

Referenzhandbuch für Kabel-/DSL-Wireless- Router, Modell MR814 v2

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054

SM-MR814NA-2
Version 4.12
Dezember 2002

©2003 by NETGEAR, Inc. Alle Rechte vorbehalten.

Marken

NETGEAR ist eine Marke von Netgear, Inc.

Microsoft, Windows und Windows NT sind eingetragene Marken der Microsoft Corporation.

Andere Marken- und Produktnamen sind eingetragene Marken oder Marken der entsprechenden Unternehmen.

Haftungsausschluss

Im Hinblick auf die Verbesserung des Designs, der Funktionen und der Zuverlässigkeit behält sich NETGEAR das Recht vor, die in diesem Dokument beschriebenen Produkte ohne vorherige Ankündigung zu ändern.

NETGEAR übernimmt keine Haftung für Schäden, die durch die Verwendung oder den Einsatz der in diesem Dokument aufgeführten Produkte entstehen können.

Federal Communications Commission (FCC) : Hinweis zu Störstrahlungen

Dieses Gerät wurde nach Maßgabe der Klasse B, Digitale Geräte, entsprechend Paragraph 15 der FCC-Ordnung erfolgreich getestet. Diese Grenzwerte bieten einen angemessenen Schutz gegen schädliche Strahlungen in Wohngebieten. Dieses Gerät erzeugt und arbeitet mit elektromagnetischen Wellen. Bei unsachgemäßem Gebrauch, insbesondere wenn das Gerät entgegen den Empfehlungen betrieben wird, können Störstrahlungen auftreten. Es wird keine Garantie dafür gegeben, dass bei einer bestimmten Installation keine Störstrahlungen auftreten. Wenn dieses Gerät schädliche Störungen des Rundfunk- oder Fernsehempfangs verursacht, was sich durch Ein- und Ausschalten des Geräts feststellen lässt, wird dem Benutzer empfohlen, eine oder mehrere der folgenden Maßnahmen zu ergreifen:

- Die Empfangsantenne neu ausrichten oder umsetzen.
- Den Abstand zwischen dem Gerät und dem Empfänger vergrößern.
- Das Gerät an eine Steckdose anschließen, die zu einem anderen Stromkreis gehört als die Steckdose, an der der Empfänger angeschlossen ist.
- Den Fachhändler oder einen erfahrenen Radio-/Fernsehtechniker hinzuziehen.

Bestätigung der Konformität nach EN 55 022

Hiermit wird bestätigt, dass das Modell MR814 v2 Kabel-/DSL-Wireless-Router entsprechend der Richtlinie 89/336/EWG, Artikel 4a, der Europäischen Union entstört ist und keine Funkstörstrahlung erzeugt. Die Konformität wird durch Anwendung von EN 55 022 Klasse B (CISPR 22) bestätigt.

Bestätigung des Herstellers/Importeurs

Hiermit wird bestätigt, dass der Kabel-/DSL-Wireless-Router, Modell MR814 v2, gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Der ordnungsgemäße Betrieb einiger Geräte (z. B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung. Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, dass diese Geräte auf den Markt gebracht wurden, und es wurde berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

VCCI-Bestätigung (Voluntary Control Council for Interference)

Bei diesem Gerät handelt es sich um ein Gerät der Klasse B (Datenaustauschgerät, das in Wohngebieten oder angrenzenden Gebieten eingesetzt wird). Es entspricht den vom „Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines“ zur Vermeidung von Funkstörungen in solchen Wohngebieten festgelegten Normen. Bei Einsatz in der Nähe eines Rundfunk- oder Fernsehempfängers kann es Funkstörungen verursachen. Lesen Sie die Anweisungen zur ordnungsgemäßen Handhabung.

Kunden-Support

Diesbezügliche Informationen finden Sie auf der Support-Informationskarte, die im Lieferumfang Ihres Kabel-/DSL-Wireless-Router, Modell MR814 v2, enthalten ist.

Internet

NETGEAR unterhält unter der Internetadresse <http://www.netgear.de> eine Website im Internet. Für den Zugriff auf diese Website benötigen Sie eine direkte Internet-Verbindung und einen Web-Browser, z. B. Internet Explorer oder Netscape Navigator.

Vorwort

Informationen zu diesem Handbuch

Kapitel 1

Einführung

Die wichtigsten Merkmale des Routers.	1-1
Wireless-Netzwerkbetrieb entsprechend der Norm 802.11b	1-2
Leistungsstarke, echte Firewall mit Content Filtering	1-2
Sicherheit	1-3
Ethernet-Verbindungen mit automatischer Erkennung und Auto Uplink™	1-3
Umfassende Unterstützung der gängigen Protokolle	1-3
Einfache Installation und Verwaltung	1-4
Wartung und Support.	1-4
Packungsinhalt	1-5
Vorderseite des Routers	1-6
Rückseite des Routers.	1-7

Kapitel 2

Router an das Internet anschließen

Voraussetzungen	2-1
Anforderungen bezüglich Verkabelung und Computer-Hardware.	2-1
Voraussetzungen für die Konfiguration des Computers im Netzwerk	2-1
Voraussetzungen für die Internet-Konfiguration	2-2
Wo finde ich die Parameter für die Internet-Konfiguration?.	2-2
Arbeitsblatt für Angaben zum Internet-Anschluss notieren	2-3
Kabel-/DSL-Wireless Router, Modell MR814 v2, an das LAN anschließen	2-4
Erkennung von PPPoE durch den Assistenten.	2-8
Erkennung der dynamischen IP durch den Assistenten	2-10
Erkennung der statischen IP durch den Assistenten	2-11
Manuelle Konfiguration der Internet-Verbindung.	2-12

Kapitel 3

Wireless-Konfiguration

Hinweise zu Wireless-Netzwerken	3-1
Hinweise zur Leistung, Platzierung und Reichweite.	3-1
Geeignete Wireless-Sicherheit einrichten.	3-2
Bedeutung der Wireless-Einstellungen	3-2
Einstellungen für ein Wireless-Netzwerk	3-3
Wireless-Zugriff auf das Netzwerk einschränken	3-3
Zugriff auf das Netzwerk durch Deaktivierung der Wireless-Konnektivität einschränken	3-4
Drahtlosen Zugriff über den Namen des Wireless-Netzwerks (SSID) einschränken	3-4
Drahtlosen Zugriff über die Wireless-Zugriffsliste einschränken.	3-4
Methoden für die Authentifizierung und die Sicherheitsverschlüsselung auswählen.	3-5
Authentifizierungssystem auswählen.	3-5
Verschlüsselungsmodus auswählen	3-6

Kapitel 4

Content Filtering

Übersicht zu Content Filtering	4-1
Zugriff auf Internet-Seiten sperren	4-2
Zugriff auf Internet-Dienste sperren	4-3
Benutzerdefinierten Dienst konfigurieren.	4-4
Konfiguration zum Sperren von Diensten über den IP-Adressbereich	4-5
Zeitplan zum Sperren von Seiten/Diensten.	4-5
Protokolle zum Internet-Zugriff und zu Zugriffsversuchen anzeigen.	4-6
E-Mail-Warnungen und Protokollberichte zum Internet-Zugriff konfigurieren	4-7

Kapitel 5

Wartung

Statusinformationen des Routers anzeigen.	5-1
Liste der angeschlossenen Geräte anzeigen	5-5
Upgrade der Router-Software.	5-5
Handhabung der Konfigurationsdatei.	5-6
Konfiguration sichern und wieder herstellen.	5-7
Konfiguration löschen	5-8
Administrator-Kennwort ändern	5-8

Kapitel 6

Erweiterte Konfiguration des Routers

Konfiguration der Port-Weiterleitung an lokale Server.	6-1
Benutzerdefinierten Dienst hinzufügen.	6-2
Eintrag für Port-Weiterleitung bearbeiten oder löschen.	6-3
Beispiel: Lokaler Web- und FTP-Server	6-3
Optionen für die WAN-Konfiguration	6-4
Standard-DMZ-Server einrichten	6-4
Ping an Internet-WAN-Anschluss beantworten	6-5
MTU-Größe festlegen.	6-5
Optionen für LAN-IP-Konfiguration verwenden.	6-6
LAN-TCP/IP-Konfigurationsparameter einstellen	6-6
Router als DHCP-Server verwenden.	6-7
Adressen reservieren	6-8
Dynamischen DNS-Dienst verwenden	6-9
Statisches Routing konfigurieren	6-10
Zugriff für dezentrale Verwaltung aktivieren	6-12
Universal Plug and Play (UPnP) verwenden.	6-14

Kapitel 7

Fehlerbehebung

Grundbetrieb	7-1
Netz-LED leuchtet nicht.	7-1
Test-LED leuchtet nicht oder leuchtet permanent	7-2
LEDs für LAN- oder WAN-Port leuchten nicht	7-2
Fehlerbehebung an der Schnittstelle für die Web-Konfiguration	7-3
Fehlerbehebung bei der ISP-Verbindung	7-4
Fehlerbehebung in einem TCP/IP-Netzwerk mit einem Ping-Dienstprogramm	7-5
LAN-Pfad zum Router prüfen	7-5
Pfad von PC zu einem dezentralen Gerät prüfen	7-6
Standardkonfiguration und -kennwort wieder herstellen	7-7
Probleme bei Datum und Uhrzeit.	7-7

**Anhang A
Technische Daten**

**Anhang B
Netzwerke, Routing, Firewalls: Grundlagen**

Zugehörige Publikationen	B-1
Basisinformationen zu Routern	B-1
Was ist ein Router?	B-2
Routing Information Protocol	B-2
IP-Adressen und das Internet.	B-2
Netzmaske.	B-4
Subnetz-Adressierung.	B-5
Private IP-Adressen	B-7
Betrieb mit einer IP-Adresse und NAT.	B-8
MAC-Adressen und Adressenauflösungsprotokoll.	B-9
Zugehörige Dokumente	B-9
Domain-Namensserver	B-10
IP-Konfiguration über DHCP	B-10
Internet-Sicherheit und Firewalls.	B-10
Was ist eine Firewall?	B-11
Stateful Packet Inspection.	B-11
DoS-Angriff (Denial of Service)	B-11
Ethernet-Verkabelung	B-12
Uplink-Schalter, Crossover-Kabel und MDI/MDIX-Schaltung	B-12
Kabelqualität	B-13

**Anhang C
Netzwerk vorbereiten**

Computer für den Einsatz im TCP/IP-Netzwerk vorbereiten	C-1
Konfiguration von Windows 95, 98 und Me für die Verwendung eines TCP/IP-Netzwerks.	C-2
Windows-Komponenten für Netzwerkbetrieb installieren oder überprüfen	C-2
Automatische Konfiguration der TCP/IP-Einstellungen durch DHCP unter Windows 95B, 98 und Me aktivieren	C-4
Internet-Zugriffsmethode unter Windows auswählen	C-6
TCP/IP-Eigenschaften überprüfen	C-6

Windows NT4, 2000 oder XP für den Betrieb eines IP-Netzwerks konfigurieren . . .	C-7
Windows-Komponenten für Netzwerkbetrieb installieren oder überprüfen . . .	C-7
DHCP-Konfiguration von TCP/IP unter Windows XP, 2000 oder NT4	C-8
DHCP-Konfiguration von TCP/IP unter Windows XP	C-8
DHCP-Konfiguration von TCP/IP unter Windows 2000	C-10
DHCP-Konfiguration von TCP/IP unter Windows NT4.	C-13
TCP/IP-Eigenschaften für Windows XP, 2000 und NT4 überprüfen	C-15
Macintosh für die Verwendung eines TCP/IP-Netzwerks konfigurieren	C-15
MacOS 8.6 oder 9.x	C-15
MacOS X	C-16
TCP/IP-Eigenschaften für Macintosh-Computer überprüfen	C-17
Betriebsbereitschaft des Internet-Kontos überprüfen	C-18
Werden Anmeldeprotokolle verwendet?	C-18
Wie lauten die Konfigurationseinstellungen?	C-18
ISP-Konfigurationsangaben für Windows-Computer ermitteln	C-19
ISP-Konfigurationsangaben für Macintosh-Computer ermitteln.	C-20
Netzwerk neu starten.	C-21

Anhang D

Basisinformationen zu Wireless-Netzwerken

Wireless-Netzwerke, Übersicht	D-1
Infrastrukturmodus	D-1
Ad-hoc-Modus (Peer-to-Peer Workgroup)	D-2
Netzwerkname: Extended Service Set Identification (ESSID).	D-2
Authentifizierung und WEP	D-3
Authentifizierung nach 802.11b.	D-3
Open System-Authentifizierung	D-4
Shared Key-Authentifizierung	D-4
Übersicht der WEP-Parameter	D-5
Codegröße	D-6
Optionen zur WEP-Konfiguration	D-7
Wireless-Kanäle	D-7

Glossar

Index

Vorwort

Informationen zu diesem Handbuch

Herzlichen Glückwunsch zum Kauf des Kabel-/DSL-Wireless Routers Modell MR814 v2 von NETGEAR®.

Der Router MR814 v2 ermöglicht die Anbindung mehrerer PCs an das Internet; verwendet wird dabei ein externes Breitband-Zugangsgerät (z. B. ein Kabel- oder ein DSL-Modem), das normalerweise für einzelne PCs eingesetzt wird.

Zielgruppe

Das vorliegende Referenzhandbuch wendet sich an Leser, die über grundlegende bis fortgeschrittene Computer- und Internet-Kenntnisse verfügen. Dennoch finden Sie in den Anhängen und auf der Website von Netgear Informationen zu den Grundlagen von Computer-Netzwerken, dem Internet, einer Firewall und der VPN-Technologie sowie zahlreiche Praxis-Beispiele.

Konventionen zur Schreibweise

In dem vorliegenden Handbuch gelten folgende Schriftkonventionen:

<i>Kursivschrift</i>	Bezeichnungen von Medien, UNIX-Dateien, Befehle, URLs und Verzeichnisnamen.
Times Roman, fett	Benutzereingaben.
Internet Protocol (IP)	Bei der erstmaligen Verwendung einer Abkürzung wird auch der vollständige, ausgeschriebene Begriff angegeben.
Courier	Am Bildschirm angezeigter Text, Benutzereingaben in der Befehlszeile.
[Eingabe]	Tastenbezeichnungen werden im Text in eckigen Klammern dargestellt. Die Bezeichnung [Eingabe] wird für die Eingabetaste und die Return-Taste verwendet.
[Strg]+C	Zwei oder mehr Tasten, die gleichzeitig gedrückt werden müssen, werden im Text durch ein Plus-Zeichen (+) miteinander verbunden.
KAPITÄLCHEN	DOS-Dateien und Verzeichnisnamen.

Formate für wichtige Meldungen

In dem vorliegenden Handbuch werden wichtige Meldungen durch folgende Formate hervorgehoben:



Hinweis: Mit diesem Format werden Informationen von besonderer Bedeutung hervorgehoben.

Kapitel 1

Einführung

In diesem Kapitel werden die wichtigsten Merkmale und Funktionen des Kabel-/DSL-Wireless-Routers Modell MR814 v2 von NETGEAR beschrieben.

Die wichtigsten Merkmale des Routers

Der Kabel-/DSL-Wireless-Router Modell MR814 v2 verfügt über einen Switch mit vier Ports und ermöglicht die Anbindung Ihres LANs (Local Area Network) an das Internet; zu diesen Zweck wird ein externes Zugangsgerät wie ein Kabel- oder DSL-Modem verwendet.

Der Router MR814 v2 bietet verschiedene Optionen zum Content Filtering der Internet-Inhalte sowie eine Berichtsfunktion zur Browsing-Aktivität und eine schnelle Alarmfunktion - beide über E-Mail. Benutzer und Netzwerkadministratoren können entsprechend der Tageszeit, der Website-Adressen und der Keywords der Web-Adressen Regelungen für einen eingeschränkten Internet-Zugang festlegen und für bis zu 253 PCs einen schnellen Kabel-/DSL-Internet-Zugang einrichten. Daneben schützt Sie die NAT-Funktion (Network Address Translation - Netzwerk-Adressumsetzung), der integrierte Firewall, vor Hackerangriffen.

Der Konfigurationsaufwand für den Router ist minimal - schon nach wenigen Minuten ist der Router installiert und betriebsbereit.

Der Router MR814 v2 bietet folgende Leistungsmerkmale:

- Wireless-Netzwerkbetrieb entsprechend der Norm 802.11b
- Einfache, web-gestützte Installation und Verwaltung
- Content Filtering und Sperrung einzelner Websites
- Integrierter Switch mit vier Ports mit 10/100 MBit/s
- Ethernet-Anschluss an ein WAN-Gerät (Wide Area Network - Fernnetz), z. B. ein Kabel- oder DSL-Modem
- Umfassende Unterstützung der gängigen Protokolle
- Anmeldefunktion

- LEDs an der Vorderseite zur bequemen Kontrolle von Status und Betrieb
- Flash-Speicher für Firmware-Upgrades

Wireless-Netzwerkbetrieb entsprechend der Norm 802.11b

Der Router MR814 v2 verfügt über einen Wireless Access Point gemäß 802.11b und ermöglicht damit eine permanente, schnelle Verbindung (11 MBit/s) zwischen Ihrem Wireless Gerät und dem Ethernet-Gerät. Die wichtigsten Merkmale dieses Access Point sind:

- Betrieb eines Wireless-Netzwerks gemäß der Norm 802.11b mit bis zu 11 MBit/s
- Sicherheit durch 64-Bit- und 128-Bit-WEP-Verschlüsselung
- Generierung der WEP-Codes manuell oder über Passphrase
- Möglichkeit der Einschränkung des drahtlosen Zugangs über MAC-Adresse
- Die Rundsendung des Namens des Wireless-Netzwerks kann deaktiviert werden, sodass sich nur Geräte, die den Netzwerknamen kennen (SSID), auf das Netzwerk zugreifen können.

Leistungsstarke, echte Firewall mit Content Filtering

Im Gegensatz zu einfachen, Internet-gestützten NAT-Routern ist der MR814 v2 eine echte Firewall, die Hackerangriffe über eine Stateful Packet Inspection (Paketüberprüfung) abwehrt.

Leistungsmerkmale der Firewall:

- DoS-Schutz (Denial of Service - Unterbrechung der Verfügbarkeit von Websites).
Erkennt und unterbindet DoS-Angriffe wie Ping of Death, SYN Flood, LAND Attack und IP-Spoofing automatisch.
- Blockiert unerwünschten Datenverkehr aus dem Internet in Ihr LAN.
- Sperrt den Zugriff von Ihrem LAN aus auf die Internet-Seiten oder -Dienste, die Sie festlegen.
- Führt ein Protokoll über sicherheitsrelevante Zwischenfälle.

Der MR814 v2 protokolliert sicherheitsrelevante Ereignisse wie blockierte eingehende Datenübertragungen, Port-Abfragen, Angriffe und Anmeldungen durch den Administrator. Bei der Konfiguration des Routers können Sie festlegen, dass dieses Protokoll in bestimmten Abständen per E-Mail an Sie gesendet werden soll. Außerdem können Sie den Router so konfigurieren, dass bei einem signifikanten Ereignis sofort eine Alarmmeldung an Ihre E-Mail-Adresse oder Ihren E-Mail-Pager gesendet wird.

- Durch die Content Filtering-Funktion verhindert der MR814 v2, dass fragwürdige Inhalte aus dem Internet auf Ihren PC gelangen. Den Zugriff auf Internet-Inhalte können Sie durch Prüfung der Keywords von Web-Adressen steuern. Daneben können Sie bei der Konfiguration festlegen, dass Zugriffsversuche auf fragwürdige Internet-Seiten protokolliert und gemeldet werden sollen.

Sicherheit

Der Router MR814 v2 verfügt über verschiedene Sicherheitsfunktionen, die in diesem Kapitel beschrieben werden.

- Durch NAT geschützte PCs
NAT (Netzwerk-Adressumsetzung) erzeugt für Anfragen aus dem lokalen Netzwerk einen temporären Pfad ins Internet. Anfragen, die außerhalb des LANs gestartet wurden, werden gelöscht; dadurch wird verhindert, dass Benutzer außerhalb des LANs die zum LAN gehörigen PCs finden und auf sie zugreifen.
- Port-Weiterleitung mit NAT
Obwohl NAT den direkten Zugriff von Internet-Adressen auf die PCs innerhalb des LANs verhindert, können Sie mit Hilfe des Routers die Weiterleitung eingehender Daten an einzelne PCs (entsprechend der Port-Nummer der eingehenden Anfrage) oder an einen festgelegten "DMZ"-Host-Computer veranlassen. Diese Weiterleitung kann für einzelne Ports oder für Port-Bereiche definiert werden.

Ethernet-Verbindungen mit automatischer Erkennung und Auto Uplink™

Mit dem internen 10/100-Switch mit acht Ports ermöglicht der Router MR814 v2 den Anschluss an ein Standard-Ethernet-Netzwerk mit 10 MBit/s oder an ein Fast Ethernet-Netzwerk mit 100 MBit/s. Sowohl die LAN- als auch die WAN-Schnittstelle verfügen über eine automatische Erkennungsfunktion und unterstützen den Vollduplex- und den Halbduplex-Betrieb.

Der Router verwendet die Auto Uplink™-Technologie. Jeder Ethernet-Port erkennt automatisch, ob das an dem Port eingesteckte Ethernet-Kabel eine "normale" Verbindung, z. B. zu einem PC, oder eine "Uplink"-Verbindung, z. B. zu einem Switch oder Hub, benötigt. Daraufhin wird der Port automatisch für die erforderliche Verbindung konfiguriert. Damit können Sie auf die Verwendung eines Crossover-Kabels verzichten, da Auto Uplink in jedem Fall die korrekte Verbindung für den jeweiligen Kabeltyp herstellt.

Umfassende Unterstützung der gängigen Protokolle

Der Router MR814 v2 unterstützt das Transmission Control Protocol/Internet Protocol (TCP/IP) und das Routing Information Protocol (RIP). Weitere Informationen zu TCP/IP finden Sie in Anhang B, "Netzwerke, Routing, Firewalls: Grundlagen".

- Gemeinsame Nutzung einer IP-Adresse durch NAT
Mit dem Router MR814 v2 können mehrere PCs innerhalb eines Netzwerks ein gemeinsames Internet-Konto mit nur einer IP-Adresse verwenden, die von Ihrem Internet Service Provider (ISP) statisch oder dynamisch zugewiesen wird. Dieses als NAT bezeichnete Verfahren (Netzwerk-Adressumsetzung) erlaubt die Verwendung eines kostengünstigen Einzelplatz-ISP-Kontos.

- Automatische Konfiguration angeschlossener PCs durch DHCP
Informationen zur Netzwerkkonfiguration, z. B. IP-, Gateway- und DNS-Adressen (Domain Name Server) werden durch den Router MR814 v2 den an das LAN angeschlossenen PCs dynamisch zugewiesen; dabei kommt die DHCP-Funktion (Dynamic Host Configuration Protocol) zur Anwendung. Diese Funktion vereinfacht die Konfiguration von PCs im lokalen Netzwerk beträchtlich.
- DNS-Proxy
Wenn DHCP aktiviert ist und keine DNS-Adressen angegeben sind, stellt der Router den angeschlossenen PCs seine eigene Adresse als DNS-Server zur Verfügung. Während des Aufbaus der Verbindung fragt der Router die tatsächlichen DNS-Adressen bei dem SIP ab und leitet DNS-Anfragen aus dem LAN weiter.
- PPP over Ethernet (PPPoE)
PPPoE ist ein Protokoll für den Anschluss dezentraler Hosts an das Internet; dabei wird durch Simulation einer Wählverbindung eine DSL-Verbindung hergestellt. Diese Funktion macht die Ausführung eines Anmeldeprogramms wie Entersys oder WinPOET auf Ihrem PC überflüssig.

Einfache Installation und Verwaltung

Nach Anschluss an das Netzwerk können Sie den Kabel-/DSL-Wireless-Router Modell MR814 v2 innerhalb weniger Minuten installieren, konfigurieren und in Betrieb nehmen. Folgende Funktionen erleichtern Ihnen dabei die Installation und Verwaltung:

- Browser-gestütztes Management
Mit der Browser-gestützten Konfiguration können Sie Ihren Router mühelos von beinahe jedem PC aus (z. B. Windows, Macintosh oder Linux) konfigurieren. Dabei hilft Ihnen ein benutzerfreundlicher Konfigurationsassistent; und darüber hinaus verfügt die Browser-gestützte Web-Management-Schnittstelle über eine integrierte Online-Hilfe-Dokumentation.
- Smart Wizard
Der Router MR814 v2 erkennt automatisch den Typ der Internet-Verbindung und fordert von Ihnen nur die Informationen an, die für Ihren ISP-Kontentyp erforderlich sind.
- Überwachungsanzeigen
Die Leuchtanzeigen an der Vorderseite des Routers MR814 v2 ermöglichen eine einfache Überwachung des Status und der Aktivität des Routers.

Wartung und Support

NETGEAR unterstützt Sie bei der optimalen Nutzung Ihres Routers MR814 v2 mit folgenden Angeboten:

- Flash-Speicher für Firmware-Upgrades
- Kostenloser technischer Support an sieben Tagen in der Woche, rund um die Uhr

Packungsinhalt

Im Lieferumfang des Pakets sollten folgende Teile enthalten sein:

- Kabel-/DSL-Wireless Router Modell MR814 v2
- Wechselstrom-Netzteil
- Ethernet-Kabel der Kategorie 5 (CAT5)
- Modell MR814 v2 Ressourcen-CD, einschließlich:
 - des vorliegenden Handbuchs
 - der Anwendungshinweise und weiterer hilfreicher Informationen
- Installationshandbuch für Kabel-/DSL-Wireless Router Modell MR814 v2
- Registrierungs- und Garantiekarte.
- Karte mit Support-Informationen. Falls eines dieser Elemente fehlerhaft, beschädigt oder nicht vorhanden ist, wenden Sie sich bitte an Ihren NETGEAR-Fachhändler. Bewahren Sie den Karton sowie das Original-Verpackungsmaterial bitte auf, falls Sie den Router zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

Falls eines dieser Elemente fehlerhaft, beschädigt oder nicht vorhanden ist, wenden Sie sich bitte an Ihren NETGEAR-Fachhändler. Bewahren Sie den Karton sowie das Original-Verpackungsmaterial bitte auf, falls Sie den Router zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

Vorderseite des Routers

An der Vorderseite des Kabel-/DSL-Wireless-Router Modell MR814 v2 (Abbildung 1-1) befinden sich Status-LEDs.

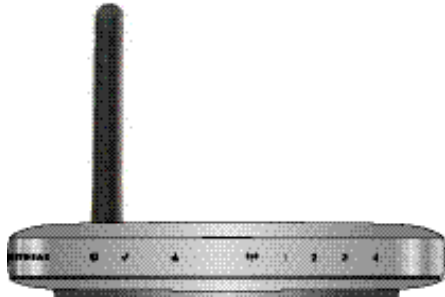






Abbildung 1-1: Frontansicht des MR814 v2

Mit einigen dieser LEDs können Sie den Status von Verbindungen überprüfen. In Tabelle 1 werden die LEDs an der Vorderseite des Routers von links nach rechts beschrieben. Diese LEDs leuchten grün, wenn sie aktiviert sind.

Tabelle 1. Beschreibung der LED-Leuchten

Symbol	Verhalten	Beschreibung
 Netz	Ein Aus	Der Router ist an die Netzversorgung angeschlossen. Der Router ist nicht an die Netzversorgung angeschlossen.
 Internet	Ein (Grün) Blinken (Grün)	Der Internet-Port (WAN) hat eine Verbindung mit einem angeschlossenen Gerät erkannt. Daten werden über den Internet-Port gesendet oder empfangen.
 Wireless	Ein	Der Wireless-Port wurde initialisiert.
 Local	Ein (Grün) Blinken (Grün) Ein (Gelb) Blinken (Gelb) Aus	Der Local-Port (LAN) hat eine Verbindung mit 100 MBit/s zu einem angeschlossenen Gerät erkannt. Daten werden mit 100 MBit/s gesendet oder empfangen. Der Local-Port hat eine Verbindung mit 10 MBit/s zu einem angeschlossenen Gerät erkannt. Daten werden mit 10 MBit/s gesendet oder empfangen. An diesem Port wurde keine Verbindung festgestellt.

Rückseite des Routers

An der Rückseite des Routers Modell MR814 (Abbildung 1-2) befinden sich die verschiedenen Ports und Anschlüsse.

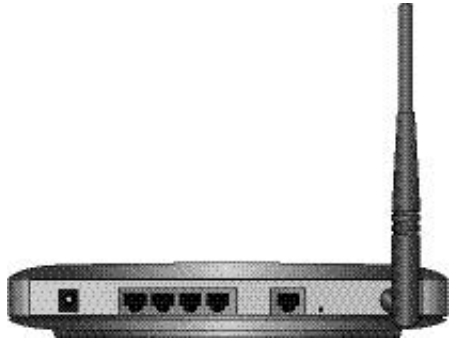


Abbildung 1-2: Rückseite des MR814 v2

An der Rückseite des Routers befinden sich folgende Anschlüsse (von links nach rechts):

- Anschluss für Wechselstrom-Netzteil
- Vier lokale ('Local') Ethernet-Ports (LAN) für den Anschluss des Routers an die lokalen PCs
- Internet-Ethernet-Port (WAN) für den Anschluss des Routers an ein Kabel- oder DSL-Modem
- Taste für Zurücksetzen auf Standardeinstellungen
- Wireless-Antenne

Kapitel 2

Router an das Internet anschließen

In diesem Kapitel wird beschrieben, wie Sie den Router in Ihrem lokalen Netzwerk (LAN) einrichten und an das Internet anschließen. Dabei wird erläutert, wie der Internet-Zugang an dem Kabel-/DSL-Wireless-Router Modell MR814 v2 mit Hilfe des Konfigurationsassistenten oder manuell konfiguriert werden kann.

Voraussetzungen

Zunächst sollten Sie überprüfen, ob die folgenden drei Voraussetzungen erfüllt sind:

1. Sie verfügen über einen aktiven Internet-Dienst, z. B. über ein Kabel- oder DSL-Breitbandkonto.
2. Sie kennen die Konfigurationsdaten des Internet Service Provider (ISP) für Ihr DSL-Konto.
3. Der Router ist an ein Kabel- oder DSL-Modem und einen Computer angeschlossen (siehe unten).

Anforderungen bezüglich Verkabelung und Computer-Hardware

Sie können den Router MR814 v2 nur in einem Netzwerk einsetzen, wenn in jedem Computer eine Ethernet-Netzwerkschnittstellenkarte (Network Interface Card, NIC) sowie ein Ethernet-Kabel installiert bzw. angeschlossen ist. Für eine 100 MBit/s-Anbindung des Computers an das Netzwerk ist das Kabel der Kategorie 5 (CAT5) zu verwenden, das im Lieferumfang des Routers enthalten ist.

Voraussetzungen für die Konfiguration des Computers im Netzwerk

Der MR814 v2 verfügt über einen integrierten Web-Konfigurationsmanager. Zur Verwendung der Konfigurationsmenüs des MR814 v2 benötigen Sie ein Java-gestütztes Web-Browser-Programm, das HTTP-Uploads unterstützt, z. B. Microsoft Internet Explorer oder Netscape Navigator. NETGEAR empfiehlt die Verwendung des Internet Explorer oder des Netscape Navigator ab Version 4.0. Kostenlose Browser-Programme werden von Windows, Macintosh und UNIX/Linux zur Verfügung gestellt.

Zur Herstellung der erstmaligen Verbindung zum Internet und für die Konfiguration des Routers ist der Router an einen Computer anzuschließen, an dem die Option für die automatische Übernahme der TCP/IP-Konfiguration vom Router über DHCP aktiviert ist.

Hinweis: Weitere Informationen zur DHCP-Konfiguration finden Sie in Anhang C, "Netzwerk vorbereiten".

Das Kabel- oder DSL-Modem für den Breitbandzugang muss über eine 10 MBit/s-Standard-Ethernet-Schnittstelle (10BASE-T) verfügen.

Voraussetzungen für die Internet-Konfiguration

In Abhängigkeit von der durch Ihren ISP gewählten Konfiguration Ihres Internet-Kontos benötigen Sie einen oder mehrere der nachfolgenden Konfigurationsparameter, um den Router an das Internet anzuschließen:

- Host- und Domain-Name
- ISP-Anmeldename und Kennwort
- ISP-DNS-Adressen (Domain Name Server)
- feste IP-Adresse (wird auch als statische IP-Adresse bezeichnet)

Wo finde ich die Parameter für die Internet-Konfiguration?

Die für den Internet-Anschluss benötigten Informationen können Sie auf unterschiedliche Weise ermitteln.

- Ihr ISP stellt alle Informationen zur Einrichtung einer Internet-Verbindung bereit. Falls Sie diese Informationen nicht finden, können Sie sich mit der Bitte um Zusendung der Daten direkt an Ihren ISP wenden oder sich wie folgt auf die Suche machen.
- Wenn Sie einen Computer besitzen, der bereits über das aktive Internet-Zugangskonto angeschlossen ist, können Sie die Konfigurationsdaten an diesem Computer ermitteln.
 - Windows 95/98/ME: Öffnen Sie das Fenster "Netzwerkverbindungen bzw. Network", wählen Sie den Eintrag TCP/IP für den Ethernet-Adapter aus und klicken Sie auf "Eigenschaften bzw. Properties". Notieren Sie alle Einstellungen auf den verschiedenen Registerkarten.
 - Windows 2000/XP: Öffnen Sie die LAN-Verbindung, wählen Sie den Eintrag TCP/IP für den Ethernet-Adapter aus und klicken Sie auf "Eigenschaften bzw. Properties". Notieren Sie alle Einstellungen auf den verschiedenen Registerkarten.
 - Macintosh-Computers: Öffnen Sie das Fenster "TCP/IP oder Netzwerk bzw. TCP/IP or Network". Notieren Sie alle Einstellungen der verschiedenen Bereiche.
- Auf der *MR814 v2 Ressourcen-CD* zum NETGEAR Router-ISP-Handbuch finden Sie zahlreiche ISP Informationen zum Internet-Anschluss.

Wenn Sie die Parameter für die Konfiguration des Internet-Anschlusses gefunden haben, empfiehlt es sich, diese Daten auf der nachfolgenden Seite einzutragen.

Arbeitsblatt für Angaben zum Internet-Anschluss

Drucken Sie diese Seite aus und tragen Sie die für Ihren ISP gültigen Konfigurationsparameter ein.

ISP-Anmeldename: Achten Sie beim Anmeldenamen und dem Kennwort auf die Groß- und Kleinschreibung und geben Sie diese Daten in exakt der Weise ein, die Ihnen von Ihrem ISP mitgeteilt wurde. Manche ISPs verwenden die vollständige E-Mail-Adresse des Benutzers als Anmeldename. Der Dienstname ist nicht bei allen ISPs erforderlich. Tragen Sie den Anmeldenamen und das Kennwort, den/das Sie für den Internet-Anschluss verwenden, nachfolgend ein:

Anmeldename: _____ Kennwort: _____
Dienstname: _____

Feste oder statische IP-Adresse: Wenn Sie eine statische IP-Adresse besitzen, tragen Sie folgende Angaben ein. Eine gültige IP-Adresse könnte beispielsweise lauten: 169.254.141.148.

Feste oder statische Internet-IP-Adresse: _____ . _____ . _____ . _____

Gateway-IP-Adresse: _____ . _____ . _____ . _____

Subnetzmaske: _____ . _____ . _____ . _____

DNS-Serveradressen des ISP: Falls Ihnen DNS-Serveradressen mitgeteilt wurden, notieren Sie folgende Angaben:

IP-Adresse primärer DNS-Server: _____ . _____ . _____ . _____

IP-Adresse sekundärer DNS-Server: _____ . _____ . _____ . _____

Host- und Domain-Name Einige ISPs verwenden einen speziellen Host- oder Domain-Namen wie **CCA7324-A** oder **home**. Wenn Ihnen der Host- oder Domainname nicht mitgeteilt wurde, können Sie die folgenden Beispiele zur Orientierung verwenden:

- Wenn Ihr E-Mail-Hauptkonto bei Ihrem ISP **aaa@yyy.com** lautet, ist "aaa" der Host-Name. Die verschiedenen ISPs bezeichnen dies auch als Konto, Benutzer-, Host-, Computer- oder Systemname.
- Wenn die Adresse des Mail-Servers Ihres ISP **mail.xxx.yyy.com** lautet, ist **xxx.yyy.com** der Domain-Name.

ISP Host-Name: _____ ISP Domain-Name: _____

Bei drahtlosem Zugang: Notieren Sie folgende Angaben für die Konfiguration des Wireless-Netzwerks:

Name des Wireless-Netzwerks (SSID): _____

Verschlüsselung (einen Modus auswählen): WEP 64, WEP 128 oder IPSec

WEP-Passphrase oder -Code: _____

Kabel-/DSL-Wireless Router, Modell MR814 v2, an das LAN anschließen

In diesem Abschnitt wird beschrieben, wie Sie den Router MR814 v2 anschließen. Außerdem enthält die *Model MR814 v2 Ressourcen-CD*, die im Lieferumfang des Routers enthalten ist, einen Installationsassistenten, der Sie bei diesem Vorgang unterstützt.

Router anschließen

Zum Anschließen des Routers sind drei Schritte auszuführen:

1. Den Router an das Netzwerk anschließen.
2. Beim Router anmelden.
3. Verbindung zum Internet aufbauen.

Führen Sie folgende Schritte aus, um den Router an Ihr Netzwerk anzuschließen. Außerdem finden Sie auf der Ressourcen-CD, die im Lieferumfang des Routers enthalten ist, einen Installationsassistenten, der Sie bei diesem Vorgang unterstützt.

1. Den Router an das Netzwerk anschließen.

- a. Schalten Sie den Computer und das Kabel- oder DSL-Modem aus.
- b. Ziehen Sie das Ethernet-Kabel (A), das die Verbindung zum Kabel- oder DSL-Modem herstellt, am Computer heraus.

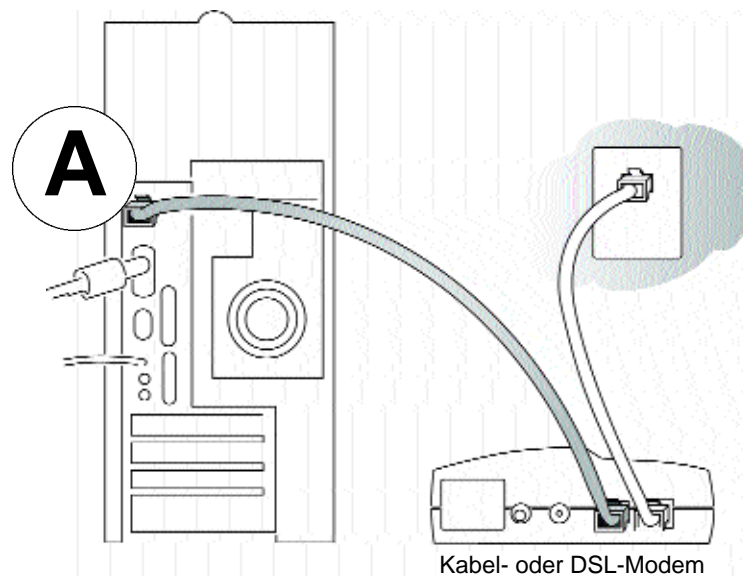


Abbildung 2-1: Kabel zu Kabel- oder DSL-Modem ausstecken

- c. Stecken Sie das vom Kabel- oder DSL-Modem kommende Ethernet-Kabel in den Internet-Anschluss (A) am MR814 v2 ein.

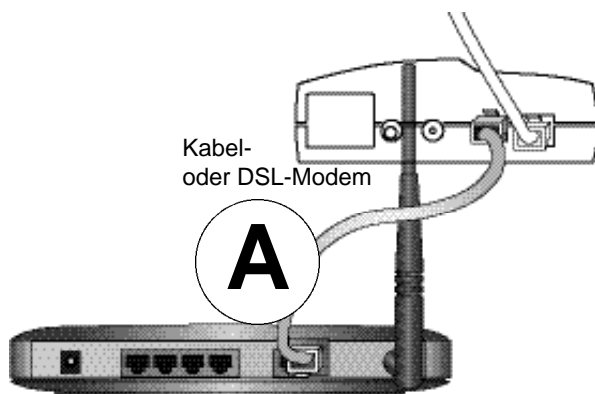


Abbildung 2-2: Kabel- oder DSL-Modem mit dem Router verbinden

- d. Stellen Sie mit Hilfe des mit dem Router gelieferten Ethernet-Kabels eine Verbindung zwischen einem 'Local'-Anschluss am Router (B) und Ihrem Computer her.

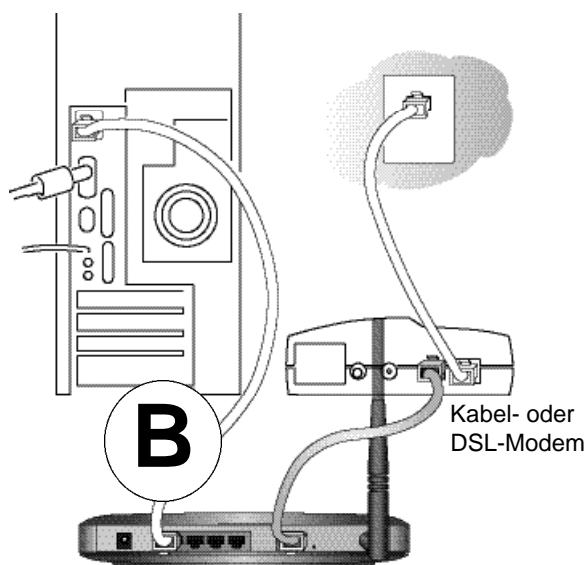


Abbildung 2-3: Verbinden Sie die Computer in Ihrem Netzwerk mit dem Router.

Hinweis:Der Router MR814 v2 verwendet die Auto Uplink™-Technologie. Jeder lokale Ethernet-Port ('Local') erkennt automatisch, ob für das Kabel eine normale Verbindung oder ein Uplink-Verbindung erforderlich ist. Damit können Sie auf die Verwendung eines Crossover-Kabels verzichten, da Auto Uplink in jedem Fall die korrekte Verbindung für den jeweiligen Kabeltyp herstellt.

- e. Schalten Sie jetzt Ihren Computer ein. Wenn Sie normalerweise über eine Software eine Anmeldung für eine Internet-Verbindung vornehmen, führen Sie diese Software jetzt nicht aus bzw. brechen Sie deren Ausführung im Falle eines automatischen Starts ab.

f. Prüfen Sie Folgendes:



Beim Einschalten des Routers leuchtet die Netz-LED auf.



Die Local-LEDs leuchten für alle Computer, die an den Router angeschlossen sind.



Die Internet-LED des Routers leuchtet auf. Daran ist zu erkennen, dass eine Verbindung zum Kabel- oder DSL-Modem hergestellt wurde.

2. Beim Router anmelden.

Hinweis: Damit Ihr Computer eine Verbindung zum Router herstellen kann, muss in der Konfiguration des Computers die Option für den automatischen Empfang einer IP-Adresse über DHCP aktiviert werden. Informationen zur Aktivierung dieser Option finden Sie in Anhang C, "Netzwerk vorbereiten".

- a. Stellen Sie die Verbindung zum Router her, indem Sie *http://192.168.0.1* im Adressfeld des Internet Explorers oder Netscape® Navigators eingeben.

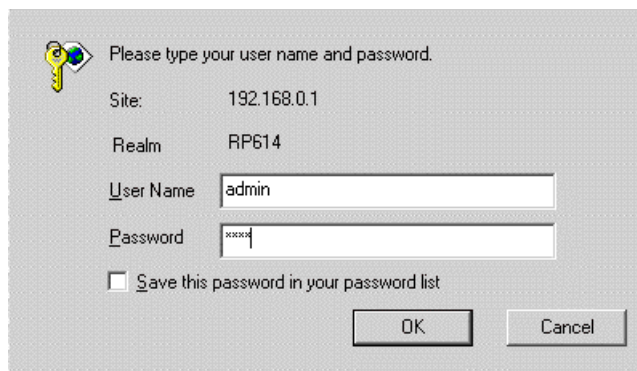


Abbildung 2-4: Beim Router anmelden

- b. Aus Gründen der Sicherheit hat der Router einen eigenen Benutzernamen und ein Kennwort. Geben Sie bei entsprechender Aufforderung als Benutzernamen 'admin' und als Kennwort 'password' (beides in Kleinbuchstaben) ein.

Hinweis: Der Benutzernamen und das Kennwort des Routers sind nicht identisch mit den Angaben, die Sie für die Anmeldung beim Internet verwenden.

Ein Anmeldefenster wie das nachfolgende erscheint:



Please type your user name and password.

Site: 192.168.0.1

Realm: RP614

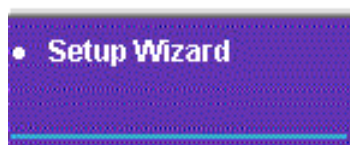
User Name: admin

Password: ****

Save this password in your password list

OK Cancel

Abbildung 2-5: Anmeldefenster



Setup Wizard

System Can Now Detect The Connection Type Of WAN Port, Or You Can Configure It By Yourself.

Do You Want System To Detect The Connection Type?

- Yes.
- No. I Want To Configure By Myself.

Next

3. Verbindung zum Internet aufbauen

Abbildung 2-6: Konfigurationsassistent

- Sie sind jetzt mit dem Router verbunden. Wenn das oben dargestellte Menü nicht angezeigt wird, klicken Sie in der oberen linken Ecke des Hauptmenüs auf den Link "Konfigurationsassistent bzw. Setup Wizard".
- Klicken Sie auf "Weiter bzw. Next" und führen Sie die Schritte aus, die durch den Konfigurationsassistenten vorgegeben werden, um die Konfigurationsparameter Ihres ISP für die Herstellung einer Internet-Verbindung einzugeben.

Hinweis: Wenn Sie den Konfigurationsassistenten nicht verwenden wollen, können Sie die Einstellungen für die Internet-Verbindung auch manuell konfigurieren; die dabei erforderliche Vorgehensweise wird unter "Manuelle Konfiguration der Internet-Verbindung" auf Seite 2-16 beschrieben.

Wenn Ihnen Ihre Konfiguration von Ihrem ISP nicht automatisch über DHCP zugewiesen wurde, benötigen Sie nun die Konfigurationsparameter Ihres ISP, die Sie zuvor auf dem "Arbeitsblatt für Angaben zum Internet-Anschluss" auf Seite 2-3 notiert haben.

- c. Wenn der Router einen aktiven Internet-Dienst entdeckt, leuchtet die Internet-LED des Routers. Im Konfigurationsassistenten wird der festgestellte Verbindungstyp angezeigt; daraufhin erscheint das entsprechende Konfigurationsmenü. Falls der Konfigurationsassistent keine Verbindung findet, werden Sie aufgefordert, die physikalische Verbindung zwischen dem Router und dem Kabel- oder DSL-Anschluss zu überprüfen.
- d. Der Konfigurationsassistent zeigt die Verbindungstypen an, die gefunden wurden. Dabei kann es sich um folgende Verbindungstypen handeln:
 - Verbindungen, für die eine protokollgestützte Anmeldung erforderlich ist, z. B. PPPoE- oder PPTP-Breitbandverbindungen
 - Verbindungen mit dynamischer IP-Adresszuordnung
 - Verbindungen mit statischer IP-Adresszuordnung

Wie Sie das Konfigurationsmenü für die einzelnen Verbindungstypen ausfüllen, wird nachfolgend beschrieben.

Erkennung von PPPoE durch den Assistenten

Wenn der Konfigurationsassistent feststellt, dass Ihr ISP PPPoE verwendet, wird das folgende Menü angezeigt:

The screenshot shows a configuration window for PPPoE. It has a title bar with 'PPPoE' in blue. Below the title bar are four input fields: 'Login', 'Password', 'Service Name (If Required)', and 'Idle Timeout' (with a value of 5). Below these is a section for 'Domain Name Server (DNS) Address' with two radio buttons: 'Get automatically from ISP' (selected) and 'Use these DNS servers'. Under 'Use these DNS servers' are two rows of IP address input fields: 'Primary DNS' and 'Secondary DNS', both showing '0.0.0.0'. At the bottom are three buttons: 'Apply', 'Cancel', and 'Test'.

Abbildung 2-7: Konfigurationsmenü für PPPoE-Konten

- Geben Sie für den “Kontennamen bzw. Account Name”, den “Domain-Namen bzw. Domain Name”, den “Anmeldenamen bzw. Login” und das “Kennwort bzw. Passwort” die Angaben ein, die Sie von Ihrem ISP erhalten haben. Bei der Eingabe in diesen Felder ist die Groß- und Kleinschreibung zu beachten. Unter Umständen kann der Router die Domäne automatisch ermitteln, wenn Sie keinen Domain-Namen eingeben. Andernfalls müssen Sie diesen Namen manuell eingeben.

- Für den Parameter “Abmeldung nach bzw. Login Timeout” können Sie einen neuen Wert in Minuten eingeben. Dieser Parameter bestimmt, wie lange die Internet-Verbindung gehalten wird, wenn von dem LAN keine Internet-Aktivität ausgeht. Bei Eingabe des Werts Null (“0”) wird die Verbindung permanent gehalten.

Hinweis: Das Anmeldeprogramm Ihres ISPs, das sich auf Ihrem PC befindet, müssen Sie ab jetzt nicht mehr ausführen, um in das Internet zu gelangen. Wenn Sie eine Internet-Anwendung starten, führt der Router die Anmeldung automatisch aus.

- Wenn Sie wissen, dass Ihr ISP die DNS-Adressen während der Anmeldung nicht automatisch an den Router überträgt, wählen Sie “Diese DNS-Server verwenden bzw. Use these DNS servers” aus und geben Sie für “Primary DNS” die IP-Adresse des primären DNS-Servers Ihres ISP ein. Falls auch die Adresse eines sekundären DNS-Servers verfügbar ist, geben Sie diese unter “Secondary DNS” ein.

Hinweis: Starten Sie Ihre Computer nach Eingaben der DNS-Adressen neu, damit diese Einstellungen wirksam werden.

- Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern
- Überprüfen Sie, ob Ihre Internet-Verbindung funktioniert. Falls die Website von NETGEAR nicht innerhalb einer Minute angezeigt wird, lesen Sie bitte in Kapitel 7, “Fehlerbehebung”, nach.

Erkennung der dynamischen IP durch den Assistenten

Wenn der Konfigurationsassistent feststellt, dass Ihr ISP die dynamische IP-Zuordnung verwendet, wird das folgende Menü angezeigt:

The screenshot shows a web form titled "Dynamic IP". It contains the following fields and options:

- Account Name** (If Required): A text input field.
- Domain Name** (If Required): A text input field.
- Domain Name Server (DNS) Address**: A section with two radio buttons:
 - Get Automatically From ISP
 - Use These DNS Servers
- Primary DNS**: A four-digit IP address input field (0.0.0.0).
- Secondary DNS**: A four-digit IP address input field (0.0.0.0).
- At the bottom, there are three buttons: **Apply**, **Cancel**, and **Test**.

Abbildung 2-14: Konfigurationsmenü für Konten mit dynamischer IP-Adresse

- Geben Sie Ihren Kontennamen unter “Account Name” (hier kann auch “Host Name” stehen) und den Domain-Namen ein. Diese Parameter sind unter Umständen erforderlich, wenn Sie auf Dienste Ihres ISP wie Mail- oder Nachrichten-Server zugreifen wollen. Wenn Sie keinen Domain-Namen eingeben, versucht der Router, die Domäne automatisch zu ermitteln. Andernfalls müssen Sie diesen Namen manuell eingeben.
- Wenn Sie wissen, dass Ihr ISP die DNS-Adressen während der Anmeldung nicht automatisch an den Router überträgt, wählen Sie “Diese DNS-Server verwenden bzw. Use these DNS servers” aus und geben Sie für “Primary DNS” die IP-Adresse des primären DNS-Servers Ihres ISP ein. Falls auch die Adresse eines sekundären DNS-Servers verfügbar ist, geben Sie diese unter “Secondary DNS” ein.

Hinweis: Starten Sie Ihre Computer nach Eingabe der DNS-Adressen neu, damit diese Einstellungen wirksam werden.

- Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern.
- Klicken Sie auf “Überprüfen bzw. Test”, um Ihre Internet-Verbindung zu überprüfen. Falls die Website von NETGEAR nicht innerhalb einer Minute angezeigt wird, lesen Sie bitte in Kapitel 6, “Fehlerbehebung”, nach.

Erkennung der statischen IP durch den Assistenten

Wenn der Konfigurationsassistent feststellt, dass Ihr ISP die statische IP-Zuordnung verwendet, wird das folgende Menü angezeigt:

Fixed IP

Internet IP Address

IP Address 0 . 0 . 0 . 0

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Apply Cancel Test

Abbildung 2-15: Konfigurationsmenü für Konten mit statischer IP-Adresse

- Die statische IP wird manchmal auch als feste IP bzw. “Fixed IP” bezeichnet. Geben Sie die Ihnen zugewiesene IP-Adresse bzw. “IPAddress”, die Subnetzmaske bzw. “Subnet Mask” und die IP-Adresse bzw. “IP-Address” des Gateway-Routers Ihres ISP ein. Diese Angaben sollten Sie von Ihrem ISP erhalten haben. Außerdem benötigen Sie die Konfigurationsparameter Ihres ISP, die Sie auf dem “Arbeitsblatt für Angaben zum Internet-Anschluss” auf Seite 2-3 notiert haben.
- Geben Sie die IP-Adresse des primären und des sekundären DNS-Servers Ihres ISP unter “Primary DNS” und “Secondary DNS” ein.

Hinweis: Starten Sie die Computer im Netzwerk nach Eingaben der DNS-Adressen neu, damit diese Einstellungen wirksam werden.

- Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern.
- Klicken Sie auf “Überprüfen bzw. Test”, um Ihre Internet-Verbindung zu überprüfen. Falls die Website von NETGEAR nicht innerhalb einer Minute angezeigt wird, lesen Sie bitte in Kapitel 7, “Fehlerbehebung”, nach.

Manuelle Konfiguration der Internet-Verbindung

Sie können Ihren Router mit Hilfe des nachfolgenden Menüs manuell konfigurieren oder die Konfiguration durch den Konfigurationsassistenten vornehmen lassen (wie im vorherigen Abschnitt beschrieben).

Keine Anmeldung bei ISP erforderlich

Basic Settings

Does Your Internet Connection Require A Login?

Yes

No

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Router MAC Address

Use Default MAC Address

Use Computer MAC Address

Use This MAC Address

Apply Cancel Test

Anmeldung bei ISP erforderlich

Basic Settings

Does Your Internet Connection Require A Login?

Yes

No

Internet Service Provider

Login

Password

Service Name (If Required)

Idle Timeout (In Minutes)

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Apply Cancel Test

Abbildung 2-16: Menüs "Grundeinstellungen bzw. Basic Settings" für Browser-gestützte Konfiguration

Vorgehensweise: Manuelle Konfiguration der Internet-Verbindung

In dem Menü “Grundeinstellungen bzw. Basic Settings”, das in Abbildung 2-16 dargestellt ist, können Sie den Router mit folgenden drei Schritten manuell konfigurieren:

1. Klicken Sie im Menü “Konfiguration bzw. Setup” auf den Link “Grundeinstellungen bzw. Basic Settings”.
2. Falls für die Herstellung einer Internet-Verbindung keine Anmeldung erforderlich ist, klicken Sie bei der ersten Frage des Menüs “Grundeinstellungen bzw. Basic Settings” (“Anmeldung für Internet-Verbindung erforderlich? bzw. Does Your Internet Connection Require A Login”) auf “Nein bzw. No” und legen Sie die Einstellungen entsprechend der nachfolgenden Anweisungen fest. Wenn für die Herstellung einer Internet-Verbindung eine Anmeldung erforderlich ist, klicken Sie auf “Ja bzw. Yes” und fahren Sie mit dem 3. Schritt fort.
 - a. Geben Sie Ihren Kontennamen unter “Account Name” (hier kann auch “Host Name” stehen) und den Domain-Namen ein. Diese Parameter sind unter Umständen erforderlich, wenn Sie auf Dienste Ihres ISP wie Mail- oder Nachrichten-Server zugreifen wollen.
 - b. Internet-IP-Adresse bzw. Internet IP Address: Wenn Ihnen von Ihrem ISP eine permanente, feste (oder statische) IP-Adresse für Ihren PC zugewiesen wurde, wählen Sie “Statische IP-Adresse verwenden bzw. Use static IP address” aus. Geben Sie die IP-Adresse ein, die Ihnen von Ihrem ISP zugewiesen wurde. Geben Sie außerdem die Netzmaske und die Gateway-IP-Adresse ein. Der Gateway ist der Router des ISP, zu dem Ihr Router eine Verbindung herstellt.
 - c. DNS-Adresse bzw. Domain Name Server (DNS) Address: Wenn Sie wissen, dass Ihr ISP die DNS-Adressen während der Anmeldung nicht automatisch an den Router überträgt, wählen Sie “Diese DNS-Server verwenden bzw. Use these DNS servers” aus und geben Sie für “Primary DNS” die IP-Adresse des primären DNS-Servers Ihres ISP ein. Falls auch die Adresse eines sekundären DNS-Servers verfügbar ist, geben Sie diese unter “Secondary DNS” ein.

Hinweis: Starten Sie Ihre Computer nach Eingabe der DNS-Adressen neu, damit diese Einstellungen wirksam werden.

- d. MAC-Adresse des Routers bzw. Router MAC Address: In diesem Bereich wird die Ethernet-MAC-Adresse festgelegt, die an dem Internet-Anschluss von dem Router verwendet wird. Manche ISPs registrieren beim erstmaligen Öffnen Ihres Kontos die Ethernet-MAC-Adresse der Netzwerkschnittstellenkarte Ihres PCs. Dann werden nur Datenübertragungen von der MAC-Adresse des betreffenden PCs angenommen. Mit dieser Funktion wird Ihr Router als dieser betreffende PC dargestellt.

Wenn Sie die MAC-Adresse ändern wollen, wählen Sie “MAC-Adresse des Computers verwenden bzw. Use Computer MAC address” aus. Daraufhin erfasst und verwendet der Router die MAC-Adresse des PCs, den Sie zum betreffenden Zeitpunkt benutzen. Danach müssen Sie immer den PC verwenden, der durch den ISP freigegeben ist, oder “Diese MAC-Adresse verwenden bzw. Use this MAC address” auswählen und eine andere Adresse eingeben.

- e. Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern.

3. Wenn für Ihre Internet-Verbindung eine Anmeldung erforderlich ist, legen Sie die Einstellungen entsprechend der nachfolgenden Anweisungen fest. Wählen Sie “Ja bzw. Yes” aus, wenn Sie normalerweise ein Anmeldeprogramm wie Enternet oder WinPOET starten müssen, um in das Internet zu gelangen.

Hinweis: Nach Abschluss der Konfiguration Ihres Routers müssen Sie das Anmeldeprogramm Ihres ISPs, das sich auf Ihrem PC befindet, nicht mehr ausführen, um in das Internet zu gelangen. Wenn Sie eine Internet-Anwendung starten, führt der Router die Anmeldung automatisch aus.

- a. Wählen Sie in der Dropdown-Liste Ihren Internet Service Provider aus.

Basic Settings

The screenshot shows the 'Basic Settings' configuration page. At the top, there is a section titled 'Does Your Internet Connection Require A Login?' with two radio buttons: 'Yes' (which is selected) and 'No'. Below this, there is a section for 'Internet Service Provider' with a dropdown menu. The dropdown menu is open, showing two options: 'Other' and 'Austria (PPTP)'. To the left of the dropdown menu, there are two input fields labeled 'Login' and 'Password'.

Abbildung 2-17: ISP-Liste in “Grundeinstellungen bzw. Basic Settings”

- b. Das Fenster wird entsprechend der erforderlichen ISP-Einstellungen des ISP aktualisiert, den Sie ausgewählt haben.
- c. Geben Sie die Parameter für Ihren ISP entsprechend der durch den Konfigurationsassistenten unterstützten Vorgehensweise ab Seite 2-9 ein.
- d. Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern.

Kapitel 3

Wireless-Konfiguration

In diesem Kapitel wird die Vorgehensweise bei der Konfiguration der Wireless-Funktionen Ihres Routers MR814 v2 erläutert.

Hinweise zu Wireless-Netzwerken

Bei der Planung Ihres Wireless-Netzwerks sollten Sie die erforderliche Sicherheitsstufe beachten. Daneben sollten Sie den physikalischen Standort Ihrer Firewall im Hinblick auf eine Maximierung der Netzwerkgeschwindigkeit festlegen. Weitere Informationen zu Wireless-Netzwerken finden Sie in Anhang D, "Basisinformationen zu Wireless-Netzwerken".

Hinweise zur Leistung, Platzierung und Reichweite

Die Reichweite Ihrer Wireless Verbindung kann in Abhängigkeit vom physikalischen Standort Ihres Wireless Routers beträchtlich variieren. Daneben sind die Latenzzeit, der Datendurchsatz und der Stromverbrauch von Notebooks von den gewählten Konfigurationseinstellungen abhängig.



Hinweis: Eine Nicht-Beachtung der vorliegenden Richtlinien kann zu einem deutlichen Abfall der Leistung oder zu einem Fehlschlag bei dem Versuch, eine Wireless Verbindung zu Ihrem Router herzustellen, führen. Eine vollständige Aufstellung der Daten zur Reichweite und Leistung finden Sie in Anhang A, "Technische Daten".

Die besten Ergebnisse erzielen Sie, wenn Sie Ihren Wireless Router wie folgt platzieren:

- In der Nähe des Mittelpunkts des Bereichs, in dem Ihre PCs betrieben werden.
- An einer erhöhten Stelle, z. B. auf einem Regal, von der aus eine direkte, ungehinderte Verbindung zu den drahtlos angeschlossenen PCs besteht (selbst wenn dazwischen noch Wände liegen).
- Abseits möglicher Störungsquellen wie PCs, Mikrowellengeräte und schnurloser Telefone mit 2,4 GHz.
- Abseits großer Metalloberflächen.

Die Zeit, bis eine Wireless Verbindung hergestellt wurde, kann entsprechend der gewählten Sicherheitseinstellungen und des Standorts variieren. Die Herstellung von WEP-Verbindungen dauert etwas länger. Daneben kann die WEP-Verschlüsselung auf einem Notebook zu einem erhöhten Batterie- bzw. Akkuverbrauch führen.

Geeignete Wireless-Sicherheit einrichten



Hinweis: In geschlossenen Räumen können Computer bis zu einem maximalen Abstand von 150 Metern eine Verbindung zu einem Wireless-Netzwerk 802.11b herstellen. Bei diesen Reichweiten besteht die Gefahr, dass auch andere Benutzer außerhalb Ihres direkten Arbeitsbereich auf Ihr Netzwerk zugreifen können.

Im Gegensatz zur Übertragung von Daten über leitungsgestützte Verbindungen können drahtlose Datenübertragungen die Wände Ihrer Büroräume durchdringen und von anderen Benutzern empfangen werden, die einen geeigneten Adapter besitzen. Aus diesem Grund sollten Sie die Sicherheitsfunktionen Ihrer Wireless-Geräte nutzen. Der Router MR814 v2 bietet ausgesprochen wirksame Sicherheitsfunktionen, die in diesem Kapitel ausführlich beschrieben werden. Setzen Sie diese Sicherheitsfunktionen entsprechend Ihrer spezifischen Anforderungen ein.

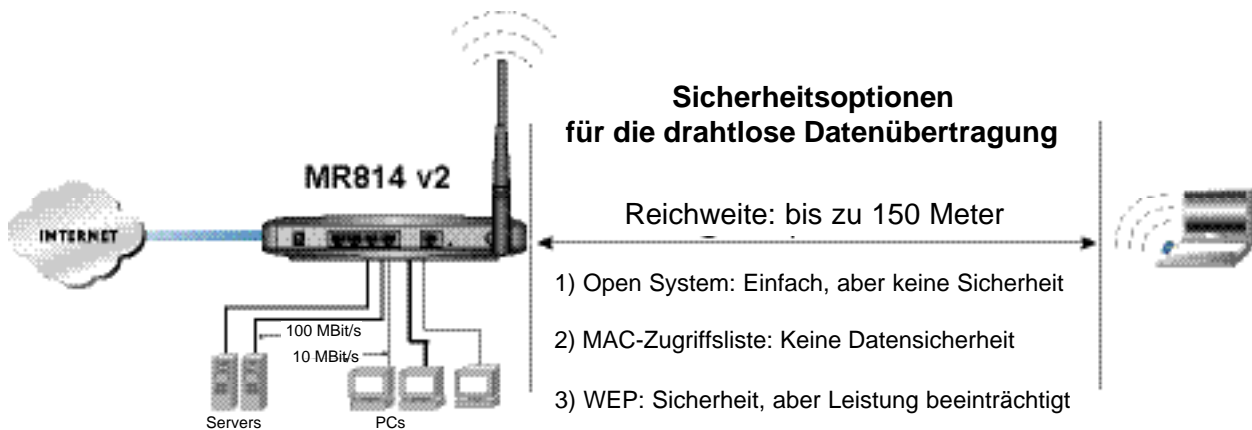
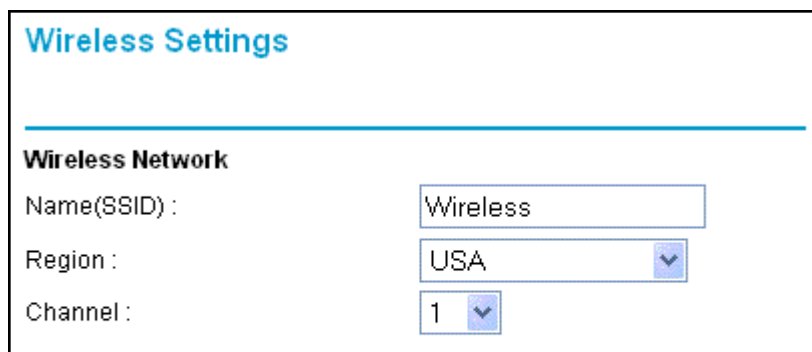


Abbildung 3-1: Sicherheitsoptionen des Routers MR814 v2 für die drahtlose Datenübertragung

Die Beschränkung des Zugriffs durch einen MAC-Adressfilter liefert einen zusätzlichen Schutz gegen unerwünschte Netzwerkzugriffe, doch die Datenversendung über die drahtlose Verbindung bleibt dabei vollständig ungeschützt. Um einen hartnäckigen Lauschangriff abzuwehren, sollten Sie eine der Datenverschlüsselungsoptionen der Firewall verwenden. Die WEP-Datenverschlüsselung (Wired Equivalent Privacy) bietet einen geeigneten Datenschutz.

Bedeutung der Wireless-Einstellungen

Klicken Sie zur Konfiguration der Wireless-Einstellungen Ihrer Firewall im Hauptmenü der Browser-Schnittstelle auf den Link "Wireless". Daraufhin erscheint das nachfolgend abgebildete Menü "Wireless-Einstellungen bzw. Wireless Settings".



The image shows a screenshot of the 'Wireless Settings' menu. At the top, the title 'Wireless Settings' is displayed in blue. Below the title, there is a section header 'Wireless Network'. Under this header, there are three configuration fields: 'Name(SSID):' with a text input field containing 'Wireless', 'Region:' with a dropdown menu showing 'USA', and 'Channel:' with a dropdown menu showing '1'.

Abbildung 3-2: Menü “Wireless-Einstellungen bzw. Wireless Settings”

Einstellungen für das Wireless-Netzwerk

Die verschiedenen Bereiche des Menüs “Wireless-Einstellungen bzw. Wireless Settings” werden nachfolgend erläutert.

- Name (SSID). Die Service Set Identification wird auch als Name des Wireless-Netzwerks bezeichnet. Geben Sie einen aus bis zu 32 alphanumerischen Zeichen bestehenden Wert ein. In einem Umfeld, in dem mehrere Wireless-Netzwerke verwendet werden, bieten unterschiedliche Bezeichnungen der Wireless-Netzwerke eine Möglichkeit zur Trennung des Datenverkehrs. Jegliches Gerät, das an dieses Wireless Netz angebunden werden soll, muss diese SSID verwenden. Die Standard-SSID des Routers MR814 v2 lautet: Wireless.
- Region. Dieses Feld bezeichnet die Region, in der der Router MR814 v2 verwendet werden darf. Unter Umständen ist es gesetzlich verboten, die Wireless-Funktionen eines Routers außerhalb der in dieser Dropdown-Liste aufgeführten Regionen zu verwenden.
- Kanal bzw. Channel. In diesem Feld wird die zu verwendende Betriebsfrequenz festgelegt. Der Kanal für die drahtlose Datenübertragung muss in der Regel nur geändert werden, wenn Interferenzen mit anderen Access Points in der näheren Umgebung auftreten. Weitere Informationen zu den Frequenzen des Wireless-Kanals finden Sie unter “Wireless-Kanäle” auf Seite D-7.

Wireless-Zugriff auf das Netzwerk einschränken

Der Kabel-/DSL-Wireless-Router Modell MR814 v2 bietet verschiedene Möglichkeiten zur Einschränkung des Wireless-Zugriffs auf Ihr Netzwerk:

- Die Wireless-Konnektivität vollständig ausschalten.
- Die Zugriffsmöglichkeiten auf der Grundlage des Namens des Wireless-Netzwerks (SSID) einschränken.
- Die Zugriffsmöglichkeiten auf der Grundlage der Zugriffsliste der Wireless-Karte einschränken. Diese Optionen werden nachfolgend erläutert.

Zugriff auf das Netzwerk durch Deaktivierung der Wireless-Konnektivität einschränken

Sie können den Wireless-Teil des Routers MR814 v2 vollständig ausschalten. Wenn beispielsweise Ihr Notebook normalerweise über eine drahtlose Verbindung auf Ihren Router zugreift und Sie sich auf eine Geschäftsreise begeben, können Sie den Wireless-Teils des Routers während der Geschäftsreise ausschalten. Andere Mitglieder Ihres Haushalts, deren Computer über Ethernet-Kabel mit dem Router verbunden sind, können den Router weiterhin benutzen.

Drahtlosen Zugriff über den Namen des Wireless-Netzwerks (SSID) einschränken

Der Router MR814 v2 kann den drahtlosen Zugriff auf Ihr Netzwerk einschränken, indem der Name des Wireless-Netzwerks (SSID) in Rundsendungen nicht genannt wird. Diese Funktion ist jedoch standardmäßig ausgeschaltet. Wenn Sie diese Funktion einschalten, kann kein Wireless Gerät Ihren Router MR814 v2 "sehen" oder erkennen. In diesem Fall müssen Sie bei der Konfiguration Ihrer eigenen Wireless Geräte denselben Namen des Wireless-Netzwerks (SSID) eingeben, den Sie auch für den Router MR814 v2 festgelegt haben.

Hinweis: Die SSID aller Adapter für den drahtlosen Zugriff muss der SSID entsprechen, die Sie in der Konfiguration des Kabel-/DSL-Wireless-Routers Modell MR814 v2 definiert haben. Falls dies nicht der Fall ist, können die betreffenden Geräte keine drahtlose Verbindung zu dem Router MR814 v2 aufbauen.

Drahtlosen Zugriff über die Wireless-Zugriffsliste einschränken

In dieser Liste wird festgelegt, welche Hardware-Geräte eine Verbindung zu der Firewall aufbauen dürfen.

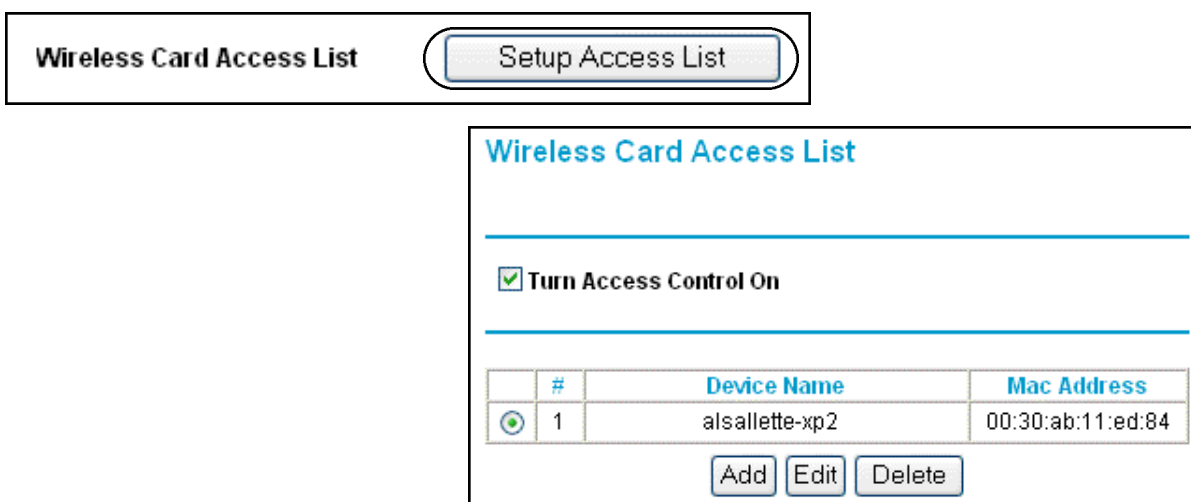


Abbildung 3-3: Konfiguration der Zugriffsliste für die Wireless-Karte

- Klicken Sie auf die Schaltfläche “Zugriffsliste konfigurieren bzw. Setup Access List”, um diese Funktion zu aktivieren.
- Wählen Sie das Markierungsfeld “Zugriffskontrolle einschalten bzw. Turn Access Control On” aus.
- Wählen Sie dann in der Liste der verfügbaren Wireless-Karten, die der Router MR814 v2 in Ihrem Bereich gefunden hat, die gewünschten Geräte aus, oder geben Sie die MAC-Adresse und den Gerätenamen des Geräts ein, das Sie verwenden wollen. Die MAC-Adresse ist normalerweise auf dem Wireless-Adapter angebracht.

Nun können nur die Geräte, die in dieser Liste aufgeführt sind, eine drahtlose Verbindung zu dem Router MR814 v2 aufbauen.

Methoden für die Authentifizierung und die Sicherheitsverschlüsselung auswählen

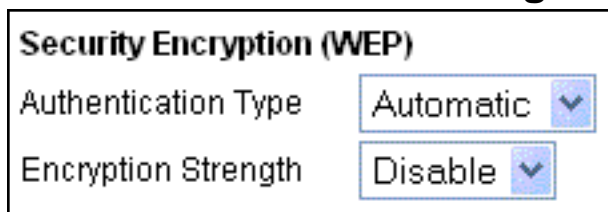


Abbildung 3-4: Verschlüsselungsmodus

Durch Einschränkung des drahtlosen Zugriffs auf Ihr Netzwerk können Sie verhindern, dass Eindringlinge eine Verbindung zu Ihrem Netzwerk aufbauen. Allerdings sind die drahtlosen Datenübertragungen dennoch gegenüber Lauschangriffen gefährdet. Mit Hilfe der nachfolgend beschriebenen Einstellungen für die WEP-Datenverschlüsselung können auch hartnäckige Lauschangriffe auf Ihre drahtlose Datenkommunikation abgewehrt werden. Internet-Seiten, über die Einkäufe oder Bankgeschäfte getätigt werden können, verwenden darüber hinaus eine weitere, besonders sichere Verschlüsselungsmethode namens SSL. Eine Website, die diese SSL-Verschlüsselung verwendet, können Sie daran erkennen, dass die Internet-Adresse nicht mit HTTP, sondern mit HTTPS beginnt.

Authentifizierungssystem auswählen

Mit dem Router MR814 v2 stehen Ihnen folgende Authentifizierungssysteme für die drahtlose Datenübertragung zur Verfügung:

- Automatisch
- Open System
- Shared Key



Hinweis: Das Authentifizierungssystem und die Datenverschlüsselung sind zwei verschiedene Einrichtungen. Sie können ein Authentifizierungssystem auswählen, das einen gemeinsamen Schlüssel (Shared Key) verwendet, und die Daten dennoch unverschlüsselt übertragen. Wenn Sie ein hohes Maß an Sicherheit wünschen, wählen Sie die Option Shared Key in Kombination mit der WEP-Verschlüsselung aus.

Konfigurieren Sie Ihren Wireless-Adapter entsprechend dem Authentifizierungssystem, das Sie für den Router MR814 v2 ausgewählt haben. Eine vollständige Erläuterung dieser Optionen entsprechend der Definition in der IEEE-Norm 802.11b für die drahtlose Datenübertragung finden Sie unter “Authentifizierung und WEP” auf Seite D-3.

Verschlüsselungsmodus auswählen

Wählen Sie in der Dropdown-Liste den gewünschten Verschlüsselungsmodus aus. Eine vollständige Erläuterung dieser Optionen entsprechend der Definition in der IEEE-Norm 802.11b für die drahtlose Datenübertragung finden Sie unter “Übersicht der WEP-Parameter” auf Seite D-5.

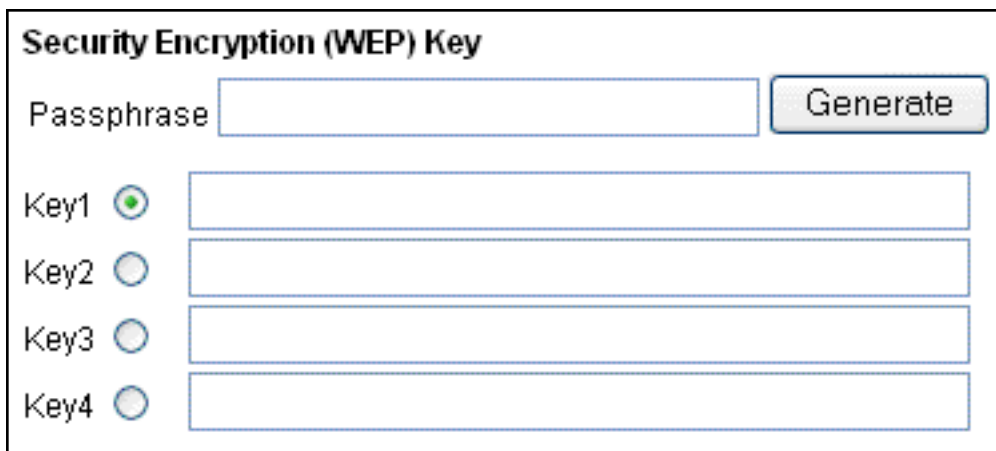
Deaktivieren bzw. Disable

Keine Verschlüsselung. Diese Einstellung ist bei der Fehlersuche und -behebung einer drahtlosen Verbindung nützlich, bietet aber keinerlei Schutz für Ihre drahtlos übertragenen Daten.

WEP mit 64 oder 128 Bit bzw. 64 or 128 bit WEP

Bei Auswahl von “WEP mit 64 oder 128 Bit bzw. 64 Bit WEP or 128 Bit WEP” wird die WEP-Verschlüsselung angewendet.

WEP bietet eine einfache Schutzfunktion. Wenn WEP aktiviert wurde, können Sie die vier Datenverschlüsselungscodes manuell oder automatisch programmieren. Diese Werte müssen auf allen PCs und Access Points im Netzwerk identisch sein.



The image shows a web interface for configuring WEP keys. The title is "Security Encryption (WEP) Key". There is a "Passphrase" input field and a "Generate" button. Below this, there are four radio buttons labeled "Key1", "Key2", "Key3", and "Key4", each followed by an empty input field. The "Key1" radio button is selected.

Abbildung 3-5: Verschlüsselungsmodus “WEP mit 64 oder 128 Bit bzw. 64 or 128 bit WEP”

Zur Erzeugung von WEP-Verschlüsselungscodes stehen zwei Möglichkeiten zur Auswahl:

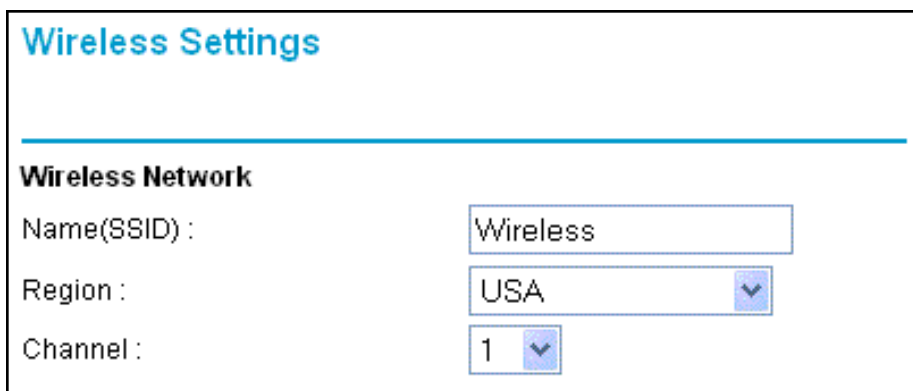
- Passphrase. Geben Sie in dem Feld “Passphrase” ein Wort oder eine Gruppe druckbarer Zeichen ein und klicken Sie auf die Schaltfläche “Erzeugen bzw. Generate”.
- Manuell. 64-Bit-WEP: Geben Sie zehn hexadezimale Zeichen (beliebige Kombination aus 0-9, a-f und A-F) ein. 128-Bit-WEP: Geben Sie 26 hexadezimale Zeichen (beliebige Kombination aus 0-9, a-f und A-F) ein.

Durch Anklicken einer der Punkte wählen Sie den jeweils zu aktivierenden Code aus.

Vorgehensweise 3-1: Grundeinstellungen der Wireless-Konnektivität konfigurieren und testen

Gehen Sie wie folgt vor, um die Grundeinstellungen der Wireless-Konnektivität zu konfigurieren und zu testen. Nachdem Sie die grundsätzliche Wireless-Konnektivität eingerichtet haben, können Sie die Sicherheitseinstellungen entsprechend Ihrer spezifischen Anforderungen aktivieren.

1. Melden Sie sich bei dem Wireless-Router von MR814 v2 unter der Standard-LAN-Adresse <http://192.168.0.1> mit dem Standard-Benutzernamen “admin” und dem Standardkennwort “password” an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem zugehörigen Kennwort.
2. Klicken Sie im Hauptmenü des Wireless-Routers MR814 v2 auf den Link “Wireless-Einstellungen bzw. Wireless Settings”.



The screenshot shows the 'Wireless Settings' page. Under the heading 'Wireless Network', there are three configuration options: 'Name(SSID):' with a text box containing 'Wireless', 'Region:' with a dropdown menu set to 'USA', and 'Channel:' with a dropdown menu set to '1'.

Abbildung 3-6: Menü “Wireless-Einstellungen bzw. Wireless Settings”

3. Wählen Sie einen geeigneten, nachvollziehbaren Namen für das Wireless-Netzwerk (SSID) aus. Geben hierzu in dem Feld “Name (SSID)” einen aus bis zu 32 alphanumerischen Zeichen bestehenden Wert ein. Die Standard-SSID lautet “Wireless”.

Hinweis:Die SSID aller Adapter für den drahtlosen Zugriff muss der SSID entsprechen, die Sie in der Konfiguration des Kabel-/DSL-Wireless-Routers Modell MR814 v2 definiert haben. Falls dies nicht der Fall ist, können die betreffenden Geräte keine drahtlose Verbindung zu dem Router MR814 v2 aufbauen.

4. Wählen Sie die Region aus. Dabei ist die Region auszuwählen, in der die Wireless-Schnittstelle betrieben werden soll.

5. Wählen Sie den “Kanal bzw. Channel” aus. Der Standardkanal ist 6.
In diesem Feld wird die zu verwendende Betriebsfrequenz festgelegt. Der Kanal für die drahtlose Datenübertragung muss in der Regel nur geändert werden, wenn Interferenzen mit anderen Wireless-Routern oder Access Points in der näheren Umgebung auftreten. Wählen Sie einen Kanal aus, der von keinem anderen Wireless-Netzwerk in einem Umkreis von mehreren hundert Metern um Ihren Wireless-Router verwendet wird. Weitere Informationen zu den Frequenzen des Wireless-Kanals finden Sie unter “Wireless-Kanäle” auf Seite D-7.
6. Übernehmen Sie für die erstmalige Konfiguration und Prüfung in der Zugriffsliste der Wireless-Karte die Einstellung “Alle bzw. Everyone” und den Verschlüsselungsmodus “Deaktivieren bzw. Disabled.”
7. Klicken Sie auf “Anwenden bzw. Apply”, um die Änderungen zu speichern.
8. Konfigurieren und testen Sie Ihre PCs hinsichtlich der Wireless-Konnektivität.

Legen Sie an dem Wireless-Adapter der PCs dieselbe SSID und denselben Kanal wie an dem Router fest. Vergewissern Sie sich, dass die PCs über eine drahtlose Verbindung verfügen und in der Lage sind, eine IP-Adresse per DHCP von dem Wireless-Router entgegenzunehmen.



Hinweis: Wenn Sie die Sicherheitseinstellungen der Wireless-Verbindung an einem Wireless-PC konfigurieren und die SSID, den Kanal oder die Sicherheitseinstellungen der Wireless-Verbindung ändern, wird die drahtlose Verbindung bei Anklicken von “Anwenden bzw. Apply” beendet. In diesem Fall müssen Sie an Ihrem PC dieselben neuen Wireless-Einstellungen wie an Ihrem Wireless-Router vornehmen.

Nachdem die PCs über die grundsätzliche Wireless-Konnektivität zu dem Wireless-Router verfügen, können Sie die erweiterten Wireless-Sicherheitseinstellungen des Wireless-Router konfigurieren.

Vorgehensweise 3-2: Wireless-Zugang über MAC-Adresse einschränken

Gehen Sie wie folgt vor, um den Zugriff auf der Grundlage der MAC-Adressen einzuschränken:

1. Melden Sie sich bei dem Wireless-Router von MR814 v2 unter der Standard-LAN-Adresse <http://192.168.0.1> mit dem Standard- Benutzernamen “admin” und dem Standardkennwort “password” an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem zugehörigen Kennwort.
2. Klicken Sie im Hauptmenü des Wireless-Routers MR814 v2 auf den Link “Wireless-Einstellungen bzw. Wireless Settings”.

3. Klicken Sie im Menü “Wireless-Einstellungen bzw. Wireless Settings” auf die Schaltfläche “Zugriffsliste konfigurieren bzw. Setup Access List”, um das nachfolgend abgebildete Menü “Wireless-Zugang bzw. Wireless Access” zu öffnen.

Abbildung 3-7. Menü “Wireless-Zugang bzw. Wireless Access”

4. Klicken Sie auf “Hinzufügen bzw. Add”, um der Zugriffsliste für Wireless-Geräte ein drahtloses Gerät hinzuzufügen. Die Liste “Verfügbare Wireless-Karten bzw. Available Wireless Cards” wird angezeigt.

Abbildung 3-8. Menü “Wireless-Zugang bzw. Wireless Access”

5. Klicken Sie auf den Punkt neben einem Gerät in der Liste und anschließend auf die Schaltfläche “Hinzufügen bzw. Add”, um dieses Gerät der Liste hinzuzufügen.

Hinweis: Sie können die MAC-Adressen aus dem Menü “Angeschlossene Geräte bzw. Attached Devices” des Wireless-Routers in den Zwischenspeicher kopieren und in das Feld “MAC-Adresse bzw. MAC Address” in diesem Menü einfügen. Konfigurieren Sie zu diesem Zweck jeden Wireless-PC so, dass er eine drahtlose Verbindung zu dem Wireless-Router aufbauen kann. Dann sollte der PC in dem Menü “Angeschlossene Geräte bzw. Attached Devices” aufgeführt werden.

6. Klicken Sie auf “Abbrechen bzw. Cancel”, um zum Menü “Zugriffsliste Wireless-Karte bzw. Wireless Card Access List” zurückzukehren.
7. Klicken Sie auf “Anwenden bzw. Apply”, um die Einstellungen der Zugriffsliste für Wireless-Geräte zu speichern.

Wenn Sie eine MAC-Adresse in der Tabelle bearbeiten wollen, wählen Sie die betreffende Adresse durch Mausklicken aus und klicken Sie dann auf die Schaltfläche “Bearbeiten bzw. Edit” oder “Löschen bzw. Delete”.



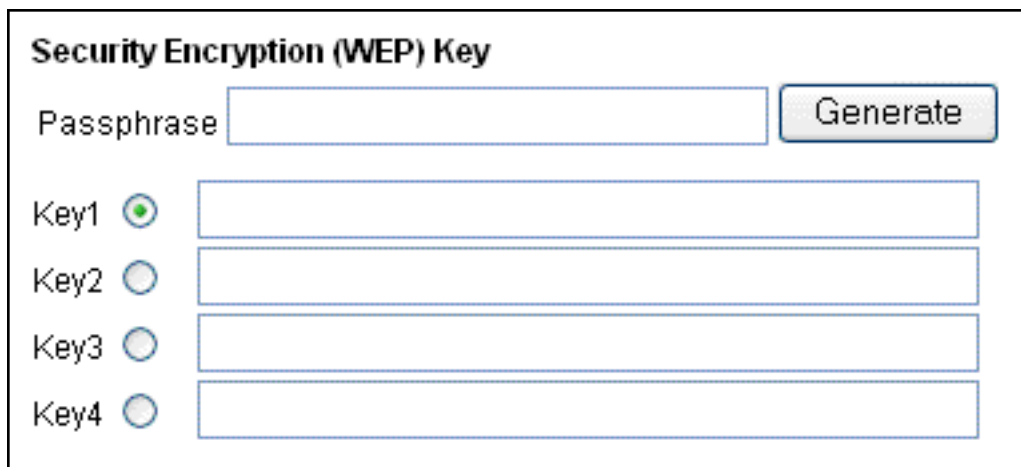
Hinweis: Wenn Sie den Wireless-Router an einem Wireless-PC konfigurieren, dessen MAC-Adresse nicht auf der Liste der zugelassenen PCs befindet, und die Option “Zugriffskontrolle einschalten bzw. Turn Access Control On” aktivieren, wird die drahtlose Verbindung bei Auswahl von “Anwenden bzw. Apply” beendet. Sie müssen dann über einen leitungsgebundenen PC oder einen Wireless-PC, der auf der Zugriffsliste steht, auf den Router zugreifen, um weitere Änderungen vorzunehmen.

Vorgehensweise 3-3: WEP konfigurieren

Gehen Sie wie folgt vor, um die WEP-Datenverschlüsselung zu konfigurieren:

1. Melden Sie sich bei dem Wireless-Router von MR814 v2 unter der Standard-LAN-Adresse <http://192.168.0.1> mit dem Standard- Benutzernamen “admin” und dem Standardkennwort “password” an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem zugehörigen Kennwort.
2. Klicken Sie im Hauptmenü des Wireless-Routers MR814 v2 auf den Link “Wireless-Einstellungen bzw. Wireless Settings”.

3. Wählen Sie in der Dropdown-Liste “Sicherheitsverschlüsselung bzw. Security Encryption” den gewünschten WEP-Verschlüsselungstyp aus.



Security Encryption (WEP) Key

Passphrase

Key1

Key2

Key3

Key4

Abbildung 3-9: Menü “Wireless-Einstellungen bzw. Wireless Settings”

4. Sie können die vier Datenverschlüsselungscodes manuell oder automatisch programmieren. Diese Werte müssen auf allen PCs und Access Points im Netzwerk identisch sein.
 - Automatisch - Geben Sie in dem Feld “Passphrase” ein Wort oder eine Gruppe druckbarer Zeichen ein und klicken Sie auf die Schaltfläche “Erzeugen bzw. Generate”. In den vier Code-Feldern werden automatisch Code-Werte eingesetzt.
 - Manuell - Geben Sie zehn hexadezimale Zeichen (beliebige Kombination aus 0-9, a-f und A-F) ein. Wählen Sie den zu aktivierenden Code aus.

Eine vollständige Erläuterung dieser Optionen entsprechend der Definition in der IEEE-Norm 802.11b für die drahtlose Datenübertragung finden Sie unter “Übersicht der WEP-Parameter” auf Seite D-5.

5. Klicken Sie auf “Anwenden bzw. Apply”, um die gewählten Einstellungen zu speichern.



Hinweis: Wenn Sie den Router an einem Wireless-PC konfigurieren und die WEP-Einstellungen festlegen, wird die drahtlose Verbindung bei Anklicken von “Anwenden bzw. Apply” beendet. In diesem Fall müssen Sie an Ihrem Wireless-Adapter dieselben neuen WEP-Einstellungen wie an dem Router vornehmen oder über einen leitungsgebundenen PC auf den Router zugreifen, um weitere Änderungen vorzunehmen.

Kapitel 4

Content Filtering

In diesem Kapitel wird beschrieben, wie Sie die Funktionen des Content Filtering des Kabel-/DSL-Wireless-Routers Modell MR814 v2 zum Schutz Ihres Netzwerks einsetzen können. Diese Funktionen stehen Ihnen zur Verfügung, wenn Sie im Hauptmenü der Browser-Oberfläche auf die Überschrift “Content Filtering” klicken.

Übersicht Content Filtering

Der Kabel-/DSL-Wireless-Router Modell MR814 v2 bietet verschiedene Optionen zum Content Filtering der Internet-Inhalte sowie eine Berichtsfunktion zur Browsing-Aktivität und eine schnelle Alarmfunktion - beide über E-Mail. Benutzer wie auch Netzwerkadministratoren können entsprechend der Tageszeit, der Website-Adressen und der Keywords der Web-Adressen Regelungen für einen eingeschränkten Internet-Zugang festlegen. Daneben kann der Internet-Zugang für bestimmte Anwendungen und Dienste, z. B. Chat-Anwendungen oder Spiele, gesperrt werden.

Wenn Sie diese Funktionen Ihres Routers konfigurieren wollen, klicken Sie im Hauptmenü der Browser-Oberfläche auf die Unterüberschriften unter “Content Filtering”. Diese Unterüberschriften werden nachfolgend beschrieben.

Zugriff auf Internet-Seiten sperren

Mit dem Router MR814 v2 können Sie den Internet-Zugang entsprechend der Internet-Adressen und deren Keywords einschränken. In der Liste "Keyword" werden bis zu 255 Einträge unterstützt. Das Menü "Seiten sperren bzw. Block Sites" ist in Abbildung 3-1 (unten) dargestellt:

The screenshot shows the 'Block Sites' configuration page. At the top, there is a title 'Block Sites'. Below it, the 'Keyword Blocking' section has three radio buttons: 'Never' (selected), 'Per Schedule', and 'Always'. A text input field labeled 'Type Keyword Or Domain Name Here:' is followed by an 'Add Keyword' button. Below this is a list area titled 'Block Sites Containing These Keywords Or Domain Names:' with a 'Delete Keyword' button and a 'Clear List' button. At the bottom, there is a checkbox for 'Allow Trusted IP Address To Visit Blocked Sites' and a 'Trusted IP Address' field with four input boxes (the first three contain '192', '168', and '0'). 'Apply' and 'Cancel' buttons are at the very bottom.

Abbildung 4-1: Menü "Seiten sperren bzw. Block Sites"

Wenn Sie eine Sperrung für bestimmte Keywords aktivieren wollen, wählen Sie entweder "Nach Zeitplan bzw. Per Schedule" oder "Immer bzw. Always" aus und klicken dann auf "Anwenden bzw. Apply". Wenn die Sperrung nach einem Zeitplan vorgenommen werden soll, ist darauf zu achten, dass in dem Menü "Zeitplan bzw. Schedule" auch tatsächlich ein Zeitraum festgelegt ist.

Zum Hinzufügen eines Keywords oder einer Domäne geben Sie die betreffende Bezeichnung im Feld "Keyword" ein und klicken Sie dann zunächst auf "Keyword hinzufügen bzw. Add Keyword" und dann auf "Anwenden bzw. Apply".

Zum Löschen eines Keywords oder einer Domäne wählen Sie die betreffende Bezeichnung in der Liste aus und klicken Sie dann auf "Keyword löschen bzw. Delete Keyword" und dann auf "Anwenden bzw. Apply". Beispiele für die Anwendung von Keywords:

- Wenn Sie das Keyword "XXX" angeben, wird die URL `<http://www.schmutzig.com/xxx.html>` gesperrt.

- Wenn Sie das Keyword “.com” angeben, können nur Websites mit anderen Domänen-Endungen (z. B. .edu oder .gov) angezeigt werden.
- Wenn Sie für einen bestimmten Zeitraum den gesamten Zugang zum Internet sperren wollen, geben Sie das Keyword “.” ein und legen Sie den Zeitraum im Menü “Zeitplan bzw. Schedule” fest.

Wenn Sie einen von dieser Sperre ausgenommenen Benutzer festlegen wollen, geben Sie die IP-Adresse des betreffenden PC in dem Feld “Verlässlicher Benutzer bzw. Trusted User” ein und klicken Sie auf “Anwenden bzw. Apply”.

Sie können einen verlässlichen Benutzer festlegen; dies ist der PC, der von der Sperrung und Protokollierung ausgenommen ist. Da dieser verlässliche Benutzer über eine IP-Adresse definiert wird, sollten Sie den betreffenden PC mit einer statischen (festen) IP-Adresse konfigurieren.

Zugriff auf Internet-Dienste sperren

Mit dem Router MR814 v2 können Sie die Benutzung bestimmter Internet-Dienste über PCs in Ihrem Netzwerk sperren. Diese Funktion wird als Dienstesperre oder Port-Filterfunktion bezeichnet. Das Menü “Dienste sperren bzw. Block Services” ist nachfolgend abgebildet:

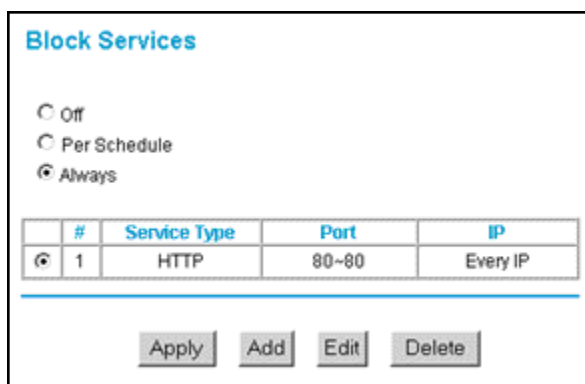


Abbildung 4-2: Menü “Dienste sperren bzw. Block Services”

Dienste sind Funktionen, die von Server-Rechnern auf Anforderung von Client-Rechnern ausgeführt werden. So werden beispielsweise von Web-Servern Web-Seiten geliefert, während Zeit-Server das Datum und die Uhrzeit bereitstellen und Spiele-Hosts die Daten zu den Zügen anderer Spieler übertragen. Wenn ein Computer in Ihrem Netzwerk eine Diensteanforderung an einen Server-Rechner im Internet sendet, wird der angeforderte Dienst durch eine Dienst- oder Port-Nummer gekennzeichnet. Diese Nummer wird in den gesendeten IP-Paketen als Ziel-Port-Nummer aufgeführt. So ist beispielsweise ein Paket, das mit der Ziel-Port-Nummer 80 übertragen wird, eine HTTP-Anforderung an einen Web-Server.

Wenn Sie eine Sperrung für bestimmte Dienste aktivieren wollen, wählen Sie entweder “Nach Zeitplan bzw. Per Schedule” oder “Immer bzw. Always” aus und klicken dann auf “Anwenden bzw. Apply”. Wenn die Sperrung nach einem Zeitplan vorgenommen werden soll, ist darauf zu achten, dass in dem Menü “Zeitplan bzw. Schedule” auch tatsächlich ein Zeitraum festgelegt ist.

Wenn Sie einen zu sperrenden Dienst angeben wollen, klicken Sie auf “Hinzufügen bzw. Add”. Daraufhin erscheint das nachfolgend abgebildete Menü “Dienste hinzufügen bzw. Add Services”.

The screenshot shows the 'Block Services' configuration window. It includes fields for Service Type (HTTP), Protocol (TCP), Starting Port (80), Ending Port (80), and Service Type:User Defined (HTTP). There are also radio buttons for filtering IP addresses: 'Only this IP' (selected), 'IP address range', and 'Every IP'. The 'Only this IP' option has input fields for IP address components (192, 168, 0, and an empty field). The 'IP address range' option has two sets of input fields for IP address components (192, 168, 0, and an empty field). At the bottom are 'OK' and 'Cancel' buttons.

Abbildung 4-3: Menü “Dienste hinzufügen bzw. Add Services”

Wählen Sie in der Liste “Dienstetyp bzw. Service Type” die Anwendungen oder den Dienst aus, der/die zugelassen oder gesperrt werden soll. Diese Liste enthält bereits einige häufig verwendete Dienste, aber Sie sind in Ihrer Auswahl nicht auf diese Einträge beschränkt. Wenn Sie weitere Dienste oder Anwendungen hinzufügen wollen, wählen Sie “Benutzerdefiniert bzw. User Defined” aus.

Benutzerdefinierten Dienst konfigurieren

Wenn Sie einen Dienst definieren wollen, müssen Sie zunächst die Port-Nummer oder den Nummernbereich bestimmen, die/der von der Anwendung verwendet wird. Die Dienstenummern zahlreicher gängiger Protokolle werden durch die Internet Engineering Task Force (IETF) definiert und in RFC1700, “Assigned Numbers”, veröffentlicht. Dienstenummern anderer Anwendungen werden in der Regel durch die Autoren der Anwendung aus dem Bereich von 1024 bis 65535 ausgewählt. Diese Angaben können Sie in der Regel direkt bei dem Herausgeber der Anwendung oder über eine User Group erfragen.

Geben Sie den “Ersten Port bzw. Starting Port” und den “Letzten Port bzw. Ending Port” ein. Falls die Anwendung nur eine Port-Nummer verwendet, geben Sie diese Nummer in beiden Feldern ein.

Wenn Sie wissen, dass die Anwendung TCP oder UDP verwendet, wählen Sie das betreffende Protokoll aus. Wenn Sie sich nicht sicher sind, wählen Sie “Beide bzw. Both” aus.

Konfiguration zum Sperren von Diensten über den IP-Adressbereich

Unter “Dienste filtern nach bzw. Filter Services For” können Sie den betreffenden Dienst für einen einzelnen PC, eine Gruppe von PCs (mit fortlaufenden IP-Adressen) oder für alle PCs im Netzwerk sperren.

Zeitplan zum Sperren von Seiten/Diensten

Mit dem Router MR814 v2 können Sie auch festlegen, wann bestimmte Seiten/Dienste gesperrt werden sollen. Das Menü “Zeitplan bzw. Schedule” ist nachfolgend dargestellt:

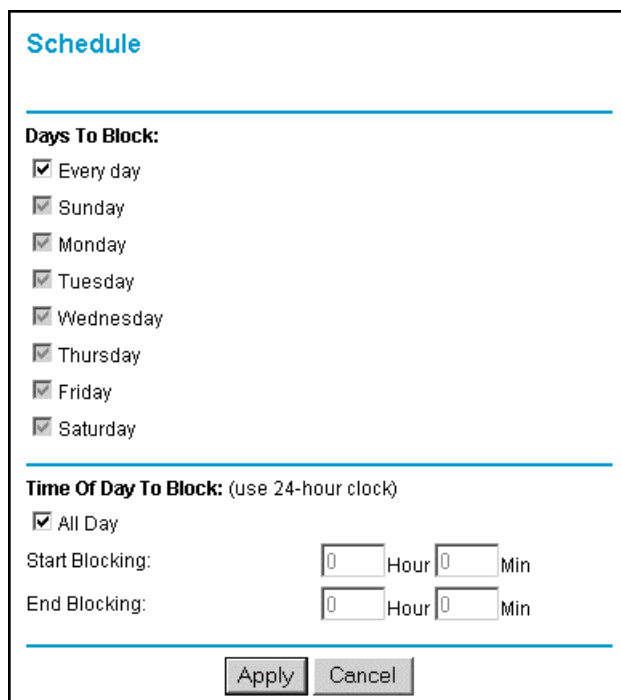


Abbildung 4-4: Menü “Zeitplan bzw. Schedule”

- Verwenden Sie diesen Zeitplan zum Sperren von Internet-Inhalten. Wählen Sie dieses Markierungsfeld aus, wenn Sie einen Zeitplan für das Content Filtering aktivieren wollen. Klicken Sie auf “Anwenden bzw. Apply”.
- Sperren an Tagen bzw. Days to Block. Wählen Sie die Wochentage aus, an denen die Sperre aktiv sein soll. Wählen Sie “Jeden Tag bzw. Everyday” aus, wenn die Sperre an allen Wochentagen gültig sein soll. Klicken Sie auf “Anwenden bzw. Apply”.
- Tageszeit bzw. Time of Day to Block. Wählen Sie eine Anfangs- und eine Endzeit im 24-Stundenformat aus. Wählen Sie “Ganztags bzw. All day” aus, wenn die Sperre rund um die Uhr gelten soll. Klicken Sie auf “Anwenden bzw. Apply”.

Vergewissern Sie sich, dass im Menü “E-Mail” Ihre Zeitzone ausgewählt ist.

Protokolle zum Internet-Zugriff und zu Zugriffsversuchen anzeigen

Das Protokoll enthält detaillierte Aufzeichnungen zu den Websites, auf die zugegriffen wurde oder auf die ein Zugriffsversuch unternommen wurde. In dem Protokoll werden bis zu 128 Einträge gespeichert. Protokolleinträge werden nur erzeugt, wenn eine Keyword-Sperre aktiviert ist; für den verlässlichen Benutzer werden keine Protokolleinträge erzeugt. Nachfolgend ein Beispiel:

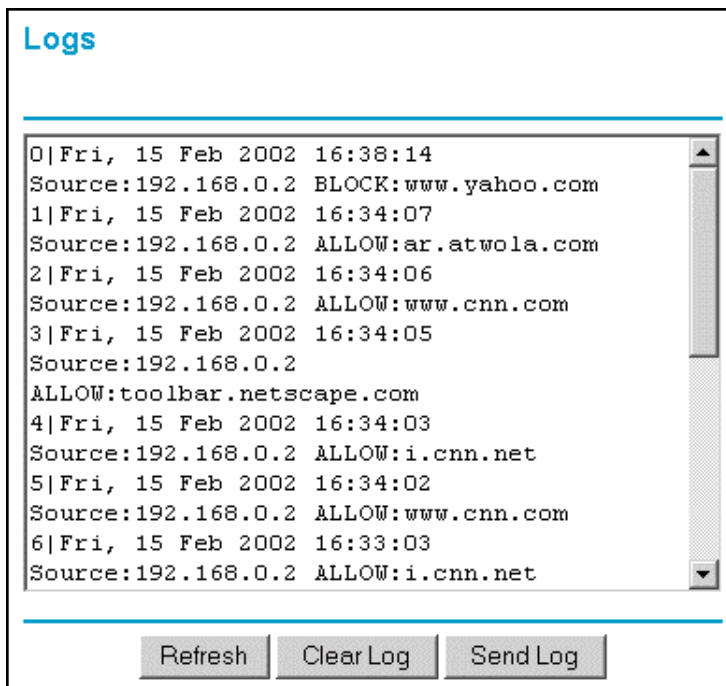


Abbildung 4-5: Menü "Protokoll bzw. Logs"

Die Protokolleinträge werden in Tabelle 4-1 beschrieben.

Tabelle 4-1. Beschreibung der Protokolleinträge

Feld	Beschreibung
Nummer	Die laufende Nummer des Protokolleintrags für das Content Filtering. Insgesamt können 128 Einträge mit den Nummern von 0 bis 127 gespeichert werden. Im Protokoll werden jeweils die letzten 128 Einträge aufbewahrt.
Datum und Uhrzeit	Das Datum und die Uhrzeit, an dem/der der Protokolleintrag erstellt wurde.
Quellen-IP bzw. Source IP	Die IP-Adresse des Geräts, von dem der Zugriff initiiert wurde, für den der betreffende Eintrag erzeugt wurde.
Maßnahme	In diesem Feld wird angezeigt, ob der Zugriff gesperrt oder freigegeben wurde.
	Der Name oder die IP-Adresse der Website oder Newsgroup, auf die der Zugriff oder der Zugriffsversuch erfolgte.

Die Schaltflächen im Protokollfenster werden in Tabelle 4-2 beschrieben.

Tabelle 4-2. Schaltflächen im Protokollfenster

Feld	Beschreibung
Aktualisieren bzw. Refresh	Klicken Sie auf diese Schaltfläche, um das angezeigte Protokollfenster zu aktualisieren.
Protokoll löschen bzw. Clear Log	Klicken Sie auf diese Schaltfläche, um die Protokolleinträge zu löschen.
Protokoll senden bzw. Send Log	Klicken Sie auf diese Schaltfläche, um das Protokoll unmittelbar als E-Mail zu versenden.

E-Mail-Warnungen und Protokollberichte zum Internet-Zugriff konfigurieren

Damit Ihnen Protokolle und Warnungen per E-Mail zugestellt werden können, müssen Sie im Menü “E-Mail” (siehe unten) Ihre E-Mail-Daten eingeben:

E-mail

Turn E-mail Notification On.

Send Alert And Logs Via E-mail
 Your Outgoing Mail Server:

 Send To This E-mail Address:

Send Alert Immediately
 When Someone Attempts To Visit Blocked Site.

Send Logs According To This Schedule

 A.M. P.M.

Time Zone

 Adjust for Daylight Savings Time

Current Time : 10:14:38, Fri.

Abbildung 4-6: Menü “E-Mail”

Referenzhandbuch für den Kabel-/DSL-Wireless-Router, Modell MR814 v2

- E-Mail-Benachrichtigung ein bzw. Turn e-mail notification on: Wählen Sie dieses Markierungsfeld aus, wenn Sie Protokolle und Warnungen per E-Mail von Ihrem Router erhalten wollen.
- Server für Mail-Versand bzw. Your outgoing mail server
Geben Sie den Namen des Servers Ihres ISP für den Mail-Versand (SMTP) ein (z. B. mail.meinISP.com). Diese Angaben finden Sie unter Umständen im Konfigurationsmenü Ihres E-Mail-Programms. Wenn Sie dieses Markierungsfeld nicht auswählen, erhalten Sie keine Protokollmeldungen und Warnungen per E-Mail.
- Empfängeradresse bzw. Send to this e-mail address
Geben Sie die E-Mail-Adresse ein, an die Protokolle und Warnungen gesendet werden sollen. Diese E-Mail-Adresse wird auch als Absenderadresse bzw. From verwendet. Wenn Sie dieses Markierungsfeld nicht auswählen, erhalten Sie keine Protokollmeldungen und Warnungen per E-Mail.

Für die automatische Zustellung von Protokollen und Warnungen an die genannte E-Mail-Adresse können Sie außerdem noch folgende Optionen festlegen:

- Warnung sofort senden bzw. Send alert immediately
Wählen Sie dieses Markierungsfeld aus, wenn Sie im Falle eines Zugriffsversuchs auf eine gesperrte Website sofort benachrichtigt werden wollen.
- Protokolle nach Zeitplan senden bzw. Send logs according to this schedule
Hier können Sie angeben, in welchen Intervallen die Protokolle gesendet werden sollen: Stündlich bzw. Hourly, Täglich bzw. Daily, Wöchentlich bzw. Weekly oder bei Vollbelegung bzw. When Full.
 - Tag des Protokollversands
Hier können Sie den Wochentag angeben, an dem das Protokoll gesendet werden soll. Diese Option ist relevant, wenn die Protokolle wöchentlich oder täglich zugestellt werden sollen.
 - Uhrzeit des Protokollversands
Hier können Sie die Uhrzeit angeben, zu der das Protokoll gesendet werden soll. Diese Option ist relevant, wenn die Protokolle täglich oder wöchentlich gesendet werden sollen.

Wenn die Option “Wöchentlich bzw. Weekly”, “Täglich bzw. Daily” oder “Stündlich bzw. Hourly” ausgewählt wurde und das Protokoll bereits vor Erreichen des nächsten Versandzeitpunkt voll belegt ist, wird das Protokoll automatisch per E-Mail an die angegebene E-Mail-Adresse geschickt. Nach Versand des Protokolls wird es aus dem Speicher des Routers gelöscht. Wenn der Versand der Protokolldatei fehlschlägt, wird unter Umständen die Kapazitätsgrenze des Protokolls erreicht. In diesem Fall wird das bestehende Protokoll überschrieben und sein Inhalt gelöscht.

Der Router MR814 v2 verwendet das Network Time Protocol (NTP), um die korrekte Uhrzeit und das korrekte Datum bei einem der zahlreichen Network Time Server im Internet abzufragen. Damit die Uhrzeit für die Protokolleinträge korrekt ermittelt werden kann, müssen Sie Ihre Zeitzone angeben:

- Zeitzone bzw. Time Zone Wählen Sie Ihre Zeitzone aus. Diese Einstellung wird für den Sperrplan und die Uhrzeitermittlung für die Protokolleinträge verwendet.
- Sommerzeit bzw. Daylight Savings Time Wählen Sie dieses Markierungsfeld aus, wenn in Ihrer Zeitzone momentan die Sommerzeit gilt.

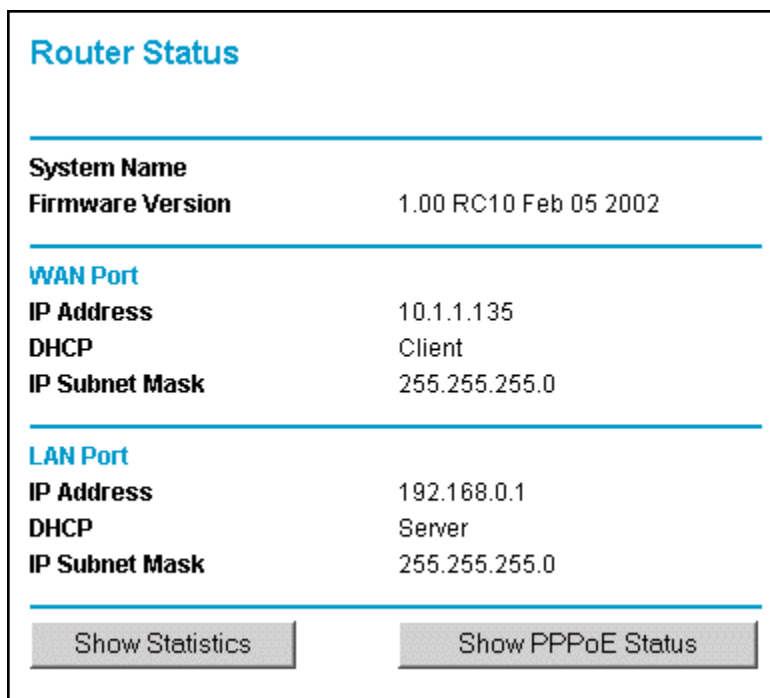
Kapitel 5

Wartung

In diesem Kapitel wird die Verwendung der Wartungsfunktionen des Kabel-/DSL-Wireless-Routers Modell MR814 v2 beschrieben. Diese Funktionen stehen Ihnen zur Verfügung, wenn Sie im Hauptmenü der Browser-Oberfläche auf die Überschrift “Wartung bzw. Maintenance” klicken.

Statusinformationen des Routers anzeigen

Das Menü “Router-Status” enthält in begrenztem Umfang Status- und Nutzungsinformationen. Klicken Sie auf der Browser-Oberfläche im Hauptmenü auf “Wartung bzw. Maintenance” und wählen Sie dann “Systemstatus bzw. System Status” aus, um das nachfolgend dargestellte Fenster “Systemstatus bzw. System Status” zu öffnen.



The screenshot shows a window titled "Router Status" with a blue header. It is divided into three sections by horizontal lines. The first section, "System Name", shows "Firmware Version" as "1.00 RC10 Feb 05 2002". The second section, "WAN Port", shows "IP Address" as "10.1.1.135", "DHCP" as "Client", and "IP Subnet Mask" as "255.255.255.0". The third section, "LAN Port", shows "IP Address" as "192.168.0.1", "DHCP" as "Server", and "IP Subnet Mask" as "255.255.255.0". At the bottom, there are two buttons: "Show Statistics" and "Show PPPoE Status".

Router Status	
System Name	
Firmware Version	1.00 RC10 Feb 05 2002
WAN Port	
IP Address	10.1.1.135
DHCP	Client
IP Subnet Mask	255.255.255.0
LAN Port	
IP Address	192.168.0.1
DHCP	Server
IP Subnet Mask	255.255.255.0
Show Statistics	
Show PPPoE Status	

Abbildung 5-1. Fenster “Router-Status”

Dieses Fenster enthält folgende Parameter:

Tabelle 5-1.Menü 3.2 - Felder im Fenster "Router-Status"

Feld	Beschreibung
Kontoname bzw. Account Name	In diesem Feld wird der Host-Name angezeigt, der dem Router zugeordnet ist.
Firmware-Version	In diesem Feld wird die Version der Router-Firmware angezeigt.
Internet-Port MAC-Adresse bzw. MAC Address IP-Adresse bzw. IP Address IP-Subnetzmaske bzw. IP Subnet Mask DHCP	<p>Diese Parameter gelten für den Internet- bzw. WAN-Anschluss des Routers.</p> <p>Dieses Feld enthält die MAC-Adresse (Media Access Control), die von dem Internet- bzw. WAN-Anschluss des Routers verwendet wird.</p> <p>Dieses Feld enthält die IP-Adresse, die von dem Internet- bzw. WAN-Anschluss des Routers verwendet wird. Wenn hier keine Adresse angezeigt wird, kann der Router keine Verbindung zum Internet aufbauen.</p> <p>Dieses Feld enthält die IP-Subnetzmaske, die von dem Internet- bzw. WAN-Anschluss des Routers verwendet wird.</p> <p>Falls hier "Nein bzw. None" angezeigt wird, verwendet der Router in dem WAN eine feste (statische) IP-Adresse. Wenn hier "Client" angezeigt wird, wird dem Router dynamisch eine IP-Adresse durch den ISP zugewiesen.</p>
LAN-Port MAC-Adresse bzw. MAC Address IP-Adresse bzw. IP Address IP-Subnetzmaske bzw. IP Subnet Mask DHCP	<p>Diese Parameter gelten für den Local- bzw. LAN-Anschluss des Routers.</p> <p>Dieses Feld enthält die MAC-Adresse (Media Access Control), die von dem LAN-Anschluss des Routers verwendet wird.</p> <p>Dieses Feld enthält die IP-Adresse, die von dem Local- bzw. LAN-Anschluss des Routers verwendet wird. Die Standardadresse lautet 192.168.0.1</p> <p>Dieses Feld enthält die IP-Subnetzmaske, die von dem Local- bzw. LAN-Anschluss des Routers verwendet wird. Die Standardeinstellung lautet 255.255.255.0</p> <p>Gibt an, ob der integrierte DHCP-Server des Routers für die an das LAN angeschlossenen Geräte aktiv ist.</p>
Wireless-Port MAC-Adresse bzw. MAC Address Name (SSID) Region Kanal	<p>Diese Parameter gelten für den Wireless-Anschluss des Routers.</p> <p>Dieses Feld enthält die MAC-Adresse (Media Access Control), die von dem Wireless-Anschluss des Routers verwendet wird.</p> <p>In diesem Feld wird der Name des Wireless-Netzwerks (SSID) angezeigt, der von dem Wireless-Anschluss des Routers verwendet wird. Die Standard-SSID lautet "Wireless".</p> <p>In diesem Feld wird die geografische Region angezeigt, in der der Router verwendet wird. Unter Umständen ist die Nutzung der Wireless-Funktionen des Routers in manchen Teilen der Welt gesetzlich verboten.</p> <p>Bezeichnet den Kanal, den der Wireless-Anschluss verwendet. Die für die einzelnen Kanäle verwendeten Frequenzen finden Sie unter "Wireless-Kanäle" auf Seite D-7.</p>

Klicken Sie auf die Schaltfläche “Verbindungsstatus bzw. Connection Status”, um den Verbindungsstatus anzuzeigen (siehe unten).

Connection Time	0:18:29
Connection Method	Dynamic IP
IP Address	0.0.0.0
Network Mask	0.0.0.0
Default Gateway	0.0.0.0
<input type="button" value="Renew"/>	

Abbildung 5-3: Fenster “Verbindungsstatus bzw. Connection Status”

Dieses Fenster enthält folgende statistische Angaben:

Tabelle 5-1. Felder zum Verbindungsstatus

Feld	Beschreibung
Dauer der Verbindung bzw. Connection Time	Die bisherige Dauer der Verbindung des Routers zu dem Netzwerk Ihres Internet Service Providers.
Verbindungsmethode bzw. Connection Method	Die Methode, mit der eine IP-Adresse von Ihrem Internet Service Provider angefordert wurde.
IP-Adresse bzw. IP Address	Die WAN-IP-Adresse, die dem Router zugewiesen wurde.
Netzwerkmaske bzw. Network Mask	Die WAN-Subnetzmaske, die dem Router zugewiesen wurde.
Standard-Gateway bzw. Default Gateway	Der Standard-WAN-Gateway, mit dem der Router kommuniziert.

Die Schaltflächen des Fensters “Verbindungsstatus bzw. Connection Status” werden in Tabelle 5-2 beschrieben.

Tabelle 5-2. Schaltflächen im Fenster “Verbindungsstatus bzw. Connection Status”

Feld	Beschreibung
Aktualisieren bzw. Renew	Klicken Sie auf die Schaltfläche “Aktualisieren bzw. Renew”, um die DHCP-Vereinbarung zu aktualisieren.

Klicken Sie auf die Schaltfläche “Statistik anzeigen bzw. Show Statistics”, um Statistiken zur Routernutzung anzuzeigen (siehe unten).

System Up Time 0:13:22							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	10M/Half	52	0	0	118	0	0:13:22
LAN	100M/Full	959	728	0	1921	720	0:13:22
WLAN	11M	959	728	0	1921	720	0:13:22

Poll Interval: (secs)

Abbildung 5-3: Fenster “Routerstatistik bzw. Router Statistics”

Dieses Fenster enthält folgende statistische Angaben:

Tabelle 5-1. Felder im Fenster “Routerstatistik bzw. Router Statistics”

Feld	Beschreibung
Port	Die statistischen Angaben zum WAN-Port (Internet) und zum LAN-Port (lokal). Dabei werden zu jedem Port folgende Angaben angezeigt:
Status	Der Verbindungsstatus des Ports.
TxPkts	Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen über diesen Port versendet wurden.
RxPkts	Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen über diesen Port empfangen wurden.
Kollisionen bzw. Collisions	Die Anzahl der Kollisionen, die seit dem letzten Zurücksetzen oder manuellen Löschen an diesem Port aufgetreten sind.
Tx B/s	Die aktuelle Übertragungsbandbreite (ausgehend), die an dem WAN- und dem LAN-Port verwendet wird.
Rx B/s	Die aktuelle Übertragungsbandbreite (ankommend), die an dem WAN- und dem LAN-Port verwendet wird.
Betriebsdauer bzw. Up Time.	Die seit dem letzten Neustart des Routers vergangene Zeit
Verbindungsdauer bzw. Up Time	Die seit Herstellung der Verbindung an diesem Port vergangene Zeit.
Aktualisierungsintervall bzw. Poll Interval	Gibt die Intervalle an, in denen die statistischen Angaben in diesem Fenster aktualisiert werden. Klicken Sie auf “Stopp bzw. Stop”, um die Anzeige “einzufrieren”.

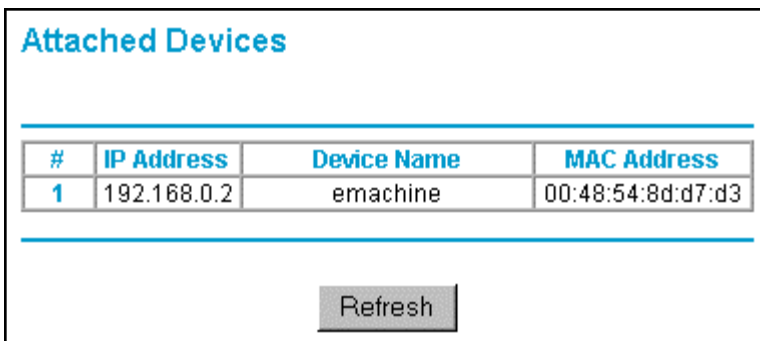
Die Schaltflächen im WAN-Statusfenster werden in Tabelle 5-3 beschrieben.

Tabelle 5-3. Schaltflächen im Fenster “Verbindungsstatus bzw. Connection Status”

Feld	Beschreibung
Intervall festlegen bzw. Set Interval	Geben Sie ein Intervall ein und klicken Sie auf diese Schaltfläche, um ein neues Aktualisierungsintervall festzulegen.
Stopp bzw. Stop	Klicken Sie auf diese Schaltfläche, um die Statistikanzeige “einzufrieren”.

Liste der angeschlossenen Geräte anzeigen

Das Menü “Angeschlossene Geräte bzw. Attached Devices” enthält eine Tabelle aller IP-Geräte, die der Router im lokalen Netzwerk erkannt hat. Wählen Sie im Hauptmenü der Browser-Oberfläche unter dem Titel “Wartung bzw. Maintenance” die Option “Angeschlossene Geräte bzw. Attached Devices” aus, um die nachfolgend dargestellte Tabelle anzuzeigen.



The screenshot shows a web interface titled "Attached Devices". It contains a table with the following data:

#	IP Address	Device Name	MAC Address
1	192.168.0.2	emachine	00:48:54:8d:d7:d3

Below the table is a "Refresh" button.

Abbildung 5-4: Menü “Angeschlossene Geräte bzw. Attached Devices”

Die Tabelle enthält zu jedem Gerät die IP-Adresse, den NetBIOS-Host-Namen (falls verfügbar) und die Ethernet-MAC-Adresse. Bei einem Neustart des Routers werden die in der Tabelle dargestellten Daten zunächst gelöscht; sie sind erst wieder verfügbar, wenn der Router die Geräte erneut erkannt hat. Klicken Sie auf die Schaltfläche “Aktualisieren bzw. Refresh”, um eine erneute Suche nach angeschlossenen Geräten zu starten.

Upgrade der Router-Software

Die Routing-Software des Routers MR814 v2 ist im FLASH-Speicher abgelegt und kann aktualisiert werden, sobald eine neue Software von NETGEAR herausgebracht wird. Upgrade-Dateien können von der Website von Netgear heruntergeladen werden. Im Falle komprimierter Upgrade-Dateien (ZIP-Datei) muss vor der Weiterleitung an den Router die Binärdatei (.BIN) extrahiert werden. Sie können die Upgrade-Datei mit Hilfe Ihres Browsers an den Router schicken.

Hinweis: Der Web-Browser, mit dem die neue Firmware auf den Router MR814 v2 übertragen wird, muss HTTP-Übertragungen unterstützen. NETGEAR empfiehlt die Verwendung des Internet Explorer oder des Netscape Navigator ab Version 3.0.

Wählen Sie im Hauptmenü der Browser-Oberfläche unter dem Titel “Wartung bzw. Maintenance” die Option “Router Upgrade” aus, um das nachfolgend dargestellte Menü anzuzeigen.

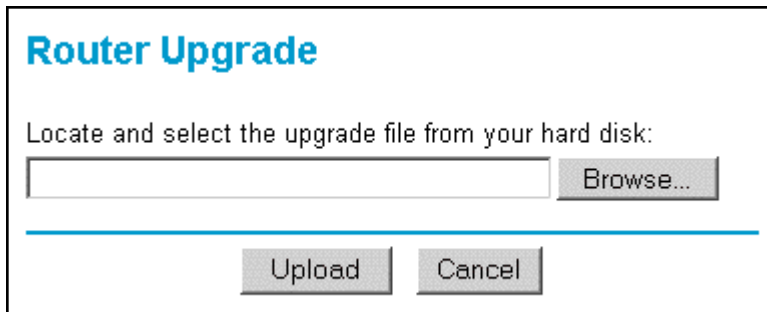


Abbildung 5-5: Menü “Router Upgrade”

Gehen Sie zum Hochladen einer neuen Firmware wie folgt vor:

1. Laden Sie die neue Software-Datei von NETGEAR herunter, und dekomprimieren Sie diese Datei (UNZIP).
2. Klicken Sie in dem Menü “Router Upgrade” auf die Schaltfläche “Durchsuchen bzw. Browse” und navigieren Sie zum Standort der binären Upgrade-Datei (.BIN).
3. Klicken Sie auf “Hochladen bzw. Upload”.

Hinweis: Beim Hochladen der Software auf den Router MR814 v2 darf der Web-Browser nicht durch Schließen des Fensters, Anklicken eines Links oder Laden einer neuen Seite unterbrochen werden. Eine Unterbrechung des Browsers kann zu einer Beschädigung der Software führen. Nach Abschluss des Hochladevorgangs wird der Router automatisch neu gestartet. Der Upgrade-Vorgang dauert in der Regel etwa eine Minute.

In manchen Fällen muss der Router nach dem Upgrade neu konfiguriert werden.

Handhabung der Konfigurationsdatei

Die Konfigurationseinstellungen des Routers MR814 v2 sind im Router in einer Konfigurationsdatei gespeichert. Sie können eine Sicherungskopie dieser Datei auf einem Benutzer-PC erstellen, die Datei mit Hilfe der Sicherungskopie von dem Benutzer-PC wieder herstellen oder die Konfigurationsdatei auf die werksseitigen Standardeinstellungen zurücksetzen.

Wählen Sie im Hauptmenü der Browser-Oberfläche unter dem Titel “Wartung bzw. Maintenance” die Option “Einstellungen sichern bzw. Settings Backup” aus, um das nachfolgend dargestellte Menü anzuzeigen.

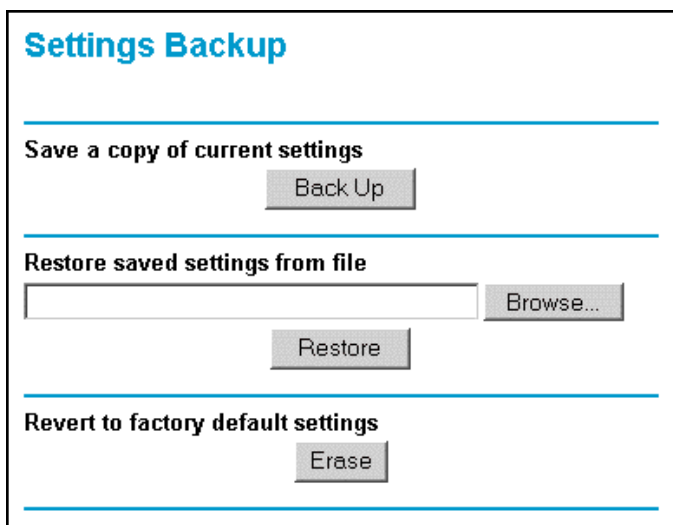


Abbildung 5-6: Menü “Einstellungen sichern bzw. Settings Backup”

Die drei verfügbaren Optionen werden nachfolgend beschrieben.

Konfiguration sichern und wieder herstellen

Über die Optionen “Sichern bzw. Backup” und “Wiederherstellen bzw. Restore” des Menüs “Einstellungen sichern bzw. Settings Backup” können Sie eine Datei, die die Konfigurationseinstellungen des Routers enthält, in einer Datei sichern und die Einstellungen über diese Datei wiederherstellen.

Wenn Sie eine Sicherungskopie der Einstellungen erstellen wollen, klicken Sie auf die Schaltfläche “Sichern bzw. Backup”. Ihr Browser extrahiert die Konfigurationsdatei des Routers und fordert Sie zur Eingabe eines Pfads auf Ihrem PC auf, unter dem die Datei gespeichert werden soll. Dabei können Sie einen nachvollziehbaren Dateinamen festlegen, z. B. bueronez.cfg.

Wenn Sie die Einstellungen mit Hilfe einer Sicherungskopie der Konfigurationsdatei wiederherstellen wollen, geben Sie den vollständigen Pfad der Datei auf Ihrem PC ein oder klicken Sie auf die Schaltfläche “Durchsuchen bzw. Browse”, um die Datei zu suchen. Sobald Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche “Wiederherstellen bzw. Restore”, um die Datei an den Router zu schicken. Der Router wird danach automatisch neu gestartet.

Konfigurationlöschen

Manchmal kann es erforderlich sein, den Router auf bekannte Standardeinstellungen zurückzusetzen. Verwenden Sie zu diesem Zweck die Funktion “Löschen bzw. Erase”, mit der alle Parameter auf die werksseitigen Standardwerte zurückgesetzt werden. Nach einer derartigen Aktion lautet das Kennwort des Routers “password”, die LAN-IP-Adresse lautet 192.168.0.1, und der DHCP-Client des Routers ist aktiviert.

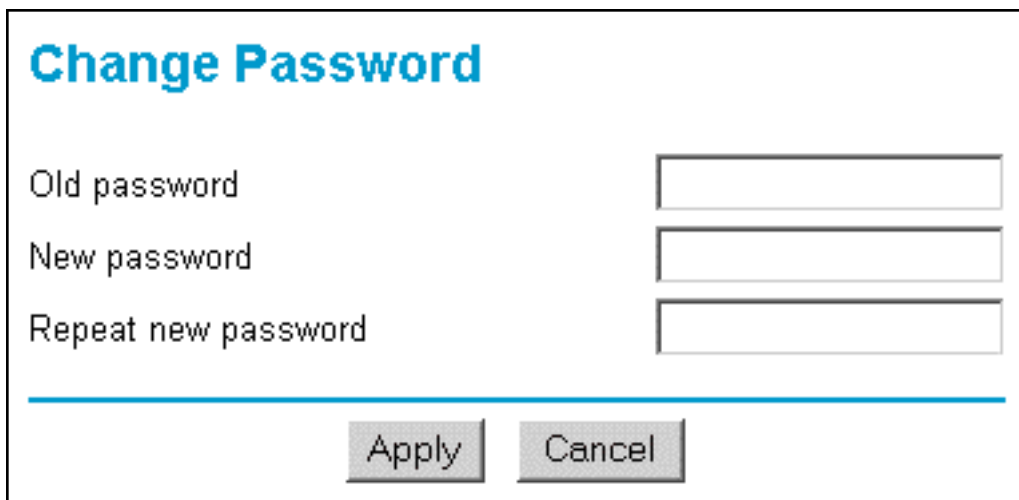
Klicken Sie auf die Schaltfläche “Löschen bzw. Erase”, wenn Sie die Konfiguration löschen wollen.

Wenn Sie die werksseitigen Standardeinstellungen wiederherstellen wollen und das Anmeldekennwort oder die IP-Adresse nicht kennen, müssen Sie die Taste zum Zurücksetzen auf die Standardeinstellungen an der Rückseite des Routers drücken. Siehe “Standardkonfiguration und -kennwort wiederherstellen” auf Seite 7-7.

Kennwort für Konfiguration ändern

Das Standardkennwort für den Web Configuration Manager des Routers lautet “password”. Netgear empfiehlt, dieses Kennwort durch ein sicheres Kennwort zu ersetzen.

Wählen Sie im Hauptmenü der Browser-Oberfläche unter dem Titel “Wartung bzw. Maintenance” die Option “Kennwort festlegen bzw. Set Password” aus, um das nachfolgend dargestellte Menü anzuzeigen.



Change Password

Old password

New password

Repeat new password

Abbildung 5-7: Menü “Kennwort festlegen bzw. Set Password”

Geben Sie zum Ändern des Kennworts zunächst das alte Kennwort und danach zweimal das neue Kennwort ein. Klicken Sie auf “Anwenden bzw. Apply”.

Kapitel 6

Erweiterte Konfiguration des Routers

In diesem Kapitel wird die Konfiguration der erweiterten Funktionen des Kabel-/DSL-Wireless-Routers Modell MR814 v2 beschrieben. Diese Funktionen stehen Ihnen zur Verfügung, wenn Sie im Hauptmenü der Browser-Oberfläche auf die Überschrift “Erweitert bzw. Advanced” klicken.

Konfiguration der Port-Weiterleitung an lokale Server

Obwohl Ihr gesamtes lokales Netzwerk durch den Router im Internet als eine einzelne Maschine dargestellt wird, können Sie einen lokalen Server (z. B. einen Web-Server oder eine Spiel-Server) im Internet sichtbar und verfügbar machen. Dazu verwenden Sie das Menü “Port-Weiterleitung bzw. Port Forwarding”. Klicken Sie im Hauptmenü der Browser-Oberfläche unter der Überschrift “Erweitert bzw. Advanced” auf “Port-Weiterleitung bzw. Port Forwarding”, um das Menü für die Port-Weiterleitung (siehe unten) anzuzeigen.

#	Service Name	Start Port	End Port	Server IP Address
1	FTP	21	21	192.168.0.100
2	HTTP	80	80	192.168.0.101

Abbildung 6-1: Menü “Port-Weiterleitung bzw. Port Forwarding”



Hinweis: Wenn Sie im Umgang mit Netzwerken und Weiterleitungen unsicher sind, können Sie sich in Anhang B, "Netzwerke, Routing, Firewalls: Grundlagen" zunächst mit den in diesem Handbuch verwendeten Begriffen und Vorgehensweisen vertraut machen.

Verwenden Sie das Menü "Port-Weiterleitung bzw. Port Forwarding", um an dem Router die Weiterleitung eingehender Protokolle an Computer im lokalen Netzwerk einzurichten. Neben den für bestimmte Anwendungen verwendeten Servern können Sie auch einen DMZ-Standard-Server angeben, an den alle eingehenden Protokolle weitergeleitet werden sollen. Der DMZ-Server wird im Menü "Sicherheit bzw. Security" konfiguriert.

Zunächst sollten Sie festlegen, welchen Dienst, welche Anwendung oder welches Spiel Sie bereitstellen und wie die IP-Adresse des Computers lautet, über den der Dienst, die Anwendung oder das Spiel bereitgestellt wird. Achten Sie darauf, dass sich die IP-Adresse des Computers nie ändert. Gehen Sie wie folgt vor, um die Port-Weiterleitung an einen lokalen Server zu konfigurieren:

1. Wählen Sie in dem Listenfenster "Dienst & Spiel bzw. Service & Game" den Dienst oder das Spiel aus, den/das Sie in Ihrem Netzwerk bereitstellen wollen. Wenn der betreffende Dienst nicht in der Liste erscheint, lesen Sie im folgenden Abschnitt, "Benutzerspezifischen Dienst hinzufügen", nach.
2. Geben Sie die IP-Adresse des lokalen Servers in dem Feld "Server-IP-Adresse bzw. Server IPAddress" ein.
3. Klicken Sie auf die Schaltfläche "Hinzufügen bzw. Add".

Benutzerdefinierten Dienst hinzufügen

Wenn Sie Dienste, Spiele oder Anwendungen definieren wollen, die nicht in der Liste "Dienst & Spiel bzw. Service & Game" aufgeführt sind, müssen Sie zunächst die Port-Nummern ermitteln, die von dem betreffenden Dienst verwendet werden. Hierfür müssen Sie sich unter Umständen mit dem Hersteller des Programms in Verbindung setzen, das Sie verwenden wollen. Wenn Ihnen die Port-Nummern vorliegen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche "Benutzerspezifischen Dienst hinzufügen bzw. Add Custom Service".
2. Geben Sie in einem freien Feld "Erster Port bzw. Start Port" die erste Port-Nummer ein.
3. Wenn die Weiterleitung nur an einen Port erfolgen soll, geben Sie dieselbe Port-Nummer auch im Feld "Letzter Port bzw. End Port" ein. Wenn Sie einen mehrere Ports umfassenden Bereich festlegen wollen, geben Sie in dem Feld "Letzter Port bzw. End Port" den letzten Port ein, an den eine Weiterleitung erfolgen soll.
4. Geben Sie die IP-Adresse des lokalen Servers in dem Feld "Server-IP-Adresse bzw. Server IPAddress" ein.
5. Geben Sie den Namen des Dienstes ein.
6. Klicken Sie am unteren Rand des Menüs auf "Anwenden bzw. Apply".

Eintrag für Port-Weiterleitung bearbeiten oder löschen

Gehen Sie wie folgt vor, um einen Eintrag für die Port-Weiterleitung zu bearbeiten oder zu löschen.

1. Wählen Sie in der Tabelle das Markierungsfeld neben dem Namen des betreffenden Dienstes aus.
2. Klicken Sie auf “Dienst bearbeiten bzw. Edit Service” oder “Dienst löschen bzw. Delete Service”.

Beispiel: Lokaler Web- und FTP-Server

Wenn ein lokaler PC mit der privaten IP-Adresse 192.168.0.33 als Web- und FTP-Server eingesetzt wird, richten Sie im Menü “Ports” eine Weiterleitung von HTTP (Port 80) und FTP (Port 21) an die lokale Adresse 192.168.0.33 ein.

Damit ein dezentraler Benutzer über das Internet auf diesen Server zugreifen kann, muss dieser dezentrale Benutzer die IP-Adresse kennen, die Ihnen von Ihrem ISP zugewiesen wurde. Wenn diese Adresse beispielsweise 172.16.1.23 lautet, kann ein Internet-Benutzer durch Weiterleitung des Browsers an <http://172.16.1.23> auf Ihren Web-Server zugreifen. Die Ihnen zugeordnete IP-Adresse finden Sie im Menü “Wartungsstatus bzw. Maintenance Status”, wo sie als WAN-IP-Adresse aufgeführt ist.

Verschiedene Hinweise zu dieser Anwendung:

- Wenn die IP-Adresse Ihres Kontos durch Ihren ISP dynamisch zugewiesen wird, kann sich die IP-Adresse in regelmäßigen Abständen mit Ablauf der DHCP-Vereinbarung ändern.
- Wenn die IP-Adresse des lokalen PC über DHCP zugewiesen wird, kann sie sich beim Neustart des PC ändern. Um dies zu verhindern können Sie den PC manuell konfigurieren und die Verwendung einer festen (statischen) Adresse festlegen.
- Lokale PCs müssen über die lokale LAN-Adresse des PC (in diesem Beispiel 192.168.0.33) auf den lokalen Server zugreifen. Versuche lokaler PCs, über die externe IP-Adresse (in diesem Beispiel 172.16.1.23) auf den Server zuzugreifen, schlagen fehl.

Optionen für die WAN-Konfiguration

Mit den Optionen für die “WAN-Konfiguration bzw. WAN Setup” können Sie einen DMZ-Server konfigurieren, die MTU-Größe ändern und die Beantwortung eines Pings an einem WAN-Port des Routers aktivieren. Diese Optionen werden nachfolgend beschrieben.

Standard-DMZ-Server einrichten

Der Standard-DMZ-Server kann hilfreich sein bei der Verwendung mancher Online-Spiele und Videokonferenz-Anwendungen, die nicht mit NAT kompatibel sind. Der Router MR814 v2 erkennt dank seiner Programmierung einige dieser Anwendungen und kann daher korrekt mit ihnen arbeiten; andererseits gibt es andere Anwendungen, die möglicherweise nicht ordnungsgemäß funktionieren. In manchen Fällen kann die Anwendung auf einem lokalen PC ordnungsgemäß ausgeführt werden, wenn die IP-Adresse dieses PCs als Standard-DMZ-Server eingegeben wird.



Hinweis: DMZ-Server stellen ein Sicherheitsrisiko dar. Ein als Standard-DMZ-Server definierter Computer verliert einen Großteil der Schutzwirkung der Firewall und ist gegen Angriffe aus dem Internet relativ ungeschützt. Somit kann unter Umständen über den DMZ-Server ein Angriff auf Ihr Netzwerk ausgeführt werden.

Eingehende Daten und Nachrichten aus dem Internet werden in der Regel durch den Router gelöscht, falls diese Daten nicht eine Antwort an einen der lokalen Computer oder einen Dienst darstellen, die in dem Menü “Ports” konfiguriert wurden. Anstatt diese Daten und Meldungen zu löschen, können Sie sie an einen Computer im Netzwerk weiterleiten. Dieser Computer wird als Standard-DMZ-Server bezeichnet.

In dem nachfolgend abgebildeten Menü “WAN-Konfiguration bzw. WAN Setup” kann ein Standard-DMZ-Server konfiguriert werden.

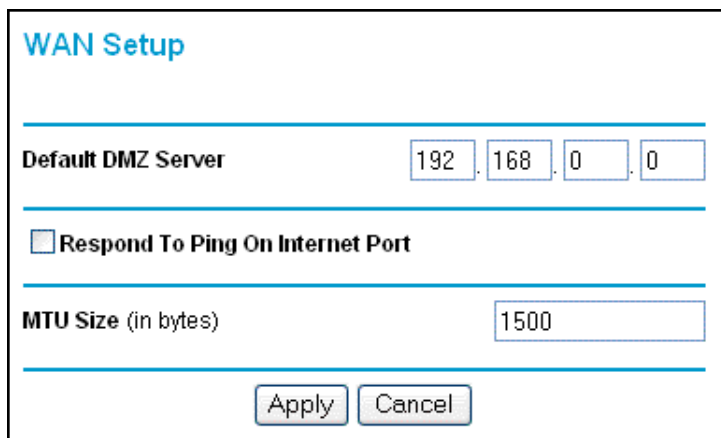


Abbildung 6-2: Menü “WAN-Konfiguration bzw. WAN Setup”

Gehen Sie wie folgt vor, um einen Computer oder Server als Standard-DMZ-Server zu definieren:

1. Klicken Sie im Hauptmenü im Bereich “Erweitert bzw. Advanced” auf den Link “WAN-Konfiguration bzw. WAN Setup”.
2. Geben Sie die IP-Adresse des betreffenden Servers ein. Wenn Sie den Standard-DMZ-Server löschen wollen, geben Sie als IP-Adresse nur Nullen ein.
3. Klicken Sie auf “Anwenden bzw. Apply”.

Ping an Internet-WAN-Anschluss beantworten

Wenn der Router ein “Ping” aus dem Internet beantworten soll, wählen Sie das Markierungsfeld “Ping an Internet-WAN-Port beantworten bzw. Respond to Ping on Internet WAN Port” aus. Diese Funktion sollten Sie nur zu Diagnosezwecke verwenden, da Ihr Router bei Aktivierung dieser Option im Internet sicht- bzw. erkennbar ist. Aktivieren Sie diese Funktion daher nur, wenn gute Gründe dafür sprechen.

MTU-Größe festlegen

Die Standard-MTU-Größe muss in der Regel nicht verändert werden. Der normale MTU-Wert (Maximum Transmit Unit) beträgt für die meisten Ethernet-Netzwerke 1500 Byte. Bei manchen ISPs, insbesondere wenn diese PPPoE verwenden, muss die MTU unter Umständen verringert werden. Nehmen Sie eine derartige Verringerung jedoch nur vor, wenn dies seitens des ISP unbedingt erforderlich ist.

Alle Pakete, die über den Router verschickt werden und die konfigurierte MTU-Größe überschreiten, werden in kleinere Pakete aufgeteilt, die das MTU-Kriterium erfüllen. Gehe Sie wie folgt vor, um die MTU-Größe zu ändern:

1. Geben Sie unter “MTU-Größe bzw. MTU Size” einen neuen Wert zwischen 64 und 1500 ein.
2. Klicken Sie auf “Anwenden bzw. Apply”, um die neue Konfiguration zu aktivieren.

Optionen für LAN-IP-Konfiguration verwenden

Die zweite Optionsmenü unter der Überschrift “Erweitert bzw. Advanced” lautet “LAN-IP-Konfiguration bzw. LAN IP Setup”. In diesem Menü können LAN-IP-Dienste wie DHCP und RIP konfiguriert werden. Klicken Sie im Hauptmenü der Browser-Oberfläche unter der Überschrift “Erweitert bzw. Advanced” auf “LAN-IP-Konfiguration bzw. LAN IP Setup”, um das nachfolgend abgebildete Menü “LAN-IP-Konfiguration bzw. LAN IP Setup” anzuzeigen.

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: RIP-1

Use Router As DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 50

Address Reservation

#	IP Address	Device Name	MAC Address
---	------------	-------------	-------------

Add Edit Delete

Apply Cancel

Abbildung 6-3: Menü “LAN-IP-Konfiguration bzw. LAN IP Setup”

LAN-TCP/IP-Konfigurationsparameter einstellen

Im Auslieferungszustand ist der Router für die Verwendung privater IP-Adressen auf der LAN-Seite und den Einsatz als DHCP-Server vorkonfiguriert. Die Standard-LAN-IP-Konfiguration des Routers lautet:

- LAN-IP-Adresse—192.168.0.1
- Subnetzmaske—255.255.255.0

Diese Adressen sind Teil des von IETF festgelegten, privaten Adressbereichs für die Verwendung in privaten Netzwerken; sie sind für die meisten Anwendungen geeignet. Falls in Ihrem Netzwerk ein anderes IP-Adressierungssystem verwendet werden muss, können Sie die betreffenden Änderungen in diesem Menü vornehmen.

Die LAN-IP-Parameter lauten:

- IP-Adresse bzw. IP Address Dies ist die LAN-IP-Adresse des Routers.
- IP-Subnetzmaske bzw. IP Subnet Mask
Dies ist die LAN-Subnetzmaske des Routers. In Verbindung mit der IP-Adresse ermöglicht die IP-Subnetzmaske einem Gerät die Erkennung der anderen, lokalen Adressen und der über ein Gateway oder einen Router zu erreichenden Adressen.
- RIP-Richtung bzw. RIP Direction
Mit Hilfe des RIP (Router Information Protocol) kann ein Router Routing-Informationen mit anderen Routern austauschen. Über die Auswahl der RIP-Richtung wird festgelegt, wie der Router RIP-Pakete versendet und empfängt. Die Standardeinstellung lautet "Beide bzw. Both".
 - Bei Auswahl von "Beide bzw. Both" oder "Nur ausgehend bzw. Out Only" versendet der Router seinen Routing-Tabelle in regelmäßigen Abständen.
 - Bei Auswahl von "Beide bzw. Both" oder "Nur ankommend bzw. In Only" nimmt der Router die empfangenen RIP-Informationen zur Kenntnis.
 - Bei Auswahl von "Keine bzw. None" versendet der Router keine RIP-Pakete und ignoriert ankommende RIP-Pakete.
- RIP-Version
Über diesen Parameter werden das Format und die Rundsendemethode für die durch den Router versendeten Pakete festgelegt. (Beim Empfang werden beide Formate erkannt.) Die Standardeinstellung lautet RIP-1.
 - RIP-1 wird generell unterstützt. RIP-1 ist für die meisten Netzwerke geeignet, sofern keine ungewöhnliche Netzwerkkonfiguration vorliegt.
 - RIP-2 enthält mehr Informationen. RIP-2B verwendet die Subnetz-Rundsendemethode.



Hinweis: Wenn Sie die LAN-IP-Adresse des Routers ändern, während eine Verbindung zum Browser besteht, wird die Verbindung unterbrochen. Sie müssen dann eine neue Verbindung zu der neuen IP-Adresse herstellen und die Anmeldung wiederholen.

Router als DHCP-Server verwenden .

Der Router arbeitet standardmäßig als DHCP-Server (Dynamic Host Configuration Protocol), der allen Computern, die an das LAN des Routers angeschlossen sind, Adressen für IP- und DNS-Server sowie Standard-Gateways zuweisen kann. Die zugewiesene Standard-Gateway-Adresse ist die LAN-Adresse des Routers. IP-Adressen werden die angeschlossenen PCs aus einem Adressbereich zugewiesen, der in diesem Menü festgelegt wird. Jede Adresse aus diesem Adressbereich wird vor ihrer Zuweisung geprüft, um doppelte Adressen innerhalb des LAN zu vermeiden.

Die Standardeinstellungen für DHCP und TCP/IP sind für die meisten Anwendungen geeignet. Unter "IP-Konfiguration über DHCP" auf Seite B-11 finden Sie eine Erklärung zu DHCP sowie Informationen zur Zuweisung der IP-Adressen in einem Netzwerk.

Falls ein anderes Gerät in Ihrem Netzwerk als DHCP-Server eingesetzt werden soll oder Sie die Netzwerkeinstellungen für alle Computer manuell konfigurieren, heben Sie die Auswahl der Option "Router als DHCP-Server verwenden bzw. Use router as DHCP server" auf. In allen anderen Fällen kann die Option aktiviert bleiben.

Geben Sie den Adressbereich für die Zuordnung der Adressen an, indem Sie die "Erste IP-Adresse bzw. Starting IP Address" und die "Letzte IP-Adresse bzw. Ending IP Address" angeben. Diese Adressen sollten zu demselben IP-Adress-Subnetz gehören wie die LAN-IP-Adresse des Routers. Bei einem Standard-Adressierungssystem sollten Sie einen Bereich zwischen 192.168.0.2 und 192.168.0.253 festlegen; allerdings können Sie einen Teil dieses Bereichs für Geräte mit festen Adressen reservieren.

Der Router übergibt jedem LAN-Gerät, das DHCP anfordert, folgende Parameter:

- Eine IP-Adresse aus dem Bereich, den Sie festgelegt haben.
- Subnetzmaske
- Gateway-IP-Adresse (LAN-IP-Adresse des Routers)
- Primärer DNS-Server (sofern in dem Menü "Grundeinstellungen bzw. Basic Settings" eine primäre DNS-Adresse eingegeben wurde; andernfalls die LAN-IP-Adresse des Routers)
- Sekundärer DNS-Server (sofern in dem Menü "Grundeinstellungen bzw. Basic Settings" eine sekundäre DNS-Adresse eingegeben wurde;

Adressen reservieren

Wenn Sie eine reservierte IP-Adresse für eine PC im LAN festlegen, erhält der betreffende PC bei jedem Zugriff auf den DHCP-Server des Routers dieselbe IP-Adresse. Servern, für die permanente IP-Einstellungen erforderlich sind, sollten reservierte IP-Adressen zugewiesen werden.

Gehen Sie wie folgt vor, um eine IP-Adresse zu reservieren:

1. Klicken Sie auf die Schaltfläche "Hinzufügen bzw. Add".
2. Geben Sie in dem Feld "IP-Adresse bzw. IP Address" die IP-Adresse ein, die dem PC oder Server zugewiesen werden soll. (Verwenden Sie dabei eine IP-Adresse aus dem LAN-Subnetz des Routers, z. B. 192.168.0.X.)
3. Geben Sie die MAC-Adresse des PCs oder Servers ein.
(Tipp: Wenn der PC bereits im Netzwerk definiert ist, können Sie die MAC-Adresse in dem Menü "Angeschlossene Geräte bzw. Attached Devices" kopieren und hier einfügen.)
4. Klicken Sie auf "Anwenden bzw. Apply", um die reservierte Adresse in die Tabelle aufzunehmen.

Hinweis:Die reservierte Adresse wird erst zugewiesen, wenn der PC das nächste Mal mit dem DHCP-Server des Routers Verbindung aufnimmt. Starten Sie den PC neu oder greifen Sie auf die IP-Konfiguration des PCs zu, um eine DHCP-Freigabe und -Aktualisierung zu erzwingen.

Gehen Sie wie folgt vor, um einen reservierten Adresseintrag zu bearbeiten oder zu löschen:

1. Wählen Sie das Markierungsfeld neben der reservierten Adresse aus, die Sie bearbeiten oder löschen wollen.
2. Klicken Sie auf “Bearbeiten bzw. Edit” oder “Löschen bzw. Delete”.

Dynamischen DNS-Dienst verwenden

Wenn Ihr Netzwerk über eine permanent zugeordnete IP-Adresse verfügt, können Sie einen Domain-Namen registrieren und über öffentliche Domain Name Server (DNS) einen Link zu Ihrer IP-Adresse einrichten lassen. Wenn Ihr Internet-Konto jedoch eine dynamisch zugeordnete IP-Adresse verwendet, kennen Sie Ihre IP-Adresse nicht im Voraus; außerdem kann sich die Adresse häufig ändern. In diesem Fall können Sie einen kommerziellen dynamischen DNS-Dienst verwenden, der Ihnen die Registrierung Ihrer Domain auf der IP-Adresse des Dienstes ermöglicht und alle an Ihre Domain gerichteten Meldungen und Daten an Ihre häufig wechselnde IP-Adresse weiterleitet.



Hinweis: Wenn Ihnen Ihr ISP eine private WAN-IP-Adresse (z. B. 192.168.x.x oder 10.x.x.x) zuweist, funktioniert der dynamische DNS-Dienst nicht, da private Adressen im Internet nicht weitergeleitet werden.

Der Router enthält einen Client, der eine Verbindung zu zahlreichen, gängigen dynamischen DNS-Diensten herstellen kann. Sie können einen dieser Dienste auswählen und dort ein Konto einrichten. Sobald dann Ihre durch den ISP zugewiesene IP-Adresse wechselt, nimmt Ihr Router automatisch mit dem dynamischen DNS-Dienst auf, meldet sich unter Ihrem Konto an und registriert Ihre neue IP-Adresse.

Klicken Sie im Hauptmenü der Browser-Oberfläche unter “Erweitert bzw. Advanced” auf “Dynamischer DNS bzw. Dynamic DNS”. Gehen Sie wie folgt vor, um die dynamische DNS-Funktion zu konfigurieren:

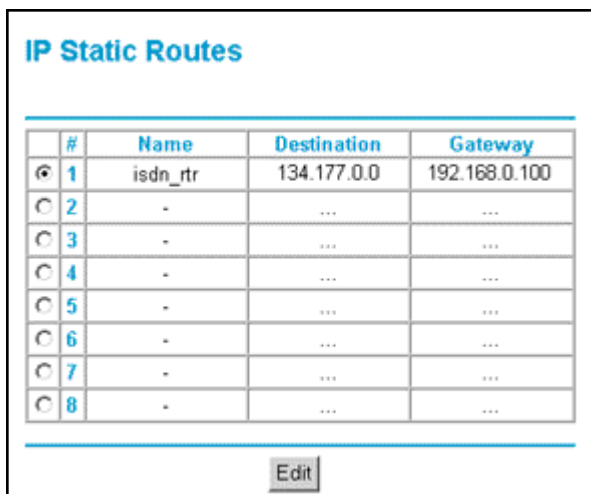
1. Richten Sie bei einem der Anbieter dynamischer DNS-Dienste, die in dem Feld “Service Provider auswählen bzw. Select Service Provider” aufgeführt werden, ein Konto ein. Beispiel: Wählen Sie für dyndns.org das Konto www.dyndns.org.
2. Wählen Sie das Markierungsfeld “Dynamischen DNS-Dienst verwenden bzw. Use a dynamic DNS service” aus.
3. Wählen Sie den Namen eines Providers eines dynamischen DNS-Dienstes aus.
4. Geben Sie den Host-Namen (oder Domain-Namen) ein, den Sie von dem Provider des dynamischen DNS-Dienstes erhalten haben.
5. Geben Sie den Benutzernamen des dynamischen DNS-Kontos ein.
6. Geben Sie das Kennwort (oder den Code) des dynamischen DNS-Kontos ein.

7. Falls der Provider des dynamischen DNS-Dienstes die Verwendung von Platzhalterzeichen bei der Darstellung Ihrer URL zulässt, können Sie das Markierungsfeld "Platzhalterzeichen verwenden bzw. Use wildcards" auswählen, um diese Funktion zu aktivieren. Beispielsweise wird über diese Funktion der Ausdruck *.yourhost.dyndns.org derselben IP-Adresse zugeordnet wie yourhost.dyndns.org.
8. Klicken Sie auf "Anwenden bzw. Apply", um die Konfiguration zu speichern.

Statische Routen konfigurieren

Statische Routen liefern Ihrem Router zusätzliche Routing-Informationen. Unter normalen Umständen verfügt der Router nach der Konfiguration des Internet-Zugangs über ausreichende Routing-Informationen, sodass keine zusätzlichen statischen Routen konfiguriert werden müssen. Statische Routen sind nur in Ausnahmesituationen erforderlich, z. B. wenn sich mehrere Router oder mehrere IP-Subnetze in einem Netzwerk befinden.

Klicken Sie im Hauptmenü der Browser-Oberfläche unter der Überschrift "Erweitert bzw. Advanced" auf "Statische Routen bzw. Static Routes", um das Menü "Statische Routen bzw. Static Routes" (siehe unten) anzuzeigen.

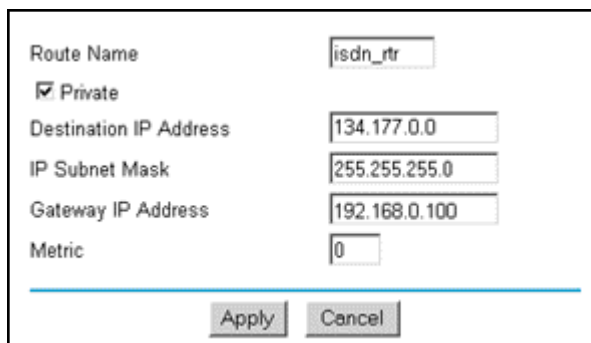


#	Name	Destination	Gateway
1	isdn_rtr	134.177.0.0	192.168.0.100
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Abbildung 6-4: Tabelle mit Zusammenfassung der statischen Routen

Gehen Sie wie folgt vor, um eine statische Route hinzuzufügen oder zu bearbeiten:

1. Klicken Sie auf die Schaltfläche “Hinzufügen bzw. Add”, um das Menü “Hinzufügen/Bearbeiten bzw. Add/Edit” (siehe unten) anzuzeigen.



Route Name	isdn_rtr
<input checked="" type="checkbox"/> Private	
Destination IP Address	134.177.0.0
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.0.100
Metric	0

Apply Cancel

Abbildung 6-5. Menü für die Eingabe und Bearbeitung statischer Routen

2. Geben Sie in dem Feld “Routenname bzw. Route Name” unter der Tabelle einen Namen für die statische Route ein. (Diese Name dient nur zur Wiedererkennung.)
3. Wählen Sie “Privat bzw. Private” aus, wenn nur ein Zugang zum LAN möglich sein soll. Die statische Route wird in RIP nicht dargestellt.
4. Wählen Sie “Aktiv bzw. Active” aus, um diese Route zu aktivieren.
5. Geben Sie die “Ziel-IP-Adresse bzw. Destination IPAddress” ein.
6. Geben Sie die “IP-Subnetzmaske bzw. IP Subnet Mask” für dieses Ziel ein. Wenn es sich bei dem Ziel um einen einzelnen Host handelt, geben Sie 255.255.255.255 ein.
7. Geben Sie die “Gateway-IP-Adresse bzw. Gateway IPAddress” ein bei der es sich um einen Router in demselben LAN-Segment wie Ihr Router handeln muss.
8. Geben Sie für “Anzahl bzw. Metric” einen Wert zwischen 1 und 15 ein. Diese Zahl stellt die Anzahl der Router zwischen Ihrem Netzwerk und dem Ziel dar. In der Regel ist der Wert 2 oder 3 geeignet, doch können Sie den Wert bei einer direkten Verbindung auf 1 setzen.
9. Klicken Sie auf “Anwenden bzw. Apply”, um die statische Route der Tabelle hinzuzufügen.

In dem folgenden Beispiel ist eine statische Route erforderlich:

- Der primäre Internet-Zugang erfolgt über eine Verbindung per Kabelmodem zu einem ISP.
- Sie verfügen in Ihrem Privatbüro über einen ISDN-Router, über den Sie eine Verbindung zu dem Unternehmen herstellen können, bei dem Sie beschäftigt sind. Die Adresse des Routers im LAN lautet 192.168.0.100.
- Die Adresse des Netzwerks Ihres Unternehmens lautet 134.177.0.0.

Bei der erstmaligen Konfiguration des Routers wurden zwei statische Routen automatisch erzeugt. Ein Standardleitweg wurde unter Verwendung Ihres ISP als Gateway erzeugt, und eine zweite statische Route wurde in Ihrem lokalen Netzwerk für alle Adressen mit 192.168.0.x erzeugt. Wenn Sie in dieser Konfiguration versuchen, auf ein Gerät im Netzwerk 134.177.0.0 zuzugreifen, leitet Ihr Router die Anfrage an den ISP weiter. Der ISP wiederum leitet die Anfrage an das Unternehmen weiter, bei dem Sie beschäftigt sind, wo die Anfrage höchstwahrscheinlich durch die Firewall des Unternehmens blockiert wird.

In diesem Fall müssen Sie eine statische Route definieren, durch den Ihr Router angewiesen wird, über den ISDN-Router unter 192.168.0.100 auf das Netzwerk 134.177.0.0 zuzugreifen. Eine mögliche statische Route für diesen Zweck ist in Abbildung 5-5 dargestellt.

Bei diesem Beispiel ist Folgendes zu beachten:

- In den Feldern “Ziel-IP-Adresse bzw. Destination IP Address” und “IP-Subnetzmaske bzw. IP Subnet Mask” wird angegeben, dass die betreffende statische Route für alle Adressen mit 134.177.x.x gilt.
- In dem Feld “Gateway-IP-Adresse bzw. Gateway IPAddress” wird angegeben, dass alle an diese Adressen gerichteten Meldungen und Daten an den ISDN-Router unter 192.168.0.100 weiterzuleiten sind.
- Als “Anzahl bzw. Metric” kann der Wert 1 eingegeben werden, das sich der ISDN-Router im LAN befindet.
- “Privat bzw. Private” wird nur als vorbeugende Sicherheitsmaßnahme für den Fall einer Aktivierung von RIP ausgewählt.

Zugriff für dezentrale Verwaltung aktivieren

Auf der Seite “Dezentrale Verwaltung bzw. Remote Management” können Sie einem oder mehreren Benutzern im Internet gestatten, für Ihren Router MR814 v2 eine Konfiguration, ein Upgrade oder eine Statusabfrage durchzuführen.



Hinweis: Achten Sie darauf, dass als Standardkennwort für die Konfiguration des Routers ein besonders sicheres Kennwort festgelegt ist. Das ideale Kennwort sollte keine in einem Wörterbuch einer beliebigen Sprache aufgeführten Wörter enthalten und eine Mischung aus Buchstaben (Groß- und Kleinbuchstaben), Zahlen und Symbolen darstellen. Die maximale Länge beträgt 30 Zeichen.

Gehen Sie wie folgt vor, um den Router für die dezentrale Verwaltung zu konfigurieren:

1. Wählen Sie das Markierungsfeld “Dezentrale Verwaltung ein bzw. Turn Remote Management On” aus.
2. Geben Sie die externe Adresse ein, die einen Zugriff auf die dezentrale Verwaltung des Routers erhalten sollen.

Hinweis: Aus Sicherheitsgründen sollten Sie diesen Zugriff auf möglichst wenige externe IP-Adressen beschränken.

- a. Wenn Sie den Zugriff von jeder beliebigen IP-Adresse im Internet gestatten wollen, wählen Sie “Alle bzw. Everyone” aus.

- b. Wenn der Zugriff für einen Bereich von IP-Adressen im Internet freigegeben werden soll, wählen Sie einen IP-Adressbereich aus. Geben Sie hierfür die erste und die letzte IP-Adresse des zugelassenen Bereichs ein.
 - c. Wenn nur eine einzelne IP-Adresse im Internet einen Zugriff erhalten soll, wählen Sie “Nur dieser PC bzw. Only this PC” aus. Geben Sie die IP-Adresse ein, die einen Zugriff erhalten soll.
3. Geben Sie die Port-Nummer ein, die für den Zugriff auf die Verwaltungsschnittstelle verwendet wird.

Für den Web-Browser-Zugriff wird in der Regel der Standard-HTTP-Port 80 verwendet. Zur Verstärkung der Sicherheit können Sie für die Web-Schnittstelle für die dezentrale Verwaltung einen kundenspezifischen Port festlegen, dessen Nummer Sie einfach in dem betreffenden Feld eingeben. Wählen Sie dafür eine Zahl zwischen 1024 und 65535 aus, aber verwenden Sie keinen Port eines gängigen Dienstes. Der Standardwert lautet 8080, der häufig als Alternativwert für HTTP verwendet wird..

4. Klicken Sie auf “Anwenden bzw. Apply”, um die Änderungen zu aktivieren.

Hinweis: Wenn Sie über das Internet auf Ihren Router zugreifen, geben Sie die WAN-IP-Adresse Ihres Routers in dem Feld “Adresse bzw. Address” (Internet Explorer) oder “Standort bzw. Location” (Netscape), gefolgt von einem Doppelpunkt (:) und der kundenspezifischen Port-Nummer ein. Wenn beispielsweise Ihre externe Adresse 134.177.0.123 lautet und Sie die Port-Nummer 8080 verwenden, müssen Sie in Ihrem Browser Folgendes eingeben:

`http://134.177.0.123:8080`

Universal Plug and Play (UPnP) verwenden

Universal Plug and Play (UPnP) ermöglicht Geräten, z. B. Internet-Geräten und Computern, auf das Netzwerk zuzugreifen und Verbindungen zu anderen Geräten herzustellen. UPnP-Geräte erkennen automatisch die Dienste, die von anderen registrierten UPnP-Geräten im Netzwerk angeboten werden.

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Abbildung 6-6. Menü “UPnP”

Klicken Sie im Hauptmenü der Browser-Oberfläche unter “Erweitert bzw. Advanced” auf “UPnP”. Richten Sie UPnP entsprechend der nachfolgenden Anleitung ein.

UPnP aktivieren bzw. Turn UPnP On: UPnP kann für die automatische Gerätekonfiguration aktiviert oder deaktiviert werden. In der Standardeinstellung ist UPnP aktiviert. Bei Deaktivierung ist kein anderes Gerät in der Lage, automatisch die Ressourcen, z. B. die Port-Weiterleitung (Mapping), des Routers zu steuern.

Rundsendefrequenz bzw. Advertisement Period: Dieser Parameter gibt an, wie oft der Router seine UPnP-Informationen per Rundsendung bekanntgibt. Dabei kann ein Wert zwischen 1 und 1440 Minuten festgelegt werden. Die Standardeinstellung lautet 30 Minuten. Bei einer kürzeren Frequenz ist sichergestellt, dass die Schaltpunkte immer über den aktuellen Gerätestatus verfügen; allerdings wird hierdurch zusätzlicher Verkehr im Netzwerk erzeugt. Bei einer längeren Frequenz ist der Gerätestatus unter Umständen nicht immer aktuell, doch dafür wird der Netzwerkverkehr signifikant reduziert.

Rundsendedauer bzw. Advertisement Time To Live: Die Rundsendedauer wird für jedes gesendete UPnP-Paket in Stufen (oder Schritten) gemessen. Der für die Rundsendedauer festgelegte Wert ist die Anzahl der Weitergabeschritte, die ein Rundsendepaket bei der UPnP-Ankündigung durchlaufen kann, bevor es verschwindet. Die Anzahl dieser Weitergabeschritte kann zwischen 1 und 255 liegen. Der Standardwert für die Rundsendedauer ist vier Schritte; dieser Wert ist für die meisten privaten Netzwerke geeignet. Sollten Sie feststellen, dass manche Geräte nicht ordnungsgemäß aktualisiert oder erreicht werden, muss dieser Wert unter Umständen erhöht werden.

UPnP-Port-Zuordnungstabelle bzw. UPnP Portmap Table: Die UPnP-Port-Zuordnungstabelle enthält die IP-Adressen aller UPnP-Geräte, die aktuell auf den Router zugreifen, sowie die durch die einzelnen Geräte geöffneten Ports (intern und extern). In der UPnP-Port-Zuordnungstabelle werden außerdem der Typ der geöffneten Ports sowie die Information angezeigt, ob der betreffende Port nach wie vor für jede IP-Adresse aktiv ist.


Kapitel 7

Fehlerbehebung

Dieses Kapitel enthält Informationen zur Fehlersuche und -behebung bei dem Kabel-/DSL-Wireless-Router Modell MR814 v2. Nach jeder Problembeschreibung finden Sie Anweisungen zur Diagnose und Behebung des jeweiligen Problems.

Grundbetrieb

Wenn Sie den Router einschalten, sollten nacheinander folgende Ereignisse eintreten:

1. Vergewissern Sie sich beim erstmaligen Einschalten, dass die Netz-LED  leuchtet.
2. Vergewissern Sie sich nach etwa 10 Sekunden, dass
 - a. die Test-LED nicht leuchtet.
 - b. die LAN-Port-LEDs für alle verbundenen lokalen Ports leuchten.
 - c. die WAN-Port-LED leuchtet.

Wenn die LED eines Ports leuchtet, bedeutet dies, dass eine Verbindung zu dem angeschlossenen Gerät hergestellt wurde. Wenn ein LAN-Port mit einem 100 MBit/s-Gerät verbunden ist, muss die LED des Ports grün leuchten. Bei einem 10 MBit/s-Port leuchtet die LED gelb.

Falls keine dieser Bedingungen erfüllt ist, lesen Sie in den nachfolgenden Abschnitten nach.

Netz-LED leuchtet nicht

Wenn die Netz-LED und andere LEDs nach dem Einschalten des Routers nicht leuchten, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass das Netzkabel ordnungsgemäß an dem Router angeschlossen und das Netzteil ordnungsgemäß mit einer betriebsbereiten Netzsteckdose verbunden ist.
- Vergewissern Sie sich, dass Sie das von NETGEAR zu diesem Produkt mitgelieferte Netzteil mit 7,5 V Gleichspannung angeschlossen haben.

Falls der Fehler weiterhin auftritt, liegt ein Hardware-Problem vor und Sie sollten sich an den technischen Support wenden.

Test-LED leuchtet nicht oder leuchtet permanent

Nach dem Einschalten des Routers leuchtet die Test-LED etwa 10 Sekunden lang und erlischt dann. Wenn die Test-LED nicht leuchtet oder permanent leuchtet, liegt ein Router-Fehler vor.

Wenn alle LEDs einschließlich der Test-LED eine Minute nach dem Einschalten des Routers nach wie vor leuchten, gehen Sie wie folgt vor:

- Schalten Sie die Netzspannung aus und wieder ein und überprüfen Sie, ob der Router-Fehler damit behoben wurde.
- Setzen Sie die Konfiguration des Routers auf die werksseitigen Standardeinstellungen zurück. Damit lautet die IP-Adresse des Routers wieder 192.168.0.1. Die empfohlene Vorgehensweise wird unter “Standardkonfiguration und -kennwort wiederherstellen” auf Seite 7-7 beschrieben.

Falls der Fehler weiterhin auftritt, liegt möglicherweise ein Hardware-Problem vor und Sie sollten sich an den technischen Support wenden.

LEDs für LAN- oder WAN-Port leuchten nicht

Wenn die LAN-LEDs oder die WAN-LED nach Herstellen einer Ethernet-Verbindung nicht leuchten, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass das Ethernet-Kabel ordnungsgemäß mit dem Router und dem Hub oder der Workstation verbunden ist.
- Vergewissern Sie sich, dass der angeschlossene Hub bzw. die angeschlossene Workstation eingeschaltet ist.
- Vergewissern Sie sich, dass Sie das korrekte Kabel angeschlossen haben:
 - Bei Verbindung des WAN-Ports des Routers mit einem Kabel- oder DSL-Modem verwenden Sie das Kabel, das zusammen mit dem Kabel- oder DSL-Modem geliefert wurde. Hierbei kann es sich um ein Standard-Ethernet-Durchgangskabel oder ein Ethernet-Crossover-Kabel handeln.

Fehlerbehebung an der Schnittstelle für die Web-Konfiguration

Wenn Sie von einem PC in Ihrem lokalen Netzwerk aus nicht auf die Web-Konfigurationsschnittstelle des Routers zugreifen können, gehen Sie wie folgt vor:

- Überprüfen Sie die Ethernet-Verbindung zwischen PC und Router wie im vorherigen Abschnitt beschrieben.
- Vergewissern Sie sich, dass die IP-Adresse Ihres PC sich in demselben Subnetz befindet wie der Router. Wenn Sie das empfohlene Adressierungssystem verwenden, sollte die Adresse Ihres PC in dem Bereich von 192.168.0.2 bis 192.168.0.254 liegen. Wie Sie die IP-Adresse Ihres PC ermitteln können, wird unter “TCP/IP-Eigenschaften überprüfen” auf Seite 4-5 und “TCP/IP-Eigenschaften für Macintosh überprüfen” auf Seite 4-8 beschrieben. Konfigurieren Sie den PC entsprechend der Anleitung in Kapitel 4.

Hinweis: Wenn die IP-Adresse Ihres PC 169.254.x.x lautet: Jüngere Versionen von Windows und MacOS erzeugen eine IP-Adresse und weisen diese zu, wenn der Computer keinen DHCP-Server erreicht. Diese automatisch generierten Adressen liegen im Adressbereich von 169.254.x.x. Falls Ihre IP-Adresse in diesem Bereich liegt, überprüfen Sie die Verbindung zwischen PC und Router und starten Sie den PC neu.

- Wenn die IP-Adresse Ihres Routers geändert wurde und Sie die aktuelle IP-Adresse nicht kennen, setzen Sie die Konfiguration des Routers auf die werksseitigen Standardeinstellungen zurück. Damit lautet die IP-Adresse des Routers wieder 192.168.0.1. Die empfohlene Vorgehensweise wird unter “Standardkonfiguration und -kennwort wiederherstellen” auf Seite 7-7 beschrieben.
- Vergewissern Sie sich, dass Java, JavaScript oder ActiveX auf Ihrem Browser aktiviert ist. Wenn Sie mit dem Internet Explorer arbeiten, klicken Sie auf “Aktualisieren bzw. Refresh”, um sicherzustellen, dass das Java-Applet geladen wurde.
- Beenden Sie den Browser und starten Sie ihn erneut.
- Vergewissern Sie sich, dass Sie die korrekten Anmeldeinformationen angegeben haben. Die werksseitige Standardeinstellung für den Anmeldenamen lautet “admin”, das Standard-Kennwort heißt “password”. Achten Sie darauf, dass die Feststelltaste bei der Eingabe dieser Daten nicht gedrückt ist.

Wenn die Änderungen, die Sie an der Web-Konfigurationsschnittstelle vorgenommen haben, nicht auf dem Router gespeichert werden, gehen Sie wie folgt vor:

- Klicken Sie bei der Eingabe der Konfigurationseinstellungen unbedingt auf die Schaltfläche “Anwenden bzw. Apply”, bevor Sie in dem nächsten Menü oder der nächsten Registerkarte fortfahren; andernfalls sind die Änderungen verloren.
- Klicken Sie in dem Web-Browser auf die Schaltfläche “Aktualisieren bzw. Refresh” oder “Neu laden bzw. Reload”. Möglicherweise wurden die Änderungen vorgenommen, doch der Web-Browser verwendet noch die alte Konfiguration aus dem Zwischenspeicher.

Fehlerbehebung bei der ISP-Verbindung

Wenn Ihr Router keinen Zugriff auf das Internet hat, sollten Sie zunächst überprüfen, ob der Router in der Lage ist, eine WAP-IP-Adresse von Ihrem ISP zu empfangen. Sofern Ihnen keine statische IP-Adresse zugewiesen wurde, muss Ihr Router bei dem ISP eine IP-Adresse anfordern. Mit Hilfe des Web-Konfigurationsmanagers können Sie feststellen, ob diese Anforderung erfolgreich war.

Gehen Sie wie folgt vor, um die WAN-IP-Adresse zu überprüfen:

1. Starten Sie Ihren Browser und wählen Sie eine externe Webseite, z. B. www.netgear.de.
2. Öffnen Sie das Hauptmenü der Router-Konfiguration unter <http://192.168.0.1>.
3. Wählen Sie unter der Überschrift "Wartung bzw. Maintenance" die Option "Router Status" aus.
4. Vergewissern Sie sich, dass für den WAN-Port eine IP-Adresse angezeigt wird. Wenn die angezeigte Adresse 0.0.0.0 lautet, hat Ihr Router keine IP-Adresse von Ihrem ISP erhalten.

Wenn Ihr Router keine IP-Adresse von Ihrem ISP empfangen hat, müssen Sie Ihr Kabel- oder DSL-Modem unter Umständen zwingen, den neuen Router zu erkennen; gehen Sie dabei wie folgt vor:

1. Schalten Sie das Kabel- oder DSL-Modem aus.
2. Schalten Sie den Router aus.
3. Schalten Sie das Kabel- oder DSL-Modem nach fünf Minuten wieder ein.
4. Wenn die LEDs des Modems anzeigen, dass die Synchronisierung mit dem ISP abgeschlossen ist, schalten Sie auch den Router wieder ein.

Wenn Ihr Router weiterhin keine IP-Adresse von Ihrem ISP empfängt, hat das Problem möglicherweise eine der folgenden Ursachen:

- Für Ihren ISP ist ein Anmeldeprogramm erforderlich.
Erkundigen Sie sich bei Ihrem ISP, ob PPP over Ethernet (PPPoE) oder ein anderes Anmeldeprogramm erforderlich ist.
- Wenn für Ihren SIP eine Anmeldung erforderlich ist, wurden der Anmeldename und das Kennwort unter Umständen nicht korrekt eingegeben.
- Ihr ISP überprüft möglicherweise den Host-Namen Ihres PCs.
Geben Sie im Menü "Grundeinstellungen bzw. Basic Settings" als "Kontoname bzw. Account Name" den Host-Namen des PCs mit Ihrem ISP-Konto ein.
- Ihr ISP gestattet nur eine Verbindung von einer Ethernet-MAC-Adresse in das Internet und überprüft die MAC-Adresse Ihres PCs. Gehen Sie in diesem Fall wie folgt vor:

Informieren Sie Ihren ISP darüber, dass Sie ein neues Netzwerkgerät erworben haben, und bitten Sie den ISP, die MAC-Adresse des Routers zu verwenden.

ODER

Konfigurieren Sie Ihren Router so, dass er die MAC-Adresse Ihres PC ermittelt. Auch dies ist im Menü “Grundeinstellungen bzw. Basic Settings” möglich. Weitere Informationen finden Sie unter “Manuelle Konfiguration der Internet-Verbindung” auf Seite 2-15.

Wenn Ihr Router eine IP-Adresse empfangen kann, der PC jedoch keine Web-Seiten aus dem Internet laden kann, gehen Sie wie folgt vor:

- Ihr PC erkennt möglicherweise keine DNS-Server-Adressen.

Ein DNS-Server ist ein Host im Internet, der Internet-Name (z. B. www-Adressen) in numerische IP-Adressen umsetzt. In der Regel erhalten Sie von Ihrem ISP die Adressen von einem oder zwei DNS-Servern, den/die Sie verwenden können. Wenn Sie während der Konfiguration des Routers eine DNS-Adresse eingegeben haben, starten Sie den PC neu und überprüfen Sie die DNS-Adresse (siehe hierzu “TCP/IP-Eigenschaften überprüfen” auf Seite 4-5. Alternativ dazu können Sie die DNS-Adressen auch manuell auf Ihrem PC konfigurieren; die entsprechende Vorgehensweise wird in der Dokumentation zu Ihrem Betriebssystem beschrieben.

- Auf Ihrem PC ist der Router möglicherweise nicht als TCP/IP-Gateway konfiguriert.

Wenn Ihr PC die erforderlichen Informationen von dem Router über DHCP erhält, starten Sie den PC neu und überprüfen Sie die Gateway-Adresse (siehe hierzu “TCP/IP-Eigenschaften überprüfen” auf Seite 4-5.

Fehlerbehebung in einem TCP/IP-Netzwerk mit einem Ping-Dienstprogramm

Die meisten TCP/IP-Endgeräte und -Router enthalten ein Ping-Dienstprogramm, das ein Echoanforderungspaket an das Zielgerät sendet. Das Zielgerät sendet daraufhin ein Echo als Antwort. Die Fehlersuche und -behebung in einem TCP/IP-Netzwerk ist dank des Ping-Dienstprogramms auf Ihrem PC oder Ihrer Workstation sehr einfach.

LAN-Pfad zum Router prüfen

Sie können von Ihrem PC aus ein Ping an den Router senden um zu überprüfen, ob der LAN-Pfad zu Ihrem Router korrekt eingerichtet ist.

Gehen Sie wie folgt vor, um von einem PC mit Windows 95 oder höher eine Ping-Anforderungen an den Router zu senden:

1. Klicken Sie in der Windows Taskleiste auf “Start” und wählen Sie “Ausführen bzw. Run” aus.
2. Geben Sie in dem Feld, das daraufhin angezeigt wird, “Ping” gefolgt von der IP-Adresse des Routers ein, z. B.:

```
ping 192.168.0.1
```

3. Klicken Sie auf OK.

Daraufhin sollte eine Meldung angezeigt werden, die etwa den folgenden Inhalt hat:

```
Pinging <IP address> with 32 bytes of data
```


Wenn der Pfad in Ordnung ist, wird folgende Meldung angezeigt:

```
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```

Wenn der Pfad nicht in Ordnung ist, wird folgende Meldung angezeigt:

```
Request timed out
```

Wenn der Pfad nicht in Ordnung ist, kann dies verschiedene Gründe haben:

- Falsche physikalische Verbindungen
 - Vergewissern Sie sich, dass die LED des LAN-Ports leuchtet. Wenn die LED nicht leuchtet, folgen Sie den Anweisungen unter "LEDs für LAN-Port oder WAN-Port leuchten nicht" auf Seite 7-2.
 - Vergewissern Sie sich, dass die betreffenden Verbindungs-LEDs für die Netzwerkschnittstellenkarte und die Hub-Ports (sofern vorhanden), die mit Ihrer Workstation und Ihrem Router verbunden sind, leuchten.
- Falsche Netzwerkkonfiguration
 - Vergewissern Sie sich, dass die Treibersoftware der Ethernet-Karte und die TCP/IP-Software auf Ihrem PC oder Ihrer Workstation installiert und konfiguriert wurden.
 - Vergewissern Sie sich, dass die IP-Adresse Ihres Routers und Ihrer Workstation korrekt sind und sich beide Adressen in demselben Subnetz befinden.

Pfad von PC zu einem dezentralen Gerät prüfen

Nachdem Sie sich davon überzeugt haben, dass der LAN-Pfad korrekt ist, überprüfen Sie den Pfad von Ihrem PC zu einem dezentralen Gerät. Wählen Sie in Windows "Start" und dann die Option "Ausführen bzw. Run" aus und geben Sie folgenden Befehl ein:

```
PING -n 10 <IP address>
```

Dabei ist *<IP address>* die IP-Adresse eines dezentralen Geräts, z. B. des DNS-Servers Ihres ISPs.

Wenn der Pfad korrekt ist, werden die im vorherigen Abschnitt dargestellten Antworten angezeigt. Wenn Sie diese Antworten nicht erhalten, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass die IP-Adresse Ihres Routers auf Ihrem PC als Standard-Gateway definiert ist. Wenn die IP-Konfiguration Ihres PC durch DHCP festgelegt wird, sind diese Informationen im Netzwerksteuerungsfenster Ihres PC nicht dargestellt. Gehen Sie entsprechend der Beschreibung unter "TCP/IP-Eigenschaften überprüfen" auf Seite 4-5 vor, um zu überprüfen, ob die IP-Adresse des Routers als Standard-Gateway definiert ist.
- Vergewissern Sie sich, dass die Netzwerkadresse Ihres PCs (der Teil der IP-Adresse, der durch die Netzmaske angegeben ist) nicht mit der Netzwerkadresse des dezentralen Geräts identisch ist.
- Vergewissern Sie sich, dass Ihr Kabel- oder DSL-Modem angeschlossen und betriebsbereit ist.

- Wenn Ihrem PC von Ihrem SIP ein Host-Name zugewiesen wurde, geben Sie diesen Host-Namen im Menü “Grundeinstellungen bzw. Basic Settings” als “Kontoname bzw. Account Name” ein.
- Unter Umständen weist Ihr ISP die Ethernet-MAC-Adressen aller Ihrer PCs mit Ausnahme eines PCs zurück. Zahlreiche Breitband-ISPs beschränken den Zugriff, indem Sie nur Datenübertragungen von der MAC-Adresse Ihres Breitbandmodems zulassen; manche ISPs haben jedoch eine zusätzliche Beschränkung vorgesehen, indem Sie nur der MAC-Adresse eines einzelnen PC, der mit diesem Modem verbunden ist, einen Zugriff ermöglichen. Wenn dies der Fall ist, müssen Sie Ihren Router so konfigurieren, dass er die MAC-Adresse des freigegebenen PCs erkennt und verwendet. Weitere Informationen finden Sie unter “Manuelle Konfiguration der Internet-Verbindung” auf Seite 2-15.

Standardkonfiguration und -kennwort wieder herstellen

In diesem Abschnitt wird erläutert, wie Sie die Konfiguration auf die werksseitigen Standardeinstellungen zurücksetzen, das Administratorkennwort des Routers auf “password” setzen und die IP-Adresse auf 192.168.0.1 setzen können. Sie haben zwei Möglichkeiten, die aktuelle Konfiguration zu löschen und die werksseitigen Standardeinstellungen wiederherzustellen:

- Mit der Funktion “Löschen bzw. Erase” des Routers (siehe “Konfiguration löschen” auf Seite 5-8).
- Mit der Taste zum Zurücksetzen auf die Standardeinstellungen an der Rückseite des Routers. Wenden Sie diese Methode an, wenn das Administratorkennwort oder die IP-Adresse nicht bekannt ist.

Wenn Sie die werksseitigen Standardeinstellungen wiederherstellen wollen und das Administratorkennwort oder die IP-Adresse nicht kennen, müssen Sie die Taste zum Zurücksetzen auf die Standardeinstellungen an der Rückseite des Routers drücken.

1. Drücken Sie die Taste zum Zurücksetzen und halten Sie sie gedrückt, bis die Test-LED leuchtet (etwa 10 Sekunden).
2. Geben Sie die Taste zum Zurücksetzen frei und warten Sie, bis der Router neu gestartet wurde.

Probleme bei Datum und Uhrzeit

In dem Menü “E-Mail” werden in dem Bereich “Content Filtering” das aktuelle Datum und die aktuelle Uhrzeit angezeigt. Der Router MR814 v2 verwendet das Network Time Protocol (NTP), um die aktuelle Uhrzeit bei einem der zahlreichen Network Time Server im Internet abzufragen. Jeder Eintrag im Protokoll wird mit Datum und Uhrzeit gespeichert. Bei der Funktion für das Datum und die Uhrzeit können folgende Probleme auftreten:

- Als Datum wird der 1. Januar 2000 angezeigt. Ursache: Der Router konnte noch keinen Network Time Server erreichen. Vergewissern Sie sich, dass Ihre Einstellungen für den Internet-Zugang korrekt konfiguriert sind. Wenn Sie die Konfiguration des Routers gerade erst abgeschlossen haben, warten Sie mindestens fünf Minuten, und prüfen Sie dann nochmals das Datum und die Uhrzeit.
- Die angezeigte Uhrzeit weicht um eine Stunde von der tatsächlichen Uhrzeit ab. Ursache: Der Router erkennt nicht automatisch die Sommerzeit. Wählen Sie im Menü “E-Mail” das Markierungsfeld “An Sommerzeit anpassen bzw. Adjust for Daylight Savings Time” aus oder heben Sie diese Auswahl auf.

Anhang A

Technische Daten

Dieser Anhang enthält die technischen Daten für den Kabel-/DSL-Wireless-Router Modell MR814.

Kompatibilität mit Netzwerkprotokollen und Standards

Daten und Routing-Protokolle: TCP/IP, RIP-1, RIP-2, DHCP, PPP over Ethernet (PPPoE)

Netzteil

Nordamerika: 120 V, 60 Hz, Eingang
Großbritannien, Australien: 240 V, 50 Hz, Eingang
Europa: 230 V, 50 Hz, Eingang
Japan: 100 V, 50/60 Hz, Eingang
Alle Regionen (Ausgang): 7,5 V DC bei 1 A Ausgang, max. 20 W

Physische Daten

Abmessungen: 28 x 175 x 118 mm
Gewicht: 0,3 kg

Umgebungsdaten

Betriebstemperatur: 0° bis 40° C
Luftfeuchtigkeit bei Betrieb: max. 90 % relative Luftfeuchtigkeit, ohne Kondensation

Elektromagnetische Strahlung

Entspricht Anforderungen von: FCC Teil 15 Klasse B
VCCI Klasse B
EN 55 022 (CISPR 22), Klasse B

Spezifikation der Schnittstellen

Lokal: 10BASE-T oder 100BASE-Tx, RJ-45
Internet: 10BASE-T, RJ-45
Luftfeuchtigkeit bei Betrieb: max. 90 % relative Luftfeuchtigkeit, ohne Kondensation

Elektromagnetische Strahlung

Entspricht Anforderungen von: FCC Teil 15 Klasse B
VCCI Klasse B
EN 55 022 (CISPR 22), Klasse B

Spezifikation der Schnittstellen

LAN: 10BASE-T oder 100BASE-Tx, RJ-45
WAN: 10BASE-T, RJ-45

Wireless

Datenübertragungs-

geschwindigkeit per Funk

1, 2, 5,5, 11 MBit/s, automatische Erkennung der Übertragungsgeschwindigkeit

Frequenz

2,4-2,5 Ghz

Datencodierung:

Direct Sequence Spread Spectrum (DSSS)

Reichweite nach 802.11b

	<u>Außerhalb von Gebäuden</u>	<u>In Gebäuden</u>
bei 11 MBit/s	120 m	60 m
bei 5,5 MBit/s	170 m	80 m
bei 2 MBit/s	270 m	130 m
bei 1 MBit/s	450 m	200 m

Max. Anzahl Computer pro
Wireless-Netzwerk:

Beschränkt durch Umfang des Verkehrs im Wireless-Netzwerk, der pro Netzknoten erzeugt wird. In der Regel 30-70 Netzknoten.

Betriebsfrequenz-
bereiche nach 802.11b

2,412~2,462 GHz (USA)	2,457~2,462 GHz (Spanien)
2,412~2,484 GHz (Japan)	2,457~2,472 GHz (Frankreich)
2,412~2,472 GHz (Europa ETSI)	

Verschlüsselung nach 802.11b

40-Bit (auch als 64-Bit bezeichnet), 128-Bit-WEP-Datenverschlüsselung

Anhang B

Netzwerke, Routing, Firewalls: Grundlagen

Dieser Anhang enthält eine Übersicht zu IP-Netzwerken, zum Routing und zu Firewalls.

Zugehörige Publikationen

Das vorliegende Dokument enthält diverse Verweise auf verschiedene RFC-Dokumente, die weitere Informationen enthalten. Ein RFC ist eine von der Internet Engineering Task Force (IETF) veröffentlichte Kommentaranforderung; diese offene Organisation definiert die Architektur und den Betrieb des Internets. In den RFC-Dokumenten werden die Standardprotokolle und -verfahren für das Internet beschrieben und definiert. Die Dokumente sind im Internet unter www.ietf.org aufgeführt und werden auf zahlreichen anderen Websites auf der ganzen Welt indiziert.

Basisinformationen zu Routern

In einem lokalen Netzwerk (Local Area Network, LAN) lassen sich große Bandbreiten einfach und relativ kostengünstig bereitstellen. Die Bereitstellung großer Bandbreiten zwischen einem lokalen Netzwerk und dem Internet hingegen kann sehr teuer werden. Auf Grund dieser hohen Kosten wird der Internet-Zugang in der Regel über eine langsame WAN-Verbindung (Wide-Area Network, WAN) dargestellt, z. B. ein Kabel- oder DSL-Modem. Im Hinblick auf die optimale Nutzung der langsamen WAN-Verbindung muss ein Mechanismus eingesetzt werden, der sicherstellt, dass nur die tatsächlich für das Internet bestimmten Daten ausgewählt und übertragen werden. Diese Funktion der Auswahl und Weiterleitung der Daten wird durch einen Router wahrgenommen.

Was ist ein Router?

Ein Router ist ein Gerät, das Datenübertragungen zwischen Netzwerken auf der Grundlage der in den Daten enthaltenen Netzwerk-Layer-Informationen und der durch den Router unterhaltenen Routing-Tabellen weiterleitet. In diesen Routing-Tabellen erstellt ein Router durch Erfassen und Austauschen von Informationen mit anderen Routern im Netzwerk ein logisches Abbild des gesamten Netzwerks. Anhand dieser Informationen wählt der Router den besten Pfad für die Weiterleitung von Daten im Netzwerk aus.

Die zahlreichen verfügbaren Router unterscheiden sich nach der Leistungsfähigkeit und Größe, der Anzahl der unterstützten Routing-Protokolle und den unterstützten Typen physischer WAN-Verbindungen.

Routing Information Protocol

Eines der Protokolle, das von einem Router verwendet wird, um ein Abbild des Netzwerks zu erstellen und zu aktualisieren, ist das Routing Information Protocol (RIP). Mit Hilfe von RIP tauschen Router in regelmäßigen Abständen aktualisierte Informationen untereinander aus und ermitteln so die Änderungen, die in der Routing-Tabelle erforderlich sind.

Der Router MR814 v2 unterstützt sowohl das ältere Protokoll RIP-1 als auch das neuere Protokoll RIP-2. Zu den wichtigsten Verbesserungen bei RIP-2 zählt die Unterstützung von Subnetz- und Multicast-Protokollen. Für die meisten Privatanwendungen ist RIP nicht unbedingt erforderlich.

IP-Adressen und das Internet

Da TCP/IP-Netzwerke auf der ganzen Welt miteinander verbunden sind, muss jede Maschine im Internet über eine eindeutige Adresse verfügen um sicherzustellen, dass übertragene Daten den richtigen Empfänger erreichen. Die Internet Assigned Numbers Authority (IANA) weist Organisationen so genannte Adressblöcke zu. Einzelbenutzer und kleinere Organisationen erhalten ihre Adressen von der IANA oder von einem Internet Service Provider (ISP). Sie erreichen die IANA unter www.iana.org.

Das Internet Protocol (IP) verwendet eine 32-Bit-Adressstruktur. Bei der Darstellung der Adresse werden in der Regel Punkte als Dezimaltrennzeichen verwendet (auch bekannt als Dezimalschreibweise mit Dezimalpunkten), die jeweils zwischen zwei in Dezimalform dargestellten Gruppen mit jeweils acht Bit stehen.

So wird beispielsweise die binäre Adresse

```
11000011 00100010 00001100 00000111
```

normalerweise dargestellt als

```
195.34.12.7
```

Die zweite Schreibweise lässt sich leichter merken und in den Computer eingeben.

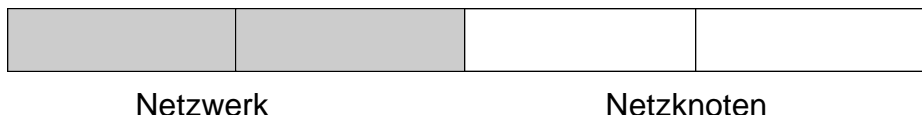
Daneben sind die 32 Bit der Adresse in zwei Bereiche unterteilt. Der erste Teil der Adresse bezeichnet das Netzwerk, der zweite Teil den Host-Knoten oder die Host-Station im Netzwerk. Die Position des Trennpunkts kann je nach Adressbereich und Anwendung variieren.

Für IP-Adressen sind fünf Standardklassen festgelegt. Diese Adressklassen verwenden unterschiedliche Methoden zur Bestimmung des Netzwerk- und des Host-Teils der Adresse und ermöglichen damit die Präsenz unterschiedlichen Anzahlen von Hosts in einem Netzwerk. Jeder Adresstyp beginnt mit einem eindeutigen Bit-Muster, anhand dessen die TCP/IP-Software die Adressklasse erkennt. Nach Bestimmung der Adressklasse ist die Software in der Lage, auch den Host-Teil der Adresse zu bestimmen. Die nachfolgende Abbildung zeigt die drei wichtigsten Adressklassen sowie für jeden Adresstyp den Netzwerk- und den Host-Teil der Adresse.

Klasse A



Klasse B



Klasse C

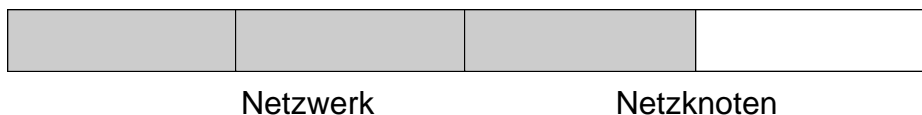


Abbildung 7-1: Die drei wichtigsten Adressklassen

Die fünf Adressklassen lauten:

- Klasse A
Bei Adressen der Klasse A kann ein Netzwerk bis zu 16.777.214 Hosts enthalten. Dabei ist die Netzwerknummer durch acht Bits und die Knotennummer durch 24 Bits dargestellt. Adressen der Klasse A gehören zu folgendem Bereich:
`1.x.x.x bis 126.x.x.x.`
- Klasse B
Bei Adressen der Klasse B kann ein Netzwerk bis zu 65.354 Hosts enthalten. Die Netzwerknummer und die Knotennummer sind dabei jeweils durch 16 Bits dargestellt. Adressen der Klasse B gehören zu folgendem Bereich:
`128.1.x.x bis 191.254.x.x.`

- Klasse C
Bei Adressen der Klasse C kann ein Netzwerk bis zu 254 Hosts enthalten. Die Netzwerknummer ist dabei durch 24 Bits und die Knotennummer durch acht Bits dargestellt. Adressen der Klasse C gehören zu folgendem Bereich:
192.0.1.x bis 223.255.254.x.
- Klasse D
Adressen der Klasse werden für Rundschreibnachrichtenübertragungen (Versand einer Nachricht an mehrere Hosts) verwendet. Adressen der Klasse D gehören zu folgendem Bereich:
224.0.0.0 bis 239.255.255.255.
- Klasse E
Adressen der Klasse E werden zu Versuchszwecken verwendet.

Dank dieser Adressierungsstruktur ist sichergestellt, dass jedes physische Netzwerk und jeder Knoten in jedem physikalischen Netzwerk eindeutig durch eine IP-Adresse gekennzeichnet ist.

Für jeden eindeutigen Wert des Netzwerkteils der Adresse wird die niedrigste Adresse des Bereichs (rein aus Nullen bestehende Host-Adresse) als Netzwerkadresse bezeichnet und in der Regel keinem Host zugeordnet. Die höchste Adresse des Bereichs (rein aus Einsern bestehende Host-Adresse) wird ebenfalls nicht zugeordnet, sondern als Rundsendeadresse für die gleichzeitige Übertragung eines Pakets an alle Hosts mit derselben Netzwerkadresse verwendet.

Netzmaske

Bei jeder der oben beschriebenen Adressklassen ist die Größe der beiden Bestandteile (Netzwerkadresse und Host-Adresse) durch die Klasse festgelegt. Dieses Unterteilungssystem kann auch in Form einer Netzmaske dargestellt werden, die der IP-Adresse zugeordnet ist. Eine Netzmaske ist eine 32-Bit-Quantität, die bei logischer Kombination mit einer IP-Adresse (unter Verwendung eines UND-Operanden) die Netzwerkadresse ergibt. Beispielsweise lauten die Netzmasken von Adressen der Klasse A, B und C 255.0.0.0, 255.255.0.0 und 255.255.255.0.

Beispiel: Die Adresse 192.168.170.237 ist eine IP-Adresse der Klasse C, deren obere 24 Bit den Netzwerkteil bilden. Bei Kombination (mit Hilfe eines UND-Operanden) mit der Netzmaske der Klasse C (wie hier dargestellt), bleibt nur der Netzwerkteil der Adresse übrig:

```
11000000 10101000 10101010 11101101 (192.168.170.237)
```

kombiniert mit:

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

Ergibt:

```
11000000 10101000 10101010 00000000 (192.168.170.0)
```


Als kürzere Alternative zur Dezimalpunktschreibweise kann die Netzmaske auch in Form der Anzahl der Einser (bei Zählung von links) dargestellt werden. Diese Zahl wird an die IP-Adresse angehängt und durch einen umgekehrten Schrägstrich (/) abgehoben, also als “/n.” Im vorliegenden Beispiel könnte die Adresse auch als 192.168.170.237/24 dargestellt werden; dies bedeutet, dass die Netzmaske aus 24 Einsern gefolgt von 8 Nullen besteht.

Subnetz-Adressierung

Selbst bei einer Adresse der Klasse C kann ein Netzwerk eine große Anzahl an Hosts enthalten. Eine derartige Struktur bedeutet eine ineffiziente Nutzung der Adressen, wenn für jedes Ende einer durch Routing generierten Verbindung eine andere Netzwerknummer erforderlich ist. Bei kleineren Büro-LANs ist nicht von einer derartig großen Anzahl an Geräten auszugehen. Daher lässt sich das Problem durch Verwendung der so genannten Subnetz-Adressierung lösen.

Bei der Subnetz-Adressierung kann eine IP-Netzwerkadresse in mehrere kleine physische Netzwerke aufgeteilt werden, die als Subnetzwerke bezeichnet werden. Einige der Netzknottennummern werden als Subnetznummern verwendet. Eine Adresse der Klasse B bietet 16 Bit für die Darstellung von Netzknottennummern, wodurch sich 64.000 Netzknotten ergeben. Die meisten Organisationen verfügen nicht über 64.000 Netzknotten; daher sind mehrere Bits unbelegt, die neu zugeordnet werden können. Bei der Subnetz-Adressierung werden genau diese unbelegten Bits verwendet (siehe unten).

Klasse B

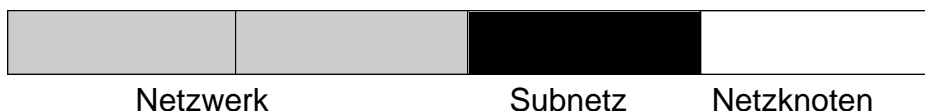


Abbildung 7-2: Beispiel für Subnetz-Darstellung bei Adresse der Klasse B

Eine Adresse der Klasse B kann wirkungsvoll in mehrere Adressen der Klasse C übersetzt werden. Ein Beispiel: Die IP-Adresse 172.16.0.0 wurde zugeordnet, doch die Netzknottenadressen sind auf maximal 255 begrenzt, womit acht freie Bits für Subnetz-Adressen zur Verfügung stehen. Die IP-Adresse 172.16.97.235 würde interpretiert als IP-Netzwerkadresse 172.16, Subnetz-Nummer 97 und Netzknottennummer 235. Neben der Erweiterung der Anzahl der verfügbaren Adressen bietet die Subnetz-Adressierung weitere Vorteile. Sie erlaubt die Subnetz-Adressierung dem Netzwerkmanager den Aufbau eines Adressensystems für das Netzwerk, das verschiedene Subnetze für die verschiedenen geografischen Standorte im Netzwerk oder für die verschiedenen Abteilungen einer Organisation enthält.

Obwohl in dem vorherigen Beispiel das gesamte dritte Oktett für eine Subnetz-Adresse verwendet wird, ist die Bildung von Subnetzwerken nicht unbedingt durch die Oktettgrenzen beschränkt. Wenn Sie mehr Netzwerknummern erzeugen wollen, müssen nur einige Bits aus der Host-Adresse in die Netzwerkadresse verschieben. Um beispielsweise eine Netzwerknummer der Klasse C (192.68.135.0) in zwei Teile zu unterteilen, verschieben Sie ein Bit aus der Host-Adresse in die Netzwerkadresse. Die neue Netzmaske (oder Subnetzmaske) lautet 255.255.255.128. Das erste Subnetz hat die Netzwerknummer 192.68.135.0 mit den Hosts 192.68.135.1 bis 192.68.135.126, und das zweite Subnetz hat die Netzwerknummer 192.68.135.128 mit den Hosts 192.68.135.129 bis 192.68.135.254.



Hinweis: Die Nummer 192.68.135.127 ist nicht zugeordnet, da dies die Rundsendeadresse des ersten Subnetzes ist. Die Nummer 192.68.135.128 ist nicht zugeordnet, da dies die Netzwerkadresse des zweiten Subnetzes ist.

In der nachfolgenden Tabelle sind die Bits für die zusätzlichen Subnetzmasken mit der zugehörigen Dezimalschreibweise mit Dezimalpunkten aufgeführt. Zur Verwendung der Tabelle notieren Sie die Netzmaske in der ursprünglichen Klassendarstellung und ersetzen die Oktette mit dem Wert 0 durch den Dezimalpunktwert der zusätzlichen Subnetz-Bits. Wenn beispielsweise das Netzwerk der Klasse C mit der Subnetzmaske 255.255.255.0 in 16 Subnetze (4 Bits) unterteilt wird, lautet die neue Subnetzmaske 255.255.255.240.

Tabelle 7-1. Umsetzungstabelle der Netzmaskendarstellung für ein Oktett

Anzahl Bits	Wert in	Dezimalschreibweise
1		128
2		192
3		224
4		240
5		248
6		252
7		254
8		255

In der folgenden Tabelle sind verschiedene, häufig verwendete Netzmaskenwerte in der Dezimalschreibweise und als Maskenlängenwert dargestellt.

Tabelle 7-2. Netzmaskenformate

Dezimalschreibweise	Maskenlänge
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Aus folgenden Gründen sollten alle Hosts in einem LAN-Segment so konfiguriert werden, dass sie dieselbe Netzmaske verwenden:

- Die Hosts können auf diese Weise die von einer lokalen IP versendeten Pakete erkennen.
Wenn ein Gerät eine Rundsendenachricht an seine Nachbarn innerhalb des Segments verschickt, verwendet es dabei eine Zieladresse der lokalen Netzwerkadresse, deren Host-Adresse ausschließlich aus Einsern besteht. Damit dieses System funktioniert, muss für alle Geräte innerhalb des Segments eindeutig festgelegt sein, welche Bits die Host-Adresse bilden.
- Ein lokaler Router oder eine Brücke erkennt auf diese Weise, bei welchen Adressen es sich um lokale oder dezentrale Adressen handelt.

Private IP-Adressen

Wenn Ihr lokales Netzwerk vom Internet isoliert ist (z. B. bei Verwendung von NAT), können Sie den Hosts problemlos jede beliebige IP-Adresse zuweisen. Allerdings hat die IANA die folgenden drei IP-Adressblöcke spezielle für private Netzwerke reserviert:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Wähle Sie die Nummer für Ihr privates Netzwerk aus diesem Bereich aus. Der DHCP-Server der Firewall FVM318 ist für die automatische Zuordnung privater Adressen vorkonfiguriert.

Unabhängig von Ihrer spezifischen Situation sollten Sie in keinem Fall in willkürlicher Weise IP-Adressen erstellen; halten Sie sich immer an die in diesem Handbuch vorgegebenen Richtlinien. Weitere Informationen zur Zuordnung von Adressen finden Sie im RFC-Dokument 1597, "Address Allocation for Private Internets" (Adresszuordnung für private Internets) und im RFC-Dokument 1466, "Guidelines for Management of IP Address Space" (Richtlinien für die Verwaltung von IP-Adressraum). Die Internet Engineering Task Force (IETF) veröffentlicht diese RFC-Dokumente auf ihrer Website unter www.ietf.org

Betrieb mit einer IP-Adresse und NAT

In der Vergangenheit mussten Sie einen IP-Adressbereich bei Ihrem ISP beantragen, um mehreren PCs in einem LAN gleichzeitig den Zugriff auf das Internet zu ermöglichen. Ein derartiges Internet-Konto ist kostspieliger als ein Einzeladresskonto, das in der Regel von einem einzelnen Benutzer verwendet wird, der nicht mit einem Router, sondern einem Modem arbeitet. Der Router MR814 v2 wendet eine Methode zur gemeinsamen Adressnutzung an, die als Netzwerk-Adressumsetzung (Network Address Translation, NAT) bezeichnet wird. Mit dieser Methode können mehrere PCs innerhalb eines Netzwerks ein gemeinsames Internet-Konto mit nur einer IP-Adresse verwenden, die von Ihrem ISP statisch oder dynamisch zugewiesen wird.

Der Router realisiert diese gemeinsame Nutzung einer Adresse durch Umsetzung der internen LAN-IP-Adressen in nur eine Adresse, die im gesamten Internet eindeutig ist. Bei den internen LAN-IP-Adressen kann es sich um private oder eingetragene Adressen handeln. Weitere Informationen zur IP-Adress-Umsetzung finden Sie im RFC-Dokument 1631, "The IP Network Address Translator (NAT)" (Die IP-Netzwerk-Adressumsetzung).

Anhand der nachfolgenden Abbildung wird das Prinzip einer einzelnen IP-Adresse erläutert.

Private IP-Adressen,
durch Benutzer zugewiesen

IP-Adressen,
durch ISP zugewiesen

Abbildung 7-3: Betrieb mit einer IP-Adresse und NAT

Dieses Prinzip bietet den zusätzlichen Vorteil einer mit der Firewall vergleichbaren Schutzfunktion, da die internen LAN-Adressen im Internet auf Grund der umgesetzten Verbindung nicht verfügbar sind. Alle eingehenden Anfragen werden durch den Router gefiltert. Dieser Filtervorgang kann Eindringlinge davon abhalten, einen ernsthaften Angriff auf Ihr System zu starten. Bei Verwendung der Port-Weiterleitung hingegen können Sie einen PC (z. B. einen Web-Server) im lokalen Netzwerk für externe Benutzer zugänglich machen.

MAC-Adressen und Adressenauflösungsprotokoll

Eine IP-Adresse allein ist für die Übertragung von einem LAN-Gerät zu einem anderen noch nicht ausreichend. Für die Übertragung von Daten zwischen LAN-Geräten muss die IP-Adresse des Zielgeräts in die MAC-Adresse (Media Access Control) konvertiert werden. Jedes Gerät in einem Ethernet-Netzwerk besitzt eine MAC-Adresse, bei der es sich um eine 48-Bit-Zahl handelt, die jedem Gerät durch den jeweiligen Hersteller zugewiesen wird. Das Verfahren, das die IP-Adresse mit einer MAC-Adresse verknüpft, wird als Adressenauflösung bezeichnet. Das Internet-Protokoll verwendet das Address Resolution Protocol (ARP, Adressenauflösungsprotokoll) für die Auflösung von MAC-Adressen.

Wenn ein Gerät Daten an eine andere Station im Netzwerk schickt und die Ziel-MAC-Adresse noch nicht eingetragen ist, wird ARP verwendet. Eine ARP-Anfrage wird durch eine Rundsendenachricht im Netzwerk verschickt. Alle Stationen im Netzwerk empfangen und lesen die Anfrage. Die Ziel-IP-Adresse der ausgewählten Station ist Bestandteil der Nachricht, sodass nur die Station mit dieser IP-Adresse auf die ARP-Anfrage antwortet. Alle anderen Stationen löschen die Anfrage.

Zugehörige Dokumente

Die Station mit der korrekten IP-Adresse sendet als Antwort ihre eigene MAC-Adresse direkt an das sendende Gerät. Die Empfängerstation liefert der Senderstation die erforderliche Ziel-MAC-Adresse. Die IP-Adressdaten und die MAC-Adressdaten jeder Station werden in einer ARP-Tabelle geführt. Bei der nächsten Übertragung von Daten kann die Adresse über die in der Tabelle gespeicherten Adressinformationen ermittelt werden.

Weitere Informationen zur Adresszuordnung finden Sie in den IETF-Dokumenten RFC 1597, *Address Allocation for Private Internets (Adresszuordnung für private Internets)* und RFC 1466, *Guidelines for Management of IP Address Space (Richtlinien für die Verwaltung von IP-Adressraum)*.

Weitere Informationen zur IP-Adress-Umsetzung finden Sie im RFC-Dokument 1631, *The IP Network Address Translator (NAT) (Die IP-Netzwerk-Adressumsetzung)*.

Domain-Namensserver

Viele der Ressourcen im Internet sind über einfache, nachvollziehbare Namen wie www.NETGEAR.com erreichbar. Diese Adressierung ist auf der Anwendungsebene sehr hilfreich, doch müssen diese beschreibenden Namen in eine IP-Adresse umgesetzt werden, um den tatsächlichen Kontakt zu der Ressource herzustellen. Wie bei der Zuordnung von Namen zu Telefonnummern in einem Telefonbuch oder von IP-Adressen zu MAC-Adressen in einer ARP-Tabelle ordnet ein DNS-Server (Domain-Namenssystem) die beschreibenden Namen von Netzwerkressourcen den entsprechenden IP-Adressen zu.

Wenn ein PC über den beschreibenden Namen auf eine Ressource zugreift, fordert dieser PC zunächst bei einem DNS-Server die IP-Adresse der Ressource an. Dann überträgt der PC die betreffende Nachricht mit Hilfe der IP-Adresse. Zahlreiche große Organisationen wie ISPs verfügen über eigene DNS-Server und ermöglichen Ihren Kunden die Nutzung dieser Server für die Suche nach Adressen.

IP-Konfiguration über DHCP

Bei der Installation eines IP-gestützten lokalen Netzwerks muss jeder PC mit einer IP-Adresse konfiguriert werden. Wenn die PCs auch einen Zugang zum Internet benötigen, sollte die Konfiguration der PCs außerdem eine Gateway-Adresse und eine oder mehrere DNS-Serveradressen enthalten. Als Alternative zu einer manuellen Konfiguration besteht die Möglichkeit der automatischen Abfrage dieser Konfigurationsangaben durch die einzelnen PCs im Netzwerk. Dabei wird ein Gerät im Netzwerk als DHCP-Server (Dynamic Host Configuration Protocol) eingesetzt. Auf dem DHCP-Server sind eine Liste oder eine Reihe von IP-Adressen sowie weitere Informationen gespeichert (z. B. Gateway- und DNS-Adressen), die den anderen Geräten im Netzwerk zugeordnet werden können.

Der Router MR814 v2 kann als DHCP-Server verwendet werden. Daneben ist der Router MR814 v2 bei der Herstellung der Verbindung zum ISP auch als DHCP-Client einsetzbar. Die Firewall kann automatisch eine IP-Adresse, eine Subnetzmaske, DNS-Serveradressen und eine Gateway-Adresse abfragen, wenn der ISP diese Informationen über DHCP bereitstellt.

Internet-Sicherheit und Firewalls

Wenn Ihr LAN über einen Router eine Verbindung ins Internet aufbaut, besteht für Außenstehende die Möglichkeit, in Ihr Netzwerk einzudringen oder dessen Betrieb zu stören. Ein NAT-Router bietet auf Grund der spezifischen Merkmale des NAT-Prozesses (Network Address Translation, Netzwerk-Adressumsetzung) einen gewissen Schutz, durch den das Netzwerk hinter dem NAT-Router gegen einen Zugriff von Außenstehenden aus dem Internet abgeschirmt ist. Dennoch gibt es verschiedene Methoden, mit denen ein entschlossener Hacker möglicherweise an Informationen über Ihr Netzwerk gelangen oder zumindest Ihren Zugang zum Internet stören oder lahmlegen kann. Ein Firewall-Router bietet hier einen besseren Schutz.

Was ist eine Firewall?

Eine Firewall ist ein Gerät, das ein Netzwerk gegenüber einem anderen Netzwerk schützt und gleichzeitig die Kommunikation zwischen diesen Netzwerken zulässt. Eine Firewall umfasst die Funktionen eines NAT-Routers und bietet darüber hinaus zusätzliche Funktionen zur Abwehr eines Hackerangriffs. Verschiedene bekannte Arten von Angriffen werden dabei erkannt. Wenn die Firewall einen Vorfall feststellt, werden die Einzelheiten dieses Zugriffsversuchs in einem Protokoll aufgezeichnet; optional können diese Informationen als Benachrichtigung per E-Mail an einen Administrator gesendet werden. Mit Hilfe dieser Protokollinformationen kann der Administrator den ISP des Hackers kontaktieren und geeignete Maßnahmen einleiten. Bei manchen Angriffsversuchen ist die Firewall in der Lage, den Hackerangriff durch vorübergehendes Löschen aller von der IP-Adresse des Hackers gesendeten Pakete abzuwehren.

Stateful Packet Inspection

Im Gegensatz zu einfachen Internet-Routern verwendet eine Firewall einen Prozess zur Paketüberprüfung (die so genannte Stateful Packet Inspection), um eine sichere Firewall-Filterung zum Schutz Ihres Netzwerks gegen Angreifer und Eindringlinge zu gewährleisten. Da Benutzeranwendungen wie FTP- und Web-Browser komplexe Datenübertragungsmuster im Netzwerk erzeugen können, muss die Firewall den Netzwerkverbindungsstatus für verschiedene Gruppen überprüfen. Bei der Stateful Packet Inspection wird ein ankommendes Paket auf der Netzwerkschicht abgefangen und im Hinblick auf Status-bezogene Informationen zu allen Netzwerkverbindungen untersucht. Ein zentraler Cache-Speicher in der Firewall verfolgt die Statusinformationen aller Netzwerkverbindungen. Der gesamte Verkehr, der die Firewall passiert, wird anhand des Status dieser Verbindungen untersucht, um festzustellen, ob die einzelnen Übertragungen und Nachrichten passieren dürfen oder abgewiesen werden.

DoS-Angriff (Denial of Service)

Durch einen DoS-Angriff können Hacker unter Umständen die Funktions- oder Kommunikationsfähigkeit Ihres Netzwerks beeinträchtigen. Eine einfache Version eines derartigen Angriffs besteht darin, Ihre Website mit mehr Anfragen zu "bombardieren", als die Website bearbeiten kann. Bei einem etwas subtileren Angriff könnte der Hacker versuchen, diverse Schwächen im Betriebssystem des Routers oder Gateways zu nutzen. Manche Betriebssysteme können durch einfache Zustellung eines Pakets mit falschen Längenangaben lahmgelegt werden.

Ethernet-Kabel

Obwohl für Ethernet-Netzwerke ursprünglich dicke oder dünne Koaxialkabel verwendet wurden, werden bei den meisten Systemen gegenwärtig UTP-Kabel (Unshielded Twisted Pair, ungeschirmte verdrehte Doppelleitung) eingesetzt. Das UTP-Kabel enthält acht Leiter, die zu vier verdrehten Doppelleitungen zusammengefasst sind und über einen RJ45-Stecker als Abschluss verfügen. Ein normales UTP-Ethernet-Durchgangskabel entspricht der Standardverdrahtung nach EIA568B, die in Tabelle 7.3 dargestellt ist.

Tabelle 7.3. Verdrahtung eines UTP-Ethernet-Durchgangskabels

Stift	Leiterfarbe	Signal
1	Orange/Weiß	Senden (Tx) +
2	Orange	Senden (Tx) -
3	Grün/Weiß	Empfangen (Rx) +
4	Blau	
5	Blau/Weiß	
6	Grün	Empfangen (Rx) -
7	Braun/Weiß	
8	Braun	

Uplink-Schalter, Crossover-Kabel und MDI/MDIX-Schaltung

In der obigen Verdrahtungstabelle sind der Sende- und der Empfangsvorgang aus Sicht des PCs dargestellt, der als Media Dependant Interface (MDI, Mediumschnittstelle) verdrahtet ist. Bei dieser Verdrahtung erfolgt der Versand durch den PC über die Anschlussstifte 1 und 2. Im Hub ist die Perspektive umgekehrt und der Empfang erfolgt über die Anschlussstifte 1 und 2. Diese Art der Verdrahtung wird als Media Dependant Interface - Crossover (MDI-X) bezeichnet.

Bei Anschluss eines PCs an einen anderen PC oder eines Hub-Ports an einen anderen Hub-Port muss das Sendepaar durch das Empfangspaar vertauscht werden. Dieser Austausch kann auf unterschiedliche Weise erfolgen. Die meisten Hubs verfügen über einen Uplink-Schalter, der die Paare an einem Port vertauscht und damit die Verbindung zwischen den beiden Ports über ein normales Ethernet-Kabel ermöglicht. Bei der zweiten Methode wird ein Crossover-Kabel verwendet; dies ist ein spezielles Kabel, bei dem die Sende- und Empfangspaare an einem der beiden Kabelstecker vertauscht sind. Crossover-Kabel sind oftmals nicht als solche gekennzeichnet und können nur durch einen Vergleich der beiden Stecker identifiziert werden. Da die Kabelstecker aus transparentem Kunststoff gefertigt sind, können sie einfach nebeneinander gelegt und die Reihenfolgen der Leiterfarben verglichen werden. Bei einem Durchgangskabel ist die Farbanordnung bei beiden Steckern identisch. Bei einem Crossover-Kabel sind das orangefarbene und das blaue Paar an einem Stecker vertauscht.

Der Router MR814 v2 verwendet die Auto Uplink™-Technologie (oder MDI/MDIX). Jeder lokale Ethernet-Port (LOCAL) erkennt automatisch, ob das an dem Port eingesteckte Ethernet-Kabel eine “normale” Verbindung, z. B. zu einem PC, oder eine “Uplink”-Verbindung, z. B. zu einem Router, Switch oder Hub, benötigt. Daraufhin wird der Port automatisch für die erforderliche Verbindung konfiguriert. Damit können Sie auf die Verwendung eines Crossover-Kabels verzichten, da Auto Uplink™ in jedem Fall die korrekte Verbindung für den jeweiligen Kabeltyp herstellt.

Kabelqualität

Bei Netzwerken mit verdrehten Ethernet-Kabeln, die mit 10 MBit/Sekunde (10BASE-T) arbeiten, kann eine geringere Kabelqualität oftmals hingenommen werden, doch bei 100 MBit/Sekunde (100BASE-TX) muss das Kabel der Kategorie 5 (Cat 5) der Electronic Industry Association (EIA) entsprechen. Die Kategorie ist auf die Kabelummantelung gedruckt. Ein Kabel der Kategorie 5 erfüllt bestimmte Anforderungen bezüglich Verlust und Störsignalen. Daneben sind bei beiden Netzwerktypen, 10 und 100 MBit/Sekunde, Einschränkungen hinsichtlich der maximalen Kabellänge zu berücksichtigen.

Anhang C

Netzwerk vorbereiten

In diesem Anhang wird beschrieben, welche Vorbereitungen Sie in Ihrem Netzwerk treffen müssen, um über den Kabel-DSL-Wireless-Router Modell MR814 v2 eine Verbindung zum Internet herzustellen, und wie Sie die Verfügbarkeit des Breitband-Internet-Angebots eines Internet Service Provider (ISP) überprüfen können.



Hinweis: Wenn Ihr Computer während der Installation eines Breitbandmodems durch einen ISP-Techniker konfiguriert wurde oder Sie die Installation selbst anhand der Anleitung Ihres ISP durchgeführt haben, müssen Sie möglicherweise die aktuellen Konfigurationsangaben für die Konfiguration Ihrer Firewall kopieren. Notieren Sie diese Angaben, bevor Sie Ihre Computer konfigurieren. Weitere Informationen finden Sie unter “ISP-Konfigurationsangaben für Windows-Computer ermitteln” auf Seite C-19 oder unter “ISP-Konfigurationsangaben für Macintosh-Computer ermitteln” auf Seite C-20.

Computer für den Einsatz im TCP/IP-Netzwerk vorbereiten

Computer verwenden für den Zugriff auf das Internet ein Protokoll namens TCP/IP (Transmission Control Protocol/Internet Protocol). Auf jedem Computer in Ihrem Netzwerk muss TCP/IP installiert und als Netzwerkprotokoll ausgewählt sein. Wenn in Ihrem PC bereits eine Netzwerkschnittstellenkarte (Network Interface Card, NIC) installiert ist, dann ist vermutlich auch TCP/IP bereits installiert.

Die meisten Betriebssysteme enthalten Software-Komponenten, die für die Arbeit in Netzwerken mit TCP/IP erforderlich sind:

- Windows® 95 oder höher enthält die Software-Komponenten für die Einrichtung eines TCP/IP-Netzwerks.
- Windows 3.1 enthält keine TCP/IP-Komponenten. Sie müssen ein TCP/IP-Anwendungspaket eines anderen Herstellers erwerben, z. B. NetManage Chameleon.
- Das Macintosh Betriebssystem 7 oder höher enthält die Software-Komponenten für die Einrichtung eines TCP/IP-Netzwerks.

- Alle Versionen von UNIX und Linux enthalten TCP/IP-Komponenten. Installieren Sie TCP/IP entsprechend der Anleitung, die mit dem Betriebssystem oder Netzwerk-Software geliefert wurde, auf Ihrem Computer.

In Ihrem IP-Netzwerk muss jedem PC und der Firewall jeweils eine eindeutige IP-Adresse sein. Außerdem müssen auf jedem PC bestimmte weitere IP-Konfigurationsangaben wie eine Subnetzmaske (Netzmaske), eine DNS-Adresse (Domain Name Server) und eine Standard-Gateway-Adresse vorliegen. In den meisten Fällen sollten Sie TCP/IP so installieren, dass der PC die jeweils relevanten Angaben zur Netzwerkkonfiguration während des Startvorgangs automatisch von einem DHCP-Server erhält. Eine ausführliche Erläuterung der Bedeutung und des Zwecks dieser Konfigurationsangaben finden Sie in Anhang B, "Netzwerke, Routing, Firewalls: Grundlagen".

Der Router MR814 v2 ist im Auslieferungszustand bereits als DHCP-Server vorkonfiguriert. Die Firewall legt beim Neustart des PC automatisch folgende TCP/IP-Konfiguration fest:

- IP-Adressen für PCs oder Workstations—192.168.0.2 bis 192.168.0.254
- Subnetzmaske—255.255.255.0
- Gateway-Adresse (die Firewall)—192.168.0.1

Diese Adressen sind Teil des von der IETF festgelegten Bereichs privater Adressen, die für private Netzwerke reserviert sind.

Konfiguration von Windows 95, 98 und Me für die Verwendung eines TCP/IP-Netzwerks

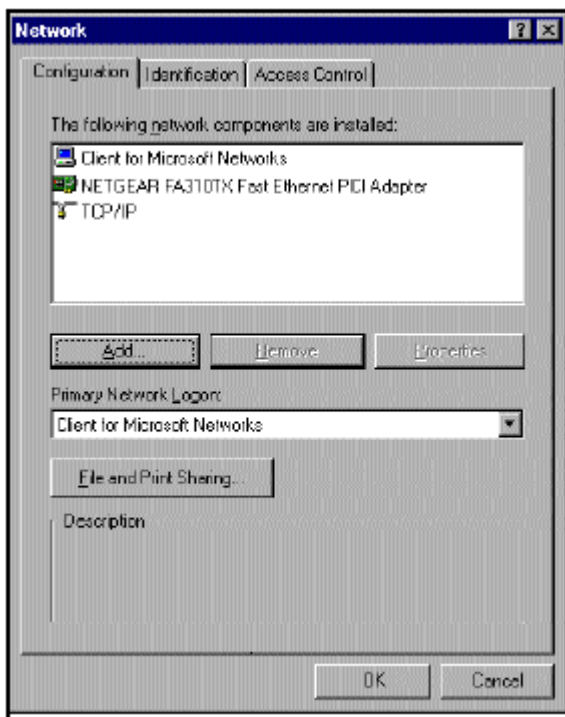
Als Teil der Vorbereitungen der PCs müssen Sie auf jedem PC im Netzwerk TCP/IP installieren und konfigurieren. Halten Sie dabei Ihre Windows-CD bereit, die Sie unter Umständen während der TCP/IP-Installation einlegen müssen.

Windows-Komponenten für Netzwerkbetrieb installieren oder überprüfen

Gehen Sie wie folgt vor, um die erforderlichen Komponenten für den IP-Netzwerkbetrieb zu installieren oder zu überprüfen:

1. Klicken Sie in der Windows Taskleiste auf "Start" und wählen Sie dann "Einstellungen bzw. Settings" und "Systemsteuerung bzw. Control Panel" aus.
2. Doppelklicken Sie auf "Netzwerk- und DFÜ-Verbindungen bzw. Network".

Das Fenster "Netzwerk- und DFÜ-Verbindungen bzw. Network" wird geöffnet; in diesem Fenster sehen Sie eine Liste aller installierten Komponenten:



Sie benötigen einen Ethernet-Adapter, das TCP/IP-Protokoll und Client for Microsoft Networks.



Hinweis: Die anderen Netzwerkkomponenten, die in dem Fenster “Netzwerk- und DFÜ-Verbindungen bzw. Network” aufgeführt sind, müssen für die Installation des Adapters, das TCP/IP-Protokolls oder des Client for Microsoft Networks nicht gelöscht werden.

Wenn Sie einen neuen Adapter installieren, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche “Hinzufügen bzw. Add”.
- Wählen Sie “Adapter” aus und klicken Sie dann auf die Schaltfläche “Hinzufügen bzw. Add”.
- Wählen Sie den Hersteller und das Modell Ihres Ethernet-Adapters aus und klicken Sie auf “OK”.

Wenn Sie TCP/IP benötigen, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche “Hinzufügen bzw. Add”.
- Wählen Sie “Protokoll bzw. Protocol” aus und klicken Sie dann auf die Schaltfläche “Hinzufügen bzw. Add”.
- Wählen Sie “Microsoft” aus.
- Wählen Sie “TCP/IP” und klicken Sie dann auf “OK”.

Wenn Sie Client for Microsoft Networks benötigen, gehen Sie wie folgt vor:

- a. Klicken Sie auf die Schaltfläche “Hinzufügen bzw. Add”.
 - b. Wählen Sie “Client” aus und klicken Sie dann auf die Schaltfläche “Hinzufügen bzw. Add”.
 - c. Wählen Sie “Microsoft” aus.
 - d. Wählen Sie “Client for Microsoft Networks” aus und klicken Sie dann auf “OK”.
3. Starten Sie den PC neu, um die Änderungen zu aktivieren.

Automatische Konfiguration der TCP/IP-Einstellungen durch DHCP unter Windows 95B, 98 und Me aktivieren

Nach Installation der Komponenten des TCP/IP-Protokolls müssen jedem PC spezifische Informationen zu dem betreffenden PC sowie zu den Ressourcen, die im Netzwerk verfügbar sind, zuteilt werden. Am einfachsten können diese Informationen konfiguriert werden, wenn der PC die Informationen PC selbst bei einem DHCP-Server im Netzwerk abfragt.

Die Vorgehensweise bei der Konfiguration von TCP/IP über DHCP ist bei den verschiedenen Windows-Systemen sehr ähnlich.

Die folgenden Schritte leiten Sie für jede dieser Windows-Versionen durch den jeweiligen Konfigurationsprozess.

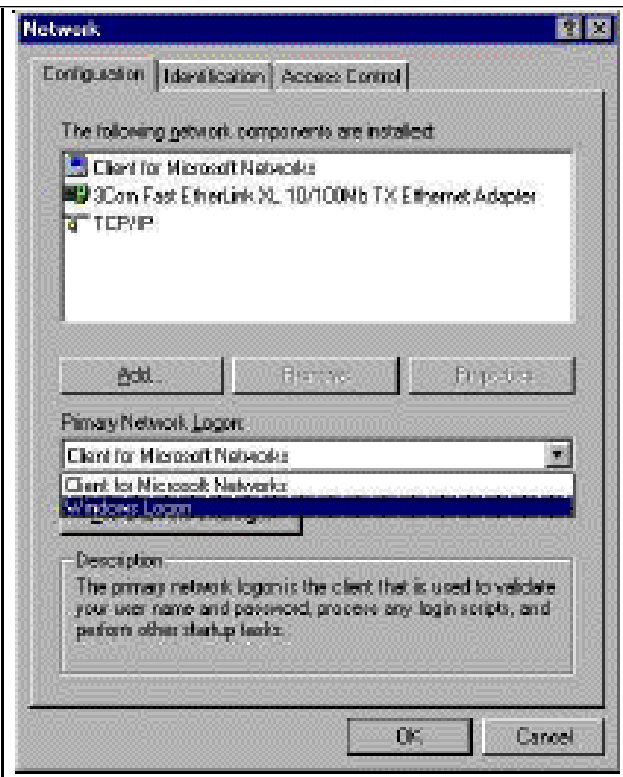


Auf Ihrem PC befindet sich das Symbol **Netzwerkumgebung**.

- Falls sich das Symbol “Netzwerkumgebung bzw. Network Neighborhood” auf der Windows-Arbeitsoberfläche (Desktop) befindet, richten Sie den Mauszeiger auf dieses Symbol und klicken Sie dann mit der rechten Maustaste.
- Gehen Sie wie folgt vor, falls sich das Symbol nicht auf der Arbeitsoberfläche befindet:
 - Klicken Sie in der Taskleiste am unteren Rand des Fensters auf **Start**.
 - Wählen Sie **Einstellungen** und anschließend **Systemsteuerung** aus.
 - Klicken Sie auf das Symbol **Netzwerkumgebung**. Daraufhin wird das Fenster “Netzwerk- und DFÜ-Verbindungen” geöffnet (siehe unten).

2

- Vergewissern Sie sich, dass folgende Einstellungen bzw. Bedingungen gelten:
 - 'Client für Microsoft-Netzwerk' ist vorhanden
 - Der Ethernet-Adapter ist vorhanden
 - TCP/IP ist vorhanden
 - Für **Primary Network Logon** ist die Windows-Anmeldung ausgewählt
- Klicken Sie auf die Schaltfläche **Einstellungen bzw. Properties**. Daraufhin wird das folgende Fenster "TCP/IP-Eigenschaften bzw. TCP/IP Properties" angezeigt.



3

- Standardmäßig ist in diesem Fenster die Registerkarte "IP-Adresse bzw. IPAddress" geöffnet.
- Prüfen Sie folgendes:
IP-Adresse automatisch beziehen ist ausgewählt. Falls dies nicht der Fall ist, wählen Sie diese Option über den Drehknopf links neben dem Optionstext aus. Diese Einstellung ist für die Aktivierung der automatischen Zuordnung einer IP-Adresse durch den DHCP-Server erforderlich.
- Klicken Sie auf OK, um fortzufahren.
- Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC in Ihrem Netzwerk, der mit dieser Windows-Version arbeitet.

Internet-Zugriffsmethode unter Windows auswählen

1. Klicken Sie in der Windows Taskleiste auf "Start" und wählen Sie dann "Einstellungen bzw. Settings" und "Systemsteuerung bzw. Control Panel" aus.
2. Doppelklicken Sie auf dem Symbol "Internet-Optionen bzw. Internet Options".
3. Wählen Sie "Internet-Verbindung manuell einrichten bzw. I want to set up my Internet connection manually" oder "Verbindung über LAN bzw. I want to connect through a Local Area Network" und klicken Sie auf "Weiter bzw. Next".
4. Wählen Sie "Verbindung über LAN bzw. I want to connect through a Local Area Network" aus und klicken Sie auf "Weiter bzw. Next".
5. Heben Sie die Auswahl aller Optionen im Fenster "LAN-Internet-Konfiguration bzw. LAN Internet Configuration" auf und klicken Sie auf "Weiter bzw. Next".
6. Beenden Sie den Assistenten.

TCP/IP-Eigenschaften überprüfen

Nach der Konfiguration und dem Neustart des PCs können Sie die TCP/IP-Konfiguration mit dem Dienstprogramm winipcfg.exe überprüfen:

1. Klicken Sie in der Windows Taskleiste auf "Start" und wählen Sie "Ausführen bzw. Run" aus.

2. Geben Sie "winipcfg" ein und klicken Sie auf "OK": Das Fenster "IP-Konfiguration bzw. IP Configuration" wird geöffnet, das (unter anderem) Ihre IP-Adresse, Ihre Subnetzmaske und das Standard-Gateway enthält.
3. Wählen Sie in der Auswahlliste Ihren Ethernet-Adapter aus.

In dem Fenster werden Ihre aktualisierten Einstellungen angezeigt, die mit den nachfolgenden Werten übereinstimmen sollten, sofern Sie die TCP/IP-Standardereinstellungen verwenden, die von NETGEAR für die Herstellung von Verbindungen über einen Router oder ein Gateway empfohlen werden:

- Die IP-Adresse liegt zwischen 192.168.0.2 und 192.168.0.254.
- Die Subnetzmaske lautet 255.255.255.0.
- Das Standard-Gateway lautet 192.168.0.1.

Windows NT4, 2000 oder XP für den Betrieb eines IP-Netzwerks konfigurieren

Als Teil der Vorbereitungen der PCs müssen Sie auf jedem PC im Netzwerk TCP/IP installieren und konfigurieren. Halten Sie dabei Ihre Windows-CD bereit, die Sie unter Umständen während der TCP/IP-Installation einlegen müssen.

Windows-Komponenten für Netzwerkbetrieb installieren oder überprüfen

Gehen Sie wie folgt vor, um die erforderlichen Komponenten für den IP-Netzwerkbetrieb zu installieren oder zu überprüfen:

1. Klicken Sie in der Windows Taskleiste auf "Start" und wählen Sie dann "Einstellungen bzw. Settings" und "Systemsteuerung bzw. Control Panel" aus.
2. Doppelklicken Sie auf dem Symbol "Netzwerk- und DFÜ-Verbindungen bzw. Network and Dialup Connections".
3. Falls auf Ihrem PC ein Ethernet-Adapter vorhanden ist, sollten Sie einen Eintrag für eine LAN-Verbindung sehen. Doppelklicken Sie auf diesen Eintrag.
4. Wählen Sie "Eigenschaften bzw. Properties" aus.
5. Vergewissern Sie sich, dass 'Client für Microsoft-Netzwerke' und 'Internetprotokoll (TCP/IP)' vorhanden sind. Wenn nicht, wählen Sie "Installieren bzw. Install" aus, um diese Komponenten hinzuzufügen.
6. Wählen Sie 'Internetprotokoll (TCP/IP) bzw. Internet Protocol (TCP/IP)' aus, klicken Sie auf "Eigenschaften bzw. Properties", und vergewissern Sie sich, dass "IP-Adresse automatisch beziehen bzw. Obtain an IP address automatically" ausgewählt ist.
7. Klicken Sie auf "OK", um alle Fenster zu "Netzwerk- und DFÜ-Verbindungen bzw. Network and Dialup Connections" zu schließen.
8. Starten Sie dann den PC neu.

DHCP-Konfiguration von TCP/IP unter Windows XP, 2000 oder NT4

Die Vorgehensweise bei der Konfiguration von TCP/IP über DHCP ist bei den verschiedenen Windows-Systemen sehr ähnlich.

Die folgenden Schritte leiten Sie für jede dieser Windows-Versionen durch den jeweiligen Konfigurationsprozess.

DHCP-Konfiguration von TCP/IP unter Windows XP

1

Auf Ihrem PC befindet sich das Symbol **Netzwerkumgebung** bzw. **Network Neighborhood**.

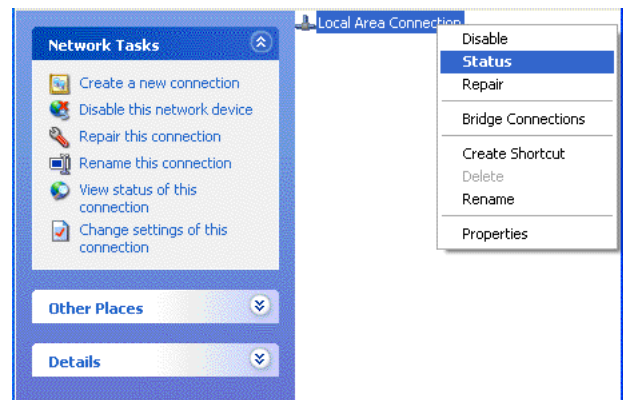
- Wählen Sie im Menü "Start" die Option **Systemsteuerung** bzw. **Control Panel** aus.
- Wählen Sie das Symbol **Netzwerkverbindungen** bzw. **Network Connections** aus. Damit gelangen Sie zum nächsten Schritt.

2

- Das Fenster "Netzwerkverbindung bzw. Network Connections" wird angezeigt.

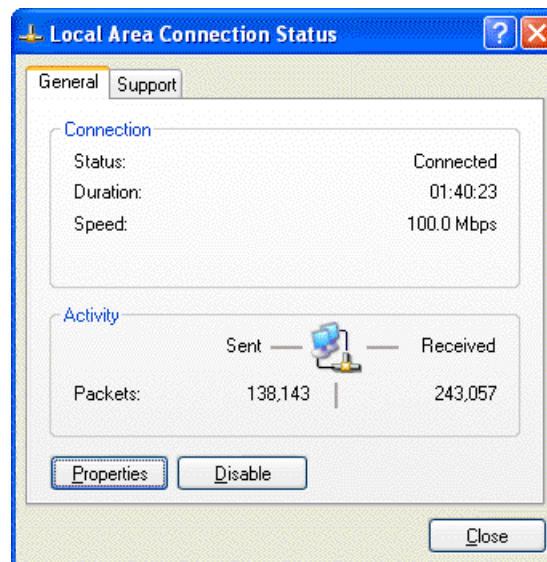
Die Verbindungsliste in der rechten Hälfte des Fensters enthält alle Netzwerkverbindungen, die auf Ihrem PC eingerichtet wurden.

- Klicken Sie mit der rechten Maustaste auf die **Verbindung**, die Sie verwenden wollen, und wählen Sie **Status** aus.



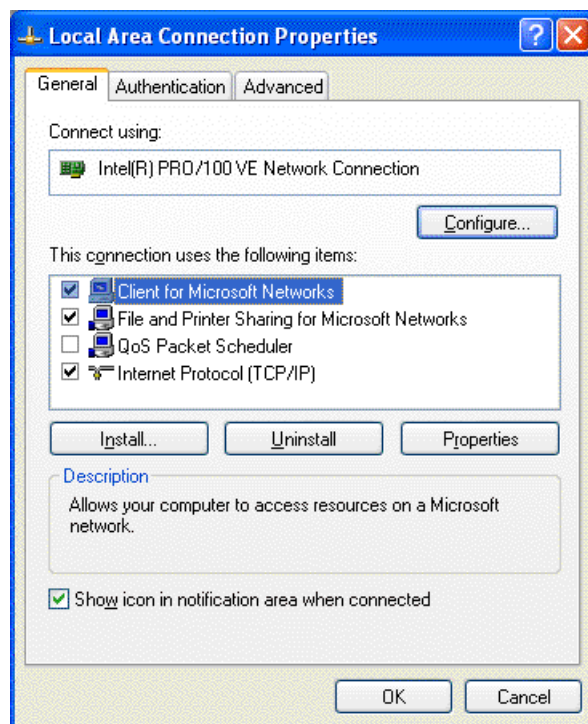
3

- Nun sollte das Fenster **LAN-Verbindungsstatus** bzw. **Local Area Network Connection Status** angezeigt werden. Darin werden der Status, die Dauer und die Übertragungsgeschwindigkeit der Verbindung sowie statistische Daten zur Aktivität angezeigt.
- Sie benötigen Administratorrechte, um diese Optionen in diesem Fenster zu benutzen.
- Klicken Sie auf die Schaltfläche **Eigenschaften** bzw. **Properties**, um Detailangaben zu der Verbindung anzuzeigen.



4

- Die TCP/IP-Angaben werden auf der Registerkarte "Support" angezeigt.
- Wählen Sie **Internetprotokoll** bzw. **Internet Protocol** aus und klicken Sie auf **Eigenschaften** bzw. **Properties**, um die Konfigurationsdaten anzuzeigen.



5

- Vergewissern Sie sich, dass die Option **IP-Adresse automatisch beziehen bzw. Obtain an IP address automatically** ausgewählt ist.
- Vergewissern Sie sich, dass die Option **DNS-Serveradresse automatisch beziehen bzw. Obtain DNS server address automatically** ausgewählt ist.
- Klicken Sie auf die Schaltfläche **OK**.

Damit ist die DHCP-Konfiguration von TCP/IP unter Windows XP abgeschlossen.

Wiederholen Sie diese Schritte auf jedem PC in Ihrem Netzwerk, der mit dieser Windows-Version arbeitet.

DHCP-Konfiguration von TCP/IP unter Windows 2000

Nach der Installation der Netzwerkkarte wird TCP/IP für Windows 2000 konfiguriert. TCP/IP wird in der Regel standardmäßig hinzugefügt und auf DHCP gesetzt, ohne dass manuelle Eingriffe durch den Benutzer erforderlich sind. Falls jedoch Probleme auftreten, können Sie TCP/IP mit DHCP anhand folgender Schritte unter Windows 2000 konfigurieren.

1

- Klicken Sie auf der Windows-Arbeitsoberfläche (Desktop) auf das Symbol **Netzwerkumgebung**. Das Fenster “Netzwerk- und DFÜ-Verbindungen bzw. Network and Dial-up Connections” wird geöffnet.
- Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung bzw. Local Area Connection** und wählen Sie **Eigenschaften bzw. Properties** aus.

2

- Das Dialogfenster **Eigenschaften von LAN-Verbindung bzw. Local Area Connection Properties** wird angezeigt.
- Vergewissern Sie sich, dass in dem Feld **Verbindung herstellen unter Verwendung von: bzw. Connect using:** die richtige Ethernet-Karte ausgewählt ist.
- Vergewissern Sie sich, dass mindestens zwei der folgenden Einträge in dem Feld “Aktivierte Komponenten werden von dieser Verbindung verwendet bzw. Components checked are used by this connection” angezeigt werden und ausgewählt sind:
 - “Client für MicrosoftNetzwerke” und
 - Internetprotokoll (TCP/IP).
- Klicken Sie auf **OK**.

3

- Klicken Sie nach Auswahl von “Internetprotokoll (TCP/IP) bzw. Internet Protocol (TCP/IP)” auf die Schaltfläche **Eigenschaften bzw. Properties**, um das Dialogfenster “Eigenschaften von Internetprotokoll (TCP/IP) bzw. Protocol (TCP/IP) Properties” zu öffnen.
- Vergewissern Sie sich, dass die Optionen
 - **IP-Adresse automatisch beziehen bzw. Obtain an IP address automatically** und
 - **DNS-Serveradresse automatisch beziehen bzw. Obtain DNS server address automatically** ausgewählt sind.
- Klicken Sie auf **OK**, um zum Fenster “Eigenschaften von LAN-Verbindung bzw. Local Area Connection Properties” zurückzukehren.

4

- Klicken Sie erneut auf **OK**, um die Konfiguration für Windows 2000 abzuschließen.

Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC in Ihrem Netzwerk, der mit dieser Windows-Version arbeitet.

DHCP-Konfiguration von TCP/IP unter Windows NT4

Nach Installation der Netzwerkkarte müssen Sie die TCP/IP-Umgebung unter Windows NT 4.0 konfigurieren. Gehen Sie wie folgt vor, um TCP/IP mit DHCP unter Windows NT 4.0 zu konfigurieren.

1

- Wählen Sie im Menü “Start” die Option “Einstellungen bzw. Settings” und anschließend **Systemsteuerung bzw. Control Panel** aus.
Das Fenster “Systemsteuerung bzw. Control Panel” wird angezeigt.

2

- Doppelklicken Sie im Fenster “Systemsteuerung bzw. Control Panel” auf dem Symbol **Netzwerk bzw. Network**.
Das Fenster “Netzwerk bzw. Network” wird angezeigt.
- Wählen Sie die Registerkarte **Protokolle bzw. Protocols** aus.

3

- Wählen Sie in dem Feld **Netzwerk-Protokolle** bzw. **Network Protocols** das **TCP/IP-Protokoll** aus und klicken Sie auf die Schaltfläche **Eigenschaften** bzw. **Properties**.

4

- Das Dialogfenster **TCP/IP-Eigenschaften** bzw. **TCP/IP Properties** wird angezeigt.
- Klicken Sie die Registerkarte **IP-Adresse** bzw. **IPAddress**.
- Wählen Sie den Punkt **IP-Adresse von DHCP-Server beziehen** bzw. **Obtain an IP address from a DHCP server** aus.
- Klicken Sie auf **OK**. Damit ist die Konfiguration von TCP/IP unter Windows NT abgeschlossen.
- Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC in Ihrem Netzwerk, der mit dieser Windows-Version arbeitet.

TCP/IP-Eigenschaften für Windows XP, 2000 und NT4 überprüfen

Gehen Sie wie folgt vor, um die TCP/IP-Konfiguration Ihres PCs zu überprüfen:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche "Start" und dann auf die Option "Ausführen bzw. Run". Das Fenster "Ausführen bzw. Run" wird angezeigt.
2. Geben Sie "cmd" ein und klicken Sie auf "OK". Ein Befehlsfenster wird angezeigt.
3. Geben Sie `ipconfig /all` ein.

Ihre IP-Konfigurationseinstellungen werden angezeigt; diese sollten mit den nachfolgenden Werten übereinstimmen, sofern Sie die TCP/IP-Standardinstellungen verwenden, die von NETGEAR für die Herstellung von Verbindungen über einen Router oder ein Gateway empfohlen werden:

- Die IP-Adresse liegt zwischen 192.168.0.2 und 192.168.0.254.
- Die Subnetzmaske lautet 255.255.255.0.
- Das Standard-Gateway lautet 192.168.0.1.

4. Geben Sie `exit` ein.

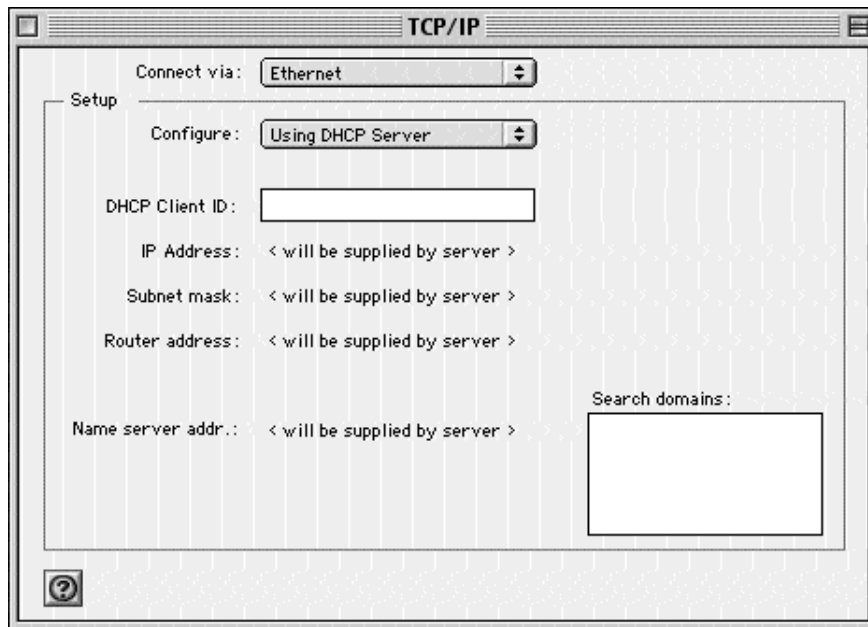
Macintosh für die Verwendung eines TCP/IP-Netzwerks konfigurieren

Ab Version 7 des Macintosh Betriebssystems ist TCP/IP bereits auf dem Macintosh-Rechner vorinstalliert. Auf jedem Macintosh im Netzwerk müssen Sie TCP/IP für DHCP konfigurieren.

MacOS 8.6 oder 9.x

1. Wählen Sie im Apple-Menü die Option "Systemsteuerungen bzw. Control Panels" und anschließend TCP/IP aus.

Das Fenster “TCP/IP-Systemsteuerung bzw. TCP/IP Control Panel” wird geöffnet.



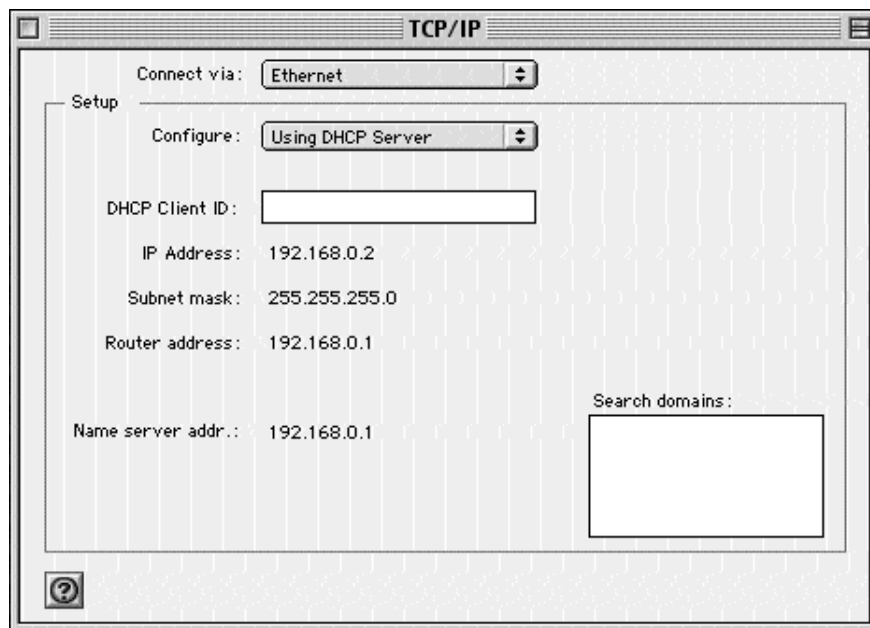
2. Wählen Sie in dem Feld “Verbindung herstellen über bzw. Connect via” die Ethernet-Schnittstelle Ihres Macintosh-Rechners aus.
3. Wählen Sie in dem Feld “Konfigurieren bzw. Configure” die Option “DHCP-Server verwenden bzw. Using DHCP Server” aus. In dem Feld “DHCP Client ID” ist kein Eintrag erforderlich.
4. Schließen Sie das Fenster “TCP/IP-Systemsteuerung bzw. TCP/IP Control Panel”.
5. Wiederholen Sie diese Schritte an jedem Macintosh im Netzwerk.

MacOS X

1. Wählen Sie im Apple-Menü die Optionen “Systempräferenzen bzw. System Preferences” und dann “Netzwerk bzw. Network” aus.
2. Wählen Sie in der Liste “Konfigurieren bzw. Configure” den Eintrag “Integriertes Ethernet bzw. Built-in Ethernet” aus.
3. Wählen Sie auf der Registerkarte “TCP/IP” die Option “DHCP verwenden bzw. Using DHCP” aus.
4. Klicken Sie auf “Save bzw. Speichern”.

TCP/IP-Eigenschaften für Macintosh-Computer überprüfen

Nach der Konfiguration und dem Neustart Ihres Macintosh-Rechners können Sie die TCP/IP-Konfiguration in der TCP/IP-Systemsteuerung überprüfen. Wählen Sie im Apple-Menü die Option “Systemsteuerungen bzw. Control Panels” und anschließend TCP/IP aus.



In dem Fenster werden Ihre aktualisierten Einstellungen angezeigt, die mit den folgenden Werten übereinstimmen sollten, wenn Sie die von NETGEAR empfohlenen TCP/IP-Standard-Einstellungen verwenden:

- Die IP-Adresse liegt zwischen 192.168.0.2 und 192.168.0.254.
- Die Subnetzmaske lautet 255.255.255.0.
- Die Router-Adresse lautet 192.168.0.1.

Wenn diese Werte nicht angezeigt werden, müssen Sie unter Umständen Ihren Macintosh neu starten oder für die Option “Konfigurieren bzw. Configure” eine andere Einstellung auswählen und dann zu “DHCP-Server verwenden bzw. Using DHCP Server” zurückkehren.

Betriebsbereitschaft des Internet-Kontos überprüfen

Für den Breitbandzugang zum Internet benötigen Sie einen Vertrag mit einem Internet Service Provider (ISP) über die Bereitstellung eines Einzelplatz-Internet-Zugangskontos über ein Kabel- oder DSL-Modem. Bei diesem Modem muss es sich um ein physisch separates Gerät handeln (keine Karte), das über einen Ethernet-Anschluss für die Verbindung zu einer Netzwerkschnittstellenkarte (NIC) in einem Computer verfügt. Über den USB-Port angeschlossene Breitbandmodems werden von Ihrer Firewall nicht unterstützt.

Von Ihrem ISP erhalten Sie die TCP-/IP-Konfigurationsdaten für einen Computer, auf dem ein Einzelplatz-Internet-Konto eingerichtet wird. Bei einem normalen Konto wird ein Großteil dieser Konfigurationsdaten dynamisch zugewiesen, wenn Sie Ihrem PC zum ersten Mal bei bestehender Verbindung zum ISP starten; das heißt, Sie müssen diese dynamischen Daten gar nicht wissen.

Damit die Internet-Verbindung von mehreren Computern gemeinsam genutzt werden kann, übernimmt Ihre Firewall die Funktion eines einzelnen PCs; daher müssen an der Firewall die TCP/IP-Einstellungen konfiguriert werden, die normalerweise am Einzel-PC vorgenommen werden. Wenn Sie den Internet-Port der Firewall an das Breitbandmodem anschließen, erscheint die Firewall aus Sicht des ISP als Einzel-PC. Über die Firewall können sich dann die PCs im lokalen Netzwerk als dieser Einzel-PC “verkleiden”, um über das Breitbandmodem auf das Internet zuzugreifen. Die dabei durch die Firewall angewandte Methode wird als Netzwerk-Adressumsetzung (Network Address Translation, NAT) oder IP-Maskierung bezeichnet.

Werden Anmeldeprotokolle verwendet?

Bei manchen ISPs ist die Verwendung eines speziellen Anmeldeprotokolls erforderlich, mit dem Sie erst nach Eingabe eines Anmeldenamens und eines Kennworts Zugang zum Internet erhalten. Wenn Sie sich normalerweise über ein Programm wie WinPOET oder EnterNet bei Ihrem Internet-Konto anmelden, verwendet Ihr Konto PPP over Ethernet (PPPoE).

Bei der Konfiguration Ihres Routers müssen Sie im Konfigurationsmenü des Routers Ihren Anmeldenamen und das Kennwort eingeben. Nach der Konfiguration des Netzwerks und der Firewall führt die Firewall die Anmeldung durch (wenn erforderlich), und Sie müssen das Anmeldeprogramm nicht mehr auf Ihrem PC ausführen. Es ist jedoch nicht erforderlich, dieses Anmeldeprogramm zu deinstallieren.

Wie lauten die Konfigurationseinstellungen?

Konfigurationsdaten werden von ISPs in zunehmendem Maße dynamisch zugeteilt. Falls Ihr ISP die Konfigurationsdaten nicht dynamisch zuweist, sondern feste Konfigurationen verwendet, sollten Sie von Ihrem ISP folgende Basisdaten zu Ihrem Konto erhalten haben:

- Eine IP-Adresse und eine Subnetzmaske.
- Eine Gateway-IP-Adresse, bei der es sich um die Adresse des Routers des ISP handelt.
- Eine oder mehrere DNS-IP-Adressen.
- Host-Name und Domain-Erweiterung.

Beispielsweise könnte der vollständige Server-Name Ihres Kontos wie folgt lauten:

`mail.xxx.yyy.com`

Bei diesem Beispiel lautet die Domain-Erweiterung `xxx.yyy.com`.

Falls diese Daten durch den ISP dynamisch bereitgestellt werden, kann Ihre Firewall sie automatisch abfragen.

Wenn Ihr Computer während der Installation eines Breitbandmodems durch einen ISP-Techniker konfiguriert wurde oder Sie die Installation selbst anhand der Anleitung Ihres ISP durchgeführt haben, müssen Sie die aktuellen Konfigurationsangaben im Fenster "TCP/IP-Eigenschaften bzw. TCP/IP Properties" Ihres PCs oder (bei Macintosh-Rechnern) im Fenster "TCP/IP-Systemsteuerung bzw. TCP/IP Control Panel" kopieren, bevor Sie die Konfiguration des PCs für die Verwendung der Firewall ändern. Die dabei erforderlichen Schritte werden nachfolgend beschrieben.

ISP-Konfigurationsangaben für Windows-Computer ermitteln

Wie bereits erwähnt, müssen Sie die Konfigurationsdaten an Ihrem PC möglicherweise selbst ermitteln, um diese Daten dann bei der Konfiguration des Routers MR814 v2 zu verwenden. Die nachfolgenden Schritte sind nur erforderlich, wenn Sie die Kontoinformationen nicht dynamisch von Ihrem ISP erhalten.

Gehen Sie wie folgt vor, um die Informationen zu ermitteln, die Sie für die Konfiguration der Firewall für einen Internet-Zugriff benötigen:

1. Klicken Sie in der Windows Taskleiste auf "Start" und wählen Sie dann "Einstellungen bzw. Settings" und "Systemsteuerung bzw. Control Panel" aus.
2. Doppelklicken Sie auf das Symbol "Netzwerk bzw. Network". Das Fenster "Netzwerk bzw. Network" mit einer Liste der installierten Komponenten wird angezeigt.
3. Wählen Sie "TCP/IP" aus und klicken Sie auf "Eigenschaften bzw. Properties". Das Dialogfenster "TCP/IP-Eigenschaften bzw. TCP/IP Properties" wird angezeigt.
4. Wählen Sie die Registerkarte "IP-Adresse bzw. IP Address" aus.

Wenn eine IP-Adresse und eine Subnetzmaske angezeigt werden, notieren Sie diese Informationen. Wenn eine Adresse angezeigt wird, verwendet Ihre Konto eine feste (statische) IP-Adresse. Wenn keine Adresse angezeigt wird, verwendet Ihre Konto eine dynamisch zugewiesene IP-Adresse. Klicken Sie auf "IP-Adresse automatisch beziehen bzw. Obtain an IP address automatically".

5. Wählen Sie die Registerkarte "Gateway" aus.

Falls unter "Installierte Gateways bzw. Installed Gateways" eine IP-Adresse angezeigt wird, notieren Sie diese Adresse. Diese ist die Adresse des Gateways des ISPs. Wählen Sie die Adresse aus und klicken Sie auf "Löschen bzw. Remove", um die Gateway-Adresse zu löschen.

6. Wählen Sie die Registerkarte "DNS-Konfiguration bzw. DNS Configuration" aus.

Falls DNS-Serveradressen angezeigt werden, notieren Sie diese Adressen. Falls in dem Feld "Host oder Domain bzw. Host or Domain" Angaben stehen, notieren Sie diese Angaben. Klicken Sie auf "DNS ausschalten bzw. Disable DNS".

7. Klicken Sie auf "OK", um die Änderungen zu speichern, und schließen Sie das Dialogfenster "TCP/IP-Eigenschaften bzw. TCP/IP Properties".

Daraufhin wird wieder das Fenster "Netzwerk bzw. Network" angezeigt.

8. Klicken Sie auf "OK".

9. Starten Sie den PC neu, wenn die entsprechende Aufforderung erscheint. Möglicherweise werden Sie auch aufgefordert, die Windows-CD einzulegen.

ISP-Konfigurationsangaben für Macintosh-Computer ermitteln

Wie bereits erwähnt, müssen Sie die Konfigurationsdaten an Ihrem Macintosh möglicherweise selbst ermitteln, um diese Daten dann bei der Konfiguration des Routers MR814 v2 zu verwenden. Die nachfolgenden Schritte sind nur erforderlich, wenn Sie die Kontoinformationen nicht dynamisch von Ihrem ISP erhalten.

Gehen Sie wie folgt vor, um die Informationen zu ermitteln, die Sie für die Konfiguration der Firewall für einen Internet-Zugriff benötigen:

1. Wählen Sie im Apple-Menü die Option "Systemsteuerungen bzw. Control Panels" und anschließend TCP/IP aus.

Das Fenster "TCP/IP-Systemsteuerung bzw. TCP/IP Control Panel" mit einer Liste der Konfigurationseinstellungen wird angezeigt. Wenn für die Option "Konfigurieren bzw. Configure" die Einstellung "DHCP-Server verwenden bzw. Using DHCP Server" ausgewählt ist, verwendet Ihre Konto eine dynamisch zugewiesene IP-Adresse. In diesem Fall können Sie die Systemsteuerung schließen und die weiteren Schritte überspringen.

2. Wenn eine IP-Adresse und eine Subnetzmaske angezeigt werden, notieren Sie diese Informationen.
3. Falls unter "Router-Adresse bzw. Router address" eine IP-Adresse angezeigt wird, notieren Sie diese Adresse. Diese ist die Adresse des Gateways des ISPs.
4. Falls Namensserver-Adressen angezeigt werden, notieren Sie diese Adressen. Diese sind die DNS-Adressen Ihres ISPs.
5. Falls in dem Feld "Domain suchen bzw. Search domains" Angaben stehen, notieren Sie diese Angaben.
6. Setzen Sie die Option "Konfigurieren bzw. Configure" auf "DHCP-Server verwenden bzw. Using DHCP Server".
7. Schließen Sie die TCP/IP-Systemsteuerung.

Netzwerk neu starten

Nachdem Sie Ihre Computer für die Verwendung der Firewall eingerichtet haben, müssen Sie das Netzwerk zurücksetzen, damit die Gerät in der vorgeschriebenen Weise miteinander kommunizieren können. Starten Sie alle Computer, die mit der Firewall verbunden sind, neu.

Wenn Sie alle Computer für den TCP/IP-Netzwerkbetrieb konfiguriert, neu gestartet und mit dem lokalen Netzwerk des Routers MR814 v2 verbunden haben, können Sie auf die Firewall zugreifen und diesen konfigurieren.

Anhang D

Basisinformationen zu Wireless-Netzwerken

Dieses Kapitel bietet eine Übersicht zum Betrieb von Wireless-Netzwerken.

Wireless-Netzwerke, Übersicht

Der Router MR814v2 entspricht der IEEE-Norm 802.11b (Institute of Electrical and Electronics Engineers) für drahtlose LANs (oder Wireless-LAN, WLANs). Bei einer drahtlosen Verbindung entsprechend 802.11b werden die Daten mit Hilfe der DSSS-Methode (Direct-Sequence Spread-Spectrum) verschlüsselt und in dem frei verfügbaren Funkbereich von 2,4 GHz übertragen. Die maximale Datenübertragungsrate für die drahtlose Verbindung beträgt 11 MBit/s; bei schwachem Funksignal oder bei Störungen wird diese Geschwindigkeit jedoch automatisch auf 5,5, 2 oder 1 MBit/s reduziert.

Die Norm 802.11b wird von der WECA (Wireless Ethernet Compatibility Alliance, siehe <http://www.wi-fi.net>), einer Vereinigung mit dem Ziel der Förderung der Interoperabilität zwischen 802.11b-konformen Geräten, als Wireless Ethernet oder Wi-Fi bezeichnet. Die Norm 802.11b bietet zwei Methoden zur Konfiguration eines drahtlosen Netzwerks - Ad-hoc und Infrastruktur.

Infrastrukturmodus

Wenn ein Access Point vorhanden ist, können Sie das Wireless-LAN im Infrastrukturmodus betreiben. Dieser Modus bietet mehreren Wireless-Netzwerkgeräten innerhalb einer festen Reichweite eine drahtlose Konnektivität, indem er mit einem Wireless-Knoten über eine Antenne kommuniziert.

Im Infrastrukturmodus setzt der Wireless Access Point Funkdaten in Ethernet-Daten um und nimmt so eine Mittlerposition zwischen dem verkabelten LAN und drahtlosen Clients ein. Durch Einbindung mehrerer Access Points über ein verkabeltes Ethernet Backbone kann die Reichweite des Wireless-Netzwerks noch weiter ausgedehnt werden. Mobilcomputer, die den durch einen Access Point abgedeckten Bereich verlassen, treten in den Bereich eines anderen ein. So können sich Wireless-Clients frei zwischen den Access Point-Domains bewegen, ohne dass die Verbindung unterbrochen wird.

Ad-hoc-Modus (Peer-to-Peer Workgroup)

In einem Ad-hoc-Netzwerk werden die Verbindungen zwischen Computern nach Bedarf hergestellt; das heißt, es gibt keine Strukturen oder Fixpunkte im Netzwerk — jeder Knoten kann mit jedem anderen Knoten kommunizieren. Bei dieser Konfiguration gibt es keinen Access Point. In diesem Modus können Sie schnell eine kleine Wireless-Workgroup einrichten, deren Mitglieder mit Hilfe der Microsoft-Netzwerkfunktionen in den verschiedenen Windows-Betriebssystemen Daten austauschen oder Drucker gemeinsam nutzen können. Manche Anbieter bezeichnen Ad-hoc-Netzwerke auch als Peer-to-Peer-Group-Netzwerke.

Bei dieser Konfiguration werden Netzwerkpakete direkt von den vorgesehenen Übertragungs- und Empfangsstationen gesendet und empfangen. Solange sich die Stationen innerhalb der gegenseitigen Reichweite befinden, ist dies die einfachste und kostengünstigste Methode zur Einrichtung eines Wireless-Netzwerks.

Netzwerkname: Extended Service Set Identification (ESSID)

ESSID ist einer von zwei Typen der Service Set Identification (SSID). In einem Ad-hoc-Wireless-Netzwerk ohne Access Points wird die Basic Service Set Identification (BSSID) verwendet. In einem Infrastruktur-Wireless-Netzwerk, das über einen Access Point verfügt, wird ESSID verwendet, das jedoch manchmal weiterhin als SSID bezeichnet wird.

Die SSID ist eine aus max. 32 alphanumerischen Zeichen bestehende Zeichenfolge, die den Namen des Wireless-LAN darstellt. Manche Hersteller bezeichnen die SSID als Netzwerknamen. Damit die drahtlosen Geräte in einem Netzwerk miteinander kommunizieren können, müssen alle Geräte mit derselben SSID konfiguriert werden.

Authentifizierung und WEP

Aufgrund der fehlenden physischen Verbindung zwischen den Knoten sind die drahtlosen Verbindungen anfällig für Lauschangriffe und Datendiebstahl. Um ein bestimmtes Sicherheitsniveau zu bieten, sind in der IEEE-Norm 802.11 zwei Authentifizierungsmethoden (Open System und Shared Key) definiert. Bei der Methode Open System kann ein Wireless-PC sich jedem beliebigen Netzwerk anschließen und Nachrichten empfangen, sofern diese nicht verschlüsselt sind. Bei der Methode Shared Key können nur die PCs, die den korrekten Authentifizierungscode besitzen, an das Netzwerk angebunden werden. Standardmäßig werden IEEE 802.11 Wireless-Geräte in einem Open System-Netzwerk betrieben.

Die WEP-Datenverschlüsselung (Wired Equivalent Privacy) wird verwendet, wenn für die drahtlosen Geräte der Authentifizierungsmodus Shared Key eingestellt wurde. Bei den meisten handelsüblichen Produkten sind zwei Shared Key-Methoden realisiert, die 64-Bit- und die 128-Bit-WEP-Verschlüsselung.

Authentifizierung nach 802.11b

Die Norm 802.11b definiert verschiedene Dienste, durch die die Kommunikation zwischen zwei 802.11b-konformen Geräten geregelt wird. Nur wenn die nachfolgenden Ereignisse eingetreten sind, kann eine 802.11b-Station über einen Access Point (z. B. den integrierten Access Point des FVM318) mit einem Ethernet-Netzwerk kommunizieren:

1. Schalten Sie die Wireless-Station ein.
2. Die Station sucht nach Nachrichten von Access Points, die in Reichweite liegen.
3. Die Station findet an einem Access Point eine Nachricht mit einer identischen SSID.
4. Die Station sendet eine Authentifizierungsanforderung an den Access Point.
5. Der Access Point authentifiziert die Station, d. h. überprüft die Identität der Station.
6. Die Station sendet eine Verknüpfungsanforderung an den Access Point.
7. Der Access Point stellt eine Verbindung zu der Station her.
8. Nun kann die Station über den Access Point mit dem Ethernet-Netzwerk kommunizieren.

Erst nach der Authentifizierung durch einen Access Point kann eine Station eine Verbindung zu dem betreffenden Access Point herstellen oder mit dem Netzwerk kommunizieren. Die Norm IEEE 802.11b definiert zwei Authentifizierungstypen: Open System und Shared Key.

- Bei der Open System-Authentifizierung kann sich jedes Gerät dem Netzwerk anschließen, sofern die SSID des Geräts der SSID des Access Points entspricht. Alternativ dazu kann das Gerät die SSID-Option "ALLE bzw. ANY" verwenden, um eine Verbindung zu allen innerhalb der Reichweite verfügbaren Access Points herzustellen, unabhängig von deren SSID.

- Bei der Shared Key-Authentifizierung müssen die Station und der Access Point denselben WEP-Code besitzen. Diese beiden Authentifizierungsverfahren werden nachfolgend erläutert.

Open System-Authentifizierung

Wenn zwei Geräte die Open System-Authentifizierung verwenden, werden folgende Schritte ausgeführt:

1. Die Station sendet eine Authentifizierungsanforderung an den Access Point.
2. Der Access Point authentifiziert die Station, d. h. überprüft die Identität der Station.
3. Die Station stellt eine Verbindung zu dem Access Point und damit zum Netzwerk her.

Dieser Vorgang ist in der nachfolgenden Abbildung dargestellt.

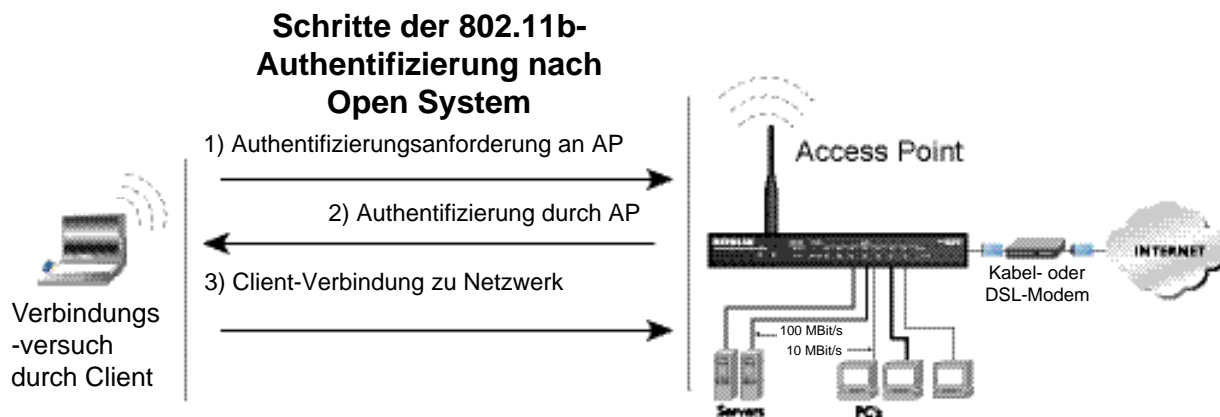
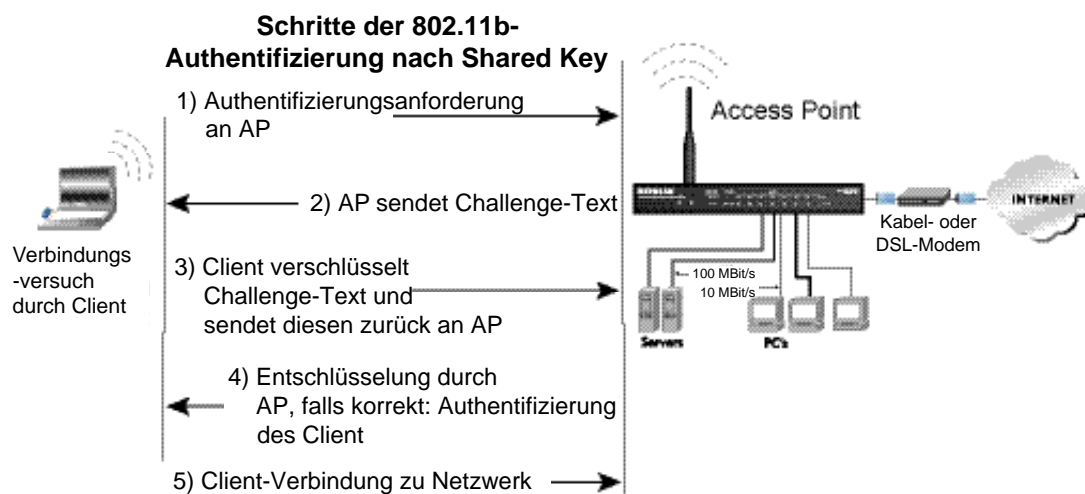


Abbildung 7-4: Open System-Authentifizierung entsprechend 802.11 Shared Key-Authentifizierung

Wenn zwei Geräte die Shared Key-Authentifizierung verwenden, werden folgende Schritte ausgeführt:

1. Die Station sendet eine Authentifizierungsanforderung an den Access Point.
2. Der Access Point sendet den Challenge-Text (Test-Text) an die Station.
3. Die Station verschlüsselt den Challenge-Text mit Hilfe des konfigurierten 64-Bit-oder 128-Bit-Standardcodes und sendet den verschlüsselten Text an den Access Point.
4. Der Access Point entschlüsselt den verschlüsselten Text mit Hilfe des konfigurierten WEP-Codes, der dem Standardcode der Station entspricht. Der Access Point vergleicht den entschlüsselten Text mit dem ursprünglichen Challenge-Text. Wenn die beiden Texte übereinstimmen, bedeutet dies, dass der Access Point und die Station denselben WEP-Code verwenden; der Access Point bestätigt die Identität der Station.
5. Die Station stellt eine Verbindung zum Netzwerk her.

Wenn der entschlüsselte Text nicht mit dem ursprünglichen Challenge-Text übereinstimmt (der Access Point und die Station also nicht denselben WEP-Code verwenden), verweigert der Access Point die Authentifizierung der Station; das heißt, die Station kann weder mit dem 802.11b-Netzwerk noch mit dem Ethernet-Netzwerk kommunizieren.



Dieser Vorgang ist in der nachfolgenden Abbildung dargestellt.

Abbildung 7-5: Shared Key-Authentifizierung nach 802.11

Übersicht der WEP-Parameter

Vor der Aktivierung von WEP in einem 802.11b-konformen Netzwerk müssen Sie den erforderlichen Verschlüsselungstyp und die gewünschte Codegröße festlegen. In der Regel sind für Produkte nach 802.11b drei Optionen für die WEP-Verschlüsselung verfügbar:

1. **Do Not Use WEP bzw. WEP nicht verwenden:** In dem 802.11b-Netzwerk ist keine Verschlüsselung der Daten erforderlich. Zur Authentifizierung verwendet das Netzwerk das Authentifizierungsverfahren Open System.
2. **Use WEP for Encryption bzw. WEP für Verschlüsselung verwenden:** Ein 802.11b-Sendegerät verschlüsselt den Datenteil jedes Pakets, das es sendet, mit einem konfigurierten WEP-Code. Das 802.11b-Empfangsgerät entschlüsselt die Daten mit demselben WEP-Code. Zur Authentifizierung verwendet das 802.11b-Netzwerk das Authentifizierungsverfahren Open System.
3. **Use WEP for Authentication and Encryption bzw. WEP für Authentifizierung und Verschlüsselung verwenden:** Ein 802.11b-Sendegerät verschlüsselt den Datenteil jedes Pakets, das es sendet, mit einem konfigurierten WEP-Code. Das 802.11b-Empfangsgerät entschlüsselt die Daten mit demselben WEP-Code. Zur Authentifizierung verwendet das 802.11b-Netzwerk das Authentifizierungsverfahren Shared Key.

Hinweis: Manche Access Points gemäß 802.11b unterstützen auch die Option “WEP nur für Authentifizierung verwenden bzw. Use WEP for Authentication Only” (Shared Key-Authentifizierung ohne Datenverschlüsselung).

Codegröße

Die Norm IEEE 802.11b definiert zwei WEP-Verschlüsselungsverfahren: 40-Bit und 128-Bit.

Bei der 64-Bit-WEP-Datenverschlüsselung ist eine aus fünf Zeichen (40 Bit) bestehende Eingabe zulässig. In Kombination mit den 24 vom Hersteller definierten Bit wird ein 64-Bit-Verschlüsselungscode generiert. (Die 24 vom Hersteller definierten Bit können nicht vom Benutzer konfiguriert werden.) Dieser Verschlüsselungscode wird zum Ver- und Entschlüsseln aller über die Wireless-Schnittstelle übermittelten Daten verwendet. Einige Anbieter bezeichnen die 64-Bit-WEP-Datenverschlüsselung als 40-Bit-WEP-Datenverschlüsselung, da der vom Benutzer konfigurierbare Schlüssel, der bei der Verschlüsselung verwendet wird, nur 40 Bit lang ist.

Die 128-Bit WEP-Datenverschlüsselungsmethode besteht aus 104 konfigurierbaren Bit. Ähnlich wie bei der 40-Bit-WEP-Datenverschlüsselung werden die restlichen 24 Bit vom Hersteller festgelegt und können nicht vom Benutzer konfiguriert werden. Manche Hersteller gestatten die Eingabe von Passphrasen an Stelle der Hexadezimalzeichen, um die Erzeugung des Verschlüsselungscodes zu erleichtern.

Die 128-Bit-Verschlüsselung bietet ein größeres Maß an Sicherheit als die 40-Bit-Verschlüsselung; allerdings ist die 128-Bit-Verschlüsselung außerhalb der Vereinigten Staaten unter Umständen auf Grund von US-Exportbestimmungen nicht verfügbar.

802.11b-Produkte, die für die 40-Bit-Verschlüsselung konfiguriert wurden, unterstützen in der Regel bis zu vier WEP-Codes. Jeder 40-Bit-WEP-Code wird dargestellt als fünf Zeichenpaare, die jeweils aus zwei Hexadezimalzeichen (0-9 und A-F) bestehen. Ein Beispiel eines 40-Bit-WEP-Codes wäre "12 34 56 78 90".

802.11b-Produkte, die für die 128-Bit-Verschlüsselung konfiguriert wurden, unterstützen in der Regel vier WEP-Codes; manche Hersteller unterstützen jedoch nur einen 128-Bit-Code. Der 128-Bit-WEP-Code wird dargestellt als 13 Zeichenpaare, die jeweils aus zwei Hexadezimalzeichen (0-9 und A-F) bestehen. Ein Beispiel eines 128-Bit-WEP-Codes wäre "12 34 56 78 90 AB CD EF 12 34 56 78 90".

Hinweis: Access Points gemäß 802.11b können in der Regel bis zu vier 128-Bit-WEP-Codes speichern; auf manchen 802.11b-konformen Client-Adaptern kann jedoch nur ein 128-Bit-WEP-Code gespeichert werden. Daher sollten Sie in jedem Fall sicherstellen, dass die Konfigurationen Ihres 802.11b-konformen Zugangs- und des Client-Adapters übereinstimmen.

Optionen bei der WEP-Konfiguration

Die WEP-Einstellungen müssen auf allen 802.11b-Geräten übereinstimmen, die zu demselben, durch die SSID gekennzeichneten Wireless-Netzwerk gehören. Wenn Ihre mobilen Clients sich zwischen mehreren Access Points hin- und herbewegen, müssen alle 802.11b-Access Points und alle 802.11b-Client-Adapter im Netzwerk dieselben WEP-Einstellungen aufweisen.

Hinweis: Unabhängig von den für einen Access Point eingegeben Codes ist sicherzustellen, dass für den Client-Adapter dieselben Codes in derselben Reihenfolge eingegeben werden. Das heißt, WEP-Code 1 auf dem Access Point muss mit WEP-Code 1 auf dem Client-Adapter übereinstimmen, WEP-Code 2 auf dem Access Point muss mit WEP-Code 2 auf dem Client-Adapter übereinstimmen, usw.

Hinweis: Der Access Point und die Client-Adapter können verschiedene WEP-Standardcodes besitzen, sofern die Codes in derselben Reihenfolge vorliegen. Das heißt, der Access Point kann WEP-Code 2 als Standardcode für die Übertragung verwenden, während ein Client-Adapter WEP-Code 3 als Standardcode für die Übertragung verwenden kann. Die beiden Geräte können dennoch miteinander kommunizieren, sofern der WEP-Code 2 des Access Points mit dem WEP-Code 2 des Clients und der WEP-Code 3 des Access Points mit dem WEP-Code 3 des Clients identisch ist.

Wireless-Kanäle

Wireless-Knoten entsprechend IEEE 802.11 kommunizieren über Funkfrequenzsignale innerhalb des für industrielle, wissenschaftliche und medizinische Zwecke reservierten ISM-Frequenzbands zwischen 2,4 und 2,5 GHz miteinander. Benachbarte Kanäle liegen dabei jeweils um 5 MHz auseinander. Aufgrund des Spread-Spektrum-Effekts der Signale verwendet jedoch ein Knoten, der Signale über einen bestimmten Kanal sendet, ein Frequenzspektrum, das die zentrale Kanalfrequenz um 12,5 MHz über- und unterschreitet. Das bedeutet, dass es bei zwei separaten Wireless-Netzwerken, die benachbarte Kanäle (z. B. Kanal 1 und Kanal 2) im selben Bereich verwenden, zu Interferenzen kommt. Durch Nutzung zweier Kanäle mit maximaler Kanaltrennung werden die Störsignale verringert und im Vergleich zu Netzwerken mit minimaler Kanaltrennung deutliche Leistungssteigerungen erzielt.

Die verwendeten Funkfrequenzkanäle sind in Tabelle 7-4 aufgeführt:

Tabelle 7-4. Funkfrequenzkanäle gemäß 802.11

Kanal	Mittelfrequenz	Frequenzstreuungsbereich
1	2412 MHz	2399,5 MHz - 2424,5 MHz
2	2417 MHz	2404,5 MHz - 2429,5 MHz
3	2422 MHz	2409,5 MHz - 2434,5 MHz
4	2427 MHz	2414,5 MHz - 2439,5 MHz
5	2432 MHz	2419,5 MHz - 2444,5 MHz
6	2437 MHz	2424,5 MHz - 2449,5 MHz
7	2442 MHz	2429,5 MHz - 2454,5 MHz
8	2447 MHz	2434,5 MHz - 2459,5 MHz
9	2452 MHz	2439,5 MHz - 2464,5 MHz
10	2457 MHz	2444,5 MHz - 2469,5 MHz
11	2462 MHz	2449,5 MHz - 2474,5 MHz
12	2467 MHz	2454,5 MHz - 2479,5 MHz
13	2472 MHz	2459,5 MHz - 2484,5 MHz

Hinweis: Welche der verfügbaren Kanäle von Wireless-Produkten unterstützt werden, variiert von Land zu Land.

Die bevorzugte Kanaltrennung zwischen Kanälen in benachbarten Wireless-Netzwerken beträgt 25 MHz (5 Kanäle). Das bedeutet, Sie können innerhalb Ihres Wireless-Netzwerks bis zu drei verschiedene Kanäle verwenden. In den Vereinigten Staaten gibt es nur 11 verwendbare Wireless-Kanäle. Es wird empfohlen, mit Kanal 1 zu beginnen und dann im Fall eines Netzwerkausbaus mit Kanal 6 und Kanal 11 fortzufahren, da diese drei Kanäle nicht überlappen.

10BASE-T	IEEE-Spezifikation 802.3 für Ethernet mit 10 MBit/s mit Verkabelung durch verdrehte Doppelleitungen.
100BASE-Tx	IEEE-Spezifikation 802.3 für Ethernet mit 100 MBit/s mit Verkabelung durch verdrehte Doppelleitungen.
802.11b	IEEE-Spezifikation für Wireless-Netzwerke mit 11 MBit/s und DSSS-Technologie (Direct-Sequence Spread-Spectrum für Betrieb im frei verfügbaren Funkfrequenzbereich von 2,5 GHz.
Denial of Service -Angriff	DoS. Ein Hackerangriff, der den Betrieb oder die Kommunikation Ihres Computer oder Netzwerks lahmlegen soll.
DHCP	Siehe Dynamic Host Configuration Protocol.
DNS	Siehe Domain-Namensserver.
Domain-Name	Ein beschreibender Name einer Adresse oder Adressgruppe im Internet. Domain-Namen bestehen aus dem registrierten Namen sowie einer Reihe fester Top-Level-Endungen wie .com, .edu, .uk, usw. Bei der Adresse mail.NETGEAR.com beispielsweise ist "mail" ein Servername und "NETGEAR.com" die Domäne.
Domain -Namensserver	Ein Domain-Namensserver (DNS) setzt beschreibende Namen von Netzwerkressourcen (z. B. www.NETGEAR.com) in numerische IP-Adressen um.
Dynamic Host Configuration Protocol	DHCP. Ein Ethernet-Protokoll, das festlegt, wie ein zentraler DHCP-Server Angaben zur Netzwerkkonfiguration an mehrere DHCP-Clients verteilen kann. Zu diesen zugewiesenen Informationen gehören IP-Adressen, DNS-Adressen und Gateway- bzw. Router-Adressen.
Gateway	Ein lokales Gerät, in der Regel ein Router, das die Hosts in einem lokalen Netzwerk mit anderen Netzwerken verbindet.
IP	Siehe Internet Protocol.

IP-Adresse	Eine aus vier Byte bestehende Zahl, die jeden Host im Internet eindeutig definiert. Adressbereiche werden von Internic, einer für diesen Zweck gegründeten Vereinigung, zugewiesen. Wird normalerweise in der Dezimalschreibweise mit Dezimalpunkten zur Trennung der Bytes angegeben (z. B. 134.177.244.57).
ISP	Internet Service Provider.
Internet Protocol	Das wichtigste Netzwerkprotokoll im Internet. Bildet in Verbindung mit dem Transfer Control Protocol (TCP) das TCP/IP.
LAN	Siehe Lokales Netzwerk.
Lokales Netzwerk	Local Area Network, LAN. Ein Kommunikationsnetzwerk für Benutzer innerhalb eines abgegrenzten Bereichs, z. B. eines Stockwerks eines Gebäudes. Durch ein LAN werden in der Regel mehrere PC mit gemeinsam verwendeten Netzwerkgeräten wie Speichermedien und Druckern verbunden. Obwohl zahlreiche Verfahren zur Realisierung eines LAN vorhanden sind, bildet Ethernet die häufigste Form der Verbindung von PCs.
MAC-Adresse	Media Access Control-Adresse. Eine eindeutige 48-Bit-Hardwareadresse, die jedem Ethernet-Knoten zugewiesen wird. Wird normalerweise angegeben im Format 01:23:45:67:89:ab.
MBit/s	Megabit pro Sekunde.
MSB	Siehe Most Significant Bit oder Most Significant Byte.
MTU	Siehe Maximum Transmission Unit.
NAT	Siehe Network Address Translation.
Netzmaske	Ein Zahl, aus der hervorgeht, welcher Teil einer IP-Adresse die Netzwerkadresse und welcher Teil die Host-Adresse des Netzwerks darstellt. Kann in Dezimalschreibweise oder als Zahl, die an die IP-Adresse angehängt wird, dargestellt werden. Beispielsweise kann ein 28-Bit-Maske ab dem MSB als 255.255.255.192 oder als an die IP-Adresse angehängter Ausdruck "/28" dargestellt werden.
Network Address Translation	Netzwerk-Adressumsetzung. Ein Verfahren, bei dem mehrere Hosts gemeinsam ein IP-Adresse verwenden, um auf das Internet zuzugreifen.
Paket	Ein Informationsblock, der in einem Netzwerk versendet wird. Ein Paket enthält in der Regel die Netzwerkadresse der Quelle und des Ziels, diverse Protokoll- und Längenangaben, einen Datenblock sowie eine Prüfsumme (Checksum).
PPP	Siehe Point-to-Point Protocol.

PPP over Ethernet	PPPoE. PPP over Ethernet ist ein Protokoll für die Anbindung dezentraler Hosts an das Internet über eine Standleitung; dabei wird eine Wählverbindung simuliert.
PPTP	Point-to-Point Tunneling Protocol. Eine Methode zur Einrichtung eines virtuellen Privatnetzes (VPN) durch Einbettung des Netzwerkprotokolls von Microsoft in Internet-Pakete.
Point-to-Point Protocol	PPP. Ein Protokoll, mit dessen Hilfe ein Computer über TCP/IP eine direkte Verbindung zum Internet herstellen kann.
RFC	Request For Comment (Kommentaranforderung). Bezieht sich auf Dokumente, die durch die Internet Engineering Task Force (IETF) veröffentlicht wurden und Vorschläge zu Standardprotokollen und -verfahren für das Internet enthalten. RFCs werden veröffentlicht unter www.ietf.org .
RIP	Siehe Routing Information Protocol.
Router	Ein Gerät, das Daten zwischen Netzwerken weiterleitet. Ein IP-Router leitet Daten auf der Basis einer IP-Quellenadresse und einer IP-Zieladresse weiter.
Routing Information Protocol	Ein Protokoll, bei dem Router in regelmäßigen Abständen Informationen untereinander austauschen, um zwischen Quellen und Zielen die Pfade mit dem kürzesten Übertragungsweg zu ermitteln.
Subnetzmaske	Siehe Netzmaske.
UPnP	Siehe Universal Plug and Play.
Universal Plug and Play	UPnP. Eine Netzwerkarchitektur, die die Kompatibilität von Netzwerkgeräten, Software und Peripheriegeräten der über 400 Hersteller sicherstellt, die Mitglied des Universal Plug and Play Forums sind. UPnP-konforme Router bieten Breitbenutzern zu Hause und in kleineren Unternehmen die Möglichkeit, nahtlos und ohne erkennbaren Bruch an Online-Spielen, Videokonferenzen und anderen Peer-zu-Peer-Diensten teilzunehmen.
UTP	Unshielded Twisted Pair (ungeschirmte verdrehte Doppelleitung). Das Kabel, das für Ethernet-Netzwerke 10BASE-T und 100BASE-Tx verwendet wird.
WAN	Siehe Wide Area Network.
WEP	Wired Equivalent Privacy. WEP ist ein Datenverschlüsselungsprotokoll für Wireless-Netzwerke gemäß 802.11b. Alle Wireless-Knoten und Access Points im Netzwerk werden mit einem 64-Bit- oder 128-Bit-Shared Key für die Datenverschlüsselung konfiguriert.
Wide Area Network	WAN, Fernnetz. Eine Fernverbindung, mit der lokale Netze erweitert werden können oder mehrere lokale Netze an verschiedenen Standorten zusammengeschaltet werden können. Das Internet ist ein großes WAN.

Windows Internet Naming Service WINS. Windows Internet Naming Service ist ein Serverprozess zur Umsetzung der Windows-gestützten Computernamen in IP-Adressen. Wenn ein dezentrales Netzwerk einen WINS-Server enthält, kann Ihr Windows PCs Informationen zu seinen lokalen Hosts bei diesem WINS-Server abfragen. Damit können Sie sich mit Ihrem PCs über die Netzwerkumgebung in diesem dezentralen Netzwerk bewegen.

WINS Siehe Windows Internet Naming Service.

Zahlen

64- oder 128-Bit-WEP 3-6

802.11b D-1

A

Address Resolution Protocol B-9

Ad-hoc-Modus D-2

Anmeldung 2-11

Anschlussbelegung, Ethernet-Kabel B-12

Authentifizierungs-Server 2-12

Auto MDI/MDI-X B-13

Auto Uplink 1-3, B-13

B

BSSID D-2

Bereich 3-1

Bereich, Portweiterleitung 6-2

C

Content Filtering 1-2, 4-1

Crossover-Kabel 1-3, 7-2, B-12, B-13

D

Datum und Uhrzeit 7-7

Dezentrale Verwaltung 6-12

Dienstnummern 4-4

DMZ-Standardserver 6-4

DoS-Angriff (Denial of Service) B-11

DHCP 1-4, B-10

DHCP-Client ID C-16

DMZ 1-3, 6-2, 6-5

DNS, dynamisch 6-9

DNS-Proxy 1-4

DNS-Server 6-4, 2-14, 2-15, 2-17, C-20

Domain C-20

Domain-Name 2-14, 2-17

Domain-Namensserver (DNS) B-10

Dynamischer DNS 6-9

E

Einstellungen für Wireless-Netzwerk 3-3

EnterNet C-18

Erster Port 6-2

ESSID 3-7, D-2

Ethernet 1-3

Ethernet-Kabel B-12

F

Funktionen der Firewall 1-2

Flash-Speicher für Firmware-Upgrades 1-2

Front 1-6, 1-7

Funktionsweise eines Routers B-1

Fehlersuche 7-1

G

Gateway-Adresse C-20

Grundlagen der drahtlosen Konnektivität 3-7

H

Hardwareanforderungen 2-1

Host-Name 2-3, 5-2

I

IANA

Kontakt B-2

IETF B-1

Website-Adresse B-7

Infrastrukturmodus D-2

Installation 1-4

Internet-Konto

Adressdaten C-18

ermitteln C-18

Internet Service Provider 2-1

IP-Adressen C-19, C-20

und NAT B-8

und das Internet B-2

zuweisen B-2, B-9

automatisch generiert 7-3

privat B-7

umsetzen B-9

IP-Konfiguration über DHCP B-10

IP-Netzwerke

für Macintosh C-16

für Windows C-2, C-7

ISP2-1

K

Kabel, Belegung B-12

Kabel der Kategorie 5 2-1, B-13

Kanal 3-5

Kennwort 2-13

Kennwort

wiederherstellen 7-7

Konfiguration

automatisch über DHCP 1-4

Sicherungskopie 5-7

löschen 5-8

wieder herstellen 5-6

Router, Anfang 2-1

Kontoname 2-14, 2-17, 5-2

Konventionen

Schreibweise xii

Konfiguration löschen 5-8

Konfiguration wiederherstellen 5-6

Konfigurationsassistent 2-1

Kunden-Support iii

L

LED-Beschreibung 1-6

Fehlersuche 7-2

Protokoll senden 4-7

Protokolleinträge 4-6

Letzter Port 6-2

M

MAC-Adresse 7-7, B-9

Daten ausspähen 2-14, 2-17, 7-5

MAC-Adresse ausspähen 7-5

Macintosh C-19

für IP-Netzwerkbetrieb konfigurieren C-16

DHCP-Client ID C-16

ISP-Konfigurationsdaten empfangen C-20

Maskierung C-18

MDI/MDI-X B-13

MDI/MDI-X-Verkabelung B-12

Metric bzw. Anzahl 6-11

Menü für LAN-IP-Konfiguration 6-6

Menü Portweiterleitung 6-1

N

NAT C-18

NAT. Siehe Network Address

Translation Netzwerkmaske

Umsetzungstabelle B-6

Network Time Protocol 4-8, 7-7
Netzwerk Adress-Umsetzung 1-3, B-8, C-18
NTP 4-8, 7-7

O

Open System-Authentifizierung D-3

P

Packungsinhalt 1-5
Passphrase 1-2, 3-7, 3-11
PC, für Konfiguration verwenden C-21
Ping 6-5
Platzierung 3-1
Port-Filter 4-3
Portnummern 4-3
Portweiterleitung 6-1
Portweiterleitung hinter NAT B-9
PPPoE 1-4, C-18
PPP over Ethernet 1-4, C-18
Primärer DNS-Server 2-9, 2-15, 2-17
Protokolle
 Address Resolution B-9
 DHCP 1-4, B-10
 Routing Information 1-3, B-2
 Support 1-1
Publikationen, zugehörige B-1

R

Reservierte IP-Adressen 6-8
RFC
 1466 B-7, B-9
 1597 B-7, B-9
 1631 B-8, B-9
 Suchen B-7
Richtlinien für Wireless-Reichweite 3-1

RIP (Router Information Protocol) 6-7
Routerstatus 5-1
Routing Information Protocol 1-3, B-2
Rückseite 1-7

S

Schutz vor Denial of Service (DoS) 1-2
Sekundärer DNS-Server 2-9, 2-15, 2-17
Shared Key-Authentifizierung D-3
Sicherheit 1-1, 1-3
Sicherheit bei Wireless-Betrieb 3-2
Sicherungskopie der Konfiguration 5-7
SMTP 4-8
Sommerzeit 4-8, 7-7
SSID 3-3, 3-7, 3-8, D-2
Stateful Packet Inspection 1-2, B-11
Statisches Routing 6-9
Subnetz-Adressierung B-5
Subnetzmaske B-6, C-19, C-20
System für Wireless-Authentifizierung 3-5

T

TCP/IP-Eigenschaften

überprüfen für Macintosh C-17

überprüfen für Windows C-6, C-15

TCP/IP konfigurieren C-1

Netzwerk, Fehlersuche 7-5

U

Uhrzeit 7-7

Uplink-Schalter B-12

USB C-18

V

Verkabelung B-12

Verlässlicher Host 4-3

Verschlüsselungsmodus 3-6

W

WAN 6-4

WEP D-3

WEP-Verschlüsselung 1-2

Werkseinstellungen wiederherstellen 5-8

Wi-Fi D-1

Windows, für IP-Routing konfigurieren C-2, C-7

winipcfg, Dienstprogramm C-6

WinPOET C-18

Wired Equivalent Privacy. Siehe WEP

Wireless-Zugang 2-3

Wireless-Authentifizierung 3-5

Wireless-Verschlüsselung 3-5

Wireless-Ethernet D-1

Wireless-Leistungsfähigkeit 3-1

Wireless-Zugang über MAC-Adresse
einschränken 3-8

World Wide Web iii

Z

Zeitstempel 4-8

Zeitzone 4-8

Zugriffsliste für Wireless-Karte 3-3