LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz
802.11g

Wireless-G

ADSL-Gateway Benutzerhandbuch

WIRELESS

Modell-Nr. **WAG54G**

CISCO SYSTEMS

Copyright und Marken

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Gateway ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:

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“.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1: Einführung

Willkommen

Das Wireless-G ADSL-Gateway von Linksys ist die kompakte Lösung für Internetverbindungen. 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. Verbinden Sie vier Computer direkt miteinander, oder hängen Sie weitere Hubs und Switches an, um die Größe des Netzwerks Ihren Bedürfnissen gemäß zu gestalten. Der integrierte Wireless-G Access Point (802.11g) ermöglicht den Anschluss von bis zu 32 Wireless-Geräten an Ihr Netzwerk bei einer herausragenden Geschwindigkeit von 54 MBit/s - ganz ohne Kabelverlegung quer durch das Gebäude. Die Kompatibilität mit Wireless-B-Geräten (802.11b) bei einer Geschwindigkeit von 11 MBit/s ist ebenfalls gegeben. Mit der Router-Funktion des Gateways werden all diese Vorteile vereinigt, so dass das gesamte Netzwerk von der High Speed-Internetverbindung profitieren kann.

Zum Schutz Ihrer Daten und Privatsphäre verfügt das Wireless-G ADSL-Gateway über eine erweiterte Firewall, mit der Eindringlinge und Angriffe über das Internet abgewehrt werden. Wireless-Datenübertragungen werden durch leistungsstarke Datenverschlüsselung geschützt. Die Konfiguration ist mit jedem beliebigen Web-Browser kinderleicht.

Mit dem Wireless-G ADSL-Gateway im Zentrum Ihres Netzwerks sind Sie auf dem besten Weg in die Zukunft.

Der Inhalt dieses Handbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Gateways erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Gateways sowie dieses Benutzerhandbuch beschrieben.
- Kapitel 2: Planen Ihres Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.
- Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.
- Kapitel 4: Anschließen des Wireless-G Broadband-Gateways
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an Ihr 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 einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Gateways erörtert.
- Anhang B: Sicherheit im Wireless-Netzwerkbetrieb
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.
- Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000-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 D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Firmware des Gateways, sollte dies einmal erforderlich sein.
- Anhang E: Aktualisieren der Firmware
  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 F: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang G: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.
- Anhang H: Zulassungsinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.
- Anhang I: Garantieinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.
- Anhang J: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressoucen, darunter der Kundendienst.

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, so dass 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 durch den Internetanschluss eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, falls 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.

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 „Standpunkt“ 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 zugehörige Gerät stets über dieselbe IP-Adresse verfügt, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, wie z. B. Server-Computern oder Druckservern, verwendet.

Abbildung 2-1: Netzwerk

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

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, so dass 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. Standardmäßig ist die DHCP-Serverfunktion des Gateways aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der 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 arbeitet, 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).

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, so dass 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 C: 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 einem Gateway und einem VPN-Gateway 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 C: Konfigurieren von IPSec zwischen einem Windows 2000/XP-Computer und dem VPN-Gateway“.

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?

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 VPN-Client-Software befinden, die IPSec unterstützt.

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 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.

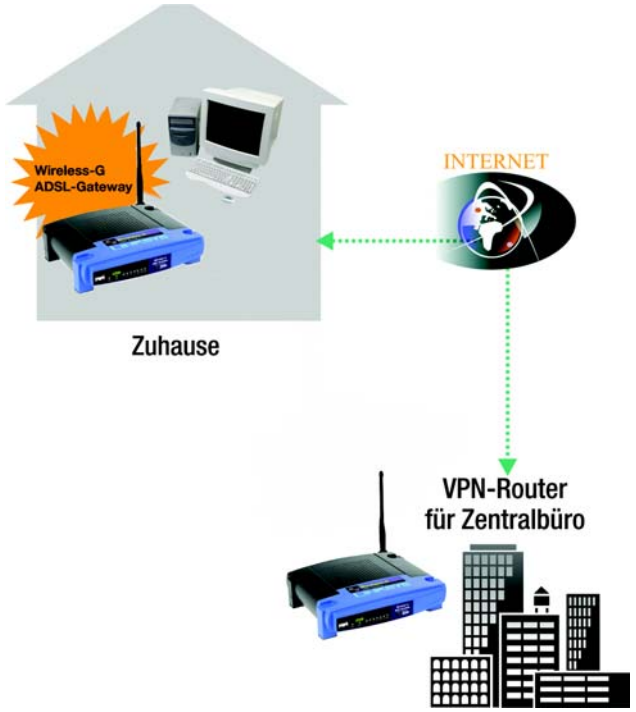

Abbildung 2-3: VPN-Gateway - VPN-Gateway

Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways

Rückseite

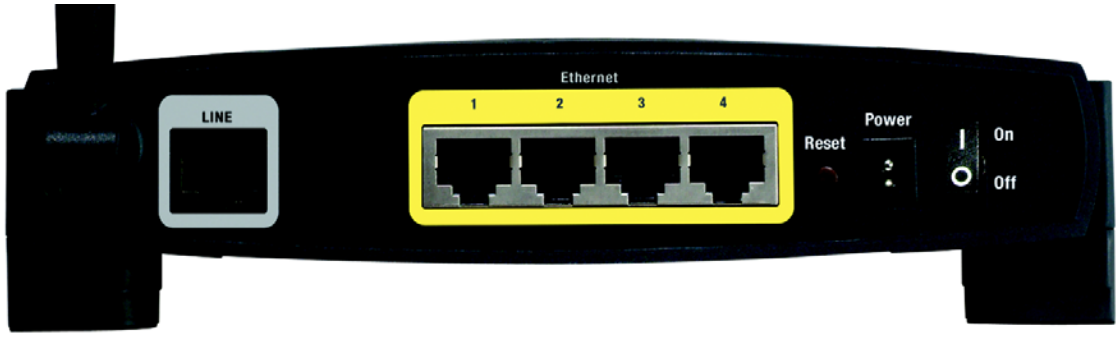

Abbildung 3-1: Rückseite

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.

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

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.

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

Mit diesem Produkt, wie mit vielen anderen 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 an 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.

WLAN Grün. Die **WLAN-**LED leuchtet bei jeder erfolgreichen Wireless-Verbindung auf. Wenn die LED blinkt, sendet oder empfängt das Gateway aktiv Daten über das Netzwerk.

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 Internet-Dienstanbieters (ISP) hergestellt wurde. Die **Internet**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist.

Kapitel 4: Anschließen des Wireless-G Broadband-Gateways

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.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Verdrahtete Verbindung mit einem Computer“ fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Wireless-Verbindung mit einem Computer“ fort.

Verdrahtete 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 1-4 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.

WICHTIG: Wenn Sie Mikrofilter verwenden, schalten Sie diese nur zwischen das Telefon und die Wandbuchse und nicht zwischen das Gateway und die Wandbuchse. Andernfalls schlägt die ADSL-Verbindung fehl.

4. Schließen Sie ein Ende des Telefonkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an die Wandbuchse der ADSL-Leitung an. Benutzer von Annex A sollten jeweils einen Mikrofilter zwischen Telefon und Wandbuchse verwenden, um Störungen zu vermeiden. Benutzer von Annex B (ADSL über ISDN) sollten ggf. Splitter verwenden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.
5. Schließen Sie den Netzstromadapter an den Stromanschluss 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.

Abbildung 4-1: Ethernet-Verbindung

Abbildung 4-2: ADSL-Verbindung

Wireless-Verbindung mit einem Computer

Befolgen Sie diese Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

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

HINWEIS: Schließen Sie das Netzgerät des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

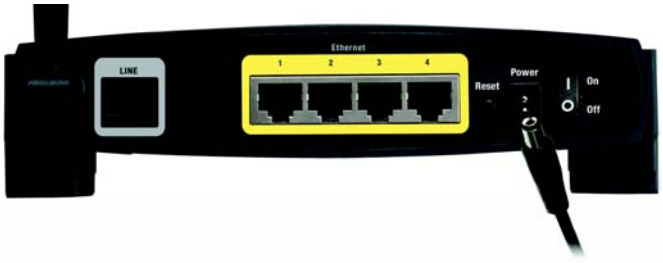

Abbildung 4-3: Netzstromverbindung

WICHTIG: Wenn Sie Mikrofilter verwenden, schalten Sie diese nur zwischen das Telefon und die Wandbuchse und nicht zwischen das Gateway und die Wandbuchse. Andernfalls schlägt die ADSL-Verbindung fehl.

2. Schließen Sie ein Ende des Telefonkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an die Wandbuchse der ADSL-Leitung an. Ein sogenannter Mikrofilter muss u. U. zwischen Telefon und Wandbuchse geschaltet werden, um Störungen zu vermeiden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.
3. Schließen Sie den Netzstromadapter an den Stromanschluss 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 Netz-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“.
4. Schalten Sie einen der Computer in Ihrem Wireless-Netzwerk ein.
5. Stellen Sie für den erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters des Computers auf **linksys** (die Standardeinstellung des Gateways) eingestellt ist und dass die WEP-Verschlüsselung deaktiviert ist. Wenn Sie auf das Gateway zugegriffen haben, können Sie die Einstellungen des Gateways und des Adapters von diesem Computer Ihren üblichen Netzwerkeinstellungen anpassen.

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

Die Installation der Gateway-Hardware ist jetzt abgeschlossen.

Fahren Sie mit „Kapitel 5: Konfigurieren des Gateways“ fort.

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 wird jede Webseite des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können über Ihren Web-Browser mithilfe eines an das Gateway angeschlossenen Computers auf das Dienstprogramm zugreifen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

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

Es stehen sieben Hauptregisterkarten zur Verfügung: **Setup** (Einrichtung), **Wireless** (Wireless), **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen und Spiele), **Administration** (Verwaltung) und **Status** (Status). Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

Setup (Einrichtung)

- **Basic Setup** (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.
- **Advanced Routing** (Erweitertes Routing): Sie können in diesem Fenster die Konfigurationseinstellungen für dynamisches und statisches Routing ändern.

Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): Sie können in diesem Fenster den Wireless-Netzwerkmodus und die Wireless-Sicherheitseinstellungen auswählen.
- **Wireless Network Access** (Wireless-Netzwerkzugriff): In diesem Fenster ist die Zugriffsliste für das Wireless-Netzwerk aufgeführt.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Sie können über dieses Fenster auf die erweiterten Wireless-Funktionen zugreifen.

Security (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 im Abschnitt „Windows-Hilfe“ in Anhang D.

Hinweis: Für zusätzliche Sicherheit sollten Sie das Kennwort über die Registerkarte **Administration** (Verwaltung) ändern.

Access Restrictions (Zugriffsbeschränkungen)

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

Applications & Gaming (Anwendungen und Spiele)

- **Single Port Forwarding** (Einfaches Port-Forwarding): Verwenden Sie dieses Fenster, um die gängigsten Dienste und Anwendungen auf Ihrem Netzwerk einzurichten.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): Klicken Sie auf diese Registerkarte, um öffentliche Dienste oder weitere spezielle Internet-Anwendungen auf Ihrem Netzwerk einzurichten.
- **Port Triggering** (Port-Triggering): Klicken Sie auf diese Registerkarte, um für Internet-Anwendungen die Bereiche für Port-Triggering und Port-Forwarding festzulegen.
- **DMZ**: Verwenden Sie dieses Fenster, um für einen Benutzer die Internetverbindung zur Verwendung von speziellen Diensten einzurichten.

Administration (Verwaltung)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie Zugriffsrechte für das Gateway sowie SNMP- und UPnP-Einstellungen ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): Verwenden Sie dieses Fenster, um einen Ping-Test durchzuführen.
- **Factory Defaults** (Werkseinstellungen): Verwenden Sie dieses Fenster, wenn Sie das Gateway of die Werkseinstellungen zurücksetzen möchten.
- **Firmware Upgrade** (Aktualisieren der Firmware): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.

Status (Status)

- **Gateway** (Gateway-Adresse): In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des drahtlosen Netzwerks aufgeführt.
- **DSL Connection** (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 Kennworts 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 dann auf **OK**.

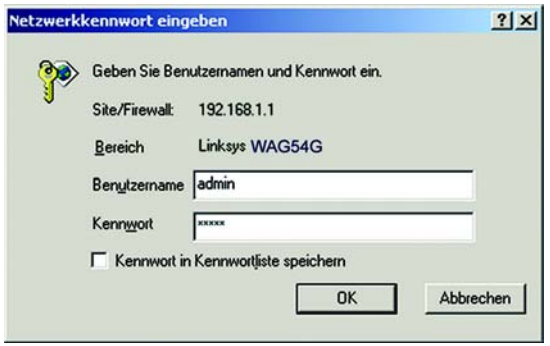

Abbildung 5-1: Fenster zur Kennworteingabe

Die Registerkarte „Setup“ (Einrichtung)

Die Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten dargestellten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt (siehe Abbildung 5-2). Über diese Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Internet Setup (Internet-Einrichtung)

- **VC Settings** (VC-Einstellungen - **Virtual Circuit** Virtueller Kreis): Für diese Option sind zwei Einstellungen erforderlich, **VPI** (*Virtual Path Identifier;* Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier;* Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP. **Multiplexing** (Multiplexing): Wählen Sie entsprechend dem verwendeten ISPs für diese Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
- **ADSL Settings** (ADSL-Einstellungen): Das Gateway unterstützt fünf Kapselungstypen: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA und Bridged Mode Only. Das jeweilige Fenster **Basic Setup** (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

RFC 1483 Bridged (RFC 1483-Überbrückung)

Dynamic IP (Dynamische IP-Adresse)

IP Settings (IP-Einstellungen): Wählen Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISPs die Verbindung über eine dynamische IP-Adresse herstellen (siehe Abbildung 5-3).

Abbildung 5-2: Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Static IP (Statische IP-Adresse)

Wenn Sie für die Internetverbindung eine permanente IP-Adresse verwenden, wählen Sie **Use the following IP Address** (Folgende IP-Adresse verwenden) aus (siehe Abbildung 5-4).

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

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

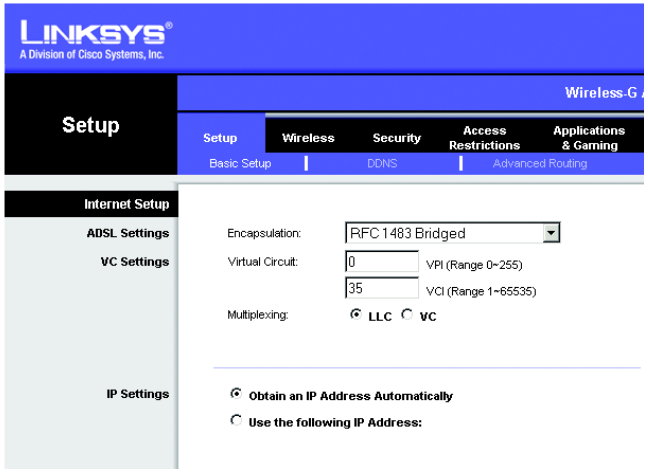

Abbildung 5-3: Dynamic IP (Dynamische IP-Adresse)

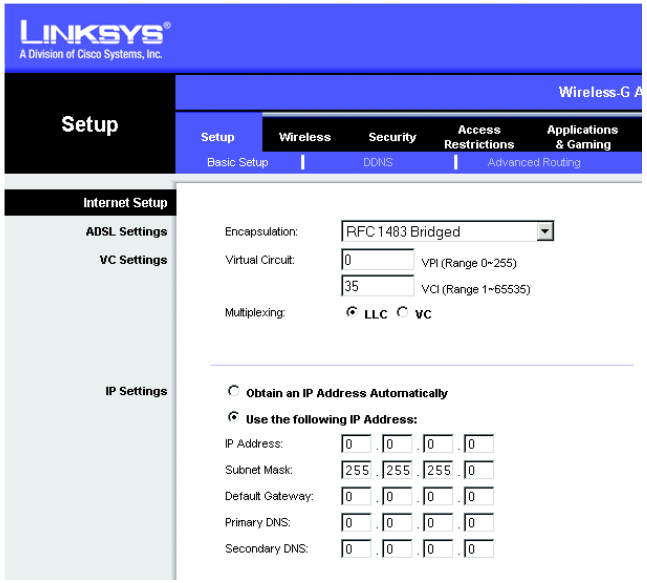

Abbildung 5-4: Static IP (Statische IP-Adresse)

RFC 1483 Routed (RFC 1483-Weiterleitung)

Wählen Sie zur Verwendung des Modus „RFC 1483 Routed“ die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus (siehe Abbildung 5-5).

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

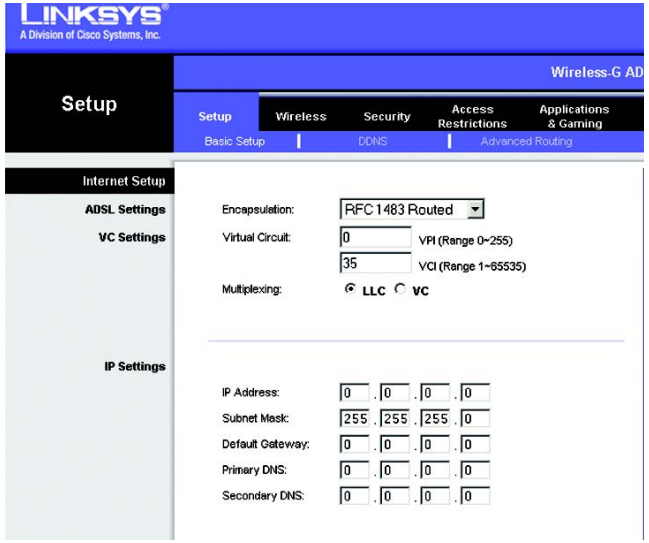

Abbildung 5-5: RFC 1483 Routed (RFC 1483-Weiterleitung)

RFC 2516 PPPoE (RFC 2516 PPP over Ethernet)

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, wählen Sie die Option **PPPoE** aus (siehe Abbildung 5-6).

- **Service Name** (Dienstname): Geben Sie den Dienstnamen ein, wenn dies für Ihren IP erforderlich ist.
- **User Name** (Benutzername) und **Password** (Kennwort): Geben Sie den Benutzernamen und das Kennwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (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 **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Connect on Demand** (Bei Bedarf verbinden) zu aktivieren. Geben Sie im Feld **Max Idle Time** (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (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. Klicken Sie zur Verwendung dieser Option auf die Optionsschaltfläche neben **Keep Alive** (Verbindung aufrechterhalten). Im Feld **Redial Period** (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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

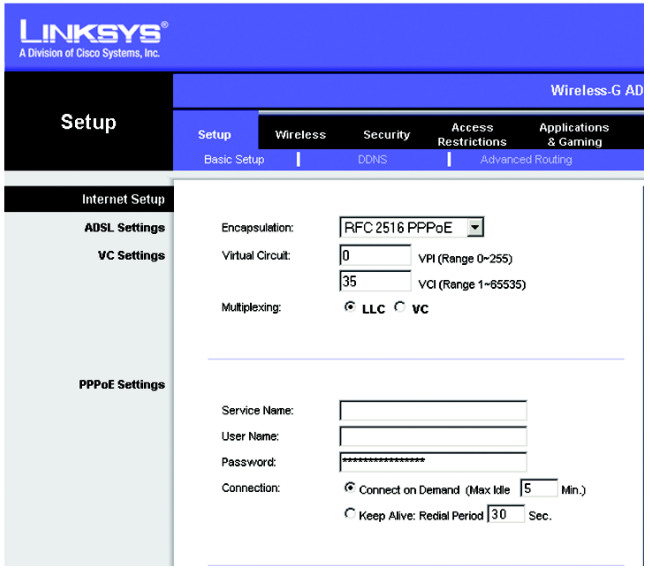

Abbildung 5-6: RFC 2516 PPPP over Ethernet

RFC 2364 PPPoA (RFC 2364 PPP over ATM)

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, wählen Sie die Option **PPPoA** aus (siehe Abbildung 5-7).

- **User Name** (Benutzername) und **Password** (Kennwort): Geben Sie den Benutzernamen und das Kennwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (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 **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Connect on Demand** (Bei Bedarf verbinden) zu aktivieren. Geben Sie im Feld **Max Idle Time** (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (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. Klicken Sie zur Verwendung dieser Option auf die Optionsschaltfläche neben **Keep Alive** (Verbindung aufrechterhalten). Im Feld **Redial Period** (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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

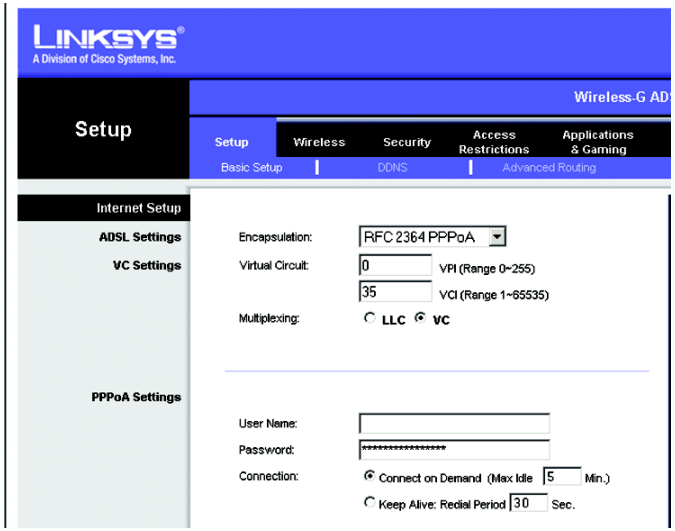

Abbildung 5-7: RFC 2364 PPP over ATM

Bridged Mode Only (Nur Überbrückungsmodus):

Wenn Sie Ihr Gateway als Überbrückung verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Bridged Mode Only** (Nur Überbrückungsmodus) aus (siehe Abbildung 5-8). 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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

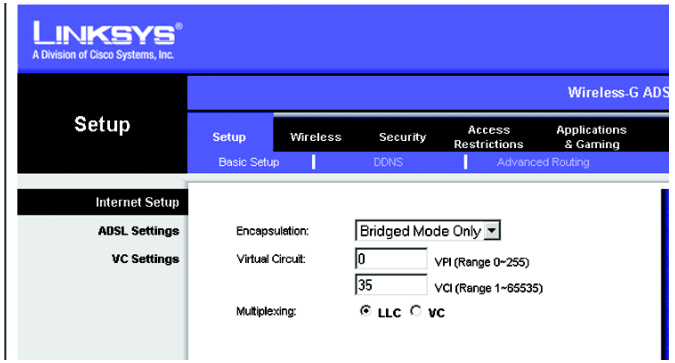

Abbildung 5-8: Bridged Mode Only (Nur Überbrückungsmodus)

Optional Settings (Required by some ISPs) (Zusätzliche Einstellungen, für einige ISPs erforderlich) (siehe Abbildung 5-9)

- **Host Name/Domain Name** (Hostname/Domänenname): In diese Felder können Sie einen Hostnamen bzw. Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Wenden Sie sich an Ihren ISP, um zu ermitteln, ob Ihr Broadband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU:** Durch die MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie die Option **Manual** (Manuell) aus, und geben Sie den gewünschten Wert ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

Network Setup (Netzwerkeinrichtung)

- **Router IP** (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.
  - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist 192.168.1.1.
  - **Subnet Mask** (Subnetzmaske): Der Standardwert ist 255.255.255.0.
- **Network Address Server Settings (DHCP)** [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.
  - **Local DHCP Server** (Lokaler DHCP-Server): Die DHCP-Option ist standardmäßig aktiviert. Wenn auf Ihrem Netzwerk bereits ein DHCP-Server vorhanden ist, legen Sie für die DHCP-Option des Gateways **Disable** (Deaktivieren) fest.
  - **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.12 betragen, da die Standard-IP-Adresse für das Gateway 192.168.1.1 ist.
  - **Number of Address** (Adressenanzahl): Geben Sie die maximale Anzahl der PCs ein, denen der DHCP-Server IP-Adressen zuweisen soll. Diese Zahl darf nicht größer als 253 sein. Der Standardbereich liegt zwischen 192.168.1.100 und 192.168.1.149 (siehe Abbildung 5-9).
  - **DHCP Address Range** (DHCP-Adressenbereich): Der Bereich der DHCP-Adressen ist hier aufgeführt.
  - **Client Lease Time** (Client-Leasedauer): Geben Sie in dieses Feld die Minutenanzahl ein.
- **Time Setting** (Zeiteinstellung): Mit dieser Option legen Sie die Zeitzone für Ihr Gateway fest.

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

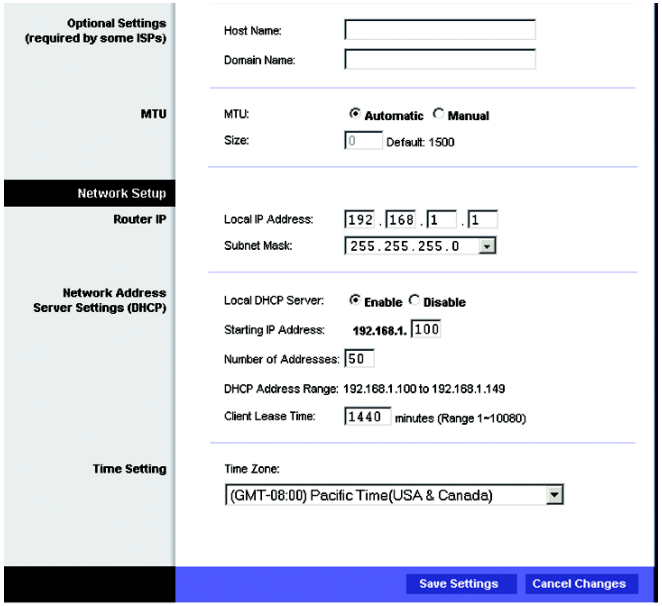

Abbildung 5-9: Optional Settings (Optionale Einstellungen)

Die 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 Service (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 **Disabled** (Deaktivieren) aus.

DynDNS.org

- **User Name** (Benutzername), **Password** (Kennwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Kennwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet IP Address** (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**: Der Status der Verbindung zum DDNS-Dienst ist hier aufgeführt.

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

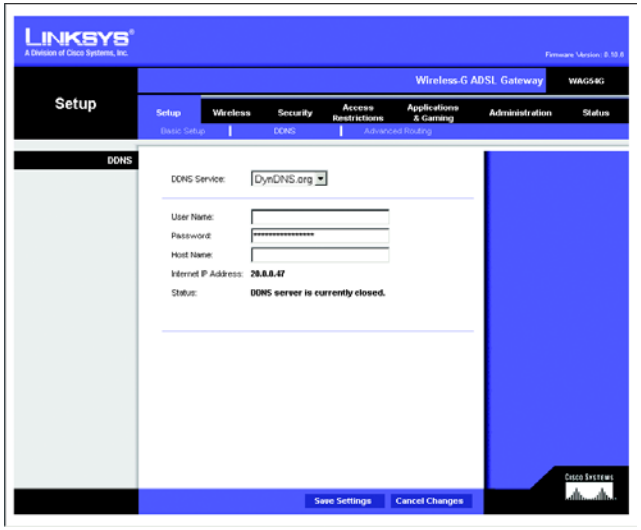

Abbildung 5-10: DynDNS.org

Die Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster **Advanced Routing** (Erweitertes Routing) können Sie die Einstellungen für dynamisches und statisches Routing konfigurieren (siehe Abbildung 5-11).

Advanced Routing (Erweitertes Routing):

- **Dynamic Routing** (Dynamisches Routing): Mithilfe der Option **Dynamic Routing** (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-Information an andere Gateways im Netzwerk. Klicken Sie zum Aktivieren des RIP-Protokolls auf **Enabled** (Aktiviert). Klicken Sie zum Deaktivieren des RIP-Protokolls auf **Disabled** (Deaktiviert).
- **Receive RIP Version** (RIP-Version empfangen): Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**. Wenn Sie keine RIP-Nachrichten empfangen möchten, wählen Sie **None** (Keine).
- **Transmit RIP Version** (RIP-Version übertragen): Wählen Sie zum Übertragen von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1, RIP1-Compatible** (RIP1-kompatibel) oder **RIP2**. Wenn Sie keine RIP-Nachrichten übertragen möchten, wählen Sie **None** (Keine).

Static Routing (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:

- **Select Entry** (Eintrag 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 **Delete Entry** (Eintrag löschen).
- **Destination IP Address** (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.
- **Subnet Mask** (Subnetzmaske): Mithilfe der Subnetzmaske (auch Netzwerkmaske genannt) wird festgelegt, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.
- **Gateway** (Gateway-Adresse): 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.
- **Hop Count** (Routeranzahl): Hiermit wird die maximale Anzahl von Schritten zwischen den Netzwerkknoten festgelegt, die die Datenpakete passieren. Ein Knoten ist jeder Router im Pfad zum entfernten Netzwerk.

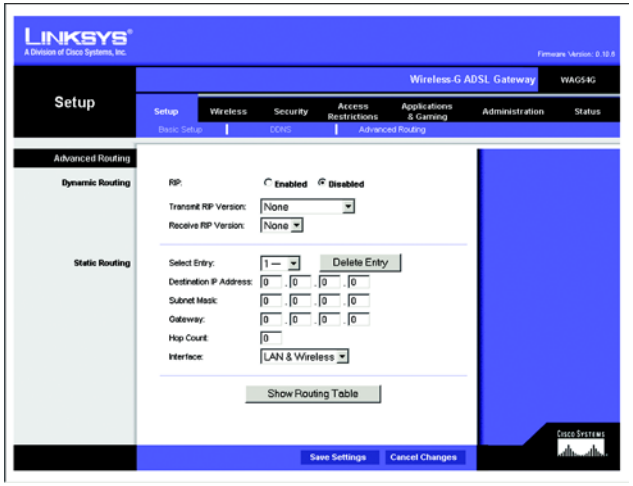

Abbildung 5-11: Advanced Routing (Erweitertes Routing)

- **Interface** (Schnittstelle): Wählen Sie hierfür die Option **LAN**, **Wireless** oder **Internet** entsprechend der Position des Endziels der statischen Route aus.
- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um dadurch ein Fenster anzuzeigen, in dem die durch ihr LAN übertragenen Daten aufgeführt sind (siehe Abbildung 5-12). Für jede Route wird die Ziel-IP-Adresse, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren.

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

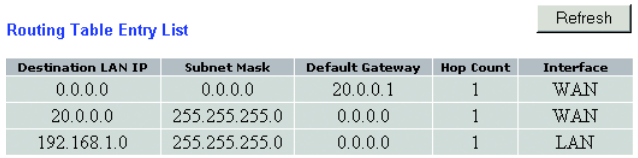

Abbildung 5-12: Routing Table (Routing-Tabelle)

Die Registerkarte „Wireless“

Die Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)
(siehe Abbildung 5-13)

Mithilfe dieses Fensters können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.

Wireless Network (Wireless-Netzwerk)

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **802.11g** aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **802.11b** aus. Um das drahtlose Netzwerk zu deaktivieren, wählen Sie **Disable** (Deaktivieren).
- **Wireless Network Name (SSID)** [Wireless-Netzwerk-Name (SSID)]: Geben Sie in dieses Feld den Namen für Ihr Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerk-Namen, der von allen Geräten im drahtlosen Netzwerk verwendet wird. Die SSID muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird in Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.
- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Hierbei handelt es sich um einen Wert zwischen 1 und 11 (für Nordamerika). Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Clients von Linksys erkennen automatisch den Wireless-Kanal des Gateways.
- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Clients im lokalen Netzwerk nach einer Verbindung zu Wireless-Netzwerken suchen, erkennen sie die Übertragung der SSID über den Router. Zur Übertragung der SSID des Routers behalten Sie die Standardeinstellung **Enabled** (Aktiviert) bei. Wenn Sie die SSID des Routers nicht übertragen möchten, wählen Sie **Disabled** (Deaktiviert) aus.

Abbildung 5-13: Wireless Network Mode (Wireless-Netzwerkmodus)

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

Die Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit Ihres Wireless-Netzwerks konfiguriert. Vom Router werden vier Wireless-Sicherheitsoptionen unterstützt: **WPA Pre-Shared Key** (WPA Vorläufiger gemeinsamer Schlüssel), **WPA RADIUS**, **RADIUS** und **WEP**. (WPA steht für *Wi-Fi Protected Access*; dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung. WEP steht für *Wired Equivalent Privacy* und RADIUS für *Remote Authentication Dial-In User Service*.) Im Folgenden erhalten Sie einen Überblick über diese vier Sicherheitsstandards. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Routers erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.

WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel): Bei WPA steht Ihnen die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln zur Verfügung. Wählen Sie den Algorithmus **TKIP** aus: Geben Sie einen gemeinsamen WPA-Schlüssel mit einer Länge von 8 bis 32 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Router mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind (siehe Abbildung 5-14).

Abbildung 5-14: WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel)

WPA/RADIUS: Bei dieser Option wird WPA in Kombination mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit dem Router verbunden ist.) Wählen Sie zuerst den gewünschten WPA-Algorithmus aus (**TKIP**). Geben Sie die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch den Router und den Server freigegeben ist. Legen Sie zuletzt den Wert **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Router mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind (siehe Abbildung 5-15).

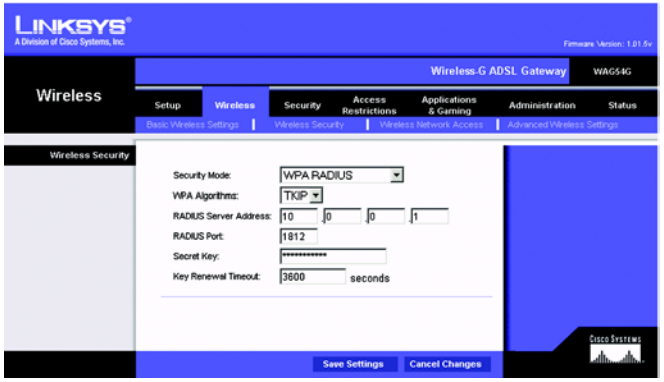

Abbildung 5-15: WPA RADIUS

RADIUS: Bei dieser Option wird WEP in Kombination mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit dem Router verbunden ist.) Geben Sie zuerst die IP-Adresse des RADIUS-Servers in das Feld **RADIUS Server Address** (Adresse des RADIUS-Servers) und die Portnummer in das Feld **RADIUS Port** (RADIUS-Port) sowie den Schlüssel in das Feld **Shared Key** (Freigegebener Schlüssel) ein, der für die Verwendung durch den Router und den Server freigegeben ist. Wählen Sie anschließend als WEP-Verschlüsselungsebene **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) und den Wert für **Default Key** (Standard-Schlüssel) (wählen Sie den gewünschten Schlüssel aus) aus. Erstellen Sie zuletzt einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben (siehe Abbildung 5-16).

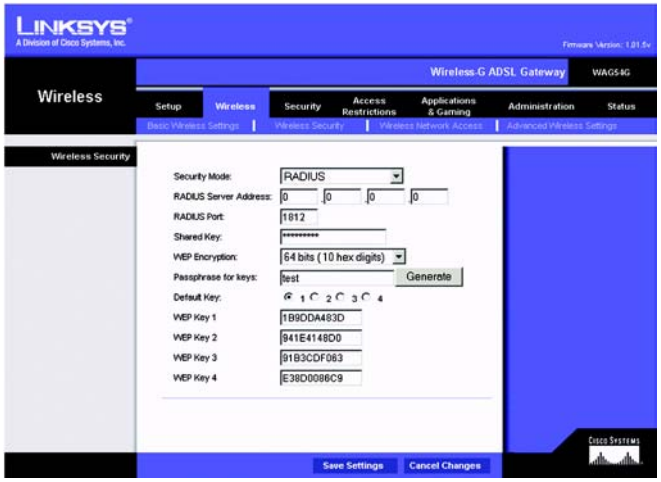

Abbildung 5-16: RADIUS

WEP: WEP ist eine grundlegende Verschlüsselungsmethode, die nicht so sicher wie WPA ist. Um WEP zu verwenden, wählen Sie einen Wert für **Default Key** (Standard-Schlüssel) (wählen Sie den gewünschten Schlüssel aus) sowie als WEP-Verschlüsselungsebene **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) aus. Erstellen Sie anschließend einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben (siehe Abbildung 5-17).

- Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen anzuwenden, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Routers erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.
- **WEP Encryption Level** (WEP-Verschlüsselungsebene): WEP ist die Abkürzung für *Wired Equivalent Privacy.* Hierbei handelt es sich um eine Verschlüsselungsmethode zum Schutz der Wireless-Datenkommunikation. WEP basiert auf einem 64-Bit oder 128-Bit-Schlüssel zur Steuerung des Zugriffs auf Ihr Netzwerk und zur höheren Sicherheit durch Verschlüsselung der Datenübertragung. Um übertragene Daten zu entschlüsseln, müssen alle Geräte im Netzwerk den gleichen WEP-Schlüssel verwenden. Höhere Verschlüsselungsebenen bieten eine höhere Sicherheitsstufe, durch die Komplexität der Verschlüsselung kann jedoch die Netzwerkleistung vermindert werden. Um WEP zu aktivieren, wählen Sie **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) (siehe Abbildung 5-13) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) (siehe Abbildung 5-14) aus.
- **Passphrase for keys** (Schlüssel-Passphrase): Sie können anstelle der manuellen Eingabe von WEP-Schlüssels eine Passphrase eingeben. Mit dieser Passphrase können Sie mindestens einen WEP-Schlüssel erstellen. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Diese Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Um mit Wireless-Produkten anderer Hersteller oder mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung zu kommunizieren, notieren Sie sich den im Feld **WEP Key 1** (Schlüssel 1) generierten WEP-Schlüssel und geben ihn manuell in den Wireless-Client ein.) Klicken Sie nach Eingabe der Passphrase auf **Generate** (Generieren), um WEP-Schlüssel zu erstellen.
- **Default Key** (Standard-Schlüssel): Legen Sie fest, welcher WEP-Schlüssel (1 bis 4) verwendet werden soll, wenn Daten über das Gateway übertragen werden. Stellen Sie sicher, dass das Empfangsgerät (Wireless-Client) den gleichen Schlüssel verwendet.
- **WEP Keys 1-4** (WEP-Schlüssel 1 - 4): Mithilfe von WEP-Schlüsseln können Sie ein Verschlüsselungsschema für Übertragungen im Wireless-Netzwerk erstellen. Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie ein Schlüsselfeld nicht leer, und geben Sie nicht in alle Schlüsselfelder den Wert 0 ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie eine 64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 hexadezimale Zeichen betragen. Wenn Sie eine 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zeichen von 0 bis 9 und von A bis F.

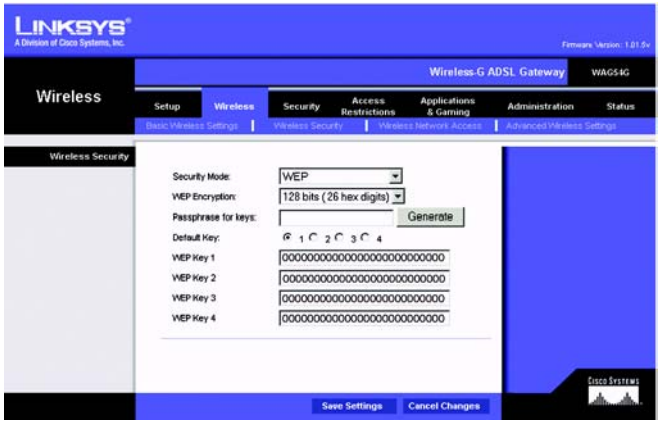

Abbildung 5-17: WEP

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

Wireless Netzwork Access (Wireless-Netzwerkzugriff) (siehe Abbildung 5-18)

Wireless Network Access (Wireless-Netzwerkzugriff): Wenn Sie die Option **Allow All** (Alle zulassen) auswählen, haben alle Computer Zugriff auf das Wireless-Netzwerk. Wählen Sie die Option **Restrict Access** (Zugriff beschränken) aus, um den Zugriff auf das Netzwerk zu beschränken. Klicken Sie auf die Schaltfläche **Select MAC Address From Networked Computers** (MAC-Adresse von Netzwerk-PCs auswählen), um das in Abbildung 5-19 aufgeführte Fenster anzuzeigen.

Wählen Sie aus der Liste den Eintrag **MAC Address** (MAC-Adresse) aus, aktivieren Sie das Kontrollkästchen **Select** (Auswahl), und klicken Sie auf die Schaltfläche **Select** (Auswahl).

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster zurückzukehren.

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

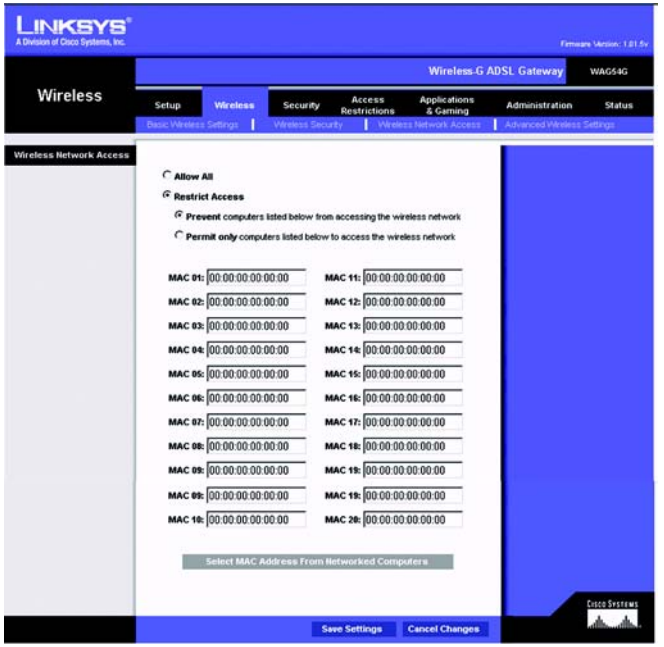

Abbildung 5-18: Wireless Network Access (Wireless-Netzwerkzugriff)

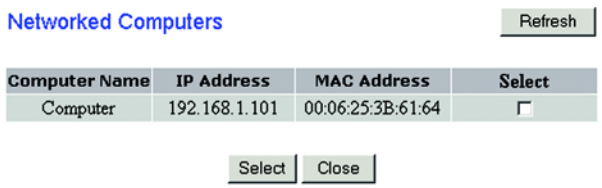

Abbildung 5-19: Networked Computers (Netzwerk-Computer)

Die Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)
(siehe Abbildung 5-20)

Sie können über dieses Fenster auf die folgenden erweiterten Wireless-Funktionen zugreifen: **Authentication Type** (Authentifizierungstyp), **Basic Data Rates** (Basis-Datenrate), **Control Tx Rates** (Gesteuerte Übertragungsraten), **Beacon Interval** (Beacon-Intervall), **DTIM Interval** (DTIM-Intervall), **RTS Threshold** (RTS-Schwelle) und **Fragmentation Threshold** (Fragmentierungsschwelle).

- **Control Tx Rates** (Gesteuerte Übertragungsraten): Die Standardübertragungsrate ist auf **Auto** (Automatisch) festgelegt. Der Bereich liegt zwischen 1 und 54 MBit/s. Die Datenübertragungsrate sollte gemäß der Geschwindigkeit des Wireless-Netzwerks eingestellt werden. Sie können aus einer Reihe von Übertragungsgeschwindigkeiten auswählen oder die standardmäßig eingestellte Option **Auto** (Automatisch) beibehalten, mit der das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt.
- **Beacon Interval** (Beacon-Intervall): Der Standardwert ist 100. Geben Sie einen Wert zwischen 1 und 65.535 Millisekunden ein. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.
- **DTIM Interval** (DTIM-Intervall): Der Standardwert ist 3. Der Wert (zwischen 1 und 255) gibt das Intervall der DTIM (*Delivery Traffic Indication Message*) an. Ein DTIM-Feld ist ein Zeitkontrollfeld, das die Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet er die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit.
- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert sollte bei dem Standardwert von 2346 belassen werden. Der Bereich liegt bei 256 bis 2346 Byte. Er gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Wenn die Fragmentierungsschwelle zu niedrig liegt, kann dies zu einer Verringerung der Netzwerkleistung führen. Es wird nur eine geringfügige Senkung dieses Werts empfohlen.
- **RTS Threshold** (RTS-Schwelle): Dieser Wert sollte bei dem Standardwert von 2347 belassen werden. Der Bereich liegt bei 0 bis 2347 Byte. Bei einem schwankenden Datenfluss wird eine nur geringfügige Senkung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*RTS = Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Daten-Blocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*CTS = Clear to Send*), um das Recht, mit der Übertragung zu beginnen, anzuerkennen.
- **Authentication Type** (Authentifizierungstyp): Standardmäßig ist die Option **Auto** (Automatisch, Standard) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Freigegebener Schlüssel) verwendet werden kann. Beim Authentifizierungstyp **Open System** (Offenes System) verwenden Absender und Empfänger zur Authentifizierung keinen WEP-Schlüssel, sondern WEP zur Datenverschlüsslung. Wenn Sie nur den Open System-Authentifizierungstyps verwenden möchten, wählen Sie die Option **Open System** (Offenes System) aus. Beim Authentifizierungstyp **Shared Key** (Freigegebener Schlüssel) verwenden Absender und Empfänger sowohl zur Authentifizierung als auch zur Datenverschlüsselung einen WEP-Schlüssel. Wenn Sie nur den Shared Key-Authentifizierungstyp verwenden möchten, wählen Sie die Option **Shared Key** (Freigegebener Schlüssel) aus. Es wird empfohlen, diese Option auf dem Standardmodus **Auto** (Automatisch) zu belassen, da einige Clients nicht für die Option **Shared Key** (Freigegebener Schlüssel) konfiguriert werden können.

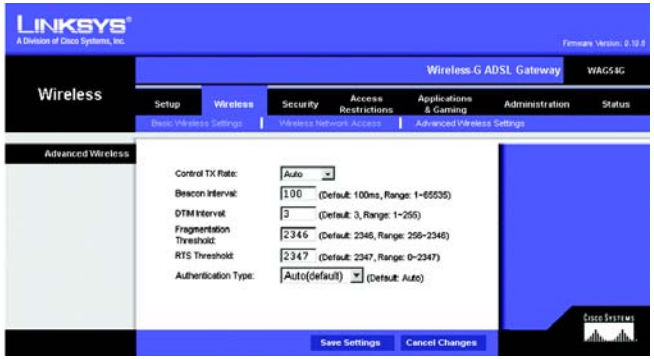

Abbildung 5-20: Advanced Wireless Settings (Erweiterte Wireless-Einstellungen)

Die Registerkarte „Security“ (Sicherheit)

Firewall

Wenn Sie auf die Registerkarte „Security“ (Sicherheit) klicken, wird das Fenster **Firewall** angezeigt (siehe Abbildung 5-21). 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.

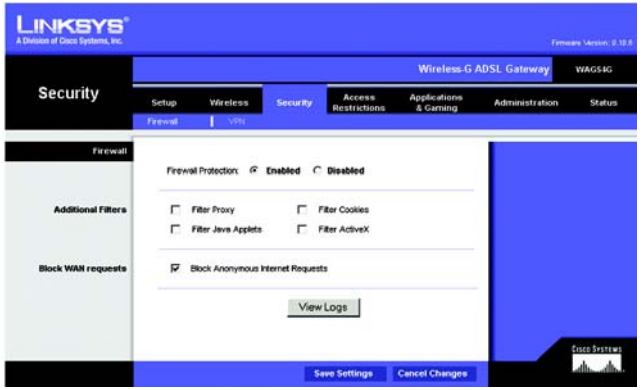

Abbildung 5-21: Firewall

- **Firewall** (Firewall): Klicken Sie zum Hinzufügen des Firewall-Schutzes auf **Enabled** (Aktiviert). Klicken Sie zum deaktivieren des Firewall-Schutzes auf **Disabled** (Deaktiviert).

  Additional Filters (Zusätzliche Filter)

- **Filter Proxy** (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 **Enabled** (Aktiviert).
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Internetsites beim Zugriff auf diese Sites verwendet werden. Um die Cookie-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, haben Sie möglicherweise keinen Zugriff auf Internetsites, die mit dieser Programmiersprache erstellt wurden. Um die Java Applet-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, haben Sie möglicherweise keinen Zugriff auf Internetsites, die mit dieser Programmiersprache erstellt wurden. Um die ActiveX-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).

  Block WAN Requests (WAN-Anfragen blockieren)

- **Block Anonymous Internet Requests** (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 **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen), um Protokolle von Firewall-Ereignissen anzuzeigen.

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

VPN (*Virtual Private Networking*)

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten erstellt wird. Über das in Abbildung 5-22 aufgeführte Fenster können Sie Ihre VPN-Einstellungen konfigurieren, um dadurch die Sicherheit Ihres Netzwerks zu erhöhen.

VPN Passthrough (VPN-Passthrough)

- **IPSec 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 **Enabled** (Aktiviert). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).
- **PPTP Passthrough** (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 **Enabled** (Aktiviert). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).

IPSec VPN Tunnel (IPSec VPN-Tunnel)

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

- Um den Tunnel festzulegen, wählen Sie den Tunnel, den Sie erstellen möchten, aus der Dropdown-Liste **Select Tunnel Entry** (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 **Tunnel Name** (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.
- **Local Secure Group** (Lokale sichere Gruppe) und **Remote Secure Group** (Entfernte sichere Gruppe): Die **Local Secure Group** (Lokale sichere Gruppe) umfasst die Computer in Ihrem LAN, die auf den Tunnel zugreifen können. Die **Remote Secure Group** (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.
- **Remote Security Gateway** (Entferntes Sicherheits-Gateway): Bei dem **Remote Security Gateway** (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 **Any** (Alle) auswählen, kann mit jeder IP-Adresse auf den Tunnel zugegriffen werden.

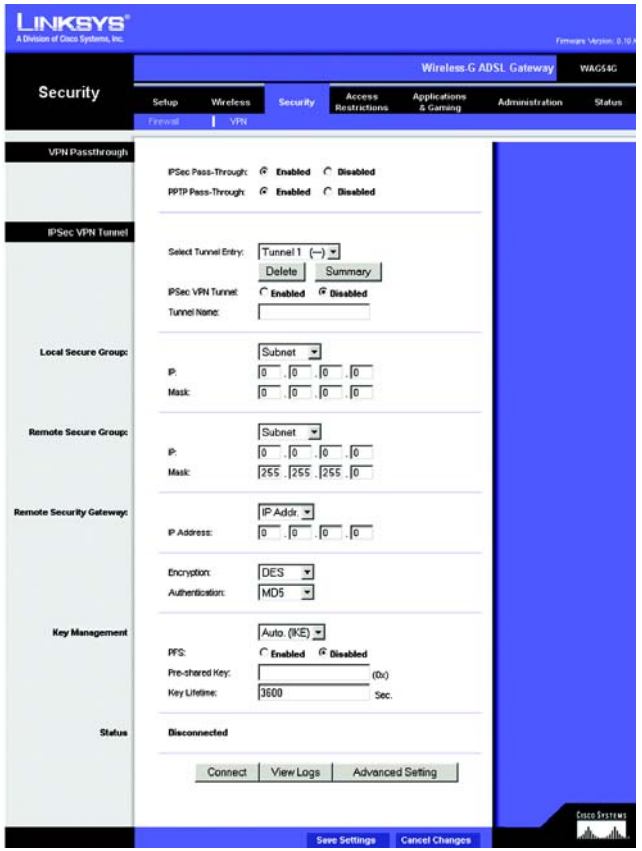

Abbildung 5-22: VPN

- **Encryption** (Verschlüsselung): Mit **Encryption** (Verschlüsselung) machen Sie die Verbindung noch sicherer. Es stehen zwei Verschlüsselungstypen zur Verfügung: DES und 3DES (empfohlen wird 3DES, weil 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 **Disable** (Deaktivieren) auswählen. In Abbildung 5-22 wurde DES ausgewählt (Standardeinstellung).
- **Authentication** (Authentifizierung): Die Authentifizierung wirkt wie eine weitere Sicherheitsstufe. Es stehen zwei Authentifizierungstypen zur Verfügung: MD5 und SHA (empfohlen wird **SHA**, weil 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. In Abbildung 5-22 wurde MD5 gewählt (Standardeinstellung).
- **Key Management** (Schlüsselverwaltung): Wählen Sie aus dem Dropdown-Menü **Auto (IKE)** oder **Manual** (Manuell) aus. Beide 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 **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, so dass 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.

  Manual (Manuell): (siehe Abbildung 5-23)
  Wählen Sie **Manual** (Manuell) aus, und wählen Sie anschließend den Verschlüsselungsalgorithmus aus der Dropdown-Liste aus. Geben Sie den Verschlüsselungsschlüssel 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 der Dropdown-Liste 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 **Connect** (Verbinden), um Ihren VPN-Tunnel zu verbinden. Klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen), um Protokolle anzuzeigen. Klicken Sie auf die Schaltfläche **Advanced Setting** (Weitere Einstellungen), um das Fenster **Advanced IPSec VPN Tunnel Setup** (Erweiterte IPSec VPN-Tunnel-Einrichtung) anzuzeigen (siehe Abbildung 5-24).

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

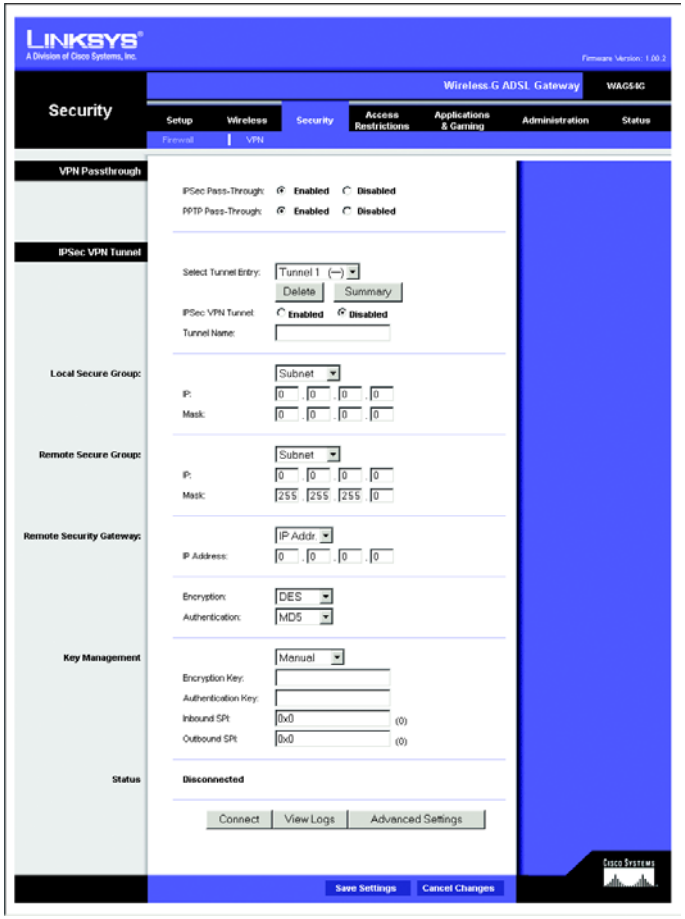

Abbildung 5-23: Manual Key Management (Manuelle Schlüsselverwaltung)

Advanced VPN Tunnel Setup (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Sie können über das in Abbildung 5-24 dargestellte Fenster **Advanced IPSec VPN Tunnel Setup** (Erweiterte IPSec VPN-Tunnel-Einrichtung) die Einstellungen für bestimmte VPN-Tunnel anpassen.

Phase 1

- **Phase 1** wird zur Erstellung einer Sicherheitsverknüpfung, auch „IKE SA“ (*Internet Key Exchange, Security Assosication*) genannt, verwendet. Nach Abschluss von Phase 1 wird in Phase 2 mindestens eine „IPSec SA“ erstellt und für IPSec-Sitzungen verwendet.
- **Operation Mode** (Betriebsmodus): Die beiden verfügbaren Betriebsmodi **Main** (Hauptmodus) und **Aggressive** (Aggressiver Modus) tauschen die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen aus. 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. Wählen Sie **Username** (Benutzername), und geben Sie den Benutzername ein.
- **Encryption** (Verschlüsselung): Wählen Sie die Länge des Schlüssels aus, der zum Verschlüsseln/Entschlüsseln von ESP-Paketen verwendet wird. Sie können zwischen zwei Verschlüsselungsarten wählen: DES und 3DES.Die Verwendung von 3DES wird empfohlen, da diese Verschlüsselungsart sicherer ist.
- **Authentication** (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.
- **Group** (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.
- **Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie optional einen Zeitraum festlegen, wie lange der Schlüssel verfügbar ist, bevor ein abläuft. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, so dass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Phase 2

- **Encryption** (Verschlüsselung): Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.
- **Authentication** (Authentifizierung): Die in Phase 2 ausgewählte Authentifizierungsmethode wird angezeigt.
- **PFS** (PFS, *Perfect Forward Secrecy*): In dieser Zeile wird der PFS-Status angezeigt.
- **Group** (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.
- **Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, so dass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

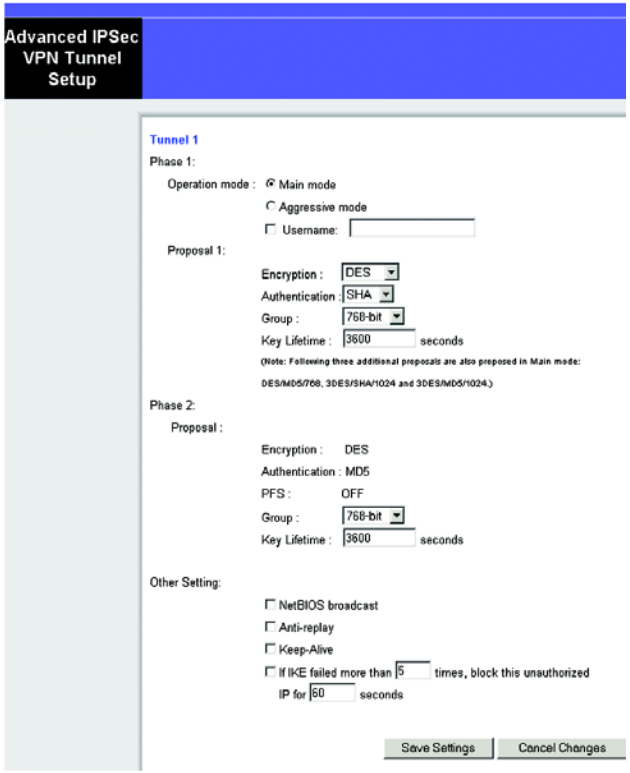

Abbildung 5-24: Advanced VPN Tunnel Setup (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Other Setting (Zusätzliche Einstellung)

- **NetBIOS broadcast** (NetBIOS-Broadcast): Aktivieren Sie das Kontrollkästchen neben **NetBIOS broadcast** (NetBIOS-Broadcast), um den NetBIOS-Datenverkehr durch den VPN-Tunnel zu leiten.
- **Anti-replay** (Anti-Replay): Aktivieren Sie das Kontrollkästchen neben **Anti-replay** (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.
- **Keep-Alive** (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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf die Schaltfläche **Help** (Hilfe), um weitere Informationen zu dieser Registerkarte zu erhalten.

Die Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

Internet Access (Internetzugriff)

Über die Registerkarte „Access Restrictions“ (siehe Abbildung 5-25) 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.

- **Internet Access Policy** (Richtlinien für Internetzugriff): Mehrfache Filter können als Sicherheitsrichtlinien für den Internetzugriff gespeichert werden. Wählen zur Bearbeitung einer Richtlinie die entsprechende Nummer aus der Dropdown-Liste 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 **Delete** (Löschen). Klicken Sie zur Anzeige einer Zusammenfassung aller Richtiglinien auf die Schaltfläche **Summary** (Zusammenfassung).

  Die Zusammenfassung wird in einem Fenster (siehe Abbildung 5-26) mit dem entsprechenden Namen und den entsprechenden Einstellungen angezeigt. Um zur Registerkarte **Filters** (Filter) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).

- **Enter Policy Name** (Richtliniennamen eingeben): Richtlinien werden auf Grundlage der hier aufgeführten Felder erstellt.

  So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Geben Sie im Feld **Policy Name** (Richtlinienname) einen Namen für die Richtlinie ein. Wählen Sie **Internet Access** (Internetzugriff) als Richtlinientyp aus.

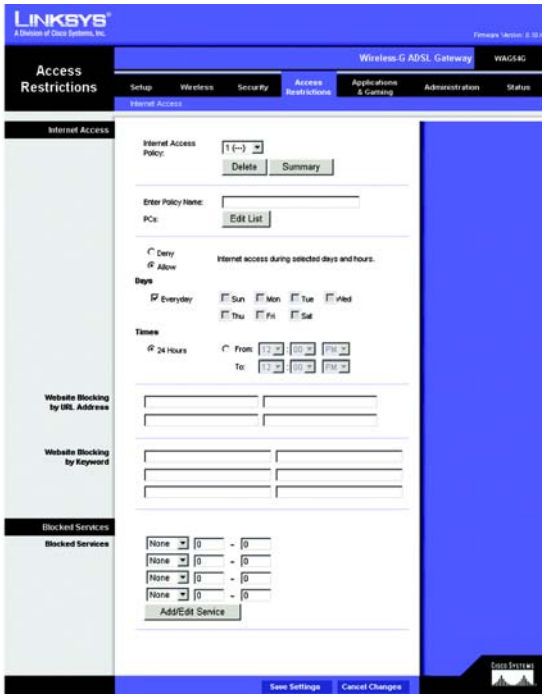

Abbildung 5-25: Access Restriction (Zugriffsbeschränkungen)

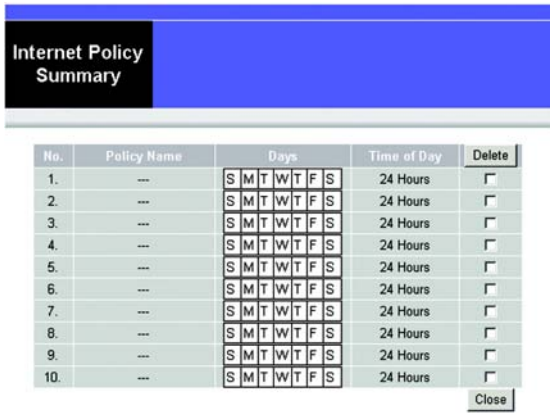

Abbildung 5-26: Internet Policy Summary (Internet-Richtlinien - Zusammenfassung)

2. Klicken Sie auf die Schaltfläche **Edit List** (Liste bearbeiten). Dadurch wird ein Fenster angezeigt, in dem die PC-Liste aufgeführt ist (siehe Abbildung 5-27). In diesem Feld 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 **Apply** (Anwenden), um Ihre Einstellungen zu speichern, auf die Schaltfläche **Cancel** (Abbrechen), um Änderungen rückgängig zu machen, und die Schaltfläche **Close** (Schließen), um zur Registerkarte **Filters** (Filter) zurückzukehren.

3. Klicken Sie auf die entsprechende Option [**Deny** (Verweigern) oder **Allow** (Zulassen)], um den Internetzugriff für die PCs, die im Fenster **List of PCs** (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 **Blocked Services** (Blockierte Dienste) auswählen. Wenn ein Dienst nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Add/Edit Service** (Dienst hinzufügen/bearbeiten), um das Fenster **Port Services** (Anschlussdienste) (siehe Abbildung 5-28) 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 **Save Settings** (Einstellungen speichern), um die Richtlinie zu aktivieren.

Der Internetzugriff kann auch über die URL-Adresse gefiltert werden, die Sie für den Zugriff auf Internetadressen eingegeben haben. Geben Sie hierfür die Adresse in eines der Felder **Website Blocking by URL Address** (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 **Website Blocking by Keyword** (Website nach Schlüsselwort blockieren) ein.

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

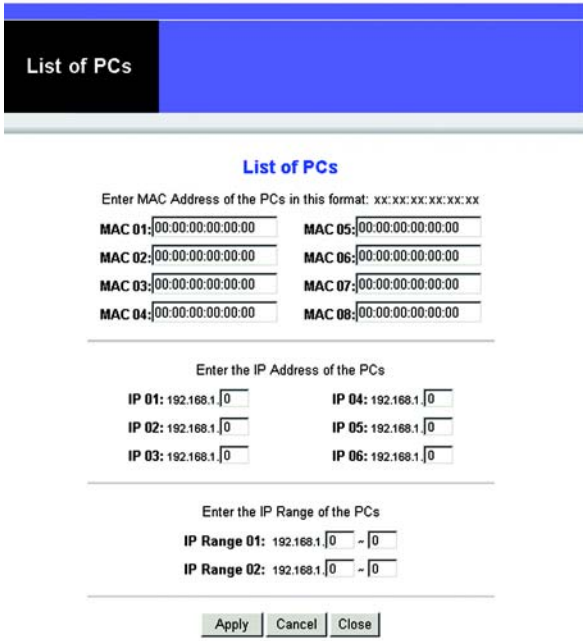

Abbildung 5-27: List of PCs (PC-Liste)

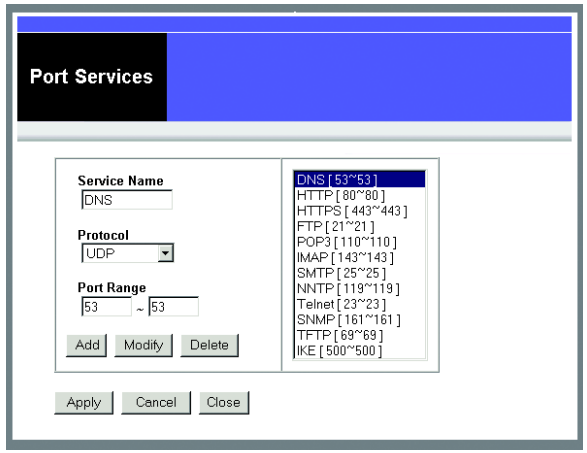

Abbildung 5-28: Port Services (Anschlussdienste)

Die Registerkarte „Applications and Gaming“ (Anwendungen und Spiele)

Single Port Forwarding (Einfaches Port-Forwarding)

Das Fenster **Single Port Forwarding** (Einfaches Port-Forwarding) bietet Optionen zur Anpassung der Anschlussdienste der gängigsten Anwendungen (siehe Abbildung 5-29).

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 **Enabled** (Aktiviert), um das UPnP-Forwarding für die ausgewählte Anwendung zu aktivieren.

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

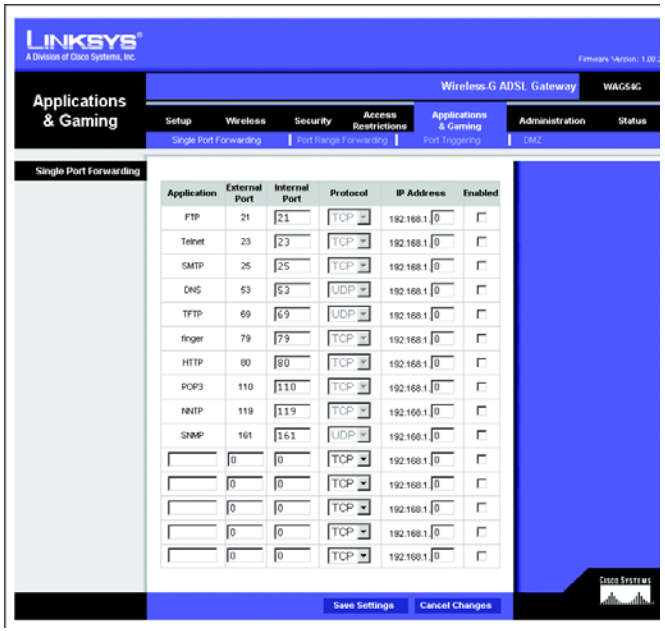

Abbildung 5-29: Single Port Forwarding (Einfaches Port-Forwarding)

Port Range Forwarding (Weiterleitung an einen Anschlussbereich)

Im Fenster **Port Forwarding** (Port-Forwarding) können Sie öffentliche Dienste auf Ihrem Netzwerk, wie z. B. Web-, FTP-, E-Mail-Server oder spezielle Internet-Anwendungen, festlegen. (Unter speziellen Internet-Anwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internet-Anwendungen ist keine Weiterleitung erforderlich (siehe Abbildung 5-30).

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.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start** (Von) und **End** (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 **Both** (Beide).
- **IP Address** (IP-Adresse): Geben Sie die IP-Adresse ein, und klicken Sie auf **Enabled** (Aktiviert).

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

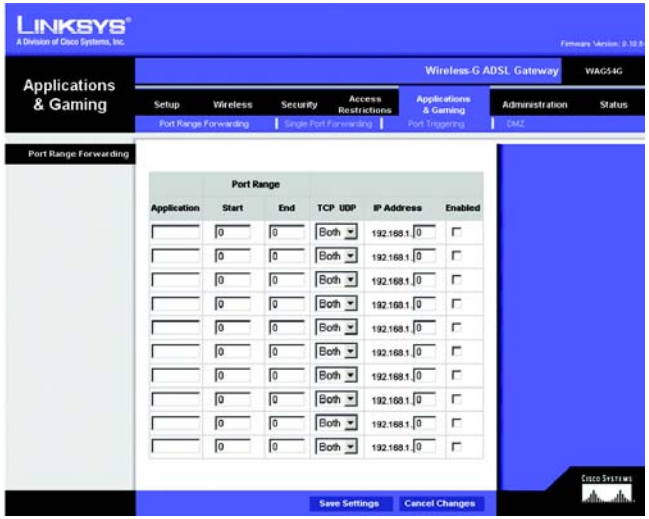

Abbildung 5-30: Port Range Forwarding (Weiterleitung an einen Anschlussbereich)

Port Triggering (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 (siehe Abbildung 5-31). 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 dem richtigen Computer weitergeleitet.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start Port** (Start-Port) und **End Port** (End-Port): Geben Sie Anfang und Ende der Bereichsnummern für Ausgangs-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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

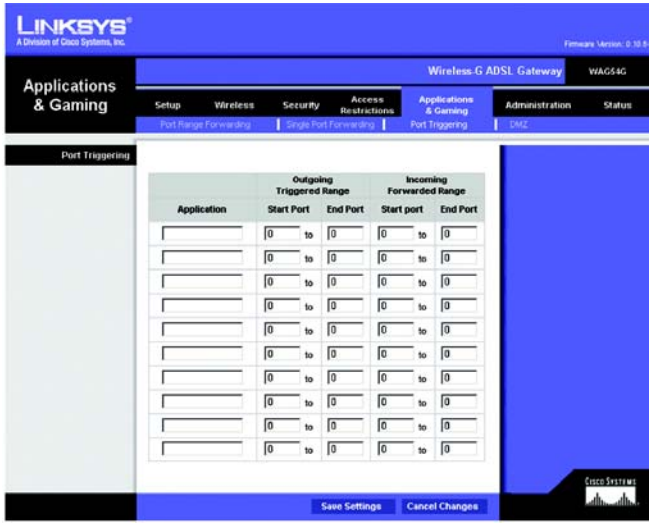

Abbildung 5-31: Port-Triggering

DMZ

Über das Fenster **DMZ** (siehe Abbildung 5-32) kann mithilfe von DMZ-Hosting für einen Netzwerkbenutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Mit DMZ-Hosting werden alle Anschlüsse gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

- „DMZ Hosting“ (DMZ-Hosting): Mit der DMZ-Funktion (*DMZ = Demilitarized Zone*; entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Enabled** (Aktiviert), um diese Funktion zu verwenden. Klicken Sie auf **Disabled** (Deaktiviert), 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 D: 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 **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

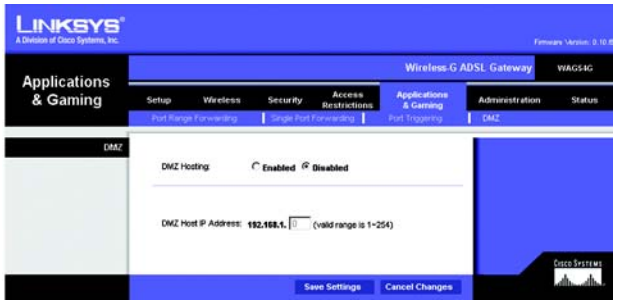

Abbildung 5-32: DMZ

Die Registerkarte „Administration“ (Verwaltung)

Management (Verwaltungsfunktionen)

Über das Fenster **Management** (Verwaltungsfunktionen) (siehe Abbildung 5-33) können Sie die Einstellungen für den Gatewayzugriff sowie die SNMP (Simple Network Management Protocol)- und UPnP (Universal Plug and Play)-Einstellungen ändern.

Gateway Access (Gateway-Zugriff)

Local Gateway Access (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Kennworts aufgefordert. Der Standardbenutzername und das Standardkennwort sind **admin**.

- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen ein: **admin**. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Kennwort): Es wird empfohlen, dass Sie Ihr Standardkennwort in ein persönliches Kennwort ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Kennwort nochmals ein, um es zu bestätigen.

Remote Gatway Access (Entfernter Gateway-Zugriff): Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

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

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

SNMP (Simple Network Management Protocol)

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

Identification (Identifikation): Um SNMP zu verwenden, klicken Sie auf **Enabled** (Aktiviert). Um SNMP zu deaktivieren, klicken Sie auf **Disabled** (Deaktiviert).

- Geben Sie im Feld **Device Name** (Gerätename) den Namen des Gateways ein.
- **Get Community** (Gemeinschaft abrufen): Geben Sie das Kennwort ein, mit dem ein schreibgeschützter Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Gemeinschaft einrichten): Geben Sie das Kennwort ein, mit dem ein Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.

Abbildung 5-33: Management (Verwaltungsfunktionen)

UPnP (Universal Plug and Play)

Mit UPnP kann unter Windows XP das Gateway automatisch für verschiedene Internet-Anwendungen, wie z. B. Internet-Spiele oder Videokonferenzen, konfiguriert werden.

UPnp (Universal Plug and Play): Um UPnP zu verwenden, klicken Sie auf **Enabled** (Aktiviert).

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

Reporting (Berichtaufzeichnung)

Über die Registerkarte **Reporting** (Berichtaufzeichnung) (siehe Abbildung 5-34) 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.

Log (Protokoll)

Log (Protokoll): Um die Berichtaufzeichnung zu verwenden, klicken Sie auf **Enabled** (Aktiviert).

- **Logviewer IP Address** (Logviewer-IP-Adresse): Geben Sie in dieses Feld die IP-Adresse ein, um Protokolle empfangen zu können.

Email Alerts (E-Mail-Warnungen)

Email Alerts (E-Mail-Warnungen): Um E-Mail-Warnungen zu verwenden, klicken Sie auf die Option **Enabled** (Aktiviert).

- **Denial of Service Thresholds** (DoS-Schwellwerte): Geben Sie die Schwellwerte der Ereignisse an, die Sie empfangen möchten.
- **SMTP Mail Server** (SMTP Mail-Server): Geben Sie in dieses Feld die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie in dieses Feld die E-Mail-Adresse für die Warnungsprotokolle ein.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die E-Mail-Adresse für Antwort-E-Mails ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen).

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

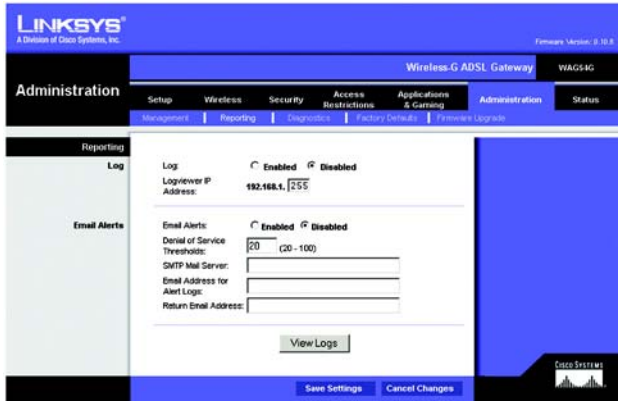

Abbildung 5-34: Reporting (Berichtaufzeichnung)

Diagnostics (Diagnose)

Ping Test (Ping-Test) (siehe Abbildung 5-35)

„Ping Test Parameters“ (Ping-Test-Parameter)

- **Ping Target IP** (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 Size** (Ping-Größe): Geben Sie die Größe des Ping-Pakets an.
- **No. of Pings** (Anzahl der Pings): Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping Interval** (Ping-Intervall): Geben Sie das Ping-Intervall in Millisekunden an.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Wartezeit in Millisekunden an.
- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

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

Abbildung 5-35: Ping Test (Ping-Test)

Factory Defaults (Werkseinstellungen) (siehe Abbildungen 5-36)

Restore Factory Defaults (Werkseinstellungen wiederherstellen): Wenn Sie alle verfügbaren Optionen angewandt haben und das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Yes** (Ja).

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, kicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) bzw. klicken Sie auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Abbildung 5-36: Factory Defaults (Werkseinstellungen)

„Firmware Upgrade“ (Firmware aktualisieren) (siehe Abbildung 5-37)

So aktualisieren Sie die Gateway-Firmware:

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

Abbildung 5-37: Firmware Upgrade (Firmware aktualisieren)

Die Registerkarte „Status“ (Status)

Gateway

In diesem Fenster werden Informationen zu Ihrem Gateway und den WAN-Internetverbindungen angezeigt (siehe Abbildung 5-38).

Gateway Information (Gateway-Informationen)

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

Internet Connections (Internet-Verbindungen)

Im Bereich der Internet-Verbindungen sind Angaben zu ADSL-Link, PPP-Login, Internet-IP-Adresse, öffentliche Subnetzmaske, Standard-Gateway, Primärer DNS-Server sowie zum Ablauf der DHCP-IP-Adresse enthalten.

System Statistics (Systemangaben)

Im Bereich der Systemangaben sind Angaben zu gesendeten und empfangenen Datenpaketen enthalten.

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

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

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

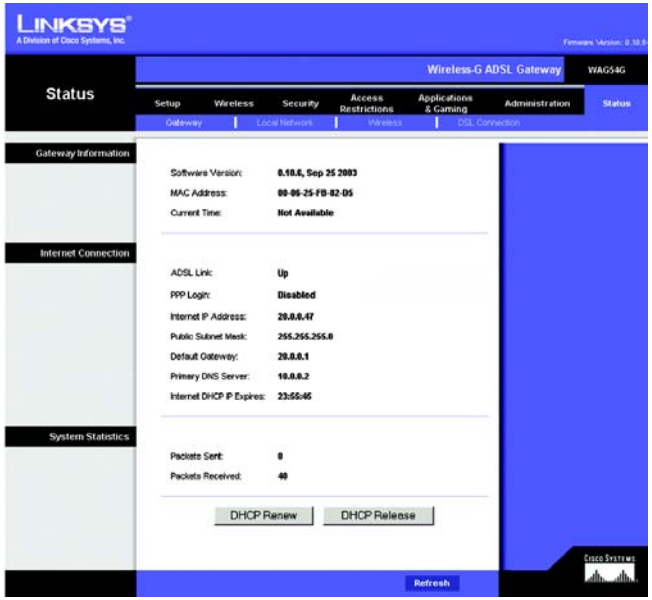

Abbildung 5-38: Status

Local Network (Lokales Netzwerk)

Im Bereich der Angaben zum lokalen Netzwerk sind Informationen zur lokalen Mac-Adresse, IP-Adresse, Subnetzmaske und zum DHCP-Server aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP Client Table** (DHCP-Client-Tabelle) (siehe Abbildung 5-39).

DHCP Client Table (DHCP-Client-Tabelle): Klicken Sie auf die Schaltfläche **DHCP Client Table** (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.) Siehe Abbildung 5-40.

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

Abbildung 5-39: Local Network (Lokales Netzwerk)

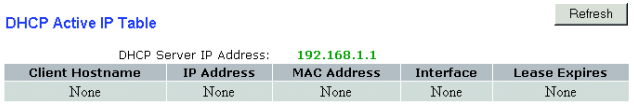

Abbildung 5-40: DHCP-Client-Tabelle

„Wireless“ (Wireless-Netzwerk)

Im Bereich der Wireless-Netzwerkinformationen sind Angaben zu Wireless-Firmware-Version, MAC-Adresse, Status, Modus, Kanal, SSID sowie Verschlüsselung aufgeführt (siehe Abbildung 5-41).

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Wireless-Clients verbunden), um die Wireless-Clients anzuzeigen, die mit dem Gateway verbunden sind.

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

Abbildung 5-41: Local Network (Wireless-Netzwerk)

DSL Connection (DSL-Verbindung)

Im Bereich der DSL-Verbindung sind Informationen zu Status, Downstream-Rate, Upstream-Rate, Kapselungsmethode, VPI (*Virtual Path Identifier*, Virtueller Pfadidentifizierer), VCI (*Virtual Channel Identifier*, Virtueller Kanalidentifizierer) sowie Multiplexing aufgeführt (siehe Abbildung 5-42).

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

Abbildung 5-42: DSL Connection (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 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 Standardgateway 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 Standardgateway 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 „Kapitel 4: Konfigurieren der Computer“. 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 zum automatischen Beziehen einer IP-Adresse von einem DHCP-Server (**IP-Adresse automatisch 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 Webseite 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, dass 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 ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

4. Ich kann auf die Setup-Seite 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. Informationen zur Überprüfung, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in „Anhang D: 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 auf ein anderes Subnetz, so dass 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 zu 192.168.2.1. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine IP-Adresse dementsprechend zu 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 Internet-Anwendungen 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 Port-Forwarding 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 **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (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 D: Ermitteln der MAC-Adresse und 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 **Save Settings** (Einstellungen speichern).

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

Zum Verwenden von Online-Spielen oder Internet-Anwendungen ist i. d. R. kein Port-Forwarding oder DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internet-Anwendungen 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 Internet-Anwendungen 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 Internet-Anwendung 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 **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (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 D: 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 **Save Settings** (Einstellungen speichern).

8. Weder Internetspiel, Internetserver noch Internetanwendung funktionieren.

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ (*DeMilitarized Zone*)-Hosting 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 Weiterleitungseinträge 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 nach den Forwarding-Einstellungen überprüft. Falls die Daten von einer Portnummer 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 **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (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 **Save Settings** (Einstellungen speichern).

9. Ich habe das Kennwort vergessen bzw. die Aufforderung zur Eingabe des Kennworts 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 Kennworts 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 Standardkennwort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
  2. Geben Sie in das Feld für das Gateway-Kennwort ein anderes Kennwort ein. Geben Sie anschließend das gleiche Kennwort in das zweite Feld ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

10. Wie kann ich als PPoE-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 das Gateway das Gateway für die Internetverbindung ist, 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 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 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 vorne zu beginnen.

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Kennwort, 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 **Products** (Produkte), und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Webseite 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 **Administration** (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 auf dem Computer eine statische IP-Adresse fest. Folgen Sie dazu den Anweisungen 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 **Administration** (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 Setup-Option 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 Kennwort ein. (Der Standardbenutzername und das Standardkennwort sind **admin**.)
3. Wählen Sie im Setup-Fenster die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest.
4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status** (Status), und klicken Sie auf Schaltfläche **Connect** (Verbinden).
5. Möglicherweise wird für den Anmeldestatus **Connecting** (Verbindung wird hergestellt) angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Connected** (Verbunden) für den Anmeldestatus angezeigt wird.
6. Klicken Sie auf die Schaltfläche **Save Settings** (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 Kennwort ein. (Der Standardbenutzername und das Standardkennwort sind **admin**.)
  3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert 1492 ein.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Wenn Sie weiterhin Schwierigkeiten erfahren haben, ändern Sie den MTU-Wert auf 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 nochmals 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, Standardgateway 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, dass 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-/DSL-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 an ein 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 Netzwerk-Adressen-Übersetzung (*Network Address Translation*, NAT) 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 Kundendienst hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als für die Windows-Betriebssysteme an.

Unterstützt das Gateway die ICQ-Dateiübertragung?
Ja, mithilfe der folgenden Lösung: Klicken Sie auf das Menü **ICQ**, **Preference** (Einstellungen) und auf die Registerkarte **Connections** (Verbindungen), und aktivieren Sie die Option **I am behind a firewall or proxy** (Ich bin hinter einer Firewall oder einem Proxy). Legen Sie nun in den Einstellungen für die Firewall für die Zeitüberschreitung 80 Sekunden fest. Ein Internetbenutzer kann nun eine Datei an einen Benutzer hinter dem Gateway senden.

Ich kann einen Unreal Tournament-Server einrichten, 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 sowie die Weiterleitungs-Ports 7777, 7778, 7779, 7780, 7781 und 27900 für die IP-Adresse des Servers einrichten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie die Weiterleitung an einen weiteren Port vornehmen. (Die Einstellung „Port 8080“ kann hier eingesetzt werden, findet jedoch nur bei einer Remote-Administration Verwendung. 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. vom verwendeten Server ab. So unterstützt z. B. Unreal Tournament eine mehrfache Anmeldung bei 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 sich mehrere Computer mit dem gleichen Server verbinden. Problem: Bei Version 1.0.1.6 können mehrere Computer, die die gleiche CD-Kennnummer 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 Webseite 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 die Einheit 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 **System** 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, es kann jedoch nur über Internet Explorer 4.0 bzw. über Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugegriffen werden.

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. 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 D: 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-Forwarding, 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 für diese Informationen an Ihren ISP.

Wie kann ich mIRC mit dem Gateway verwenden?
Legen Sie in der Registerkarte **Port Forwarding** (Port-Weiterleitung) 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.

Kann ich eine Anwendung von einem standortfernen Computer aus über das Wireless-Netzwerk ausführen?
Dies ist abhängig davon, ob die Anwendung zur Verwendung in einem Netzwerk entwickelt wurde. Weitere Informationen dazu, ob die Anwendung in einem Netzwerk verwendet werden kann, finden Sie in der Dokumentation zur Anwendung.

Was ist der IEEE 802.11g-Standard?
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, jedoch nur unter der Voraussetzung, dass die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?
Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Kanal-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Paketauftrennung
- Energieverwaltung

Was bedeutet Ad-Hoc-Modus?
Wenn für ein Wireless-Netzwerk der Ad-Hoc-Modus festgelegt ist, sind die Wireless-fähigen Computer so konfiguriert, dass sie ohne Zugriffspunkt direkt miteinander kommunizieren (Peer-to-Peer).

Was bedeutet Infrastrukturmodus?
Ist für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt, ist es so konfiguriert, dass es mit einem Netzwerk über einen drahtlosen Zugriffspunkt kommuniziert.

Was ist Roaming?
Roaming bezeichnet die Möglichkeit, bei Verwendung von tragbaren Computern kontinuierlich über eine größere Distanz hinweg zu kommunizieren, als durch einen einzigen Zugriffspunkt abgedeckt werden kann. Vor Verwendung des Roaming muss der Computer auf die gleiche Kanalnummer wie der Zugriffspunkt des dedizierte Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das drahtlose LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Zugriffspunkt bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Um diese Funktionen gleichzeitig verwenden zu können, ist eine dynamische Netzwerktechnologie erforderlich, durch die Zugriffspunkte und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Zugriffspunkt verarbeitet wird, und die Entfernung zwischen jedem Zugriffspunkt zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Zugriffspunkt und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem Original-Zugriffspunkt vorliegt oder ob ein neuer Zugriffspunkt gesucht werden soll. Wenn ein Knoten keine Bestätigung des Original-Zugriffspunkts mehr erhält, wird eine neue Verbindungssuche gestartet. Wenn ein neuer Zugriffspunkt gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

Was bedeutet ISM-Band?

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High-Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

Was bedeutet Bandspreizung?

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*, Frequenzsprungverfahren).

Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

Können die Daten bei der Funkübertragung abgefangen werden?
WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*; direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

Was ist WEP?
WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

Was ist eine MAC-Adresse?
Eine MAC (*Media Access Control*)-Adresse ist eine eindeutige Nummer, die vom Hersteller jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, 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.

Wie behebe ich einen Signalverlust?
Ohne Überprüfung ist es nicht möglich, den genauen Bereich Ihres Wireless-Netzwerks zu bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer und stellen Sie beide Geräte schrittweise weiter entfernt auf, um dadurch die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da dies Störungen, die nur einen Kanal betreffen, vermindert.

Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.
WEP ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass die gleichen WEP-Schlüssel und -Ebenen (64 bzw. 128) in allen Knoten in Ihrem Wireless-Netzwerk verwendet werden.

Wie viele Kanäle/Frequenzen sind mit dem Gateway verfügbar?
Es stehen insgesamt 11 Kanäle, von 1 bis 11 (für Nordamerika), zur Verfügung.

Falls Sie hier keine Antworten auf Ihre Fragen erhalten haben, finden Sie weitere Informationen auf der internationalen Website von Linksys unter http://www.linksys.com/international.

Anhang B: Sicherheit im Wireless-Netzwerkbetrieb

Wichtige Informationen für drahtlose Produkte

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres drahtlosen Netzwerks.

1. Leistung:

Die Leistung Ihres drahtlosen Netzwerks hängt von einer Reihe von Faktoren ab:

Die Entfernung vom Zugriffspunkt in einer Infrastrukturumgebung. Je weiter Sie entfernt sind, desto geringer wird die Übertragungsgeschwindigkeit.

Strukturelle Interferenzen: Die bauliche Auslegung bzw. Struktur Ihres Gebäudes sowie die Bauart und die Baumaterialien wirken sich unter Umständen negativ auf die Signalqualität und -geschwindigkeit aus.

Der Standort und die Ausrichtung der drahtlosen Geräte.

2. Interferenzen:

Jedes Gerät, das innerhalb des 2,4-GHz-Spektrums arbeitet, kann Netzwerkinterferenzen bei drahtlosen 802.11b- oder 802.11g-Geräten verursachen. Störungen können unter anderem von schnurlosen 2,4-GHz-Telefonen, Mikrowellenöfen, sich in der Nähe befindlichen öffentlichen „Hotspots“ und drahtlosen 802.11b- oder 802.11g-Wireless-LANs ausgehen.

3. Sicherheit:

Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen, die ein Eingreifen Ihrerseits erfordern, um diese umsetzen zu können.

Führen Sie von der nachfolgend aufgeführten vollständigen Liste mindestens die Schritte A bis E durch:

A. Ändern Sie die Standard-SSID.

B. Deaktivieren Sie SSID-Übertragungen.

C. Ändern Sie das Standardkennwort für das Administrator-Konto.

D. Aktivieren Sie die MAC-Adressfilterung.

E. Ändern Sie die SSID regelmäßig.

F. Aktivieren Sie die 128-Bit-WEP-Verschlüsselung. Beachten Sie, dass die Netzwerkleistung hierdurch verringert wird.

G. Ändern Sie die WEP-Verschlüsselungsschlüssel regelmäßig.

Informationen zum Umsetzen dieser Sicherheitsfunktionen finden Sie im Benutzerhandbuch.

4. Sicherheitsrisiken für Wireless-Netzwerke

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen sind entschlüsselt und enthalten umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set Identifier*) des Netzwerks und die IP-Adresse des Netzwerk-PCs oder Zugriffspunkts. Dagegen können Sie sich folgendermaßen schützen:

Ändern Sie das Administratorkennwort regelmäßig. Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorkennwort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorkennwort regelmäßig.

SSID: In Zusammenhang mit der SSID ist Folgendes zu beachten:

A. Deaktivieren Sie Übertragungen.

B. Wählen Sie eine individuelle SSID.

C. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind ab Werk auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys“.) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID zu einer individuellen Angabe, die keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr drahtloses Netzwerk verschafft haben, erneut das Kennwort knacken müssen.

MAC-Adressen: Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur drahtlosen Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es den Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

WEP-Verschlüsselung: WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel gegen Sicherheitsrisiken bei drahtlosen Geräten gesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es dem Hacker das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

A. Verwenden Sie die höchste Verschlüsselungsebene.

B. Verwenden Sie einen freigegebenen Schlüssel.

C. Verwenden Sie mehrere WEP-Schlüssel.

D. Ändern Sie Ihre WEP-Schlüssel regelmäßig.

Verschlüsselungsfunktionen haben negative Auswirkungen auf die Netzwerkleistung. Wenn Sie sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Durch die Einhaltung dieser Sicherheitsempfehlungen können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos nutzen.

Anhang C: 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.

Für Windows 2000 oder 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

HINWEIS: Die Anweisungen und Abbildungen in diesem Abschnitt der Anleitung beziehen sich auf den Router. Ersetzen Sie „Gateway“ durch „Router“. 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.

Hinweise zum Einrichten eines sicheren IPSecTunnels

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 C-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.

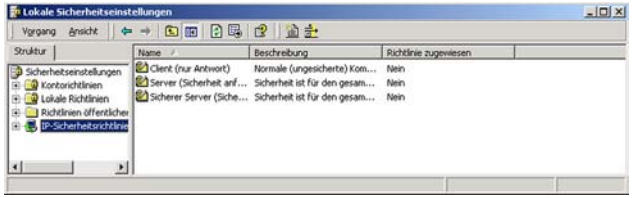

Abbildung C-1: Fenster „Lokale Sicherheitseinstellungen“

HINWEIS: Jeder Bezug in diesem Kapitel auf „win” verweist auf Windows 2000 und Windows XP. Ersetzen Sie die Hinweise auf „Router“ mit „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 C-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 C-3). Das Fenster **IP-Filterliste** wird angezeigt (siehe Abbildung C-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**.

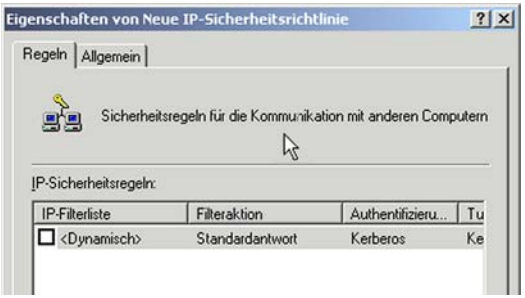

Abbildung C-2: Registerkarte „Regeln“

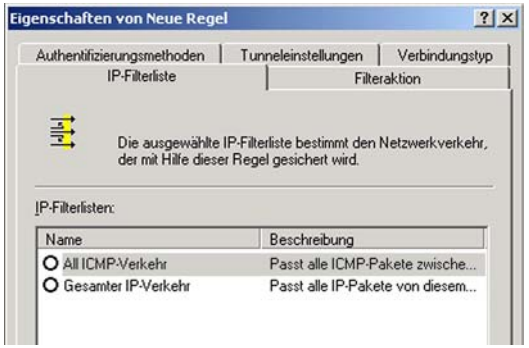

Abbildung C-3: Registerkarte „IP-Filterliste“

3. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung C-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 C-6). Wählen Sie die Registerkarte **IP-Filterliste** aus, und stellen Sie sicher, dass **win -> Router** markiert ist. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

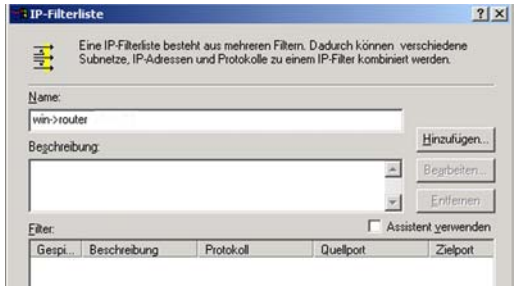

Abbildung C-4: Dialogfeld „IP-Filterliste“

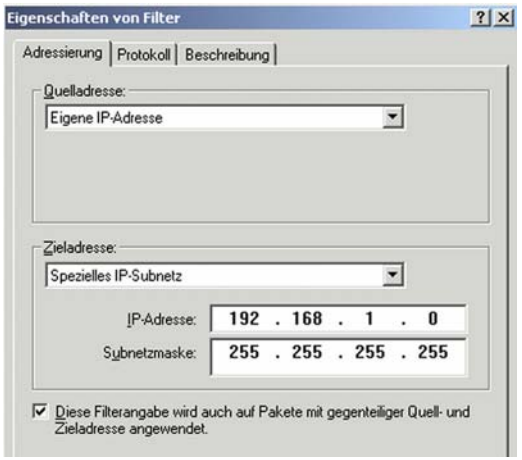

Abbildung C-5: Dialogfeld „Eigenschaften von Filter“

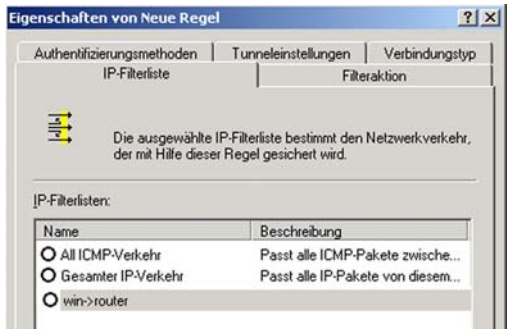

Abbildung C-6: Eigenschaften von Neue Regel

7. Das Fenster **IP-Filterliste** wird angezeigt (siehe Abbildung C-7). Geben Sie für die Filterliste einen geeigneten Namen, wie 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 C-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 C-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).

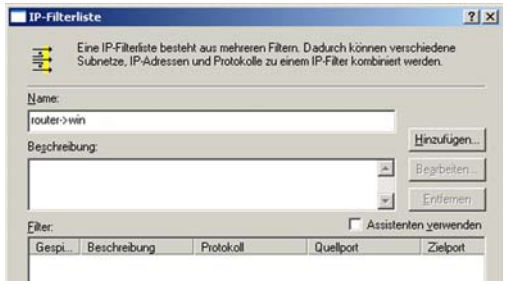

Abbildung C-7: Dialogfeld „IP-Filterliste“

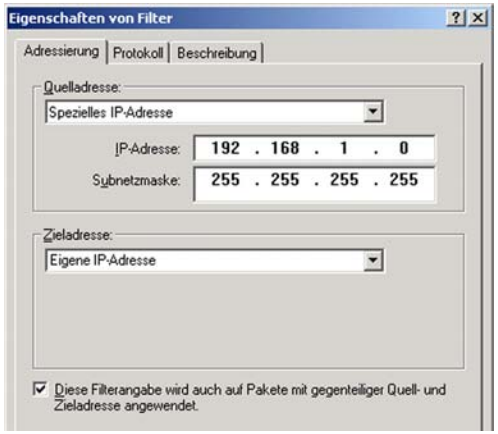

Abbildung C-8: Dialogfeld „Eigenschaften von Filter“

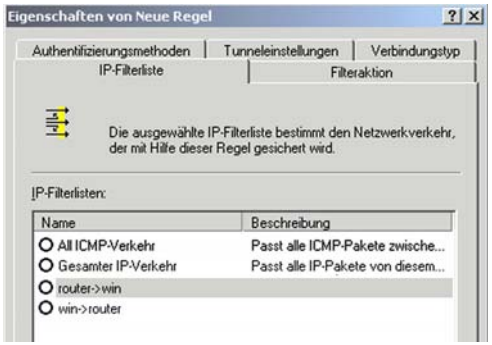

Abbildung C-9: Eigenschaften von Neue Regel

Schritt 3: Konfigurieren von individuellen Tunnelregeln

Tunnel 1: win -> Router

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

2. Klicken Sie auf die Registerkarte **Filteraktion** (siehe Abbildung C-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 C-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**.

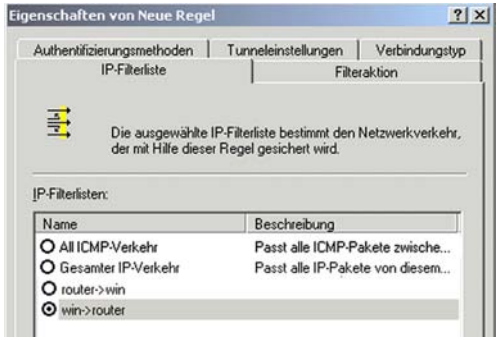

Abbildung C-10: Registerkarte „IP-Filterliste“

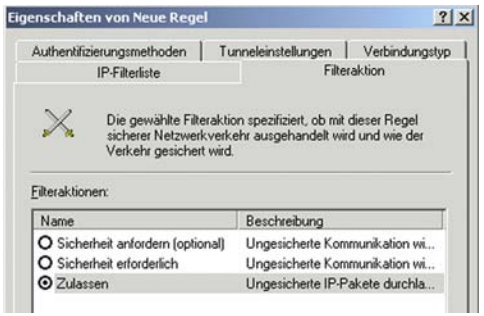

Abbildung C-11: Registerkarte „Filteraktion“

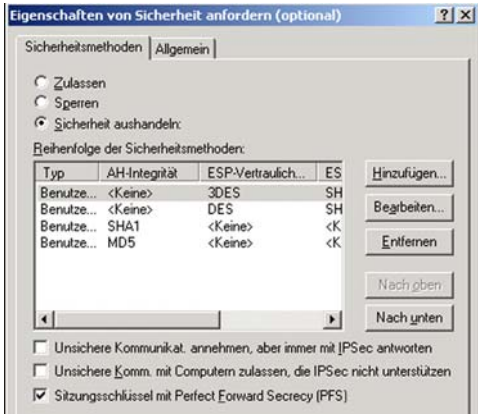

Abbildung C-12: Registerkarte „Sicherheitsmethoden“

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

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

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

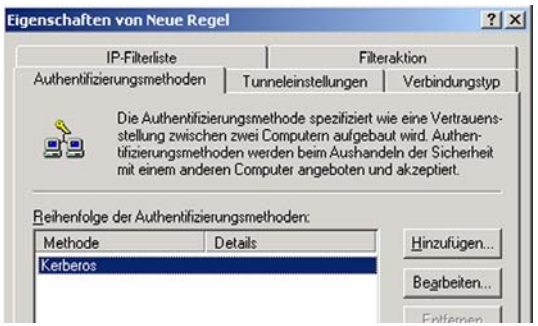

Abbildung C-13: Registerkarte „Authentifizierungsmethoden“

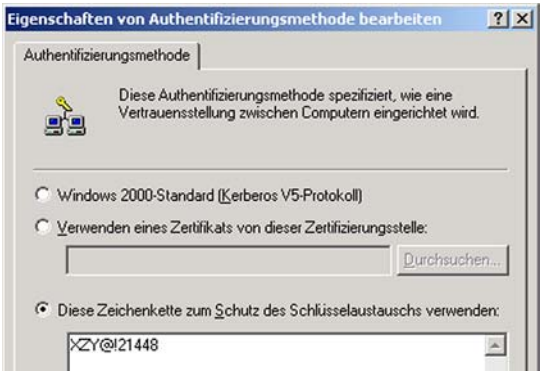

Abbildung C-14: Vorinstallierter Schlüssel

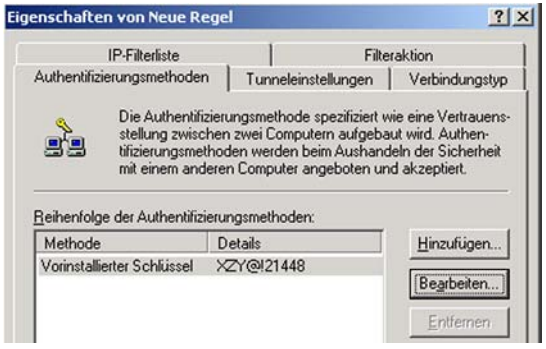

Abbildung C-15: Neuer vorinstallierter Schlüssel

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

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

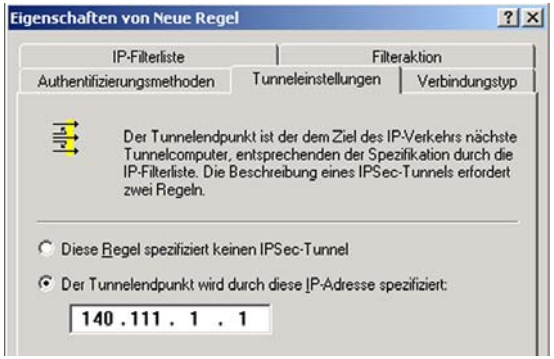

Abbildung C-16: Registerkarte „Tunneleinstellungen“

Tunnel 2: Router -> win

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

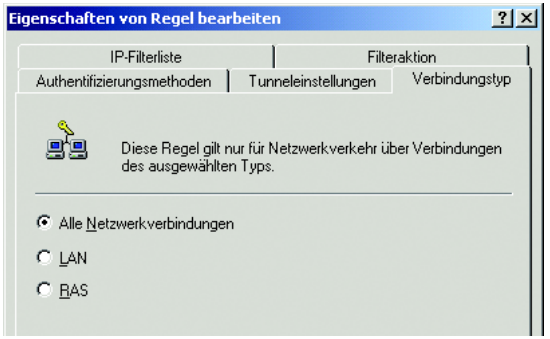

Abbildung C-17: Registerkarte „Verbindungstyp“

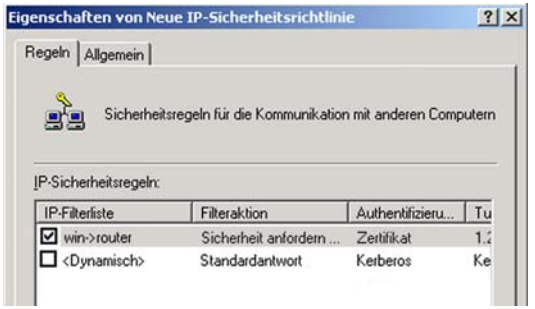

Abbildung C-18: Fenster für die Eigenschaften der neuen Richtlinie

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

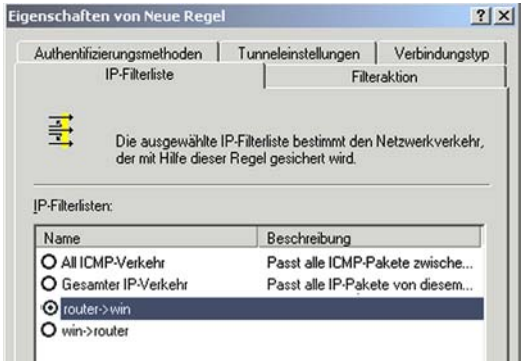

Abbildung C-19: Registerkarte „IP-Filterliste“

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

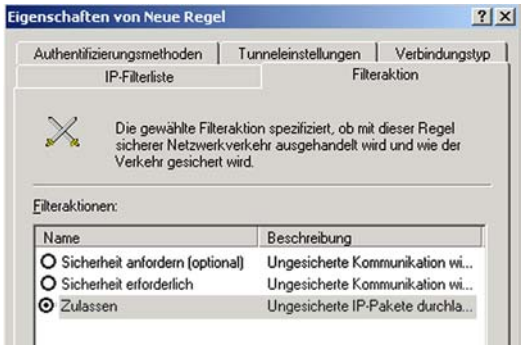

Abbildung C-20: Registerkarte „Filteraktion“

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

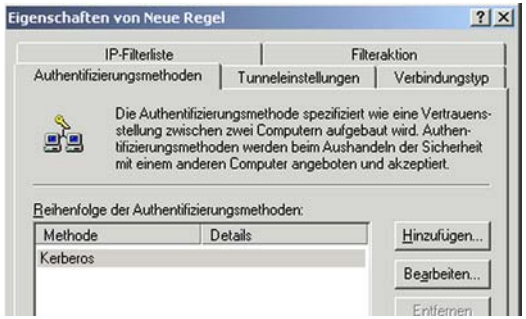

Abbildung C-21: Registerkarte „Authentifizierungsmethode“

13. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden** (siehe Abbildung C-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**.

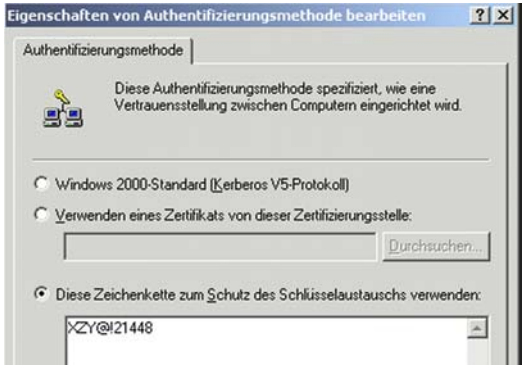

Abbildung C-22: Vorinstallierter Schlüssel

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

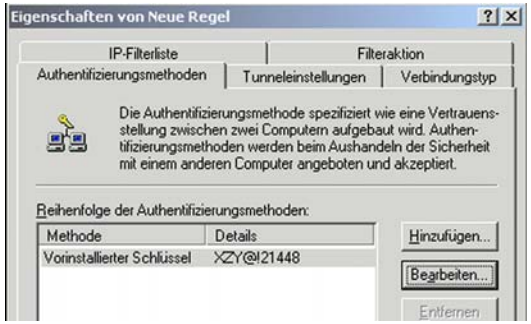

Abbildung C-23: Neuer vorinstallierter Schlüssel

15. Aktivieren Sie in der Registerkarte **Tunneleinstellungen** (siehe Abbildung C-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.

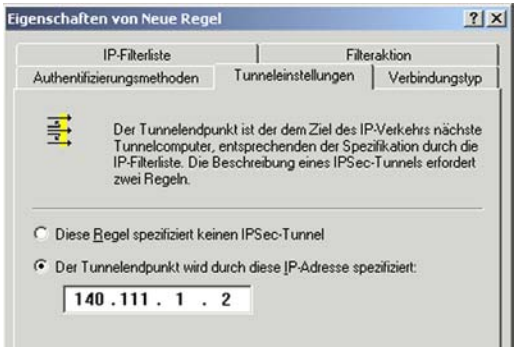

Abbildung C-24: Registerkarte „Tunneleinstellungen“

16. Klicken Sie auf die Registerkarte **Verbindungstyp** (siehe Abbildung C-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 C-26) auf die Schaltfläche **OK** bzw. auf **Schließen**, um zum secpol-Bildschirm zurückzukehren.

Abbildung C-25: Verbindungstyp

Schritt 4: Zuweisen einer neuen IPSec-Richtlinie

Klicken Sie mit der rechten Maustaste auf den Eintrag **IP-Sicherheitsrichtlinien auf lokalem Computer** (Abbildung C-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.

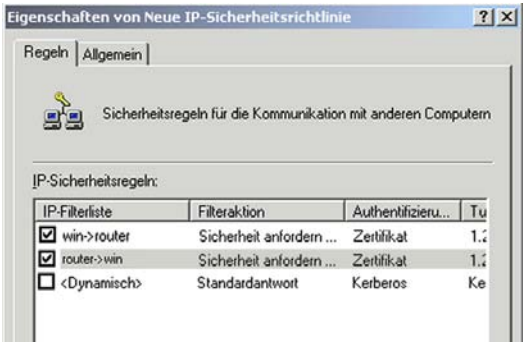

Abbildung C-26: Regeln

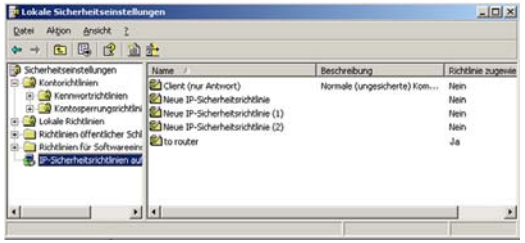

Abbildung C-27: Lokaler Computer

Schritt 5: Erstellen eines Tunnels mithilfe des webbasierten Dienstprogramms

1. Geben Sie im Adressfeld des Browsers **192.168.1.1** ein. Drücken Sie die Eingabetaste.
2. Wenn die Felder **Benutzername** und **Kennwort** angezeigt werden, geben Sie den Standard-Benutzernamen und das -Kennwort **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 C-28 dargestellt, den zu erstellenden Tunnel aus der Dropdown-Liste **Select Tunnel Entry** (Tunneleintrag auswählen) aus. Klicken Sie dann auf **Enabled** (Aktiviert). Geben Sie im Feld **Tunnel Name** (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 **Local Secure Group** (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 **Remote Security Gateway** (Entferntes Sicherheits-Gateway) 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** oder **3DES** (empfohlen wird **3DES**, weil 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 **Disable** (Deaktivieren) auswählen.
8. Wählen Sie aus zwei Authentifizierungstypen aus: **MD5** und **SHA** (empfohlen wird **SHA**, weil 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 **Pre-shared Key** (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 **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, so dass der Schlüssel unbegrenzt lange zur Verfügung steht.
10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern.

Der Tunnel ist nun hergestellt.

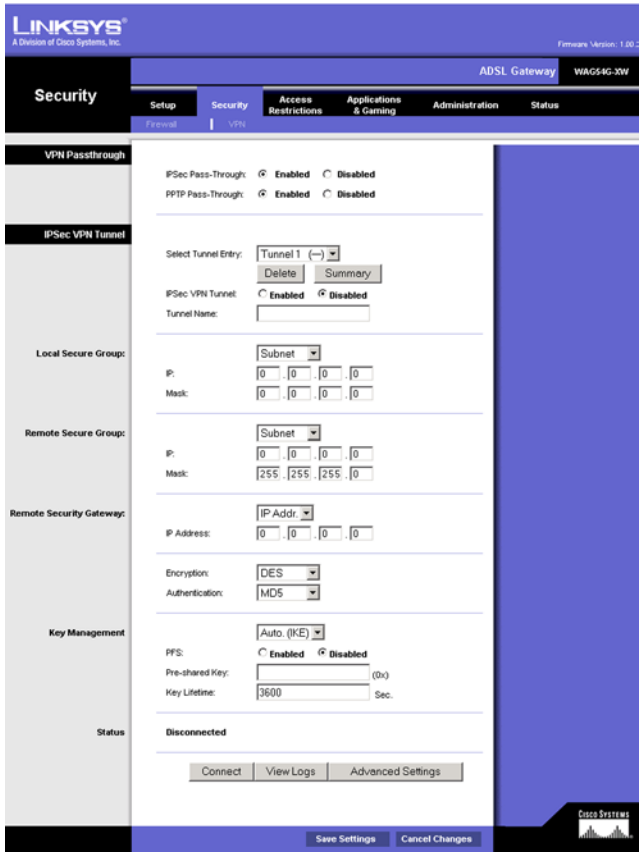

Abbildung C-28: Registerkarte „VPN“

Anhang D: 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-, Weiterleitungs- 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 winipcfg** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

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

3. Notieren Sie die Adapteradresse so, wie sie auf dem Bildschirm Ihres Computers angezeigt wird (siehe Abbildung D-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 D-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

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

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

Abbildung D-1: Fenster „IP-Konfiguration“

Abbildung D-2: MAC-Adresse/Adapteradresse

Anweisung für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen 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 D-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 D-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung E-1 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

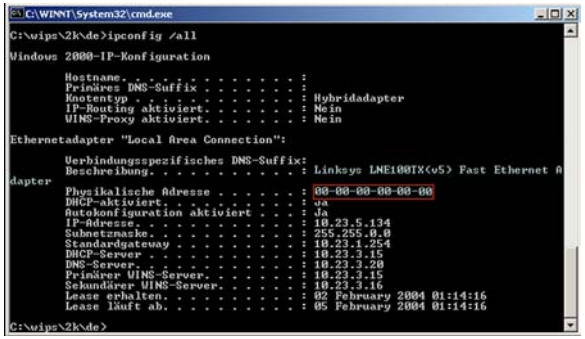

Abbildung D-3: MAC-Adresse/physikalische Adresse

Anhang E: Aktualisieren der Firmware

Die Firmware des Gateways wird über die Registerkarte **Administration** (Verwaltung) des webbasierten Dienstprogramms aktualisiert. Führen Sie die folgenden Schritte aus:

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

Abbildung E-1: Firmware aktualisieren

Anhang F: 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 eines Wireless-Netzwerks zu erweitern.

Adapter - Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhalten kann.

Ad-hoc (Ad-hoc-Modus) - Eine Gruppe drahtloser Geräte, die direkt miteinander kommunizieren (Peer-to-Peer) statt über einen Access Point.

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 bestimmen Geräts oder Netzwerks.

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

Bit - Eine Informationseinheit.

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, üblicherweise Computern, temporäre IP-Adressen zuzuweisen.

DMZ (*Demilitarized Zone*) - Hebt den Firewall-Schutz des Gateways für einen Computer auf, so dass 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 drahtloser 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 Bereich Computer und Telekommunikation sowie andere Informationstechnologiegeräte.

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

Hochfahren - Starten des Computers, so dass dieser Befehle ausführt.

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 - Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse eines bestimmten Geräts 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 einem jeden Netzwerkbetriebsgerät 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 nutzen, 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 ein Netzwerk gesendet wird.

Passphrase - Wird wie ein Kennwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Verschlüsselungsschlüssel 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 Kennwort) 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 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. Ein Satz an Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, bezeichnet man als „Programm“.

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

Standard-Gateway - Ein Gerät, über das der Internetdatenverkehr von Ihrem LAN 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.

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

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, so dass 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 Kennwortfunktionalitäten 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 eines Netzwerkgeräts, 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 Funkverbindungen miteinander kommunizieren.

Anhang G: Spezifikationen

Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), T1.413i2, UR-2 Deutsche Telekom (nur Deutschland)
Ports	Netzstrom, LINE (ADSL), Ethernet (1-4)
Tasten	Reset-Taste, Ein-/Aus-Taste
Kabeltyp	UTP Kat. 5 oder höher
Datenrate	Bis zu 54 MBit/s im Wireless-Betrieb Bis zu 8 MBit/s im ADSL-Downstream-Betrieb Bis zu 800 KBit/s im ADSL-Upstream-Betrieb
Übertragungsleistung	18 dBm
LEDs	Netzstrom, Ethernet (1-4), Wireless-G WLAN, DSL, Internet
Sicherheitsmerkmale	WEP
WEP-Schlüssel	64 Bit, 128 Bit
Abmessungen (B x H x T)	186 mm x 48 mm x 188 mm
Gerätegewicht	0,48 kg
Stromversorgung	Extern, 12 V GS, 1 A
Zertifizierungen	FCC Teil 15B Klasse B, FCC Teil 15C Klasse B, FCC Teil 68, UL 1950, CSA, 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 H: 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 andere Buchse als an die des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung
Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte in einem Mindestabstand von 20 cm zwischen dem Heizer und Ihrem Körper installiert und betrieben werden.

KANADISCHE INDUSTRIEBESTIMMUNGEN

Dieses digitale Gerät der Klasse B erfüllt die kanadischen Bestimmungen der Richtlinie ICES-003.
Bei der Verwendung dieses Geräts innerhalb eines Systems, das teilweise oder vollständig im Freien betrieben wird, ist es möglicherweise gemäß kanadischen Bestimmungen erforderlich, eine Genehmigung für das System zu beantragen.

EU-KONFORMITÄTSERKLÄRUNG (EUROPA)

Linksys erklärt, dass das Wireless-G ADSL-Gateway die unten stehenden Spezifikationen erfüllt und den Bestimmungen der europäischen R&TTE-Richtlinie 1999/5/EC nachkommt:

- EN 301 489-1, 301 489-17 EMV-Voraussetzungen für Funkausrüstungen
- EN 609 50 Sicherheit
- EN 300-328-1, EN 300-328-2 Technische Voraussetzungen für Funkausrüstungen

Warnung: Dieses Gerät ist zur Verwendung in allen EU- und EFTA-Mitgliedsstaaten bestimmt. Die Verwendung im Freien ist u. U. auf bestimmte Frequenzen beschränkt bzw. erfordert eine Betriebslizenz. Informationen zur Verfahrensweise erhalten Sie von der örtlichen Behörde.

Hinweis: Kombinationen von Leistungspegeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW (EIRP; *Effective Isotropic Radiated Power*) führen, erfüllen nicht die Bestimmungen der oben genannten Richtlinien und sind deshalb nicht für die Verwendung innerhalb der EU und jenen Ländern zulässig, die die europäische Richtlinie R&TTE 1999/5/EC übernommen haben.

Weitere Informationen zu rechtlich zulässigen Kombinationen von Leistungspegeln und Antennen erhalten Sie von der Abteilung für Unternehmensvorschriften von Linksys.

- Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
- Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.
- Belgique:

  Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.
- France:

  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le department. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

FCC TEIL 68 ERKLÄRUNG

Dieses Gerät entspricht Teil 68 der FCC-Bestimmungen. Am Gerät befindet sich ein Etikett, das u. a. die FCC-Registrierungsnummer und die Rufäquivalenzzahl (*Ringer Equivalence Number*; REN) des Geräts aufweist. Falls erforderlich, müssen Sie der Telefongesellschaft diese Angaben mitteilen.

Dieses Gerät verwendet die folgende USOC-Buchse: RJ-11.

Im Lieferumfang dieses Geräts sind ein FCC-kompatibles Telefonkabel und ein Modularstecker enthalten. Dieses Gerät ist zum Anschluss an das Telefon- oder Unternehmensnetz mithilfe eines kompatiblen Modularsteckers bestimmt, der FCC Teil 68 entspricht. Die Verbindung zum Telefonnetz sollte über die Standardmodularbuchse für Telefonverbindungen hergestellt werden.

Mit der REN kann die Anzahl der Geräte ermittelt werden, die an die Telefonleitung angeschlossen werden können. All diese Geräte können einen Klingelton abgeben, wenn Ihre Telefonnummer gewählt wird. In den meisten (nicht allen) Fällen sollte die Gesamtzahl der RENs nicht 5 überschreiten. Um die Anzahl der Geräte, die gemäß der Gesamtzahl der RENs an die Leitung angeschlossen werden können, zu überprüfen, wenden Sie sich an die Telefongesellschaft; diese informiert sie über die maximale Anzahl an RENs für den Anrufbereich.

Wenn durch dieses Gerät Schäden am Telefonnetz verursacht werden, kann die Telefongesellschaft Ihren Dienst vorübergehend einstellen. Wenn keine Vorankündigungen möglich sind, wird die Telefongesellschaft den Kunden so früh wie möglich benachrichtigen. Sie werden außerdem über Ihr Recht in Kenntnis gesetzt, eine Beschwerde bei der FCC einzureichen, falls Sie dies als notwendig erachten.

Die Telefongesellschaft nimmt u. U. Änderungen an ihrem System, ihrer Ausrüstung, ihrer Betriebs- oder Vorgehensweise vor, die den Betrieb des Geräts beeinträchtigen können. In diesem Fall kündigt die Telefongesellschaft dies im Voraus an, so dass Sie die für einen durchgehenden Betrieb nötigen Änderungen vornehmen können.

Sollte dieses Gerät nicht einwandfrei funktionieren, trennen Sie es von der Telefonleitung. Versuchen Sie, ein anderes FCC-kompatibles Gerät in derselben Telefonbuchse zu verwenden. Falls das Problem weiterhin besteht, wenden Sie sich an den Kundendienst der Telefongesellschaft. Falls das Problem behoben ist und somit im Gerät vorzuliegen scheint, trennen Sie das Gerät von der Telefonleitung, und verwenden Sie es erst nach entsprechender Reparatur wieder. Bitte beachten Sie, dass Sie von der Telefongesellschaft dazu aufgefordert werden können, das Gerät vom Telefonnetz zu trennen, bis das Problem behoben ist oder bis Sie sichergestellt haben, dass keine Funktionsstörung im Gerät vorliegt. Für eine optimale Leistung des Geräts sind Zubehör und Kabel vom Hersteller zu verwenden.

Vom Kunden sind keine Reparaturarbeiten vorzunehmen. Wenn bei Verwenden dieses Geräts Probleme auftreten, erhalten Sie bei einem autorisierten Kundendienstanbieter Informationen zu Reparatur- und Garantieleistungen. Wenn das Problem Schäden am Telefonnetz hervorruft, können Sie von der Telefongesellschaft dazu aufgefordert werden, das Gerät vom Netz zu trennen, bis das Problem behoben ist. Dieses Gerät kann nicht mit von der Telefongesellschaft bereitgestellten Münzfernsprechern verwendet werden. Die Verbindung zu einem Gemeinschaftsanschluss-Dienst unterliegt der staatlichen Gebührenordnung.

SICHERHEITSHINWEISE

- Warnung: Verwenden Sie zur Reduzierung der Brandgefahr ein Telefonkabel der AWG-Klasse Nr. 26 oder größer.
- Verwenden Sie dieses Gerät nicht in der Umgebung von Wasser, wie z. B. in einem feuchten Keller oder in der Nähe eines Schwimmbeckens.
- Vermeiden Sie die Verwendung dieses Produkts (außer der kabellosen Variante) während eines Gewitters. Es besteht das (geringe) Risiko eines elektrischen Schlags durch Blitzschlag.

Anhang I: Garantieinformationen

Eingeschränkte Gewährleistung

Linksys sichert Ihnen für einen Zeitraum von drei 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 eigener Wahl 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 Kundendienst von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN KUNDENDIENST 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 eigene Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanada 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 bei Ihnen 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 bzw. keine Beschränkungen von zufälligen oder mittelbaren Schäden; die oben genannte Beschränkung oder der oben genannte Ausschluss finden daher unter Umständen bei Ihnen 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 J: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits etablierte 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