren. Klicken Sie auf die Schaltfläche **Schließen**, um das Fenster zu schließen.

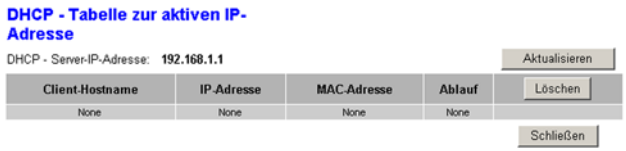

Abbildung 5-39: DHCP-Client-Tabelle

DSL-Verbindung

Die angezeigten DSL-Verbindungsinformationen beziehen sich auf den Status, die Downstream- und die Upstream-Rate.

Im Bereich der PVC-Verbindung sind folgende Informationen aufgeführt: Kapselungsmethode, Multiplexing, QoS (*Quality of Service*; Dienstqualität), PCR-Rate, SCR-Rate, automatische Erkennungsfunktion, VPI (*Virtual Path Identifier*; Virtueller Pfadidentifizierer), VCI (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer) sowie PVC-Status.

Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Anzeige zu aktualisieren.

Abbildung 5-40: DSL-Verbindung

Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: "Behebung häufig auftretender Probleme" und "Häufig gestellte Fragen". Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

Behebung häufig auftretender Probleme

1. ***Wie lege ich eine statische IP-Adresse auf einem Computer fest?***
   Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:
   - Für Benutzer von Windows 98 und ME:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
     2. Wählen Sie im Feld **Die folgenden Netzwerkkomponenten sind installiert** die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile "TCP/IP" ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
     3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften in der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
     4. Klicken Sie auf die Registerkarte **Gateway**, und geben Sie 192.168.1.1 ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
     5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass die Option **DNS** aktiviert ist. Geben Sie den Host- und den Domänennamen ein (z. B. "Johann" als Hostname und "home" als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
     6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster *Netzwerk* zu schließen.
     7. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.
   - Für Benutzer von Windows 2000:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.

2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
3. Wählen Sie im Feld **Aktivierte Komponenten werden von dieser Verbindung verwendet** die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
5. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
6. Geben Sie für das Standard-Gateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK** sowie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.
  1. Klicken Sie auf **Start** und **Systemsteuerung**.
  2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
  3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
  4. Wählen Sie im Feld **Diese Verbindung verwendet folgende Elemente** die Option **Internetprotokoll (TCP/IP)**. Klicken Sie auf die Schaltfläche **Eigenschaften**.
  5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
  6. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
  7. Geben Sie für das Standard-Gateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
  8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  9. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK**. Klicken Sie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.

2. Ich möchte meine Internetverbindung prüfen.

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in der Windows-Hilfe. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option **IP-Adresse von einem DHCP-Server beziehen** ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster *Netzwerk* auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie in das Feld **Öffnen** den Eintrag **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld Öffnen den Eintrag cmd ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie in die Eingabeaufforderung den Eintrag **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie in die Eingabeaufforderung den Eintrag **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie den Eintrag **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie in die Eingabeaufforderung den Eintrag **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Internet verbunden. Wenn Sie KEINE Website öffnen können, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.

- Lesen Sie sich den oben aufgeführten Abschnitt "2. Ich möchte meine Internetverbindung prüfen" durch, und überprüfen Sie anhand dessen Ihre Verbindung.
  1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: RFC 1483 Bridged (RFC 1483-Überbrückung), RFC 1483 Routed (RFC 1483-Übertragung), RFC 2516 PPPoE oder RFC 2364 PPPoA. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in "Kapitel 5: Konfigurieren des Gateways" im Abschnitt zur Einrichtung.
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob in der Spalte für das Gateway die ADSL-LED konstant leuchtet.
  3. Stellen Sie sicher, dass das an den ADSL-Port Ihres Gateways angeschlossene Kabel in die Wandbuchse der ADSL-Verbindung eingesteckt ist. Überprüfen Sie, ob in der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse Ihres ISP aufgeführt ist.
  4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer wieder ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

4. Ich kann auf die Einrichtungsseite des webbasierten Dienstprogramms des Gateways nicht zugreifen.

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter "2. Ich möchte meine Internetverbindung prüfen".
  1. Weitere Informationen dazu, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".
  2. Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter "1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?".
  3. Folgen Sie den Anweisungen unter "10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?".

5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.
- Ändern Sie die IP-Adresse des Gateways in ein anderes Subnetz, sodass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei "X" für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei "X" mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways in 192.168.2.1. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Einrichtung**.
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine IP-Adresse dementsprechend in 192.168.2.Y (wobei "Y" für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Port 500/UDP-Pakete an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter "7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden."
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP Ausgang) sowie Port 110 (POP3 Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um die Port-Weiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mail-Servern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Anwendungen und Spiele** die Registerkarte **Weiterleitung an einen Anschlussbereich** auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben

Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".

6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
Webserver	80 bis 80	X		192.168.1.100	X
FTP-Server	21 bis 21	X		192.168.1.101	X
SMTP (Ausgang)	25 bis25	X		192.168.1.102	X
POP3 (Eingang)	110 bis 110	X		192.168.1.102	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Einstellungen speichern**.

7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden.

Zum Verwenden von Online-Spielen oder Internetanwendungen ist i. d. R. kein Port-Forwarding bzw. kein DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internetanwendungen anwenden. Dafür müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internetanwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internetanwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Anwendungen und Spiele** die Registerkarte **Weiterleitung an einen Anschlussbereich** auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
UT	7777 bis 27900	X	X	192.168.1.100	X
Halflife	27015 bis 27015	X	X	192.168.1.105	X
PCAnywhere	5631 bis 5631		X	192.168.1.102	X
VPN/IPSEC	500 bis 500		X	192.168.1.100	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Einstellungen speichern**.

8. Weder Internetspiele, Internetserver noch Internetanwendungen funktionieren.

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ-Hosting (*DeMilitarized Zone*) mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Forwarding-Einträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da das Forwarding Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: In dem Gateway eingehende Daten werden zuerst hinsichtlich ihrer Forwarding-Einstellungen überprüft. Falls die Daten von einer Port-Nummer eingehen, für die kein Port-Forwarding aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)

- Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Anwendungen und Spiele** die Registerkarte **DMZ** auf. Wählen Sie **Aktiviert** aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zum Port-Forwarding, und deaktivieren bzw. entfernen Sie die Einträge zum Forwarding. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Einstellungen speichern**.

9. Ich habe das Passwort vergessen bzw. die Aufforderung zur Eingabe des Passworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.

- Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Passworts aufgefordert werden, führen Sie die folgenden Schritte aus:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein, und rufen Sie unter **Verwaltung** die Registerkarte **Verwaltungsfunktionen** auf.
  2. Geben Sie in das Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend das gleiche Passwort in das zweite Feld ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Einstellungen speichern**.

10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?

Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da es sich bei dem Gateway um das Gateway für die Internetverbindung handelt, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Benutzer von Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Benutzer von Netscape 4.7 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorn zu beginnen.

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Passwort, die Forwarding-Funktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway greift auf die werkseitigen Konfigurationseinstellungen zurück.

12. Ich möchte die Firmware aktualisieren.

Um die aktuellsten Funktionen für Ihre Firmware zu erhalten, gehen Sie auf die internationale Website von Linksys und laden Sie die neueste Firmware unter www.linksys.com/international herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Produkte**, und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Website des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.

4. Um die Firmware zu aktualisieren, führen Sie die in "Kapitel 5: Konfigurieren des Gateways" im Abschnitt **Verwaltung** aufgeführten Schritte durch.

13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.
- Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter "1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?". Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder der Registerkarte **Verwaltung** im webbasierten Dienstprogramm des Gateways vor.

14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Einrichtungsoption zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie im Setup-Fenster die Option **Verbindung aufrechterhalten** aus, und legen Sie für die Option **Wahlwiederholung** 20 Sekunden fest.
  4. Klicken Sie auf die Schaltfläche **Einstellungen speichern**. Klicken Sie auf die Registerkarte **Status**, und klicken Sie auf Schaltfläche **Verbinden**.
  5. Möglicherweise wird **Verbindung wird hergestellt** als Anmeldestatus angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Verbunden** als Anmeldestatus angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um fortzufahren.
- Falls die Verbindung erneut unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung wiederherzustellen.

15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich bekomme nur beschädigte Daten aus dem Internet.

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie für die MTU-Option **Manuell** aus. Geben Sie in das Feld Size (Größe) den Wert **1492** ein.
  4. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um fortzufahren.
- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert in einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis Ihr Problem gelöst ist:
  1462
  1400
  1362
  1300

16. Die Netzstrom-LED leuchtet durchgehend.

Die Netzstrom-LED leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Zwischenzeitlich fährt der Computer hoch und wird auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED immer noch blinkt, funktioniert das Gerät nicht ordnungsgemäß. Führen Sie einen Firmware-Flash durch, indem Sie dem Computer eine statische IP-Adresse zuweisen, und aktualisieren Sie anschließend die Firmware. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse 192.168.1.50, Subnetzmaske 255.255.255.0.

17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang erneut auszuführen.

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standard-Gateway und DNS). Starten Sie den Computer, bei dem das Problem aufgetreten ist, erneut.
- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, ob es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Gateway her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/ADSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.
- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.

- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Häufig gestellte Fragen

Wie viele IP-Adressen kann das Gateway maximal unterstützen?
Das Gateway unterstützt bis zu 253 IP-Adressen.

Unterstützt das Gateway IPSec-Passthrough?
Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

An welcher Stelle im Netzwerk wird das Gateway installiert?
In einer typischen Umgebung wird das Gateway zwischen der ADSL-Wandbuchse und dem LAN installiert.

Unterstützt das Gateway IPX oder AppleTalk?
Nein. TCP/IP ist der einzige Internet-Protokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets mit einem LAN verwendet werden.

Unterstützt die LAN-Verbindung des Gateways 100-Mbit/s-Ethernet?
Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 Mbit/s.

Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?
Die NAT-Funktion (*Network Address Translation*; Netzwerk-Adressen-Übersetzung) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheitsstufe erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private Adressen hinter einer einzigen vom ISP zur Verfügung gestellten Adresse verwenden.

Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?
Ja. Linksys bietet jedoch derzeit keinen technischen Support hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als die Windows-Betriebssysteme an.

Unterstützt das Gateway die ICQ-Dateiübertragung?
Ja. Führen Sie folgende Schritte dazu aus: Klicken Sie auf das Menü **ICQ**, dann auf **Einstellungen** und auf die Registerkarte **Verbindungen**. Aktivieren Sie dann die Option **Ich bin hinter einer Firewall oder einem Proxy**. Legen Sie nun in den Einstellungen für die Firewall für die Zeitüberschreitung 80 Sekunden fest. Der Internetbenutzer kann nun Dateien an Benutzer hinter dem Gateway senden.

Ich habe einen Unreal Tournament-Server eingerichtet, andere Benutzer im LAN können sich jedoch nicht mit dem Server verbinden. Was muss ich tun?
Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN erstellen sowie die Ports 7777, 7778, 7779, 7780, 7781 und 27900 an die IP-Adresse des Servers weiterleiten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie einen weiteren Port weiterleiten. (Das kann Port 8080 sein, der jedoch für die Remote-Verwaltung verwendet wird. Sie müssen u. U. diese Funktion deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für "ListenPort" den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für "ServerName" die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?
Das hängt vom verwendeten Netzwerkspiel bzw. dem verwendeten Server ab. So unterstützt z. B. Unreal Tournament das mehrfache Anmelden mit nur einer öffentlichen IP-Adresse.

Wie kann ich Half-Life - Team Fortress mit dem Gateway verwenden?
Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen "+clientport 2700x" hinzugefügt werden, wobei "x" dann 6, 7, 8 usw. entspricht. Dadurch können mehrere Computer mit dem gleichen Server eine Verbindung herstellen. Problem: Bei Version 1.0.1.6 können mehrere Computer, die den gleichen CD-Schlüssel verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Ausführen von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

Die Website reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?
Legen Sie für Ihren Ethernet-Adapter 10 Mbit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Aushandlung. (Rufen Sie über die Netzwerksystemsteuerung die Registerkarte für die erweiterten Eigenschaften des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste drücken, bis die Netzstrom-LED aufleuchtet und wieder erlischt. Setzen Sie das DSL-Modem zurück, indem Sie es aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?
Sämtliche Aktualisierungen für Linksys-Firmware werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **Administration** (Verwaltung) des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

Funktioniert das Gateway in einer Macintosh-Umgebung?
Ja, Sie können jedoch nur über Internet Explorer 4.0 bzw. Netscape Navigator 4.0 oder höher für Macintosh auf die Einrichtungsseiten des Gateways zugreifen.

Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Was bedeutet DMZ-Hosting?
Mithilfe der DMZ (*Demilitarized Zone*; Entmilitarisierte Zone) kann über eine IP-Adresse (d. h. über einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in "Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters".

Verwenden bei DMZ-Hosting sowohl Benutzer als auch Gateway die öffentliche IP-Adresse?
Nein.

Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

Ist das Gateway auch plattformübergreifend einsetzbar?
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

Wie viele Ports können gleichzeitig weitergeleitet werden?
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

Über welche erweiterten Funktionen verfügt das Gateway?
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Weiterleitung, Routing und DDNS.

Wie viele VPN-Sitzungen unterstützt das Gateway maximal?
Die maximale Anzahl hängt von vielen Faktoren ab. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?
Wenden Sie sich an Ihren ISP, um diese Informationen zu erhalten.

Wie kann ich mIRC mit dem Gateway verwenden?
Legen Sie in der Registerkarte **Port Forwarding** (Port-Forwarding) den Wert 113 für den Computer fest, auf dem Sie mIRC verwenden möchten.

Kann das Gateway als DHCP-Server eingesetzt werden?
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

Was ist eine MAC-Adresse?
Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Nummer, die jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, vom Hersteller zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

Wie setze ich das Gateway zurück?
Halten Sie die Reset-Taste auf der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

Wenn Ihre Fragen hier nicht beantwortet wurden, finden Sie weitere Informationen auf der internationalen Linksys-Website unter www.linksys.com/international.

Anhang B: Konfigurieren von IPSec zwischen einem Windows 2000-/XP-Computer und dem Gateway

Einführung

In diesem Dokument finden Sie Anweisungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden. Detaillierte Informationen zur Konfiguration von Windows 2000-Servern finden Sie auf der Website von Microsoft:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

HINWEIS: Zeichnen und bewahren Sie sämtliche von Ihnen vorgenommenen Änderungen auf. Diese Änderungen sind für die Windows-Anwendung "secpol" und dem webbasierten Dienstprogramm des Routers identisch.

Umgebung

Die hier erwähnten IP-Adressen und weiteren Einstellungen sind lediglich zu Darstellungszwecken aufgeführt.

HINWEIS: Die Anweisungen und Abbildungen in diesem Abschnitt der Anleitung beziehen sich auf den Router. Ersetzen Sie "Router" durch "Gateway". Die Optionen "OK" bzw. "Schließen" können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Windows 2000 oder Windows XP
IP-Adresse: 140.111.1.2 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0

WAG54G

WAN-IP-Adresse: 140.111.1.1 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte WAN-IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0
LAN-IP-Adresse: 192.168.1.1
Subnetzmaske: 255.255.255.0

Hinweise zum Einrichten eines sicheren IPSec-Tunnels

Schritt 1: Erstellen einer IPSec-Richtlinie

1. Klicken Sie auf die Schaltfläche **Start**, wählen Sie **Ausführen** aus, und geben Sie in das Feld **Öffnen** den Eintrag **secpol.msc** ein. Das in Abbildung B-1 dargestellte Fenster *Lokale Sicherheitseinstellungen* wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Lokaler Computer** (Win XP) bzw. auf **IP-Sicherheitsrichtlinien auf lokalem Computer** (Win 2000), und wählen Sie anschließend **IP-Sicherheitsrichtlinie erstellen** aus.

3. Klicken Sie auf die Schaltfläche **Weiter**, und geben Sie für Ihre Richtlinie einen Namen ein (zum Beispiel "an_Router"). Klicken Sie anschließend auf **Weiter**.

4. Deaktivieren Sie das Kontrollkästchen **Die Standardantwortregel aktivieren**, und klicken Sie anschließend auf die Schaltfläche **Weiter**.

5. Klicken Sie auf die Schaltfläche **Fertig stellen**, und vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert ist.

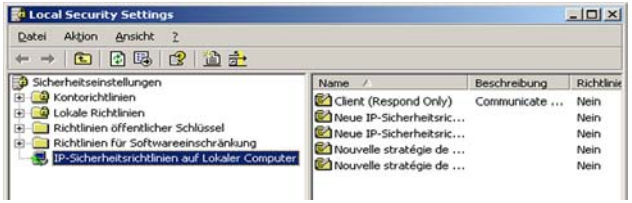

Abbildung B-1: Fenster "Lokale Sicherheitseinstellungen"

HINWEIS: Jeder Bezug in diesem Kapitel auf "win" verweist auf Windows 2000 und Windows XP. Ersetzen Sie die Hinweise auf "Router" durch "Gateway". Die Optionen "OK" bzw. "Schließen" können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Schritt 2: Erstellen von Filterlisten

Filterliste 1: win->Router

1. Vergewissern Sie sich, dass im Fenster für die Eigenschaften der neuen Richtlinie die Registerkarte **Regeln** ausgewählt ist (siehe Abbildung B-2). Deaktivieren Sie das Kontrollkästchen **Assistent verwenden**, und klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel zu erstellen.

2. Stellen Sie sicher, dass die Registerkarte **IP-Filterliste** ausgewählt ist, und klicken Sie auf die Schaltfläche **Hinzufügen** (siehe Abbildung B-3). Das Fenster *IP-Filterliste* wird angezeigt (siehe Abbildung B-4). Geben Sie für die Filterliste einen geeigneten Namen, wie z. B. win -> Router, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

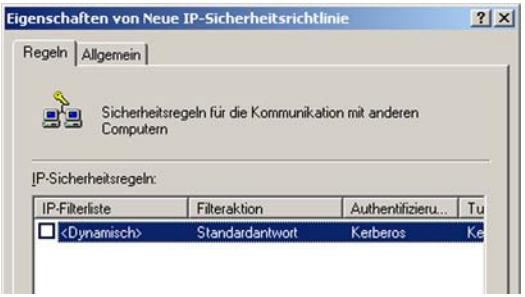

Abbildung B-2: Registerkarte "Regeln"

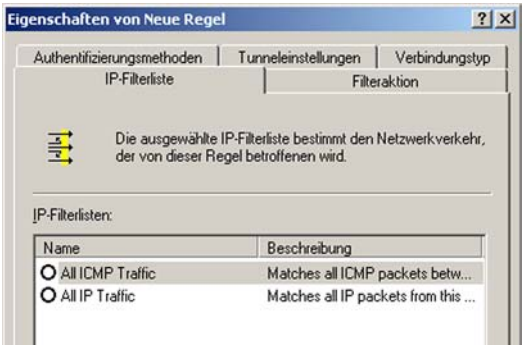

Abbildung B-3: Registerkarte "IP-Filterliste"

3. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung B-5).Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Eigene IP-Adresse** aus. Wählen Sie im Feld **Zieladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse. 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Dabei handelt es sich um die Standardeinstellungen des Routers. Falls Sie an diesen Einstellungen Änderungen vorgenommen haben, geben Sie die geänderten Werte ein.)

4. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

5. Klicken Sie auf **OK**. Klicken Sie anschließend im Fenster *Filterliste* auf die Schaltfläche **OK** bzw. **Schließen**.

Filterliste 2: Router ->win

6. Das Fenster *Eigenschaften von Neue Regel* wird angezeigt (siehe Abbildung B-6). Wählen Sie die Registerkarte **IP-Filterliste** aus, und stellen Sie sicher, dass **win -> Router** markiert ist. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

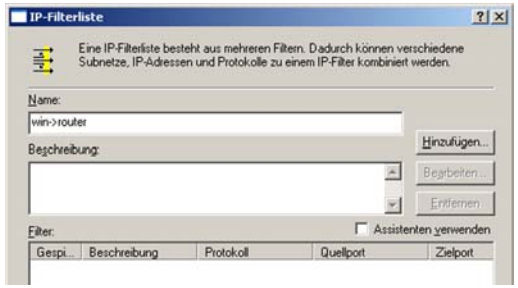

Abbildung B-4: Dialogfeld "IP-Filterliste"

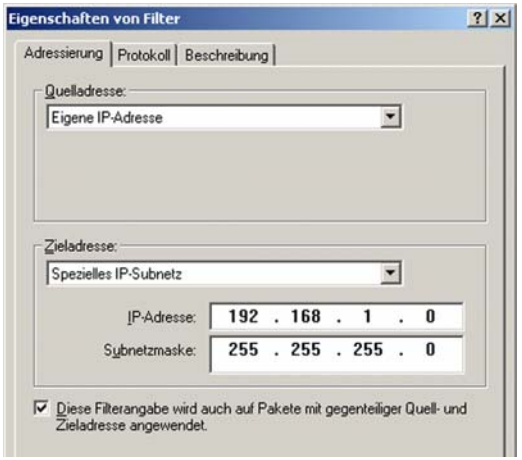

Abbildung B-5: Dialogfeld "Eigenschaften von Filter"

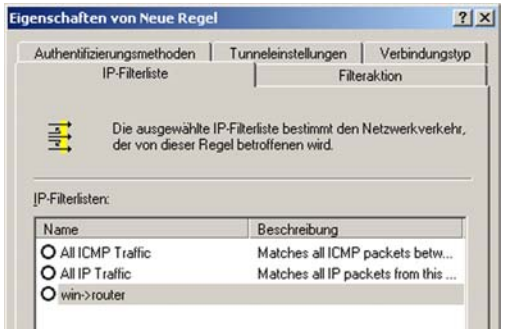

Abbildung B-6: Dialogfeld "Eigenschaften von Neue Regel"

7. Das Fenster *IP-Filterliste* wird angezeigt (siehe Abbildung B-7). Geben Sie für die Filterliste einen geeigneten Namen, z. B. Router->win, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

8. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung B-8). Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Falls Sie an diesen Standardeinstellungen Änderungen vorgenommen haben, geben Sie hier die neuen Werte ein.) Wählen Sie im Feld **Zieladresse** die Option **Eigene IP-Adresse** aus.

9. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

10. Klicken Sie auf die Schaltfläche **OK** bzw. **Schließen**, woraufhin das Fenster *Eigenschaften von Neue Regel* angezeigt wird und die Registerkarte **IP-Filterliste** ausgewählt ist (siehe Abbildung B-9). Hier sollte der Listeneintrag "Router -> win" und "win -> Router" aufgeführt sein. Klicken Sie im Fenster *IP-Filterliste* auf die Schaltfläche **OK** (unter Windows XP) bzw. die Schaltfläche **Schließen** (unter Windows 2000).

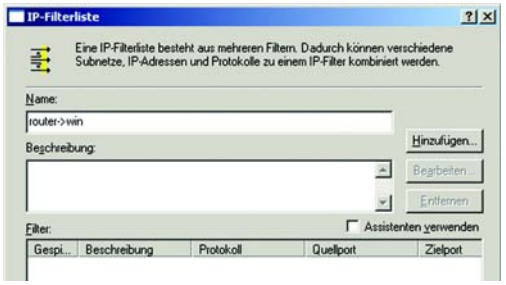

Abbildung B-7: Dialogfeld "IP-Filterliste"

Abbildung B-8: Dialogfeld "Eigenschaften von Filter"

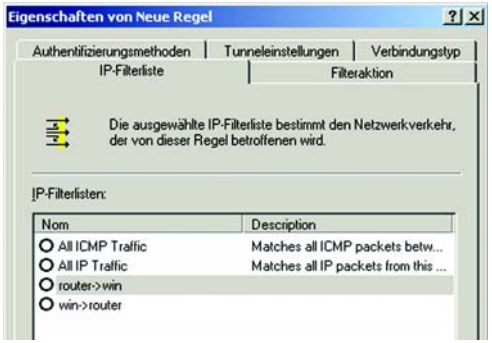

Abbildung B-9: Dialogfeld "Eigenschaften von Neue Regel"

Schritt 3: Konfigurieren von individuellen Tunnelregeln

Tunnel 1: win->Router

1. Klicken Sie, wie in Abbildung B-10 dargestellt, auf die Registerkarte **IP-Filterliste** und anschließend auf die Filterliste "win -> Router".

2. Klicken Sie auf die Registerkarte **Filteraktion** (siehe Abbildung B-11), und klicken Sie auf die für die Filteraktion erforderliche Optionsschaltfläche **Sicherheit erforderlich**. Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

3. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung B-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

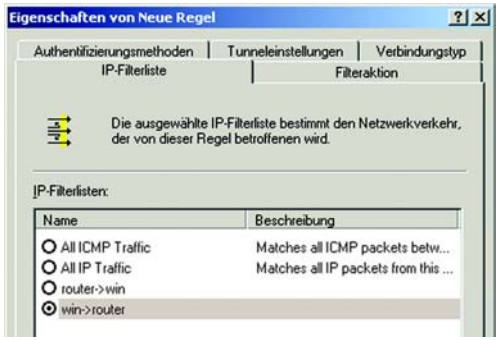

Abbildung B-10: Registerkarte "IP-Filterliste"

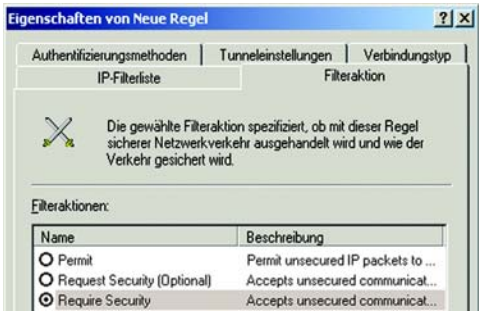

Abbildung B-11: Registerkarte "Filteraktion"

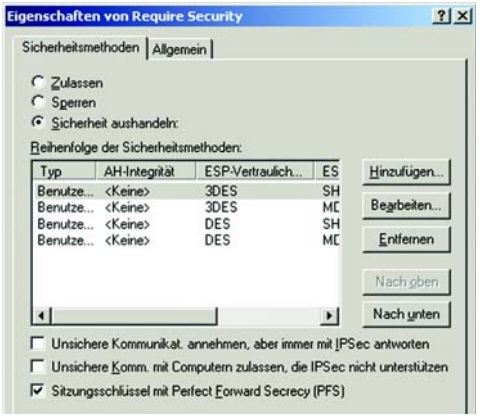

Abbildung B-12: Registerkarte "Sicherheitsmethoden"

4. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden** (siehe Abbildung B-13), und klicken Sie auf die Schaltfläche **Bearbeiten**.

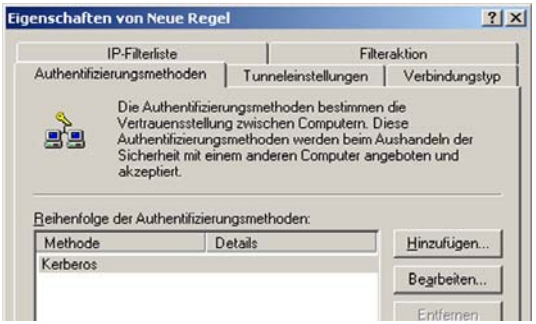

Abbildung B-13: Registerkarte "Authentifizierungsmethoden"

5. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette (vorinstallierter Schlüssel) verwenden** (siehe Abbildung B-14), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. Klicken Sie auf **OK**.

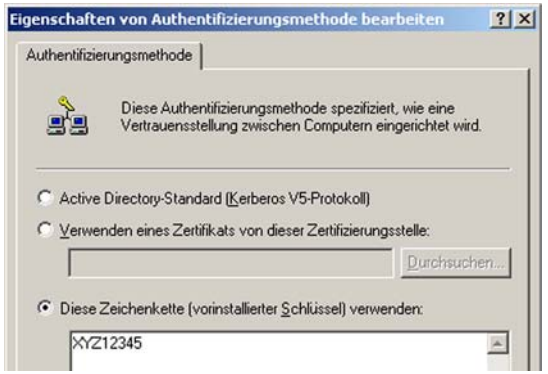

Abbildung B-14: Vorinstallierter Schlüssel

6. Dieser neue vorinstallierte Schlüssel ist in Abbildung B-15 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

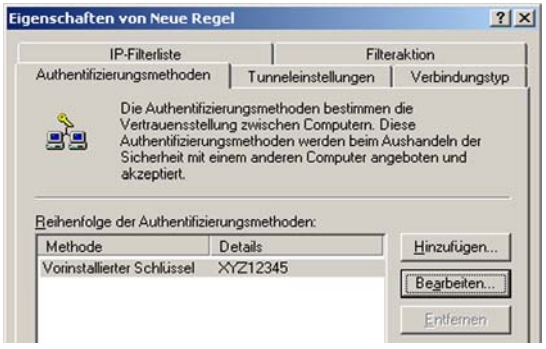

Abbildung B-15: Neuer vorinstallierter Schlüssel

7. Wählen Sie die Registerkarte **Tunneleinstellungen** (siehe Abbildung B-16), und aktivieren Sie die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**. Geben Sie anschließend die WAN-IP-Adresse des Routers ein.

Abbildung B-16: Registerkarte "Tunneleinstellungen"

8. Wählen Sie die Registerkarte **Verbindungstyp** (siehe Abbildung B-17), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um diese Regel abzuschließen.

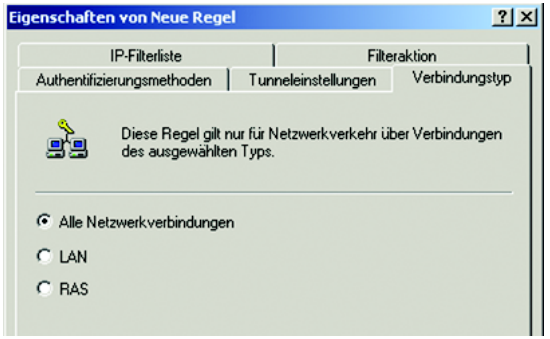

Abbildung B-17: Registerkarte "Verbindungstyp"

Tunnel 2: Router->win

9. Vergewissern Sie sich, dass im Dialogfeld für die Eigenschaften der neuen Richtlinie (siehe Abbildung B-18) der Eintrag "win -> Router" ausgewählt ist, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um einen zweiten IP-Filter zu erstellen.

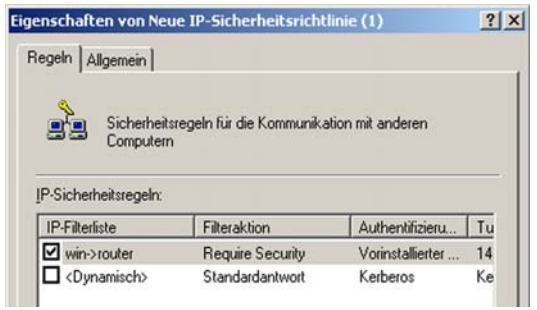

Abbildung B-18: Fenster für die Eigenschaften der neuen Richtlinie

10. Aktivieren Sie in der Registerkarte **IP-Filterliste** die Optionsschaltfläche für die Filterliste **Router -> win** (siehe Abbildung B-19).

Abbildung B-19: Registerkarte "IP-Filterliste"

11. Klicken Sie auf die Registerkarte **Filteraktion**, und wählen Sie die Filteraktion **Sicherheit erforderlich** aus (siehe Abbildung B-20). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung B-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

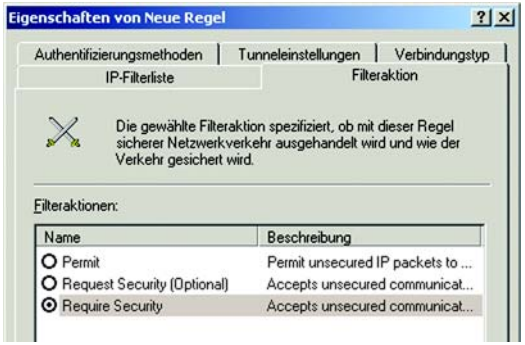

Abbildung B-20: Registerkarte "Filteraktion"

12. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden**, und stellen Sie sicher, dass die Kerberos-Authentifizierungsmethode aktiviert ist (siehe Abbildung B-21). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

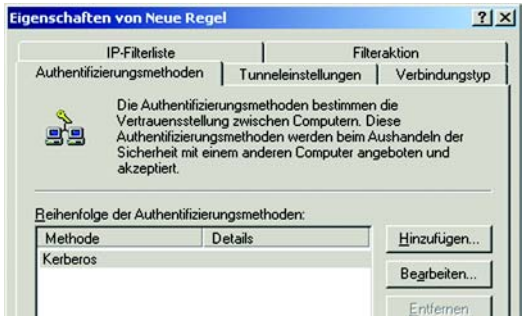

Abbildung B-21: Registerkarte "Authentifizierungsmethode"

13. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden** (siehe Abbildung B-22), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. (Die hier aufgeführte Schlüsselzeichenkette dient als Beispiel. Ihre Schlüsselzeichenkette sollte eindeutig und leicht zu merken sein.) Klicken Sie anschließend auf die Schaltfläche **OK**.

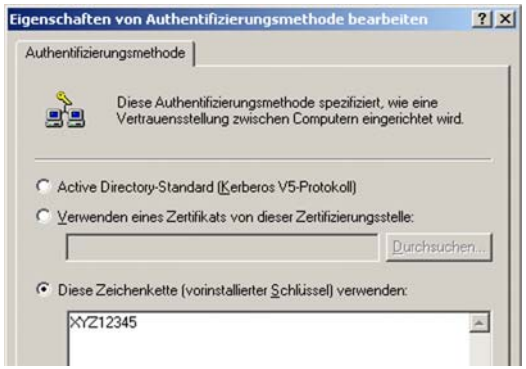

Abbildung B-22: Vorinstallierter Schlüssel

14. Dieser neue vorinstallierte Schlüssel ist in Abbildung B-23 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

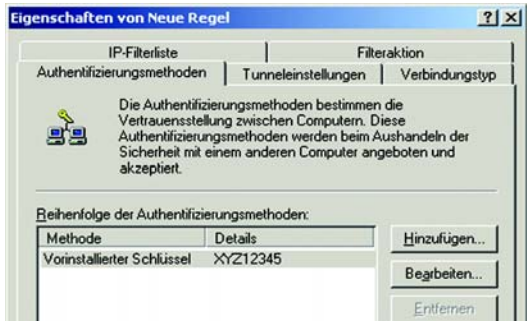

Abbildung B-23: Neuer vorinstallierter Schlüssel

15. Aktivieren Sie in der Registerkarte **Tunneleinstellungen** (siehe Abbildung B-24) die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**, und geben Sie die IP-Adresse des Computers ein, auf dem Windows 2000 bzw. Windows XP verwendet wird.

Abbildung B-24: Registerkarte "Tunneleinstellungen"

16. Klicken Sie auf die Registerkarte **Verbindungstyp** (siehe Abbildung B-25), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um den Vorgang zu beenden.

17. Klicken Sie in der Registerkarte **Regeln** (siehe Abbildung B-26) auf die Schaltfläche **OK** bzw. auf **Schließen**, um zum secpol-Bildschirm zurückzukehren.

Abbildung B-25: Registerkarte "Verbindungstyp"

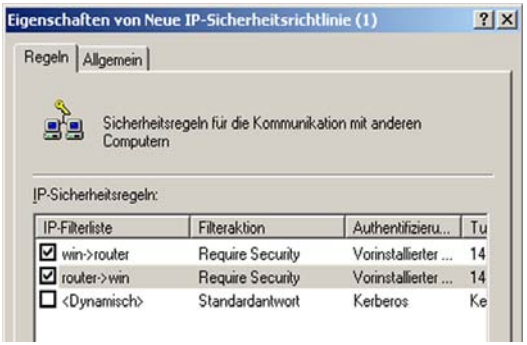

Abbildung B-26: Registerkarte "Regeln"

Schritt 4: Zuweisen einer neuen IPSec-Richtlinie

Klicken Sie im Bereich **Struktur** auf den Eintrag **IP-Sicherheitsrichtlinien auf lokalem Computer** (Abbildung B-27) und anschließend mit der rechten Maustaste auf die Richtlinie "an_Router". Klicken Sie nun auf die Option **Zuweisen**. Im Ordnersymbol wird ein grüner Pfeil angezeigt.

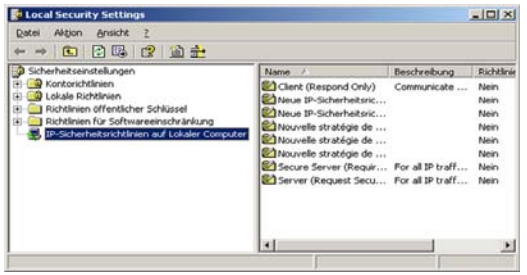

Abbildung B-27: Dialogfeld "Lokale Sicherheitseinstellungen"

Schritt 5: Erstellen eines Tunnels mithilfe des webbasierten Dienstprogramms

1. Geben Sie im Adressfeld des Web-Browsers **192.168.1.1** ein. Drücken Sie die Eingabetaste.
2. Wenn die Felder für den Benutzernamen und das Passwort angezeigt werden, geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein. Drücken Sie die Eingabetaste.
3. Klicken Sie in der Registerkarte **Setup** (Einrichtung) auf die Registerkarte **VPN**.
4. Wählen Sie in der Registerkarte **VPN**, wie in Abbildung B-28 dargestellt, den zu erstellenden Tunnel aus der Dropdown-Liste **Tunneleintrag auswählen** aus. Klicken Sie dann auf **Aktivieren**. Geben Sie im Feld **Tunnelname** den Namen des Tunnels ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird.
5. Geben Sie im Feld **Lokale sichere Gruppe** die IP-Adresse und Subnetzmaske des lokalen VPN-Routers ein. Geben für den letzten IP-Adressensatz **0** ein, um das gesamte IP-Subnetz freizugeben (z. B. 192.168.1.0).
6. Geben Sie im Feld **Entfernter Sicherheits-Router** die IP-Adresse und die Subnetzmaske des VPN-Geräts am anderen Ende des Tunnels ein (der entfernte VPN-Router oder das Gerät, mit dem Sie kommunizieren möchten).
7. Wählen Sie aus zwei unterschiedlichen Verschlüsselungstypen aus: **DES** und **3DES** (empfohlen wird **3DES**, da dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Deaktivieren** auswählen.
8. Wählen Sie aus zwei Authentifizierungstypen aus: **MD5** und **SHA** (empfohlen wird **SHA**, da dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit **Disable** (Deaktivieren) an beiden Enden des Tunnels deaktiviert werden.
9. Wählen Sie die Schlüsselverwaltung aus. Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Vorläufiger gemeinsamer Schlüssel** ein. Markieren Sie das Kontrollkästchen neben **PFS** (Perfect Forward Secrecy) [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden. Im Feld **Schlüssel-Verwendungsdauer** können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, sodass der Schlüssel unbegrenzt lange zur Verfügung steht.
10. Klicken Sie auf die Schaltfläche **Einstellungen speichern**, um die Änderungen zu speichern.

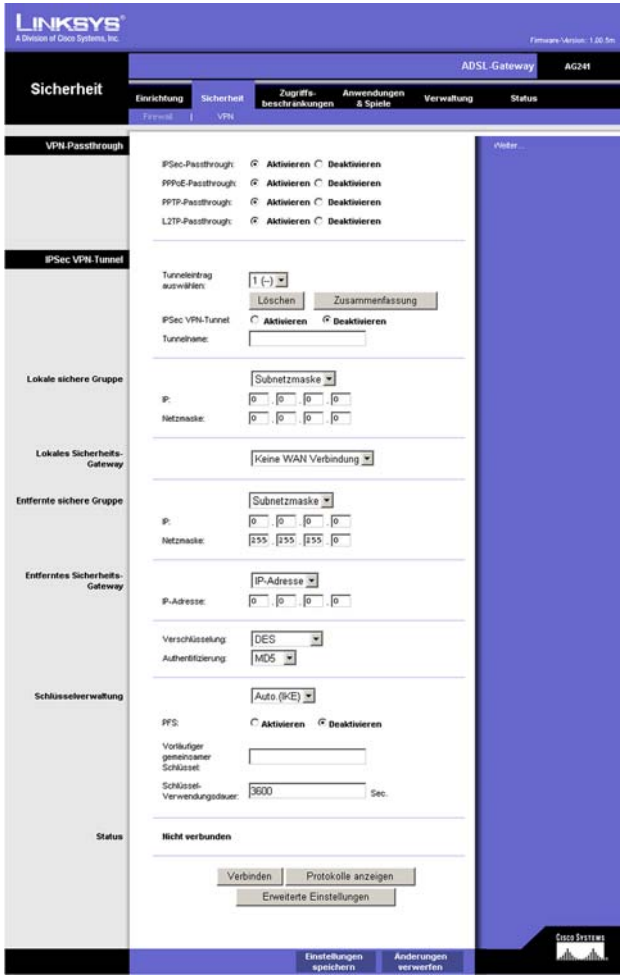

Abbildung B-28: Registerkarte "VPN"

Der Tunnel ist nun hergestellt.

Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Forwarding- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag **winipcfg** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster *IP Configuration* (IP-Konfiguration) den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung C-1.

3. Notieren Sie die Adapteradresse so, wie sie auf dem Bildschirm Ihres Computers angezeigt wird (siehe Abbildung C-2). Sie bildet die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.

Hinweis: Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

Abbildung C-1: Fenster IP-Konfiguration

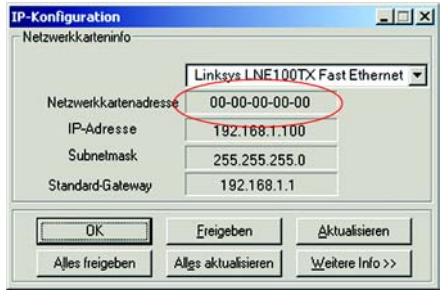

Abbildung C-2: MAC-Adresse/ Adapteradresse

Anweisungen für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Hinweis: Die MAC-Adresse wird auch als physikalische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **ipconfig /all** ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physikalische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse Ihres Ethernet-Adapters dar. Sie wird als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/physikalische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-3 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.

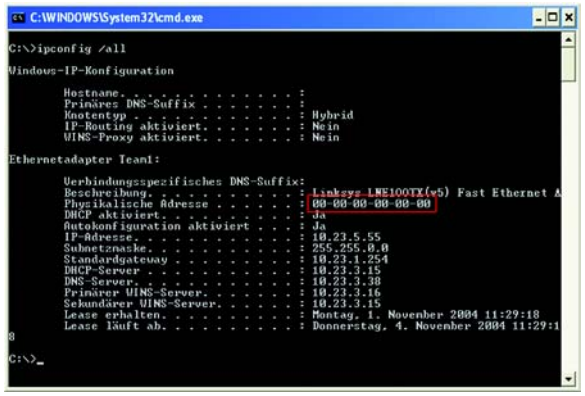

Abbildung C-3: MAC-Adresse/physikalische Adresse

Anhang D: Glossar

802.11a: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s sowie eine Betriebsfrequenz von 5 GHz festlegt.

802.11b: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 Mbit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

802.11g: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz festlegt sowie Abwärtskompatibilität mit Geräten garantiert, die dem Standard 802.11b entsprechen.

Access Point: Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem Kabelnetzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

Adapter: Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhält.

Ad-Hoc: Eine Gruppe von Wireless-Geräten, die statt über einen Access Point direkt miteinander kommunizieren (Peer-to-Peer).

Aktualisierung: Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

Backbone: Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

Bandbreite: Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

Bandspreizung: Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

Beacon-Intervall: Das Sendeintervall des Beacons, einer Paketübertragung eines Gateways zur Synchronisierung eines Wireless-Netzwerks.

Bit: Eine binäre Einheit.

Breitband: Eine stets aktive, schnelle Internetverbindung.

Bridge: Ein Gerät, das zwei verschiedene lokale Netzwerke verbindet, wie beispielsweise ein Wireless-Netzwerk mit einem verdrahteten Netzwerk.

Browser: Ein Browser ist eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen zugegriffen werden kann.

CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenverluste im Netzwerk zu verhindern.

CTS (*Clear To Send*): Ein von einem Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

Daisy Chain (Verkettung): Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

Datenbank: Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

DDNS (*Dynamic Domain Name System*): System, in dem eine Website, ein FTP- oder E-Mail-Server mit einer dynamischen IP-Adresse einen festen Domänennamen verwenden kann.

DHCP (*Dynamic Host Configuration Protocol*): Ein Protokoll, das es einem Gerät in einem LAN (auch als DHCP-Server bezeichnet) ermöglicht, anderen Geräten im Netzwerk, in der Regel Computern, temporäre IP-Adressen zuzuweisen.

DMZ (*Demilitarized Zone*): Hebt den Firewall-Schutz des Gateways für einen Computer auf, sodass dieser im Internet "sichtbar" wird.

DNS (*Domain Name Server*): Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

Domäne: Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

DSL (*Digital Subscriber Line*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

DSSS (*Direct-Sequence Spread-Spectrum*): Eine bestimmte Art der Funkübertragungstechnologie, die ein redundantes Bit-Muster enthält, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken. Wird für 802.11b-Netzwerke verwendet.

DTIM (*Delivery Traffic Indication Message*): Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz von Wireless-Verbindungen beitragen kann.

Durchsatz: Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

Dynamische IP-Adresse: Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

Ethernet: IEEE-Standardnetzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

Finger: Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

Firewall: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.

Firmware: 1. Die Programmierung in Netzwerkgeräten, mit der das Gerät gesteuert wird. 2. In den Lesespeicher (ROM) bzw. programmierbaren Lesespeicher (PROM) geladene Programmierung, die von Endbenutzern nicht geändert werden kann.

Fragmentierung: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über ein Netzwerkmedium, das die ursprüngliche Größe des Pakets nicht unterstützt.

FTP (*File Transfer Protocol*): Standardprotokoll für das Senden von Dateien zwischen Computern über ein TCP/IP-Netzwerk und das Internet.

Gateway: System zur Verbindung von Netzwerken untereinander.

Halbduplex: Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

Hardware: Als Hardware bezeichnet man die physischen Geräte im Computer- und Telekommunikationsbereich sowie andere Informationstechnologiegeräte.

Herunterladen: Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

Hochfahren: Starten von Geräten, sodass diese Befehle ausführen.

HTTP (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird.

IEEE (*The Institute of Electrical and Electronics Engineers*): Unabhängiges Institut, das Standards für den Netzwerkbetrieb entwickelt.

Infrastruktur: Die aktuell installierten Computer und Geräte im Netzwerk.

Infrastrukturmodus: Konfiguration, bei der ein Wireless-Netzwerk über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

IP (*Internet Protocol*): Zum Senden von Daten über das Netzwerk verwendetes Protokoll.

IP-Adresse: Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

IPCONFIG: Ein Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse von bestimmten Geräten im Netzwerk anzeigt.

IPSec (*Internet Protocol Security*): VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

ISM-Band: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendetes Funkband.

ISP (*Internet Service Provider;* Internetdienstanbieter): Anbieter, über den auf das Internet zugegriffen werden kann.

Kabelmodem: Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

Knoten: Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

Laden: Das Übertragen einer Datei über das Netzwerk.

LAN (*Local Area Network*): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.

MAC-Adresse (*Media Access Control*): Die eindeutige Adresse, die ein Hersteller den einzelnen Netzwerkbetriebsgeräten zuweist.

Mbit/s (Megabit pro Sekunde): Eine Million Bit pro Sekunde. Messeinheit für die Datenübertragung.

Multicasting: Das gleichzeitige Senden von Daten an mehrere Ziele.

NAT (*Network Address Translation*): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

Netzwerk: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und untereinander übertragen können.

NNTP (*Network News Transfer Protocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

OFDM (*Orthogonal Frequency Division Multiplexing*): Eine bestimmte Art der Modulationstechnologie, bei der der Datenstrom in eine Reihe von Datenströmen mit geringerer Geschwindigkeit geteilt wird, die dann parallel

übertragen werden. Wird in 802.11a- und 802.11g-Netzwerken sowie beim Netzwerkbetrieb über Stromkabel verwendet.

Paket: Eine Dateneinheit, die über Netzwerke gesendet wird.

Passphrase: Wird wie ein Passwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Codierschlüssel erstellt werden.

Ping (*Packet INternet Groper*): Internetdienstprogramm, mit dem bestimmt werden kann, ob eine bestimmte IP-Adresse online ist.

POP3 (*Post Office Protocol 3*): Standardprotokoll, das zum Abrufen von E-Mails verwendet wird, die auf einem Mail-Server gespeichert sind.

Port: 1. Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an dem ein Kabel oder ein Adapter angeschlossen wird. 2. Der virtuelle Anschlusspunkt, über den ein Computer auf eine bestimmte Anwendung auf dem Server zugreift.

PPPoE (*Point to Point Protocol over Ethernet*): Eine Art Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

PPTP (*Point-to-Point Tunneling Protocol*): VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art der Breitbandverbindung verwendet.

Präambel: Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

Puffer: Ein Speicherblock, der vorübergehend Daten zur späteren Bearbeitung zurückhält, wenn ein Gerät zum betreffenden Zeitpunkt zu beschäftigt ist, um die Daten zu empfangen.

RJ-45 (*Registered Jack-45*): Ethernet-Anschluss für bis zu acht Drähte.

Roaming: Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne die Verbindung zu unterbrechen.

Router: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden, wie beispielsweise das lokale Netzwerk und das Internet.

RTS (Request To Send): Ein Paket, das gesendet wird, wenn ein Computer über Daten zur Übertragung verfügt. Der Computer wartet den Eingang einer CTS-Mitteilung (*Clear To Send*) ab, bevor die Daten gesendet werden.

Server: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

SMTP (*Simple Mail Transfer Protocol*): Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (*Simple Network Management Protocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

Software: Befehle für den Computer. Eine Folge von Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, wird als "Programm" bezeichnet.

SSID (*Service Set IDentifier*): Der Name Ihres Wireless-Netzwerks.

Standard-Gateway: Ein Gerät, über das der Internetdatenverkehr Ihres LANs weitergeleitet wird.

Statische IP-Adresse: Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

Statisches Routing: Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

Subnetzmaske: Ein Adressencode, der die Größe des Netzwerks festlegt.

Switch: 1. Gerät, das den zentralen Verbindungspunkt für Computer und andere Geräte in einem Netzwerk darstellt, sodass Daten bei voller Übertragungsgeschwindigkeit gemeinsam genutzt werden können. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen.

TCP/IP (*Transmission Control Protocol/Internet Protocol*): Ein Netzwerkprotokoll zum Übertragen von Daten, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

Telnet: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf entfernte Computer.

TFTP (*Trivial File Transfer Protocol*): Eine Version des TCP/IP-FTP-Protokolls, das UDB verwendet und über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

Topologie: Die physische Anordnung eines Netzwerks.

TX-Rate: Übertragungsrate.

UDP (*User Datagram Protocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

URL (*Uniform Resource Locator*): Die Adresse einer sich im Internet befindlichen Datei.

Verschlüsselung: Die Kodierung von Daten, um diese vor einem Zugriff durch nicht autorisierte Dritte zu schützen.

Vollduplex: Die Fähigkeit von Netzwerkgeräten, Daten gleichzeitig empfangen und übertragen zu können.

VPN (*Virtual Private Network*): Sicherheitsmaßnahme zum Schutz von Daten im Internet zwischen dem Verlassen eines Netzwerks und dem Eingehen bei einem anderen.

WAN (*Wide Area Network*): Das Internet.

WEP (*Wired Equivalent Privacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Daten, die in einem Wireless-Netzwerk übertragen werden.

WINIPCFG: Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse für ein bestimmtes Netzwerkbetriebsgerät anzeigt.

WLAN (*Wireless Local Area Network*): Eine Reihe von Computern und Geräten, die über Wireless-Verbindungen miteinander kommunizieren.

Anhang E: Aktualisieren der Firmware

Mit dem ADSL-Gateway können Sie die Firmware des Gateways für LAN (Netzwerk) über die Registerkarte **Verwaltung** des webbasierten Dienstprogramms aktualisieren. Führen Sie die folgenden Schritte aus:

Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Klicken Sie auf die Schaltfläche **Durchsuchen**, um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der Linksys Website heruntergeladen und extrahiert haben.

2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Aktualisieren**, und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung E-1: Firmware aktualisieren

Anhang F: Spezifikationen

Standards	IEEE 802.3u, IEEE 802.3, G.992.1 (G.dmt), G.992.2 (G.lite), ITU G.992.3, ITU G.992.5, ANSI T1.413i2, AG241-E1: Annex-B, AG241-DE: UR-2
Ports	Netzstrom, LINE (ADSL), Ethernet (1-4)
Tasten	Reset-Taste, Ein-/Aus-Taste
Kabeltyp	UTP CAT 5 oder höher, Telefonkabel (analog)
LEDs	Netzstrom, Ethernet (1 bis 4), DSL, Internet
Abmessungen	186 mm x 48 mm x 154 mm
Gewicht	0,36 kg
Stromversorgung	Extern, 12 V GS, 1 A
Zertifizierungen	FCC Teil 15B Klasse B, FCC Teil 68, UL 1950, CE
Betriebstemperatur	0 ºC bis 40 ºC
Lagertemperatur	-20 ºC bis 70 ºC
Luftfeuchtigkeit bei Betrieb	10 % bis 85 %, nicht kondensierend
Luftfeuchtigkeit bei Lagerung	5 % bis 90 %, nicht kondensierend

Anhang G: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Erhöhen Sie den Abstand zwischen der Ausrüstung oder den Geräten.
- Schließen Sie das Gerät an eine anderen Anschluss als den des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

KANADISCHE INDUSTRIEBESTIMMUNGEN

Dieses digitale Gerät der Klasse B erfüllt die kanadischen Bestimmungen der Richtlinie ICES-003.
This Class B digital apparatus complies with Canadian ICES-003
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

EU-KONFORMITÄTSERKLÄRUNG (EUROPA)

In Einklang mit der EWG-Richtlinie 89/336/EWG, der Niederspannungsrichtlinie 73/23/EWG sowie dem Merkblatt zur EU-Richtlinie 93/68/EWG entspricht dieses Produkt den folgenden Standards:

- EN55022 Emission
- EN55024 Immunität

Anhang H: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von zwei Jahren (die "Gewährleistungsfrist") zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigenem Ermessen das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Support von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN SUPPORT WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanadas sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen auf Sie keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGSTHEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss von bzw. keine Beschränkungen auf zufällige oder Folgeschäden; die oben genannte Beschränkung oder der oben genannte Ausschluss findet daher unter Umständen auf Sie keine Anwendung.

Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA.

Anhang I: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits installierte Produkte finden Sie online unter: http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

In Europa	E-Mail-Adresse
Belgien	support.be@linksys.com
Dänemark	support.dk@linksys.com
Deutschland	support.de@linksys.com
Frankreich	support.fr@linksys.com
Großbritannien & Irland	support.uk@linksys.com
Italien	support.it@linksys.com
Niederlande	support.nl@linksys.com
Norwegen	support.no@linksys.com
Österreich	support.at@linksys.com
Portugal	support.pt@linksys.com
Schweden	support.se@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com

Außerhalb von Europa	E-Mail-Adresse
Lateinamerika	support.la@linksys.com
USA und Kanada	support@linksys.com