Cisco Modell DPC/EPC2325 DOCSIS Residential Gateway mit Wireless Access Point - Benutzerhandbuch

Inhalt

- WICHTIGE SICHERHEITSHINWEISE 2
- Einleitung 9
- Packungsinhalt 11
- Beschreibung der Steuerungsanzeige 12
- Beschreibung der Rückseite 13
- Idealer Aufstellungsort für das DOCSIS Residential Gateway 14
- Wandmontage (Optional) 15
- Systemanforderungen für den Internetzugang 19
- High-Speed-Internetdienst 20
- Internetanschluss 22
- Konfiguration des DOCSIS Residential Gateway 25
- Problembehebung bei der Einrichtung des Internets 104
- Häufig gestellte Fragen 105
- Problembehebung 113
- Tipps für eine bessere Leistung 114
- Funktionen der LED-Statusanzeigen 115
- Technische Fragen 118
- Hinweise 120
- Hinweise zu Drittanbieter-Softwarelizenzen für das Cisco-Modell DPC/EPC2325 DOCSIS Residential Gateway mit Wireless Access Point 121

WICHTIGE SICHERHEITSHINWEISE

Notice to Installers

The servicing instructions in this notice are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions, unless you are qualified to do so.

Note to System Installer

For this apparatus, the coaxial cable shield/ screen shall be grounded as close as practical to the point of entry of the cable into the building. For products sold in the US and Canada, this reminder is provided to call the system installer's attention to Article 820-93 and Article 820-100 of the NEC (or Canadian Electrical Code Part 1), which provides guidelines for proper grounding of the coaxial cable shield.

CAUTION: To reduce the risk of electric shock, do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.

WARNING
TO PREVENT FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE.

This symbol is intended to alert you that uninsulated voltage within this product may have sufficient magnitude to cause electric shock. Therefore, it is dangerous to make any kind of contact with any inside part of this product.

This symbol is intended to alert you of the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.

Notice à l'attention des installateurs de réseaux câblés

Les instructions relatives aux interventions d'entretien, fournies dans la présente notice, s'adressent exclusivement au personnel technique qualifié. Pour réduire les risques de chocs électriques, n'effectuer aucune intervention autre que celles décrites dans le mode d'emploi et les instructions relatives au fonctionnement, à moins que vous ne soyez qualifié pour ce faire.

Remarque à l'attention de l'installateur du système

Avec cet appareil, le blindage/écran du câble coaxial doit être mis à la terre aussi près que possible du point d'entrée du câble dans le bâtiment. En ce qui concerne les produits vendus aux États-Unis et au Canada, ce rappel est fourni pour attirer l'attention de l'installateur sur les articles 820-93 et 820-100 du Code national de l'électricité (ou Code de l'électricité canadien, Partie 1) qui fournissent des lignes directrices concernant la mise à la terre correcte du blindage (écran) du câble coaxial.

ATTENTION : Pour réduire les risques de chocs électriques, ne pas enlever le couvercle (ou le panneau arrière). Ne contient aucune pièce réparable par l'utilisateur. Confier les interventions aux techniciens d'entretien qualifiés.

AVERTISSEMENT
POUR ÉVITER LES INCENDIES OU LES CHOCS ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.

Ce symbole a pour but de vous prévenir que des tensions électriques non isolées existent à l'intérieur de ce produit, pouvant être d'une intensité suffisante pour causer des chocs électriques. Il est donc dangereux d'établir un contact quelconque avec l'une des pièces comprises à l'intérieur de ce produit.

Ce symbole a pour but de vous prévenir de la présence d'instructions importantes relatives au fonctionnement ou à l'entretien (et aux réparations) dans la documentation accompagnant ce produit.

Mitteilung für CATV-Techniker

Die in dieser Mitteilung aufgeführten Wartungsanweisungen sind ausschließlich für qualifiziertes Fachpersonal bestimmt. Um die Gefahr eines elektrischen Schlags zu reduzieren, sollten Sie keine Wartungsarbeiten durchführen, die nicht ausdrücklich in der Bedienungsanleitung aufgeführt sind, außer Sie sind zur Durchführung solcher Arbeiten qualifiziert.

Mitteilung an den Systemtechniker

Für dieses Gerät muss der Koaxialkabelschutz/ Schirm so nahe wie möglich am Eintrittspunkt des Kabels in das Gebäude geerdet werden Dieser Erinnerungshinweis liegt den in den USA oder Kanada verkauften Produkten bei. Er soll den Systemtechniker auf Paragraph 820-93 und Paragraph 820-100 der US-Elektrovorschrift NEC (oder der kanadischen Elektrovorschrift Canadian Electrical Code Teil 1) aufmerksam machen, in denen die Richtlinien für die ordnungsgemäße Erdung des Koaxial-kabelschirms festgehalten sind.

Dieses Symbol weist den Benutzer auf das Vorhandensein von nicht isolierten gefährlichen Spannungen im Gerät hin, die Stromschläge verursachen können. Ein Kontakt mit den internen Teilen dieses Produktes ist mit Gefahren verbunden.

ACHTUNG: Zur Vermeidung eines Stromschlags darf die Abdeckung (bzw. die Geräterückwand) nicht entfernt werden. Das Gerät enthält keine vom Benutzer wartbaren Teile. Wartungsarbeiten dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

WARNUNG

DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN.

Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.

Aviso a los instaladores de sistemas CATV

Las instrucciones de reparación contenidas en el presente aviso son para uso exclusivo por parte de personal de mantenimiento cualificado. Con el fin de reducir el riesgo de descarga eléctrica, no realice ninguna otra operación de reparación distinta a las contenidas en las instrucciones de funcionamiento, a menos que posea la cualificación necesaria para hacerlo.

Nota para el instalador del sistema

En lo que se refiere a este aparato, el blindaje del cable coaxial debe conectarse a tierra lo más cerca posible al punto por el cual el cable entra en el edificio. En el caso de los productos vendidos en los EE. UU. y Canadá, el presente aviso se suministra para llamar la atención del instalador del sistema sobre los Artículos 820-93 y 820-100 del NEC (o Código Eléctrico de Canadá, Parte 1), que proporcionan directrices para una correcta conexión a tierra del blindaje del cable coaxial.

Este símbolo tiene como fin advertirle de que una tensión sin aislamiento en el interior de este producto podría ser de una magnitud suficiente como para provocar una descarga eléctrica. Por consiguiente, resulta peligroso realizar cualquier tipo de contacto con alguno de los componentes internos de este producto.

ATENCIÓN: con el fin de reducir el riesgo de descarga eléctrica, no retire la tapa (ni la parte posterior). No existen en el interior componentes que puedan ser reparados por el usuario. Encargue su revisión a personal de mantenimiento cualificado.

ADVERTENCIA

PARA EVITAR EL RIESGO DE INCENDIO O DESCARGA ELÉCTRICA, NO EXPONGA LA UNIDAD A LA LLUVIA O A LA HUMEDAD.

Este símbolo tiene como fin alertarle de la presencia de importantes instrucciones de operación y mantenimiento (revisión) contenidas en la literatura que acompaña al producto.

20080814_Installer820_Intl

WICHTIGE SICHERHEITSHINWEISE

1) Lesen Sie diese Sicherheitshinweise.
2) Bewahren Sie diese Sicherheitshinweise auf.
3) Beachten Sie alle Warnhinweise.
4) Befolgen Sie alle Anweisungen.
5) Benutzen Sie dieses Gerät nicht in der Nähe von Wasser.
6) Reinigen Sie es ausschließlich mit einem trockenen Tuch.
7) Achten Sie darauf, dass die Belüftungsöffnungen nicht blockiert sind. Richten Sie das Gerät entsprechend den Anweisungen des Herstellers ein.
8) Stellen Sie das Gerät nicht in der Nähe von Wärmequellen wie Heizkörpern, Heizungsklappen, Herden oder anderen Geräten (einschließlich Verstärkern) auf, die Wärme abgeben.
9) Setzen Sie die Sicherheitsvorrichtung des verpolungssicheren Steckers bzw. des Steckers mit Schutzkontaktbügel nicht außer Kraft. Ein verpolungssicherer Stecker besitzt zwei Stifte, von denen der eine breiter ist als der andere. Ein Stecker mit Schutzkontaktbügel ist zusätzlich zu den beiden Stiften mit einem Schutzkontaktbügel ausgestattet. Der breitere Stift bzw. der Schutzkontaktbügel dienen Ihrer Sicherheit. Sollte der mitgelieferte Stecker nicht in Ihre Steckdose passen, lassen Sie die veraltete Steckdose von einem Elektriker austauschen.
10) Achten Sie darauf, dass niemand versehentlich auf das Netzkabel treten kann und dass es – besonders am Stecker, den Gerätesteckdosen oder an der Kabelaustrittsstelle am Gerät – nicht abgeklemmt werden kann.
11) Verwenden Sie ausschließlich die vom Hersteller vorgesehenen Zusatz- und Zubehörteile.

12) Verwenden Sie das Gerät nur mit Vorrichtungen wie Wagen, Ständer, Dreibein, Halterung oder Tisch, die vom Hersteller empfohlen oder zusammen mit dem Gerät verkauft werden. Bei Verwendung eines Wagens sollten Sie Vorsicht walten lassen, um ein Umkippen des Wagens mitsamt dem Gerät beim Transport zu verhindern.
13) Ziehen Sie den Netzstecker des Gerätes während eines Gewitters oder bei längerer Nichtbenutzung des Gerätes.
14) Alle Wartungsarbeiten sollten entsprechend geschulten Fachkräften überlassen werden. Eine Wartung bzw. Reparatur ist dann erforderlich, wenn das Gerät nicht mehr betriebstauglich ist. Das ist dann der Fall, wenn ein Netzkabel oder Netzstecker beschädigt ist, Flüssigkeit über das Gerät verschüttet wurde, Gegenstände in das Gerät gefallen sind, das Gerät Regen oder Feuchtigkeit ausgesetzt wurde, das Gerät nicht mehr ordnungsgemäß funktioniert oder fallen gelassen wurde.

Hinweis zur Stromquelle

Die für dieses Produkt geeignete Stromquelle können Sie einem Etikett auf dem Produkt entnehmen. Schließen Sie dieses Gerät nur an eine Steckdose mit der auf dem Produkt angegebenen Spannung und Frequenz an. Bei Fragen zum Typ des zuhause oder im Büro genutzten Stromnetzes wenden Sie sich an Ihren Dienstanbieter oder das zuständige Energieversorgungsunternehmen.

Der AC-Eingang des Gerätes muss jederzeit zugänglich und betriebstauglich sein.

Erdung des Gerätes

WARNUNG: Vermeiden Sie Stromschläge und Brandrisiken! Sollte dieses Gerät mit Koaxialkabeln verbunden sein, vergewissern Sie sich, dass das Kabelsystem geerdet ist. Die Erdung bietet einen gewissen Schutz gegen Spannungsstöße und statische Aufladung.

Schutz vor Blitzschlag

Zusätzlich zum Trennen des Netzkabels von der Steckdose sollten Sie an den Signaleingängen angeschlossene Kabel ausstecken.

Überprüfen der Stromzufuhr

Auch wenn die Anzeigelampe (Power) nicht leuchtet, ist das Gerät möglicherweise immer noch an das Stromnetz angeschlossen. Die Anzeigelampe kann beim Ausschalten des Gerätes erlöschen, auch wenn dieses weiterhin mit der Steckdose verbunden ist.

Überlastung des Stromnetzes

WARNUNG: Vermeiden Sie Stromschläge und Brandrisiken! Vermeiden Sie eine Überlastung von Stromnetz, Steckdosen, Verlängerungskabeln und Gerätesteckdosen. Lesen Sie bei Verwendung von Geräten, für deren Betrieb Batterien oder andere Stromquellen erforderlich sind, die dazugehörige Betriebsanleitung.

Belüftung und Standortwahl

- Entfernen Sie alles Verpackungsmaterial, bevor Sie das Gerät an das Stromnetz anschließen.
- Platzieren Sie das Gerät nicht auf einem Bett, Sofa, Teppich oder ähnlichen Oberflächen.
- Platzieren Sie dieses Gerät nicht auf einer instabilen Oberfläche.
- Installieren Sie dieses Gerät nur dann in einem Gehäuse wie einem Bücherschrank oder Rack, wenn für ausreichende Belüftung gesorgt ist.
- Platzieren Sie keine Unterhaltungsgeräte (z. B. Videorekorder oder DVD-Player), Lampen, Bücher, mit Flüssigkeit gefüllte Vasen oder andere Gegenstände auf diesem Gerät.
- Blockieren Sie nicht die Belüftungsöffnungen.

Schutz vor Feuchtigkeit und Fremdkörpern

WARNUNG: Vermeiden Sie Stromschläge und Brandrisiken! Schützen Sie dieses Gerät vor tropfenden oder spritzenden Flüssigkeiten, Regen und Feuchtigkeit. Mit Flüssigkeit gefüllte Behälter wie beispielsweise Vasen sollten nicht auf das Gerät gestellt werden.

WARNUNG: Vermeiden Sie Stromschläge und Brandrisiken! Trennen Sie dieses Gerät vor dem Reinigen vom Stromnetz. Verwenden Sie keine flüssigen Reinigungsmittel oder Aerosolreiniger. Verwenden Sie keine magnetischen oder statischen Reinigungsgeräte (Staubentferner) zur Reinigung dieses Gerätes.

WARNUNG: Vermeiden Sie Stromschläge und Brandrisiken! Schieben Sie niemals Gegenstände durch die Öffnungen dieses Gerätes. Fremdkörper im Gerät können einen Kurzschluss auslösen, der wiederum zu einem Stromschlag oder einem Brand führen kann.

Wartungshinweise

WARNUNG: Vermeiden Sie Stromschläge! Öffnen Sie nicht die Abdeckung dieses Gerätes. Durch Öffnen oder Abnehmen der Abdeckung setzen Sie sich möglicherweise gefährlichen Spannungen aus. Durch Öffnen der Abdeckung verliert Ihre Garantie ihre Gültigkeit. Dieses Gerät enthält keine durch den Benutzer wartbaren Teile.

Überprüfen der Gerätesicherheit

Nach Abschluss aller Wartungsarbeiten oder Reparaturen an diesem Gerät muss der Techniker Sicherheitsprüfungen durchführen, um sicherzustellen, dass sich das Gerät in einem betriebstauglichen Zustand befindet.

Sicheres Bewegen des Gerätes

Trennen Sie das Gerät immer vom Stromnetz, wenn Sie es bewegen oder Kabel daran anschließen bzw. davon abtrennen.

20081112_Modem DSL_Safety

Einhaltung der FCC-Bestimmungen

Die FCC-Bestimmungen der Vereinigten Staaten

Dieses Gerät wurde geprüft und erfüllt die Grenzwertbestimmungen für Digitalgeräte der Klasse B gemäß Abschnitt 15 der FCC-Vorschriften (Federal Communications Commission). Diese Grenzwerte sollen beim Betrieb dieses Gerätes in einem Wohngebiet einen angemessenen Schutz vor Störstrahlungen gewährleisten. Dieses Gerät erzeugt und verwendet Hochfrequenzstrom und kann Hochfrequenzenergie abstrahlen. Wenn das Gerät nicht gemäß den Anleitungen installiert und betrieben wird, kann es Funkstörungen verursachen. Es kann jedoch nicht garantiert werden, dass in einer spezifischen Installation keine Funkstörungen auftreten. Falls dieses Gerät Funkstörungen bei Radio- oder Fernsehempfang verursacht (durch Ein- und Ausschalten des Gerätes feststellbar), können Sie diese Funkstörungen möglicherweise durch eine oder mehrere der folgenden Maßnahmen beheben:

- Richten Sie die Empfangsantenne neu aus oder positionieren Sie sie an einer anderen Stelle.
- Vergrößern Sie den Abstand zwischen Gerät und Empfänger.
- Verbinden Sie dieses Gerät mit einem vom Stromkreis des funkgestörten Gerätes unabhängigen Stromkreis.
- Wenden Sie sich an den Dienstanbieter oder einen erfahrenen Radio-/Fernsehtechniker.

Alle Änderungen und Modifizierungen, die nicht ausdrücklich von Cisco Systems, Inc. genehmigt worden sind, können zum Widerruf der Betriebsgenehmigung des Benutzers für das Gerät führen.

Die im folgenden Absatz der FCC-Konformitätserklärung enthaltenen Informationen sind Teil der FCC-Anforderungen und sollen Sie über die FCC-Zulassung dieses Gerätes informieren. *Die aufgeführten Telefonnummern sind nur für Fragen zu den FCC-Bestimmungen gedacht. Bei Fragen zu Betrieb, Installation oder Anschluss dieses Gerätes wenden Sie sich bitte an Ihren Dienstanbieter.*

FC Konformitätsklärung

Dieses Gerät entspricht den in Teil 15 der FCC-Bestimmungen aufgeführten Anforderungen. Der Betrieb unterliegt den beiden folgenden Bedingungen: 1) Das Gerät darf keine Störstrahlungen verursachen. 2) Das Gerät muss gegen alle empfangenen Störstrahlungen störsicher sein.

DOCSIS Residential Gateway
Modell: DPC/EPC2325
Hergestellt von:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044, USA
Telefon: +1-678-277-1120

Kanadische EMI-Vorschrift

Dieses Digitalgerät der Klasse B entspricht der kanadischen Norm ICES-003.

Cet appareil numérique de la class B est conforme à la norme NMB-003 du Canada.

FCC-Erklärung zur Strahlenbelastung

Hinweis: Dieser Sender darf sich nicht am selben Aufstellort wie andere Antennen oder Sender befinden oder mit diesen gemeinsam betrieben werden. Dieses Gerät sollte mit einem Mindestabstand von 20 cm (7, 9 Zoll) zwischen dem Strahler und Personen aufgestellt und betrieben werden.

USA

Die HF-Belastung von Personen durch dieses System wurde entsprechend den ANSI C 95.1-Grenzwerten des American National Standards Institute bewertet. Die Bewertung erfolgte gemäß ANI C 95.1 und FCC OET Bulletin 65C rev 01.01. Zur Einhaltung der Vorschriften ist ein Mindestabstand von 20 cm (auf 7, 9 Zoll) zwischen Antenne und Personen erforderlich.

Kanada

Die HF-Belastung von Personen durch dieses System wurde entsprechend den ANSI C 95.1-Grenzwerten bewertet. Die Bewertung erfolgte gemäß RSS-102 Rev 2. Zur Einhaltung der Vorschriften ist ein Mindestabstand von 20 cm (auf 7, 9 Zoll) zwischen Antenne und Personen erforderlich.

EU

Die HF-Belastung von Personen durch dieses System wurde entsprechend den Grenzwerten der Internationalen Kommission zum Schutz vor nicht ionisierender Strahlung (ICNIRP) bewertet. Die Bewertung erfolgte gemäß der EN 50385 Produktnorm zur Konformitätsüberprüfung von Mobilfunk-Basisstationen und stationären Teilnehmergeräten für schnurlose Telekommunikationsanlagen im Hinblick auf die Basisgrenz- und Referenzwerte bezüglich der Exposition von Personen gegenüber elektromagnetischen Feldern (110 MHz bis 40 GHz). Der Mindestabstand zwischen Antenne und Personen beträgt 20 cm (auf 7, 9 Zoll).

Australien

Die HF-Belastung von Personen durch dieses System wurde gemäß der australischen Strahlenschutznorm sowie entsprechend den Grenzwerten der Internationalen Kommission zum Schutz vor nicht ionisierender Strahlung (ICNIRP) bewertet. Der Mindestabstand zwischen Antenne und Personen beträgt 20 cm (auf 7, 9 Zoll).

20081016 FCC DSL_Dom and Intl

Einleitung

Einleitung

Willkommen in der aufregenden Welt des High-Speed-Internets! Ihr neues Cisco® Modell DPC/EPC2325 DOCSIS® Residential Gateway ist ein den Industrienormen für High-Speed-Datenverbindungen entsprechendes Kabelmodem. Das DPC/EPC2325 Residential Gateway verbindet für die verkabelte (Ethernet) oder kabellose Datenübertragung eine Vielzahl von Geräten zuhause oder in einem kleinen Unternehmen und ermöglicht High-Speed-Datenzugriff in einem einzigen Gerät. Mit einem DPC/EPC2325 Residential Gateway sind Ihre Internetnutzung, Ihre privaten und geschäftlichen Mitteilungen und Ihre Produktivität effektiver als je zuvor.

Dieses Handbuch enthält Verfahren und Empfehlungen für Aufstellung, Installation, Konfiguration und Betrieb Ihres DPC/EPC2325 Residential Gateway sowie zur Fehlerbehebung für optimalen High-Speed-Internetzugang zuhause oder in der Arbeit. Informationen zu spezifischen Situationen finden Sie in den entsprechenden Abschnitten dieses Handbuchs. Nähere Informationen dazu, wie Sie Internetdienste beziehen können, erhalten Sie von Ihrem Dienstanbieter.

Vorteile und Funktionen

Ihr neues DPC/EPC2325 Residential Gateway bietet die folgenden hervorragenden Vorteile und Funktionen:

- konform mit den Standards DOCSIS/EuroDOCSIS™ 2.0, 1.1 und 1.0 sowie den PacketCable™/EuroPacketCable™-Spezifikationen zur Lieferung von Spitzenleistungen und Zuverlässigkeit
- leistungsstarke Breitband-Internetverbindung, um Ihrem Online-Erlebnis größeren Schwung zu verleihen
- vier 10/100BASE-T-Ethernet-Ports für Kabelverbindungen
- 802.11g Wireless Access Point mit 4 SSIDs (Service Set Identifier)
- Wi-Fi Protected Setup (WPS), eine Funktion für ein vereinfachtes und sicheres Wireless-Setup, die Sie mit einem Tastendruck aktivieren können
- benutzerdefinierbarer Kinderschutz, um Zugriff auf unerwünschte Websites zu verhindern
- erweiterte Firewall-Technologie zur Abschreckung von Hackern und zum Schutz Ihres Heimnetzwerks vor unbefugtem Zugriff
- attraktives, kompaktes Design für sowohl vertikale als auch horizontale Aufstellung oder Wandbefestigung

- farbkodierte TR-068-konforme Schnittstellenports mit dazu passenden Kabeln für vereinfachte Installation und Setup
- LED-Beschriftung und -verhalten DOCSIS-5-konform für einfache Überprüfung des Betriebszustands für Benutzer und Techniker sowie Unterstützung bei der Fehlerbehebung
- automatische Software-Aktualiserungen durch Ihren Dienstanbieter

Packungsinhalt

Nach Erhalt Ihres kabellosen Heim-Gateways sollten Sie sicherstellen, dass alle Geräte- und Zubehörteile vorhanden und unbeschädigt sind. Packungsinhalt:

eine Version des DPC/EPC2325 DOCSIS Residential Gateway

ein Netzteil (für Modelle mit externer Stromversorgung)

ein Ethernet-Kabel (CAT5/RJ-45)

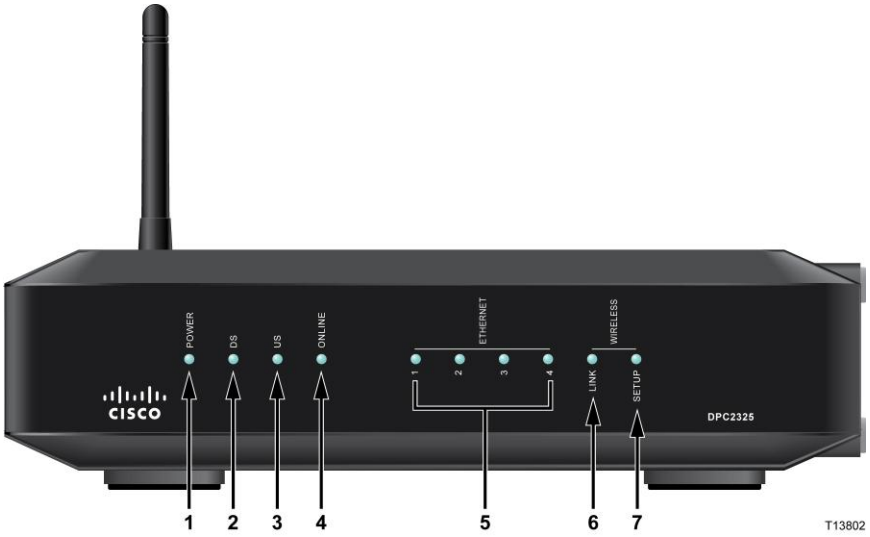
eine CD-ROM mit diesem Benutzerhandbuch

Sollte eines dieser Teile fehlen oder beschädigt sein, wenden Sie sich bitte an Ihren Dienstanbieter.

Hinweis: Wenn Sie einen Videorekorder, ein Digital Home Communications Terminal (DHCT) oder einen Set-Top-Konverter oder ein Fernsehgerät über dieselbe Kabelverbindung wie Ihr kabelloses Heim-Gateway anschließen möchten, benötigen Sie einen optionalen Signalsplitter und zusätzliche Standard-HF-Koaxialkabel.

Beschreibung der Steuerungsanzeige

Auf der Vorderseite Ihres Heim-Gateways befinden sich LED-Statusanzeigen, denen Sie Betriebsqualität und -status entnehmen können. Im Abschnitt ***Funktionen der LED-Statusanzeigen*** (Seite 115) finden Sie nähere Informationen zu den LED-Funktionen der Steuerungsanzeige.



Modell DPC2325

1 **POWER**: LED leuchtet; das kabellose Heim-Gateway wird mit Strom versorgt.

2 **DS**: LED leuchtet; das kabellose Heim-Gateway empfängt Daten vom Kabelnetzwerk.

3 **US**: LED leuchtet; das kabellose Heim-Gateway sendet Daten an das Kabelnetzwerk.

4 **ONLINE**: LED leuchtet; das kabellose Heim-Gateway ist im Netzwerk registriert und vollständig betriebsbereit.

5 **ETHERNET 1 – 4**: Eine leuchtende LED zeigt an, dass ein Gerät an einen der Ethernet-Ports angeschlossen ist. BLINKEN zeigt an, dass Daten über die Ethernet-Verbindung übertragen werden.

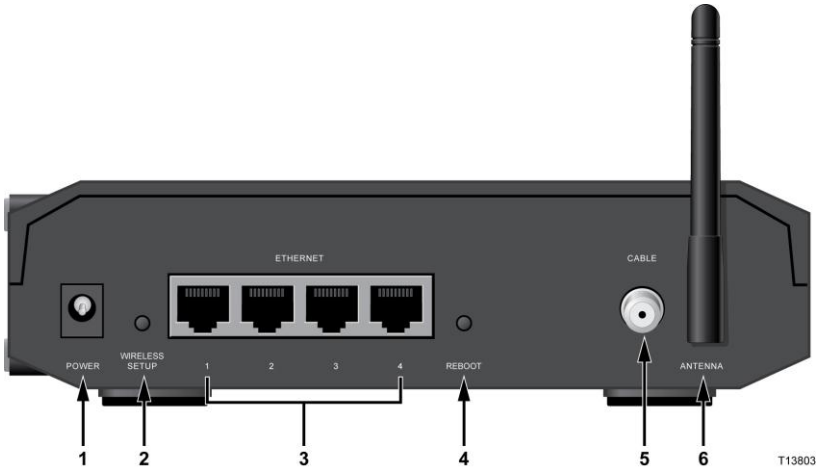
6 **WIRELESS LINK**: LED leuchtet; der Wireless Access Point ist betriebsbereit. BLINKEN zeigt an, dass Daten über die kabellose Verbindung übertragen werden. LED leuchtet nicht; der Wireless Access Point wurde vom Benutzer deaktiviert.

7 **WIRELESS SETUP**: LED leuchtet nicht (Normalzustand); Wireless-Setup ist nicht aktiv. BLINKEN zeigt an, dass der Benutzer das Wireless-Setup aktiviert hat, um neue kabellose Clients zum kabellosen Netzwerk hinzuzufügen.

Beschreibung der Rückseite

Die folgende Abbildung zeigt die Komponenten auf der Rückseite des DPC/EPC2325, deren Funktion anschließend beschrieben werden.

Modell mit externer Stromversorgung



Modell DPC/EPC2325

1 **POWER**: Anschluss für das im Lieferumfang Ihres Heim-Gateways enthaltene Netzteil.

> **ACHTUNG:**
>
> **Um eine Beschädigung des Gerätes zu vermeiden, sollten Sie ausschließlich das im Lieferumfang enthaltene Netzteil verwenden.**

2 **WIRELESS SETUP**: Durch Drücken dieses Knopfes wird das Wireless-Setup initiiert, das es dem Benutzer ermöglicht, dem Heimnetzwerk neue für den Wi-Fi Protected Setup (WPS) geeignete kabellose Clients hinzuzufügen.

3 **ETHERNET**: Vier RJ-45 Ethernet-Ports für die Verbindung mit dem Ethernet-Port an Ihrem PC oder Ihrem Heimnetzwerk.

4 **REBOOT**: Halten Sie diesen Knopf 1-2 Sekunden lang gedrückt, um das Heim-Gateway neu zu starten. Wenn Sie den Knopf länger als 10 Sekunden gedrückt halten, werden alle Einstellungen auf die Werkseinstellungen zurückgesetzt und das Gateway neu gestartet.

> **ACHTUNG:**
>
> **Der Reboot-Knopf ist nur für Wartungszwecke gedacht. Sie sollten ihn nur auf Anweisung Ihres Dienstanbieters drücken, da bei diesem Vorgang möglicherweise alle von Ihnen vorgenommenen Einstellungen des Kabelmodems verloren gehen.**

5 **CABLE**: F-Anschluss für den Empfang eines aktiven Kabelsignals von Ihrem Dienstanbieter.

6 **ANTENNA**: Anschluss für externe 802.11-Antenne.

Idealer Aufstellungsort für das DOCSIS Residential Gateway

Der ideale Aufstellungsort für Ihr Heim-Gateway ist dort, wo das Gerät Zugang zu Steckdosen und anderen Geräten hat. Berücksichtigen Sie deswegen bei der Auswahl des Aufstellungsortes den Grundriss Ihrer Wohnung oder Ihres Arbeitsplatzes und lassen Sie sich von Ihrem Dienstanbieter beraten. Lesen Sie sich dieses Benutzerhandbuch sorgfältig durch, bevor Sie sich für einen Aufstellungsort entscheiden.

Beachten Sie dabei Folgendes:

- Platzieren Sie Ihren PC und Ihr Heim-Gateway in der Nähe einer Steckdose.
- Platzieren Sie Ihren PC und Ihr Heim-Gateway in der Nähe eines vorhandenen Kabelanschlusses, damit kein zusätzlicher Kabelausgang benötigt wird. Es sollte ausreichend Platz vorhanden sein, um die vom Modem und PC wegführenden Kabel so zu führen, dass sie nicht übermäßig gestreckt oder geknickt werden.
- Die Luftzirkulation um das Heim-Gateway darf nicht beeinträchtigt sein.
- Wählen Sie einen Standort, an dem das Heim-Gateway vor versehentlichen Störungen oder Beschädigungen geschützt ist.

Wandmontage (optional)

Mit zwei Mauerankern, zwei Schrauben und den Befestigungsschlitzen am Gerät können Sie das Heim-Gateway an einer Wand befestigen. Das Modem kann sowohl vertikal als auch horizontal angebracht werden.

Vorbereitung

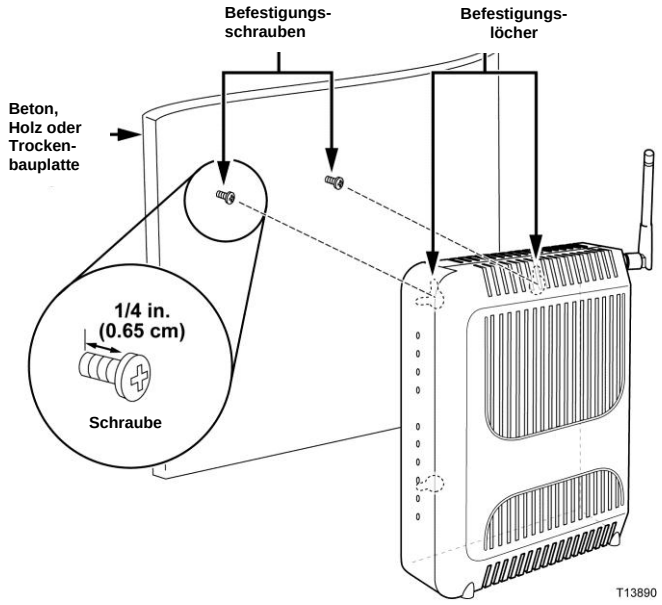
Wählen Sie zuerst einen geeigneten Platz für die Wandmontage aus. Die Wand kann aus Beton, Holz oder Trockenbauplatten bestehen. Der Montageplatz sollte auf allen Seiten frei zugänglich sein, und die Kabel sollten das Heim-Gateway problemlos ohne Strecken erreichen können. Lassen Sie an der Unterseite des Heim-Gateways genügend Abstand zum Fußboden oder Regalen, um den Zugang zu den Kabeln zu ermöglichen. Achten Sie außerdem darauf, dass alle Kabel locker genug sind, damit das Heim-Gateway für eventuell erforderliche Wartungsarbeiten ohne Abtrennen der Kabel von der Wand genommen werden kann. Für die Montage sollten Sie Folgendes bereithalten:

- zwei Wandanker für #8 x 1-Zoll Schrauben
- zwei #8 x 1-Zoll Flachkopf-Blechschrauben
- Bohrmaschine mit einem 3/16 Zoll (etwa 5 mm) starken Holz- oder Steinbohrer
- eine Kopie der Abbildungen zur Wandbefestigung auf den folgenden Seiten

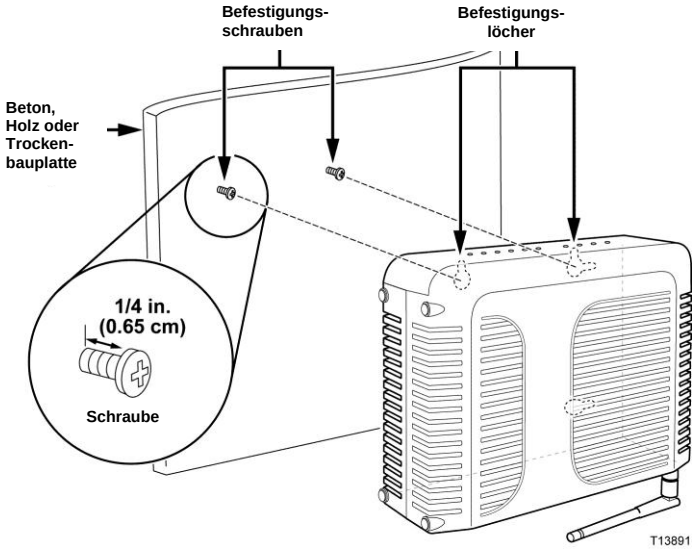
Wandmontage (optional)

Befestigen Sie das Gateway wie in einer der folgenden Abbildungen gezeigt an der Wand.

Vertikale Montage

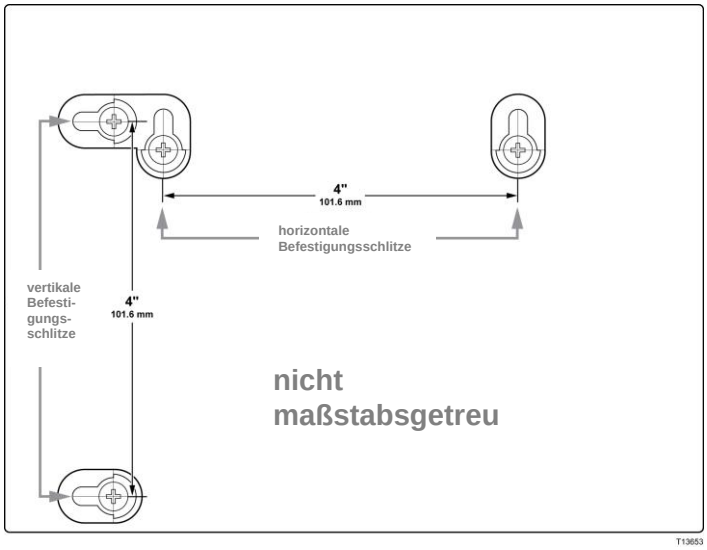


Horizontale Montage



Position und Abmessungen der Wandbefestigungsschlitze

Die folgende Abbildung zeigt Position und Abmessungen der Wandbefestigungsschlitze auf der Unterseite des Gateways. Befestigen Sie das Gateway entsprechend den Informationen auf dieser Seite an der Wand.



Anleitung für die Wandbefestigung des Heim-Gateways

1 Bohren Sie mit einem Bohrer und einer 3/16 Zoll (etwa 5 mm) starken Bohrspitze zwei Löcher in derselben Höhe mit einem Abstand von 4 Zoll (10,16 cm).

Hinweis: Die obige Abbildung zeigt die Position der Befestigungslöcher auf der Rückseite des Heim-Gateways.

2 Soll das Heim-Gateway an einer Trockenbauplatte oder Betonoberfläche befestigt werden, unter der sich ein Holzpfosten befindet?

- Wenn **ja**, machen Sie mit Schritt 3 weiter.
- Wenn **nein**, befestigen Sie die Ankerschrauben in der Wand und schrauben Sie die Befestigungsschrauben ein; lassen Sie zwischen dem Schraubenkopf und der Wand einen Abstand von etwa 6,5 mm. Machen Sie mit Schritt 4 weiter.

3 Schrauben Sie die Befestigungsschrauben in die Wand; lassen Sie zwischen dem Schraubenkopf und der Wand einen Abstand von etwa 6,5 mm. Machen Sie mit Schritt 4 weiter.

4 Vergewissern Sie sich, dass am Heim-Gateway keine Kabel angeschlossen sind.

5 Halten Sie das Heim-Gateway an die vorgesehene Position. Führen Sie die beiden Schlüssellochschlitze auf der Rückseite des Gateways mit der größeren Öffnung zuerst über die Befestigungsschrauben. Schieben Sie anschließend das Gateway nach unten, bis die engere Öffnung der Schlitze am Schraubenhals anliegt.

Wichtig: Stellen Sie sicher, dass das Heim-Gateway sicher von den Schrauben gehalten wird, bevor Sie das Gerät loslassen.

Systemanforderungen für den Internetzugang

Damit Ihr Heim-Gateway eine für den High-Speed-Internetzugang ausreichende Leistung erbringen kann, müssen alle Internetgeräte in Ihrem System die folgenden Mindestanforderungen für Hardware und Software erfüllen.

Hinweis: Sie benötigen außerdem einen aktiven Kabeleingang und eine Internetverbindung.

Mindestsystemanforderungen für PC

- Pentium MMX 133 Prozessor oder höher
- 32 MB RAM
- Webbrowser
- CD-ROM-Laufwerk

Mindestsystemanforderungen für Macintosh

- MAC OS 7.5 oder höher
- 32 MB RAM

Systemanforderungen für eine Ethernet-Verbindung

- PC mit Microsoft Windows 2000 (oder höher) mit installiertem TCP/IP-Protokoll oder ein Apple Macintosh Computer mit installiertem TCP/IP-Protokoll
- eine aktive 10/100BASE-T Ethernet-NIC (Network Interface Card)

High-Speed-Internetdienst

Zur Nutzung Ihres Heim-Gateways benötigen Sie einen High-Speed-Internetzugang. Falls Sie noch nicht über ein Konto verfügen, müssen Sie ein Konto für den High-Speed-Internetzugang bei Ihrem Internetdienstanbieter vor Ort einrichten. Machen Sie mit dem auf Sie zutreffenden Abschnitt weiter.

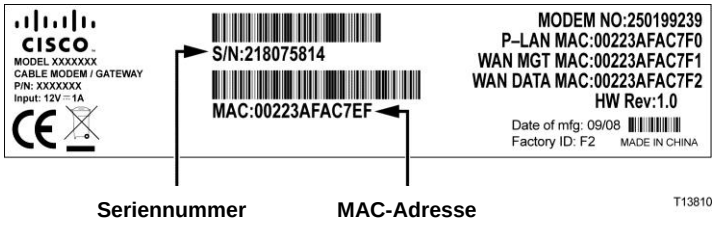
Ich habe kein Konto für den High-Speed-Internetzugang

Falls Sie *kein* Konto für den High-Speed-Internetzugang haben, richtet Ihr Dienstanbieter ein Konto für Sie ein und wird damit zu Ihrem Internetdienstanbieter (ISP). Der Internetzugang ermöglicht Ihnen, E-Mails zu senden und zu empfangen, auf das World Wide Web zuzugreifen und andere Internetdienste zu beziehen.

Zum Einrichten Ihres Kontos benötigt Ihr Dienstanbieter die folgenden Informationen:

- die Seriennummer des Gateways
- die MAC-Adresse des Gateways (Media Access Control Address)

Diese Zahlen finden Sie auf einem Barcodeetikett an Ihrem Heim-Gateway. Die Seriennummer besteht aus der Abkürzung **S/N** gefolgt von einer Reihe alphanumerischer Zeichen. Die MAC-Adresse besteht aus der Abkürzung **CM MAC** gefolgt von einer Reihe alphanumerischer Zeichen. Die folgende Abbildung zeigt ein Beispiel eines solchen Barcodeetiketts.



Schreiben Sie sich diese Nummern hier auf:

Seriennummer _____

MAC-Adresse _____

Ich habe bereits ein Konto für den High-Speed-Internetzugang

Wenn Sie bereits ein Konto für den High-Speed-Internetzugang haben, müssen Sie Ihrem Dienstanbieter die Seriennummer und die MAC-Adresse Ihres Heim-Gateways mitteilen. Informationen zur Seriennummer und der MAC-Adresse finden Sie weiter oben in diesem Abschnitt.

Hinweis: Es besteht die Möglichkeit, dass Sie mit Ihrem Heim-Gateway Ihr bisheriges E-Mail-Konto nicht mehr verwenden können. Nähere Informationen hierzu erhalten Sie von Ihrem Dienstanbieter.

Internetanschluss

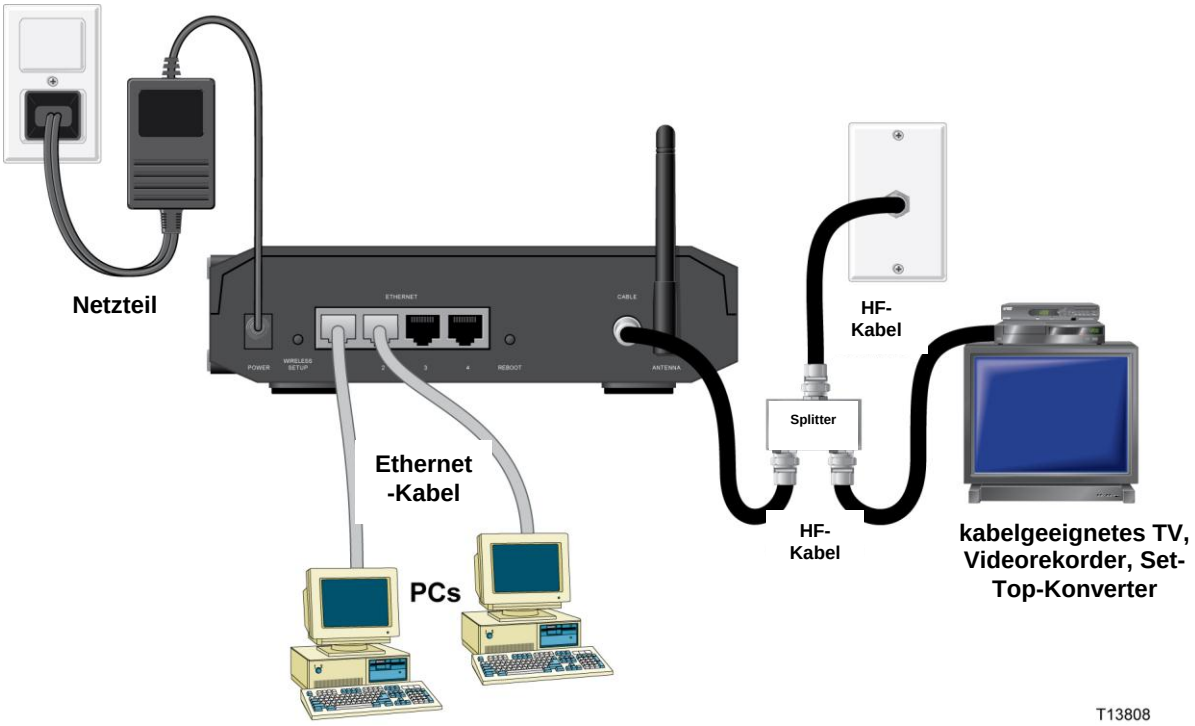
Mit Ihrem Heim-Gateway können Sie auf das Internet zugreifen, und Sie können diese Internetverbindung mit anderen Internetgeräten zuhause oder in Ihrem Büro gemeinsam nutzen. Durch die gemeinsame Nutzung einer Verbindung durch mehrere Geräte entsteht ein Netzwerk.

Anschluss und Installation von Internetgeräten

Um auf das Internet zugreifen zu können, müssen Sie Ihr Heim-Gateway anschließen und installieren. Möglicherweise bietet Ihr Dienstanbieter die Installation durch Fachpersonal an. Wenden Sie sich an Ihren Dienstanbieter vor Ort, wenn Sie weitere Hilfe benötigen.

So schließen Sie Geräte an:

Die folgende Abbildung ist ein Beispiel einer der möglichen Netzwerkkonstellationen.



Anschluss des Gateways für High-Speed-Datendienste

WARNUNG:

- **Befolgen Sie diese Schritte in der angegebenen Reihenfolge, um Verletzungen oder eine Beschädigung des Gerätes zu vermeiden.**
- **Zur Vermeidung eines Stromschlags müssen Kabel und Anschlüsse ordnungsgemäß isoliert sein.**
- **Trennen Sie das Heim-Gateway vom Stromnetz, bevor Sie andere Geräte anschließen.**

1. Schalten Sie den PC und andere Netzwerkgeräte aus und trennen Sie sie vom Stromnetz.
2. Schließen Sie das aktive HF-Koaxialkabel Ihres Dienstanbieters an den mit **CABLE** beschrifteten Koaxialanschluss auf der Rückseite des Gateways an.

   Hinweis: Wenn Sie ein Fernsehgerät, ein Digital Home Communications Terminal (DHCT), einen Set-Top-Konverter oder einen Videorekorder über dieselbe Kabelverbindung anschließen möchten, müssen Sie einen Signalsplitter installieren (nicht im Lieferumfang enthalten).
3. Verbinden Sie jetzt das eine Ende des gelben Ethernet-Kabels mit dem Ethernet-Port an Ihrem PC und das andere Ende des Kabels mit einem der **ETHERNET**-Ports am Gateway. Die Ethernet-Ports sind die gelben Anschlüsse auf der Rückseite des Gateways.
4. Verbinden Sie weitere Ethernet-Netzwerkgeräte auf dieselbe Weise mit noch nicht belegten Ethernet-Ports auf der Rückseite des Gateways.

   Hinweis: Wenn Sie mehr Ethernet-Geräte anschließen möchten, als Ports vorhanden sind, benötigen Sie einen externen Multiport-Ethernet-Switch.
5. Verbinden Sie jetzt das mitgelieferte Wechselstrom-Netzteil. Schließen Sie dazu den über ein dünnes zweiadriges Kabel mit dem Netzteil verbundenen Stecker an den schwarzen **POWER**-Anschluss auf der Rückseite des Heim-Gateways an. Stecken Sie dann den Stecker des Netzkabels in eine Steckdose, um das Gateway zu starten. Das Heim-Gateway sucht automatisch nach dem Breitband-Datennetzwerk und meldet sich dort an. Dieser Vorgang dauert etwa 2-5 Minuten. Wenn die mit POWER, DS, US und ONLINE beschrifteten LEDs auf der Vorderseite des Gateways zu blinken aufhören und ununterbrochen leuchten, ist das Gateway betriebsbereit.
6. Schließen Sie die Netzkabel Ihres PCs und der anderen Geräte in Ihrem Heimnetzwerk an und schalten Sie sie ein. Die ETHERNET-LEDs der Ports des Gateways, an denen Geräte angeschlossen sind, sollten entweder leuchten oder blinken.

7 Sobald das Gateway online ist, können die meisten Internetgeräte sofort auf das Internet zugreifen.

Hinweis: Sollte Ihr PC keinen Internetzugang haben, lesen Sie im Abschnitt ***Konfiguration des TCP/IP-Protokolls*** (Seite 108) nach, wie Sie Ihren PC für den Internetzugang konfigurieren können. Informationen zur Konfiguration der anderen Internetgeräte finden Sie im Abschnitt zur Konfiguration von DHCP oder IP-Adresse im Benutzerhandbuch oder der Betriebsanleitung dieser Geräte.

Konfiguration des DOCSIS Residential Gateway

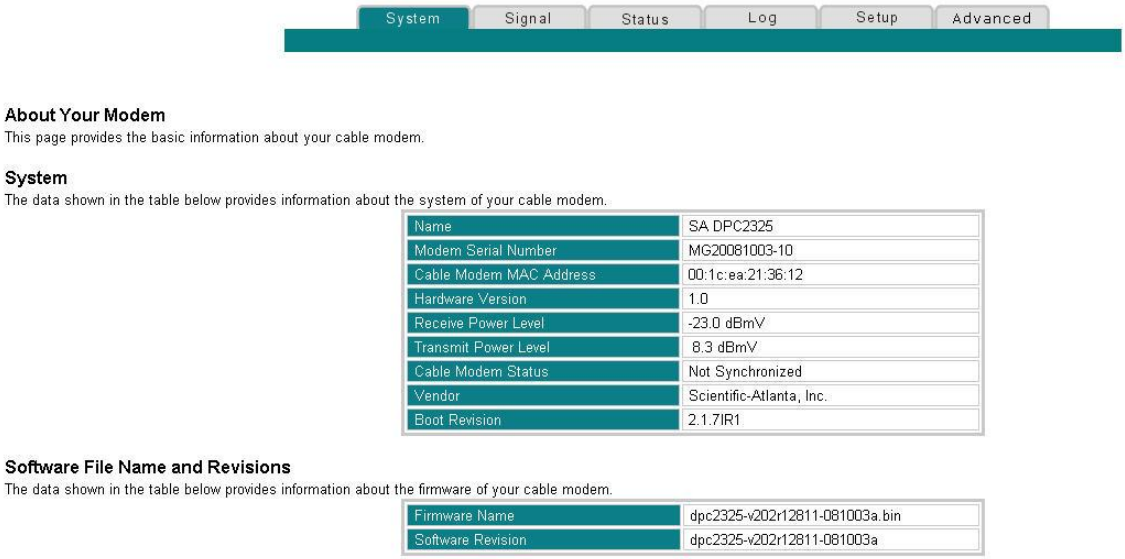
Die Konfiguration Ihres Heim-Gateways erfolgt über die Konfigurationsseiten des WebWizards. Wie Sie auf die Seiten des WebWizards zugreifen und Ihr Heim-Gateway für den ordnungsgemäßen Betrieb konfigurieren können, wird im Folgenden ausführlich beschrieben. Dieser Abschnitt enthält außerdem Beispiele und Beschreibungen der einzelnen WebWizard-Konfigurationsseiten. Anstatt die Standardeinstellungen zu verwenden, können Sie Ihr Heim-Gateway über die WebWizard-Seiten ganz Ihren Bedürfnissen anpassen. Dabei werden die WebWizard-Seiten in diesem Abschnitt in der Reihenfolge behandelt, in der sie auf der **Setup**-Seite angezeigt werden.

Wichtig: Die in diesem Abschnitt abgebildeten WebWizard-Seiten und Beispiele dienen nur der Veranschaulichung; die Seiten, die Sie im WebWizard sehen, können sich von diesen Beispielen unterscheiden.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren zur Netzwerkkonfiguration nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

„About Your Modem“ – Beispielseite

Die folgende Abbildung ist ein Beispiel der Seite „About Your Modem“.



Zugriff auf das Heim-Gateway

Zur Konfiguration Ihres Heim-Gateways müssen Sie über den auf Ihrem PC installierten Webbrowser auf den WebWizard zugreifen. Führen Sie dazu die folgenden Schritte durch:

1. Öffnen Sie den Webbrowser auf Ihrem PC.
2. Geben Sie die folgende IP-Adresse ein und klicken Sie anschließend auf **Go**: **http://192.168.0.1**.
3. Der Webbrowser öffnet den WebWizard und zeigt standardmäßig die Seite „**About Your Modem**“ an. Auf dieser Seite finden Sie Informationen über Ihr Kabelmodem sowie eine Reihe Registerkarten, über die Sie auf die anderen Konfigurations- und Betriebsfunktionen des WebWizards zugreifen können.

Beschreibung der Seite „About Your Modem“

In der folgenden Tabelle werden die einzelnen Felder der Seite „About Your Modem“ beschrieben.

Feldname	Beschreibung
Name	Name des Heim-Gateways
Modem Serial Number	Seriennummer des Modems. Eine eindeutige Reihe alphanumerischer Zeichen, die jedem Modem während der Herstellung zugewiesen wird.
Cable Modem MAC Address	MAC-Adresse des Kabelmodems. Eine eindeutige alphanumerische Adresse der Koaxialschnittstelle, über die die Verbindung mit dem Cable Modem Termination System (CMTS) an der Kopfstelle (Headend) hergestellt wird. Eine MAC-Adresse (Media Access Control Address) ist eine Hardware-Adresse, anhand der die einzelnen Knoten eines Netzwerks eindeutig identifiziert werden können.
Hardware Version	Die Versionsnummer des Leiterplattendesigns.
Receive Power Level	Die Empfangsleistung des Downstream-CMTS-Trägers.
Transmit Power Level	Die Upstream-Sendeleistung.

Feldname	Beschreibung
Cable Modem Status	Status des Kabelmodems. Angezeigt wird einer der folgenden möglichen aktuellen Status des Modems: ■ other (anderer) ■ notReady (nicht bereit) ■ notSynchronized (nicht synchronisiert) ■ phySynchronized (PHY synchronisiert) ■ usParametersAcquired (US-Parameter erfasst) ■ rangingComplete (Ranging abgeschlossen) ■ ipComplete (IP abgeschlossen) ■ todEstablished ■ securityEstablished (Sicherheit aufgebaut) ■ psrsmTransferComplete (psrsm-Übertragung abgeschlossen) ■ registrationComplete (Registrierung abgeschlossen) ■ operational (betriebsbereit) ■ accessDenied (Zugriff verweigert)
Vendor	Name des Herstellers
Boot Revision	Revisionsversion des Bootcodes

Dateiname und Revision der Software

Feldname	Beschreibung
Firmware Name	Name der Firmware
Software Revision	Revisionsversion der Firmware

Konfigurationsoptionen

Über die Setup-Seite können Sie auf die verschiedenen Konfigurationsoptionen Ihres Heim-Gateways zu greifen. Ausführliche Beschreibungen der einzelnen Konfigurationsoptionen finden Sie weiter unten in diesem Handbuch.

Wichtig: Wenn Sie den WebWizard durch Eingabe der IP-Adresse 192.168.0.1 in die Adresszeile Ihres Webbrowsers geöffnet haben, während das Gateway online ist, wird ein der folgenden Abbildung ähnliches Authentifizierungsfenster angezeigt:

Geben Sie Ihr Kennwort ein und klicken Sie auf **OK**, um die Setup-Seite aufzurufen.

Erstbenutzer

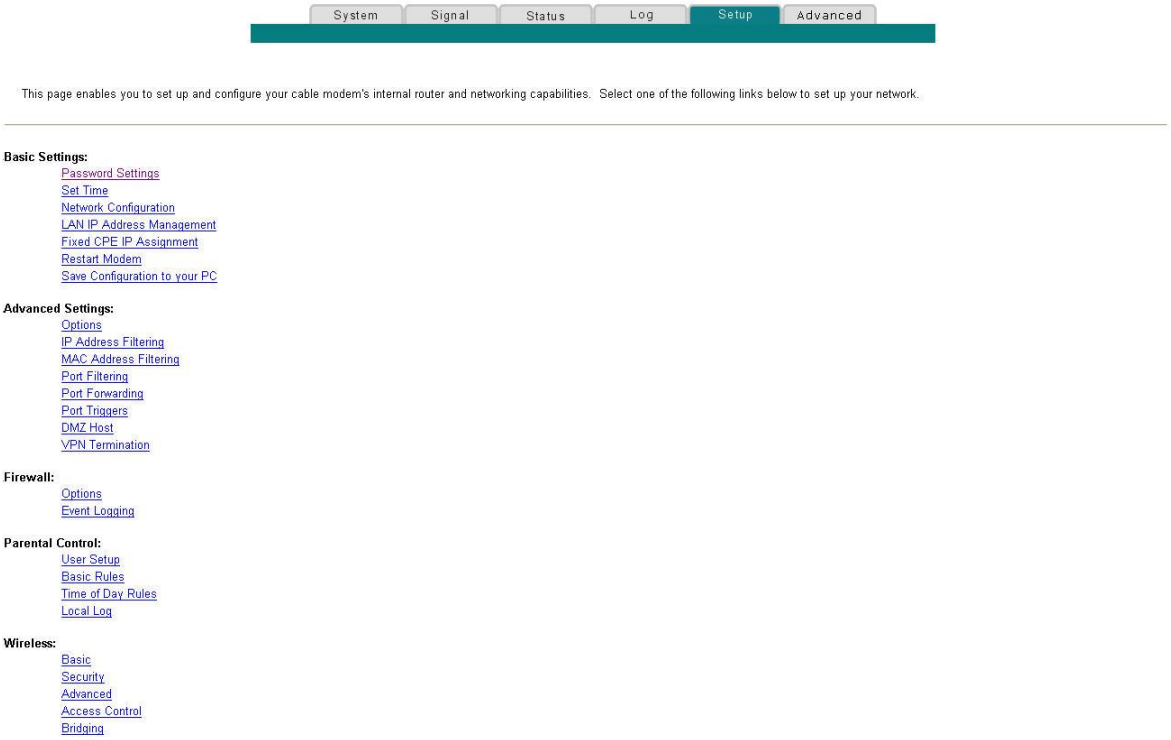
Das Gateway wird vom Hersteller ohne vordefiniertes oder Standardkennwort geliefert.

Lassen Sie die Felder für Benutzernamen und Kennwort leer. Klicken Sie dann auf **OK**, um zur Seite mit den Kennworteinstellungen weitergeleitet zu werden.

Hinweis: Sie werden zur Einrichtung eines Kennworts aufgefordert. Um unbefugten Zugriff auf die Einstellungen Ihres Gateways zu verhindern, sollten Sie unbedingt ein Kennwort einrichten. Wenn Sie kein Kennwort eingeben, wird diese Seite bei jedem Öffnen der Setup-Seiten angezeigt. Anleitungen zum Einrichten Ihres Kennworts finden Sie im Abschnitt ***Konfiguration Ihrer Kennworteinstellungen*** (Seite 34). Wenn Sie den Kennwortschutz nicht nutzen möchten, klicken Sie auf die Registerkarte **Setup** oben auf der Seite „Password Settings“, um fortzufahren.

Die Seite „Setup“

Die folgende Abbildung ist ein Beispiel der Seite „Setup“.



Abschnitte der Setup-Seite

Die Setup-Seite ist in die folgenden Abschnitte unterteilt:

- Basic Settings (Grundeinstellungen)
- Advance Settings (Erweiterte Einstellungen)
- Firewall
- Parental Control (Kinderschutz)
- Wireless

Klicken Sie auf der Setup-Seite auf eine der in diesem Abschnitt aufgeführten Optionen, um die WebWizard-Seite für diese Einstellungen zu öffnen. Im Folgenden werden die in den einzelnen Abschnitten verfügbaren Optionen beschrieben.

Basic Settings (Grundeinstellungen)

Die folgende Tabelle enthält eine Beschreibung der Seiten, auf die Sie über den Abschnitt „Basic Settings“ der Setup-Seite zugreifen können.

Feldname	Beschreibung
Password Settings	Kennworteinstellungen. Klicken Sie auf diesen Link, um Ihre Kennworteinstellungen einzurichten oder zu ändern.
Set Time	Uhrzeiteinstellung. Klicken Sie auf diesen Link, um die Synchronisierung der Uhrzeit durch das Network Time Protocol zu aktivieren bzw. deaktivieren.
Network Configuration	Netzwerkkonfiguration. Klicken Sie auf diesen Link, um die Grundeinstellungen Ihres Netzwerks einzugeben oder zu ändern.
LAN IP Address Management	Verwaltung der LAN-IP-Adressen. Klicken Sie auf diesen Link, um die Zuweisung und Verwaltung der Internetprotokolladressen (IP-Adressen) in Ihrem Netzwerk zu konfigurieren.
Fixed CPE IP Assignment	Zuweisung statischer IP-Adressen für CPE (Customer Premises Equipment, Endgeräte). Klicken Sie auf diesen Link, um im DHCP-Pool IP-Adressen zu reservieren, die in Ihrem lokalen Netzwerk als statische IP-Adressen verwendet werden.
Restart Modem	Modem-Neustart. Klicken Sie auf diesen Link, um Ihr Heim-Gateway neu zu starten.
Save Configuration to your PC	Konfiguration auf PC speichern. Klicken Sie auf diesen Link, um die Residential Gateway-Konfiguration Ihres Kabelmodems auf Ihrem lokalen PC zu speichern oder gegebenenfalls die RG-Konfiguration auf Ihrem Heim-Gateway wieder herzustellen.

Advance Settings (Erweiterte Einstellungen)

Die folgende Tabelle enthält eine Beschreibung der Seiten, auf die Sie über den Abschnitt „Advanced Settings“ der Setup-Seite zugreifen können.

Feldname	Beschreibung
Options	Optionen. Klicken Sie auf diesen Link, um die erweiterten Funktionen Ihres Netzwerks zu aktivieren bzw. deaktivieren.
IP Address Filtering	IP-Adressfilter. Klicken Sie auf diesen Link, um die IP-Adressfilter zu konfigurieren. Diese Filter verhindern, dass bestimmte IP-Adressen auf das Internet zugreifen.

Feldname	Beschreibung
MAC Address Filtering	MAC-Adressfilter. Klicken Sie auf diesen Link, um die MAC-Adressfilter zu konfigurieren. Diese Filter verhindern, dass bestimmte MAC-Adressen auf das Internet zugreifen.
Port Filtering	Portfilter. Klicken Sie auf diesen Link, um die Filter für das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) zu konfigurieren. Diese Filter verhindern, dass bestimmte TCP/UDP-Portbereiche auf das Internet zugreifen.
Port Forwarding	Portweiterleitung. Klicken Sie auf diesen Link, um die Portweiterleitung für lokale IP-Adressen zu konfigurieren. Die Portweiterleitung ermöglicht es Ihnen, durch Zuordnung von TCP/UDP-Ports zu lokalen PCs oder den IP-Adressen anderer Geräte einen Server auf dem lokalen Netzwerk (LAN) auszuführen. Dabei handelt es sich um eine statische Einstellung, durch die Ports ständig offen gehalten werden.
Port Triggers	Klicken Sie auf diesen Link, um TCP/UDP-Port-Trigger zu konfigurieren. Port-Trigger funktionieren auf ähnliche Weise wie die Portweiterleitung; im Gegensatz dazu haben sie jedoch eine dynamische Funktion. Das heißt, die Ports werden nicht offen gehalten, sondern sie schließen sich, wenn innerhalb eines Zeitraums von 10 Minuten auf den ausgewählten Ports keine ausgehenden Daten festgestellt werden.

Feldname	Beschreibung
DMZ Host (Demilitarized Zone)	Klicken Sie auf diesen Link, um eine IP-Adresse zu konfigurieren, die über das Wide Area Network (WAN) sichtbar ist. Ein DMZ-Host wird häufig als „exposed host“ (etwa: ungeschützter Host) bezeichnet. Er ermöglicht Ihnen, einen Standardempfänger für den WAN-Verkehr anzugeben, der durch Network Address Translation (NAT) keinem anderen bekannten lokalen PC zugeordnet werden kann. Eine „entmilitarisierte Zone“ wird beispielsweise von einem Unternehmen eingesetzt, das seine eigenen Internetdienste hosten möchte, ohne dabei nicht autorisierten Zugang zu seinem privaten Netzwerk aufgeben zu müssen. Dies geschieht, indem eine IP-Adresse ungeschützt bleibt, während alle anderen IP-Adressen geschützt werden. Die DMZ befindet sich zwischen dem Internet und der Verteidigungslinie eines internen Netzwerks, die aus einer Kombination von Firewalls und Bastion Hosts besteht. Normalerweise enthält die DMZ Geräte wie Webserver (HTTP-Server), FTP-Server, SMTP-Server (E-Mail-Server) und DNS-Server (Domain Name System Server).
VPN Termination	Klicken Sie auf diesen Link, um VPN-Protokolle (Virtual Private Network) zu erstellen, zu konfigurieren und zu kontrollieren sowie Internet Protocol Security (IPsec) VPN-Tunnel zu verwalten.

Firewall

Die folgende Tabelle enthält eine Beschreibung der Seiten, auf die Sie über den Abschnitt „Firewall“ der Setup-Seite zugreifen können.

Feldname	Beschreibung
Options	Optionen. Klicken Sie auf diesen Link, um Webseiten-Filter und Firewall-Schutz zu konfigurieren.
Event Logging	Ereignisprotokollierung. Klicken Sie auf diesen Link, um auf das Firewall-Ereignisprotokoll zuzugreifen und Ihre E-Mail-Adresse einzugeben, wenn Sie bei Firewall-Angriffen durch Hacker E-Mail-Benachrichtigungen erhalten möchten.

Parental Control (Kinderschutz)

Die folgende Tabelle enthält eine Beschreibung der Seiten, auf die Sie über den Abschnitt „Parental Control“ der Setup-Seite zugreifen können.

Feldname	Beschreibung
User Setup	Benutzer-Setup. Klicken Sie auf diesen Link, um Benutzerprofile hinzuzufügen oder zu löschen sowie Zugriffsregeln auf diese Benutzer anzuwenden.
Basic Rules	Grundregeln. Klicken Sie auf diesen Link, um Zugriffsregeln einzurichten, die bestimmte Internetinhalte und Websites blockieren.
Time of Day Rules	Tageszeitenregeln. Klicken Sie auf diesen Link, um Internetzugriffsfilter zu konfigurieren, die zu von Ihnen festgelegten Tageszeiten sämtlichen Internetverkehr von und zu bestimmten Netzwerkgeräten blockieren.
Local Log	Lokales Protokoll. Klicken Sie auf diesen Link, um im Kinderschutz-Ereignisprotokoll festgehaltene Ereignisse anzuzeigen.

Wireless

Die folgende Tabelle enthält eine Beschreibung der Seiten, auf die Sie über den Abschnitt „Wireless“ der Setup-Seite zugreifen können.

Feldname	Beschreibung
Basic	Standard. Klicken Sie auf diesen Link, um die Parameter Ihres Wireless Access Point (WAP) wie beispielsweise die SSID (Service Set Identifier) und den Kanal zu konfigurieren.
Security	Sicherheit. Klicken Sie auf diesen Link, um WAP-Authentifizierung und Datenverschlüsselung zu konfigurieren. Durch Verwendung von Verschlüsselung und Authentifizierung können Sie unbefugten Zugriff auf Ihre kabellosen Geräte verhindern.
Advanced	Erweitert. Klicken Sie auf diesen Link, um Ihre WAP-Datenraten und Wi-Fi-Grenzwerte zu konfigurieren.

Feldname	Beschreibung
Access Control	Zugriffskontrolle. Klicken Sie auf diesen Link, um durch Konfigurierung des WAP den Zugriff auf ausgewählte kabellose Client-Geräte zu beschränken. Befugte Clients werden anhand ihrer MAC-Adresse ausgewählt. Klicken Sie auf diesen Link, um für die Authentifizierung „Open System“ (offenes System) oder „Shared Key“ (gemeinsamer Schlüssel) auszuwählen sowie die Unterdrückung der WAP SSID zu aktivieren bzw. deaktivieren.
Bridging	Überbrückung. Klicken Sie auf diesen Link, um ein Wireless Distribution System (WDS) in Ihrem Netzwerk einzurichten.

Konfiguration der Kennworteinstellungen

Auf der Seite „Basic Settings - Password Settings“ können Sie ein Kennwort einrichten oder ändern, um den unbefugten Zugriff auf die Einstellungen Ihres Heim-Gateways zu verhindern. Klicken Sie im Abschnitt „Basic Settings“ der Setup-Seite auf „**Password Settings**“, um die Seite mit den Kennworteinstellungen aufzurufen.

Hinweise:

- Der Hersteller hat auf Ihrem Gateway-Modem kein Kennwort aktiviert. Um zu verhindern, dass unbefugte Benutzer die Einstellungen Ihres Netzwerks ändern, sollten Sie unbedingt ein Kennwort einrichten.
- Wenn Sie sich für die Verwendung eines Kennworts entscheiden, sollten Sie ein Kennwort auswählen, an das Sie sich leicht erinnern können. Sie dürfen Ihr Kennwort auf keinen Fall vergessen!

Die Seite „Setup Basic Settings - Password Settings“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - Password Settings“.

So richten Sie Ihr Kennwort ein:

1. Um ein Kennwort einzurichten, geben Sie zuerst Ihr aktuelles Kennwort in das Feld „**Current Password**“ ein.
2. Geben Sie als Nächstes Ihr neues Kennwort in das Feld „**New Password**“ ein. Geben Sie zur Bestätigung Ihr neues Kennwort noch einmal in das Feld „**Re-Enter New Password**“ ein.
3. Klicken Sie auf „**Apply**“, um Ihr Kennwort zu speichern. Daraufhin wird eine Webseite mit der Meldung angezeigt, dass Sie Ihr Kennwort erfolgreich eingerichtet haben.
4. Klicken Sie auf die Registerkarte „**Setup**“, um mit dem Setup Ihres Gateways fortzufahren. Das Dialogfeld zur Eingabe von Benutzernamen und Kennwort wird angezeigt (siehe unten).
5. Geben Sie Ihr Kennwort ein und klicken Sie auf **LOGIN**, um auf die Setup-Seite zu gelangen.

Hinweis: Wenn Sie ein Kennwort einrichten, wird jedes Mal, wenn Sie anschließend auf die Setup-Seiten zugreifen, ein Fenster ähnlich dem unten abgebildeten angezeigt. Sie dürfen Ihr Kennwort auf keinen Fall vergessen! Schreiben Sie sich Ihr Kennwort auf und bewahren Sie es an einem sicheren Ort auf, der nur Ihnen bekannt ist.

Konfiguration der Uhrzeitsynchronisierung im Netzwerk

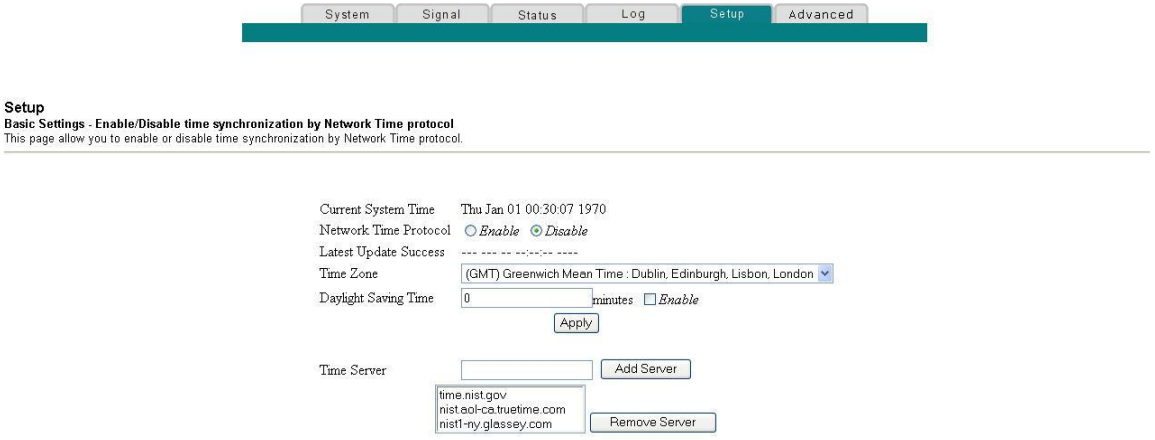
Auf der Seite „Basic Settings Enable/Disable time synchronization by Network Time protocol“ können Sie das Protokoll zur Uhrzeitsynchronisierung anhand der Netzwerkuhrzeit aktivieren bzw. deaktivieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren zur Uhrzeitkonfiguration nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen der Uhrzeitsynchronisierung Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Basic Settings“ auf der Setup-Seite auf „**Set Time**“, um die Seite „Basic Settings Enable/Disable time synchronization by Network Time protocol“ zu öffnen.

Die Seite „Setup Basic Settings - Enable/Disable Time Synchronization by Network Time Protocol“

Die folgende Abbildung zeigt die anfängliche Ansicht der Seite „Setup Basic Settings Enable/Disable time synchronization by Network Time protocol“.



Beschreibung der Seite „Setup Basic Settings - Enable/Disable Time Synchronization by Network Time Protocol“

Die folgende Tabelle enthält eine Beschreibung der Felder auf der Seite „Setup Basic Settings Enable/Disable time synchronization by Network Time protocol“.

Feldname	Beschreibung
Current System Time	Aktuelle Systemzeit. Zeigt die aktuelle Uhrzeit und das aktuelle Datum des Systems an.
Network Time Protocol	Netzwerkzeitprotokoll. Ermöglicht die Aktivierung bzw. Deaktivierung des Netzwerkzeitprotokolls. **Hinweis:** Das Heim-Gateway verwendet automatisch den Zeitserver Ihres Breitband-Netzwerks. Sollte keine aktuelle Uhrzeit angezeigt werden oder die Netzwerkzeit inkorrekt sein, können Sie das Netzwerkzeitprotokoll aktivieren, um einen öffentlichen Internet-Zeitserver für das Einstellen der Uhr des Gateways zu benutzen.
Latest Update Success	Letzte erfolgreiche Aktualisierung. Zeigt die Uhrzeit und das Datum der letzten erfolgreichen Aktualisierung der Zeiteinstellungen an.
Time Zone	Zeigt die aktuelle Zeitzone an. Aus der Dropdown-Liste können Sie Ihre Zeitzone auswählen.
Daylight Saving Time	Sommerzeit. Ermöglicht die Anpassung der Uhrzeit an die Sommerzeit. Klicken Sie auf das Kontrollkästchen „**Enable**“, um diese Einstellung zu aktivieren bzw. zu deaktivieren. **Hinweis:** Sollte der Zeitunterschied der Sommerzeit nicht 60 Minuten entsprechen, geben Sie den Zeitunterschied im Minutenfeld ein.
Time Server	Zeitserver. Geben Sie in dieses Feld die URL oder die IP-Adresse eines Zeitservers ein, um sieder Liste hinzuzufügen, oder löschen Sie diese Informationen aus der Liste, um einen Zeitserver zu entfernen. Bei Verwendung des Netzwerkzeitprotokolls können mehrere Zeitserver angegeben werden, von denen das Gateway die Uhrzeit abruft. Das Gateway geht die aufgeführten Zeitserver der Reihe nach durch, bis es die aktuelle Uhrzeit erhält. Drei der häufig verwendeten öffentlichen Zeitserver sind als Standardserver eingetragen.

Schaltflächen

Schaltfläche	Beschreibung
Apply	Anwenden. Speichert alle hinzugefügten, bearbeiteten und geänderten Daten.
Add Server	Server hinzufügen. Ermöglicht das Hinzufügen eines Netzwerk-Zeitservers.
Remove Server	Ermöglicht das Entfernen eines Netzwerk-Zeitservers.

Unter normalen Umständen sollten Sie die Standard-Netzwerkeinstellungen verwenden. Sollte die Netzwerkzeit nicht Ihrer lokalen Zeit entsprechen oder Ihr System für einen ordnungsgemäßen Betrieb andere Einstellungen benötigen, können Sie die Standard-Netzwerkeinstellungen über die Seite „Setup Basic Settings - Network Configuration“ ändern.

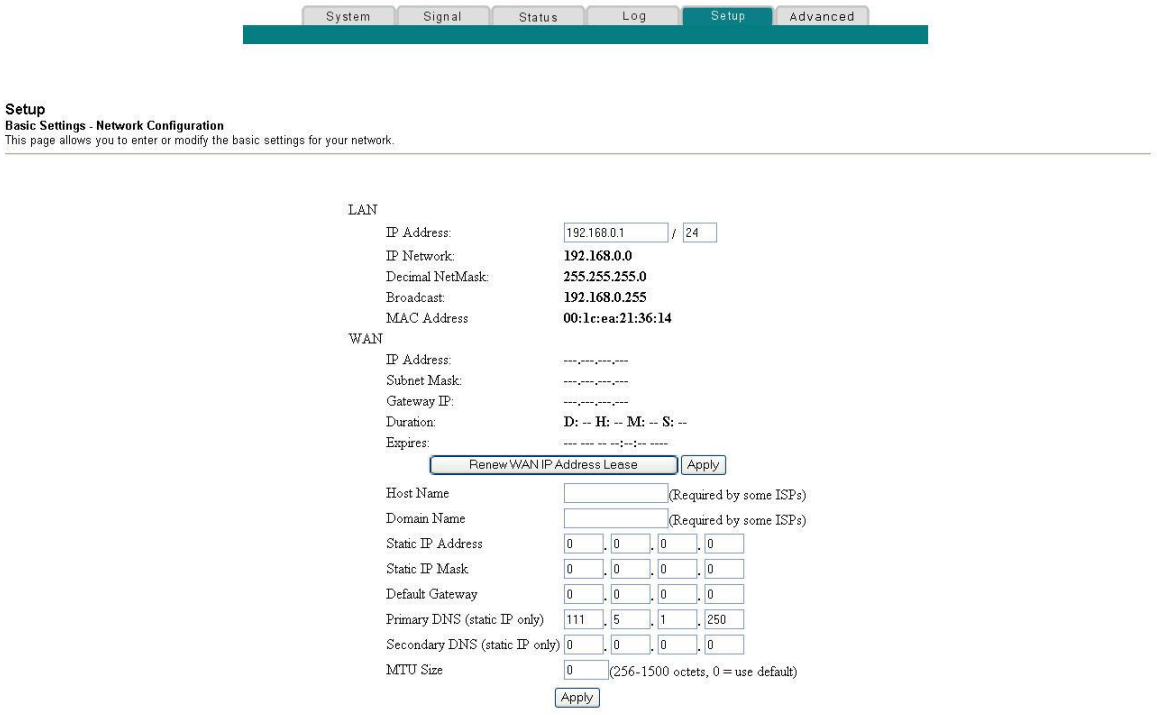
Konfiguration der Netzwerkeinstellungen

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren zur Netzwerkkonfiguration nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Basic Settings“ auf der Setup-Seite auf „**Network Configuration**“, um die Seite „Setup Basic Settings - Network Configuration“ aufzurufen.

Die Seite „Setup Basic Settings - Network Configuration“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - Network Configuration“.



Beschreibung der Seite „Setup Basic Settings - Network Configuration“

Die folgende Tabelle enthält eine Beschreibung der auf der Seite „Setup Basic Settings - Network Configuration“ verwendeten Felder.

Feldname	Beschreibung
LAN IP Address	Zeigt die grundlegende IP-Adresse des privaten Heim-LANs und die IP-Adresse des WebWizards an. Ihr Heim-Gateway weist unter Verwendung seines internen DCCP-Servers den mit Ihrem Netzwerk verbundenen Computern private IP-Adressen zu.
IP Network	Zeigt die Adresse des privaten LAN IP-Netzwerks an.
Decimal Netmask	Dezimale Netzmaske. Zeigt die Netzmaske des privaten LAN IP-Netzwerks an.
Broadcast	Übertragung. Zeigt die übertragene IP-Adresse an.
MAC Address	Zeigt die MAC-Adresse des WAN an. Die dem WAN vom Hersteller zugewiesene MAC-Adresse wird auch als WAN MGT MAC bezeichnet.
WAN IP Address	Zeigt die Ihrem Gateway von Ihrem ISP zugewiesene öffentliche IP-Adresse an. Ihr ISP weist dem WAN-Port automatisch eine öffentliche IP-Adresse zu, solange nicht wie im Folgenden beschrieben eine statische IP-Adresse eingerichtet wird. Alle PCs in Ihrem privaten LAN benutzen dieselbe WAN IP-Adresse, um auf das Internet zuzugreifen.
Subnet Mask	Subnetzmaske. Zeigt die Subnetzmaske für Ihren WAN-Port an. Ihr ISP weist dem WAN-Port diese Adresse automatisch zu, solange nicht wie im Folgenden beschrieben eine statische IP-Adresse eingerichtet wird.
Gateway IP	Zeigt eine Gateway IP-Adresse für Ihren WAN-Port an. Ihr ISP weist dem WAN-Port diese Adresse automatisch zu, solange nicht wie im Folgenden beschrieben eine statische IP-Adresse eingerichtet wird.
Duration	Gültigkeitsdauer. Zeigt an, wie lange Ihre WAN IP-Adresse gültig ist.
Expires	Gültigkeitsende. Zeigt mit Datum und Uhrzeit an, wann Ihre WAN IP-Adresse ungültig wird.
Host Name	Zeigt den Hostnamen an, der normalerweise von Ihrem ISP auf Ihr Gateway heruntergeladen wird. Einige ISPs verlangen jedoch, dass diese Informationen manuell eingegeben werden. In diesem Fall stellt Ihnen Ihr ISP die für dieses Feld erforderlichen Informationen bereit.
Domain Name	Zeigt den Domänennamen an, der normalerweise von Ihrem ISP auf Ihr Gateway heruntergeladen wird. Einige ISPs verlangen jedoch, dass diese Informationen manuell eingegeben werden. In diesem Fall stellt Ihnen Ihr ISP die für dieses Feld erforderlichen Informationen bereit.

Feldname	Beschreibung
Static IP Address	Die statische IP-Adresse muss manuell eingegeben werden. Ihr ISP stellt Ihnen die für dieses Feld benötigten Informationen bereit. **Hinweis:** Bevor die statische IP-Adresse einsatzbereit ist, müssen Sie zuerst die IP-Adresse, die Subnetzmaske und ein Standard-Gateway eingeben.
Static IP Mask	Die statische IP-Maske muss manuell eingegeben werden. Ihr ISP stellt Ihnen die für dieses Feld benötigten Informationen bereit.
Default Gateway	Das Standard-Gateway muss manuell eingegeben werden. Ihr ISP stellt Ihnen die für dieses Feld benötigten Informationen bereit.
Primary DNS (static IP only)	Primärer Domänennamen-Server (nur für statische IP-Adressen). Der primäre DNS muss manuell eingegeben werden. Ihr ISP stellt Ihnen die für dieses Feld benötigten Informationen bereit.
Secondary DNS (static IP only)	Sekundärer Domänennamen-Server (nur für statische IP-Adressen). Der sekundäre DNS muss manuell eingegeben werden. Ihr ISP stellt Ihnen die für dieses Feld benötigten Informationen bereit.
MTU Size	Größe der Maximum Transmission Unit. Legt die maximale Größe der über die Netzwerkschnittstelle übertragenen Datenpakete fest. Der Standardwert ist 0 (null). **Wichtig:** Dieser Wert sollte nur von erfahrenen Benutzern geändert werden.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Basic Settings – Network Configuration“ angezeigt.

Schaltfläche	Beschreibung
Renew WAN IP Address Lease	WAN IP-Adresse verlängern. Erzwingt Ausgabe und Verlängerung Ihrer WAN IP-Adresse.
Apply	Anwenden. Speichert die von Ihnen eingegebenen Werte, ohne das Fenster zu schließen.

Konfiguration und Verwaltung der IP-Adressen

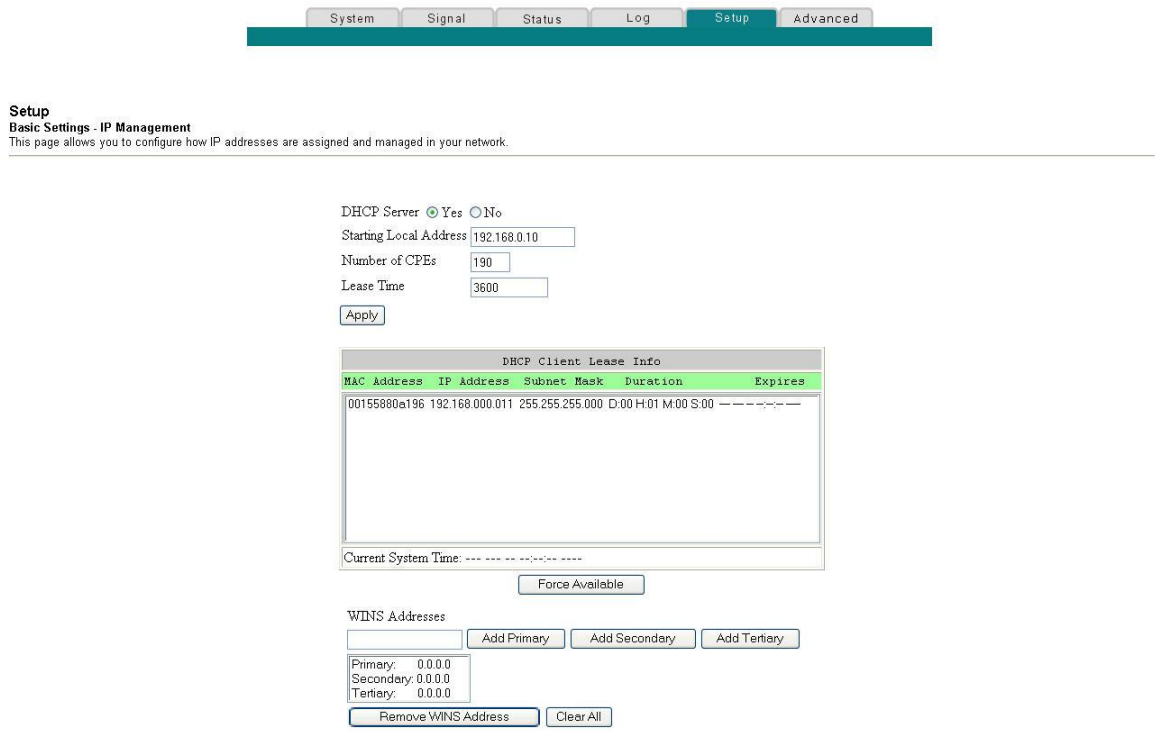
Auf der Seite „Setup Basic Settings - IP Management“ können Sie konfigurieren, wie Ihr System IP-Adressen in Ihrem Netzwerk verwaltet und zuweist.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren zur Verwaltung von IP-Adressen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways zur IP-Verwaltung ändern.

Klicken Sie im Abschnitt „Basic Settings“ auf der Setup-Seite auf „**LAN IP Address Management**“, um die Seite „Setup Basic Settings - IP Management“ aufzurufen.

Die Seite „Setup Basic Settings - IP Management“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - IP Management“.



Beschreibung der Seite „Setup Basic Settings - IP Management“

Die folgenden Tabellen enthalten Beschreibungen der auf der Seite „Setup Basic Settings - IP Management“ verwendeten Felder.

Feldname	Beschreibung
DHCP Server	Ermöglicht die Aktivierung bzw. Deaktivierung des DHCP-Servers im Heim-Gateway.
Starting Local Address	Lokale Startadresse. Zeigt die Startadresse an, die bei der Zuweisung von privaten LAN IP-Adressen durch den integrierten DHCP-Server verwendet wird. Im abgebildeten Beispiel können Adressen zwischen 2 und 9 für Geräte in Ihrem privaten LAN verwendet werden, die eine feste IP-Adresse verwenden. Dazu gehören beispielsweise Drucker oder auch ein Gerät, das als DMZ-Host dient. **Hinweis:** Die auf 1 endende LAN IP-Adresse ist für den internen Gateway-Server reserviert. Die auf 255 endende LAN IP-Adresse ist ebenfalls reserviert und sollte nicht für Endgeräte verwendet werden.
Number of CPEs	Anzahl der Endgeräte (CPE). Geben Sie die Höchstzahl der zur Verbindung mit dem privaten LAN zugelassenen Geräte an. **Hinweis:** Die Werkseinstellung ist 245. Die Höchstzahl der Geräte beträgt 253. Diese Zahl ergibt sich aus der Gesamtzahl aller für statische IP-Adressen reservierten Adressen, beispielsweise die Summe der IP-Adressen zwischen 2, dem im Feld „Starting Local Address“ eingegebenen Wert und dem im Feld „Number of CPEs“ eingegebenen Wert. **Hinweis:** Die Summe der in den Feldern „Starting Local Address“ und „Number of CPEs“ eingegebenen Werte darf 255 nicht überschreiten.
DHCP Client Lease Info	Lease-Info der DHCP-Clients. Zeigt die MAC-Adresse, die IP-Adresse, die Subnetzmaske, die Gültigkeitsdauer und das Gültigkeitsende aller Geräte an, denen vom integrierten DHCP-Server eine IP-Adresse zugewiesen worden ist. Dieses Feld zeigt ebenfalls die aktuelle Uhrzeit und das aktuelle Datum des Systems an.
WINS Addresses	Ermöglicht die manuelle Eingabe von Windows Internet Name Server (WINS) Serveradressen.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Basic Settings - IP Management“ angezeigt.

Schaltfläche	Beschreibung
Apply	Anwenden. Speichert die von Ihnen eingegebenen Werte, ohne das Fenster zu schließen.
Force Available	Verfügbare Adresse erzwingen. Erzwingt die Freigabe einer IP-Adresse zur erneuten Verwendung.
Add Primary	Primären Server hinzufügen. Speichert die WINS-Adresse des ersten Servers.
Add Secondary	Sekundären Server hinzufügen. Speichert die WINS-Adresse des zweiten Servers.
Add Tertiary	Tertiären Server hinzufügen. Speichert die WINS-Adresse des dritten Servers.
Remove WINS Address	WINS-Adresse entfernen. Entfernt die ausgewählte WINS-Adresse.
Clear All	Alle löschen. Entfernt alle definierten WINS-Adressen.

Reservierung von IP-Adressen

Auf der Seite „Setup Basic Settings - Fixed CPE IP Assignment“ können Sie IP-Adressen reservieren. Mit dieser Funktion können Sie allen Geräten in Ihrem Netzwerk eine feste IP-Adresse zuweisen, indem Sie auf Ihrem PC oder anderen Netzwerkgeräten statische IP-Adressen einrichten.

Diese Adressen werden aus dem Pool der IP-Adressen entfernt, auf die der DHCP-Server Ihres Gateways zugreift, wenn er den mit Ihrem lokalen Netzwerk verbundenen Geräten IP-Adressen zuweist.

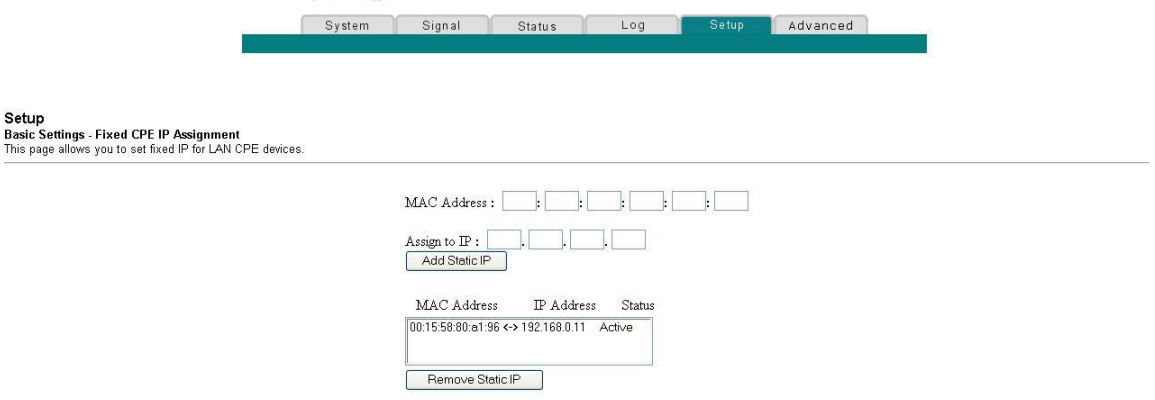
Die Reservierung von IP-Adressen hilft dabei, Konflikte von IP-Adressen im Netzwerk – wenn beispielsweise zwei Geräte dieselbe IP-Adresse verwenden – zu vermeiden. Wenn Sie einen DMZ-Host verwenden, sollte die IP-Adresse des DMZ-Hosts immer dieselbe sein.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren zur Zuweisung fester IP-Adressen an Ihre Geräte nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Basic Settings“ auf der Setup-Seite auf „**Fixed CPE IP Assignment**“, um die Seite „Setup Basic Settings - Fixed CPE IP Assignment“ aufzurufen.

Die Seite „Setup Basic Settings - Fixed CPE IP Assignment“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - Fixed CPE IP Assignment“.



Beschreibung der Seite „Setup Basic Settings - Fixed CPE IP Assignment“

Die folgenden Tabellen enthalten Beschreibungen der auf der Seite „Setup Basic Settings - Fixed CPE IP Assignment“ verwendeten Felder.

Feldname	Beschreibung
MAC Address	Die MAC-Adresse des PCs oder Gerätes (beispielsweise eines Druckers), für den bzw. das Sie eine bestimmte IP-Adresse im Netzwerk reservieren möchten.
Assign to IP	Die dem PC oder Gerät, für den bzw. das Sie eine bestimmte IP-Adresse im Netzwerk reservieren möchten, zugewiesene IP-Adresse. Dabei können nur MAC-Adressen zugewiesen werden, die innerhalb des Bereichs des DHCP-Adresspools des Gateways liegen. **Hinweis:** Die werkseitige Konfiguration Ihres Gateways sieht die IP-Adressen von 192.168.0.2 bis 192.168.0.9 für statische IP-Adressen vor.

Schaltflächen

Schaltfläche	Beschreibung
Add Static IP	Statische IP hinzufügen. Fügt der Liste zugewiesener IP-Adressen die statische IP-Adresse hinzu.
Remove Static IP	Statische IP entfernen. Entfernt die statische IP-Adresse aus der Liste zugewiesener IP-Adressen.

Neustart des Gateway-Modems

Von der Seite „Setup Basic Settings - Restart Cable Modem“ aus können Sie Ihr Kabelmodem neu starten.

1. Klicken Sie im Abschnitt „Basic Settings“ der Setup-Seite auf „**Restart Modem**“, um die Seite „Basic Settings - Restart Cable Modem“ aufzurufen.
2. Klicken Sie auf „**Reboot Cable Modem**“, um das Gateway-Modem neu zu starten.

Hinweis: Durch einen Neustart Ihres Gateway-Modems wird keine der Einstellungen zurückgesetzt.

Die Seite „Setup Basic Settings - Restart Cable Modem“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - Restart Cable Modem“.

Speichern Ihrer Konfiguration

Auf der Seite „Setup Basic Settings - Save RG Configuration to Local PC“ können Sie die aktuellen Einstellungen Ihres Heim-Gateways auf der Festplatteplatte Ihres PCs oder einem Datenträger speichern. Mithilfe dieser gespeicherten Daten können Sie bei Bedarf die Konfiguration Ihres Heim-Gateways wiederherstellen.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Verfahren nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Basic Settings“ auf der Setup-Seite auf „**Save Configuration to your PC**“, um die Seite „Setup Basic Settings - Save RG Configuration to Local PC“ aufzurufen.

Die Seite „Setup Basic Settings - Save RG Configuration to Local PC“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Basic Settings - Save RG Configuration to Local PC“.

Klicken Sie auf das Diskettensymbol im unteren Teil des Bildschirms, um Ihre aktuellen Einstellungen auf Ihrem Computer zu speichern. Sie werden zur Eingabe eines Dateinamens und des Speicherortes für die Sicherungskopie der Konfigurationsdatei aufgefordert.

Wenn Sie Ihre Einstellungen wiederherstellen möchten, klicken Sie auf „**Browse**“ und wählen Sie den Namen aus, unter dem Sie die Sicherungskopie der Konfigurationsdatei auf Ihrem PC gespeichert haben. Pfad und Dateiname der Sicherungskopie werden im Feld „File Name“ angezeigt. Klicken Sie anschließend auf „**Download**“, um die Konfigurationsdatei wiederherzustellen. Nach erfolgreichem Abschluss der Wiederherstellung erscheint die Meldung „**Download Success**“.

Die erweiterten Funktionen

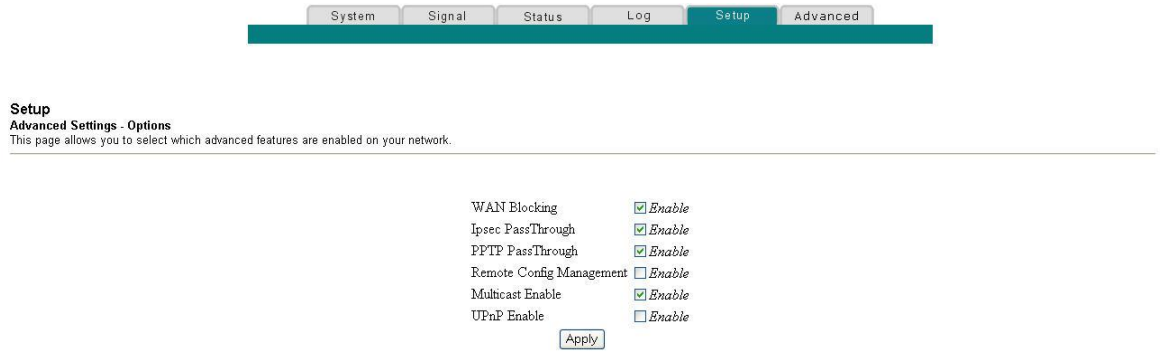
Auf der Seite „Setup Advanced Settings - Options“ können Sie die erweiterten Funktionen Ihres Netzwerks aktivieren bzw. deaktivieren. Bei deaktivierter Wireless-Schnittstelle ist der Sender abgeschaltet.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**Options**“, um die Seite „Setup Advanced Settings - Options“ aufzurufen.

Die Seite „Setup Advanced Settings - Options“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - Options“.



Beschreibung der Seite „Setup Advanced Settings - Options“

Die folgende Tabelle enthält eine Beschreibung der auf der Seite „Setup Advanced Settings - Options“ verwendeten Felder.

Hinweis: Wenn Sie auf der Seite „Setup Advanced Settings - Options“ Änderungen vornehmen, klicken Sie anschließend auf „Apply“, um die neuen Einstellungen anzuwenden und zu speichern.

Feldname	Beschreibung
WAN Blocking	Ist diese Funktion aktiviert, ist das Heim-Gateway im WAN unsichtbar. So werden beispielsweise Pings an die WAN IP-Adresse nicht beantwortet.
IPsec PassThrough	Ist diese Funktion aktiviert, werden Anwendungen, die IP-Sicherheit (IP Security) verwenden, von der Firewall durchgelassen.

Feldname	Beschreibung
PPTP PassThrough	Ist diese Funktion aktiviert, werden Anwendungen, die das PPTP (Point to Point Tunneling Protocol) verwenden, von der Firewall durchgelassen.
Remote Config Management	Konfigurationsfernverwaltung. Ist diese Funktion aktiviert, können Benutzer oder Netzwerkbetreiber die Setup-Parameter des Gateways nicht nur vom LAN aus, sondern auch über das WAN anzeigen und ändern. Der Zugriff auf die Setup-Parameter erfolgt nach Eingabe des Kennworts in den WebWizard. Klicken Sie zur Aktivierung dieser Funktion auf der Seite „Setup Advanced Settings - Options“ auf das Kontrollkästchen **Remote Config Management**. Um von einem Remote-Client aus auf Ihr Gateway zugreifen zu können, müssen Sie auch die WAN IP-Adresse des Gateways kennen. Sie finden diese Adresse unter „Basic Settings“ auf der Seite „Network Configuration“. Geben Sie die WAN IP-Adresse Ihres Gateways im folgenden Format in die Adressleiste eines Webbrowsers ein: http://xxx.xxx.xxx.xxx:8080, wobei xxx.xxx.xxx.xxx der WAN IP-Adresse Ihres Gateways entspricht. Achten Sie darauf, dass die Syntax genau dieser Vorlage entspricht. Klicken Sie anschließend auf „**Go**“ oder drücken Sie die Eingabetaste. Die Webseiten Ihres Gateways werden auf dem Remote-Computer angezeigt. Bevor Sie auf die Setup-Seiten Ihres Gateways zugreifen können, müssen Sie das Kennwort eingeben. **Hinweis:** Wenn Sie diese Funktion aktivieren, sollten Sie in jedem Fall ein Benutzerkennwort einrichten, um unbefugten Zugriff auf die Einstellungen Ihres Gateways zu verhindern.
Multicast Enable	Multicast aktivieren. Ist diese Funktion aktiviert, werden Multicasts über das WAN in das private Netzwerk weitergeleitet.
UPnP Enable	Universal Plug&Play aktivieren. Durch Markieren dieses Kontrollkästchens aktivieren Sie die universellen Plug&Play-Funktionen.

Konfiguration von IP-Adressfiltern

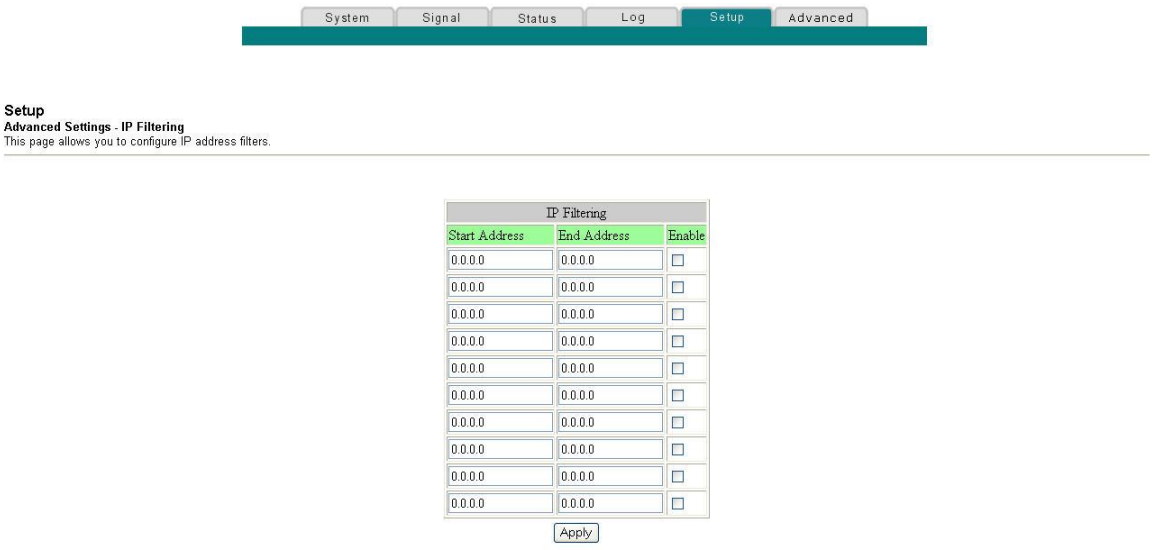
Auf der Seite „Setup Advanced Settings - IP Filtering“ können Sie IP-Adressfilter konfigurieren. Diese Filter verhindern, dass innerhalb eines bestimmten Bereichs liegende IP-Adressen auf das Internet zugreifen.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**IP Address Filtering**“, um die Seite „Setup Advanced Settings - IP Filtering“ aufzurufen.

Die Seite „Setup Advanced Settings - IP Filtering“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - IP Filtering“.



Beschreibung der Seite „Setup Advanced Settings - IP Filtering“

Auf dieser Seite können Sie einen Bereich für IP-Adressen angeben und aktivieren, die nicht auf das Internet zugreifen dürfen. Klicken Sie auf „**Apply**“, um die neuen Einstellungen des IP-Adressfilters anzuwenden und zu speichern.

Konfiguration von MAC-Adressfiltern

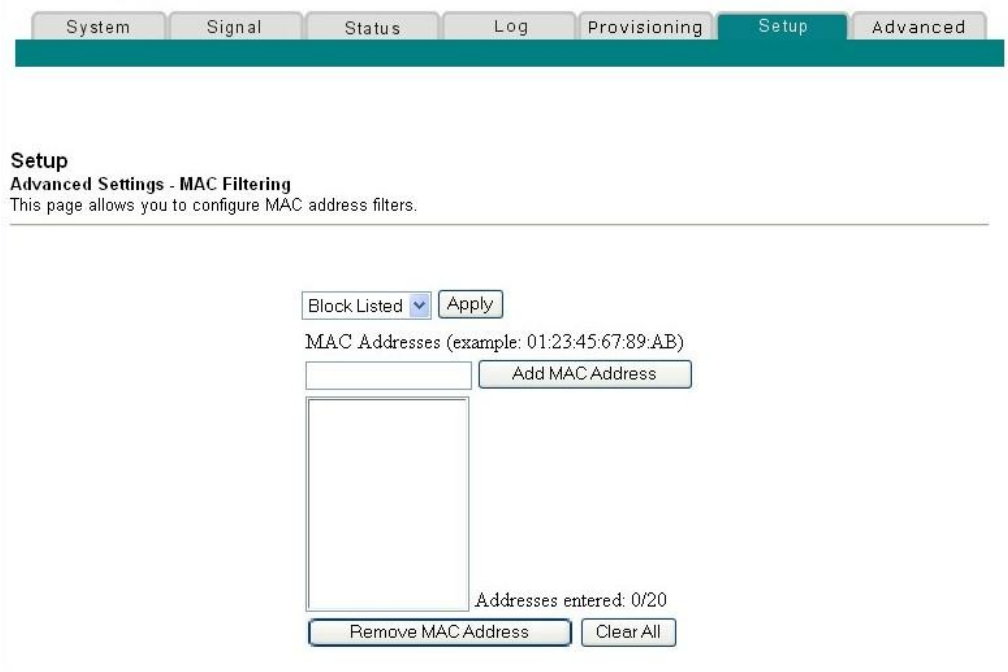
Auf der Seite „Setup Advanced Settings - MAC Filtering“ können Sie MAC-Adressfilter konfigurieren. Mit diesen Filtern können Sie einzelnen in der Liste aufgeführten MAC-Adressen den Zugriff auf das Internet verweigern. Darüber hinaus können Sie verhindern, dass individuelle PCs TCP/UDP-Datenpakete über ihre MAC-Adressen in das WAN übertragen.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**MAC Address Filtering**“, um die Seite „Setup Advanced Settings - MAC Filtering“ aufzurufen.

Die Seite „Setup Advanced Settings - MAC Filtering“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - MAC Filtering“.



Beschreibung der Seite „Setup Advanced Settings - MAC Filtering“

Auf dieser Seite können Sie die MAC-Adressen der Geräte eingeben, deren Zugriff auf das Internet Sie kontrollieren möchten. Klicken Sie auf „**Apply**“, um die neuen Einstellungen des MAC-Adressfilters anzuwenden und zu speichern.

Einrichten von MAC-Adressfiltern

Mit den Optionen des Dropdown-Menüs „Block/Pass“ können Sie den Zugang zum Internet für Geräte, deren MAC-Adressen Sie der Liste „MAC Addresses“ hinzugefügt haben, erlauben oder blockieren. Die folgende Tabelle beschreibt die Optionen des Dropdown-Menüs „Block/Pass“.

Feldname	Beschreibung
Block Listed (Default)	Aufgeführte Adressen blockieren (Vorgabe). Wählen Sie die Option „**Block**“, um den in der Liste aufgeführten MAC-Adressen den Zugriff auf das Internet zu verweigern. Allen anderen MAC-Adressen ist der Zugang zum Internet gestattet.
Pass	Aufgeführte Adressen zulassen. Wählen Sie die Option „**Pass**“, um ausschließlich den Geräten, deren MAC-Adressen in der Liste aufgeführt werden, den Zugriff auf das Internet zu gestatten. Allen anderen MAC-Adressen, die *nicht* in der Liste aufgeführt sind, wird der Zugang auf das Internet verweigert.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Advanced Settings - MAC Filtering“ angezeigt.

Schaltfläche	Beschreibung
Apply	Anwenden. Speichert die von Ihnen eingegebenen Werte, ohne das Fenster zu schließen.
Add MAC Address	MAC-Adresse hinzufügen. Speichert die im entsprechenden Feld eingegebene MAC-Adresse.
Remove MAC Address	MAC-Adresse entfernen. Entfernt die ausgewählte MAC-Adresse.
Clear All	Alle löschen. Entfernt alle definierten MAC-Adressen.

Konfiguration und Aktivierung von TCP- und UDP-Portfiltern

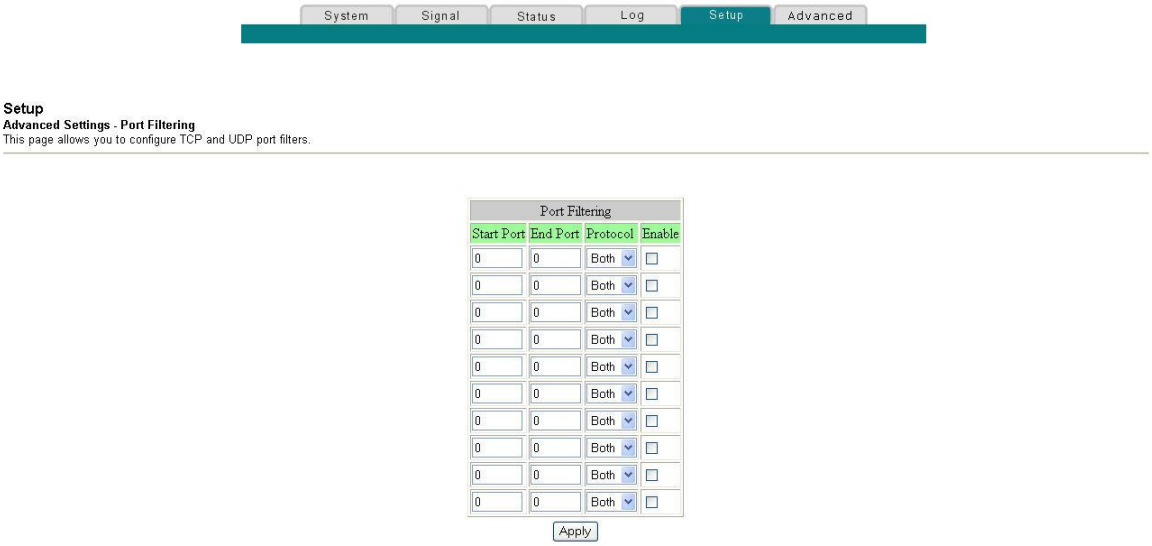
Auf der Seite „Setup Advanced Settings - Port Filtering“ können Sie TCP- und UDP-Portfilter konfigurieren und aktivieren. Diese Filter verhindern, dass bestimmte TCP/UDP-Portbereiche auf das Internet zugreifen. Darüber hinaus können Sie verhindern, dass PCs TCP/UDP-Datenpakete über bestimmte IP-Portnummern in das WAN übertragen. Diese Filter richten sich nicht an bestimmte IP- oder MAC-Adressen, sondern blockieren die angegebenen Portbereiche für alle PCs.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**Port Filtering**“, um die Seite „Setup Advanced Settings - Port Filtering“ aufzurufen.

Die Seite „Setup Advanced Settings - Port Filtering“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - Port Filtering“.



Beschreibung der Seite „Setup Advanced Settings - Port Filtering“

Auf dieser Seite können Sie die gewünschten Bereiche für die Portfilter in die entsprechenden Felder eingeben und die Protokolle auswählen. Klicken Sie anschließend auf „**Apply**“, um die neuen Einstellungen der Portfilter anzuwenden und zu speichern.

Konfiguration der Portweiterleitung für lokale IP-Adressen

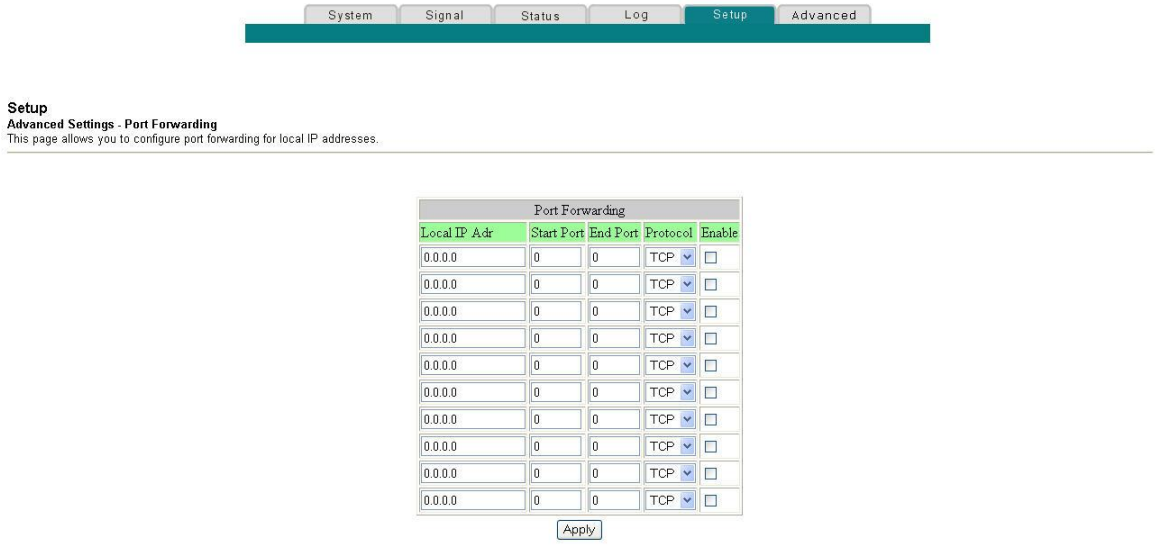
Auf der Seite „Setup Advanced Settings - Port Forwarding“ können Sie die Portweiterleitung für lokale IP-Adressen konfigurieren. Die Portweiterleitung ermöglicht es Ihnen, durch Zuordnung von TCP/UDP-Ports zu einem lokalen PC einen Server im lokalen Netzwerk (LAN) auszuführen. Für das Zielgerät müssen Sie ebenfalls eine feste private LAN IP-Adresse einrichten.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**Port Forwarding**“, um die Seite „Setup Advanced Settings - Port Forwarding“ aufzurufen.

Die Seite „Setup Advanced Settings - Port Forwarding“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - Port Forwarding“.



Beschreibung der Seite „Setup Advanced Settings - Port Forwarding“

Das folgende Beispiel zeigt, wie Sie die Portweiterleitungsfunktion zur Konfiguration der Microsoft X-Box Online Live für Internet-Gaming benutzen können.

Hinweis: Bei den gängigsten Anwendungen (einschließlich Microsoft X-Box Online Live) ordnet die integrierte Firewall diesen Anwendungen automatisch Ports zu und hält die Ports offen, solange die Anwendung ausgeführt wird.

1 Weisen Sie dem Gerät, das für die Portweiterleitung verwendet werden soll, eine feste IP-Adresse zu, beispielsweise **192.168.0.5**.

2. Geben Sie in der ersten Zeile des Portweiterleitungsbereichs auf der Seite dieselbe IP-Adresse (192.168.0.5) in das Feld „Local IP Address“ ein.
3. Geben Sie in derselben Zeile die gewünschten Portnummern in die Felder „Start Port“ und „End Port“ ein.
4. Wählen Sie aus der Dropdown-Liste im Feld „Protocol“ derselben Zeile das gewünschte Protokoll aus. Klicken Sie anschließend auf das Kontrollkästchen „**Enable**“ (Aktivieren).
5. Wenn Sie weitere Ports hinzufügen möchten, wiederholen Sie die Schritte 1 bis 4; gehen Sie im Anschluss daran zu Schritt 6.
6. Klicken Sie auf „**Apply**“, um die neuen Einstellungen der Portweiterleitung anzuwenden und zu speichern.

Konfiguration von TCP/UDP-Port-Triggern

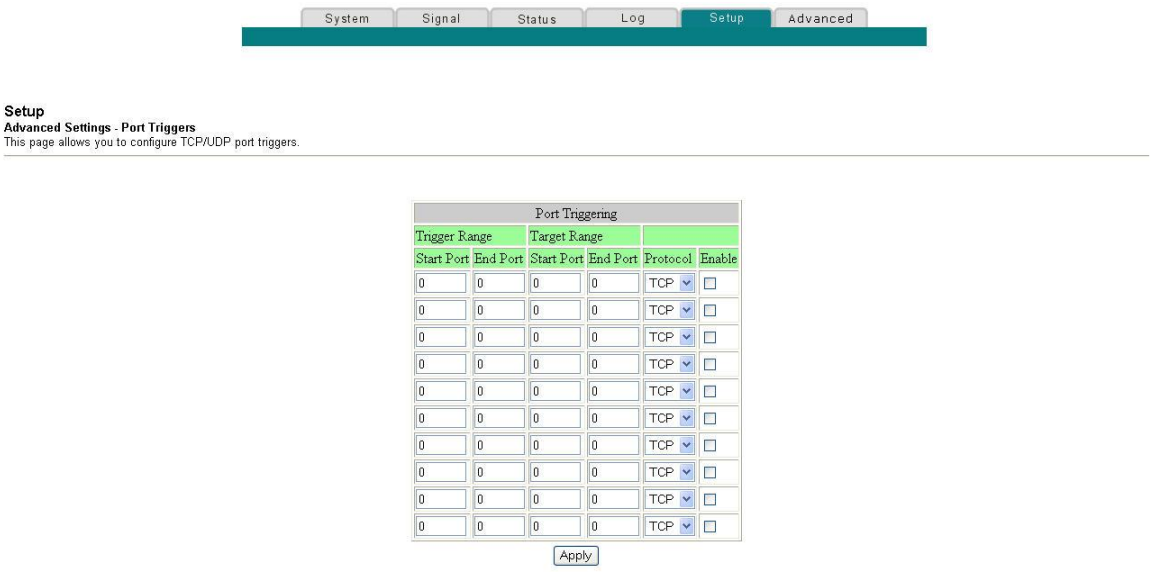
Auf der Seite „Setup Advanced Settings - Port Triggers“ können Sie TCP/UDP-Port-Trigger konfigurieren. Port-Trigger (Port-Auslöser) funktionieren auf ähnliche Weise wie die Portweiterleitung; im Gegensatz dazu haben sie jedoch eine dynamische Funktion. Das heißt, dass das System die Ports nur vorübergehend öffnet. Wenn beispielsweise das Heim-Gateway feststellt, dass über eine bestimmte im Auslöserbereich (Trigger Range) liegende IP-Portnummer Daten gesendet werden, werden die entsprechenden im Zielbereich (Target Range) liegenden Ports für den Empfang von Daten geöffnet. Stellt das System fest, dass über die im Auslöserbereich liegenden Ports über einen Zeitraum von 10 Minuten keine Daten gesendet werden, werden die Ports im Zielbereich geschlossen. Diese Methode, spezifische Ports für bestimmte Anwendungen wie beispielsweise Videokonferenzprogramme, interaktives Gaming oder Dateiübertragungen in Chat-Programmen zu öffnen, ist sicherer, da das Öffnen der Ports dynamisch ausgelöst wird und die Ports nicht ununterbrochen geöffnet sind oder versehentlich vom Router-Administrator offen gelassen werden. Diese Ports können auf diese Weise nicht von Hackern entdeckt werden.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**Port Triggers**“, um die Seite „Setup Advanced Settings - Port Triggers“ aufzurufen.

Die Seite „Setup Advanced Settings - Port Triggers“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - Port Triggers“.



Beschreibung der Seite „Setup Advanced Settings - Port Triggers“

Auf dieser Seite können Sie die Start- und End-Ports der Auslöser- und Zielbereiche für die Portweiterleitung eingeben und aktivieren sowie die gewünschten Protokolle auswählen. Das folgende Beispiel zeigt, wie Sie die Portauslöserfunktion zur Konfiguration der Microsoft X-Box Online Live für Internet-Gaming benutzen können.

Hinweis: Bei den gängigsten Anwendungen (einschließlich Microsoft X-Box Online Live) ordnet die integrierte Firewall diesen Anwendungen automatisch Ports zu und hält die Ports offen, solange die Anwendung ausgeführt wird.

1. Geben Sie in der ersten Zeile **88** in das Feld „Start Port“ und das Feld „End Port“ ein.
2. Wählen Sie aus der Dropdown-Liste im Feld „Protocol“ derselben Zeile **UDP** aus. Klicken Sie anschließend auf das Kontrollkästchen „**Enable**“ (Aktivieren).
3. Geben Sie in der zweiten Zeile **3074** in das Feld „Start Port“ und das Feld „End Port“ ein.
4. Wählen Sie aus der Dropdown-Liste im Feld „Protocol“ der zweiten Zeile „**Both**“ (Beide) aus. Klicken Sie anschließend auf das Kontrollkästchen „**Enable**“ (Aktivieren).
5. Klicken Sie auf „**Apply**“, um die neuen Einstellungen für Port-Trigger anzuwenden und zu speichern.

Konfiguration des DMZ-Hosts

Auf der Seite „Setup Advanced Settings - DMZ Host“ können Sie eine IP-Adresse konfigurieren, die vom WAN aus erkennbar ist. Ein DMZ-Host wird häufig als „exposed host“ (etwa: ungeschützter Host) bezeichnet. Er ermöglicht Ihnen, einen Standardempfänger für den WAN-Verkehr anzugeben, der durch Network Address Translation (NAT) keinem anderen bekannten lokalen PC zugeordnet werden kann. Dies geschieht, indem eine IP-Adresse ungeschützt bleibt, während alle anderen IP-Adressen geschützt werden.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**DMZ Host**“, um die Seite „Setup Advanced Settings - DMZ Host“ aufzurufen.

Die Seite „Setup Advanced Settings - DMZ Host“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Advanced Settings - Options“.

Beschreibung der Seite „Setup Advanced Settings - DMZ Host“

Auf dieser Seite können Sie ein in einem privaten LAN eingebundenes Gerät – z. B. einen FTP-, Mail- oder Webserver – direkt (d. h. die Firewall wird umgangen) in das Internet einbinden. Geben Sie dazu die IP-Adresse des Servers in das Feld „DMZ Address“ ein, um den Server so mit einer festen IP-Adresse als DMZ-Host einzurichten. Achten Sie darauf, dass die IP-Adresse nicht in dem Adressbereich liegt, der vom integrierten DHCP-Server bereitgestellt wird. Alle Ports des als DMZ-Host eingerichteten Gerätes sind jetzt für das Internet geöffnet. Es kann nur jeweils ein PC als DMZ-Host konfiguriert werden. Die DMZ-Funktion wird im Allgemeinen für PCs benutzt, auf denen „problematische“ Anwendungen ausgeführt werden, die zufällige Portnummern benutzen und deshalb mit den oben beschriebenen spezifischen Port-Triggern oder der Portweiterleitung nicht ordnungsgemäß funktionieren. Klicken Sie nach Eingabe der DMZ-Adresse auf „**Apply**“, um die neuen Einstellungen Ihres DMZ-Hosts anzuwenden und zu speichern.

Konfiguration der VPN-Terminierung

Auf der Seite „Setup Advanced Settings - VPN Termination“ können Sie VPN-Protokolle konfigurieren und VPN-Tunnel verwalten. Ein VPN (Virtual Private Network) ist eine Verbindung zwischen zwei Endpunkten in verschiedenen öffentlichen oder privaten Netzwerken, über die Daten zwischen diesen beiden Endpunkten oder Netzwerken sicher und transparent übertragen werden können. Dazu wird ein sogenannter VPN-Tunnel erstellt, der die beiden PCs oder Netzwerke miteinander verbindet. Die Datenübertragung zwischen den beiden PCs oder Netzwerken erfolgt jetzt über das Internet genau so, als befänden sich die beiden PCs oder Netzwerke innerhalb desselben Netzwerks. Der VPN-Tunnel verschlüsselt die zwischen den beiden Netzwerken gesendeten Daten mittels IPsec (Internet Protocol Security) und verkapselt die Daten innerhalb eines normalen Ethernet/IP-Frames, um das private Netzwerk sicher und nahtlos durch andere öffentliche oder private Netzwerke zu transportieren.

Ein VPN ist eine kosteneffektive und sicherere Alternative zur Nutzung einer privaten dedizierten Standleitung für ein privates Netzwerk. Mittels branchenüblicher Verschlüsselungs- und Authentifizierungsmethoden schafft ein IPsec VPN eine sichere Verbindung, die genauso funktioniert, als wären Sie direkt mit Ihrem lokalen Netzwerk verbunden.

Ein VPN ermöglicht es beispielsweise Benutzern, von zuhause aus eine Verbindung mit dem Firmennetzwerk herzustellen und in ihrem privaten Netzwerk eine IP-Adresse zu erhalten, als säßen sie in ihrem Büro und wären direkt mit dem LAN ihrer Firma verbunden.

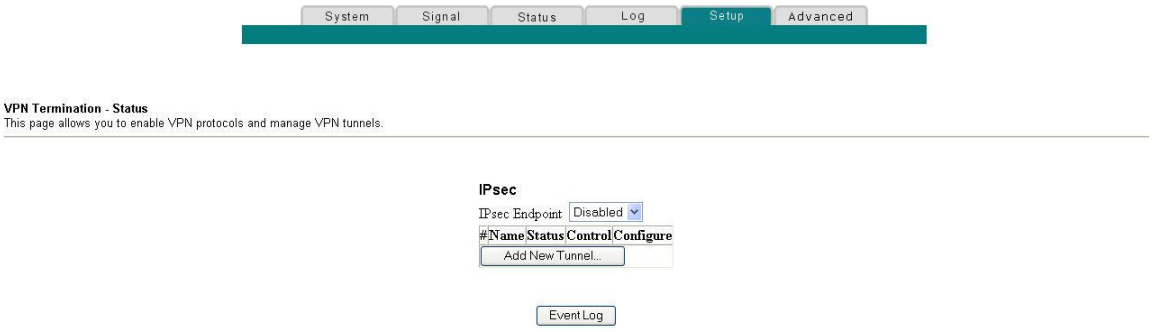
Ein weiterer Vorteil eines VPN-Netzwerks ist es, dass alle firmeneigenen auf Microsoft Windows basierenden Netzwerkprotokolle vom Router durchgelassen werden und den Zugriff auf die freigegebenen Netzwerklaufwerke des Unternehmens über den VPN-Tunnel ermöglichen.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Advanced Settings“ auf der Setup-Seite auf „**VPN Termination**“, um die Seite „Setup Advanced Settings - VPN Termination - Status“ aufzurufen. Auf der Seite „VPN Termination - Status“ können Sie IPsec VPN-Tunnel erstellen, konfigurieren und kontrollieren.

Die Seite „Setup Advanced Settings - VPN Termination - Status“

Die folgende Abbildung ist ein Beispiel einer leeren Seite „Setup Advanced Settings - VPN Termination - Status“. Es wurden noch keine VPN-Tunnel erstellt.



Beschreibung der Seite „Setup Advanced Settings - VPN Termination - Status“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Advanced Settings - VPN Termination - Status“. Auf dieser Seite können Sie IPsec VPN-Tunnel erstellen, konfigurieren und kontrollieren.

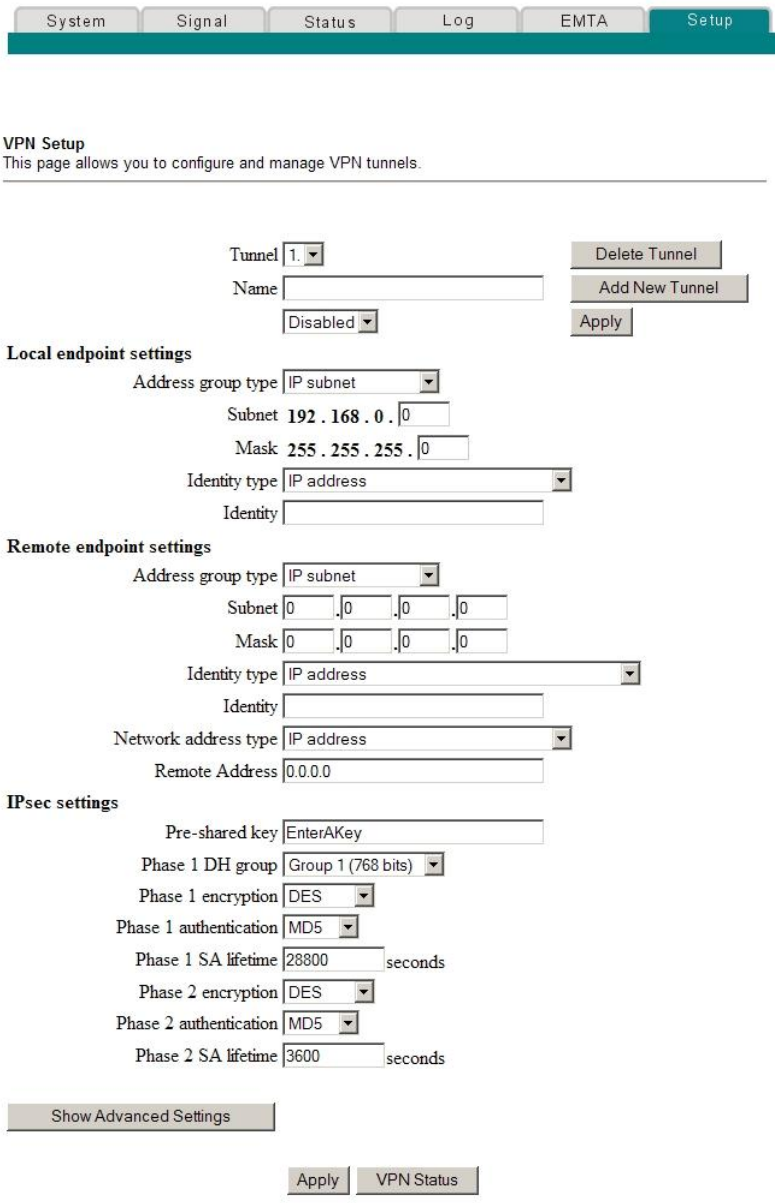
Hinweis: Sie können bis zu 50 verschiedene VPN-Tunnel einrichten und verwalten.

Feldname	Beschreibung
IPsec Endpoint	Aktiviert bzw. deaktiviert den IPsec Endpunktmodus.
Name	Zeigt den benutzerdefinierten Tunnelnamen an, der auf der VPN-Setup-Seite eingegeben worden ist.
Status	Zeigt den aktuellen Verbindungsstatus an (verbunden/NICHT verbunden).
Control	Zeigt je nach aktuellem Zustand der Tunnelfunktion eine der drei Schaltflächen an: ■ Enable (Aktivieren) ■ Connect (Verbinden) ■ Endpoint disabled (Endpunkt deaktiviert)
Configure	Zeigt die für die Einstellungsverwaltung verwendeten Schaltflächen „Edit“ (Bearbeiten) und „Delete“ (Löschen) an.
Add New Tunnel	Neuen Tunnel hinzufügen. Ermöglicht das Erstellen einer neuen Tunnelkonfiguration. Wenn Sie auf die Schaltfläche „**Add New Tunnel**“ klicken, wird die Seite „VPN Setup“ geöffnet.

Feldname	Beschreibung
Event Log	Öffnet das Ereignisprotokoll. Die Seite „Event Log“ zeigt den Verlauf der VPN-Verbindungen und -Aktivitäten in chronologischer Reihenfolge sowie die IP-Adresse der beiden Tunnelendpunkte (lokal und remote) an. **Hinweis:** Wenn Sie auf der Seite „Event Log“ auf die Schaltfläche „**Refresh**“ klicken, wird die Tabelle mit den seit dem letzten Aufruf der Seite aufgetretenen Ereignissen aktualisiert. Durch Klicken auf die Schaltfläche „**Clear**“ (Löschen) werden ältere Verlaufsinformationen aus der Tabelle gelöscht und nur die jüngsten Daten angezeigt.

Erstellen und Konfigurieren von IPsec VPN-Tunneln

Klicken Sie auf die Schaltfläche „**Add New Tunnel**“ auf der Seite „VPN Termination - Status“, um IPsec VPN-Tunnel zu erstellen und zu konfigurieren. Die Seite „VPN Setup“ wird angezeigt. Die folgende Abbildung ist ein Beispiel der Seite „VPN Setup“.



Beschreibung der Seite „Setup Advanced Settings - VPN Setup“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Advanced Settings - VPN Setup“. Auf dieser Seite können Sie IPsec VPN-Tunnel erstellen, konfigurieren und kontrollieren.

Der Tunnelabschnitt

Feldname	Beschreibung
Tunnel	Zeigt vorhandene Tunnel an und ermöglicht die Konfiguration der einzelnen Tunnel.
Name	Zeigt den Namen einer Gruppe von Einstellungen für einen einzelnen Tunnel an. Wenn kein Name eingegeben wird, werden die Tunnel der Reihe nach als 1, 2, 3 usw. bezeichnet.
Enable/Disable	Aktiviert bzw. deaktiviert einen VPN-Tunnel, nachdem er benannt und konfiguriert worden ist. Klicken Sie auf „**Apply**“, um die gewählte Einstellung (aktiviert oder deaktiviert) anzuwenden.

Schaltflächen

Die folgende Tabelle enthält eine Beschreibung der dem Tunnelabschnitt der Seite „VPN Setup“ zugeordneten Schaltflächen.

Schaltfläche	Beschreibung
Delete Tunnel	Löscht einen Tunnel.
Add New Tunnel	Neuen Tunnel hinzufügen. Ermöglicht die Eingabe bzw. Auswahl einer Bezeichnung für die Tunneleinstellungen aus dem Dropdown-Menü.
Apply	Anwenden. Aktiviert die gewählte Einstellung (Enabled oder Disabled).

Einstellungen des lokalen Endpunkts

Die folgende Tabelle enthält eine Beschreibung der Felder des Abschnitts „Local endpoint settings“ auf der Seite „VPN Setup“.

Feldname	Beschreibung
Address group type	Adressgruppentyp. Ermöglicht die Auswahl des Adressgruppentyps für die Zugriffsgruppe des lokalen VPN. Die folgenden Typen stehen zur Wahl: ■ IP subnet (IP-Subnetz) ■ Single IP address (einzelne IP-Adresse) ■ IP address range (IP-Adressbereich)
Subnet	Subnetz. Ermöglicht die Eingabe der Subnetzinformationen anhand des gewählten Adressgruppentyps: ■ Geben Sie bei „IP subnet“ das entsprechende Subnetz ein. ■ Geben Sie bei „Single IP address“ nur die spezifische IP-Adresse ein. ■ Geben Sie bei „IP address range“ die Start- und die End-IP-Adresse des Adressbereichs ein.
Mask	Maske. Ermöglicht die Eingabe der Maskeninformationen anhand des gewählten Adressgruppentyps: ■ Geben Sie bei „IP subnet“ die Subnetzmaske ein. ■ Geben Sie bei „Single IP address“ nur die spezifische IP-Adresse in das Feld „Subnet“ ein; lassen Sie dieses Feld leer. ■ Geben Sie bei „IP address range“ die Start- und die End-IP-Adresse des Adressbereichs ein.
Identity type	Identitätstyp. Ermöglicht die Auswahl des lokalen Identitätstyps unter den folgenden Optionen: ■ WAN IP address of the router (WAN IP-Adresse des Routers – Standard) ■ User-specified IP address (vom Benutzer eingegebene IP-Adresse) ■ Fully qualified domain name (FQDN; vollständiger Domänenname) ■ Email address (E-Mail-Adresse) Dies ist die Identität, anhand der der Endpunkt am anderen Ende den VPN-Endpunkt identifiziert. Diese Einstellungen müssen mit den Einstellungen des Remote-VPN-Endpunkts am anderen Ende des Tunnels übereinstimmen, die dieser Endpunkt zur Definition seines Remote-Endpunkts verwendet.

Feldname	Beschreibung
Identity	Identität. Ermöglicht nach Festlegung des Identitätstyps die Eingabe der Identitätszeichenkette in einem der folgenden Formate: ■ Benutzen Sie für IP-Adressen das Format xxx.xxx.xxx.xxx ■ Benutzen Sie für vollständige Domänennamen das Format „ihredomaene.com“ ■ Benutzen Sie für E-Mail-Adressen das Format „ihrname@ihredomaene.com“ Diese Einstellungen müssen mit den Einstellungen des Remote-VPN-Endpunkts am anderen Ende des Tunnels übereinstimmen, die dieser Endpunkt zur Definition seines Remote-Endpunkts verwendet.

Einstellungen des Remote-Endpunkts

Diese Einstellungen kontrollieren, wie der lokale Endpunkt (Router) mit dem VPN-Endpunkt am anderen Ende des VPN-Tunnels eine Verbindung herstellt.

Feldname	Beschreibung
Address group type	Adressgruppentyp. Ermöglicht die Auswahl des Adressgruppentyps für die Zugriffsgruppe des Remote-VPN. Die folgenden Typen stehen zur Wahl: ■ IP subnet (IP-Subnetz) ■ Single IP address (einzelne IP-Adresse) ■ IP address range (IP-Adressbereich) Diese Einstellungen müssen mit den Einstellungen des Remote-VPN-Endpunkts am anderen Ende des Tunnels übereinstimmen, die dieser Endpunkt zur Definition seines Remote-Endpunkts verwendet.
Subnet	Ermöglicht die Eingabe der Subnetzinformationen anhand des gewählten Adressgruppentyps: ■ Geben Sie bei „IP subnet“ das entsprechende Subnetz ein. ■ Geben Sie bei „Single IP address“ nur die spezifische IP-Adresse ein. ■ Geben Sie bei „IP address range“ die Start- und die End-IP-Adresse des Adressbereichs ein.
Mask	Ermöglicht die Eingabe der Maskeninformationen anhand des gewählten Adressgruppentyps: ■ Geben Sie bei „IP subnet“ die Subnetzmaske ein. ■ Geben Sie bei „Single IP address“ nur die spezifische IP-Adresse in das Feld „Subnet“ ein; lassen Sie dieses Feld leer. ■ Geben Sie bei „IP address range“ die Start- und die End-IP-Adresse des Adressbereichs ein.

Feldname	Beschreibung
Identity type	Identitätstyp. Ermöglicht die Auswahl des Remote-Identitätstyps unter den folgenden Optionen: ■ WAN IP address of the router (WAN IP-Adresse des Routers – Standard) ■ User-specified IP address (vom Benutzer eingegebene IP-Adresse) ■ Fully qualified domain name (FQDN; vollständiger Domänennamen) ■ Email address (E-Mail-Adresse) Dies ist die Identität, anhand der der Endpunkt am anderen Ende den VPN-Endpunkt identifiziert. Diese Einstellungen müssen mit den Einstellungen des Remote-VPN-Endpunkts am anderen Ende des Tunnels übereinstimmen, die dieser Endpunkt zur Definition seines Remote-Endpunkts verwendet.
Identity	Identität. Ermöglicht nach Festlegung des Identitätstyps die Eingabe der Identitätszeichenkette in einem der folgenden Formate: ■ Benutzen Sie für IP-Adressen das Format xxx.xxx.xxx.xxx ■ Benutzen Sie für vollständige Domänennamen das Format „ihredomaene.com“ ■ Benutzen Sie für E-Mail-Adressen das Format „ihrname@ihredomaene.com“ Diese Einstellungen müssen mit den Einstellungen des Remote-VPN-Endpunkts am anderen Ende des Tunnels übereinstimmen, die dieser Endpunkt zur Definition seines Remote-Endpunkts verwendet.
Network address type	Netzwerkadresstyp. Ermöglicht die Eingabe des Adresstyps für das Endpunkt-WAN. Wählen Sie eine der folgenden Optionen aus: ■ IP address ■ FQDN
Remote address	Remote-Adresse. Ermöglicht in Abhängigkeit des gewählten Netzwerkadresstyps die Eingabe entweder der IP-Adresse oder des vollständigen Domänennamens des Remote-Endpunkts.

IPsec-Einstellungen

Bei VPN-Tunneln gibt es zwei Phasen der Security Association (SA, Sicherheitsverbindung).

- In der ersten Phase wird eine IKE-SA (Internet Key Exchange Security Association) aufgebaut.
- Nach Abschluss von Phase 1 werden in der zweiten Phase eine oder mehr IPsec-SAs erstellt, mit deren Hilfe dann die IPsec-Sitzungen aufgebaut werden.

Feldname	Beschreibung
Pre-shared key	Vorher vereinbarter Schlüssel. Ermöglicht die Eingabe des vorher vereinbarten Schlüssels des Firewall-Identifiers, wenn die eine Seite des VPN-Tunnels eine eindeutige Firewall verwendet.
Phase 1 DH group	DH-Gruppe für Phase 1. Ermöglicht die Auswahl einer der folgenden drei Diffie-Hellman (DH) Verschlüsselungs-/Entschlüsselungsgruppen: ■ 768 Bit ■ 1024 Bit ■ 1536 Bit Diffie-Hellman ist eine kryptografische Methode, die zur Verschlüsselung und Entschlüsselung öffentliche und private Schlüssel verwendet. Je höher die gewählte Bit-Zahl, desto sicherer ist die Verbindung.
Phase 1 encryption	Verschlüsselung der Phase 2. Ermöglicht die Auswahl der Verschlüsselung, die für die Sicherung der VPN-Verbindung zwischen Endpunkten verwendet werden soll. Wählen Sie einen der folgenden fünf Verschlüsselungstypen: ■ DES ■ 3DES ■ AES-128 ■ AES-192 ■ AES-256 Sie können einen beliebigen Verschlüsselungstyp auswählen; wichtig ist nur, dass am anderen Ende des VPN-Tunnels dieselbe Methode verwendet wird.
Phase 1 authentication	Phase-2-Authentifizierung. Ermöglicht die Auswahl eines Authentifizierungstyps für eine andere Sicherheitsebene. Wählen Sie einen der folgenden Authentifizierungstypen aus: ■ MD5 ■ SHA Sie können einen beliebigen Authentifizierungstyp auswählen; wichtig ist nur, dass am anderen Ende des VPN-Tunnels dieselbe Methode verwendet wird. **Hinweis:** Da SHA sicherer ist, ist diese Methode vorzuziehen.
Phase 1 SA lifetime	SA-Lebenszeit in Phase 2. Ermöglicht die Eingabe der Lebenszeit eines sich regelmäßig ändernden individuellen Schlüssels (rotating key) in Sekunden; nach Ablauf der Lebenszeit wird ein neuer Schlüssel zwischen den beiden Endpunkten ausgehandelt. In der Regel sind kürzere Lebenszeiten sicherer, da einem Hacker zum Knacken des Schlüssels weniger Zeit verbleibt. Die Aushandlung des neuen Schlüssels nimmt jedoch Bandbreite in Anspruch, sodass bei kurzen Lebenszeiten der Netzwerkdurchsatz beeinträchtigt wird. Der Standardwert beträgt 28.800 Sekunden.

Feldname	Beschreibung
Phase 2 encryption	Verschlüsselung der Phase 2. Ermöglicht die Auswahl der Verschlüsselung, die für die Sicherung der VPN-Verbindung zwischen Endpunkten verwendet werden soll. Wählen Sie einen der folgenden fünf Verschlüsselungstypen: ■ DES-Verschlüsselung ■ 3DES ■ AES-128 ■ AES-192 ■ AES-256 Sie können einen beliebigen Verschlüsselungstyp auswählen; wichtig ist nur, dass am anderen Ende des VPN-Tunnels dieselbe Methode verwendet wird. **Hinweis:** 3DES-Verschlüsselung wird oftmals verwendet, aber da AES sehr schwer zu knacken ist, sollte dieser Typ gewählt werden.
Phase 2 authentication	Phase-2-Authentifizierung. Ermöglicht die Auswahl eines Authentifizierungstyps für eine andere Sicherheitsebene. Wählen Sie einen der folgenden drei Authentifizierungstypen aus: ■ MD5 ■ SHA ■ Null (keinen) Sie können einen beliebigen Authentifizierungstyp auswählen; wichtig ist nur, dass am anderen Ende des VPN-Tunnels dieselbe Methode verwendet wird. **Hinweis:** Da SHA sicherer ist, ist diese Methode vorzuziehen.
Phase 2 SA lifetime	SA-Lebenszeit in Phase 2. Ermöglicht die Eingabe der Lebenszeit eines sich regelmäßig ändernden individuellen Schlüssels (rotating key) in Sekunden; nach Ablauf der Lebenszeit wird ein neuer Schlüssel zwischen den beiden Endpunkten ausgehandelt. In der Regel sind kürzere Lebenszeiten sicherer, da einem Hacker zum Knacken des Schlüssels weniger Zeit verbleibt. Die Aushandlung des neuen Schlüssels nimmt jedoch Bandbreite in Anspruch, sodass bei kurzen Lebenszeiten der Netzwerkdurchsatz beeinträchtigt wird. Der Standardwert für Phase 2 beträgt 3.600 Sekunden.

Konfiguration der Firewall

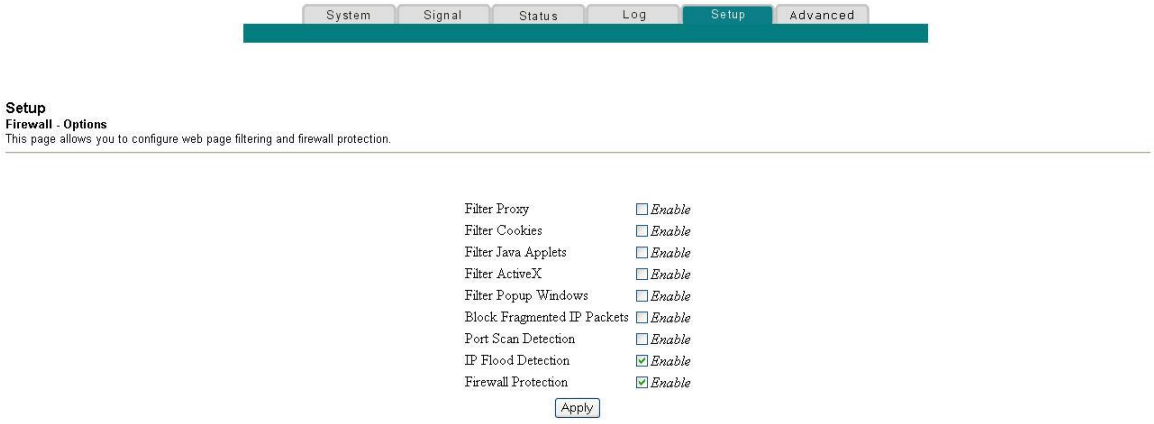
Auf der Seite „Setup Firewall - Options“ können Sie Webseiten-Filter und Firewall-Schutz konfigurieren und aktivieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Firewall“ auf der Setup-Seite auf „**Options**“, um die Seite „Setup Firewall - Options“ aufzurufen.

Die Seite „Setup Firewall - Options“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Firewall - Options“.



Beschreibung der Seite „Setup Firewall - Options“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Firewall - Options“.

Hinweis: Wenn Sie auf der Seite „Setup Firewall - Options“ Änderungen vornehmen, klicken Sie anschließend auf „**Apply**“, um die neuen Firewall-Einstellungen anzuwenden und zu speichern.

Die folgende Tabelle enthält eine Beschreibung der auf der Seite „Setup Firewall - Options“ verwendeten Felder.

Feldname	Beschreibung
Filter Proxy	Aktiviert bzw. deaktiviert den Proxy.

Feldname	Beschreibung
Filter Cookies	Aktiviert bzw. deaktiviert die Blockierung von Cookies. Diese Funktion filtert Cookies, die über das Internet unangefordert an Geräte in Ihrem privaten LAN gesendet werden. Cookies sind Dateien, die persönliche Daten oder Informationen zu Ihrem Verhalten beim Surfen im Internet erfassen.
Filter Java Applets	Aktiviert bzw. deaktiviert Java Applets. Diese Funktion schützt die Geräte in Ihrem privaten LAN vor lästigen oder böswilligen Java Applets, die über das Internet unangefordert an Geräte in Ihrem privaten LAN gesendet werden. Diese Applets werden automatisch ausgeführt, sobald sie von einem PC empfangen werden.
Filter ActiveX	Aktiviert bzw. deaktiviert ActiveX-Steuerelemente. Diese Funktion schützt die Geräte in Ihrem privaten LAN vor lästigen oder böswilligen ActiveX-Steuerelementen, die über das Internet unangefordert an Geräte in Ihrem privaten LAN gesendet werden. Diese ActiveX-Steuerelemente werden automatisch ausgeführt, sobald sie von einem PC empfangen werden.
Filter Popup Windows	Aktiviert bzw. deaktiviert Popup-Fenster. In einigen häufig benutzten Anwendungen werden Popup-Fenster als Teil der Anwendung eingesetzt. Wenn Sie Popup-Fenster deaktivieren, beeinträchtigen Sie möglicherweise damit die Funktionsweise dieser Anwendungen.
Block Fragmented IP Packets	Aktiviert bzw. deaktiviert die Filterung fragmentierter IP-Pakete. Diese Funktion schützt Ihr privates LAN vor vom Internet ausgehenden Denial-of-Service-Attacken.
Port Scan Detection	Aktiviert bzw. deaktiviert die Reaktion des Gateways auf über das Internet ausgeführte Portscans. Diese Funktion soll Ihr privates LAN vor Angriffen aus dem Internet schützen, bei denen Hacker durch Erkennung offener IP-Ports auf Ihrem Gateway versuchen, unbefugten Zugriff auf Ihr Netzwerk zu erlangen.
IP Flood Detection	Blockiert böswillig verwendete Geräte, die versuchen, Geräte oder Netzwerke mit illegalen Datenpaketen zu überfluten und lahm zu legen. Dies wird auch als Broadcast-Sturm bezeichnet.
Firewall Protection	Aktiviert bzw. deaktiviert die Firewall. Die aktivierte Firewall gestattet den gängigsten Anwendungen, IP-Ports automatisch zu öffnen und Daten zu senden, ohne dass ein besonderes Setup oder eine manuelle Konfiguration der Ports erforderlich ist.

Konfiguration von Firewall-Ereignisprotokollierung und E-Mail-Warnungen

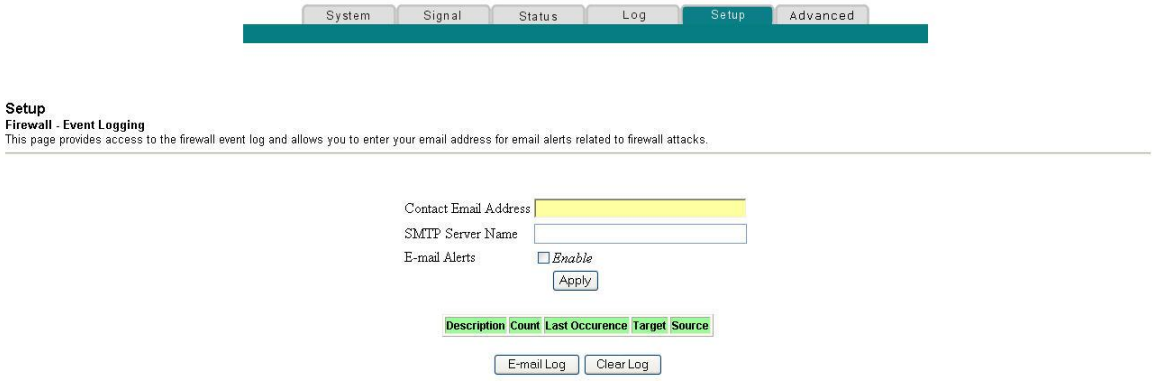
Über die Seite „Setup Firewall - Event Logging“ können Sie auf das Firewall-Ereignisprotokoll zugreifen und Ihre E-Mail-Adresse eingeben, um per E-Mail über Firewall-Angriffe durch Hacker informiert zu werden.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Firewall“ auf der Setup-Seite auf „**Event Logging**“, um die Seite „Setup Firewall - Event Logging“ aufzurufen.

Die Seite „Setup Firewall - Event Logging“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Firewall - Event Logging“.



Beschreibung der Seite „Setup Firewall - Event Logging“

Auf der Seite „Setup Firewall - Event Logging“ werden von der Firewall erfasste Ereignisse angezeigt. Das Protokoll enthält die folgenden Informationen:

- Beschreibung des Ereignisses
- Anzahl der aufgetretenen Ereignisse
- das letzte Auftreten eines Ereignisses
- Ziel- und Quelladressen

Sie können das System so konfigurieren, dass der Administrator über Protokollereignisse per E-Mail informiert wird und daraufhin die Firewall entsprechend überwachen kann.

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Firewall - Event Logging“.

Feldname	Beschreibung
Enable E-mail Address	E-Mail-Adresse aktivieren. Ermöglicht die Eingabe der E-Mail-Adresse der Person, die die Firewall überwacht. Tritt ein Ereignis auf, wird es protokolliert und automatisch eine E-Mail an diese Adresse geschickt, um das Ereignis zu melden.
SMTP Server Name	Name des SMTP-Servers. Ermöglicht die Eingabe des Namens Ihres E-Mail-Servers bzw. des Mail-Servers Ihres Internetdienstanbieters (ISP), der Ihre ausgehende E-Mail handhabt.
E-mail Alerts	E-Mail-Warnungen. Aktiviert bzw. deaktiviert das Senden von E-Mail-Warnungen, wenn bestimmte Ereignisse auftreten.
Description	Beschreibung des von der Firewall des Gateways festgestellten Ereignisses.
Count	Anzahl. Zeigt an, wie oft das Ereignis festgestellt worden ist.
Last Occurrence	Letztes Auftreten. Zeigt die Uhrzeit an, zu der dieses Ereignis zum letzten Mal aufgetreten ist.
Target	Ziel. Zeigt die IP-Adresse des Gerätes in Ihrem privaten LAN an, an das sich das Ereignis gerichtet hat, sowie die dabei benutzte IP-Portnummer.
Source	Quelle. Zeigt die IP-Adresse des internetbasierten Ausgangspunkts des Ereignisses und die dabei benutzte IP-Portnummer an.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Firewall - Event Logging“ angezeigt.

Schaltfläche	Beschreibung
Apply	Anwenden. Speichert die von Ihnen eingegebenen Werte, ohne das Fenster zu schließen.
E-mail Log	Protokoll per E-Mail senden. Zwingt das System, eine E-Mail-Warnung zu senden, auch wenn das Kontrollkästchen „E-mail Alerts“ nicht aktiviert ist.
Clear Log	Löscht alle Einträge des Protokolls.

Konfiguration des Kinderschutzes

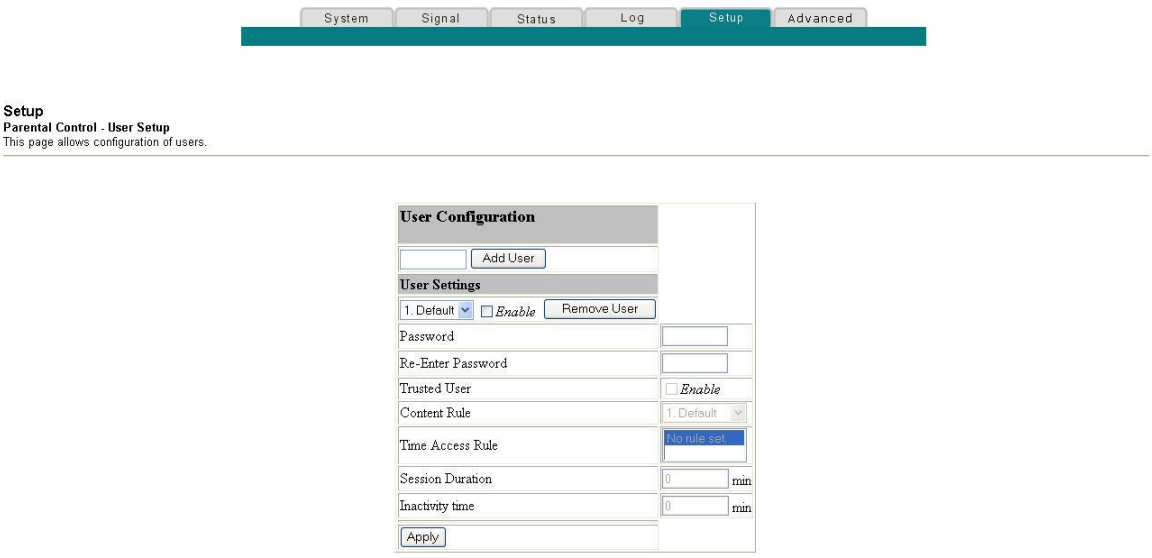
Auf der Seite „Setup Parental Control - User Setup“ können Sie den Kinderschutz auf Ihrem Heim-Gateway konfigurieren und Personen hinzufügen oder löschen, die zum Einstellen der Kinderschutzparameter berechtigt sind.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Parental Control“ auf der Setup-Seite auf „**User Setup**“, um die Seite „Setup Parental Control - User Setup“ aufzurufen.

Die Seite „Setup Parental Control - User Setup“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Parental Control - User Setup“.



Beschreibung der Seite „Setup Parental Control - User Setup“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Parental Control - User Setup“. Auf dieser Seite können Sie Benutzerprofile einrichten. Jedem Profil kann eine spezifische Zugriffsebene für das Internet zugewiesen werden, die von den diesem Benutzerprofil zugeordneten Zugriffsregeln definiert wird.

Hinweis: Nachdem Sie Benutzerprofile definiert und aktiviert haben, muss sich jeder Benutzer jedes Mal, wenn er auf das Internet zugreifen möchte, zuerst anmelden. Die Anmeldung erfolgt über das in seinem Webbrowser angezeigte Popup-Fenster; Zugang zum Internet wird erst gestattet, wenn Benutzername und Kennwort korrekt eingegeben worden sind.

Wichtig:

- Stellen Sie sicher, dass Popup-Blocker in Ihrem Webbrowser deaktiviert sind, wenn Sie Benutzerprofile verwenden.
- Bei Benutzernamen und Kennwort ist auf die Groß-/Kleinschreibung zu achten.

Feldname	Beschreibung
Add User	Benutzer hinzufügen. Ermöglicht das Erstellen eines neuen Benutzerprofils. Geben Sie den Namen des Benutzers ein und klicken Sie auf die Schaltfläche „**Add User**“, um den Benutzer der Liste hinzuzufügen.
User Settings	Benutzereinstellungen. Ermöglicht die Bearbeitung eines Benutzerprofils über das Dropdown-Menü. Rufen Sie das gewünschte Profil aus dem Dropdown-Menü auf. Bei Benutzernamen und Kennwort ist auf die Groß-/Kleinschreibung zu achten. Vergessen Sie nicht, das Kontrollkästchen „**Enable**“ zu markieren, um das Benutzerprofil zu aktivieren, da der dazugehörige Benutzer sonst nicht auf das Internet zugreifen kann. Wenn Sie ein Benutzerprofil entfernen möchten, wählen Sie das entsprechende Profil aus dem Dropdown-Menü aus und klicken Sie auf die Schaltfläche „**Remove User**“.
Password	Geben Sie das Kennwort des ausgewählten Benutzers in dieses Feld ein. Alle Benutzer müssen jedes Mal zuerst ihren Benutzernamen und ihr Kennwort eingeben, bevor sie das Internet nutzen können. Bei Benutzernamen und Kennwort ist auf die Groß-/Kleinschreibung zu achten. **Hinweis:** Das Gateway gestattet den einzelnen Benutzern entsprechend der für sie auf dieser Seite ausgewählten Regeln Zugriff auf das Internet.

Feldname	Beschreibung
Re-Enter Password	Kennwort erneut eingeben. Geben Sie das Kennwort, das Sie im vorigen Feld eingegeben haben, zur Bestätigung erneut ein.
Trusted User	Vertrauenswürdiger Benutzer. Aktivieren Sie dieses Kontrollkästchen, wenn der aktuell ausgewählte Benutzer ein vertrauenswürdiger Benutzer ist. Auf vertrauenswürdige Benutzer werden keine Zugriffsregeln für das Internet angewendet.
Content Rule	Inhaltsregel. Wählen Sie die Inhaltsregeln für das aktuelle Benutzerprofil. Inhaltsregeln müssen zuerst auf der Seite „Rules Configuration“ definiert werden. Klicken Sie dazu auf den Link „**Basic Rules**“ unter dem Abschnitt „Parental Control“ auf der Setup-Seite.
Time Access Rule	Tageszeit-Zugriffsregel. Wählen Sie die Regel für das aktuelle Benutzerprofil aus, die die Tageszeit für den Zugriff definiert. Diese Regeln müssen zuerst auf der Seite „Time of Day Filter“ definiert werden. Klicken Sie dazu auf den Link „**Time of Day Rules**“ unter dem Abschnitt „Parental Control“ auf der Setup-Seite.
Session Duration	Länge der Inaktivität. Die werkseitige Einstellung beträgt 1440 Minuten. Geben Sie ein, wie viele Minuten der Benutzer auf das Internet zugreifen darf, nachdem er sich mit Benutzernamen und Kennwort angemeldet hat. **Hinweis:** Geben Sie 0 (Null) ein, um eine Zeitüberschreitung bei der Sitzung zu verhindern.
Inactivity time	Länge der Inaktivität. Die werkseitige Einstellung beträgt 60 Minuten. Geben Sie die Länge der Inaktivität während einer Internetsitzung eines Benutzers ein, bei der davon ausgegangen werden soll, dass der Benutzer nicht länger online ist. Nach Ablauf dieser Zeit wird die Benutzersitzung automatisch geschlossen. Um wieder auf das Internet zugreifen zu können, muss sich der Benutzer erneut mit Benutzernamen und Kennwort anmelden. **Hinweis:** Geben Sie 0 (Null) ein, um eine Zeitüberschreitung aufgrund von Inaktivität zu verhindern.

Feldname	Beschreibung
Available Rules	Listet die verfügbaren Regeln auf. Wählen Sie eine Regel aus der Liste aus und fügen Sie sie dem aktuellen Benutzerprofil hinzu, um diese Regel anzuwenden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Regeln erstellt worden sind. Sie können Regeln auf den anschließend angezeigten Seiten zum Kinderschutz-Setup erstellen.
Current Used Rules	Aktuell angewendete Regeln. Führt die Regeln auf, die auf das aktuelle Benutzerprofil angewendet werden. Auf jedes Benutzerprofil können maximal vier Regeln angewendet werden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn dem Benutzerprofil eine Regel zugeordnet ist.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Parental Control - User Setup“ angezeigt.

Schaltfläche	Beschreibung
Add User	Benutzer hinzufügen. Fügt der Liste mit Benutzerprofilen einen neuen Benutzer hinzu und speichert das neue Profil.
Remove User	Benutzer entfernen. Entfernt den ausgewählten Benutzer aus der Liste mit Benutzerprofilen.
Apply	Anwenden. Speichert alle hinzugefügten, bearbeiteten und geänderten Daten.

Konfiguration der Grundregeln für den Kinderschutz

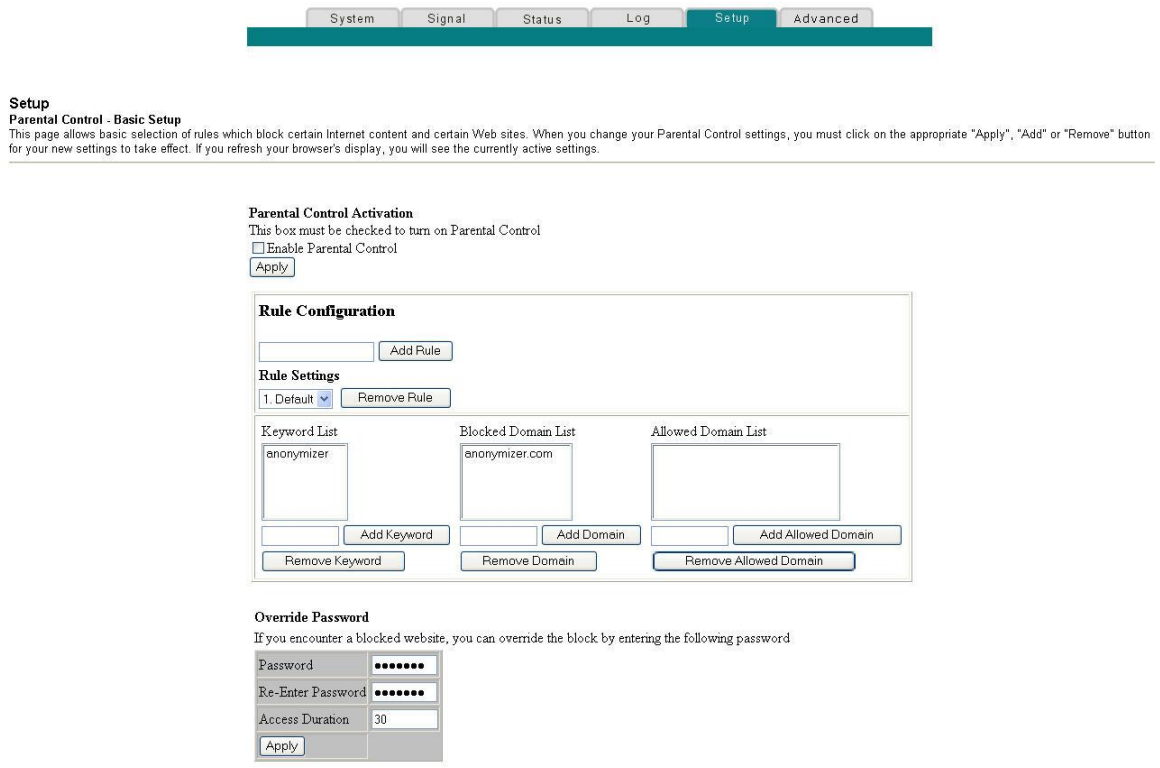
Auf der Seite „Setup Parental Control - Basic Setup“ können Sie Regeln auswählen, die bestimmte Internetinhalte und Websites sperren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Parental Control“ auf der Setup-Seite auf „**Basic Rules**“, um die Seite „Setup Parental Control - Basic Setup“ aufzurufen.

Die Seite „Setup Parental Control - Basic Setup“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Parental Control - Basic Setup“.



Beschreibung der Seite „Setup Parental Control - Basic Setup“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Parental Control - Basic Setup“. Auf dieser Seite können Sie anhand der in den URLs von Websites gefundenen Inhalte Zugriffsregeln für das Internet erstellen.

Feldname	Beschreibung
Parental Control Activation	Ermöglicht die Aktivierung bzw. Deaktivierung des Kinderschutzes. Markieren Sie zur Aktivierung des Kinderschutzes das Kontrollkästchen „**Enable Parental Control**“ und klicken Sie anschließend auf „**Apply**“. Wenn Sie den Kinderschutz deaktivieren möchten, heben Sie die Markierung des Kontrollkästchens „**Enable Parental Control**“ auf und klicken Sie anschließend auf „**Apply**“.
Rule Configuration	Regelkonfiguration. Ermöglicht das Hinzufügen neuer Inhaltsregeln. Geben Sie den Namen der Regel ein und klicken Sie auf die Schaltfläche „**Add Rule**“, um die Inhaltsregel der Liste hinzuzufügen. Inhaltsregeln schränken den Zugriff auf das Internet anhand der in den URLs von Websites gefundenen IP-Adressen, Domänen und Schlüsselwörtern ein. **Hinweis:** Es kann hilfreich sein, die erste Regel als „No Rule“ ohne jegliche Einschränkung oder Einstellung zu definieren. Auf diese Weise können Sie Benutzern, für die keine inhaltsbezogenen Zugriffseinschränkungen gelten, den Status „No Rule“ zuweisen.
Rule Settings	Regeleinstellungen. Ermöglicht die Bearbeitung einer Inhaltsregel über das Dropdown-Menü. Wenn Sie eine Regel entfernen möchten, wählen Sie die entsprechende Regel aus dem Dropdown-Menü aus und klicken Sie auf die Schaltfläche „**Remove Rule**“.
Keyword List	Schlüsselwortliste. Ermöglicht das Erstellen einer Liste mit Schlüsselwörtern. Alle Versuche, auf eine URL zuzugreifen, die eins dieser Schlüsselwörter enthält, werden vom Gateway unterbunden.
Blocked Domain List	Liste mit gesperrten Domänen. Ermöglicht das Erstellen einer Liste mit Domänen. Alle Versuche, auf eine der Domänen in dieser Liste zuzugreifen, werden vom Gateway unterbunden.
Allowed Domain List	Liste mit zugelassenen Domänen. Ermöglicht das Erstellen einer Liste mit Domänen, auf die zugegriffen werden darf.

Feldname	Beschreibung
Override Password	Kennwort zur Umgehung der Zugriffseinschränkungen. Ermöglicht das Einrichten eines Kennworts, mit dem Zugriffseinschränkungen auf eine gesperrte Website vorübergehend umgangen werden können.
Re-enter Password	Kennwort erneut eingeben. Geben Sie das Kennwort, das Sie im vorigen Feld zur Umgehung der Zugriffseinschränkungen haben, zur Bestätigung erneut ein.
Duration	Gültigkeitsdauer. Ermöglicht die Eingabe der Zeitspanne (in Minuten), für die das Kennwort den Zugriff auf eine gesperrte Website zulässt.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Parental Control - Basic Setup“ angezeigt.

Schaltfläche	Beschreibung
Add Rule	Regel hinzufügen. Fügt der Liste mit Inhaltsregeln eine neue Regel hinzu und speichert die Liste.
Remove Rule	Regel entfernen. Entfernt die ausgewählte Regel aus der Liste mit Inhaltsregeln.
Add/Remove Keyword	Schlüsselwort hinzufügen/entfernen. Durch Klicken auf diese Schaltfläche können Sie der Liste neue Schlüsselwörter hinzufügen oder ausgewählte Schlüsselwörter aus dieser Liste entfernen.
Add/Remove Domain	Domänen hinzufügen/entfernen. Durch Klicken auf diese Schaltfläche können Sie der Liste neue Domänen hinzufügen oder ausgewählte Domänen aus dieser Liste entfernen.
Add/Remove Allowed Domain	Zugelassene Domänen hinzufügen/entfernen. Durch Klicken auf diese Schaltfläche können Sie der Liste neue Domänen hinzufügen oder ausgewählte Domänen aus dieser Liste entfernen.
Apply	Anwenden. Speichert alle hinzugefügten, bearbeiteten und geänderten Daten.

So sperren Sie Websites anhand bestimmter Schlüsselwörter und Domänen

Durch Eingabe bestimmter Schlüsselwörter und Domänen können Sie den Zugriff auf Websites sperren, deren URL diese Wörter oder Zeichenketten enthält.

Durch Sperrung einer Domäne können Sie den Zugriff auf Websites einschränken, die diesen Domänennamen enthalten. Der Domänenname ist der Teil der URL, die vor einer der gängigen Erweiterungen .DE, .COM, .ORG usw. steht.

Durch Sperrung von Schlüsselwörtern können Sie den Zugriff auf Websites einschränken, deren URL – nicht nur der Domänenname – eines der Schlüsselwörter oder eine der Zeichenketten enthält.

Hinweis: Die Domänensperrfunktion verhindert den Zugriff auf alle in der Liste aufgeführten Domänen. Es werden ebenfalls Domänen gesperrt, deren Name eine genaue Entsprechung einer der Einträge der Liste enthält.

Wenn Sie beispielsweise der Liste die Domäne **beispiel.de** hinzufügen, werden alle Websites gesperrt, deren URL „beispiel.de“ enthält. Im Allgemeinen sollten Sie das Präfix „www.“ bei Domänennamen auslassen, da sonst nur die Website gesperrt wird, deren URL diesem Domänennamen genau entspricht. Wenn Sie beispielsweise der Liste die Domäne www.beispiel.de hinzufügen, wird nur die eine Website gesperrt, die genau diesem Namen entspricht. Wenn Sie das „www.“ nicht mit angegeben, werden dementsprechend alle Websites gesperrt, die „beispiel.de“ enthalten und mit dieser Domäne verbunden sind.

Konfiguration von Kinderschutz-Zugriffsfiltern anhand von Tageszeiten

Auf der Seite „Setup Parental Control - Time of Day Access Filter“ können Sie Internetzugriffsfilter konfigurieren, die zu von Ihnen festgelegten Tageszeiten sämtlichen Internetverkehr von und zu bestimmten Netzwerkgeräten blockieren.

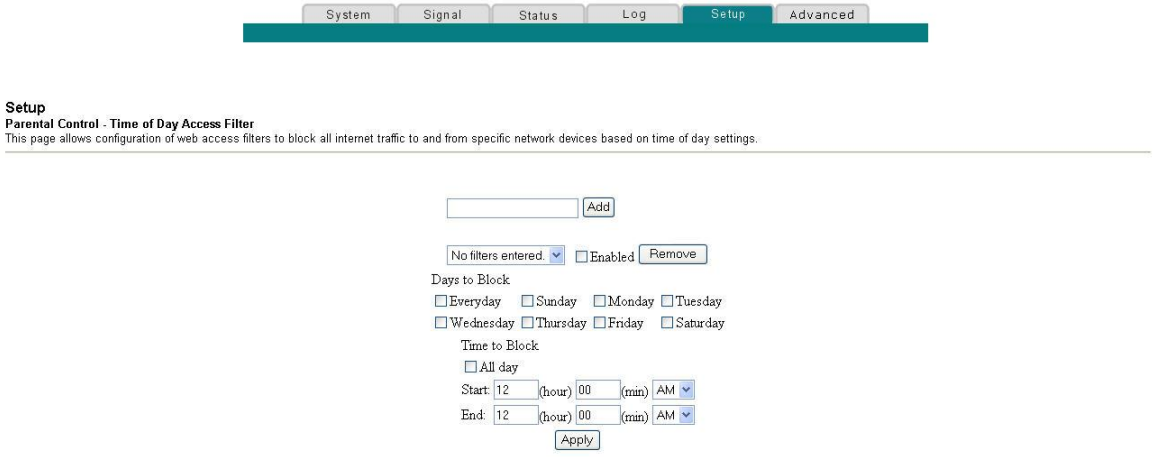
Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Parental Control“ auf der Setup-Seite auf „**Time of Day Rules**“, um die Seite „Setup Parental Control - Time of Day Access Filter“ aufzurufen.

Die Seite „Setup Parental Control - Time of Day Access Filter“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Parental Control - Time of Day Access Filter“.

Hinweis: Das Heim-Gateway benutzt für diese Funktion die Netzwerkuhr, die von Ihrem Datendienstanbieter verwaltet wird. Damit die Funktion ordnungsgemäß eingesetzt werden kann, muss die Uhr genau gehen und mit der Zeit in Ihrer Zeitzone übereinstimmen. Vergewissern Sie sich, dass die Seiten „Status“ und „Set Time“ die für Sie richtige Tageszeit anzeigen. Sollte dies nicht der Fall sein, wenden Sie sich an Ihren Datendienstanbieter. Sie können Ihre Einstellungen auch so anpassen, dass Unterschiede in der Zeit berücksichtigt werden.



Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Parental Control - Time of Day Access Filter“ angezeigt.

Schaltfläche	Beschreibung
Add	Hinzufügen. Ermöglicht das Hinzufügen eines neuen Zugriffsfilters oder einer neuen Zugriffsregel auf Basis der Tageszeit. Geben Sie den Namen des Filters ein und klicken Sie auf die Schaltfläche „Add“, um den Filter der Liste hinzuzufügen. Tageszeitenregeln schränken den Internetzugriff an bestimmten Tagen und zu bestimmten Uhrzeiten ein.
Remove	Entfernen. Entfernt den ausgewählten Filter aus der Liste mit Tageszeitenfiltern.
Apply	Anwenden. Speichert alle hinzugefügten, bearbeiteten und geänderten Daten.

Konfiguration des Kinderschutz-Ereignisprotokolls

Auf der Seite „Setup Parental Control - Event Log“ können Sie im Kinderschutz-Ereignisprotokoll festgehaltene Ereignisse anzeigen.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Parental Control“ auf der Setup-Seite auf „**Local Log**“, um die Seite „Setup Parental Control - Event Log“ aufzurufen.

Die Seite „Setup Parental Control - Event Log“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Parental Control - Event Log“.

Beschreibung der Seite „Setup Parental Control - Event Log“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Parental Control - Basic Setup“. Über diese Seite können Sie alle Versuche einzelner Besucher nachverfolgen, auf zugriffsbeschränkte Websites zuzugreifen.

Feldname	Beschreibung
Last Occurrence	Letzter Zugriffsversuch. Zeigt die Zeit des letzten Versuchs, auf eine zugriffsbeschränkte Website zu zugreifen, an.
Target	Ziel. Zeigt die URL der zugriffsbeschränkten Website an.
User	Benutzer. Zeigt den Benutzer an, der versucht hat, auf eine zugriffsbeschränkte Website zuzugreifen.
Source	Quelle. Zeigt die IP-Adresse des PCs an, der für den Zugriffsversuch auf eine zugriffsbeschränkte Website benutzt wurde.

Konfiguration der Parameter Ihres Wireless Access Point

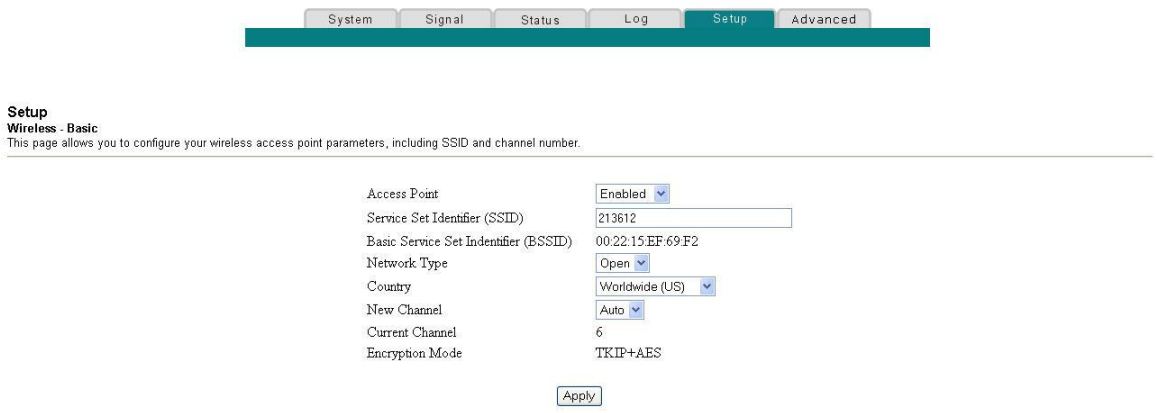
Auf der Seite „Setup Wireless - Basic“ können Sie grundlegende Parameter Ihres Wireless Access Point (WAP) wie beispielsweise die SSID (Service Set Identifier) und den Kanal konfigurieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Wireless“ auf der Setup-Seite auf „**Basic**“, um die Seite „Setup Wireless - Basic“ aufzurufen.

Die Seite „Setup Wireless - Basic“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Wireless - Basic“ mit den werksseitigen Standardeinstellungen.



Beschreibung der Seite „Setup Wireless - Basic“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Wireless - Basic“.

Hinweis: Wenn Sie auf der Seite „Setup Wireless - Basic“ Änderungen vornehmen, klicken Sie anschließend auf „**Apply**“, um die neuen Einstellungen anzuwenden und zu speichern.

Feldname	Beschreibung
Access-Point	Ermöglicht die Aktivierung bzw. Deaktivierung des Access Point des Gateways.

Feldname	Beschreibung
Service Set Identifier (SSID)	Der dem Access Point zugewiesene Name. **Hinweis:** Der werkseitige Wert des SSID-Feldes sollte die letzten 6 Ziffern der MAC-Adresse des Kabelmodems enthalten, die Sie dem Etikett auf dem Modem entnehmen können.
Basic Service Set Identifier (BSSID)	Die MAC-Adresse des Access Point.
Network Type	Ermöglicht die Auswahl von „**Open**“ (offen) oder „**Closed**“ (geschlossen) als Netzwerktyp.
Country	Land. Ermöglicht die Auswahl des Landes, in dem der Access Point verwendet wird.
New Channel (1-11)	Neuer Kanal (1-11). Ermöglicht die Auswahl eines Kommunikationskanals für den Access Point. **Hinweis:** Die Kanäle für kabellose Netzwerke überlappen einander. Die Kanäle 1, 6 und 11 überlappen einander nicht; deswegen sollten Sie für die beste Leistung einen dieser Kanäle auswählen. Falls im selben Bereich zusätzliche Access Points betrieben werden, sollten Sie einen dieser Kanäle wählen, der am weitesten von den anderen Access Points entfernt ist. **Beispiel:** Wird Kanal 8 von einem anderen Access Point benutzt, sollten Sie Kanal 1 für Ihr kabelloses Netzwerk auswählen. **Hinweis:** Wenn Ihr kabelloses Netzwerk nicht ordnungsgemäß funktioniert oder externe Geräte Ihr Signal stören, sollten Sie einen anderen Kanal auswählen. Mithilfe des Wireless-Dienstprogramms Ihres PCs können Sie nach anderen Access Points in Ihrem Bereich suchen.
Current Channel	Der gegenwärtig vom WAP verwendete Kanal.
Encryption Mode	Der aktuelle Verschlüsselungsmodus.

Konfiguration der Sicherheits- und Verschlüsselungsparameter Ihres kabellosen Netzwerks

Auf der Seite „Setup Wireless - Security“ können Sie die WEP (Wired Equivalent Privacy) Verschlüsselungscodes und die Authentifizierungsmethode für Ihren WAP konfigurieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Wireless“ auf der Setup-Seite auf „**Security**“, um die Seite „Setup Wireless - Security“ aufzurufen.

Wichtig: Bei der Lieferung ist auf Ihrem Heim-Gateway WPA-Sicherheit (Wi-Fi Protected Access) aktiviert, um wenigstens einen *grundlegenden* Schutz Ihres kabellosen Netzwerks zu gewährleisten. Bei Ihrem ersten Zugriff auf Ihr kabelloses Netzwerk müssen Sie deshalb auf dem WLAN-Adapter Ihres Computers WPA auswählen und den WPA-Schlüssel eingeben, der dem vorgegebenen Schlüssel Ihres Gateways entspricht. Bei diesem vorgegebenen WPA-Schlüssel des Gateways handelt es sich um die Seriennummer des Gerätes. Sie können diesen Standardschlüssel weiterbenutzen, sollten jedoch zur Maximierung der Sicherheit Ihres kabellosen Netzwerks einen anderen als den werksseitigen Standardschlüssel verwenden.

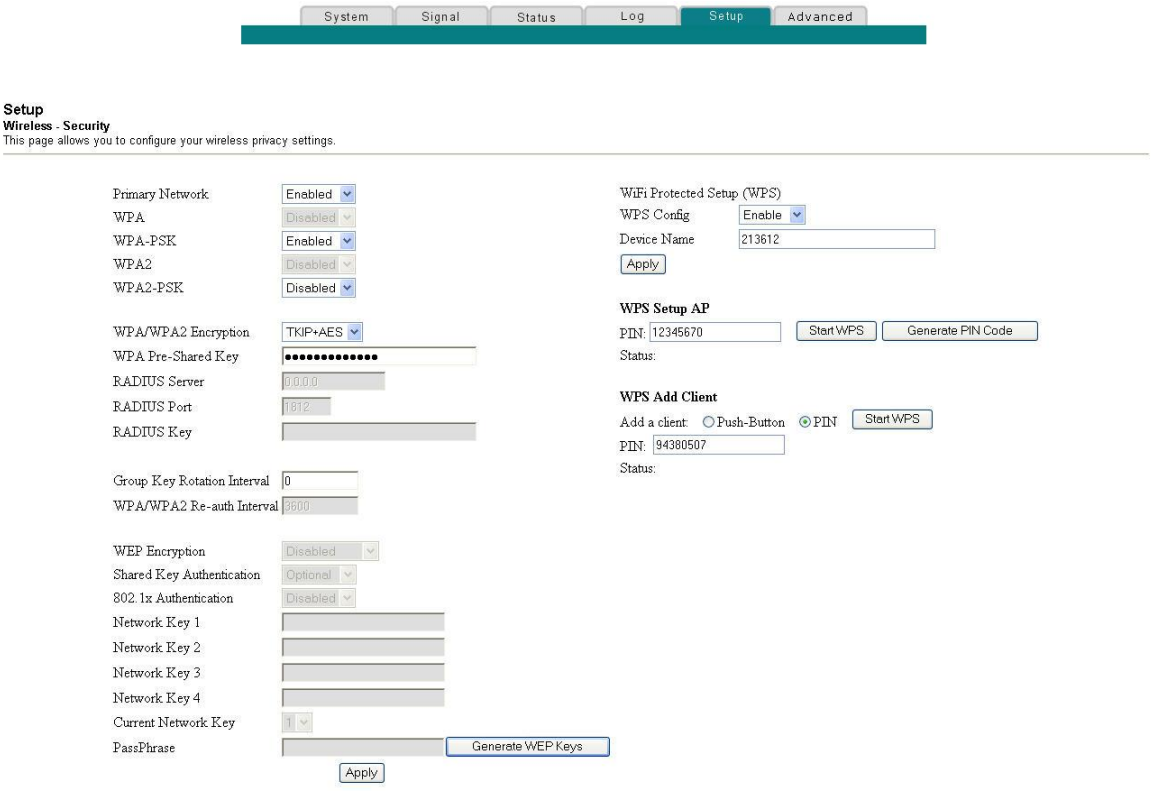
WPS (Wi-Fi Protected Setup)

Die Funktion WPS ermöglicht Ihnen, andere kabellose Geräte, die diese Funktion ebenfalls unterstützen, ganz einfach anzuschließen. Wenn die Funktion WPS aktiviert ist, können Sie einen anderen kabellosen Client mit einem Knopfdruck oder durch Eingabe der PIN des Clients anschließen.

Nach der Aktivierung von WPS können Sie die automatische Registrierung aktivieren, indem Sie auf die Schaltfläche „**Start WPS**“ im Abschnitt „WPS“ der Seite „Setup Wireless - Security“ klicken.

Die Seite „Setup Wireless - Security“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Wireless - Security“.



Beschreibung der Seite „Setup Wireless - Security“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Wireless - Security“.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen Einstellungen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern. Wenn Sie auf der Seite „Setup Wireless - Security“ Änderungen vornehmen, klicken Sie anschließend auf „**Apply**“, um die neuen Einstellungen anzuwenden und zu speichern.

Feldname	Beschreibung
Network Authentication	Die Netzwerk-Authentifizierung sorgt dafür, dass ausschließlich berechtigte Benutzer auf Ihr kabelloses Netzwerk zugreifen können. Nur Benutzern mit einem zugelassenen Benutzernamen, Kennwort oder vorher vereinbarten Schlüssel (Pre-Shared Key, PSK) wird der Zugriff auf das Netzwerk gestattet. Wählen Sie eins der folgenden Netzwerk-Authentifizierungsprotokolle aus: ■ Primary Network (primäres Netzwerk) ■ WPA ■ WPA-PSK ■ WPA2 ■ WPA2-PSK **Hinweis:** Die Netzwerk-Authentifizierung begrenzt den Zugang zu Ihrem kabellosen Netzwerk auf befugte Computer oder Benutzer. Die Authentifizierung schützt jedoch nicht die Daten, die Sie über die kabellose Netzwerkverbindung senden. Um die über Ihr kabelloses Netzwerk übertragenen Daten zu schützen, müssen Sie die Verschlüsselung aktivieren.
WPA/WPA2 Encryption	WPA/WPA2-Verschlüsselung. Ermöglicht die Auswahl einer WPA/WPA2-Sicherheitsmethode. Die vom Hersteller vorgegebene Sicherheitseinstellung ist WPA-PSK. ■ Die TKIP (Temporal Key Integrity Protocol) Datenverschlüsselung wird automatisch aktiviert, wenn WPA- oder WPA-PSK-Netzwerk Authentifizierung aktiviert ist (werkseitige Vorgabe). ■ AES (Advanced Encryption Standard) ■ TKIP-AES **Hinweis:** TKIP-AES sollte nur ausgewählt werden, wenn Ihr Client-Adapter diesen Modus unterstützt. Wenden Sie sich im Bedarfsfall an Ihren Dienstanbieter.

Feldname	Beschreibung
WPA Pre-Shared Key	Ermöglicht die Einrichtung eines WPA-PSK. Geben Sie eine Zeichenkette in dieses Feld ein. Die Zeichenkette bzw. der Kennsatz wird verwendet, um eine eindeutige Gruppe von Verschlüsselungscodes für Ihr Netzwerk zu generieren. Verwenden Sie diese Zeichenkette beim Setup der kabellosen Geräte in Ihrem Netzwerk. Der vom Hersteller vorgegebene Sicherheitsschlüssel ist die neunstellige Seriennummer des Gateways, beispielsweise 20167792. Informationen dazu, wo sich die Seriennummer auf dem Etikett befindet, finden Sie im Abschnitt ***High-Speed-Internetdienst*** (Seite 20). ■ Der PSK kann entweder aus einer Zeichenkette oder einer Hexadezimalzahl mit 64 Zeichen bestehen. ■ Die Zeichenkette muss aus mindestens 8 ASCII-Zeichen bestehen und darf eine Länge von 63 Zeichen nicht überschreiten. **Hinweis:** Nicht alle WLAN-Adapter unterstützen PSK. Bei diesen Geräten müssen Sie die Schlüssel genau so eingeben, wie sie in der vorhergehenden Abbildung der Seite „Setup Wireless Security“ in den Feldern des kabellosen Gateways aufgeführt werden.
RADIUS Server	Ermöglicht die Eingabe der IP-Adresse des RADIUS-Servers, der zur Authentifizierung und Ableitung von Verschlüsselungscodes verwendet wird. ■ Dieses Feld wird bei der 802.1x- und WPA-Netzwerkauthentifizierung benutzt. ■ Die werkseitige Einstellung dieses Feldes ist 0.0.0.0.
RADIUS Port	Legt die Portnummern des RADIUS-Servers fest. Die Portnummer ist je nach benutztem Server normalerweise 1812 (werkseitige Vorgabe) oder 1645. Dieses Feld wird bei der 802.1x- und WPA-Netzwerkauthentifizierung benutzt.
RADIUS Key	Ermöglicht die Einrichtung eines Shared Secret Key (SSK, vereinbarten Geheimschlüssels) für Ihre RADIUS-Verbindung. ■ Standardmäßig ist dieses Feld leer. ■ Dieses Feld wird bei der 802.1x- und WPA-Netzwerkauthentifizierung benutzt.

Feldname	Beschreibung
Group Key Rotation Interval	Intervall für den Wechsel des Gruppenschlüssels. Ermöglicht die Eingabe des Intervalls in Sekunden, in dem der Schlüssel gewechselt werden soll. Dies gilt nur, wenn die WPA- oder WPA2-Netzwerkauthentifizierung aktiviert ist. Geben Sie für diesen Wert 0 (werkseitige Vorgabe) ein, um die regelmäßige Authentifizierung zu deaktivieren. Der gültige Bereich reicht von 1 bis zu 4.294.967.295 Sekunden.
WPA/WPA2 Re-auth Interval	Intervall der erneuten WPA/WPA2-Authentifizierung. Ermöglicht die Eingabe des Intervalls in Sekunden, in dem die WPA/WPA2-Authentifizierung wiederholt werden soll. Dies gilt nur bei aktivierter WPA- oder WPA2-Netzwerkauthentifizierung. Geben Sie für diesen Wert 0 (werkseitige Vorgabe) ein, um die regelmäßige Authentifizierung zu deaktivieren. Der gültige Bereich reicht von 1 bis zu 4.294.967.295 Sekunden.
WEP Encryption	WEP-Verschlüsselung. Ermöglicht die Aktivierung der Datenverschlüsselung zum Schutz der über Ihr kabelloses Netzwerk übertragenen Daten. WEP 128 Bit ■ Datenverschlüsselung unter Verwendung eines statischen 128- oder 64-Bit-Schlüssels kann für Netzwerke ohne konfigurierte Authentifizierung ausgewählt werden. ■ Ist die 802.1x-Netzwerkauthentifizierung aktiviert, wird automatisch die Datenverschlüsselung unter Verwendung eines statischen 128-Bit-Schlüssels ausgewählt. **Hinweise:** ■ Die Authentifizierung mit einem statischen Schlüssel verwendet zur Verschlüsselung Ihrer Daten wie im Folgenden definiert einen der vier Verschlüsselungscodes. Sie müssen die Schlüssel manuell ändern; Anders als bei TKIP werden die Schlüssel nicht automatisch gewechselt. ■ 64-Bit- und 40-Bit-Verschlüsselung sind zwei verschiedene Bezeichnungen für dieselbe Verschlüsselungsmethode. ■ 128-Bit- und 104-Bit-Verschlüsselung sind zwei verschiedene Bezeichnungen für dieselbe Verschlüsselungsmethode.

Feldname	Beschreibung
Shared Key Authentication	Authentifizierung über einen vereinbarten Schlüssel. Ermöglicht Ihnen festzulegen, ob die Shared Key Authentication im Netzwerk verwendet wird. Die Shared Key Authentication kann dann eingesetzt werden, wenn keine andere Netzwerkauthentifizierung im Netzwerk verwendet wird. ■ Optional (werkseitige Vorgabe): Kabellose Clients können ohne Authentifizierung eine Verbindung mit dem Wireless Access Point herstellen. ■ Required (erforderlich): Nur kabellosen Clients mit einem gültigen Netzwerkschlüssel wird es gestattet, mit dem Access Point eine Verbindung herzustellen.
802.1x Authentication	802.1.x-Authentifizierung. Ermöglicht die Verwendung der 802.1x-Authentifizierung zusammen mit WEP-Verschlüsselung (vergleichbar mit aktiviertem WPA/WPA2).
Network Keys 1 - 4 64-Bit-Schlüssel	Wählen Sie diese Netzwerkschlüssel, wenn als Verschlüsselungsmodus die 64-Bit-Verschlüsselung ausgewählt ist. Geben Sie 5 Byte-Werte für einen Schlüssel ein. Sie brauchen nicht alle vier Schlüssel eingeben. Für ein Heimnetzwerk ist nur ein Schlüssel erforderlich. Jeder Wert wird als Hexadezimalzahl dargestellt. Die Schlüssel dürfen nur die folgenden Zeichen enthalten: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e und f. **Hinweis:** Im Allgemeinen sollten Sie WEP-Verschlüsselungscodes nur in Kleinbuchstaben eingeben, da Großbuchstaben manchmal mit Nummern verwechselt werden. So sieht beispielsweise der Buchstabe „B“ der Ziffer „8“ sehr ähnlich. Durch Verwendung von Kleinbuchstaben minimieren Sie das Risiko, dass beim Kopieren von Schlüsseln von einem Gerät auf ein anderes Zeichen verwechselt werden. Großbuchstaben werden automatisch in Kleinbuchstaben umgewandelt, wenn der Schlüssel angewendet und gespeichert wird. Geben Sie in jedes Kästchen zwei Zahlen oder Buchstaben ein. Schreiben Sie sich die eingegebenen Schlüssel auf, da Sie diese Werte beim Setup des WLAN-Adapters des Clients erneut eingeben müssen. Die Schlüssel aller Geräte im kabellosen Netzwerk müssen übereinstimmen.
oder	

Feldname	Beschreibung
Network Keys 1- 4 128-Bit-Schlüssel	Wählen Sie diese Netzwerkschlüssel, wenn als Verschlüsselungsmodus die 128-Bit-Verschlüsselung ausgewählt ist. Geben Sie 13 Byte-Werte für einen Schlüssel ein. Sie brauchen nicht alle vier Schlüssel eingeben. Für ein Heimnetzwerk ist normalerweise nur ein Schlüssel erforderlich. Jeder Wert wird als Hexadezimalzahl dargestellt. Die Schlüssel dürfen nur die folgenden Zeichen enthalten: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e und f. Im Allgemeinen sollten Sie WEP-Verschlüsselungscodes nur in Kleinbuchstaben eingeben, da Großbuchstaben manchmal mit Nummern verwechselt werden. So sieht beispielsweise der Buchstabe „B“ der Ziffer „8“ sehr ähnlich. Durch Verwendung von Kleinbuchstaben minimieren Sie das Risiko, dass beim Kopieren von Schlüsseln von einem Gerät auf ein anderes Zeichen verwechselt werden. Großbuchstaben werden automatisch in Kleinbuchstaben umgewandelt, wenn der Schlüssel angewendet und gespeichert wird. Geben Sie in jedes Kästchen zwei Zahlen oder Buchstaben ein. Schreiben Sie sich die eingegebenen Schlüssel auf, da Sie diese Werte beim Setup des WLAN-Adapters des Clients erneut eingeben müssen. Die Schlüssel aller Geräte im kabellosen Netzwerk *müssen* übereinstimmen.
Current Network Key	Aktueller Netzwerkschlüssel. Ermöglicht die Auswahl, welcher der vier 64- bzw. 128-Bit-Schlüssel zur Verschlüsselung Ihrer Daten verwendet werden soll, wenn Sie eine Verschlüsselungsmethode verwenden, bei der der Schlüssel manuell eingegeben werden muss. Es wird jeweils nur ein WEP-Schlüssel benutzt. Sie müssen die Schlüssel manuell ändern; sie werden nicht automatisch geändert. **Hinweise:** ■ 64-Bit- und 40-Bit-Verschlüsselung sind zwei verschiedene Bezeichnungen für dieselbe Verschlüsselungsmethode. ■ 128-Bit- und 104-Bit-Verschlüsselung sind zwei verschiedene Bezeichnungen für dieselbe Verschlüsselungsmethode.

Feldname	Beschreibung
PassPhrase	Kennsatz. Erstellt anhand des eingegebenen Kennsatzes automatisch die WEP-Schlüssel, die zur Kommunikation mit dem Netzwerk erforderlich sind. Obwohl für den WEP-Betrieb kein Kennsatz erforderlich ist, lässt sich damit die Konfiguration und das Setup der individuellen Client-WLAN-Adapter vereinfachen: Die manuelle Eingabe langer Schlüssel entfällt und das Risiko, dass bei dieser Eingabe Fehler passieren, wird reduziert. **Wichtig:** Klicken Sie nach Eingabe des Kennsatzes auf „**Generate WEP Keys**“.

Der Abschnitt „Wi-Fi Protected Setup (WPS)“

Über die Auswahlmöglichkeiten in diesem Abschnitt können Sie die Funktion WPS konfigurieren.

Feldname	Beschreibung
WPS Config	Ermöglicht die Aktivierung bzw. Deaktivierung von WPS.
Device Name	Ermöglicht die Eingabe des Gerätenamens.

Der Abschnitt „WPS Setup AP“

Über die Auswahlmöglichkeiten in diesem Abschnitt können Sie als zusätzlichen Sicherheitsschutz eine PIN konfigurieren.

Feldname	Beschreibung
PIN	Die Personal Identification Number (PIN) eines Gerätes, das versucht, eine Verbindung herzustellen.
Status	Zeigt den WPS-Status an.

Der Abschnitt „WPS Add Client“

Über die Auswahlmöglichkeiten in diesem Abschnitt können Sie einen WPS-Client hinzufügen.

Feldname	Beschreibung
Add a Client	Client hinzufügen. Ermöglicht die Auswahl der WPS-Methode (Knopf oder PIN).
WPS Status	Zeigt den WPS-Status an.

Schaltflächen

Schaltflächen	Beschreibung
Generate WEP Keys	WEP-Schlüssel generieren. Generiert anhand des eingegebenen Kennsatzes automatisch vier WEP-Schlüssel. **Hinweise:** ■ Bei 64-Bit-WEP werden vier unterschiedliche 64-Bit-WEP-Schlüssel generiert. ■ Bei 128-Bit-WEP wird nur ein einziger 128-Bit-WEP-Schlüssel generiert, der in alle vier Schlüsselfelder eingegeben wird.
Apply	Anwenden. Speichert alle im dazugehörigen Abschnitt hinzugefügten, bearbeiteten und geänderten Daten.
Start WPS	Startet WPS, nachdem Sie die gewünschte WPS-Methode ausgewählt haben.
Generate PIN Code	Generiert automatisch einen PIN-Code.

Konfiguration der Wireless-Datenraten und Wi-Fi-Schwellenwerte

Auf der Seite „Setup Wireless – Advanced“ können Sie Ihre WAP-Datenraten und Wi-Fi-Grenzwerte konfigurieren.

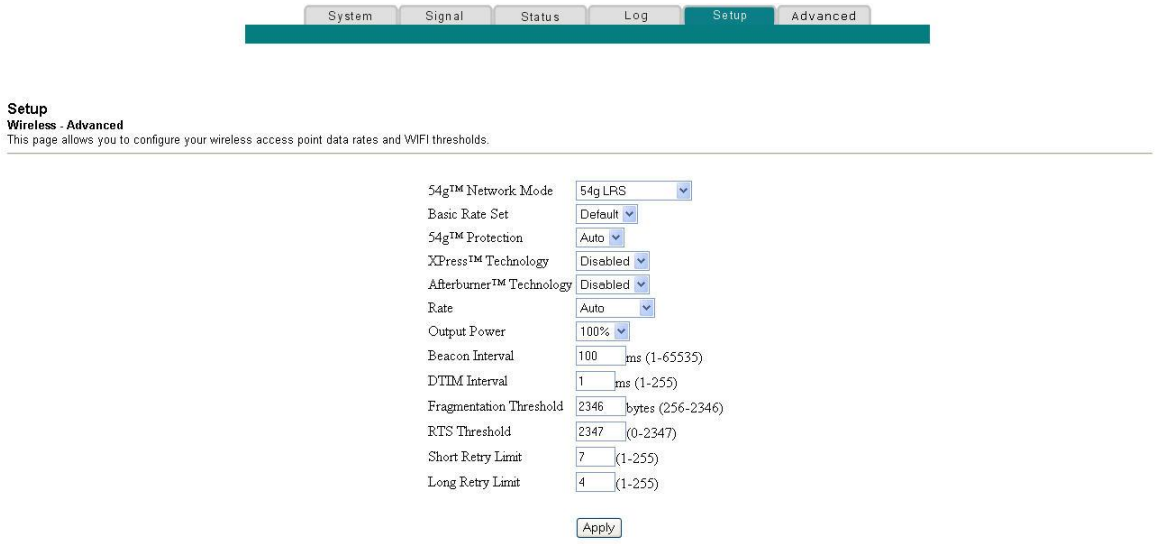
Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Wireless“ auf der Setup-Seite auf „**Advanced**“, um die Seite „Setup Wireless - Advanced“ aufzurufen.

Die Seite „Setup Wireless - Advanced“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Wireless - Advanced“.

Hinweis: Sie sollten die in der nachstehenden Abbildung gezeigten Wireless-Standardeinstellungen nur auf Anweisung Ihres Dienstanbieters ändern.



Beschreibung der Seite „Setup Wireless - Advanced“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Wireless - Advanced“.

Hinweis: Wenn Sie auf der Seite „Setup Wireless - Advanced“ Änderungen vornehmen, klicken Sie anschließend auf „**Apply**“, um die neuen Einstellungen anzuwenden und zu speichern.

Feldname	Beschreibung
54g Network Mode	54g-Netzwerkmodus. Ermöglicht die Optimierung der Leistung des kabellosen Netzwerks unter Verwendung einer der folgenden Optionen: ■ Max compatibility (factory default) Maximale Kompatibilität (werkseitige Vorgabe). Der Access Point arbeitet mit kabellosen 802.11b- und 802.11g-Client-Geräten zusammen und minimiert Störungen durch nahegelegene kabellose 802.11b-Netzwerke. ■ 54g Only Nur 54g. Der Wireless Access Point akzeptiert ausschließlich kabellose 802.11g-Clients. ■ 54g LRS 54g Limited Rate Support (Unterstützung begrenzter Raten). Der Wireless Access Point unterstützt Clients, die mit dem 802.11g-Modus nicht vollständig kompatibel sind. **Hinweis:** Der Betrieb im 54g-LRS-Modus kann die Wireless-Leistung beeinträchtigen. Deshalb sollten Sie diesen Modus nur bei den oben beschriebenen Kompatibilitätsproblemen benutzen. ■ Max Performance Maximaler Durchsatz. In diesem Modus akzeptiert der Wireless Access Point ausschließlich kabellose 802.11g-Clients. Der Betrieb in diesem Modus beeinträchtigt möglicherweise die Leistung nahegelegener kabelloser 802.11b-Netzwerke.
Basic Rate Set	Ermöglicht die Auswahl der Mindestübertragungsrate.

Feldname	Beschreibung
54g Protection	54g-Schutz. Ermöglicht die Bevorzugung von 802.11g-Datenverkehr, wenn sich im kabellosen Netzwerk sowohl 802.11b- als auch 802.11g-Geräte befinden. Zur Wahl stehen die folgenden Optionen: ■ Auto (factory default) Auto (werkseitige Vorgabe). Maximiert die 802.11g-Leistung in Netzwerken mit sowohl 802.11b- als auch 802.11g-Client-Geräten. ■ Off Aus. Maximale Leistung für Netzwerke, in denen sich ausschließlich 802.11g-Client-Geräte befinden.
Xpress Technology	Ermöglicht die Aktivierung bzw. Deaktivierung der Xpress Technology.
Afterburner Technology	Ermöglicht die Aktivierung bzw. Deaktivierung der Afterburner Technology.
Rate	Ermöglicht die Festlegung der Datenrate für kabellose Verbindungen. Die folgenden Datenraten können eingestellt werden: Auto (werkseitige Vorgabe), 1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s, 6 Mbit/s, 9 Mbit/s, 11 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, 54 Mbit/s **Hinweis:** Im automatischen Modus wird die Datenrate automatisch an Signalstärke und Signalqualität angepasst.
Output Power	Ausgangsleistung. Ermöglich die Anpassung der relativen Ausgangsleistung des Wireless-Senders Ihres Gateways. Die folgenden Einstellungen stehen zur Wahl: 100% (werkseitige Vorgabe), 75%, 50% und 25%.
Beacon Interval	Zeigt das Intervall an, in dem sich der WAP bei Remote-Geräten meldet. Das Beacon Interval sollte auf 100 ms belassen werden, um Kompatibilität mit den meisten Client-Karten zu gewährleisten. Dieses Zeitstrahl-Intervall legt fest, wie oft der Wireless Access Point (WAP) Datenpakete zur Synchronisierung zwischen kabellosem Netzwerk und Clients aussendet.

Feldname	Beschreibung
DTIM Interval	Delivery Traffic Indication Message Interval. Zeigt das Intervall zwischen Broadcast/Multicast-Übertragungen an. Das DTIM-Intervall informiert die kabellosen Clients als Countdown, wann sie Broadcast- und Multicast-Nachrichten erwarten können. Wenn der Access Point Broadcast- oder Mulicast-Nachrichten für zugeordnete Clients zwischengespeichert hat, sendet er die nächste DTIM zusammen mit einem DTIM-Intervall-Wert aus. AP-Clients hören die Beacons und werden aktiviert, um die Broadcast- und Multicast-Nachrichten zu empfangen. Das DTIM-Intervall sollte auf 3 ms belassen werden, um Kompatibilität mit den meisten Client-Karten zu gewährleisten.
Fragmentation Threshold	Ermöglicht die Einstellung der Fragmentierungsschwelle. Dieser Schwellenwert sollte der maximalen Größe der Ethernet-Frames (einschließlich des Overheads von 1536 Bytes) entsprechen, die für die Verbindung zugelassen ist. Bei niedrigeren Einstellungen wird möglicherweise der Datendurchsatz beeinträchtigt, da große Frames fragmentiert werden oder Kollisionen auftreten könnten. Die werkseitige Vorgabe ist 2346.
RTS Threshold	RTS-Schwelle. Legt die Paketgröße fest, bei deren Überschreitung der RTS/CTS-Mechanismus (ready to send/clear to send) in Kraft tritt. Die werkseitige Vorgabe ist 2347.
Short Retry Limit	Grenzwert für das Senden zu „kurzer“ Frames. Die Anzahl der Versuche des Gateways, einen unbestätigten, unterhalb der RTS-Schwelle liegenden Unicast-Frame zu übertragen, bevor er verworfen wird. Die werkseitige Vorgabe ist 7.
Long Retry Limit	Grenzwert für das Senden zu „langer“ Frames. Die Anzahl der Versuche des Gateways, einen unbestätigten, oberhalb der RTS-Schwelle liegenden Unicast-Frame zu übertragen, bevor er verworfen wird. Die werkseitige Vorgabe ist 4.

Konfiguration der Zugriffskontrolle des Wireless Access Point

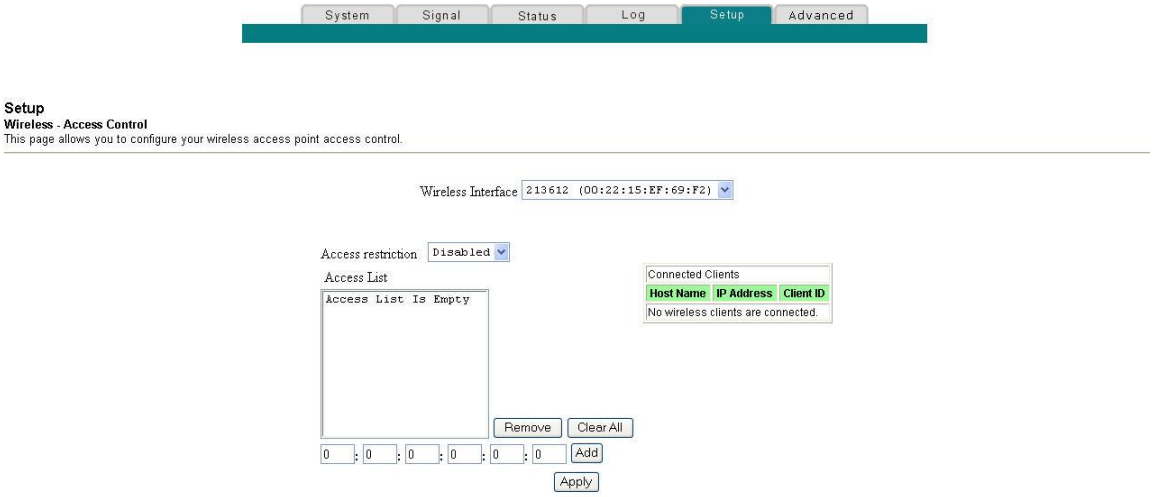
Auf der Seite „Setup Wireless - Access Control“ können Sie die Zugriffskontrolle Ihres Wireless Access Point konfigurieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Wireless“ auf der Setup-Seite auf „**Access Control**“, um die Seite „Setup Wireless - Access Control“ aufzurufen.

Die Seite „Setup Wireless - Access Control“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Wireless - Access Control“.



Beschreibung der Seite „Setup Wireless - Access Control“

Dieser Abschnitt enthält Beschreibungen der einzelnen Abschnitte und Felder auf der Seite „Setup Wireless - Access Control“.

Feldname	Beschreibung
Access restriction	Zugriffsbeschränkung. Bei aktivierter Verschlüsselung können Sie in diesem Abschnitt eine der folgenden Optionen aus der Dropdown-Liste auswählen: ■ Deaktivieren (werkseitige Vorgabe). Es findet keine Zugriffsbeschränkung anhand der MAC-Adressen kabelloser Zugriffsgeräte statt. ■ Zulassen. Gestattet ausschließlich den in der Zugriffsliste aufgeführten MAC-Adressen den kabellosen Zugriff. ■ Verweigern. Verweigert ausschließlich den in der Zugriffsliste aufgeführten MAC-Adressen den kabellosen Zugriff.
Closed Network	Geschlossenes Netzwerk. Ermöglicht Ihnen, kabellosen Clients den Zugriff auf das Netz zu verweigern. Bei „ON“ (ein) überträgt der Access Point seine SSID nicht. Das Client-Gerät muss manuell mit der SSID und MAC-Adresse des Access Point konfiguriert werden, damit es auf das kabellose Netzwerk zugreifen kann.
Access List	Zugriffsliste. Zeigt die MAC-Adressen der Clients an, deren Zugriff auf das kabellose Netzwerk kontrolliert wird.
Connected Clients	Verbundene Clients. Zeigt den Hostnamen, die IP-Adresse und die Client-ID der kabellosen Clients an, die mit dem Gateway-Modem verbunden (diesem zugeordnet) sind.

Schaltflächen

Die folgenden Schaltflächen werden auf der Seite „Setup Wireless - Access Control“ angezeigt.

Schaltfläche	Beschreibung
Apply	Anwenden. Wendet die von Ihnen eingegebenen Werte an und speichert sie, ohne das Fenster zu schließen.
Clear All	Alle löschen. Löscht die Zugriffsliste.
Remove	Entfernen. Entfernt Einträge aus der Zugriffsliste.
Add	Hinzufügen. Fügt der Zugriffsliste die MAC-Adresse eines Clients hinzu.

Konfiguration von Remote-Brücken

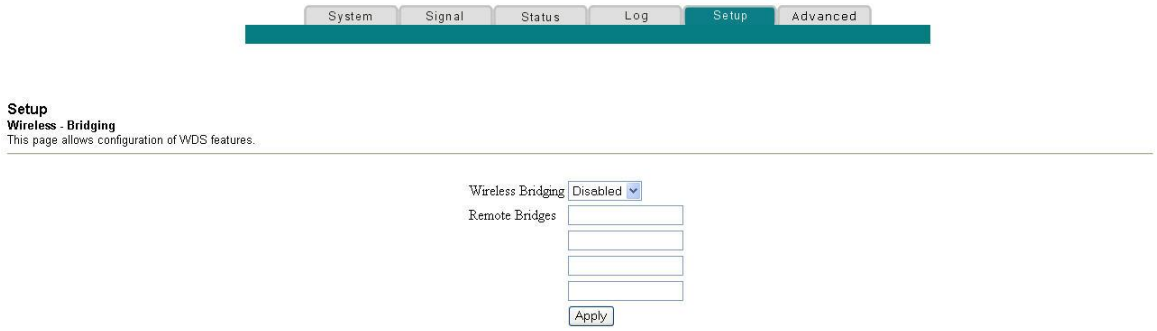
Auf der Seite „Setup Wireless - Bridging“ können Sie Remote-Brücken konfigurieren.

Hinweis: Wenn Sie mit den in diesem Abschnitt beschriebenen erweiterten Funktionen nicht vertraut sind, sollten Sie sich an Ihren Dienstanbieter wenden, bevor Sie die Standardeinstellungen Ihres Heim-Gateways ändern.

Klicken Sie im Abschnitt „Wireless“ auf der Setup-Seite auf „**Bridging**“, um die Seite „Setup Wireless - Bridging“ aufzurufen.

Die Seite „Setup Wireless - Bridging“

Die folgende Abbildung ist ein Beispiel der Seite „Setup Wireless - Bridging“.



Beschreibung der Seite „Setup Wireless - Bridging“

Auf der Seite „Setup Wireless - Bridging“ können Sie Remote-Brücken hinzufügen und aktivieren bzw. deaktivieren. Klicken Sie auf „**Apply**“, um die neuen Einstellungen anzuwenden und zu speichern.

Problembehebung bei der Einrichtung des Internets

Ich kann keine Verbindung mit dem Internet herstellen

- Vergewissern Sie sich, dass der Netzteilstecker Ihres Heim-Gateways ordnungsgemäß in eine Steckdose gesteckt ist.
- Überprüfen Sie, ob sich der Netzteilstecker Ihres Heim-Gateways in einer Steckdose befindet, die über einen Wandschalter kontrolliert wird. Sollte dies der Fall sein, achten Sie darauf, dass sich der Schalter in der **EIN**-Position befindet.
- Überprüfen Sie, ob die mit **POWER** und **CABLE** beschrifteten LED-Anzeigen auf der Vorderseite des Heim-Gateways leuchten.
- Überprüfen Sie, ob die LED-Anzeigen am Router oder anderen Netzwerkgeräten leuchten.
- Überprüfen Sie, ob alle Kabel ordnungsgemäß angeschlossen sind und ob Sie die richtigen Kabel benutzen.
- Überprüfen Sie, ob Ihr Kabeldienst aktiv ist und bidirektionale Kabelverbindungen unterstützt.
- Wenn Sie die Ethernet-Verbindungen benutzen, überprüfen Sie, ob auf allen Geräten TCP/IP ordnungsgemäß installiert und konfiguriert ist.
- Haben Sie Ihren Dienstanbieter angerufen und ihm die Seriennummer und die MAC-Adresse Ihres Heim-Gateways mitgeteilt?
- Wenn Sie einen Kabelsplitter benutzen, um das Kabelsignal an andere Geräte weiterzuleiten, entfernen Sie den Splitter und schließen Sie das Kabel erneut an, sodass das Heim-Gateway direkt mit dem Hauptkabeleingang verbunden ist. Funktioniert das Heim-Gateway jetzt ordnungsgemäß, ist der Kabelsplitter möglicherweise defekt und muss ausgetauscht werden.
- Für die beste Leistung über eine Ethernet-Verbindung sollte Ihr PC mit einer 10/100BASE-T-NIC (Network Interface Card) ausgestattet sein.

Mein Heim-Gateway erkennt das Kabelnetzwerk nicht

- Das Heim-Gateway benutzt ein herkömmliches HF-Koaxialkabel (75 Ohm). Mit einem anderen Kabel funktioniert Ihr Heim-Gateway nicht ordnungsgemäß. Wenden Sie sich an Ihren Dienstanbieter, um festzustellen, ob Sie das richtige Kabel verwenden.
- Möglicherweise müssen Sie die IP-Adresse Ihres PCs erneuern. Anleitungen zum Erneuern der IP-Adresse für Ihr bestimmtes Betriebssystem finden Sie im Abschnitt „Wie erneuere ich die IP-Adresse meines PCs?“.

Häufig gestellte Fragen

F. Wie viele Ethernet-Netzwerkgeräte kann ich anschließen?

A. Ihr Heim-Gateway verwendet ein integriertes Dynamic Host Configuration Protocol (DHCP), um Geräten, wenn sie mit Ihrem Heimnetzwerk verbunden werden, automatisch IP-Adressen zuzuweisen.

Theoretisch beträgt die Höchstzahl der von Ihrem Heim-Gateway unterstützten Geräte 253. Dabei werden allen – verkabelten (Ethernet) und kabellosen – verbundenen Geräten IP-Adressen zugewiesen. Normalerweise ist die Anzahl der verbundenen Geräte viel geringer.

Das Heim-Gateway kann mehrere Ethernet-Geräte direkt über die Ethernet-Ports auf der Rückseite oder unter Verwendung externer Multiport-Ethernet-Switches (separat erhältlich) unterstützen.

Nähere Informationen zur Höchstzahl der ohne Beeinträchtigung der optimalen Netzwerkleistung verwendbaren Ethernet-Netzwerkgeräte erhalten Sie von Ihrem Dienstanbieter.

F. Was muss ich bei der Verkabelung des Ethernet-Netzwerks beachten?

A. Die Größe des Netzwerks wird von einer Reihe praktischer Faktoren beeinflusst. Obwohl das Heim-Gateway für die Unterstützung mehrerer Ethernet-Netzwerkgeräte ausgestattet ist, müssen Sie die Eigenschaften des gesamten Netzwerks und nicht nur die einzelnen Knoten berücksichtigen.

Theoretisch können zwei 10/100BASE-T CAT-5-Ethernet-Hubs in einem Abstand von 100 Metern voneinander aufgestellt werden. Bei Fragen hierzu wenden Sie sich an Ihren Dienstanbieter oder ziehen Sie die Dokumentation Ihrer Ethernet-Netzwerkgeräte zu Rate.

Hinweis: Sie sollten Ethernet-Kabel der Qualität CAT-5 verwenden.

F. Wo ist der beste Aufstellungsort für meine Ethernet-Netzwerkgeräte?

A. Sie sollten zusammen mit Ihrem Dienstanbieter den besten Aufstellungsort für Ihre Ethernet-Netzwerkgeräte auswählen. Beachten Sie dabei Folgendes:

- Zugang zu bidirektionalen Kabelausgängen
- Entfernung der Ethernet-Netzwerkgeräte vom Heim-Gateway
- Zugang zu Netzsteckdosen für Computer und andere Geräte
- Leichte Führung des Ethernet-Kabels zu den Ethernet-Netzwerkgeräten

F. Was muss ich bei meinem kabellosen Netzwerk beachten?

A. Es ist wichtig, dass Sie die Eigenschaften des gesamten Netzwerks und nicht nur die einzelnen Knoten berücksichtigen. Der theoretisch mögliche Abstand zwischen kabellosen Netzwerkgeräten beträgt in Gebäuden etwa 30 m und im Freien etwa 90 m.

Die Größe des Netzwerks wird von einer Reihe praktischer Faktoren beeinflusst. Bei Fragen hierzu wenden Sie sich an Ihren Dienstanbieter oder ziehen Sie die Dokumentation Ihrer kabellosen Netzwerkgeräte zu Rate.

F. Wo ist der beste Aufstellungsort für meine kabellosen Netzwerkgeräte?

A. Sie können mit Ihrem Heim-Gateway eine Vielzahl kabelloser Netzwerkgeräte wie beispielsweise Computer, PDAs usw. verwenden. Alle mit dem kabellosen Netzwerk verbundenen Geräte beeinflussen die Eigenschaften des Netzwerks, da jedes dieser Geräte ein Funksignal überträgt.

Bei Fragen zur Auswahl geeigneter kabelloser Netzwerkgeräte für Ihr Heim- oder Firmennetzwerk wenden Sie sich an Ihren Dienstanbieter oder ziehen Sie die Dokumentation Ihrer kabellosen Netzwerkgeräte zu Rate.

Sie sollten zusammen mit Ihrem Dienstanbieter den besten Aufstellungsort für Ihre kabellosen Netzwerkgeräte auswählen. Beachten Sie dabei Folgendes:

- Entfernung der kabellosen Netzwerkgeräte vom Heim-Gateway
- Platzieren Sie das Heim-Gateway nicht in der Nähe von Metalloberflächen, die den Weg der Funkkommunikation blockieren können. Durch nicht metallische Wände verläuft die Funkkommunikation entlang der Sichtlinie. Je mehr Gebäudeteile (Wände) das Signal durchqueren muss, desto schwächer wird es empfangen.
- Platzieren Sie kabellose Netzwerkgeräte nicht in der Nähe eines Mikrowellenherdes, da die von laufenden Mikrowellenherden ausgehenden Strahlungen die Funkübertragung stören können.
- Platzieren Sie Ihre kabellosen Netzwerkgeräte nicht in der Nähe von schnurlosen Telefonen mit einem Frequenzbereich von 2,4 GHz.

F. Wie erneuere ich die IP-Adresse meines PCs?

A. Wenn Sie mit Ihrem PC nicht auf das Internet zugreifen können, nachdem das Heim-Gateway eine Verbindung mit dem Internet hergestellt hat, besteht die Möglichkeit, dass Ihr PC seine IP-Adresse nicht erneuert hat. Befolgen Sie die für Ihr Betriebssystem geltenden Anweisungen in diesem Abschnitt, um die IP-Adresse Ihres PCs zu erneuern.

Erneuern der IP-Adresse unter Windows NT, 2000 oder XP

1. Klicken Sie auf „**Start**“ und anschließend auf „**Ausführen**“. Das Fenster „Ausführen“ wird angezeigt.
2. Geben Sie in das Eingabefeld „**cmd**“ ein und klicken Sie anschließend auf „**OK**“. Ein Befehlszeilenfenster wird geöffnet.
3. Geben Sie nach dem C:/-Prompt „**ipconfig/release**“ ein und drücken Sie die Eingabetaste. Das System gibt die IP-Adresse frei.
4. Geben Sie nach dem C:/-Prompt „**ipconfig/renew**“ ein und drücken Sie die Eingabetaste. Das System zeigt eine neue IP-Adresse an.
5. Klicken Sie auf das **X** in der rechten oberen Ecke, um das Befehlszeilenfenster zu schließen. Sie haben die Konfiguration abgeschlossen.

   Hinweis: Wenn Sie nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Dienstanbieter.

Erneuern der IP-Adresse unter Windows 95, 98, 98SE und ME

1. Klicken Sie auf „**Start**“ und anschließend auf „**Ausführen**“, um das Fenster „Ausführen“ zu öffnen.
2. Geben Sie in das Eingabefeld „**winipcfg**“ ein und klicken Sie anschließend auf „**OK**“, um den Befehl „winipcfg“ auszuführen. Das Fenster „IP-Konfiguration“ wird angezeigt.
3. Klicken Sie auf den nach unten zeigenden Pfeil rechts neben dem obersten Feld und wählen Sie den auf Ihrem PC installierten Ethernet-Adapter aus. Das Fenster „IP-Konfiguration“ zeigt die Informationen zum Ethernet-Adapter an.
4. Klicken Sie auf „**Freigeben**“ und anschließend auf „**Erneuern**“. Das Fenster „IP-Konfiguration“ zeigt eine neue IP-Adresse an.
5. Klicken Sie auf „**OK**“ um das Fenster zu schließen. Sie haben die Erneuerung der IP-Adresse abgeschlossen.

   Hinweis: Wenn Sie nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Dienstanbieter.

F. Wie konfiguriere ich das TCP/IP-Protokoll?

A. Das TCP/IP-Protokoll ist für jedes Betriebssystem unter Microsoft Windows verschieden. Befolgen Sie die für Ihr Betriebssystem geltenden Anweisungen in diesem Abschnitt.

Konfiguration von TCP/IP unter Windows XP

1. Klicken Sie auf „**Start**“ und wählen Sie dem Setup Ihres Startmenüs entsprechend eine der folgenden Optionen:
   - Wenn Sie das Standardstartmenü von Windows XP benutzen, wählen Sie „**Verbinden mit**“ > „**Alle Verbindungen anzeigen**“ und machen Sie anschließend mit Schritt 2 weiter.
   - Wenn Sie das klassische Startmenü von Windows XP benutzen, wählen Sie „**Einstellungen**“ > „**Netzwerkverbindungen**“. Doppelklicken Sie im Abschnitt „LAN oder Hochgeschwindigkeitsinternet“ der Seite „Netzwerkverbindungen“ auf das Symbol „**LAN-Verbindung**“.
2. Klicken Sie im daraufhin angezeigten Fenster „Netzwerkverbindungen“ mit der rechten Maustaste auf „**LAN-Verbindung**“ und wählen Sie aus dem Kontextmenü die Option „**Eigenschaften**“, um das Dialogfeld „Eigenschaften“ aufzurufen.
3. Unter der Überschrift „Diese Verbindung verwendet die folgenden Elemente:“ finden Sie eine Liste. Führen Sie mit dem Pfeil auf der rechten Seite der Liste einen Bildlauf nach unten bis „Internetprotokoll (TCP/IP)“ durch. Wählen Sie „**Internetprotokoll (TCP/IP)**“und klicken Sie anschließend auf die Schaltfläche „**Eigenschaften**“ rechts unter der Liste.
4. Markieren Sie im Fenster „Internetprotokolleigenschaften (TCP/IP)“ die beiden Kontrollkästchen „**IP-Adresse automatisch beziehen**“ und „**DNS-Serveradresse automatisch beziehen**“ und klicken Sie anschließend auf „**OK**“.
5. Klicken Sie unten im Eigenschaftenfenster auf „**OK**“, um das Dialogfeld zu schließen. Jetzt fordert Ihr PC automatisch eine IP-Adresse vom Gateway an. Sobald das System die Adresse erhalten hat, kann es auf das Internet zugreifen.
6. Falls Ihr PC nach Durchführung der oben beschriebenen Schritte nicht automatisch eine IP-Adresse anfordert, sollten Sie auf die Windows-Schaltfläche „**Start**“ klicken und den Computer neu starten.
7. Wenn Sie nach dem Neustart nicht auf das Internet zugreifen können, lesen Sie den Abschnitt ***Problembehebung*** (Seite 113). Sollten Sie daraufhin noch immer nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Dienstanbieter.

Konfiguration von TCP/IP unter Windows 2000

1. Klicken Sie auf „**Start**“ > „**Einstellungen**“ > „**Netzwerk- und DFÜ-Verbindungen**“.
2. Doppelklicken Sie im Fenster „Netzwerk- und DFÜ-Verbindungen“ auf das Symbol „**LAN-Verbindung**“.
3. Klicken Sie im Fenster „LAN-Verbindungsstatus“ auf „**Eigenschaften**“.

4 Klicken Sie im Fenster „Eigenschaften von LAN-Verbindung“ auf „**Internetprotokoll (TCP/IP)**“ und anschließend auf „**Eigenschaften**“.

5 Markieren Sie im Fenster „Internetprotokolleigenschaften (TCP/IP)“ die beiden Kontrollkästchen „**IP-Adresse automatisch beziehen**“ und „**DNS-Serveradresse automatisch beziehen**“ und klicken Sie anschließend auf „**OK**“.

6 Klicken Sie, wenn sich das LAN-Fenster öffnet, zum Neustart Ihres Computers auf „**Ja**“. Der Computer wird neu gestartet. Jetzt ist das TCP/IP-Protokoll auf Ihrem PC konfiguriert, und Ihre Ethernet-Geräte sind einsatzbereit.

7 Versuchen Sie, auf das Internet zuzugreifen. Wenn Sie nach dem Neustart nicht auf das Internet zugreifen können, lesen Sie den Abschnitt ***Problembehebung*** (Seite 113). Sollten Sie daraufhin noch immer nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Dienstanbieter.

Konfiguration von TCP/IP unter Windows 95, 98, 98SE und ME

1 Klicken Sie auf „**Start**“ > „**Einstellungen**“ > „**Systemsteuerung**“.

2 Doppelklicken Sie im Fenster „Systemsteuerung“ auf das Symbol „**Netzwerk**“.

3 Gehen Sie auf der Registerkarte „**Konfiguration**“ die Liste der installierten Netzwerkkomponenten durch, um zu überprüfen, ob für Ihren PC „TCP/IP-Protokoll/Ethernet-Adapter“ aufgeführt wird.

4 Wird das TCP/IP-Protokoll unter den installierten Netzwerkkomponenten aufgeführt?

- Wenn **ja**, machen Sie mit Schritt 7 weiter.
- Wenn **nein**, klicken Sie auf „**Hinzufügen**“ > „**Protokoll**“ > „**Hinzufügen**“ und machen Sie dann mit Schritt 5 weiter.

5 Klicken Sie in der Liste der Hersteller auf „**Microsoft**“.

6 Klicken Sie in der Liste der Netzwerkprotokolle auf „**TCP/IP**“ und anschließend auf „**OK**“.

7 Klicken Sie auf das Protokoll „**TCP/IP Ethernet-Adapter**“ und anschließend auf „**Eigenschaften**“.

8 Klicken Sie auf die Registerkarte „**IP-Adresse**“ und markieren Sie das Kontrollkästchen „**IP-Adresse automatisch beziehen**“.

9 Klicken Sie auf die Registerkarteplakate „**Gateway**“ und stellen Sie sicher, dass diese Felder leer sind. Sollte dies nicht der Fall sein, markieren und löschen Sie alle Informationen aus diesen Feldern.

10 Klicken Sie auf die Registerkarte „**DNS-Konfiguration**“ und markieren Sie das Kontrollkästchen „**DNS deaktivieren**“.

11 Klicken Sie auf „**OK**“.

12 Klicken Sie, wenn das System die Dateien kopiert hat, auf „**OK**“ und schließen Sie anschließend alle Netzwerkfenster.

13 Klicken Sie, wenn sich das Dialogfeld „Geänderte Systemeinstellungen“ öffnet, zum Neustart Ihres Computers auf „**Ja**“. Der Computer wird neu gestartet. Jetzt ist das TCP/IP-Protokoll auf Ihrem PC konfiguriert, und Ihre Ethernet-Geräte sind einsatzbereit.

14 Versuchen Sie, auf das Internet zuzugreifen. Wenn Sie nach dem Neustart nicht auf das Internet zugreifen können, lesen Sie den Abschnitt ***Problembehebung*** (Seite 113). Sollten Sie daraufhin noch immer nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Dienstanbieter.

Konfiguration von TCP/IP auf Macintosh-Systemen

1 Klicken Sie oben links im Finder auf das **Apple**-Symbol. Führen Sie einen Bildlauf zu den **Kontrollfeldern** durch und klicken Sie anschließend auf „**TCP/IP**“.

2 Klicken Sie in der Menüleiste des Fensters auf „**Bearbeiten**“. Führen Sie einen Bildlauf zum Menüende durch und klicken Sie auf „**Benutzermodus**“.

3 Klicken Sie im Fenster „Benutzermodus“ auf „**Erweiterte Funktionen**“ und anschließend auf „**OK**“.

4 Klicken Sie im TCP/IP-Fenster auf die Auswahlpfeile Auf/Ab rechts neben dem Abschnitt „Verbindung“ und klicken Sie dann auf „**DHCP-Server**“.

5 Klicken Sie im TCP/IP-Fenster auf „**Optionen**“ und anschließend im Fenster „TCP/IP-Optionen“ auf „**Aktivieren**“.

Hinweis: Stellen Sie sicher, dass das Kontrollkästchen „**Nur bei Bedarf laden**“ *nicht* markiert ist.

6 Stellen Sie sicher, dass die Option „**802.3**“ in der rechten oberen Ecke des TCP/IP-Fensters nicht aktiviert ist. Wenn sich neben der Option ein Häkchen befindet, deaktivieren Sie die Option. Klicken Sie anschließend in der unteren linken Ecke auf „**Info**“.

7 Wird in diesem Fenster eine Hardware-Adresse angegeben?

- Wenn **ja**, klicken Sie auf „**OK**“. Klicken Sie zum Schließen des TCP/IP-Kontrollfeldes auf „**Datei**“ und klicken Sie unten im Menü auf „**Beenden**“. Sie haben die Konfiguration abgeschlossen.
- Wenn **nein**, müssen Sie Ihren Macintosh herunterfahren.

8 Drücken Sie bei ausgeschaltetem Computer gleichzeitig die **Befehlstaste (Apple)**, die **Wahltaste**, **P** und **R** auf der Tastatur. Halten Sie diese Tasten gedrückt, während Sie Ihren Macintosh hochfahren. Lassen Sie die Tasten erst los, nachdem der „Apple-Klang“ mindestens drei Mal ertönte. Starten Sie den Computer neu.

9 Wiederholen Sie nach Abschluss des Neustarts die Schritte 1 bis 7, um sicherzustellen, dass alle TCP/IP-Einstellungen korrekt sind. Besitzt Ihr Computer immer noch keine Hardware-Adresse, wenden Sie sich an Ihren Apple-Vertragshändler oder den technischen Support von Apple.

F. Was mache ich, wenn ich kein Kabelfernsehen abonniere?

A. Wird Kabelfernsehen in Ihrer Gegend angeboten, ist der Datendienst möglicherweise auch separat ohne Kabelfernsehen erhältlich. Vollständige Informationen zu Kabeldiensten, einschließlich High-Speed-Internetzugang, erhalten Sie von Ihrem örtlichen Dienstanbieter.

F. Wie kann ich die Installation von Fachleuten durchführen lassen?

A. Erkundigen Sie sich bei Ihrem Telefonnetzbetreiber, ob die Installation angeboten wird. Eine Installation durch Fachpersonal gewährleistet, dass die Kabel richtig an das Modem und an Ihren PC angeschlossen werden und dass alle Hardware- und Software-Einstellungen ordnungsgemäß konfiguriert sind. Nähere Informationen zur Installation durch Fachpersonal erhalten Sie von Ihrem Telefonnetzbetreiber.

F. Wie ist das Heim-Gateway mit meinem Computer verbunden?

A. Das Heim-Gateway wird an den 10/100BASE-T Ethernet-Port Ihres PCs angeschlossen. Falls Ihr PC keine Ethernet-Schnittstelle besitzt, können Sie von Ihrem örtlichen PC- oder Bürobedarffachhändler oder Ihrem Dienstanbieter eine Ethernet-Karte beziehen.

F. Wie greife ich nach dem Anschließen meines Heim-Gateways auf das Internet zu?

A. Ihr örtlicher Dienstanbieter wird zu Ihrem Internetdienstanbieter (ISP) mit einem vielfältigen Angebot an Diensten wie E-Mail, Chat, Nachrichten und Informationen. Sie erhalten die benötigte Software von Ihrem Dienstanbieter.

F. Kann ich gleichzeitig fernsehen und im Internet surfen?

A. Aber natürlich! Wenn Sie Kabelfernsehen abonnieren, können Sie gleichzeitig fernsehen und Ihr Heim-Gateway benutzen. Dazu müssen Sie Ihren Fernseher und Ihr Heim-Gateway über einen Kabelsplitter an dasselbe Kabelnetzwerk anschließen.

F. Kann ich mehr als ein Gerät am Modem anschließen?

A. Ja. Ein einzelnes Heim-Gateway kann theoretisch bis zu 253 Ethernet-Geräte unterstützen. Dazu müssen Sie Ethernet-Hubs oder -Router verwenden, die Sie von Ihrem örtlichen Computer- oder Bürobedarffachhändler erhalten.

Problembehebung

Häufige Probleme

Ich weiß nicht, was die Statusanzeigen auf der Vorderseite bedeuten

Im Abschnitt ***Funktionen der LED-Statusanzeigen*** (Seite 115) finden Sie nähere Informationen zu den LED-Funktionen der Steuerungsanzeige.

Das Modem zeigt eine Ethernet-Verbindung nicht an

- Stellen Sie sicher, dass Ihr Computer eine Ethernet-Karte besitzt und die Ethernet-Treibersoftware ordnungsgemäß installiert ist. Beachten Sie bei der Installation einer nachträglich gekauften Ethernet-Karte die Installationsanleitungen genau.
- Überprüfen Sie den Status der LED-Statusanzeigen auf der Vorderseite.

Nach dem Anschließen an einen Hub zeigt das Modem eine Ethernet-Verbindung nicht an

Wenn Sie mehrere PCs an das Heim-Gateway anschließen, sollten Sie zuerst das Modem mit dem richtigen Kreuzkabel an den Uplink-Port des Hubs anschließen. Die LINK-LED des Hubs leuchtet unterbrochen.

Das Modem zeigt eine Kabelverbindung nicht an

Das Modem benutzt ein herkömmliches HF-Koaxialkabel (75 Ohm). Mit einem anderen Kabel funktioniert Ihr Heim-Gateway nicht ordnungsgemäß. Wenden Sie sich an Ihren Dienstanbieter, um festzustellen, ob Sie das richtige Kabel verwenden.

Stellen Sie sicher, dass Sie die im Abschnitt ***Problembehebung bei der Einrichtung des Internets*** (Seite 104) beschriebenen Anweisungen korrekt ausgeführt haben.

Tipps für eine bessere Leistung

Überprüfung und Korrektur

Sollte Ihr Heim-Gateway nicht die erwartete Leistung erbringen, sind die folgenden Tipps vielleicht hilfreich. Wenn Sie zusätzliche Unterstützung benötigen, wenden Sie sich an Ihren Dienstanbieter.

- Vergewissern Sie sich, dass der Netzteilstecker Ihres Heim-Gateways ordnungsgemäß in eine Steckdose gesteckt ist.
- Überprüfen Sie, ob sich der Netzteilstecker Ihres Heim-Gateways in einer Steckdose befindet, die über einen Wandschalter kontrolliert wird. Sollte dies der Fall sein, achten Sie darauf, dass sich der Schalter in der **EIN**-Position befindet.
- Überprüfen Sie, ob die mit **POWER** und **CABLE** beschrifteten LED-Statusanzeigen auf der Vorderseite des Heim-Gateways leuchten.
- Überprüfen Sie, ob Ihr Kabeldienst aktiv ist und bidirektionale Kabelverbindungen unterstützt.
- Überprüfen Sie, ob alle Kabel ordnungsgemäß angeschlossen sind und ob Sie die richtigen Kabel benutzen.
- Wenn Sie die Ethernet-Verbindungen benutzen, überprüfen Sie, ob auf allen Geräten TCP/IP ordnungsgemäß installiert und konfiguriert ist.
- Haben Sie Ihren Dienstanbieter angerufen und ihm die Seriennummer und die MAC-Adresse Ihres Heim-Gateways mitgeteilt?
- Wenn Sie einen Kabelsplitter benutzen, um das Heim-Gateway mit anderen Geräten zu verbinden, entfernen Sie den Splitter und schließen Sie das Kabel erneut an, sodass das Heim-Gateway direkt mit dem Hauptkabeleingang verbunden ist. Funktioniert das Heim-Gateway jetzt ordnungsgemäß, ist der Kabelsplitter möglicherweise defekt und muss ausgetauscht werden.
- Für die beste Leistung über eine Ethernet-Verbindung sollte Ihr PC mit einer 10/100BASE-T-NIC (Network Interface Card) ausgestattet sein.

Funktionen der LED-Statusanzeigen

Erstes Einschalten, Kalibrierung und Registrierung (bei Stromzufuhr)

Die folgende Tabelle verdeutlicht die Schrittfolge und das jeweilige Verhalten der LED-Statusanzeigen auf der Vorderseite des Heim-Gateways während des ersten Einschaltens, der Kalibrierung und der Registrierung im Netzwerk nach Anschluss des Heim-Gateways an das Stromnetz. Verwenden Sie diese Tabelle, um Probleme beim Einschalten, der Kalibrierung und der Registrierung Ihres Heim-Gateways zu beheben.

Hinweis: Direkt nach Abschluss der Registrierung des Heim-Gateways wechselt das Modem in den Normalbetrieb. Nähere Informationen hierzu finden Sie im Abschnitt ***Normalbetrieb (bei Stromzufuhr)*** (Seite 117).

LED-Statusanzeigen der Vorderseite bei erstem Einschalten, Kalibrierung und Registrierung

		High-Speed-Datenregistrierung					
Schritt:		**1**	**2**	**3**	**4**	**5**	**6**
Anzeige auf der Vorderseite		**Selbsttest**	**Downstream-Scan**	**Downstream-Signalsperre**	**Bereichsanforderung**	**Anforderung der IP-Adresse**	**Registrierung**
1	POWER	leuchtet	leuchtet	leuchtet	leuchtet	leuchtet	leuchtet
2	DS	leuchtet	blinkt	leuchtet	leuchtet	leuchtet	leuchtet
3	US	leuchtet	aus	aus	blinkt	leuchtet	leuchtet
4	ONLINE	leuchtet	aus	aus	aus	aus	blinkt
5	LAN1-LAN4	leuchtet	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt
6	WIRELESS	aus	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt	leuchtet oder blinkt

Normalbetrieb (bei Stromzufuhr)

Die folgende Tabelle beschreibt das Verhalten der LED-Statusanzeigen auf der Vorderseite des Heim-Gateways während des Normalbetriebs, wenn das Gateway am Stromnetz angeschlossen ist.

LED-Statusanzeigen der Vorderseite unter Normalbedingungen

Anzeige auf der Vorderseite		Normalbetrieb
1	POWER	leuchtet
2	DS	leuchtet
3	US	leuchtet
4	ONLINE	leuchtet
5	LAN1-LAN4	■ leuchtet, wenn ein einzelnes Gerät an den Ethernet-Port angeschlossen ist und keine Daten vom Modem gesendet oder empfangen werden ■ blinkt, wenn nur ein Ethernet-Gerät angeschlossen ist und Daten zwischen einem Endgerät (CPE) und dem kabellosen Heim-Gateway übertragen werden ■ aus, wenn keine Geräte an den Ethernet-Ports angeschlossen sind
6	WIRELESS	■ leuchtet, wenn der Wireless Access Point aktiviert und betriebsbereit ist ■ blinkt, wenn Daten zwischen dem Endgerät (CPE) und dem kabellosen Heim-Gateway übertragen werden ■ aus, wenn der Wireless Access Point vom Benutzer deaktiviert worden ist

Besondere Bedingungen

Die folgende Tabelle beschreibt das Verhalten der LED-Statusanzeigen auf der Vorderseite des Heim-Gateways während besonderer Bedingungen, wenn Ihnen beispielsweise der Zugang zum Netzwerk verweigert worden ist oder das Modem über Batterien gespeist wird.

LED-Statusanzeigen der Vorderseite unter besonderen Bedingungen

Anzeige auf der Vorderseite		**Netzwerkzugriff verweigert**
1	POWER	blinkt langsam 1 Mal pro Sekunde
2	DS	blinkt langsam 1 Mal pro Sekunde
3	US	blinkt langsam 1 Mal pro Sekunde
4	ONLINE	blinkt langsam 1 Mal pro Sekunde
5	LAN1-LAN4	blinkt langsam 1 Mal pro Sekunde
6	WIRELESS	leuchtet

Technische Fragen

Bei Fragen

Bei technischen Fragen sollten Sie sich an Ihren örtlichen Dienstanbieter wenden.

Hinweise

Marken

Cisco, Cisco Systems, das Cisco-Logo, und Cisco Systems-Logo sind eingetragene Marken bzw. Marken der Cisco Systems, Inc. und/oder der verbundenen Unternehmen in den Vereinigten Staaten und anderen Ländern.
DOCSIS ist eine eingetragene Marke der Cable Television Laboratories, Inc.
EuroDOCSIS, PacketCable und EuroPacketCable sind Marken der Cable Television Laboratories, Inc.

Andere in diesem Dokument erwähnte Marken sind das Eigentum der jeweiligen Inhaber.

Haftungsausschluss

Cisco Systems, Inc. übernimmt keine Verantwortung für etwaige Fehler oder Auslassungen in diesem Handbuch. Änderungen vorbehalten.

Hinweis zum Copyright-Schutz der Dokumentation

Die in diesem Dokument enthalten Informationen können jederzeit ohne Vorankündigung geändert werden. Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Genehmigung von Cisco Systems, Inc. in irgendeiner Form vervielfältigt werden.

Nutzung der Software und Firmware

Die in diesem Dokument beschriebene Software ist urheberrechtlich geschützt und wird Ihnen im Rahmen einer Lizenzvereinbarung zur Verfügung gestellt. Das Verwenden oder Kopieren dieser Software ist nur unter Einhaltung der Bedingungen dieser Lizenzvereinbarung gestattet.

Die Firmware des Gerätes ist urheberrechtlich geschützt. Sie dürfen die Firmware nur in dem Gerät nutzen, in dem sie bereitgestellt worden ist. Jede Reproduktion oder Verteilung dieser Firmware oder eines Teiles davon ohne ausdrückliche schriftliche Genehmigung ist untersagt.

Hinweise zu Drittanbieter-Softwarelizenzen für das Cisco-Modell DPC/EPC2325 DOCSIS Residential Gateway mit Wireless Access Point

Hinweise

Die folgenden Hinweise beziehen sich auf Lizenzen von Drittanbietern, die für dieses Produkt gelten.

Broadcom

Dieses Produkt verwendet eine Kopierschutztechnologie, die durch US-Patentrechte und andere Rechte zum Schutz geistigen Eigentums geschützt ist. Die Nutzung dieser Kopierschutztechnologie erfordert die Genehmigung durch Broadcom. Die Technologie ist für den Privatgebrauch oder andere begrenzte Einsatzbereiche gedacht; jede andere Nutzung erfordert die Genehmigung durch Broadcom. Rückentwicklung und Disassemblierung sind untersagt.

Win32 IPSEC Layer von SSH

(Siehe http://www.cisco.com/)

Für Test- und Beurteilungszwecke enthält die CablexChange Software einen IPSEC-geeigneten Kerberized Call Agent. Dieser Call Agent verwendet die von der „SSH Communication Security Corporation“ bereitgestellte Win32-basierte IPSEC Software.

OpenSSL

(Siehe http://www.openssl.org/ und
http://www.openssl.org/source/license.html)

Das OpenSSL-Toolkit unterliegt einer dualen Lizenz, d. h. für das Toolkit gelten sowohl die Bedingungen der OpenSSL-Lizenz als auch die der ursprünglichen SSLeay-Lizenz. Den eigentlichen Wortlaut der Lizenzen finden Sie weiter unten.

A. OpenSSL-Lizenz

Copyright © 1998-2000 The OpenSSL Project. Alle Rechte vorbehalten.

1. Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:
2. Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.
3. Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgelieferten Material enthalten sein. Sämtliches Werbematerial, in dem die Funktionen oder die Verwendung dieser Software erwähnt werden, muss den folgenden Hinweis enthalten: „Dieses Produkt enthält von OpenSSL Project entwickelte Software zur Verwendung mit dem OpenSSL-Toolkit.“ (http://www.openssl.org)
4. Die Bezeichnungen „OpenSSL Toolkit“ und „OpenSSL Project“ dürfen nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden. Eine schriftliche Genehmigung können Sie anfordern von openssl-core@openssl.org.
5. Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung von OpenSSL Project mit „OpenSSL“ bezeichnet werden; des Weiteren darf die Bezeichnung „OpenSSL“ nur mit vorheriger schriftlicher Genehmigung von OpenSSL Project im Namen solcher Produkte verwendet werden.
6. Weiterverteilungen jeglicher Art müssen den folgenden Hinweis enthalten:

   „Dieses Produkt enthält von OpenSSL Project entwickelte Software zur Verwendung mit dem OpenSSL-Toolkit (http://www.openssl.org).“

DIESE SOFTWARE WIRD VON OpenSSL PROJECT OHNE MÄNGELGEWÄHR VERTEILT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. OpenSSL PROJECT UND DIE BEITRÄGER DES PROJEKTS SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Dieses Produkt enthält kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde. Dieses Produkt enthält Software, die von Tim Hudson (tjh@cryptsoft.com) geschrieben wurde.

B. SSLeay-Lizenz

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com). Alle Rechte vorbehalten.

Bei diesem Paket handelt es sich um eine von Eric Young (eay@cryptsoft.com) geschriebene SSL-Anwendung.

Die Anwendung wurde in Übereinstimmung mit Netscapes SSL geschrieben.

Diese Bibliothek kann kostenlos für kommerzielle und private Zwecke verwendet werden, sofern folgende Bedingungen eingehalten werden. Die folgenden Bedingungen gelten nicht nur für den SSL-Code, sondern für den gesamten in dieser Verteilung enthaltenen Code (RC4, RSA, lhash, DES usw.). Die im Lieferumfang enthaltene SSL-Dokumentation unterliegt denselben Copyright-Bedingungen mit der Ausnahme, dass der Rechteinhaber Tim Hudson (tjh@cryptsoft.com) ist.

Das Urheberrecht verbleibt bei Eric Young; keiner der im Code enthaltenen Copyright-Hinweise darf entfernt werden. Bei Verwendung dieses Pakets in einem Produkt muss Eric Young als Urheber der Teile der verwendeten Bibliothek genannt werden. Dies kann in Form einer Mitteilung bei Programmstart oder in der mit dem Paket (online oder als Handbuch) mitgelieferten Dokumentation erfolgen. Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

1 Bei einer Weiterverteilung des Quellcodes müssen die Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.

2 Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgelieferten Material enthalten sein.

3 Sämtliches Werbematerial, in dem die Funktionen oder die Verwendung dieser Software erwähnt werden, muss den folgenden Hinweis enthalten: „Dieses Produkt enthält kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.“ Das Wort „kryptografisch“ kann weggelassen werden, wenn die aus der verwendeten Bibliothek stammenden Routinen keine kryptografischen Routinen sind.

4 Wenn Sie Windows-spezifischen Code (oder davon abgeleiteten Code) aus dem Anwendungsverzeichnis (Anwendungscode) verwenden, müssen Sie folgenden Hinweis anführen: „Dieses Produkt enthält Software, die von Tim Hudson (tjh@cryptsoft.com) geschrieben wurde.“

DIESE SOFTWARE WIRD VON ERIC YOUNG OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE AUTOREN UND BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Eine Änderung der Lizenz- und Verteilungsbedingungen für öffentlich erhältliche oder abgeleitete Versionen dieses Codes ist nicht gestattet. Das heißt, dieser Code darf nicht einfach kopiert und im Rahmen einer anderen Verteilungslizenz (einschließlich der GNU Public Licence) verteilt werden.

Mini-HTTPD

ACME Labs Freeware-Lizenz

(Siehe http://www.acme.com/software/mini_httpd/)

Copyright © 2000 Jef Poskanzer <jef@acme.com>. Alle Rechte vorbehalten.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

1 Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.

2 Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgelieferten Material enthalten sein.

DIESE SOFTWARE WIRD VOM AUTOR UND DEN BEITRÄGERN DES PROJEKTS OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE AUTOREN UND BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

eCos

(Siehe http://ecos.sourceware.org/ und
http://ecos.sourceware.org/license-overview.html)

Dies ist der vollständige Lizenztext, der unter der eCos-Lizenz vertriebenen eCos-Dateien beigefügt ist. Er sollte zusammen mit der GNU General Public Licence (GPL) gelesen werden, da er von dieser abhängt.

eCos ist eine kostenlose Software, die unter Einhaltung der Bedingungen der GNU General Public License (Version 2 oder später, veröffentlicht von der Free Software Foundation) weiter verteilt und/oder geändert werden kann.

eCos wird in der Hoffnung verteilt, dass sich die Software nützlich erweist, aber OHNE JEGLICHE GARANTIE; selbst ohne die stillschweigende Garantie der MARKTFÄHIGKEIT oder EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Nähere Details dazu finden Sie in der folgenden GNU General Public License Version 2.

GNU GENERAL PUBLIC LICENSE Version 2, Juni 1991

Es ist generell gestattet, dieses Lizenzdokument zu vervielfältigen und unveränderte Kopien zu verteilen. Jegliche Vornahme von Änderungen ist jedoch untersagt.

Es folgen die genauen Bedingungen für die Vervielfältigung, Verteilung und Bearbeitung.

Diese Lizenz gilt für alle Programme und alle anderen Werke, bei denen ein entsprechender Vermerk des Copyright-Inhabers darauf hinweist, dass das Programm bzw. Werk unter den Bestimmungen dieser General Public License verteilt werden darf. Der im Folgenden benutzte Begriff „Programm“ bezieht sich auf ein derartiges Programm bzw. ein derartiges Werk; „auf dem Programm basierendes Werk“ bezieht sich entweder auf das Programm oder alle im urheberrechtlichen Sinne davon abgeleitete Werke, also Werke, die das Programm bzw. Teile davon, unverändert oder verändert und/oder in eine andere Sprache übersetzt, enthält. (Im Folgenden wird die Übersetzung ohne Einschränkung als „Bearbeitung“ eingestuft.) Alle Lizenznehmer werden im Folgenden als „Sie“ bezeichnet.

Andere Handlungen als Vervielfältigung, Verteilung und Bearbeitung bleiben von dieser Lizenz unberührt; sie fallen nicht in ihren Anwendungsbereich. Der Vorgang der Ausführung des Programms wird nicht eingeschränkt, und die Ausgaben des Programms unterliegen dieser Lizenz nur, wenn der Inhalt ein auf dem Programm basierendes Werk darstellt (unabhängig davon, dass die Ausgabe durch die Ausführung des Programms erfolgte). Ob dies zutrifft, hängt von den Funktionen des Programms ab.

1 Sie dürfen den Quellcode des Programms in unveränderter Form, wie Sie ihn erhalten haben, auf bzw. in beliebige Medien kopieren und verteilen. Voraussetzung hierfür ist, dass Sie mit jeder Kopie einen entsprechenden Copyright-Hinweis sowie einen Haftungsausschluss unübersehbar und in angemessener Weise veröffentlichen, alle Hinweise, die sich auf diese Lizenz und das Fehlen einer Garantie beziehen, unverändert lassen und des Weiteren allen anderen Empfängern des Programms zusammen mit dem Programm eine Kopie dieser Lizenz zukommen lassen. Sie dürfen für die physische Übertragung der Kopie eine Gebühr verlangen. Wenn Sie möchten, dürfen Sie auch gegen Gebühr eine Garantie für das Programm anbieten.

2 Sie dürfen Ihre Kopie(n) des Programms oder eines Teils davon verändern, wodurch ein auf dem Programm basierendes Werk entsteht; Sie dürfen derartige Bearbeitungen unter den in Paragraf 1 oben genannten Bedingungen vervielfältigen und verteilen, vorausgesetzt, dass zusätzlich alle im Folgenden genannten Bedingungen erfüllt werden:

a Sie müssen die veränderten Dateien mit einem auffälligen Vermerk versehen, der auf die von Ihnen vorgenommene Modifizierung und das Datum der einzelnen Änderungen hinweist.

b Sie müssen dafür sorgen, dass jedes von Ihnen verteilte oder veröffentlichte Werk, das das Programm oder Teile davon vollständig oder teilweise enthält bzw. vollständig oder teilweise von dem Programm oder Teilen davon abgeleitet ist, als Ganzes gemäß den Bedingungen dieser Lizenzvereinbarung ohne Gebühr für alle Dritten lizenziert wird.

c Erfordert das bearbeitete Programm für gewöhnlich beim Start die interaktive Eingabe von Befehlen, müssen Sie dafür sorgen, dass das Programm beim Start für eine solche interaktive Verwendung eine Meldung druckt oder ausgibt. Diese Meldung muss einen entsprechenden Copyright-Hinweis enthalten und deutlich machen, dass es keine Gewährleistung gibt (oder andernfalls, dass Sie Garantie leisten); außerdem muss der Benutzer darüber informiert werden, dass er das Programm gemäß diesen Bedingungen weiterverteilen darf und wie er eine Kopie dieser Lizenz anzeigen kann. (Ausnahme: Wenn das Programm selbst interaktiv arbeitet, aber normalerweise keine derartige Meldung ausgibt, muss Ihr auf dem Programm basierendes Werk auch keine solche Meldung ausgeben.)

Diese Anforderungen gelten für das bearbeitete Werk als Ganzes. Wenn identifizierbare Teile des Werks nicht von dem Programm abgeleitet sind und objektiv als unabhängige und eigenständige Werke zu betrachten sind, dann gelten diese Lizenz und ihre Bedingungen nicht für diese Teile, wenn Sie sie als eigenständige Werke verteilen. Wenn Sie jedoch dieselben Abschnitte als Teil eines Ganzen verteilen, das ein auf dem Programm basierendes Werk darstellt, dann muss die Weitergabe des Ganzen nach den Bedingungen dieser Lizenz erfolgen, deren Bedingungen für weitere Lizenznehmer somit auf das gesamte Ganze ausgedehnt werden – und somit auf jeden einzelnen Teil, unabhängig vom jeweiligen Autor.

Somit ist es nicht die Absicht dieses Abschnittes, Rechte für Werke in Anspruch zu nehmen oder Ihnen die Rechte für Werke streitig zu machen, die komplett von Ihnen geschrieben wurden; vielmehr besteht die Absicht darin, die Rechte zur Kontrolle der Verteilung von Werken auszuüben, die auf dem Programm basieren oder unter seiner Verwendung zusammengestellt worden sind.

Darüber hinaus fällt durch das einfache Zusammenlegen eines anderen Werks, das nicht auf dem Programm basiert, mit dem Programm oder einem auf dem Programm basierenden Werk auf ein- und demselben Speicher- oder Vertriebsmedium dieses andere Werk nicht unter diese Lizenz.

3 Sie dürfen das Programm (oder ein nach Paragraf 2 auf dem Programm basierendes Werk) als Objektcode oder in ausführbarer Form gemäß den in Paragraf 1 und 2 genannten Bedingungen kopieren und verteilen, vorausgesetzt, Sie erbringen zusätzlich eine der folgenden Leistungen:

a Liefern Sie das Programm zusammen mit dem vollständigen zugehörigen computerlesbaren Quellcode auf einem für den Datenaustausch üblichen Medium aus, wobei die Verteilung unter den in Paragrafen 1 und 2 genannten Bedingungen erfolgen muss. Oder. Oder:

b Liefern Sie das Programm zusammen mit einem mindestens drei Jahre gültigen schriftlichen Angebot aus, jedem Dritten eine vollständige computerlesbare Kopie des Quellcodes zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch die physikalische Bereitstellung des Quellcodes anfallen –, wobei der Quellcode gemäß den in Paragrafen 1 und 2 genannten Bedingungen auf einem für den Datenaustausch üblichen Medium weitergegeben wird. Oder:

c Liefern Sie das Programm zusammen mit dem schriftlichen Angebot der Zurverfügungstellung des Quellcodes aus, das Sie selbst erhalten haben. (Diese Alternative ist nur für nicht-kommerzielle Verteilung zulässig und nur, wenn Sie das Programm als Objektcode oder in ausführbarer Form mit einem entsprechenden Angebot gemäß Absatz b erhalten haben.)

Unter dem Quellcode eines Werks wird diejenige Form des Werks verstanden, die für Bearbeitungen vorzugsweise verwendet wird. Bei ausführbaren Programmen bezeichnet „der vollständige Quellcode“ den Quellcode aller im Programm enthaltenen Module einschließlich aller zugehörigen Schnittstellen-Definitionsdateien sowie der zur Kompilierung und Installation des ausführbaren Programms verwendeten Skripte. Als besondere Ausnahme jedoch braucht der verteilte Quellcode nichts von dem zu enthalten, was üblicherweise entweder als Quellcode oder in binärer Form zusammen mit den Hauptkomponenten des Betriebssystems (Kernel, Compiler usw.) geliefert wird, unter dem das Programm läuft – es sei denn, diese Komponente selbst gehört zum Lieferumfang des ausführbaren Programms.

Wenn die Verteilung eines ausführbaren Programms oder von Objektcode dadurch erfolgt, dass der Kopierzugriff auf einen dafür vorgesehenen Speicherort gewährt wird, so gilt die Gewährung eines gleichwertigen Zugriffs auf den Quellcode als Verteilung des Quellcodes, auch wenn Dritte nicht dazu gezwungen werden, den Quellcode zusammen mit dem Objektcode zu kopieren.

4 Sie dürfen das Programm nicht kopieren, verändern, weiterlizenzieren oder verteilen, außer im Rahmen der ausdrücklichen Bedingungen dieser Lizenz. Jeder anderweitige Versuch der Vervielfältigung, Modifizierung, Weiterlizenzierung und Verteilung ist nichtig und beendet automatisch Ihre Rechte unter dieser Lizenz. Jedoch werden die Lizenzen Dritter, die von Ihnen Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese die Lizenz voll anerkennen und befolgen.

5 Sie sind nicht verpflichtet, diese Lizenz anzunehmen, da Sie sie nicht unterzeichnet haben. Jedoch gewährt Ihnen nur diese Lizenz das Recht, das Programm oder von ihm abgeleitete Werke zu verändern oder zu verteilen. Diese Handlungen sind gesetzlich verboten, wenn Sie diese Lizenz nicht anerkennen. Indem Sie das Programm (oder ein darauf basierendes Werk) verändern oder verteilen, erklären Sie daher Ihr Einverständnis mit dieser Lizenz und mit allen ihren Bedingungen bezüglich der Vervielfältigung, Verteilung und Veränderung des Programms oder eines darauf basierenden Werks.

6 Jedes Mal, wenn Sie das Programm (oder ein auf dem Programm basierendes Werk) weitergeben, erhält der Empfänger automatisch vom ursprünglichen Lizenzgeber die Lizenz, das Programm entsprechend den hier festgelegten Bestimmungen zu vervielfältigen, zu verteilen und zu verändern. Sie dürfen keine weiteren Einschränkungen an den dem Empfänger durch diese Lizenz zugestandenen Rechten vornehmen. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

7 Sollten Ihnen infolge eines Gerichtsurteils, des Vorwurfs einer Patentverletzung oder aus einem anderen Grunde (nicht auf Patentfragen begrenzt) Bedingungen (durch Gerichtsbeschluss, Vergleich oder anderweitig) auferlegt werden, die den Bedingungen dieser Lizenz widersprechen, so befreien Sie diese Umstände nicht von den Bestimmungen dieser Lizenz. Wenn es Ihnen nicht möglich ist, das Programm unter gleichzeitiger Beachtung der Bedingungen dieser Lizenz und Ihrer anderweitigen Verpflichtungen zu verteilen, dann ist es Ihnen folglich untersagt, das Programm überhaupt zu verteilen. Wenn zum Beispiel ein Patent nicht die gebührenfreie Weiterverteilung des Programms durch diejenigen erlaubt, die Kopien des Programms direkt oder indirekt von Ihnen erhalten haben, dann besteht der einzige Weg, sowohl das Patentrecht als auch diese Lizenzbedingungen zu befolgen, darin, ganz auf die Verteilung des Programms zu verzichten.

Sollte sich ein Teil dieses Paragrafen unter bestimmten Umständen als ungültig oder nicht durchsetzbar erweisen, so ist der verbleibende Teil dieses Paragrafen anzuwenden; unter allen anderen Umständen ist der Paragraf in seiner Ganzheit anzuwenden.

Zweck dieses Paragrafen ist nicht, Sie dazu zu bringen, irgendwelche Patente oder andere Eigentumsansprüche zu verletzen oder die Gültigkeit solcher Ansprüche zu bestreiten; dieser Paragraf hat einzig den Zweck, die Integrität des Systems der kostenlosen Softwareverteilung zu schützen, das durch die Vergabe öffentlicher Lizenzen implementiert wird. Viele Leute haben im Vertrauen auf die durchgängige Anwendung dieses Systems großzügige Beiträge zu dem breiten Angebot der über dieses System verteilten Software geleistet; es liegt am Autor/Geber, zu entscheiden, ob er die Software über ein anderes System verteilen will; ein Lizenznehmer hat auf diese Entscheidung keinen Einfluss.

Dieser Paragraf soll gründlich verdeutlichen, was als Konsequenz aus dem Rest dieser Lizenz betrachtet wird.

8 Wenn die Verteilung und/oder die Nutzung des Programms in bestimmten Ländern entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann der Copyright-Inhaber, der das Programm unter diese Lizenz gestellt hat, eine explizite geographische Beschränkung der Verteilung zum Ausschluss dieser Länder angeben, sodass die Verteilung nur innerhalb der nicht ausgeschlossenen Staaten erlaubt ist. In einem solchen Fall beinhaltet diese Lizenz die Beschränkung, als wäre sie Bestandteil dieses Textes.

9 Die Free Software Foundation kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der General Public License veröffentlichen. Solche neuen Versionen werden vom Grundprinzip her der gegenwärtigen entsprechen, können aber im Detail abweichen, um neuen Problemen und Anforderungen gerecht zu werden.

Jede Version dieser Lizenz hat eine eindeutige Versionsnummer. Wenn in einem Programm angegeben wird, dass es dieser Lizenz in einer bestimmten Versionsnummer oder „einer späteren Version“ („any later version“) unterliegt, so haben Sie die Wahl, entweder den Bestimmungen der genannten Version zu folgen oder denen einer beliebigen späteren von der Free Software Foundation veröffentlichten Version. Wenn das Programm keine Versionsnummer angibt, können Sie eine beliebige von der Free Software Foundation veröffentlichte Version wählen.

10 Wenn Sie Teile des Programms in anderen kostenlosen Programmen verwenden möchten, die anderen Verteilungsbedingungen unterliegen, bitten Sie den Autor schriftlich um Erlaubnis. Bei Software, die unter dem Copyright der Free Software Foundation steht, schreiben Sie an die Free Software Foundation; wir machen zu diesem Zweck gelegentlich Ausnahmen. Unsere Entscheidung wird von den beiden Zielen geleitet, zum einen den kostenlosen Status aller von unserer kostenlosen Software abgeleiteten Werke zu erhalten und zum anderen das gemeinschaftliche Nutzen und Wiederverwenden von Software im Allgemeinen zu fördern.

KEINE GEWÄHRLEISTUNG

11 SOWEIT DIES NACH GELTENDEM RECHT ZULÄSSIG IST, GIBT ES FÜR DIESES PROGRAMM KEINE GEWÄHRLEISTUNG, DA ES KOSTENLOS LIZENZIERT WIRD. SOFERN NICHT ANDERWEITIG SCHRIFTLICH VEREINBART, STELLEN DIE COPYRIGHT-INHABER UND/ODER DRITTE DAS PROGRAMM OHNE MÄNGELGEWÄHR UND OHNE JEGLICHE GEWÄHRLEISTUNG SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART ZUR VERFÜGUNG, INSBESONDERE OHNE GARANTIEN DER MARKTFÄHIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. SIE ALS BENUTZER ÜBERNEHMEN BEZÜGLICH QUALITÄT UND LEISTUNGSFÄHIGKEIT DES PROGRAMMS DAS VOLLE RISIKO. SOLLTE SICH DAS PROGRAMM ALS FEHLERHAFT HERAUSSTELLEN, LIEGEN DIE KOSTEN FÜR ALLE NOTWENDIGEN REPARATUREN ODER KORREKTUREN BEI IHNEN.

12 IN KEINEM FALL, AUSSER WENN DURCH GELTENDES RECHT GEFORDERT ODER SCHRIFTLICH ZUGESICHERT, IST EIN COPYRIGHT-INHABER ODER EIN DRITTER, DER DAS PROGRAMM WIE OBEN ERLAUBT MODIFIZIERT UND/ODER VERTEILT, IHNEN GEGENÜBER FÜR SCHÄDEN JEGLICHER ART HAFTBAR, EINSCHLIESSLICH ALLGEMEINER, KONKRETER, ZUFÄLLIGER ODER NACHFOLGENDER SCHÄDEN, DIE AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PROGRAMMS FOLGEN (INSBESONDERE FÜR DATENVERLUSTE, FEHLERHAFTE VERARBEITUNG VON DATEN, IHNEN ODER ANDEREN ENTSTANDENE VERLUSTE ODER DER INKOMPATIBILITÄT DES PROGRAMMS MIT EINEM ANDEREN PROGRAMM), SELBST WENN DIESER COPYRIGHT-INHABER ODER DIESER DRITTE AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. Als besondere Ausnahme in Fällen, in denen andere Dateien Instanzen von Vorlagen, Makros oder eingebettete Funktionen dieser Datei verwenden oder Sie diese Datei kompilieren und mit anderen Werken verbinden, um ein auf dieser Datei basierendes Werk zu schaffen, reicht Verwendung dieser Datei allein noch nicht dazu aus, dass das resultierende Werk unter die GNU General Public License fällt. Trotzdem muss der Quellcode für diese Datei gemäß Paragraf 3 der GNU General Public License zur Verfügung gestellt werden.

Diese Ausnahme macht keinen der anderen Gründe ungültig, aus denen ein auf dieser Datei basierendes Werk unter die GNU General Public License fallen könnte.

Sie können eine Kopie des Quellcodes gemäß der General License Version 2 unter Angabe Ihres Namens und Ihrer Adresse unter folgender Anschrift anfordern:

Attn: Software Engineer

Cable Home Network BU

Cisco Video Technology Group

5030 Sugarloaf Highway

Lawrenceville, GA 30044, USA

Kerberos

(Siehe http://web.mit.edu/Kerberos/, und http://web.mit.edu/Kerberos/krb5-1.5/README-1.5.1.txt oder die README-Datei der jeweiligen Version)

Die Ausfuhr dieser Software aus den Vereinigten Staaten von Amerika bedarf möglicherweise einer besonderen Lizenz durch die US-Regierung. Es liegt in der Verantwortung der die Ausfuhr erwägenden Person bzw. Organisation, vor der Ausfuhr eine derartige Lizenz zu beantragen.

UNTER DIESER VORGABE wird hiermit die gebührenfreie Erlaubnis zur Nutzung, Vervielfältigung, Änderung und Verteilung dieser Software und dazugehöriger Dokumentation für alle Zwecke erteilt, vorausgesetzt, dass der obige Copyright-Hinweis allen Kopien beigefügt wird, dass sowohl dieser Copyright-Hinweis als auch diese Erlaubnis der Begleitdokumentation beigefügt werden und dass der Name M.I.T. nicht ohne ausdrückliche vorherige schriftliche Genehmigung für Werbung im Rahmen der Verteilung der Software benutzt wird. Darüber hinaus sind Sie bei einer Änderung der Software dazu verpflichtet, Ihre Software als geänderte Software kenntlich zu machen und sie so zu verteilen, dass sie nicht mit der ursprünglichen M.I.T.-Software verwechselt werden kann. M.I.T. macht keinerlei Zusicherungen bezüglich der Eignung dieser Software für einen bestimmten Zweck. Die Software wird ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie bereitgestellt.

NetSNMP

(Siehe http://net-snmp.sourceforge.net/ und
http://net-snmp.sourceforge.net/about/license.html)

Dieses Paket ist durch mehrere Copyrights geschützt, die in vier Teilen im Folgenden beschrieben werden. Lesen Sie bitte alle Teile durch. Bis 2001 wurde das Projekt von der University of California in Davis betreut, und der erste Teil bezieht sich auf sämtlichen in dieser Zeit geschriebenen Code. Ab 2001 wurde das Projekt von SourceForge betreut, und Networks Associates Technology, Inc. ist im Namen der größeren Net-SNMP-Community der Inhaber des Copyrights für alle seit diesem Zeitpunkt entstandenen abgeleiteten Werke. Als Teil 3 wurde ein weiterer Copyright-Abschnitt zusätzlich unter einer BSD-Lizenz (Berkeley Standard Distribution) für die dem Projekt von Cambridge Broadband Ltd. seit 2001 beigesteuerte Arbeit hinzugefügt. Als Teil 4 wurde ein weiterer Copyright-Abschnitt zusätzlich unter einer BSD-Lizenz für die dem Projekt von Sun Microsystems, Inc. seit 2001 beigesteuerte Arbeit hinzugefügt.

Viele Personen haben im Laufe der Jahre am Code des Projekts mitgearbeitet; eine vollständige Liste der Mitarbeiter finden Sie in der README-Datei im Danksagungsteil.

Teil 1: CMU/UCD Copyright-Hinweis: (mit BSD vergleichbar)

Copyright ©1989, 1991, 1992 Carnegie Mellon University

Abgeleitete Werke – 1996, 1998-2000 Copyright © 1996, 1998-2000 The Regents of the University of California. Alle Rechte vorbehalten.

Hiermit wird die gebührenfreie Erlaubnis zur Nutzung, Vervielfältigung, Änderung und Verteilung dieser Software und dazugehöriger Dokumentation für alle Zwecke erteilt, vorausgesetzt, dass der obige Copyright-Hinweis allen Kopien beigefügt wird, dass sowohl dieser Copyright-Hinweis als auch diese Erlaubnis der Begleitdokumentation beigefügt werden und dass die Namen CM und The Regents of the University of California nicht ohne ausdrückliche vorherige schriftliche Genehmigung für Werbung im Rahmen der Verteilung der Software benutzt werden.

CMU UND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA LEHNEN BEZÜGLICH DIESER SOFTWARE ALLE GARANTIEN AB, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GARANTIE DER MARKTFÄHIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN KEINEM FALL SIND CMU ODER THE REGENTS OF CALIFORNIA FÜR KONKRETE, INDIREKTE ODER NACHFOLGENDE SCHÄDEN ODER SCHÄDEN JEGLICHER ART HAFTBAR, DIE IN VERBINDUNG MIT DER NUTZUNG ODER LEISTUNG DIESER SOFTWARE ENTSTEHEN UND ZU NUTNUTZUNGSAUSFÄLLEN, DATENVERLUST, ENTGANGENEN GEWINNEN FÜHREN, UNGEACHTET DER ART DER KLAGE, SEI ES AUF VERTRAGS- ODER SCHADENSRECHTLICHER ANSPRUCHSGRUNDLAGE ODER WEGEN UNERLAUBTER HANDLUNGEN.

Teil 2: Networks Associates Technology, Inc. – Copyright-Hinweis (BSD)

Copyright © 2001-2003 Networks Associates Technology, Inc. Alle Rechte vorbehalten.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

- Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.
- Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgeliefertem Material enthalten sein.
- Der Name der Networks Associates Technology, Inc. und die Namen der Beiträger des Produkts dürfen nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden.

DIESE SOFTWARE WIRD VON DEN COPYRIGHT-INHABERN UND DEN BEITRÄGERN OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE COPYRIGHT-INHABER UND BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN NICHT, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Teil 3: Cambridge Broadband Ltd. – Copyright-Hinweis (BSD)

Teile dieses Codes sind durch Copyright © 2001-2003 der Cambridge Broadband Ltd. geschützt. Alle Rechte vorbehalten.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

- Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.
- Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgeliefertem Material enthalten sein.
- Der Name der Cambridge Broadband Ltd. darf nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden.

DIESE SOFTWARE WIRD VOM COPYRIGHT-INHABER OHNE MÄNGELGEWÄHR VERTRIEBEN, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DER COPYRIGHT-INHABER IST IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Teil 4: Sun Microsystems, Inc. – Copyright-Hinweis (BSD)

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, USA. Alle Rechte vorbehalten.

Die Nutzung unterliegt den im Folgenden aufgeführten Lizenzbedingungen:

Die Verteilung enthält möglicherweise Material, das von Dritten entwickelt worden ist. Sun, Sun Microsystems, das Sun Logo und Solaris sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

- Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.
- Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgeliefertem Material enthalten sein.
- Der Name von Sun Microsystems, Inc. und die Namen der an diesem Produkt Beteiligten dürfen nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden.

DIESE SOFTWARE WIRD VON DEN COPYRIGHT-INHABERN UND DEN BEITRÄGERN OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE COPYRIGHT-INHABER UND BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Apache Softwarelizenz

(Siehe http://www.apache.org und http://www.apache.org/licenses/)

Apache Softwarelizenz Version 1.1 Copyright ©2000 The Apache Software Foundation. Alle Rechte vorbehalten.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

1. Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.
2. Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgeliefertem Material enthalten sein.
3. Die dieser Weiterverteilung eventuell beigefügte Endbenutzer-Dokumentation muss den folgenden Hinweis enthalten: „Dieses Produkt enthält von der Apache Software Foundation (http://www.apache.org/) entwickelte Software.“ Als Alternative ist es möglich, diesen Hinweis in der Software selbst und an Stellen, an denen normalerweise derartige Drittanbieter-Hinweise erscheinen, anzuzeigen.
4. Die Namen Apache und Apache Software Foundation dürfen nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden. Eine schriftliche Genehmigung können Sie von apache@apache.org anfordern.

5 Produkte, die auf dieser Software basieren, dürfen nur mit vorheriger schriftlicher Genehmigung von der Apache Software Foundation mit „Apache“ bezeichnet werden; des Weiteren darf die Bezeichnung „Apache“ nur mit vorheriger schriftlicher Genehmigung der Apache Software Foundation im Namen solcher Produkte verwendet werden.

DIESE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DIE APACHE SOFTWARE FOUNDATION UND DIE BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND ANSPRUCHSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN HAFTUNGSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Kame IPv6 Stack

(Siehe http://www.kame.net und http://www.kame.net/dev/cvsweb2.cgi/kame/FAQ?rev=HEAD&content-type=text/x-cvsweb-markup)

Copyright ©1995, 1996, 1997 und 1998 WIDE Project. Alle Rechte vorbehalten.

Die Weiterverteilung und die Verwendung im Quell- oder Binärformat sind mit oder ohne Änderungen zulässig, sofern folgende Bedingungen erfüllt sind:

1 Bei einer Weiterverteilung des Quellcodes müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss angegeben werden.

2 Bei einer Weiterverteilung im Binärformat müssen die oben aufgeführten Copyright-Hinweise, diese Auflistung der Bedingungen sowie der unten aufgeführte Haftungsausschluss in der mitgelieferten Dokumentation und/oder anderem mitgelieferten Material enthalten sein.

3 Der Name des Projekts und die Namen der Beiträger dürfen nur mit vorheriger schriftlicher Genehmigung zu Werbezwecken für Produkte, die auf dieser Software basieren, verwendet werden.

4 DIESE SOFTWARE WIRD VOM PROJEKT UND DEN BEITRÄGERN OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DAS PROJEKT UND DIE BEITRÄGER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND ANSPRUCHSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN HAFTUNGSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

Global IP Solutions iLBC

Die Nutzung des gesamten Originalcodes (GIPS iLBC sowie Code, der von GIPS als Teil eines verwandten IETF- oder Entwurfstandards bereitgestellt wird), unterliegt den Bedingungen der vollständigen Global IP Sound iLBC Public License, IETF Standard, zur eingeschränkten gewerblichen Nutzung (der „Lizenz“). Durch Zugreifen auf den Originalcode erklären Sie sich mit den Lizenzbedingungen einverstanden.

WEITERE BEDINGUNGEN FINDEN SIE IN DER VOLLSTÄNDIGEN LIZENZ. Im Allgemeinten gilt:

- Private, nicht gewerbliche Nutzung ist generell erlaubt.
- Gewerbliche Nutzung ist mit gewissen Einschränkungen erlaubt. Um beispielsweise sicherzustellen, dass alle iLBC-Decoder alle iLBC-kodierten Nutzdaten dekodieren können, muss eine gewerbliche Bereitstellung dem geltenden IEFT-Standard/-Entwurf entsprechen und darf das Format des Bitstreams nicht geändert werden.
- Es werden weder Garantie noch Support angeboten und jegliche Haftung wird abgelehnt.
- Vor einer gewerblichen Bereitstellung müssen Sie diese Lizenz bei GIPS registrieren.

Sie erhalten diese Lizenz von http://www.globalipsound.com/legal/licenses/ilbc; oder von Global IP Sound Europe AB, Ölandsgatan 42, SE-116 63, Stockholm, Schweden, Tel.: +46.8.545.5.30.40, Fax: +46.8.545.5.30.49; oder von Global IP Sound Inc., 900 Kearny Street, 5th Floor, San Francisco, California 94133-5124, USA, Tel.: +1 415.397.2555, Fax: +1 415.397.2577; oder auf Anforderung von info@globalipsound.com.

Die aktuellen IETF-Standards können Sie ebenfalls unter http://www.ietf.org/rfc/rfc3951.txt und einsehen. Der ursprüngliche Entwickler des Originalcodes ist Global IP Sound Inc. Teile unter Copyright © 1999-2005. Alle Rechte vorbehalten.

iLBC ist eine Marke von Global IP Sound. Alle Weiterverteilungen unterliegen den Bedingungen dieser Lizenz; der Quellcode muss diesen Hinweis enthalten.

Apache

(Siehe http://www.apache.org/licenses/LICENSE-2.0)

Lizenziert unter der Apache-Lizenz, Version 2.0 (die „Lizenz"); diese Datei darf ausschließlich unter Einhaltung der Lizenzbedingungen verwendet werden.

Apache License, Version 2.0

Apache-Lizenz
Version 2.0, Januar 2004
http://www.apache.org/licenses/

BEDINGUNGEN FÜR DIE NUTZUNG, VERVIELFÄLTIGUNG UND VERTEILUNG

1 Definitionen.

„Lizenz" bezieht sich auf die Bedingungen für die Nutzung, Vervielfältigung und Verteilung gemäß der Definition in Paragraf 1-9 dieses Dokumentes.

„Lizenzgeber" bezieht sich auf den Copyright-Inhaber oder das Rechtssubjekt, der bzw. das die Lizenz gewährt.

„Juristische Person" bezieht sich auf die Vereinigung des aktiven Rechtssubjekts mit allen anderen Rechtssubjekten, die dieses Rechtssubjekt kontrollieren, von ihm kontrolliert werden oder gemeinsam mit ihm von Dritten kontrolliert werden. Für den Zweck dieser Definition bedeutet „Kontrolle" (i) die – direkte oder indirekte – Macht zur Leitung eines derartigen Rechtssubjekts, sei es per Vertrag oder anderweitig, oder (ii) Besitz von mindestens 50 Prozent der ausgegebenen Aktien, oder (iii) wirtschaftlicher Besitz eines derartigen Rechtssubjekts.

„Sie" (oder „Ihr") bezieht sich auf eine natürliche oder juristische Person, die ihre durch diese Lizenz gewährten Rechte ausübt.

„Quellform“ bezieht sich auf die für Änderungen bevorzugte Form, insbesondere Software-Quellcode, Quelltext von Dokumentation und Konfigurationsdateien.

„Objektform“ bezieht sich auf alle Formen, die durch mechanische Umwandlung oder Übersetzung einer Quellform entstehen, insbesondere kompilierter Objektcode, generierte Dokumentation und Umwandlungen in andere Medienarten.

„Werk“ bezieht sich auf das von einem Urheber geschaffene Werk, sei es in Quell- oder Objektform, das unter der Lizenz bereitgestellt wird. Dies wird durch einen dem Werk beigefügten oder im Werk enthaltenen Copyright-Hinweis kenntlich gemacht (ein Beispiel dafür finden Sie im Anhang weiter unten).

„Abgeleitete Werke“ bezieht sich auf alle Werke, sei es in Quell- oder Objektform, die auf dem Werk basieren oder davon abgeleitet worden sind und deren redaktionelle Revisionen, Anmerkungen, Ausarbeitungen oder sonstige Änderungen als Ganzes ein Originalwerk der Urheberschaft darstellen. Für den Zweck dieser Lizenz umfassen abgeleitete Werke keine Werke, die eine vom Werk und davon abgeleiteten Werken getrennte Komponente darstellen oder die nur physisch oder dem Namen nach mit den Schnittstellen des Werks und davon abgeleiteten Werken verbunden sind.

„Beitrag“ bezieht sich auf alle Werke eines Urhebers, einschließlich der Originalversion des Werks und aller Änderungen oder Ergänzungen dieses Werks oder der davon abgeleiteten Werke, die der Copyright-Inhaber oder eine natürliche oder juristische Person im Auftrag des Copyright-Inhabers beim Lizenzgeber absichtlich zur Einbindung in das Werk einreicht. Für den Zweck dieser Definition bezieht sich „einreichen“ auf alle Formen der dem Lizenzgeber oder dessen Vertretern zugestellten elektronischen, verbalen oder schriftlichen Kommunikation, insbesondere der Kommunikation über elektronische Adresslisten, Quellcode-Kontrollsysteme und Issue-Tracking-Systeme, die vom Lizenzgeber oder in seinem Auftrag für den Zweck der Besprechung und Verbesserung des Werks betrieben werden, jedoch unter Ausschluss von Kommunikation, die deutlich vom Copyright-Inhaber durch Kennzeichnung oder auf andere schriftliche Weise als „Kein Beitrag“ identifiziert wird.

„Beiträger“ bezieht sich auf den Lizenzgeber und alle natürlichen oder juristischen Personen, von denen der Lizenzgeber einen Beitrag erhalten hat, der anschließend in das Werk eingebunden worden ist.

2 Gewährung der Copyright-Lizenz.

Vorbehaltlich dieser Lizenzbedingungen gewährt Ihnen jeder Beiträger eine immerwährende, weltweite, nicht ausschließliche, gebühren- und tantiemenfreie, unwiderrufliche Copyright-Lizenz für die Reproduktion, die Erstellung abgeleiteter Werke, die öffentliche Präsentation, die Weiterlizenzierung und Verteilung des Werks und derartiger abgeleiteter Werke im Quell- oder Objektformat.

3 Gewährung einer Patentlizenz.

Vorbehaltlich dieser Lizenzbedingungen gewährt Ihnen jeder Beiträger eine immerwährende, weltweite, nicht ausschließliche, gebühren- und tantiemenfreie, unwiderrufliche (mit der in diesem Abschnitt beschriebenen Ausnahmen) Patentlizenz, das Werk anzufertigen, anfertigen zu lassen, zu verwenden, zum Verkauf anzubieten, zu verkaufen, zu importieren und auf andere Weise zu übertragen, wobei eine derartige Lizenz nur für die von dem einzelnen Beiträger lizenzierbaren Patentansprüche gilt, gegen die durch seinen Beitrag allein oder durch die Kombination seines Beitrags mit dem Werk, zu dem dieser Beitrag eingereicht worden ist, notwendigerweise verstoßen wird. Sollten Sie gegen eine natürliche oder juristische Person eine Patentklage einreichen (einschließlich eines Gegenanspruchs oder einer Gegenklage in einem Prozess) basierend auf der Behauptung, dass das Werk oder ein im Werk eingebundener Beitrag eine direkte oder indirekte Patentverletzung darstellt, enden alle Ihnen unter dieser Lizenz für das Werk gewährte Patentlizenzen mit dem Datum der Einreichung.

4 Weiterverteilung.

Es ist Ihnen gestattet, Kopien des Werks oder davon abgeleiteter Werke in veränderter oder unveränderter Form auf einem beliebigen Medium und im Source- oder Objektformat zu reproduzieren und zu verteilen, vorausgesetzt, dass Sie die folgenden Bedingungen erfüllen:

a Sie müssen allen Empfängern des Werks oder der davon abgeleiteten Werke eine Kopie dieser Lizenz übergeben; und

b Sie müssen die veränderten Dateien mit einem deutlich sichtbaren Vermerk versehen, der auf von Ihnen vorgenommene Änderungen hinweist; und

c Sie müssen alle in der Quellform des Werks enthaltenen Copyright-, Patent-, Marken- und Namensnennungshinweise im weiterverteilten Werk beibehalten mit Ausnahme der Hinweise, die sich nicht auf einen Teil des abgeleiteten Werks beziehen; und

d Wenn das Werk eine HINWEIS-Textdatei als Teil der Verteilung enthält, müssen alle von Ihnen verteilten abgeleiteten Werke eine lesbare Kopie der in einer derartigen HINWEIS-Datei enthaltenen Namensnennungshinweise – mit Ausnahme der Hinweise, die sich nicht auf einen Teil des abgeleiteten Werks beziehen – an mindestens einer der folgenden Stellen enthalten: in einer HINWEIS-Textdatei, die als Teil der abgeleiteten Werke verteilt wird, in der Quellform oder Dokumentation, falls diese den abgeleiteten Werken beigefügt sind, oder in einer von den abgeleiteten Werken generierten Anzeige an einer Stelle, an der normalerweise derartige Hinweise von Dritten erscheinen. Der Inhalt der HINWEIS-Datei dient nur Informationszwecken und ändert die Lizenz nicht. Es steht Ihnen frei, den von Ihnen verteilten abgeleiteten Werken Ihre eigenen Namensnennungshinweise separat oder als Zusatz zum HINWEIS-Text des Werks beizufügen, vorausgesetzt, dass derartige zusätzliche Namensnennungshinweise nicht als Änderungen der Lizenz aufgefasst werden können.

e Sie können Ihren Änderungen Ihren eigenen Copyright-Hinweis beifügen und zusätzliche oder andere Lizenzbedingungen für die Nutzung, Vervielfältigung oder Verteilung Ihrer Änderungen oder derartiger abgeleiteter Werke als Ganzes bereitstellen, vorausgesetzt, dass Ihre Nutzung, Vervielfältigung und Verteilung des Werks ansonsten die in dieser Lizenz aufgeführten Bedingungen einhält.

5 Einreichen von Beiträgen.

Jeder Beitrag, der von Ihnen beim Lizenzgeber bewusst für die Einbindung in das Werk eingereicht wird, unterliegt – ausgenommen, dies wurde von Ihnen ausdrücklich anders angegeben – ausschließlich, ohne zusätzliche Bedingungen, den Bedingungen dieser Lizenz. Ungeachtet des oben Ausgeführten tritt nichts in dieser Lizenz an die Stelle der Bedingungen einer von Ihnen möglicherweise mit dem Lizenzgeber bezüglich derartiger Beiträge eingegangenen Lizenzvereinbarung oder verändert die Bedingungen einer solchen Lizenzvereinbarung.

6 Marken.

Diese Lizenz gewährt nicht die Erlaubnis zur Verwendung der Markennamen, Marken, Dienstleistungsmarken oder Produktnamen des Lizenzgebers außer ihrer angemessenen und üblichen Verwendung in der Beschreibung der Herkunft des Werks und im reproduzierten Inhalt der HINWEIS-Datei.

7 Ausschluss der Gewährleistung.

SOFERN NICHT ANDERWEITIG GESETZLICH ERFORDERLICH ODER SCHRIFTLICH VEREINBART, STELLT DER LIZENZGEBER DAS WERK (UND JEDER BEITRÄGER SEINE BEITRÄGE) OHNE MÄNGELGEWÄHR UND OHNE JEGLICHE GEWÄHRLEISTUNG SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART ZUR VERFÜGUNG, INSBESONDERE OHNE GARANTIEN ODER BEDINGUNGEN DES TITELS, NICHTVERLETZUNG VON EIGENTUMSRECHTEN, DER MARKTFÄHIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. Sie allein sind für die Feststellung der Angemessenheit einer Verwendung oder Weiterverteilung des Werks verantwortlich und tragen alle Risiken, die mit Ausübung der Ihnen unter dieser Lizenz gewährten Rechte einhergehen.

8 Haftungsausschluss.

In keinem Fall und auf keiner Rechtsgrundlage, sei es als Recht der unerlaubten Handlung (einschließlich Fahrlässigkeit), Vertragsrecht oder eines anderen Rechts, außer wenn gesetzlich erforderlich (beispielsweise bei absichtlichen und grob fahrlässigen Handlungen) oder schriftlich vereinbart, haftet ein Beteiligter Ihnen gegenüber für Schäden, einschließlich direkter, indirekter, konkreter, beiläufiger oder nachfolgender Schäden jeder Art, die aus dieser Lizenz oder der Nutzung bzw. Nichtnutzbarkeit des Werks (insbesondere Schäden durch Goodwill-Verlust, Arbeitsausfälle, Computerausfälle oder -funktionsstörungen oder alle anderen kommerziellen Schäden oder Verlusten), selbst wenn ein derartiger Beteiligter auf die Möglichkeit derartiger Schäden hingewiesen worden ist.

9 Anerkennung von Gewährleistung oder zusätzlicher Haftung.

Für die Weiterverteilung des Werks oder davon abgeleiteter Werke steht es Ihnen frei, Support, Garantien, Haftungsausschlüsse oder andere Haftungsverpflichtungen und/oder Rechte – auch gegen Gebühr – anzubieten, die im Einklang mit dieser Lizenz stehen. Durch die Anerkennung derartiger Verpflichtungen dürfen Sie jedoch nur in Ihrem eigenen Namen und auf Ihre eigene alleinige Verantwortung handeln, nicht im Namen eines anderen Beiträgers, und nur, wenn Sie sich verpflichten, alle Beiträger für alle Haftansprüche, die von einem dieser Beiträger durch Ihr Anerkennen einer derartigen Garantie oder zusätzlichen Haftung verursacht oder die aus diesem Grund gegen einen dieser Beiträger vorgebracht werden, schadlos zu halten.

MIT-Lizenz

Copyright © 2008 Cisco-Systems, Inc.

Die folgende Erlaubnis gilt nur für den unter die „MIT-Lizenz“ fallenden Teil der Software, einschließlich Teile der SSH-Server- und XML-Parser-Software. Dieser Teil wird in der folgenden Bezugnahme als die „Software“ definiert: Die MIT-Lizenz ist erhältlich unter: http://www.opensource.org/licenses/mit-license.php

Hiermit wird allen Personen, die eine Kopie dieser Software und dazugehöriger Dokumentationsdateien (der „Software“) die kostenlose Erlaubnis erteilt, mit der Software ohne Einschränkung Handel zu treiben, insbesondere die Rechte, Kopien der Software zu nutzen, zu vervielfältigen, zu ändern, mit anderen Komponenten zusammenzufügen, zu veröffentlichen, zu verteilen, weiterzulizenzieren und/oder zu verkaufen und den Personen, denen die Software bereitgestellt wird, dies ebenfalls zu gestatten, unter den folgenden Bedingungen:

Der obige Copyright-Hinweis und diese Erlaubnis müssen in allen Kopien oder wesentlichen Teilen der Software enthalten sein.

DIESE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE GARANTIEN DER MARKTFÄHIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON EIGENTUMSRECHTEN, WERDEN AUSGESCHLOSSEN. IN KEINEM FALL SIND DIE VERFASSER ODER COPYRIGHT-INHABER FÜR HAFTUNGSANSPRÜCHE, SCHÄDEN ODER ANDERE ANSPRÜCHE HAFTBAR, DIE IN VERBINDUNG MIT DER SOFTWARE, DER NUTZUNG DER SOFTWARE ODER DEM HANDEL MIT DER SOFTWARE ENTSTEHEN.

BSD-Lizenz

Copyright ©1993 The Regents of the University of California. Alle Rechte vorbehalten.

Diese Software wurde von der Computer Systems Engineering Gruppe des Lawrence Berkeley Laboratory im Rahmen des DARPA-Vertrags BG 91-66 der Defense Advanced Research Projects Agency entwickelt und in Berkeley eingebracht.

DIESE SOFTWARE WIRD VON THE REGENTS UND DEN BEITRÄGERN OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, INSBESONDERE DIE STILLSCHWEIGENDEN GARANTIEN DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. THE REGENTS UND MITARBEITER SIND IN KEINEM FALL FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, KONKRETE ODER NACHFOLGENDE SCHÄDEN ODER VERSCHÄRFTE SCHADENSERSATZANSPRÜCHE HAFTBAR (INSBESONDERE FÜR DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTEN, NUTZUNGSAUSFÄLLE, DATENVERLUSTE, ENTGANGENE GEWINNE ODER GESCHÄFTSAUSFÄLLE), DIE AUFGRUND DER NUTZUNG DIESER SOFTWARE ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE; DIES GILT UNABHÄNGIG VON DER SCHADENSURSACHE UND HAFTUNGSGRUNDLAGE, SEI ES AUFGRUND VON VERTRAGSRECHT, UNERLAUBTER HANDLUNG ODER EINER ANDEREN ANSPRUCHSGRUNDLAGE (EINSCHLIESSLICH FAHRLÄSSIGKEIT).

GPLv2

Teile der Software werden unter den Bedingungen von Version 2 der GNU General Public License („GPL“) bereitgestellt, und alle Nutzung derartiger GPL-Komponenten und Ableitungen davon durch den Lizenznehmer hat unter Einhaltung der Bedingungen der GPL zu erfolgen. Eine Kopie der GPL finden Sie unter: http://www.gnu.org/licenses/gpl.txt. Eine computerlesbare Kopie des Quellcodes, der für die in diesem Produkt enthaltene, unter GPL Version 2 lizenzierte Software gilt, können Sie gemäß der GPL-Lizenz von Cisco Systems, Inc. anfordern (siehe GPL-Bedingungen im obigen Abschnitt zu eCOS).

Sie können eine Kopie des Quellcodes gemäß der General License Version 2 unter Angabe Ihres Namens und Ihrer Adresse unter folgender Anschrift anfordern:

Attn: Software Engineer
Cable Home Network BU
Cisco Video Technology Group
5030 Sugarloaf Highway
Lawrenceville, GA 30044, USA

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

June 2012 Printed in USA Part Number 4030832 Rev B