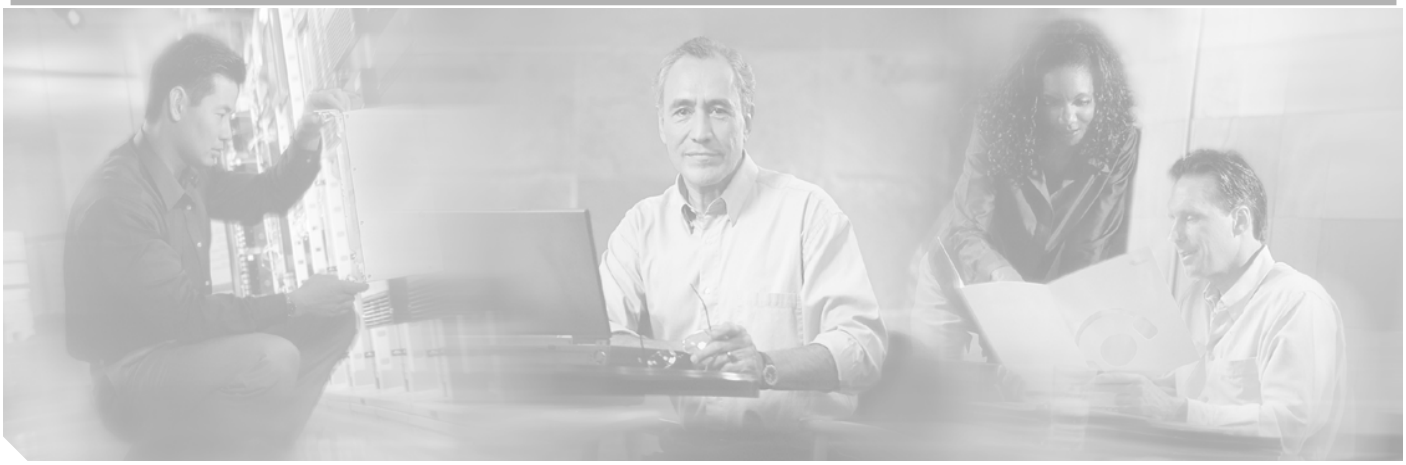


Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie – Software-Konfigurationshandbuch

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel.: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Teilenummer des Dokuments: OL-7138-01

Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie – Software-Konfigurationshandbuch

TIEL 4 **Referenzinformationen**

Einführung

Dieses Software-Konfigurationshandbuch enthält eine Anleitung zum Gebrauch der Cisco-Befehlszeilenschnittstelle (CLI, Command Line Interface) für die Konfiguration von Funktionen an den folgenden Routermodellen der Cisco 800-Serie:

- Router der Cisco 850-Serie
  - Cisco 851 Ethernet Access Router
  - DSL-Zugangsrouter Cisco 857
- Router der Cisco 870-Serie
  - Cisco 871 Ethernet Access Router
  - DSL Access Router Cisco 876, Cisco 877 und Cisco 878

In dieser Einführung werden die Ziele, die Zielgruppe sowie der Aufbau dieses Handbuchs und die für den Text sowie die Angabe von Befehlen geltenden Konventionen beschrieben. Diese Einführung ist in folgende Themen unterteilt:

Zielgruppe

Dieses Handbuch richtet sich sowohl an Netzwerkadministratoren, die noch nicht oder kaum mit der Konfiguration von Routern vertraut sind, als auch an Administratoren, die im Umgang mit Routern bereits sehr erfahren sind. Dieses Handbuch kann in folgenden Situationen nützliche Referenzinformationen bieten:

- Sie haben die Software bereits mit dem Cisco Router Web Setup-Tool konfiguriert, möchten jetzt aber zusätzliche, erweiterte Softwarefunktionen mit der Befehlszeilenschnittstelle (CLI) konfigurieren.
- Sie möchten die Software ausschließlich per CLI konfigurieren.

Hinweis Netzwerkadministratoren, die mit Cisco-Routern noch nicht ausreichend vertraut sind, wird dringend empfohlen, den Cisco Router and Security Device Manager (SDM) zu verwenden. SDM ist ein webbasiertes Konfigurationstool, mit dem LAN- und WAN-Schnittstellen, Routing, Network Address Translation (NAT), Firewalls, VPNs und andere Funktionen auf dem Router konfiguriert werden können. SDM-Versionshinweise und sonstige Dokumentation zu SDM erhalten Sie im Internet auf http://www.cisco.com/go/sdm über den Link „**Technical Documentation**“.

Lesen Sie den Abschnitt „Struktur“ in dieser Einführung, wenn Sie erfahren möchten, in welchen Kapiteln die zum Konfigurieren Ihres Routers benötigten Informationen vorliegen.

Struktur

Dieses Handbuch enthält die folgenden Informationen:

Teil 1: Erste Schritte

- Kapitel 1, „Grundlegende Routerkonfiguration“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration der grundlegenden Routerfunktionen und -schnittstellen.

Teil 2: Konfigurieren des Routers für einen Ethernet- und DSL-Zugang

- Kapitel 2, „Beispiele für den Netzwerkeinsatz“ – Dieses Kapitel bietet eine Übersicht über Teil 2 des Handbuchs.
- Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration von PPPoE mit Network Address Translation (NAT, Netzadress-Übersetzung) für Ihren Cisco-Router.
- Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration von PPPoA mit Network Address Translation (NAT, Netzadress-Übersetzung) für Ihren Cisco-Router.
- Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration des Cisco-Routers mit mehreren VLANs und zur Konfiguration des Routers als DHCP-Server.
- Kapitel 6, „Konfigurieren eines VPN mit Easy VPN und einem IPSec-Tunnel“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration eines virtuellen privaten Netzwerks (VPN) mit einem sicheren IP-Tunnel unter Verwendung von Cisco Easy VPN.
- Kapitel 7, „Konfigurieren von VPNs mit einem IPSec-Tunnel und Generic Routing Encapsulation“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration eines VPN mit einem sicheren IP-Tunnel unter Verwendung von GRE (Generic Routing Encapsulation).

- Kapitel 8, „Konfigurieren einer einfachen Firewall“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration einer einfachen Firewall auf Ihrem Cisco-Router.
- Kapitel 9, „Konfigurieren einer Wireless-LAN-Verbindung“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration einer Wireless-LAN-Verbindung auf Ihrem Cisco-Router.
- Kapitel 10, „Beispielkonfiguration“ – Dieses Kapitel enthält ein zusammenfassendes Konfigurationsbeispiel zur Verdeutlichung der Funktionen, die in den vorhergehenden Kapiteln konfiguriert wurden.

Teil 3: Konfigurieren zusätzlicher Funktionen und Fehlerbehebung

- Kapitel 11, „Weitere Konfigurationsoptionen“ – Dieses Kapitel bietet eine Übersicht über Teil 3 des Handbuchs.
- Kapitel 12, „Konfigurieren von Sicherheitsfunktionen“ – In diesem Kapitel wird die grundlegende Konfiguration der Cisco IOS-Sicherheitsfunktionen erläutert, einschließlich der Firewall- und VPN-Konfiguration.
- Kapitel 13, „Konfigurieren von Reserve-Wählleitung und Remoteverwaltung“ – Dieses Kapitel enthält eine Anleitung zur Konfiguration der Reserve-Wählleitung und Remoteverwaltung auf dem Cisco-Router.
- Kapitel 14, „Fehlerbehebung“ – Dieses Kapitel enthält Informationen zur Erkennung und Behebung von Problemen mit der ADSL-Leitung und der Telefonschnittstelle. Darüber hinaus wird erläutert, wie ein Softwarekennwort wiederhergestellt werden kann.

Teil 4: Referenzinformationen

- Anhang A, „Grundlegende Fertigkeiten für die Arbeit mit der Cisco IOS-Software“ – In diesem Anhang werden Grundkenntnisse über die Cisco IOS-Software vermittelt, die Sie vor Beginn der Konfigurationsvorgänge beherrschen sollten.
- Anhang B, „Konzepte“ – In diesem Anhang sind allgemeine Begriffserklärungen zu den Funktionen enthalten.
- Anhang C, „ROM Monitor“ – In diesem Anhang wird die Verwendung des Programms ROM Monitor (ROMMON) beschrieben.
- Anhang D, „Allgemeine Portzuweisungen“ – In diesem Anhang sind die momentan zugewiesenen TCP- und UDP-Portnummern (Transmission Control Protocol, User Datagram Protocol) aufgeführt.
- Index

Konventionen

In diesem Handbuch werden die in den folgenden Abschnitten beschriebenen Konventionen für Anweisungen und Informationen verwendet.

Hinweise, Warnungen und Tipps

Für Hinweise, Warnungen und Tipps für zeitsparende Vorgehensweisen werden folgende Konventionen und Symbole verwendet:

Hinweis Dieses Symbol bezeichnet einen *wichtigen Hinweis für den Leser*. Hinweise enthalten nützliche Empfehlungen oder Verweise auf zusätzliche Materialien, die nicht in diesem Handbuch enthalten sind.

Achtung Dieses Symbol *rät dem Leser zur Vorsicht*. In dieser Situation könnte eine von Ihnen ausgeführte Handlung zu Schäden an Geräten oder einem Datenverlust führen.

Zeitersparnis Dieses Symbol drückt aus, dass *mit dem beschriebenen Vorgang Zeit eingespart werden kann*.

Konventionen für Befehle

In Tabelle 1 wird die in diesem Handbuch verwendete Befehlssyntax beschrieben.

Tabelle 1 Konventionen für Befehlssyntax

Konvention	Beschreibung
fett gedruckt	Befehle und Schlüsselwörter
kursiv gedruckt	Befehlseingaben, die von Ihnen selbst vorgenommen werden
[ ]	Optionale Schlüsselwörter und Standardantworten auf Eingabeaufforderungen des Systems werden in eckigen Klammern angegeben.
{**x** | **x** | **x**}	Eine Auswahl von Schlüsselwörtern (durch **x** symbolisiert) wird jeweils in Klammern, durch vertikale Striche getrennt, angezeigt. Sie müssen in diesem Fall ein Schlüsselwort auswählen.
^ oder Strg	Steht für die *Strg-Taste*. Wenn beispielsweise in einer Anweisung *^D* oder *Strg-D* angegeben ist, müssen Sie die Taste D drücken und gleichzeitig die Strg-Taste gedrückt halten.
`Bildschirmschrift`	Beispiele für Informationen, die auf dem Bildschirm angezeigt werden.
`fette Bildschirmschrift`	Beispiele für Daten, die Sie selbst eingeben müssen.

Verwandte Dokumente

Die folgenden Dokumente enthalten weitere Informationen zu den jeweils genannten Routern:

- *Zugangsrouter der Cisco 850-Serie und Cisco 870-Serie – Kurzanleitung zur Verkabelung und Einrichtung*
- *Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie – Hardware-Installationshandbuch*
- *Cisco Router and Security Device Manager (SDM) Quick Start Guide*
- *Cisco Access Router Wireless Configuration Guide*
- *Upgrading Memory in Cisco 800 Routers*

- *Regulatory Compliance and Safety Information for Cisco 800 Series and SOHO Series Routers*
- *Declarations of Conformity and Regulatory Information for Cisco Access Products with 802.11a/b/g and 802.11b/g Radios*

Anfordern der Dokumentation

Dokumentation von Cisco und weitere Literatur steht Ihnen unter **Cisco.com** zur Verfügung. Cisco bietet Ihnen zudem mehrere Methoden zum Anfordern von technischer Unterstützung und anderen technischen Ressourcen. In diesen Abschnitten wird erläutert, wie Sie technische Informationen von Cisco Systems anfordern.

Cisco.com

Über folgenden URL können Sie auf die aktuellste Cisco-Dokumentation zugreifen:

http://www.cisco.com/univercd/home/home.htm

Die Cisco-Website finden Sie unter folgendem URL:

http://www.cisco.com

Über folgenden URL können Sie auf internationale Cisco-Websites zugreifen:

http://www.cisco.com/public/countries_languages.shtml

Dokumentations-DVD

Die Cisco-Dokumentation sowie weitere Unterlagen sind in einem DVD-Dokumentationspaket enthalten, die unter Umständen mit Ihrem Produkt geliefert wurde. Die Dokumentations-DVD wird regelmäßig aktualisiert und ist daher möglicherweise aktueller als die gedruckte Dokumentation. Die Dokumentations-DVD ist einzeln erhältlich.

Bei **Cisco.com** registrierte Benutzer (Cisco-Direktkunden) können die Dokumentations-DVD von Cisco (Produktnummer: DOC-DOCDVD=) über das Bestelltool (Ordering) oder über den Cisco Marketplace bestellen.

Cisco Bestelltool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Bestellen von Dokumentation

Anweisungen zum Bestellen von Dokumentation finden Sie unter folgendem URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

Sie können die Cisco-Dokumentation auf folgende Weise beziehen:

- Bei **Cisco.com** registrierte Kunden (Cisco-Direktkunden) können die Cisco-Produktdokumentation mit dem Bestelltool (Ordering) bestellen:

  http://www.cisco.com/en/US/partner/ordering/

- Nicht registrierte Benutzer von **Cisco.com** können die Dokumentation über einen örtlichen Kundenbeauftragten bestellen. Wenden Sie sich hierzu unter 001 408 526-7208 bzw. in den USA unter 1.800 553-NETS (6387) an die Firmenzentrale Cisco Systems Corporate Headquarters in Kalifornien, USA.

Feedback zur Dokumentation

Sie können uns Ihre Anmerkungen zur technischen Dokumentation an die Adresse **bug-doc@cisco.com** senden.

Sie können Ihre Kommentare per Post senden, indem Sie die Antwortkarte (sofern vorhanden) hinter dem Deckblatt verwenden oder an folgende Adresse schreiben:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883, USA

Für Ihre Kommentare bedanken wir uns im Voraus.

Überblick über Cisco-Produktsicherheit

Cisco bietet einen kostenlosen Zugang zu einem Onlineportal für Produktsicherheitsfragen, das unter folgendem URL aufgerufen werden kann:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Auf dieser Website können Sie folgende Aufgaben ausführen:

- Sicherheitslücken in Cisco-Produkten melden.
- Unterstützung bei sicherheitsrelevanten Vorfällen anfordern, die Cisco-Produkte betreffen.
- Anmelden, um Sicherheitsinformationen von Cisco zu erhalten.

Eine aktuelle Liste der Sicherheitshinweise und -informationen für Cisco-Produkte ist unter folgendem URL verfügbar:

http://www.cisco.com/go/psirt

Falls Sie in Echtzeit aktualisierte Hinweise und Benachrichtigungen anzeigen möchten, können Sie unter folgendem URL ein PSIRT RSS-Feed (Product Security Incident Response Team Really Simple Syndication) abrufen:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Melden von Sicherheitsproblemen in Cisco-Produkten

Cisco arbeitet mit hohem Engagement daran, die Sicherheit der eigenen Produkte zu verbessern. Unsere Produkte werden vor der Freigabe unternehmensintern getestet, und wir sind bestrebt, alle Sicherheitsrisiken in kürzester Zeit zu beseitigen. Falls Sie der Meinung sind, ein Sicherheitsrisiko in einem Produkt von Cisco erkannt zu haben, wenden Sie sich an das PSIRT:

- In dringenden Fällen – security-alert@cisco.com
- In nicht dringenden Fällen – psirt@cisco.com

Tipp Wir empfehlen Ihnen, zur Verschlüsselung vertraulicher Daten, die Sie an Cisco senden, PGP (Pretty Good Privacy) oder ein kompatibles Produkt zu verwenden. Das PSIRT kann mit verschlüsselten Informationen arbeiten, die mit den PGP-Versionen 2.*x* bis 8.*x* kompatibel sind.

Verwenden Sie niemals einen gesperrten oder abgelaufenen Chiffrierschlüssel. Verwenden Sie bei Ihrer Korrespondenz mit dem PSIRT den öffentlichen Schlüssel, der in der folgenden Serverliste für öffentliche Schlüssel das jeweils neueste Erstellungsdatum aufweist:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In einem Notfall können Sie das PSIRT ebenfalls telefonisch erreichen:

- 1 877 228-7302
- 1 408 525-6532

Anfordern technischer Unterstützung

Allen Kunden, Partnern, Händlern und Vertragshändlern mit gültigen Cisco-Serviceverträgen steht der mehrfach ausgezeichnete technische Support von Cisco rund um die Uhr zur Verfügung. Auf der Support-Website von Cisco auf **Cisco.com** finden Sie umfassende Online-Supportressourcen. Darüber hinaus bieten Ihnen die Mitarbeiter des Cisco Technical Assistance Center (TAC) telefonische Unterstützung. Wenn Sie nicht über einen gültigen Cisco-Servicevertrag verfügen, wenden Sie sich bitte an Ihren Händler.

Technische Support-Website von Cisco

Die technische Support-Website von Cisco enthält Onlinedokumente und Tools für die Fehlerbehebung und Lösung von technischen Problemen mit Produkten und Technologien von Cisco. Die Website steht Ihnen rund um die Uhr an 365 Tagen im Jahr unter folgendem URL zur Verfügung:

http://www.cisco.com/techsupport

Der Zugriff auf die Tools der technischen Support-Website von Cisco ist nur mit einer **Cisco.com**-Benutzer-ID und einem Kennwort möglich. Wenn Sie über einen gültigen Servicevertrag verfügen, aber keine Benutzer-ID und kein Kennwort besitzen, können Sie sich unter folgendem URL registrieren:

http://tools.cisco.com/RPF/register/register.do

Hinweis Verwenden Sie das CPI-Tool (Cisco Product Identification) zur Suche nach der Seriennummer des Produkts, bevor Sie per Internet oder telefonisch eine Serviceanfrage senden. Sie können auf der technischen Support-Website von Cisco auf das CPI-Tool zugreifen, indem Sie unter **Documentation & Tools** auf den Link **Tools & Resources** klicken. Wählen Sie **Cisco Product Identification Tool** in der Dropdown-Liste **Alphabetical Index** aus, oder klicken Sie unter **Alerts & RMAs** auf den Link **Cisco Product Identification Tool**. Das CPI-Tool bietet drei Suchoptionen: nach Produkt-ID oder Modellname, nach Strukturansicht, oder für bestimmte Produkte durch Kopieren und Einfügen der Befehlsausgabe **show**. Die Suchergebnisse zeigen eine Abbildung Ihres Produkts mit hervorgehobener Position des Seriennummernetiketts. Suchen Sie das Seriennummernetikett an Ihrem Produkt, und notieren Sie die erforderlichen Informationen, bevor Sie eine Serviceanfrage senden.

Senden einer Serviceanfrage

Das Onlinetool für Serviceanfragen im TAC (Service Request Tool) ist die schnellste Methode zum Senden von S3- und S4-Serviceanfragen. (S3- und S4-Serviceanfragen sind Anfragen, bei denen Ihr Netzwerk minimal beeinträchtigt ist oder Sie Produktinformationen anfordern.) Nachdem Sie Ihre Situation beschrieben haben, gibt das TAC Service Request Tool empfohlene Lösungen aus. Wenn sich das Problem mit den empfohlenen Ressourcen nicht lösen lässt, wird Ihre Serviceanfrage an einen Mitarbeiter des Cisco TAC weitergeleitet. Das TAC Service Request Tool befindet sich unter folgendem URL:

http://www.cisco.com/techsupport/servicerequest

Wenn es sich um S1- oder S2-Serviceanfragen handelt oder Sie keinen Zugriff auf das Internet haben, wenden Sie sich telefonisch an das Cisco TAC. (S1- oder S2-Serviceanfragen sind Anfragen, bei denen Ihr Produktionsnetzwerk ausgefallen oder in seiner Funktion erheblich beeinträchtigt ist.) S1- und S2-Serviceanfragen werden sofort Mitarbeitern des Cisco TAC zugewiesen, um eine Unterbrechung Ihrer Geschäftsabläufe zu vermeiden.

Verwenden Sie für telefonische Serviceanfragen die folgenden Telefonnummern:

Asien-Pazifik: +61 2 8446 7411 (Australien: 1 800 805 227)
Europa, Naher Osten und Afrika: +32 2 704 55 55
USA: 1 800 553-2447

Eine vollständige Liste der Cisco TAC-Kontaktanschriften finden Sie unter folgendem URL:

http://www.cisco.com/techsupport/contacts

Definition des Schweregrads von Serviceanfragen

Um zu gewährleisten, dass alle Serviceanfragen in einem standardmäßigen Format gemeldet werden, hat Cisco Schweregraddefinitionen festgelegt.

Schweregrad 1 (S1) – Ihr Netzwerk ist ausgefallen, oder die Geschäftsabläufe werden erheblich gestört. Sie und Cisco stellen rund um die Uhr alle notwendigen Ressourcen und Mitarbeiter bereit, um das Problem zu lösen.

Schweregrad 2 (S2) – Der Betrieb eines vorhandenen Netzwerks ist deutlich beeinträchtigt, oder wichtige Bereiche Ihrer Geschäftsabläufe werden durch eine unzulängliche Leistung der Produkte von Cisco gestört. Sie und Cisco stellen während der normalen Geschäftszeiten Ressourcen und vollzeitbeschäftigte Mitarbeiter bereit, um das Problem zu lösen.

Schweregrad 3 (S3) – Die Betriebsleistung Ihres Netzwerks ist beeinträchtigt, die meisten Geschäftsabläufe können jedoch fortgesetzt werden. Sie und Cisco stellen während der normalen Geschäftszeiten Ressourcen und Mitarbeiter bereit, um eine zufrieden stellende Funktionalität des Netzwerks wiederherzustellen.

Schweregrad 4 (S4) – Sie benötigen Informationen oder Unterstützung für die Funktionen, die Installation oder die Konfiguration von Cisco-Produkten. Eine solche Situation hat nur geringfügige oder keine Auswirkungen auf Ihre Geschäftsabläufe.

Anfordern von zusätzlichen Veröffentlichungen und Informationen

Informationen zu Produkten, Technologien und Netzwerklösungen von Cisco stehen Ihnen online und in gedruckter Form in verschiedenen Quellen zur Verfügung.

- Im Cisco Marketplace finden Sie eine Vielzahl von Cisco-Büchern, Referenzhandbüchern und Firmenprodukten. Besuchen Sie unseren Firmenshop Cisco Marketplace unter folgendem URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* veröffentlicht eine Vielzahl von allgemeinen Netzwerk-, Schulungs- und Zertifizierungstiteln. Sowohl neue als auch erfahrene Benutzer können von diesen Veröffentlichungen profitieren. Aktuelle Titel von Cisco Press und weitere Informationen finden Sie auf der Cisco Press-Website unter folgendem URL:

  http://www.ciscopress.com

- *Packet* ist das technische Benutzermagazin von Cisco Systems. Dieses Magazin bietet hilfreiche Informationen zum Maximieren von Internet- und Netzwerkinvestitionen. In jedem Quartal stellt Packet die neuesten Branchentrends, technologische Innovationen sowie Produkte und Lösungen von Cisco vor. Darüber hinaus bietet das Magazin Tipps für die Netzwerkbereitstellung und Fehlerbehebung, Konfigurationsbeispiele, Fallstudien von Kunden, Informationen zu Zertifizierungen und Schulungen sowie Links zu Bewertungen von umfassenden Onlineressourcen. Das Packet-Magazin steht Ihnen unter folgendem URL zur Verfügung:

  http://www.cisco.com/packet

- Das *iQ Magazine* wird vierteljährlich von Cisco Systems herausgegeben. In diesem Magazin erfahren aufstrebende und wachsende Unternehmen, wie Sie Technologie nutzen können, um ihren Umsatz zu erhöhen, Geschäftsabläufe zu optimieren und Dienste zu erweitern. Das Magazin zeigt anhand von echten Fallstudien und Geschäftsstrategien die Schwierigkeiten dieser Unternehmen und Technologien zur Lösung der Probleme auf, um dem Leser solide Investitionsentscheidungen zu ermöglichen. Das iQ Magazine steht Ihnen unter folgendem URL zur Verfügung:

  http://www.cisco.com/go/iqmagazine

- Das *Internet Protocol Journal* ist eine vierteljährlich von Cisco Systems herausgegebene Zeitschrift für Ingenieure und Techniker, die sich mit dem Entwurf, der Entwicklung und dem Betrieb von öffentlichen und privaten Internets und Intranets befassen. Das Internet Protocol Journal steht Ihnen unter folgendem URL zur Verfügung:

  http://www.cisco.com/ipj

- Cisco bietet ausgezeichnete Netzwerkschulungen an. Die aktuellen Angebote finden Sie unter folgendem URL:

  http://www.cisco.com/en/US/learning/index.html

CISCO SYSTEMS

TEIL 1

Erste Schritte

Grundlegende Routerkonfiguration

Dieses Kapitel enthält Anweisungen zum Konfigurieren der grundlegenden Parameter Ihres Cisco-Routers, einschließlich globaler Parametereinstellungen, Routingprotokolle, Schnittstellen und des Zugriffs über die Befehlszeile. Darüber hinaus wird die Standardkonfiguration beim Start beschrieben.

Hinweis Unter Umständen wird von einzelnen Routermodellen nicht jede in diesem Handbuch beschriebene Funktion unterstützt. Funktionen, die von einem bestimmten Routermodell nicht unterstützt werden, wurden daher nach Möglichkeit gekennzeichnet.

Dieses Kapitel ist in folgende Abschnitte unterteilt:

- Beschriftungen der Schnittstellenanschlüsse
- Anzeigen der Standardkonfiguration
- Zur Konfiguration benötigte Informationen
- Konfigurieren grundlegender Parameter
- Konfigurieren statischer Routen
- Konfigurieren dynamischer Routen
- Konfigurieren von Enhanced IGRP

Jeder Abschnitt enthält ein Konfigurationsbeispiel und ggf. Schritte zur Überprüfung.

Ausführliche Informationen zum Aufrufen des globalen Konfigurationsmodus finden Sie im Abschnitt „Aufrufen des globalen Konfigurationsmodus“ in Anhang A, „Grundlegende Fertigkeiten für die Arbeit mit der Cisco IOS-Software“. Weitere Informationen zu den in den folgenden Tabellen verwendeten Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3.

Beschriftungen der Schnittstellenanschlüsse

In Tabelle 1-1 werden die für jeden Router unterstützten Schnittstellen und die entsprechenden Kennzeichnungen der Gerätanschlüsse aufgeführt.

Tabelle 1-1 Unterstützte Schnittstellen und zugehörige Anschlussbeschriftungen am Cisco-Router

Router	Schnittstelle	Anschlusskennzeichnung
Cisco 851:	Fast-Ethernet-LAN	LAN (oben), FE0–FE3 (unten)
	Fast-Ethernet-WAN	WAN (oben), FE4 (unten)
	Wireless-LAN	(unbeschriftet)
Cisco 871:	Fast-Ethernet-LAN	FE0–FE3
	Fast-Ethernet-WAN	FE4
	Wireless-LAN	LEFT, RIGHT/PRIMARY
	USB	1–0
Cisco 857:	Fast-Ethernet-LAN	LAN (oben), FE0–FE3 (unten)
	ATM-WAN	ADSLoPOTS
	Wireless-LAN	(unbeschriftet)
Cisco 876:	Fast-Ethernet-LAN	LAN (oben), FE0–FE3 (unten)
	ATM-WAN	ADSLoISDN
	Wireless-LAN	LEFT, RIGHT/PRIMARY
	BRI (ISDN-Basisanschluss)	ISDN S/T
Cisco 877:	Fast-Ethernet-LAN	LAN (oben), FE0–FE3 (unten)
	ATM-WAN	ADSLoPOTS
	Wireless-LAN	LEFT, RIGHT/PRIMARY
Cisco 878:	Fast-Ethernet-LAN	FE0–FE3
	ATM-WAN	G.SHDSL
	Wireless-LAN	LEFT, RIGHT/PRIMARY
	BRI (ISDN-Basisanschluss)	ISDN S/T

Anzeigen der Standardkonfiguration

Beim erstmaligen Booten des Cisco-Routers sind einige grundlegende Konfigurationseinstellungen bereits festgelegt. Beispielsweise sind alle LAN- und WAN-Schnittstellen zu diesem Zeitpunkt bereits erstellt, die Konsole und VTY-Anschlüsse sind konfiguriert, und die innere Schnittstelle für die Netzadress-Übersetzung (Network Address Translation, NAT) ist schon zugewiesen. Verwenden Sie den Befehl **show running-config** gemäß der Beschreibung in Beispiel 1-1, um die Anfangskonfiguration anzuzeigen.

Beispiel 1-1 Cisco 851 – Standardkonfiguration beim Start

```
Router# show running-config
Building configuration...

Current configuration : 1090 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
!

ip cef
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet0
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 shutdown
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
 54.0
 rts threshold 2312
 station-role root
!
interface Vlan1
 no ip address
!
ip classless
!
no ip http server
no ip http secure-server
!
control-plane
```

```
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

Zur Konfiguration benötigte Informationen

In Abhängigkeit von Ihrem geplanten Netzwerkszenario müssen Sie vor der Konfiguration des Netzwerks einige oder alle der nachfolgend genannten Informationen erfassen.

- Wenn Sie eine Internetverbindung einrichten, müssen Sie die folgenden Informationen erfassen:
  - PPP-Clientname (Point-to-Point Protocol), der Ihnen als Anmeldename zugewiesen ist
  - PPP-Authentifizierungstyp: CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol)
  - PPP-Kennwort zum Zugriff auf Ihr Konto bei dem entsprechenden Internet-Service-Provider (ISP)
  - IP-Adresse des DNS-Servers und Standard-Gateways
- Falls Sie eine Verbindung mit einem Unternehmensnetz herstellen, müssen Sie und Ihr Netzwerkadministrator die folgenden Informationen für die WAN-Schnittstellen des Routers generieren und freigeben:
  - PPP-Authentifizierungstyp: CHAP oder PAP
  - PPP-Clientname zum Zugriff auf den Router
  - PPP-Kennwort zum Zugriff auf den Router
- Bei Einrichtung von IP-Routing:
  - Generieren Sie das Adressierungsschema für Ihr IP-Netzwerk.
  - Bestimmen Sie die IP-Routingparameterdaten, einschließlich der IP-Adresse und der ATM-PVCs (Permanent Virtual Circuits). Diese PVC-Parameter umfassen in der Regel so genannte Virtual Path Identifier (VPI), Virtual Circuit Identifier (VCI) und Verkehrssteuerungsparameter.
  - Bestimmen Sie die Anzahl der PVCs, die Ihnen der Service-Provider zugewiesen hat, sowie deren VPIs und VCIs.

  - Bestimmen Sie für jeden PVC den unterstützten AAL5-Kapselungstyp. Hierbei kann es sich um einen der folgenden Typen handeln:

    AAL5SNAP – Dies kann entweder RFC 1483 mit Routing oder RFC 1483 mit Bridging sein. Für RFC 1483 mit Routing muss Ihnen der Service-Provider eine statische IP-Adresse angeben. Bei RFC 1483 mit Bridging können Sie Ihre IP-Adresse über DHCP beziehen oder eine statische IP-Adresse von Ihrem Service-Provider anfordern.

    AAL5MUX PPP – Mit diesem Kapselungstyp müssen Sie die PPP-bezogenen Konfigurationselemente bestimmen.

- Falls Sie eine Verbindung über eine ADSL- oder G.SHDSL-Leitung herstellen möchten:
  - Bestellen Sie die entsprechende Verbindung bei Ihrem Telefonanbieter.

    Bei ADSL-Verbindungen – Vergewissern Sie sich, dass als ADSL-Signalisierungstyp DMT (auch als ANSI T1.413 bezeichnet) oder DMT Issue 2 eingestellt ist.

    Bei G.SHDSL-Verbindungen – Überprüfen Sie, ob die G.SHDSL-Verbindung dem Standard ITU G.991.2 entspricht und Annex A (Nordamerika) oder Annex B (Europa) unterstützt.

    Nachdem Sie die entsprechenden Informationen erfasst haben, können Sie, beginnend mit den Schritten in Abschnitt „Konfigurieren grundlegender Parameter“, eine vollständige Konfiguration des Routers durchführen.

Konfigurieren grundlegender Parameter

Führen Sie einen oder mehrere der folgenden Schritte aus, um den Router zu konfigurieren:

- Konfigurieren globaler Parameter
- Konfigurieren der Fast-Ethernet-LAN-Schnittstellen
- Konfigurieren von WAN-Schnittstellen
- Konfigurieren einer Loopback-Schnittstelle
- Konfigurieren des Command-Line-Zugriffs auf den Router

Für jeden Schritt ist anhand eines Konfigurationsbeispiels die Netzwerkkonfiguration nach Abschluss des betreffenden Schritts dargestellt.

Konfigurieren globaler Parameter

Führen Sie die folgenden Schritte aus, um die ausgewählten globalen Parameter für den Router zu konfigurieren:

	Befehl	Zweck

Schritt 1	**configure terminal**
	
	Beispiel:
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus bei Verwendung des Konsolenanschlusses aufgerufen.
		
		Falls Sie über ein Remote-Terminal eine Verbindung mit dem Router herstellen, verwenden Sie folgende Befehlssyntax:
		`telnet Routername oder -adresse`
		`Login: Login-ID`
		`Password: *********`
		`Router> enable`

Schritt 2	**hostname** *Name*
	
	Beispiel:
	`Router(config)# hostname Router`
	`Router(config)#`
		Mit diesem Befehl wird der Name des Routers angegeben.

Schritt 3	**enable secret** *Kennwort*
	
	Beispiel:
	`Router(config)# enable secret cr1ny5ho`
	`Router(config)#`
		Mit diesem Befehl wird ein verschlüsseltes Kennwort festgelegt, um den Router vor unbefugtem Zugriff zu schützen.

Schritt 4	**no ip domain-lookup**
	
	Beispiel:
	`Router(config)# no ip domain-lookup`
	`Router(config)#`
		Mit diesem Befehl wird verhindert, dass der Router unbekannte Wörter (Schreibfehler) in IP-Adressen übersetzt.

Ausführliche Informationen zu den Befehlen für globale Parameter finden Sie in der Dokumentation von Cisco IOS Release 12.3.

Konfigurieren der Fast-Ethernet-LAN-Schnittstellen

Die Fast-Ethernet-LAN-Schnittstellen auf dem Router werden als Bestandteil des Standard-VLAN automatisch konfiguriert und somit nicht mit einzelnen Adressen konfiguriert. Der Zugang wird durch das VLAN gewährt. Sie können die Schnittstellen bei Bedarf anderen VLANs zuweisen. Weitere Informationen zum Erstellen von VLANs finden Sie in Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“.

Konfigurieren von WAN-Schnittstellen

Die Router des Typs Cisco 851 und Cisco 871 verfügen jeweils über eine Fast-Ethernet-Schnittstelle zur Verbindung mit einem WAN. Router des Typs Cisco 857, Cisco 877 und Cisco 878 verfügen jeweils über eine ATM-Schnittstelle zur Verbindung mit einem WAN.

Konfigurieren Sie die WAN-Schnittstelle(n) in Abhängigkeit von Ihrem Routermodell mit einem der folgenden Verfahren:

- Konfigurieren der Fast-Ethernet-WAN-Schnittstelle
- Konfigurieren der ATM-Schnittstelle

Konfigurieren der Fast-Ethernet-WAN-Schnittstelle

Diese Verfahrensweise gilt nur für die Routermodelle Cisco 851 und Cisco 871. Führen Sie die folgenden Schritte aus, um die Fast-Ethernet-Schnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router(config-int)#`
		Mit diesem Befehl wird der Konfigurationsmodus für eine Fast-Ethernet-WAN-Schnittstelle des Routers aufgerufen.

Schritt 2	**ip address** *IP-Adresse Maske*
	
	Beispiel:
	`Router(config-int)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-int)#`
		Mit diesem Befehl wird die IP-Adresse und die Subnetzmaske für die angegebene Fast-Ethernet-Schnittstelle festgelegt.

Schritt 3	**no shutdown**
	
	Beispiel:
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		Mit diesem Befehl wird die Ethernet-Schnittstelle aktiviert, wobei ihr Status von „administrativ abgeschaltet“ zu „administrativ hochgefahren“ geändert wird.

Schritt 4	**exit**
	
	Beispiel:
	`Router(config-int)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-Schnittstelle beendet und der globale Konfigurationsmodus wieder aufgerufen.

Konfigurieren der ATM-Schnittstelle

Diese Verfahrensweise gilt nur für die Routermodelle Cisco 857, Cisco 876, Cisco 877 und Cisco 878.

Führen Sie die folgenden Schritte aus, um die ATM-Schnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	***Nur für Modell Cisco 878:***
	controller dsl 0
	mode atm
	exit
	
	Beispiel:
	`Router(config)# controller dsl 0`
	`Router(config-controller)# mode atm`
	`Router(config-controller)# exit`
	`Router(config)#`
		Führen Sie diese Befehle für Router mit G.SHDSL-Signalisierung aus. Ignorieren Sie diesen Schritt, wenn Sie einen Router mit ADSL-Signalisierung verwenden.

Schritt 2	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface atm0`
	`Router(config-int)#`
		In diesem Schritt wird eine ATM-Schnittstelle angegeben und der Konfigurationsmodus für diese Schnittstelle aufgerufen.

Schritt 3	**ip address** *IP-Adresse Maske*
	
	Beispiel:
	`Router(config-int)# ip address 200.200.100.1 255.255.255.0`
	`Router(config-int)#`
		Mit diesem Befehl werden die IP-Adresse und die Subnetzmaske für die angegebene ATM-Schnittstelle festgelegt.

Schritt 4	**no shutdown**
	
	Beispiel:
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		Mit diesem Befehl wird die Schnittstelle ATM 0 aktiviert.

Schritt 5	**exit**
	
	Beispiel:
	`Router(config-int)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die ATM-Schnittstelle beendet und der globale Konfigurationsmodus wieder aufgerufen.

Konfigurieren der Wireless-Schnittstelle

Durch die Wireless-Schnittstelle wird die Verbindung mit dem Router über eine Wireless-LAN-Verbindung aktiviert. Weitere Informationen zum Konfigurieren einer drahtlosen Verbindung finden Sie in Kapitel 9, „Konfigurieren einer Wireless-LAN-Verbindung“, und im *Cisco Access Router Wireless Configuration Guide*.

Konfigurieren einer Loopback-Schnittstelle

Die Loopback-Schnittstelle fungiert als Platzhalter für die statische IP-Adresse und bietet standardmäßige Routinginformationen.

Ausführliche Informationen zu den Loopback-Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3.

Führen Sie die folgenden Schritte aus, um eine Loopback-Schnittstelle zu konfigurieren:

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface Loopback 0`
	`Router(config-int)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Loopback-Schnittstelle aufgerufen.

Schritt 2	**ip address** *IP-Adresse Maske*
	
	Beispiel:
	`Router(config-int)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-int)#`
		Mit diesem Befehl werden die IP-Adresse und die Subnetzmaske für die Loopback-Schnittstelle festgelegt.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-int)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Loopback-Schnittstelle beendet und der globale Konfigurationsmodus wieder aufgerufen.

Konfigurationsbeispiel

Die Loopback-Schnittstelle in dieser Beispielkonfiguration dient zur Unterstützung der Netzadress-Übersetzung (Network Address Translation, NAT) auf der Virtual-Template-Schnittstelle. Im folgenden Konfigurationsbeispiel wird eine Loopback-Schnittstelle auf der Fast-Ethernet-Schnittstelle mit der IP-Adresse 200.200.100.1/24 konfiguriert, die als statische IP-Adresse fungiert. Die Loopback-Schnittstelle verweist zurück auf die Schnittstelle „virtual-template1“, die über eine ausgehandelte IP-Adresse verfügt.

```
!
interface loopback 0
ip address 200.200.100.1 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
!
```

Überprüfen der Konfiguration

Geben Sie den Befehl **show interface loopback** ein, wenn Sie überprüfen möchten, ob Sie die Loopback-Schnittstelle richtig konfiguriert haben. Die bei dieser Überprüfung ausgegebenen Daten sollten dem nachfolgenden Beispiel in etwa ähneln:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Ein anderes Verfahren zur Überprüfung der Loopback-Schnittstelle besteht darin, eine ping-Abfrage an diese Schnittstelle zu senden:

```
Router# ping 200.200.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Konfigurieren des Command-Line-Zugriffs auf den Router

Führen Sie die folgenden Schritte aus, um Parameter zum Steuern des Zugriffs auf den Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**line** [**aux** | **console** | **tty** | **vty**] *Leitungsnummer*
	
	Beispiel:
	`Router(config)# line console 0`
	`Router(config)#`
		Mit diesem Befehl wird der Leitungskonfigurationsmodus aufgerufen und der Leitungstyp angegeben.
		
		In diesem Beispiel wird ein Konsolenterminal für den Zugriff festgelegt.

Schritt 2	**password** *Kennwort*
	
	Beispiel:
	`Router(config)# password 5dr4Hepw3`
	`Router(config)#`
		Mit diesem Befehl wird ein eindeutiges Kennwort für die Konsolenterminalleitung angegeben.

	Befehl	Zweck

Schritt 3	**login**
	
	Beispiel:
	`Router(config)# login`
	`Router(config)#`
		Mit diesem Befehl wird die Kennwortüberprüfung bei der Anmeldung der Terminalsitzung aktiviert.

Schritt 4	**exec-timeout** *Minuten* [*Sekunden*]
	
	Beispiel:
	`Router(config)# exec-timeout 5 30`
	`Router(config)#`
		Mit diesem Befehl wird das Warteintervall bis zur Erkennung der Benutzereingabe durch den EXEC-Befehlsinterpreter festgelegt. Die Standardeinstellung ist 10 Minuten. Wahlweise können Sie auch die Anzahl der Sekunden zu dem Intervallwert hinzufügen.
		
		In diesem Beispiel wird ein Timeout-Wert von 5 Minuten und 30 Sekunden verwendet. Bei Eingabe eines Timeout-Werts von „0 0“ erfolgt kein Timeout.

Schritt 5	**line** [**aux** | **console** | **tty** | **vty**] *Leitungsnummer*
	
	Beispiel:
	`Router(config)# line vty 0 4`
	`Router(config)#`
		Mit diesem Befehl wird ein virtuelles Terminal für den Zugriff per Remote-Konsole festgelegt.

Schritt 6	**password** *Kennwort*
	
	Beispiel:
	`Router(config)# password aldf2ad1`
	`Router(config)#`
		Mit diesem Befehl wird ein eindeutiges Kennwort für die virtuelle Terminalleitung angegeben.

Schritt 7	**login**
	
	Beispiel:
	`Router(config)# login`
	`Router(config)#`
		Mit diesem Befehl wird die Kennwortüberprüfung bei der Anmeldung der virtuellen Terminalsitzung aktiviert.

Schritt 8	**end**
	
	Beispiel:
	`Router(config)# end`
	`Router#`
		Mit diesem Befehl wird der Leitungskonfigurationsmodus beendet und erneut der privilegierte EXEC-Modus aufgerufen.

Ausführliche Informationen zu den Command-Line-Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3.

Konfigurationsbeispiel

In der folgenden Konfiguration sind die Command-Line-Zugriffsbefehle dargestellt.

Mit „default“ gekennzeichnete Befehle müssen nicht eingegeben werden. Diese Befehle werden bei Eingabe des Befehls **show running-config** in der generierten Konfigurationsdatei automatisch angezeigt.

```
!
line con 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Konfigurieren statischer Routen

Statische Routen bieten feste Routingpfade durch das Netzwerk. Diese Routen werden manuell auf dem Router konfiguriert. Bei einer Änderung der Netzwerktopologie müssen die statischen Routen mit einer neuen Route aktualisiert werden. Statische Routen sind private Routen, sofern sie nicht durch ein Routingprotokoll erneut verteilt werden. Die Konfiguration statischer Routen ist für Router der Cisco 850-Serie und der Cisco 870-Serie optional.

Führen Sie die folgenden Schritte aus, um statische Routen zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip route** *Präfix Maske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]}
	
	Beispiel:
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
	`Router(config)#`
		Mit diesem Befehl wird die statische Route für die IP-Pakete angegeben.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols*.

Schritt 2	**end**
	
	Beispiel:
	`Router(config)# end`
	`Router#`
		Mit diesem Befehl wird der Routerkonfigurationsmodus beendet und der privilegierte EXEC-Modus aufgerufen.

Ausführliche Informationen zu den Befehlen für statisches Routing finden Sie in der Dokumentation zu Cisco IOS Release 12.3. Allgemeinere Informationen zum statischen Routing finden Sie in Anhang B, „Konzepte“.

Konfigurationsbeispiel

Im folgenden Konfigurationsbeispiel sendet die statische Route alle IP-Pakete mit der IP-Zieladresse 192.168.1.0 und der Subnetzmaske 255.255.255.0 auf der Fast-Ethernet-Schnittstelle an ein anderes Gerät mit der IP-Adresse 10.10.10.2. Die Pakete werden in diesem Fall an den konfigurierten Permanent Virtual Circuit (PVC) gesendet.

Mit „**default**“ gekennzeichnete Befehle müssen von Ihnen nicht eingegeben werden. Diese Befehle werden bei Eingabe des Befehls **show running-config** in der generierten Konfigurationsdatei automatisch angezeigt.

```
!
ip classless (default)
ip route 192.168.1.0 255.255.255.0 10.10.10.2!
```

Überprüfen der Konfiguration

Wenn Sie überprüfen möchten, ob Sie das statische Routing fehlerfrei konfiguriert haben, geben Sie den Befehl **show ip route** ein. Prüfen Sie dann, ob statische Routen (mit „S“ gekennzeichnet) angezeigt werden.

Die bei dieser Überprüfung ausgegebenen Daten sollten dem nachfolgenden Beispiel in etwa ähneln:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, FastEthernet0
```

Konfigurieren dynamischer Routen

Beim dynamischen Routing passt das Netzwerkprotokoll den Pfad basierend auf dem Netzwerkdatenverkehr oder der Netzwerktopologie automatisch an. Änderungen in den dynamischen Routen werden an andere Router im Netzwerk weitergegeben.

Cisco-Router können mithilfe von IP-Routingprotokollen, z. B. RIP (Routing Information Protocol) oder EIGRP (Enhanced Interior Gateway Routing Protocol), Routen dynamisch „erlernen“. Sie können jedes dieser Routingprotokolle auf Ihrem Router konfigurieren.

Konfigurieren von RIP

Führen Sie die folgenden Schritte aus, um das Routingprotokoll RIP auf dem Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Schritt

Schritt 1	**router rip**
	
	Beispiel:
	`Router> configure terminal`
	`Router(config)# router rip`
	`Router(config-router)#`
		Mit diesem Befehl wird der Routerkonfigurationsmodus aufgerufen und RIP auf dem Router aktiviert.

Schritt 2	**version** {**1** | **2**}
	
	Beispiel:
	`Router(config-router)# version 2`
	`Router(config-router)#`
		Mit diesem Befehl wird angegeben, dass die RIP-Version 1 oder 2 verwendet werden soll.

Schritt 3	**network** *IP-Adresse*
	
	Beispiel:
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
	`Router(config-router)#`
		Mit diesem Befehl wird eine Liste von Netzwerken angegeben, auf die RIP angewendet werden soll. Hierbei wird die Adresse des Netzwerks der direkt verbundenen Netzwerke verwendet.

Schritt 4	**no auto-summary**
	
	Beispiel:
	`Router(config-router)# no auto-summary`
	`Router(config-router)#`
		Mit diesem Befehl wird die automatische Zusammenfassung von Subnetzrouten in Routen auf Netzwerkebene deaktiviert. Dadurch können Subpräfix-Routinginformationen über klassenbasierte Netzwerkgrenzen hinweg übertragen werden.

Schritt 5	**end**
	
	Beispiel:
	`Router(config-router)# end`
	`Router#`
		Mit diesem Befehl wird der Routerkonfigurationsmodus beendet und der privilegierte EXEC-Modus aufgerufen.

Ausführliche Informationen zu den Befehlen über dynamisches Routing finden Sie in der Dokumentation von Cisco IOS Release 12.3. Allgemeine Informationen zu RIP finden Sie in Anhang B, „Konzepte“.

Konfigurationsbeispiel

Im folgenden Konfigurationsbeispiel ist dargestellt, wie RIP (Version 2) in den IP-Netzwerken 10.0.0.0 und 192.168.1.0 aktiviert wird.

Führen Sie im privilegierten EXEC-Modus den Befehl **show running-config** aus, um diese Konfiguration anzuzeigen.

```
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
```

Überprüfen der Konfiguration

Zum Überprüfen der ordnungsgemäßen Konfiguration von RIP geben Sie den Befehl **show ip route** ein, und suchen Sie nach RIP-Routen (durch „R“ gekennzeichnet). Die ausgegebenen Daten sollten dem nachstehend abgebildeten Beispiel in etwa entsprechen.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0
```

Konfigurieren von Enhanced IGRP

Führen Sie die folgenden Schritte aus, um Enhanced IGRP (EIGRP) zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**router eigrp** *AS-Nummer*
	
	Beispiel:
	`Router(config)# router eigrp 109`
	`Router(config)#`
		Mit diesem Befehl wird der Routerkonfigurationsmodus aufgerufen und EIGRP auf dem Router aktiviert. Die AS-Nummer (Nummer des autonomen Systems) bezeichnet die Route zu anderen EIGRP-Routern und wird zur Markierung (Tagging) der EIGRP-Informationen verwendet.

	Befehl	Zweck

Schritt 2	**network** *IP-Adresse*
	
	Beispiel:
	`Router(config)# network 192.145.1.0`
	`Router(config)# network 10.10.12.115`
	`Router(config)#`
		Mit diesem Befehl wird eine Liste von Netzwerken angegeben, auf die EIGRP angewendet werden soll. Hierbei wird die IP-Adresse des Netzwerks der direkt verbundenen Netzwerke verwendet.

Schritt 3	**end**
	
	Beispiel:
	`Router(config-router)# end`
	`Router#`
		Mit diesem Befehl wird der Routerkonfigurationsmodus beendet und der privilegierte EXEC-Modus aufgerufen.

Ausführliche Informationen zu den IP-EIGRP-Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3. Allgemeine Informationen zu den EIGRP-Konzepten finden Sie in Anhang B, „Konzepte“.

Konfigurationsbeispiel

Im folgenden Konfigurationsbeispiel ist dargestellt, wie das Routingprotokoll EIGRP in den IP-Netzwerken 192.145.1.0 und 10.10.12.115 aktiviert wird. Die autonome EIGRP-Systemnummer lautet 109.

Führen Sie im privilegierten EXEC-Modus den Befehl **show running-config** aus, um diese Konfiguration anzuzeigen.

```
!
router eigrp 109
    network 192.145.1.0
        network 10.10.12.115
!
```

Überprüfen der Konfiguration

Zum Überprüfen der ordnungsgemäßen Konfiguration von IP EIGRP geben Sie den Befehl **show ip route** ein, und suchen Sie nach EIGRP-Routen (durch „D“ gekennzeichnet). Die angezeigten Daten sollten dem nachstehend abgebildeten Beispiel in etwa entsprechen.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CISCO SYSTEMS

TEIL 2

Konfigurieren des Routers für einen Ethernet- und DSL-Zugang

Beispiele für den Netzwerkeinsatz

In diesem Teil des Software-Konfigurationshandbuchs werden verschiedene mögliche Ethernet- und DSL-basierte Netzwerkkonfigurationen mit den Zugangsroutern der Cisco 850- und Cisco 870-Serie vorgestellt. Jedes einzelne Szenario wird mit einer Netzwerktopologie, einer Schritt-für-Schritt-Anleitung zur Implementierung der Netzwerkkonfiguration sowie einem Konfigurationsbeispiel beschrieben, in dem die Ergebnisse dieser Konfiguration dargestellt werden. Die Routermodelle Cisco 851 und Cisco 871 können in den Ethernet-basierten Szenarios und die Routermodelle Cisco 857, Cisco 876, Cisco 877 und Cisco 878 entsprechend in den DSL-basierten Szenarios eingesetzt werden.

Das erste Netzwerkszenario stellt eine relativ einfache Netzwerkkonfiguration dar: PPP (Point-to-Point-Protokoll) über WAN-Schnittstelle mit NAT (Network Address Translation). Jedes nachfolgende Szenario baut auf dem vorhergehenden Szenario auf, indem lediglich eine weitere wichtige Funktion konfiguriert wird.

Durch die beschriebenen Szenarios werden nicht alle in einem Netzwerk vorkommenden Erfordernisse behandelt, sondern lediglich Modelle angeboten, nach denen Sie Ihr Netzwerk strukturieren können. Sie können je nach Bedarf die in den Beispielen genannten Funktionen ignorieren oder Funktionen hinzufügen bzw. durch andere Funktionen ersetzen, die Ihren Anforderungen besser gerecht werden.

Hinweis Wenn Sie überprüfen möchten, ob eine bestimmte Funktion mit Ihrem Router kompatibel ist, verwenden Sie das Software Advisor-Tool. Sie können auf dieses Tool unter **www.cisco.com > Technical Support & Documentation > Tools & Resources** mit Ihrem Cisco-Benutzernamen und dem entsprechenden Kennwort zugreifen.

Bei Ethernet-basierten Netzwerkszenarios

Verwenden Sie als Hilfestellung beim Konfigurieren des Routers für Ethernet-basierte Netzwerke die folgenden Konfigurationsbeispiele:

- Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“
- Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“
- Kapitel 6, „Konfigurieren eines VPN mit Easy VPN und einem IPSec-Tunnel“
- Kapitel 7, „Konfigurieren von VPNs mit einem IPSec-Tunnel und Generic Routing Encapsulation“
- Kapitel 8, „Konfigurieren einer einfachen Firewall“

Bei DSL-basierten Netzwerkszenarios

Verwenden Sie als Hilfestellung beim Konfigurieren des Routers für DSL-basierte Netzwerke die folgenden Konfigurationsbeispiele:

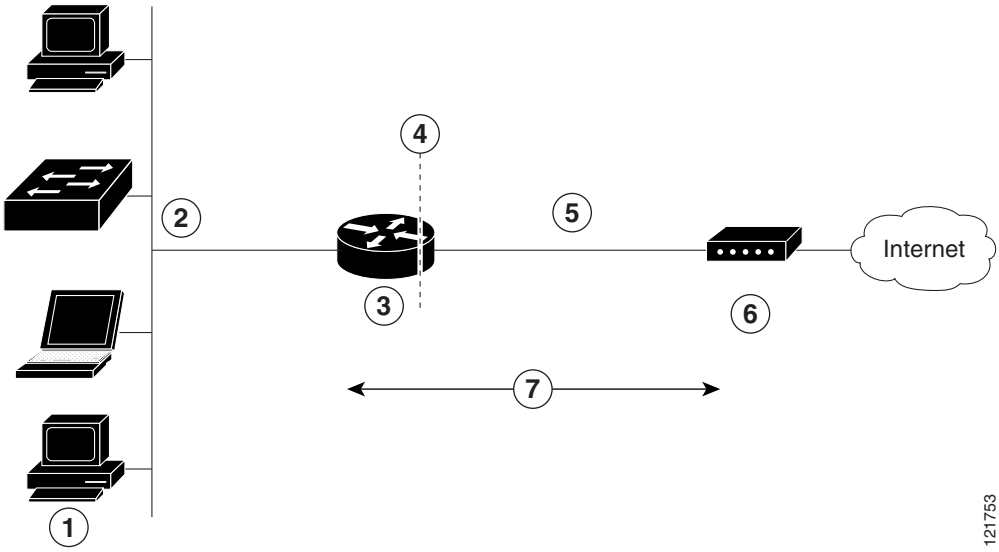
- Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“
- Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“
- Kapitel 6, „Konfigurieren eines VPN mit Easy VPN und einem IPSec-Tunnel“
- Kapitel 7, „Konfigurieren von VPNs mit einem IPSec-Tunnel und Generic Routing Encapsulation“
- Kapitel 8, „Konfigurieren einer einfachen Firewall“

Konfigurieren von PPP über Ethernet mit NAT

Die Zugangsrouter Cisco 851 und Cisco 871 unterstützen PPPoE-Clients (Point-to-Point-Protokoll über Ethernet) und NAT (Network Address Translation, Netzadress-Übersetzung).

Mehrere PCs können hinter dem Router an ein LAN angeschlossen werden. Bevor Datenverkehr von diesen PCs an die PPPoE-Sitzung gesendet wird, können die betreffenden Daten u. a. verschlüsselt und gefiltert werden. In Abbildung 3-1 ist ein typisches Einsatzszenario dargestellt, bei dem ein PPPoE-Client und NAT für den Cisco-Router konfiguriert wurden.

Abbildung 3-1 PPP über Ethernet mit NAT



1	Mehrere vernetzte Geräte – Desktop- und Laptop-PCs, Switches
2	Fast-Ethernet-LAN-Schnittstelle (innere Schnittstelle für NAT)
3	PPPoE-Client – Zugangsrouter Cisco 851 oder Cisco 871
4	Punkt, an dem NAT erfolgt
5	Fast-Ethernet-WAN-Schnittstelle (äußere Schnittstelle für NAT)
6	Kabelmodem oder anderer Server (z. B. ein Server des Typs Cisco 6400), der mit dem Internet verbunden ist
7	PPPoE-Sitzung zwischen dem Client und einem PPPoE-Server

PPPoE

Die PPPoE-Clientfunktion am Router bietet PPPoE-Clientunterstützung auf Ethernet-Schnittstellen. Eine Dialer-Schnittstelle muss zum Klonen eines virtuellen Zugangs verwendet werden. An einer Ethernet-Schnittstelle können jeweils mehrere PPPoE-Clientsitzungen konfiguriert werden. Allerdings muss jede Sitzung eine separate Dialer-Schnittstelle und einen gesonderten Dialer-Pool verwenden.

Eine PPPoE-Sitzung wird clientseitig durch den Router der Cisco 850- oder Cisco 870-Serie gestartet. Eine aktive PPPoE-Clientsitzung kann mit einem der folgenden beiden Verfahren beendet werden:

- Durch Eingabe des Befehls **clear vpdn tunnel pppoe**. Die PPPoE-Clientsitzung wird beendet. Daraufhin versucht der PPPoE-Client sofort, die Sitzung erneut zu aktivieren. Dieser Vorgang tritt ebenfalls auf, wenn eine Sitzung durch ein Timeout beendet wurde.
- Durch Eingabe des Befehls **no pppoe-client dial-pool** *Nummer*, mit dem die Sitzung gelöscht werden kann. Der PPPoE-Client versucht in diesem Fall nicht, die Sitzung erneut zu aktivieren.

NAT

NAT (dargestellt durch die gestrichelte Linie am Rand des Cisco-Routers) bezeichnet zwei Adressierungsdomänen sowie die innere Quelladresse. Durch die Quellliste wird definiert, auf welche Weise das Paket im Netzwerk übertragen wird.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren der VPDN-Gruppennummer (Virtual Private Dialup Network)
- Konfigurieren der Fast-Ethernet-WAN-Schnittstellen
- Konfigurieren der Dialer-Schnittstelle
- Konfigurieren von NAT (Network Address Translation)

Ein Beispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 3-9.

Konfigurieren der VPDN-Gruppennummer (Virtual Private Dialup Network)

Durch Konfiguration eines VPDN (Virtual Private Dialup Network, virtuelles privates DFÜ-Netzwerk) können mehrere Clients über den Router mittels einer einzigen IP-Adresse miteinander kommunizieren.

Führen Sie die folgenden Schritte aus, um ein VPDN zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus). Informationen zur Eingabe dieses Modus finden Sie im „Konfigurieren globaler Parameter“ auf Seite 1-6.

	Befehl oder Aktion	Zweck

Schritt 1	**vpdn enable**
	
	Beispiel:
	`Router(config)#vpdn enable`
	`Router(config-vpdn)#`
		Mit diesem Befehl wird VPDN auf dem Router aktiviert.

Schritt 2	**vpdn group** *Name*
	
	Beispiel:
	`Router(config-vpdn)#vpdn group 1`
	`Router(config-vpdn-grp)#`
		Mit diesem Befehl wird eine VPDN-Gruppe erstellt und einem Kunden oder VPDN-Profil zugeordnet.

Schritt 3	**request-dialin**
	
	Beispiel:
	`Router(config-vpdn-grp)# request-dialin`
	`Router(config-vpdn-grp)#`
		Mit diesem Befehl wird die VPDN-Untergruppe „request-dialin“ erstellt, die Wählrichtung angegeben und der Tunnel initiiert.

Schritt 4	**initiate to ip** *IP-Adresse*
	
	Beispiel:
	`Router(config-vpdn-grp)# initiate to 192.168.1.1`
	`Router(config-vpdn-grp)#`
		Mit diesem Befehl wird die Adresse angegeben, an die Anforderungen getunnelt werden.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Schritt 5	**protocol** {**l2f** | **l2tp** | **pppoe** | **any**}
	
	Beispiel:
	`Router(config-vpdn-grp)# protocol pppoe`
	`Router(config-vpdn-grp)#`
		Mit diesem Befehl wird der Typ der Sitzungen angegeben, die von der VPDN-Untergruppe erstellt werden können.

	Befehl oder Aktion	Zweck

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-vpdn-grp)# exit`
	`Router(config-vpdn)#`
		Mit diesem Befehl wird die Konfiguration der VPDN-Gruppe beendet.

Schritt 7	**exit**
	
	Beispiel:
	`Router(config-vpdn)#exit`
	`Router(config)#`
		Mit diesem Befehl wird die VPDN-Konfiguration beendet und der globale Konfigurationsmodus aufgerufen.

Konfigurieren der Fast-Ethernet-WAN-Schnittstellen

In diesem Szenario kommuniziert der PPPoE-Client (Ihr Cisco-Router) jeweils nach innen und außen über eine 10/100 Mbit/s-Ethernet-Schnittstelle.

Führen Sie die folgenden Schritte aus, um die Fast-Ethernet-WAN-Schnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für eine Fast-Ethernet-WAN-Schnittstelle aufgerufen.

Schritt 2	**pppoe-client dial-pool-number** *Nummer*
	
	Beispiel:
	`Router(config-if)# pppoe-client dial-pool-number 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der PPPoE-Client konfiguriert und die für das Klonen zu verwendende Dialer-Schnittstelle angegeben.

Schritt 3	**no shutdown**
	
	Beispiel:
	`Router(config-if)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die Fast-Ethernet-Schnittstelle sowie die daran vorgenommenen Konfigurationsänderungen aktiviert.

Schritt 4	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-Schnittstelle beendet und der globale Konfigurationsmodus wieder aufgerufen.

Konfigurieren der Dialer-Schnittstelle

Durch die Dialer-Schnittstelle wird angegeben, wie der von den Clients kommende Datenverkehr behandelt wird. Hierzu gehören z. B. die standardmäßigen Routinginformationen, das Kapselungsprotokoll sowie der zu verwendende Dialer-Pool. Die Dialer-Schnittstelle wird ebenfalls für das Klonen des virtuellen Zugangs verwendet. Auf einer Fast-Ethernet-Schnittstelle können jeweils mehrere PPPoE-Clientsitzungen konfiguriert werden. Allerdings muss für jede Sitzung eine separate Dialer-Schnittstelle und ein gesonderter Dialer-Pool verwendet werden.

Führen Sie die folgenden Schritte aus, um eine Dialer-Schnittstelle für eine der Fast-Ethernet-LAN-Schnittstellen am Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface dialer** *dialer-rotary-group-Nummer*
	
	Beispiel:
	`Router(config)# interface dialer 0`
	`Router (config-if)#`
		Mit diesem Befehl wird eine Dialer-Schnittstelle (mit einer Nummer zwischen 0 und 255) erstellt und der Schnittstellen-Konfigurationsmodus aufgerufen.

Schritt 2	**ip address negotiated**
	
	Beispiel:
	`Router(config-if)#ip address negotiated`
	`Router (config-if)#`
		In diesem Schritt wird angegeben, dass die IP-Adresse für die Schnittstelle über die PPP/IPCP-Adressenverhandlung (IP Control Protocol) bezogen wird.

Schritt 3	**ip mtu** *Byte*
	
	Beispiel:
	`Router(config-if)# ip mtu 1492`
	`Router (config-if)#`
		Mit diesem Befehl wird die Größe der IP-MTU (Maximum Transmission Unit; größtmögliche Dateneinheit zum Senden) festgelegt. Der standardmäßige Mindestwert beträgt 128 Byte. Der Höchstwert für Ethernet beträgt 1492 Byte.

Schritt 4	**encapsulation** *Kapselungstyp*
	
	Beispiel:
	`Router(config-if)#encapsulation ppp`
	`Router (config-if)#`
		Mit diesem Befehl wird der PPP-Kapselungstyp für die gesendeten und empfangenen Datenpakete festgelegt.

Schritt 5	**ppp authentication** {*Protokoll1* [*Protokoll2*...]}
	
	Beispiel:
	`Router(config-if)# ppp authentication chap`
	`Router (config-if)#`
		Mit diesem Befehl wird die PPP-Authentifizierungsmethode auf CHAP (Challenge Handshake Authentication Protocol) gesetzt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Security Command Reference*.

	Befehl	Zweck

Schritt 6	**dialer pool** *Nummer*
	
	Beispiel:
	`Router(config-if)#dialer pool 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Dialer-Pool angegeben, der zum Herstellen der Verbindung mit einem bestimmten Zielsubnetz verwendet werden soll.

Schritt 7	**dialer-group** *Gruppennummer*
	
	Beispiel:
	`Router(config-if)#dialer group 1`
	`Router (config-if)#`
		Mit diesem Befehl wird die Dialer-Schnittstelle einer Dialer-Gruppe (1–10) zugewiesen.
		
		Tipp Durch die Verwendung einer Dialer-Gruppe lässt sich der Zugriff auf den Router steuern.

Schritt 8	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird die Konfiguration der Schnittstelle „dialer 0“ beendet.

Schritt 9	**dialer-list** *Dialer-Gruppe* **protocol** *Protokollname* {**permit** | **deny** | **list** *Access-Listennummer* | **access-group**}
	
	Beispiel:
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		Mit diesem Befehl wird eine Dialer-Liste erstellt und einer Dialer-Gruppe zugeordnet. Datenpakete werden dann über die angegebene Dialer-Gruppe weitergeleitet.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Schritt 10	**ip route** *Präfix Maske* {*Schnittstellentyp Schnittstellennummer*}
	
	Beispiel:
	`Router(config)# ip route 10.10.25.2 0.255.255.255 dialer 0`
	`Router(config)#`
		Mit diesem Befehl wird die IP-Route für den Standard-Gateway für die Schnittstelle „dialer 0“ festgelegt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS IP Command Reference, Band 2; Routing Protocols*.

Konfigurieren von NAT (Network Address Translation)

Durch NAT (Network Address Translation, Netzadress-Übersetzung) werden Pakete von Adressen, die mit einer standardmäßigen Access-Liste übereinstimmen, anhand von globalen Adressen übersetzt, die durch die Dialer-Schnittstelle zugewiesen werden. Die über die innere Schnittstelle in den Router eingehenden Pakete und/oder die vom Router bezogenen Pakete werden anhand der Access-Liste auf eine mögliche Adressübersetzung geprüft. Sie können NAT für statische oder dynamische Adressübersetzungen konfigurieren.

Führen Sie die folgenden Schritte aus, um die äußere Fast-Ethernet-WAN-Schnittstelle mit dynamischer Netzadress-Übersetzung zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip nat pool** *Name Anfangs-IP End-IP* {**netmask** *Netzmaske* | **prefix-length** *Präfixlänge*}
	
	Beispiel:
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255`
	`Router(config)#`
		Mit diesem Befehl wird ein Pool mit globalen IP-Adressen für NAT erstellt.

Schritt 2	**ip nat inside source** {**list** *Access-Listenummer*} {**interface** *Typ Nummer* | **pool** *Name*} [**overload**]
	
	Beispiel 1:
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	
	oder
	
	Beispiel 2:
	`Router(config)# ip nat inside source list acl1 pool pool1`
		Mit diesem Befehl wird die dynamische Übersetzung von Adressen auf der inneren Schnittstelle aktiviert.
		
		Im ersten Beispiel werden die in der Access-Liste *1* zugelassenen Adressen in eine der Adressen übersetzt, die in der Dialer-Schnittstelle *0* angegeben sind.
		
		Im zweiten Beispiel werden die durch die Access-Liste *acl1* zugelassenen Adressen jeweils in eine Adresse aus dem NAT-Pool *pool1* übersetzt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 3	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface vlan 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für das VLAN aufgerufen (in dem sich die Fast-Ethernet-LAN-Schnittstellen [FE0–FE3] befinden), das als innere Schnittstelle für NAT dienen soll.

	Befehl	Zweck

Schritt 4	**ip nat** {**inside** | **outside**}
	
	Beispiel:
	`Router(config-if)# ip nat inside`
	`Router (config-if)#`
		Mit diesem Befehl wird die angegebene VLAN-Schnittstelle als innere NAT-Schnittstelle identifiziert.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 5	**no shutdown**
	
	Beispiel:
	`Router(config-if)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die an der Ethernet-Schnittstelle gerade vorgenommenen Konfigurationsänderungen aktiviert.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-Schnittstelle beendet.

Schritt 7	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-WAN-Schnittstelle (FE4) aufgerufen, die als äußere Schnittstelle für NAT dienen soll.

Schritt 8	**ip nat** {**inside** | **outside**}
	
	Beispiel:
	`Router(config-if)# ip nat outside`
	`Router (config-if)#`
		Mit diesem Befehl wird die angegebene WAN-Schnittstelle als äußere NAT-Schnittstelle festgelegt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 9	**no shutdown**
	
	Beispiel:
	`Router(config-if)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die an der Ethernet-Schnittstelle gerade vorgenommenen Konfigurationsänderungen aktiviert.

	Befehl	Zweck

Schritt 10	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-Schnittstelle beendet.

Schritt 11	**access-list** *Access-Listennummer* {**deny** | **permit**} *Quelle* [*Quellenplatzhalter*] **Beispiel:** `Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255`	In diesem Schritt wird eine standardmäßige Access-Liste definiert, durch die angegeben wird, welche Adressen übersetzt werden müssen. **Hinweis** Alle anderen Adressen werden implizit zurückgewiesen.

Hinweis Falls Sie NAT mit einer Virtual-Template-Schnittstelle verwenden möchten, müssen Sie eine Loopback-Schnittstelle konfigurieren. Informationen zum Konfigurieren einer Loopback-Schnittstelle finden Sie in Chapter 1, „Grundlegende Routerkonfiguration“.

Ausführliche Informationen zu den NAT-Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3. Allgemeinere Ausführungen zu den NAT-Konzepten finden Sie in Anhang B, „Konzepte“.

Konfigurationsbeispiel

Im nachstehenden Konfigurationsbeispiel ist ein Abschnitt der Konfigurationsdatei für das in diesem Kapitel beschriebene PPPoE-Szenario abgebildet.

Der VLAN-Schnittstelle ist die IP-Adresse 192.168.1.1 mit der Subnetzmaske 255.255.255.0 zugewiesen. NAT ist für die innere und äußere Schnittstelle konfiguriert.

Hinweis Durch „**(default)**“ gekennzeichnete Befehle werden jeweils automatisch generiert, sobald Sie den Befehl **show running-config** ausführen.

```
!
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface FastEthernet 4
ip address 192.168.12.2 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
!
```

```
interface dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
ip classless (default)
ip route 10.10.25.2 0.255.255.255 dialer 0
```

Überprüfen der Konfiguration

Geben Sie im privilegierten EXEC-Modus den Befehl **show ip nat statistics** ein, um die PPPoE-Konfiguration mit Network Address Translation (NAT) zu überprüfen. Die angezeigten Daten bei dieser Überprüfung sollten dem nachfolgenden Beispiel in etwa ähneln:

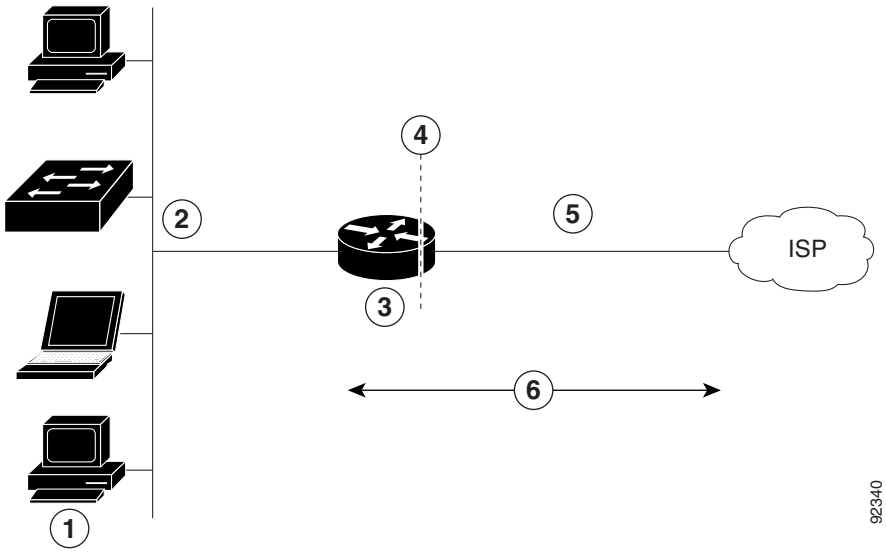
```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet4
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

Konfigurieren von PPP über ATM mit NAT

Die Zugangsrouter der Typen Cisco 857, Cisco 876, Cisco 877 und Cisco 878 unterstützen PPPoA-Clients mit NAT, d. h. Clients, die das Point-to-Point-Protokoll über ATM (asynchroner Transfermodus) und die Netzadress-Übersetzung (Network Address Translation) verwenden.

Mehrere PCs können hinter dem Router an ein LAN angeschlossen werden. Bevor Datenverkehr von den PCs an die PPPoA-Sitzung gesendet wird, können diese Daten u. a. verschlüsselt und gefiltert werden. PPP über ATM bietet eine Netzwerklösung mit vereinfachter Adressenbehandlung und direkter Benutzerüberprüfung wie bei einem Wählnetz. In Abbildung 4-1 ist ein typisches Einsatzszenario dargestellt, bei dem ein PPPoA-Client und NAT für den Cisco-Router konfiguriert wurden. In diesem Szenario wird eine einzelne statische IP-Adresse für die ATM-Verbindung verwendet.

Abbildung 4-1 PPP über ATM mit NAT



1	Kleines Unternehmen mit mehreren vernetzten Geräten – Desktop- und Laptop-PCs, Switches
2	Fast-Ethernet-LAN-Schnittstelle (innere Schnittstelle für NAT, 192.168.1.1/24)
3	PPPoA-Client – Router des Typs Cisco 857, Cisco 876, Cisco 877 oder Cisco 878

4	Punkt, an dem NAT erfolgt
5	ATM-WAN-Schnittstelle (äußere Schnittstelle für NAT)
6	PPPoA-Sitzung zwischen dem Client und einem PPPoA-Server beim Internet-Service-Provider (ISP)

In diesem Szenario kann das Kleinunternehmen oder der entfernte Benutzer im Fast-Ethernet-LAN eine Verbindung mit einem Internet-Service-Provider (ISP) unter Verwendung der folgenden Protokolle für die WAN-Verbindung herstellen:

- ADSL (Asymmetric Digital Subscriber Line) über analoge Telefonleitung (POTS, Plain Old Telephone Service) mit dem Router Cisco 857 oder Cisco 877
- ADSL über ISDN mit dem Router Cisco 876
- G.SHDSL (Single-Pair High-Speed Digital Subscriber Line) mit dem Router Cisco 878

Von der Fast-Ethernet-Schnittstelle wird das Datenpaket durch das LAN geleitet und an die PPP-Verbindung auf der ATM-Schnittstelle übergeben. Der ATM-Datenverkehr wird gekapselt und über die ADSL-, ISDN- oder G.SHDSL-Leitung gesendet. Mit der Dialer-Schnittstelle wird die Verbindung zum ISP hergestellt.

PPPoA

Die PPPoA-Clientfunktion am Router bietet PPPoA-Clientunterstützung auf ATM-Schnittstellen. Eine Dialer-Schnittstelle muss zum Klonen eines virtuellen Zugangs verwendet werden. Auf einer ATM-Schnittstelle können mehrere PPPoA-Clientsitzungen konfiguriert werden, jedoch muss für jede Sitzung jeweils eine separate Dialer-Schnittstelle und ein gesonderter Dialer-Pool verwendet werden.

Eine PPPoA-Sitzung wird auf der Clientseite durch den Router der Cisco 850- oder Cisco 870-Serie gestartet.

NAT

NAT (dargestellt durch die gestrichelte Linie am Rand des Cisco-Routers) bezeichnet zwei Adressierungsdomänen sowie die innere Quelladresse. Durch die Quellliste wird definiert, auf welche Weise das Paket im Netzwerk übertragen wird.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren der Dialer-Schnittstelle
- Konfigurieren der ATM-WAN-Schnittstelle
- Konfigurieren des DSL-Signalisierungsprotokolls
- Konfigurieren von NAT (Network Address Translation)

Ein Beispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 4-12.

Konfigurieren der Dialer-Schnittstelle

Durch die Dialer-Schnittstelle wird angegeben, wie der von den Clients kommende Datenverkehr behandelt wird. Hierzu gehören z. B. die standardmäßigen Routinginformationen, das Kapselungsprotokoll sowie der zu verwendende Dialer-Pool. Die Dialer-Schnittstelle wird ebenfalls für das Klonen eines virtuellen Zugangs verwendet. Auf einer ATM-Schnittstelle können mehrere PPPoA-Clientsitzungen konfiguriert werden, jedoch muss für jede Sitzung jeweils eine separate Dialer-Schnittstelle und ein gesonderter Dialer-Pool verwendet werden.

Führen Sie die folgenden Schritte aus, um eine Dialer-Schnittstelle für die ATM-Schnittstelle des Routers zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface dialer** *dialer-rotary-group-Nummer*
	
	Beispiel:
	`Router(config)# interface dialer 0`
	`Router (config-if)#`
		Mit diesem Befehl wird eine Dialer-Schnittstelle (mit einer Nummer zwischen 0 und 255) erstellt und der Schnittstellen-Konfigurationsmodus aufgerufen.

Schritt 2	**ip address negotiated**
	
	Beispiel:
	`Router(config-if)#ip address negotiated`
	`Router (config-if)#`
		In diesem Schritt wird angegeben, dass die IP-Adresse für die Dialer-Schnittstelle über PPP/IPCP-Adressenverhandlung (IP Control Protocol) bezogen wird.

Schritt 3	**ip mtu** *Byte*
	
	Beispiel:
	`Router(config-if)# ip mtu 4470`
	`Router (config-if)#`
		Mit diesem Befehl wird die Größe der IP-MTU (Maximum Transmission Unit; größtmögliche Dateneinheit zum Senden) festgelegt. Der standardmäßige Mindestwert beträgt 128 Byte. Der Höchstwert für ATM beträgt 4470 Byte.

Schritt 4	**encapsulation** *Kapselungstyp*
	
	Beispiel:
	`Router(config-if)#encapsulation ppp`
	`Router (config-if)#`
		Mit diesem Befehl wird der PPP-Kapselungstyp für die gesendeten und empfangenen Datenpakete festgelegt.

Schritt 5	**ppp authentication** {*Protokoll1* [*Protokoll2*...]}
	
	Beispiel:
	`Router(config-if)# ppp authentication chap`
	`Router (config-if)#`
		Mit diesem Befehl wird die PPP-Authentifizierungsmethode festgelegt.
		
		In diesem Beispiel wird CHAP (Challenge Handshake Authentication Protocol) angewendet.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 6	**dialer pool** *Nummer*
	
	Beispiel:
	`Router(config-if)#dialer pool 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Dialer-Pool angegeben, der zum Herstellen der Verbindung mit einem bestimmten Zielsubnetz verwendet werden soll.

	Befehl	Zweck

Schritt 7	**dialer-group** *Gruppennummer*
	
	Beispiel:
	`Router(config-if)# dialer-group 1`
	`Router (config-if)#`
		Mit diesem Befehl wird die Dialer-Schnittstelle einer Dialer-Gruppe (1–10) zugewiesen.
		
		Tipp Durch die Verwendung einer Dialer-Gruppe lässt sich der Zugriff auf den Router steuern.

Schritt 8	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird die Konfiguration der Schnittstelle „dialer 0“ beendet.

Schritt 9	**dialer-list** *Dialer-Gruppe* **protocol** *Protokollname* {**permit** | **deny** | **list** *Access-Listennummer* | **access-group**}
	
	Beispiel:
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		Mit diesem Befehl wird eine Dialer-Liste erstellt und einer Dialer-Gruppe zugeordnet. Datenpakete werden dann über die angegebene Dialer-Gruppe weitergeleitet.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Schritt 10	**ip route** *Präfix Maske* {*Schnittstellentyp Schnittstellennummer*}
	
	Beispiel:
	`Router(config)# ip route 10.10.25.2 0.255.255.255 dialer 0`
	`Router(config)#`
		Mit diesem Befehl wird die IP-Route für den Standard-Gateway für die Schnittstelle „dialer 0“ festgelegt.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Routing Protocols*.

Wiederholen Sie diese Schritte ggf. für alle weiteren Dialer-Schnittstellen oder Dialer-Pools.

Konfigurieren der ATM-WAN-Schnittstelle

Führen Sie die folgenden Schritte aus, um die ATM-Schnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface atm 0`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die ATM-Schnittstelle aufgerufen (diese Schnittstelle ist an der Rückseite des Routers mit der Aufschrift ADSLoPOTS oder G.SHDSL gekennzeichnet).
		
		Hinweis Diese Schnittstelle wurde während der grundlegenden Routerkonfiguration erstmals konfiguriert. Siehe „Konfigurieren von WAN-Schnittstellen“ auf Seite 1-7.

Schritt 2	**pvc** *vpi/vci*
	
	Beispiel:
	`Router(config-if)# pvc 8/35`
	`Router(config-if-atm-vc)#`
		Mit diesem Befehl wird ein ATM-PVC für jeden Endknoten (max. 10) erstellt, mit dem der Router kommuniziert. Zugleich wird der Konfigurationsmodus für den ATM-PVC aufgerufen.
		
		Wenn ein Permanent Virtual Circuit (PVC) definiert ist, wird standardmäßig die AAL5SNAP-Kapselung festgelegt. Verwenden Sie den Befehl **encapsulation**, um diese Standardeinstellung gemäß der Anleitung in Schritt 3 zu ändern. Die VPI- und VCI-Argumente können nicht gleichzeitig auf null gesetzt werden. Wenn ein Argument gleich null ist, muss das andere Argument ungleich null sein.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Wide-Area Networking Command Reference*.

Schritt 3	**encapsulation** {**aal5auto** | **aal5autoppp virtual-template** *Nummer* [**group** *Gruppenname*] | **aal5ciscoppp virtual-template** *Nummer* | **aal5mux** *Protokoll* | **aal5nlpid** | **aal5snap**}
	
	Beispiel:
	`Router(config-if-atm-vc)# encapsulation aal5mux ppp dialer`
	`Router(config-if-atm-vc)#`
		Mit diesem Befehl wird der Kapselungstyp für den PVC angegeben und auf die Dialer-Schnittstelle zurückverwiesen.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Wide-Area Networking Command Reference*.

	Befehl	Zweck

Schritt 4	**dialer pool-member** *Nummer*
	
	Beispiel:
	`Router(config-if-atm-vc)# dialer pool-member 1`
	`Router(config-if-atm-vc)#`
		Mit diesem Befehl wird die ATM-Schnittstelle als Mitglied eines Dialer-Pools des Dialer-Profils angegeben. Die Nummer des Pools muss zwischen 1 und 255 liegen.

Schritt 5	**no shutdown**
	
	Beispiel:
	`Router(config-if-atm-vc)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die an der ATM-Schnittstelle gerade vorgenommenen Schnittstellen- und Konfigurationsänderungen aktiviert.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die ATM-Schnittstelle beendet.

Konfigurieren des DSL-Signalisierungsprotokolls

Die DSL-Signalisierung muss auf der ATM-Schnittstelle für die Verbindung mit dem entsprechenden ISP konfiguriert werden. Die Router Cisco 857 und Cisco 877 unterstützen die ADSL-Signalisierung über POTS (Plain Old Telephone Service, konventionelle analoge Telefonleitung). Der Router Cisco 876 hingegen unterstützt die ADSL-Signalisierung über ISDN, und der Cisco 878 bietet Unterstützung für die SHDSL-Signalisierung. Informationen zur Konfiguration des geeigneten DSL-Signalisierungsprotokolls für den jeweils verwendeten Router finden Sie in den folgenden Abschnitten:

- Konfigurieren von ADSL
- Konfigurieren von SHDSL

Konfigurieren von ADSL

Die Standardkonfiguration für die ADSL-Signalisierung ist in Tabelle 4-1 angegeben.

Tabelle 4-1 ADSL-Standardkonfiguration

Attribut	Beschreibung	Standardwert
Operating mode	Gibt den Betriebsmodus der DSL-Leitung für eine ATM-Schnittstelle an. • ADSL über POTS – ANSI oder ITU Full Rate oder automatische Auswahl. • ADSL über ISDN – ITU Full Rate, ETSI oder automatische Auswahl.	Auto
Loss of margin	Gibt an, wie oft ein Verlust des Signal-Störabstands auftreten kann.	—
Training log	Zum Umschalten zwischen Aktivierung und Deaktivierung des „Training Log“.	Deaktiviert

Bei Bedarf können Sie diese Einstellungen im globalen Konfigurationsmodus jeweils mit einem der folgenden Befehle ändern:

- **dsl operating-mode** (im Konfigurationsmodus der ATM-Schnittstelle)
- **dsl lom** *Ganzzahl*
- **dsl enable-training-log**

Genauere Informationen zu diesen Befehlen finden Sie in der *Cisco IOS Wide-Area Networking Command Reference*.

Überprüfen der Konfiguration

Sie können überprüfen, ob die Konfiguration Ihren Vorstellungen entspricht, indem Sie den Befehl **show dsl interface atm** des privilegierten EXEC-Modus verwenden.

Konfigurieren von SHDSL

Führen Sie die folgenden Schritte aus, um den DSL-Controller im Router für die Verwendung der SHDSL-Signalisierung zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**controller dsl** *Port*
	
	Beispiel:
	`Router(config)# controller dsl 0`
	`Router(config-controller)#`
		Mit diesem Befehl wird der Konfigurationsmodus für den DSL-Controller aufgerufen.

Schritt 2	**line-term** {**co** | **cpe**}
	
	Beispiel:
	`Router(config-controller)# line-term co`
	`Router(config-controller)#`
		Gibt an, ob die DSL-Leitung in einer Ortsvermittlungsstelle (CO, Central Office) oder an einem Kundenendgerät (CPE, Customer Premises Equipment) abschließt.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-controller)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Controller-Konfigurationsmodus beendet und erneut der globale Konfigurationsmodus aufgerufen.

Schritt 4	**mode** *Protokoll*
	
	Beispiel:
	`Router(config)# mode atm`
	`Router(config-controller)#`
		Mit diesem Befehl wird der Modus des DSL-Controllers angegeben und der Controller-Konfigurationsmodus aufgerufen.

Schritt 5	**line-mode** {**4-wire** | **2-wire**}
	
	Beispiel:
	`Router(config-controller)# line-mode 4-wire`
	`Router(config-controller)#`
		Gibt an, ob diese DSL-Verbindung im Zweidraht- oder Vierdrahtmodus betrieben wird.

Schritt 6	**ignore-error-duration** *Anzahl*
	
	Beispiel:
	`Router(config-controller)#`
	`ignore-error-duration 15`
	`Router(config-controller)#`
		Gibt eine Zeitspanne im Bereich von 15 bis 30 Sekunden an, während der eventuelle Fehler ignoriert werden.

Schritt 7	**exit**
	
	Beispiel:
	`Router(config-controller)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Controller-Konfigurationsmodus beendet und erneut der globale Konfigurationsmodus aufgerufen.

Hinweis Falls Sie den Cisco-Router in ein Netz nach europäischem Standard einbinden, wählen Sie mit dem Befehl **dsl dsl-mode shdsl symmetric annex** {**A** | **B**} „Annex B“ aus. Standardmäßig verwendet der Router „Annex A“ (für USA).

Überprüfen der Konfiguration

Sie können überprüfen, ob die Konfiguration Ihren Vorstellungen entspricht, indem Sie den Befehl **show controllers dsl** des privilegierten EXEC-Modus verwenden.

```
Router# show controllers dsl 0
DSL 0 controller UP
SLOT 0: Globespan xDSL controller chipset
DSL mode: SHDSL Annex A
Frame mode: Utopia
Configured Line rate: Auto
Line Re-activated 6 times after system bootup
LOSW Defect alarm: ACTIVE
CRC per second alarm: ACTIVE
Line termination: CPE

    Current 15 min CRC: 0
    Current 15 min LOSW Defect: 0
    Current 15 min ES Defect: 0
    Current 15 min SES Defect: 0
    Current 15 min UAS Defect: 33287

    Previous 15 min CRC Defect: 0
    Previous 15 min LOSW Defect: 0
    Previous 15 min ES Defect: 0
    Previous 15 min SES Defect: 0
    Previous 15 min UAS Defect: 0

Line-0 status
Chipset Version: 0
Firmware Version: A388
Modem Status: Data, Status 1
Last Fail Mode: No Failure status:0x0
Line rate: 2312 Kbps
Framer Sync Status: In Sync
Rcv Clock Status: In the Range
Loop Attenuation: 341,1450 dB
Transmit Power: 7,5 dB
Receiver Gain: 22,5420 dB
SNR Sampling: 36.8590 dB
Dying Gasp: Present
```

Konfigurieren von NAT (Network Address Translation)

Durch NAT (Network Address Translation, Netzadress-Übersetzung) werden Pakete von Adressen, die mit einer standardmäßigen Access-Liste übereinstimmen, anhand von globalen Adressen übersetzt, die durch die Dialer-Schnittstelle zugewiesen werden. Die über die innere Schnittstelle in den Router eingehenden Pakete und/oder die vom Router bezogenen Pakete werden anhand der Access-Liste auf eine mögliche Adressübersetzung geprüft. Sie können NAT für statische oder dynamische Adressübersetzungen konfigurieren.

Führen Sie die folgenden Schritte aus, um die äußere ATM-WAN-Schnittstelle mit dynamischer NAT zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip nat pool** *Name Anfangs-IP End-IP* {**netmask** *Netzmaske* | **prefix-length** *Präfixlänge*}
	
	Beispiel:
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255`
	`Router(config)#`
		Mit diesem Befehl wird ein Pool mit globalen IP-Adressen für NAT erstellt.

Schritt 2	**ip nat inside source** {**list** *Access-Listenummer*} {**interface** *Typ Nummer* | **pool** *Name*} [**overload**]
	
	Beispiel 1:
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	
	oder
	
	Beispiel 2:
	`Router(config)# ip nat inside source list acl1 pool pool1`
		Mit diesem Befehl wird die dynamische Übersetzung von Adressen auf der inneren Schnittstelle aktiviert.
		
		Im ersten Beispiel werden die in der Access-Liste *1* zugelassenen Adressen in eine der Adressen übersetzt, die in der Dialer-Schnittstelle *0* angegeben sind.
		
		Im zweiten Beispiel werden die durch die Access-Liste *acl1* zugelassenen Adressen jeweils in eine Adresse aus dem NAT-Pool *pool1* übersetzt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 3	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface vlan 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für das VLAN aufgerufen (in dem sich die Fast-Ethernet-LAN-Schnittstellen [FE0–FE3] befinden), das als innere Schnittstelle für NAT dienen soll.

	Befehl	Zweck

Schritt 4	**ip nat** {**inside** | **outside**}
	
	Beispiel:
	`Router(config-if)# ip nat inside`
	`Router (config-if)#`
		Mit diesem Befehl wird NAT auf die Fast-Ethernet-LAN-Schnittstelle angewendet, die als innere Schnittstelle gilt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 5	**no shutdown**
	
	Beispiel:
	`Router(config-if)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die an der Ethernet-Schnittstelle gerade vorgenommenen Konfigurationsänderungen aktiviert.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Fast-Ethernet-Schnittstelle beendet.

Schritt 7	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die ATM-WAN-Schnittstelle (FE4) aufgerufen, die als äußere Schnittstelle für NAT dienen soll.

Schritt 8	**ip nat** {**inside** | **outside**}
	
	Beispiel:
	`Router(config-if)# ip nat outside`
	`Router (config-if)#`
		Mit diesem Befehl wird die angegebene WAN-Schnittstelle als äußere NAT-Schnittstelle festgelegt.
		
		Weitere Informationen über diesen Befehl und weitere einstellbare Parameter sowie Hinweise zum Aktivieren der statischen Übersetzung finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 9	**no shutdown**
	
	Beispiel:
	`Router(config-if)# no shutdown`
	`Router (config-if)#`
		Mit diesem Befehl werden die an der Ethernet-Schnittstelle gerade vorgenommenen Konfigurationsänderungen aktiviert.

	Befehl	Zweck

Schritt 10	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die ATM-Schnittstelle beendet.

Schritt 11	**access-list** *Access-Listennummer* {**deny** | **permit**} *Quelle* [*Quellenplatzhalter*] **Beispiel:** `Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255`	Mit diesem Befehl wird eine standardmäßige Access-Liste definiert, in der zulässige Adressen angegeben sind, die übersetzt werden müssen. **Hinweis** Alle anderen Adressen werden implizit zurückgewiesen.

Hinweis Falls Sie NAT mit einer Virtual-Template-Schnittstelle verwenden möchten, müssen Sie eine Loopback-Schnittstelle konfigurieren. Informationen zum Konfigurieren der Loopback-Schnittstelle finden Sie in Chapter 1, „Grundlegende Routerkonfiguration“.

Umfassende Informationen zu NAT-Befehlen finden Sie in der Dokumentation von Cisco IOS Release 12.3. Allgemeinere Ausführungen zu den NAT-Konzepten finden Sie in Anhang B, „Konzepte“.

Konfigurationsbeispiel

Im folgenden Konfigurationsbeispiel ist ein Abschnitt der Konfigurationsdatei für einen Client in dem PPPoA-Szenario dargestellt, das in diesem Kapitel beschrieben wurde.

Der VLAN-Schnittstelle ist die IP-Adresse 192.168.1.1 mit der Subnetzmaske 255.255.255.0 zugewiesen. NAT ist für die innere und äußere Schnittstelle konfiguriert.

Hinweis Durch „**(default)**“ gekennzeichnete Befehle werden jeweils automatisch generiert, sobald Sie den Befehl **show running-config** ausführen.

```
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly (default)
!
interface ATM0
 no ip address
 ip nat outside
 ip virtual-reassembly
 no atm ilmi-keepalive
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
```

```
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless (default)
!
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255
ip nat inside source list 1 interface Dialer0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit

ip route 10.10.25.2 0.255.255.255 dialer 0
!
```

Überprüfen der Konfiguration

Geben Sie im privilegierten EXEC-Modus den Befehl **show ip nat statistics** ein, um die Konfiguration des PPPoA-Clients mit Network Address Translation (NAT) zu überprüfen. Die angezeigten Daten bei dieser Überprüfung sollten dem nachfolgenden Beispiel in etwa ähneln:

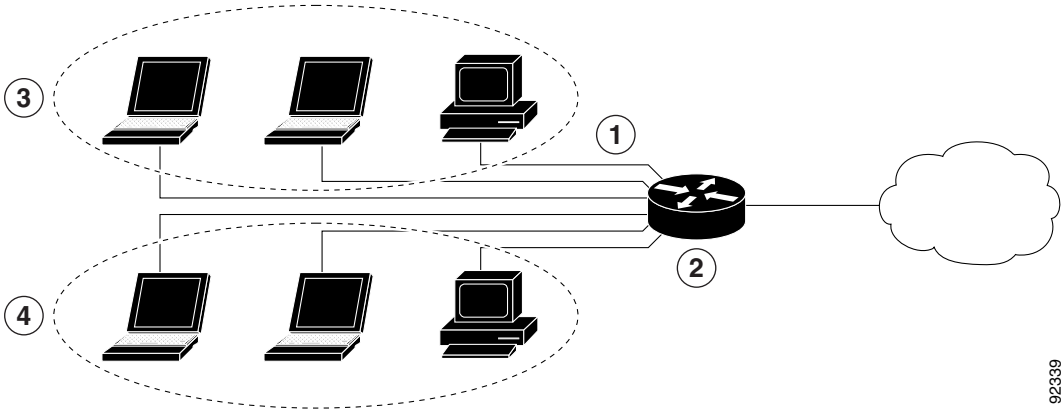
```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  ATM0
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

Konfigurieren eines LAN mit DHCP und VLANs

Die Router der Cisco 850-Serie und der Cisco 870-Serie unterstützen Clients in physischen LANs und in virtuellen LANs (VLANs). Über DHCP (Dynamic Host Configuration Protocol) können diese Router eine automatische Zuweisung von IP-Konfigurationen für Knoten in diesen Netzwerken aktivieren.

In Abbildung 5-1 ist ein typisches Einsatzszenario dargestellt, bei dem zwei physische LANs durch den Router und zwei VLANs miteinander verbunden sind.

Abbildung 5-1 Physische und virtuelle LANs – DHCP auf Cisco-Router konfiguriert



1	Fast-Ethernet-LAN (mit mehreren vernetzten Geräten)
2	Router und DHCP-Server – Zugangsrouter der Cisco 850-Serie oder Cisco 870-Serie – mit dem Internet verbunden
3	VLAN 1
4	VLAN 2

DHCP

DHCP, das in RFC 2131 beschrieben ist, nutzt für die Adressenzuweisung ein Client/Server-Modell. Als Administrator können Sie den Router der Cisco 800-Serie als DHCP-Server konfigurieren, der die IP-Adressenzuweisung und andere TCP/IP-orientierte Konfigurationsinformationen für die Arbeitsstationen bereitstellt. Mit DHCP müssen IP-Adressen nicht mehr manuell für jeden Client einzeln zugewiesen werden.

Beim Konfigurieren eines DHCP-Servers müssen die Servereigenschaften, Richtlinien und DHCP-Optionen festgelegt werden.

Hinweis Bei jeder Änderung der Servereigenschaften müssen Sie die Konfigurationsdaten aus der Network Registrar-Datenbank neu auf den Server laden.

VLANs

Die Zugangsrouter der Cisco 850-Serie und Cisco 870-Serie unterstützen vier Fast-Ethernet-Anschlüsse, die für die Konfiguration von VLANs zur Verfügung stehen.

Mit VLANs können Netzwerke segmentiert und unabhängig vom physischen Standort oder der LAN-Verbindung des Benutzers in logische Benutzergruppen aufgeteilt werden.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren von DHCP
- Konfigurieren von VLANs

Hinweis Bei den in diesem Kapitel beschriebenen Anleitungen wird davon ausgegangen, dass Sie die grundlegenden Routerfunktionen sowie PPPoE oder PPPoA mit NAT bereits konfiguriert haben. Falls Sie diese Konfigurationsschritte noch nicht ausgeführt haben, finden Sie die entsprechenden Informationen für Ihren Router in Kapitel 1, „Grundlegende Routerkonfiguration“, Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“, und Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“.

Konfigurieren von DHCP

Führen Sie die folgenden Schritte aus, um den Router für DHCP-Betrieb zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip domain name** *Name*
	
	Beispiel:
	`Router(config)# ip domain name smallbiz.com`
	`Router(config)#`
		Mit diesem Befehl wird die Standarddomäne angegeben, die vom Router verwendet wird, um unvollständige Hostnamen zu ergänzen (Namen, bei denen der Domänenname in Dezimalpunktschreibweise fehlt).

Schritt 2	**ip name-server** *Serveradresse1* [*Serveradresse2...Serveradresse6*]
	
	Beispiel:
	`Router(config)# ip name-server 192.168.11.12`
	`Router(config)#`
		Mit diesem Befehl wird die Adresse eines oder mehrerer DNS-Server (Domain Name System) angegeben, die für die Namens- und Adressauflösung verwendet werden.

	Befehl	Zweck
Schritt 3	**ip dhcp excluded-address** *Anfangsadresse* [*Endadresse*] **Beispiel:** `Router(config)# ip dhcp excluded-address 192.168.9.0`	Mit diesem Befehl werden die IP-Adressen angegeben, die ausgeschlossen, d. h. den DHCP-Clients vom DHCP-Server nicht zugewiesen werden sollen. In diesem Beispiel wird die Routeradresse ausgeschlossen.

Schritt 4	**ip dhcp pool** *Name*
	
	Beispiel:
	`Router(config)# ip dhcp pool dpool1`
	`Router(config-dhcp)#`
		Mit diesem Befehl wird ein DHCP-Adresspool auf dem Router erstellt und der Konfigurationsmodus für „DHCP Pool“ aufgerufen. Das Argument *Name* kann eine Zeichenfolge oder ein ganzzahliger Wert sein.

Schritt 5	**network** *Netzwerknummer* [*Maske* | *Präfixlänge*]
	
	Beispiel:
	`Router(config-dhcp)# network 10.10.0.0 255.255.255.0`
	`Router(config-dhcp)#`
		Mit diesem Befehl wird die Subnetz-ID (IP-Adresse) für den DHCP-Adresspool definiert, optional auch mit Maske.

Schritt 6	**import all**
	
	Beispiel:
	`Router(config-dhcp)# import all`
	`Router(config-dhcp)#`
		Mit diesem Befehl werden DHCP-Optionsparameter in den DHCP-Abschnitt der Routerdatenbank importiert.

Schritt 7	**default-router** *Adresse* [*Adresse2...Adresse8*]
	
	Beispiel:
	`Router(config-dhcp)# dns-server 10.10.10.10`
	`Router(config-dhcp)#`
		Mit diesem Befehl können bis zu 8 Standardrouter für einen DHCP-Client angegeben werden.

Schritt 8	**dns-server** *Adresse* [*Adresse2...Adresse8*]
	
	Beispiel:
	`Router(config-dhcp)# dns-server 192.168.35.2`
	`Router(config-dhcp)#`
		Mit diesem Befehl können bis zu acht DNS-Server angegeben werden, die für einen DHCP-Client verfügbar sind.

Schritt 9	**domain-name** *Domäne*
	
	Beispiel:
	`Router(config-dhcp)# domain-name cisco.com`
	`Router(config-dhcp)#`
		Mit diesem Befehl wird der Domänenname für einen DHCP-Client angegeben.

Schritt 10	**exit**
	
	Beispiel:
	`Router(config-dhcp)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der DHCP-Konfigurationsmodus beendet und der globale Konfigurationsmodus aufgerufen.

Konfigurationsbeispiel

Im nachstehenden Konfigurationsbeispiel ist ein Abschnitt der Konfigurationsdatei für die in diesem Kapitel beschriebene DHCP-Konfiguration dargestellt.

```
ip dhcp excluded-address 192.168.9.0
!
ip dhcp pool dpool1
   import all
   network 10.10.0.0 255.255.255.0
   default-router 10.10.10.10
   dns-server 192.168.35.2
   domain-name cisco.com
!
ip domain name smallbiz.com
ip name-server 192.168.11.12
```

Überprüfen einer DHCP-Konfiguration

Verwenden Sie die nachstehend genannten Befehle, um eine DHCP-Konfiguration anzuzeigen.

- **show ip dhcp import** – Zur Anzeige der optionalen Parameter, die in die DHCP-Serverdatenbank importiert wurden.
- **show ip dhcp pool** – Zur Anzeige von Informationen über die DHCP-Adresspools.
- **show ip dhcp server statistics** – Zur Anzeige der DHCP-Serverstatistik, beispielsweise der Anzahl der Adresspools, Bindungen (Bindings) usw.

```
Router# show ip dhcp import

Address Pool Name: dpool1

Router# show ip dhcp pool

Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0

Router# show ip dhcp server statistics
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
```

```
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

Konfigurieren von VLANs

Führen Sie die folgenden Schritte aus, um VLANs auf einem Router zu konfigurieren (zu Beginn befindet sich der Router im privilegierten EXEC-Modus):

	Befehl	Zweck

Schritt 1	**vlan database**
	
	Beispiel:
	`Router# vlan database`
	`Router(vlan)#`
		Mit diesem Befehl wird der VLAN-Konfigurationsmodus aufgerufen.

Schritt 2	**vlan** *VLAN-ID* [**media** *Typ*] [**name** *VLAN-Name*]
	
	Beispiel:
	`Router(vlan)# vlan 2 media ethernet name VLAN0002`
	`Router(vlan)# vlan 3 media ethernet name red-vlan`
	`Router(vlan)#`
		Mit diesem Befehl werden VLANs hinzugefügt, wobei die entsprechenden VLAN-IDs im Bereich von 2 bis 1001 liegen können.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Switching Services Command Reference*.

Schritt 3	**exit**
	
	Beispiel:
	`Router(vlan)# exit`
	`Router#`
		Mit diesem Befehl wird die VLAN-Datenbank aktualisiert und in die gesamte administrative Domäne weitergegeben. Daraufhin wird wieder der privilegierte EXEC-Modus aufgerufen.

Überprüfen einer VLAN-Konfiguration

Verwenden Sie die nachstehend genannten Befehle, um die VLAN-Konfiguration anzuzeigen.

- **show** – Dieser Befehl wird im VLAN-Datenbankmodus eingegeben. Er zeigt eine Zusammenfassung der Konfigurationsinformationen für alle konfigurierten VLANs an.
- **show vlan-switch** – Dieser Befehl wird im privilegierten EXEC-Modus eingegeben. Er zeigt detaillierte Konfigurationsinformationen für alle konfigurierten VLANs an.

```
Router# vlan database
Router(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Deaktiviert
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

  VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM
```

```
Router# show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0, Fa1, Fa2, Fa3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
Router#
```

Konfigurieren eines VPN mit Easy VPN und einem IPSec-Tunnel

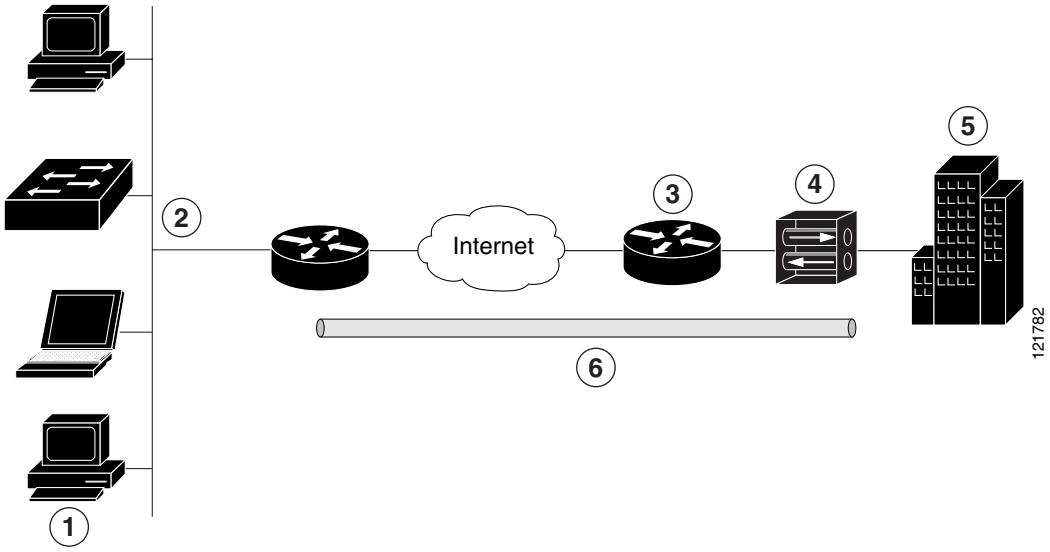
Die Router der Cisco 850-Serie und der Cisco 870-Serie unterstützen die Erstellung virtueller privater Netzwerke (VPNs).

Cisco-Router und andere Breitbandgeräte ermöglichen Hochgeschwindigkeitsverbindungen mit dem Internet. Für viele Anwendungen wird jedoch auch die Sicherheit von VPN-Verbindungen benötigt, die eine hohe Authentifizierungsstufe bieten und Daten zwischen zwei bestimmten Endpunkten verschlüsseln.

Zwei Typen von VPNs werden unterstützt: Standort-zu-Standort-VPN und Fernzugriff-VPN. Mit Standort-zu-Standort-VPNs können beispielsweise Zweigstellen mit Unternehmenszentralen verbunden werden. Über Fernzugriff-VPNs können sich entfernte Clients bei einem Unternehmensnetz anmelden und eine Verbindung mit dem Netz herstellen.

Durch das Beispiel in diesem Kapitel wird die Konfiguration eines Fernzugriff-VPNs verdeutlicht, das mithilfe von Cisco Easy VPN und einem IPSec-Tunnel eine Verbindung zwischen einem entfernten Client und dem Unternehmensnetzwerk konfiguriert und sichert. In Abbildung 6-1 ist ein typisches Einsatzszenario dargestellt.

Abbildung 6-1 Fernzugriff-VPN mit IPSec-Tunnel



1	Entfernte, vernetzte Benutzer
2	VPN-Client – Zugangsrouter der Cisco 850-Serie oder der Cisco 870-Serie
3	Router – Ermöglicht den Zugang zum Netzwerk in der Unternehmenszentrale
4	VPN-Server – Easy VPN-Server, beispielsweise ein Cisco VPN 3000-Konzentrator; die Netzadresse der äußeren Schnittstelle lautet 210.110.101.1
5	Unternehmenszentrale mit der Netzadresse 10.1.1.1
6	IPSec-Tunnel

Cisco Easy VPN

Durch Verwendung der Cisco Easy VPN-Clientfunktion entfällt ein großer Teil der aufwändigen Konfigurationsvorgänge durch Implementierung des Unity Client-Protokolls von Cisco. Mit diesem Protokoll können die meisten VPN-Parameter, z. B. interne IP-Adressen, interne Subnetzmasken, DHCP-Serveradressen, WINS-Serveradressen und Split-Tunneling-Flags, auf einem VPN-Server definiert werden, z. B. auf einem Konzentrator der Cisco VPN 3000-Serie, der als IPSec-Server eingerichtet ist.

Mit einem Easy VPN-Server-fähigen Gerät können VPN-Tunnel abgeschlossen werden, die durch mobil und entfernt arbeitende Personen initiiert wurden, die Cisco Easy VPN Remote-Software auf PCs ausführen. Mit solchen Easy VPN-Server-fähigen Geräten können entfernte Router als Easy VPN-Remoteknoten betrieben werden.

Die Cisco Easy VPN-Clientfunktion kann in zwei Modi konfiguriert werden: im Clientmodus oder im Netzerweiterungsmodus. Der Clientmodus ist die Standardkonfiguration. In diesem Modus wird nur Geräten an einem Clientstandort der Zugriff auf Ressourcen des zentralen Standorts gestattet. Am Clientstandort befindliche Ressourcen sind für den zentralen Standort hingegen nicht verfügbar. Im Netzerweiterungsmodus ist es den Benutzern am zentralen Standort (an dem sich der Konzentrator der VPN 3000-Serie befindet) gestattet, auf Netzwerkressourcen zuzugreifen, die sich am Clientstandort befinden.

Nachdem der IPSec-Server konfiguriert wurde, kann eine VPN-Verbindung mit einer Minimalkonfiguration auf einem IPSec-Client erstellt werden, z. B. einem unterstützten Router der Cisco 850-Serie oder der Cisco 870-Serie. Sobald der IPSec-Client die VPN-Tunnelverbindung initiiert, überträgt der IPSec-Server per Push-Verfahren die IPSec-Richtlinien auf den IPSec-Client und erstellt die entsprechende VPN-Tunnelverbindung.

Hinweis Die Cisco Easy VPN-Clientfunktion unterstützt die Konfiguration nur eines Zielpeers. Falls für Ihre Anwendung die Erstellung mehrerer VPN-Tunnel erforderlich ist, müssen Sie die IPSec-VPN- und NAT/PAT-Parameter (Network Address Translation/Peer Address Translation) auf dem Client sowie auf dem Server manuell konfigurieren.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um Ihren Router für dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren der IKE-Richtlinie
- Konfigurieren von Gruppenrichtlinieninformationen
- Anwenden einer Moduskonfiguration auf die Crypto-Map
- Aktivieren von Richtlinien-Lookup
- Konfigurieren von IPSec-Transformationen und Protokollen

- Konfigurieren der IPSec-Verschlüsselungsmethode und -Parameter
- Anwenden der Crypto-Map auf die physische Schnittstelle
- Erstellen einer Easy VPN-Fernkonfiguration

Ein Beispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 6-12.

Hinweis Bei den in diesem Kapitel beschriebenen Anleitungen wird davon ausgegangen, dass Sie die grundlegenden Routerfunktionen sowie PPPoE oder PPPoA mit NAT, DCHP und VLANs bereits konfiguriert haben. Falls Sie diese Konfigurationsschritte noch nicht ausgeführt haben, finden Sie die entsprechenden Informationen für Ihren Router in Kapitel 1, „Grundlegende Routerkonfiguration“, Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“, Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“, und Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“.

Konfigurieren der IKE-Richtlinie

Führen Sie die folgenden Schritte aus, um die IKE-Richtlinie (Internet Key Exchange) zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto isakmp policy** *Priorität*
	
	Beispiel:
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird eine IKE-Richtlinie erstellt, die während der IKE-Verhandlung verwendet wird. Die Priorität wird mit einer Zahl im Bereich von 1 bis 10000 definiert, wobei 1 die höchste Prioritätsstufe ist.
		
		Außerdem wird der Konfigurationsmodus für ISAKMP-Richtlinien (Internet Security Association Key and Management Protocol) aufgerufen.

Schritt 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	
	Beispiel:
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird der in der IKE-Richtlinie verwendete Verschlüsselungsalgorithmus angegeben.
		
		In diesem Beispiel wird der 168-Bit-Verschlüsselungsstandard Dreifach-DES (Triple Data Encryption Standard) verwendet.

Schritt 3	**hash** {**md5** | **sha**}
	
	Beispiel:
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird der Hash-Algorithmus festgelegt, der in der IKE-Richtlinie verwendet wird.
		
		In diesem Beispiel ist der Algorithmus MD5 (Message Digest 5) angegeben. Die Standardeinstellung ist SHA-1 (Secure Hash-Standard).

	Befehl oder Aktion	Zweck

Schritt 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	
	Beispiel:
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird die Authentifizierungsmethode festgelegt, die in der IKE-Richtlinie verwendet wird.
		
		In diesem Beispiel wird die Authentifizierungsmethode „Pre-Shared Key“ angegeben.

Schritt 5	**group** {**1** | **2** | **5**}
	
	Beispiel:
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		Gibt an, dass ein Algorithmus der Diffie-Hellman-Gruppe in einer IKE-Richtlinie verwendet wird.

Schritt 6	**lifetime** *Sekunden*
	
	Beispiel:
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		Gibt die Gültigkeitsdauer im Bereich von 60 bis 86400 Sekunden für eine IKE-Security-Association (SA) an.

Schritt 7	**exit**
	
	Beispiel:
	`Router(config-isakmp)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für IKE-Richtlinien beendet und der globale Konfigurationsmodus aufgerufen.

Konfigurieren von Gruppenrichtlinieninformationen

Führen Sie die folgenden Schritte aus, um die Gruppenrichtlinie zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	
	Beispiel:
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird eine IKE-Richtliniengruppe erstellt, in der Attribute enthalten sind, die auf den entfernten Client heruntergeladen werden sollen.
		
		Außerdem wird der Konfigurationsmodus für ISAKMP-Gruppenrichtlinien (Internet Security Association Key and Management Protocol) aufgerufen.

Schritt 2	**key** *Name*
	
	Beispiel:
	`Router(config-isakmp-group)# key secret-password`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird der IKE-Preshared-Key für die Gruppenrichtlinie angegeben.

	Befehl oder Aktion	Zweck

Schritt 3	**dns** *primärer-Server*
	
	Beispiel:
	`Router(config-isakmp-group)# dns 10.50.10.1`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird der primäre DNS-Server (Domain Name System) für die Gruppe angegeben.
		
		Hinweis Mit dem Befehl **wins** können Sie außerdem WINS-Server (Windows Internet Naming Service) für die Gruppe angeben.

Schritt 4	**domain** *Name*
	
	Beispiel:
	`Router(config-isakmp-group)# domain company.com`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird die Zugehörigkeit der Gruppe zu einer Domäne angegeben.

Schritt 5	**exit**
	
	Beispiel:
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für IKE-Gruppenrichtlinien beendet und der globale Konfigurationsmodus aufgerufen.

Schritt 6	**ip local pool** {**default** | *Poolname*} [*IP-Anfangsadresse* [*IP-Endadresse*]]
	
	Beispiel:
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		Mit diesem Befehl wird ein lokaler Adresspool für die Gruppe angegeben.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Anwenden einer Moduskonfiguration auf die Crypto-Map

Führen Sie die folgenden Schritte aus, um eine Moduskonfiguration auf die Crypto-Map anzuwenden (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto map** *Map-Name* **isakmp authorization list** *Listenname*
	
	Beispiel:
	`Router(config)# crypto map dynmap isakmp authorization list rtr-remote`
	`Router(config)#`
		Mit diesem Befehl wird die Moduskonfiguration auf die Crypto-Map angewendet und die Funktion zum Schlüssel-Lookup (IKE-Abfragen) für die Gruppenrichtlinie von einem AAA-Server (Authentifizierung, Autorisierung und Abrechnung) aktiviert.

Schritt 2	**crypto map** *Tag* **client configuration address** [**initiate** | **respond**]
	
	Beispiel:
	`Router(config)# crypto map dynmap client configuration address respond`
	`Router(config)#`
		Mit diesem Befehl wird der Router so konfiguriert, dass er Moduskonfigurationsanforderungen von entfernten Clients beantwortet.

Aktivieren von Richtlinien-Lookup

Führen Sie die folgenden Schritte aus, um Richtlinien-Lookup über AAA zu aktivieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**aaa new-model**
	
	Beispiel:
	`Router(config)# aaa new-model`
	`Router(config)#`
		Mit diesem Befehl wird das AAA-Zugriffssteuerungsmodell aktiviert.

Schritt 2	**aaa authentication login** {**default** | *Listenname*} *Methode1* [*Methode2...*]
	
	Beispiel:
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		Mit diesem Befehl wird die AAA-Authentifizierung ausgewählter Benutzer bei der Anmeldung festgelegt und die verwendete Methode angegeben.
		
		In diesem Beispiel wird eine lokale Authentifizierungsdatenbank verwendet. Sie könnten hierfür auch einen RADIUS-Server verwenden. Genauere Informationen finden Sie im *Cisco IOS Security Configuration Guide* und in der *Cisco IOS Security Command Reference*.

	Befehl oder Aktion	Zweck

Schritt 3	**aaa authorization** {**network** | **exec** | **commands** *Ebene* | **reverse-access** | **configuration**} {**default** | *Listenname*} [*Methode1* [*Methode2...*]]
	
	Beispiel:
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		In diesem Schritt wird für alle netzwerkbezogenen Dienstanforderungen, einschließlich PPP, die AAA-Autorisierung sowie die Methode der Autorisierung festgelegt.
		
		In diesem Beispiel wird eine lokale Autorisierungsdatenbank verwendet. Sie könnten hierfür auch einen RADIUS-Server verwenden. Genauere Informationen finden Sie im *Cisco IOS Security Configuration Guide* und in der *Cisco IOS Security Command Reference*.

Schritt 4	**username** *Name* {**nopassword** | **password** *Kennwort* | **password** *Verschlüsselungstyp verschlüsseltes-Kennwort*}
	
	Beispiel:
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		In diesem Schritt wird ein benutzernamenbasiertes Authentifizierungssystem eingerichtet.
		
		In diesem Beispiel wird der Benutzername *Cisco* mit dem verschlüsselten Kennwort *Cisco* implementiert.

Konfigurieren von IPSec-Transformationen und Protokollen

Ein Transformationssatz stellt eine bestimmte Kombination von Sicherheitsprotokollen und -algorithmen dar. Während der IKE-Verhandlung wird zwischen den Peers vereinbart, einen bestimmten Transformationssatz zum Schutz des Datenflusses zu verwenden.

Bei den IKE-Verhandlungen suchen die Peers in mehreren Transformationssätzen nach einer bei beiden Peers identischen Transformation. Wird ein derartiger Transformationssatz gefunden, wird er ausgewählt und auf den geschützten Datenverkehr als Bestandteil der Konfigurationen beider Peers angewendet.

Führen Sie die folgenden Schritte aus, um die IPSec-Transformationssätze und -Protokolle anzugeben (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto ipsec transform-set** *Transformationssatzname Transformation1* [*Transformation2*] [*Transformation3*] [*Transformation4*]
	
	Beispiel:
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		Mit diesem Befehl wird ein Transformationssatz, eine zulässige Kombination aus IPSec-Sicherheitsprotokollen und -Algorithmen, definiert.
		
		Ausführliche Informationen zu gültigen Transformationen und Kombinationen finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 2	**crypto ipsec security-association lifetime** {**seconds** *Sekunden* | **kilobytes** *Kilobytes*}
	
	Beispiel:
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		Mit diesem Befehl werden die Werte für die globale Gültigkeitsdauer festgelegt, die bei der Verhandlung der IPSec-Security-Associations verwendet werden.
		
		Ausführliche Informationen finden Sie in der *Cisco IOS Security Command Reference*.

Hinweis Bei manuell eingerichteten Security-Associations erfolgt keine Verhandlung mit dem Peer, und beide Seiten müssen jeweils denselben Transformationssatz angeben.

Konfigurieren der IPSec-Verschlüsselungsmethode und -Parameter

Durch eine dynamische Crypto-Map-Richtlinie werden Verhandlungsanforderungen für neue Security-Associations von entfernten IPSec-Peers verarbeitet, selbst wenn der Router nicht alle Crypto-Map-Parameter kennt (z. B. die IP-Adresse).

Führen Sie die folgenden Schritte aus, um die IPSec-Verschlüsselungsmethode zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto dynamic-map** *dynamischer-Map-Name dynamische-Seq-Num*
	
	Beispiel:
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		Mit diesem Befehl wird ein Eintrag für eine dynamische Crypto-Map erstellt und der Crypto-Map-Konfigurationsmodus aufgerufen.
		
		Ausführliche Informationen zu diesem Befehl finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 2	**set transform-set** *Transformationssatzname* [*Transformationssatzname2 ... Transformationssatzname6*]
	
	Beispiel:
	`Router(config-crypto-map)# set transform-set vpn1`
	`Router(config-crypto-map)#`
		Mit diesem Befehl wird festgelegt, welche Transformationssätze mit dem Crypto-Map-Eintrag verwendet werden können.

Schritt 3	**reverse-route**
	
	Beispiel:
	`Router(config-crypto-map)# reverse-route`
	`Router(config-crypto-map)#`
		Mit diesem Befehl werden Quellproxyinformationen für den Crypto-Map-Eintrag erstellt.
		
		Ausführliche Informationen finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 4	**exit**
	
	Beispiel:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Schritt 5	**crypto map** *Map-Name Seq-Num* [**ipsec-isakmp**] [**dynamic** *dynamischer-Map-Name*] [**discover**] [**profile** *Profilname*]
	
	Beispiel:
	`Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`
	`Router(config)#`
		Mit diesem Befehl wird ein Crypto-Map-Profil erstellt.

Anwenden der Crypto-Map auf die physische Schnittstelle

Die Crypto-Maps müssen auf jede einzelne Schnittstelle angewendet werden, über die IPSec-Datenverkehr (IP Security) fließt. Durch Anwendung der Crypto-Map auf die physische Schnittstelle wird der Router angewiesen, den gesamten Datenverkehr anhand der Security-Association-Datenbank zu evaluieren. Mit den Standardkonfigurationen bietet der Router eine sichere Konnektivität, da der zwischen den entfernten Standorten gesendete Datenverkehr verschlüsselt wird. Die öffentliche Schnittstelle gestattet jedoch auch die Durchleitung des übrigen Datenverkehrs und stellt eine Verbindung mit dem Internet bereit.

Führen Sie die folgenden Schritte aus, um eine Crypto-Map auf eine Schnittstelle anzuwenden (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die Schnittstelle aufgerufen, auf die Sie die Crypto-Map anwenden möchten.

Schritt 2	**crypto map** *Map-Name*
	
	Beispiel:
	`Router(config-if)# crypto map static-map`
	`Router (config-if)#`
		Mit diesem Befehl wird die Crypto-Map auf die Schnittstelle angewendet.
		
		Ausführliche Informationen zu diesem Befehl finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Erstellen einer Easy VPN-Fernkonfiguration

Der Router, der als entfernter IPSec-Router eingerichtet ist, muss eine Easy VPN-Fernkonfiguration erstellen und diese der Schnittstelle für den ausgehenden Datenverkehr zuweisen.

Führen Sie die folgenden Schritte aus, um die Fernkonfiguration zu erstellen (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto ipsec client ezvpn** *Name*
	
	Beispiel:
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Mit diesem Befehl wird eine Cisco Easy VPN-Fernkonfiguration erstellt und der Cisco Easy VPN-Fernkonfigurationsmodus aufgerufen.

Schritt 2	**group** *Gruppenname* **key** *Gruppenschlüssel*
	
	Beispiel:
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		Mit diesem Befehl werden die IPSec-Gruppe und der IPSec-Schlüsselwert für die VPN-Verbindung festgelegt.

Schritt 3	**peer** {*IP-Adresse* | *Hostname*}
	
	Beispiel:
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		Mit diesem Befehl wird die IP-Adresse oder der Hostname des Peers für die VPN-Verbindung angegeben.
		
		Hinweis Ein Hostname kann nur dann angegeben werden, wenn für den Router ein DNS-Server zur Hostnamenauflösung verfügbar ist.

Schritt 4	**mode** {**client** | **network-extension** | **network extension plus**}
	
	Beispiel:
	`Router(config-crypto-ezvpn)# mode client`
	`Router(config-crypto-ezvpn)#`
		Mit diesem Befehl wird der VPN-Betriebsmodus angegeben.

Schritt 5	**exit**
	
	Beispiel:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Schritt 6	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die Schnittstelle aufgerufen, auf die Sie die Cisco Easy VPN-Fernkonfiguration anwenden möchten.
		
		Hinweis Bei Routern mit einer ATM-WAN-Schnittstelle würde der Befehl **interface atm 0** lauten.

	Befehl oder Aktion	Zweck

Schritt 7	**crypto ipsec client ezvpn** *Name* [***outside*** | ***inside***]
	
	Beispiel:
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router (config-if)#`
		Mit diesem Befehl wird die Cisco Easy VPN-Fernkonfiguration der WAN-Schnittstelle zugewiesen. Daraufhin erstellt der Router automatisch die NAT- oder PAT-Konfiguration (Port Address Translation) und die Access-Listenkonfiguration, die für die VPN-Verbindung erforderlich sind.

Schritt 8	**exit**
	
	Beispiel:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Überprüfen der Easy VPN-Konfiguration

```
Router# show crypto ipsec client ezvpn

Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

Konfigurationsbeispiel

Im nachstehenden Konfigurationsbeispiel ist ein Auszug aus der Konfigurationsdatei für das VPN und den IPSec-Tunnel dargestellt, deren Konfiguration in diesem Kapitel beschrieben wurde.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
```

```
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!

interface fastethernet 4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

Konfigurieren von VPNs mit einem IPSec-Tunnel und Generic Routing Encapsulation

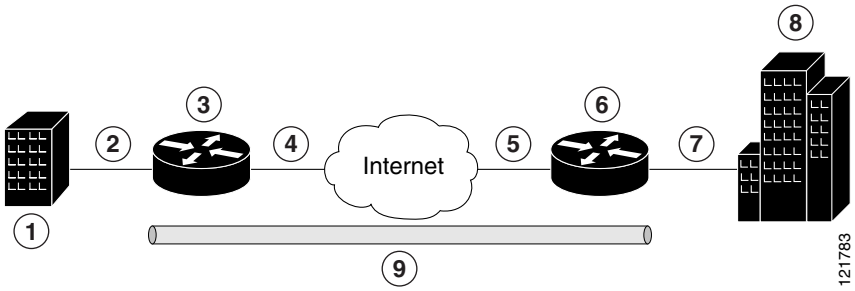
Die Router der Cisco 850-Serie und der Cisco 870-Serie unterstützen die Erstellung virtueller privater Netzwerke (VPNs).

Cisco-Router und andere Breitbandgeräte ermöglichen Hochgeschwindigkeitsverbindungen mit dem Internet. Für viele Anwendungen wird jedoch auch die Sicherheit von VPN-Verbindungen benötigt, die eine hohe Authentifizierungsstufe bieten und Daten zwischen zwei bestimmten Endpunkten verschlüsseln.

Zwei Typen von VPNs werden unterstützt: Standort-zu-Standort-VPN und Fernzugriff-VPN. Mit Standort-zu-Standort-VPNs können beispielsweise Zweigstellen mit Unternehmenszentralen verbunden werden. Über Fernzugriff-VPNs können sich entfernte Clients bei einem Unternehmensnetz anmelden und eine Verbindung mit dem Netz herstellen.

Durch das Beispiel in diesem Kapitel wird die Konfiguration eines Standort-zu-Standort-VPNs verdeutlicht, das mittels IPSec und mit dem GRE-Protokoll (Generic Routing Encapsulation) die Verbindung zwischen einer Zweigstelle und einem Unternehmensnetz sichert. In Abbildung 7-1 ist ein typisches Einsatzszenario dargestellt.

Abbildung 7-1 Standort-zu-Standort-VPN mit IPSec-Tunnel und GRE



1	Zweigstellenbüro mit mehreren LANs und VLANs
2	Fast-Ethernet-LAN-Schnittstelle – mit Adresse 192.165.0.0/16 (zugleich auch die innere Schnittstelle für NAT)
3	VPN-Client – Zugangsrouter der Cisco 850-Serie oder der Cisco 870-Serie
4	Fast-Ethernet- oder ATM-Schnittstelle – mit Adresse 200.1.1.1 (ebenfalls äußere Schnittstelle für NAT)

5	LAN-Schnittstelle – stellt Verbindung mit dem Internet her; Adresse der äußeren Schnittstelle: 210.110.101.1
6	VPN-Client – ein anderer Router, der den Zugang zum Unternehmensnetz kontrolliert
7	LAN-Schnittstelle – stellt Verbindung mit dem Unternehmensnetz her; Adresse der inneren Schnittstelle: 10.1.1.1
8	Netzwerk im Unternehmensbüro
9	IPSec-Tunnel mit GRE

GRE-Tunnel

GRE-Tunnel dienen in der Regel dazu, ein VPN zwischen dem Cisco-Router und einem entfernten Gerät herzustellen, das den Zugang zu einem Privatnetz, z. B. einem Unternehmensnetzwerk, kontrolliert. Durch den GRE-Tunnel weitergeleiteter Datenverkehr wird gekapselt und zur physischen Schnittstelle des Routers geroutet. Bei Verwendung einer GRE-Schnittstelle können der Cisco-Router und der Router, der den Zugang zum Unternehmensnetz kontrolliert, dynamische IP-Routingprotokolle unterstützen, um Routing-Updates über den Tunnel auszutauschen und IP-Multicast-Datenverkehr zu aktivieren. Beispielsweise werden folgende IP-Routingprotokolle unterstützt: EIGRP (Enhanced Interior Gateway Routing Protocol), RIP (Routing Information Protocol), IS-IS (Intermediate System-to-Intermediate System), OSPF (Open Shortest Path First) und BGP (Border Gateway Protocol).

Hinweis Bei Verwendung von IPSec (IP Security) mit GRE werden in der Access-Liste für die Verschlüsselung des Datenverkehrs das gewünschte Endnetzwerk und die gewünschten Endanwendungen nicht aufgeführt. Stattdessen verweist die Access-Liste auf die zugelassene Quelle und das zugelassene Ziel des GRE-Tunnels in ausgehender Richtung. Alle an den GRE-Tunnel weitergeleiteten Pakete werden verschlüsselt, sofern keine weiteren Zugriffssteuerungslisten (ACLs, Access Control Lists) auf die Tunnelschnittstelle angewendet werden.

VPNs

Die VPN-Konfigurationsdaten müssen jeweils an beiden Endpunkten konfiguriert werden, beispielsweise auf Ihrem Cisco-Router und beim entfernten Benutzer bzw. auf dem Cisco-Router und einem anderen Router. Sie müssen hierzu bestimmte Parameter festlegen, z. B. interne IP-Adressen, interne Subnetzmasken, DHCP-Serveradressen und Network Address Translation (NAT, Netzadress-Übersetzung).

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren eines VPN
- Konfigurieren eines GRE-Tunnels

Ein Konfigurationsbeispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 7-11.

Hinweis Bei den in diesem Kapitel beschriebenen Anleitungen wird davon ausgegangen, dass Sie die grundlegenden Routerfunktionen sowie PPPoE oder PPPoA mit NAT, DCHP und VLANs bereits konfiguriert haben. Falls Sie diese Konfigurationsschritte noch nicht ausgeführt haben, finden Sie die entsprechenden Informationen für Ihren Router in Kapitel 1, „Grundlegende Routerkonfiguration“, Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“, Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“, und Kapitel 5, „Konfigurieren eines LAN mit DHCP und VLANs“,.

Konfigurieren eines VPN

Führen Sie die folgenden Schritte aus, um ein VPN über einen IPSec-Tunnel zu konfigurieren:

- Konfigurieren der IKE-Richtlinie
- Konfigurieren von Gruppenrichtlinieninformationen
- Aktivieren des Richtlinien-Lookup
- Konfigurieren von IPSec-Transformationen und Protokollen
- Konfigurieren der IPSec-Verschlüsselungsmethode und -Parameter
- Anwenden der Crypto-Map auf die physische Schnittstelle

Konfigurieren der IKE-Richtlinie

Führen Sie die folgenden Schritte aus, um die IKE-Richtlinie (Internet Key Exchange) zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto isakmp policy** *Priorität*
	
	Beispiel:
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird eine IKE-Richtlinie erstellt, die während der IKE-Verhandlung verwendet wird. Die Priorität wird mit einer Zahl im Bereich von 1 bis 10000 definiert, wobei 1 die höchste Prioritätsstufe ist.
		
		Außerdem wird der Konfigurationsmodus für ISAKMP-Richtlinien (Internet Security Association Key and Management Protocol) aufgerufen.

Schritt 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	
	Beispiel:
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird der in der IKE-Richtlinie verwendete Verschlüsselungsalgorithmus angegeben.
		
		In diesem Beispiel wird der 168-Bit-Verschlüsselungsstandard Dreifach-DES (Triple Data Encryption Standard) verwendet.

Schritt 3	**hash** {**md5** | **sha**}
	
	Beispiel:
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird der Hash-Algorithmus festgelegt, der in der IKE-Richtlinie verwendet wird.
		
		In diesem Beispiel ist der Algorithmus MD5 (Message Digest 5) angegeben. Die Standardeinstellung ist SHA-1 (Secure Hash-Standard).

Schritt 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	
	Beispiel:
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		Mit diesem Befehl wird die Authentifizierungsmethode festgelegt, die in der IKE-Richtlinie verwendet wird.
		
		In diesem Beispiel wird eine Authentifizierung mit einem „Pre-Shared Key“ verwendet.

	Befehl oder Aktion	Zweck

Schritt 5	**group** {**1** | **2** | **5**}
	
	Beispiel:
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		Gibt an, dass ein Algorithmus der Diffie-Hellman-Gruppe in der IKE-Richtlinie verwendet werden soll.

Schritt 6	**lifetime** *Sekunden*
	
	Beispiel:
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		Gibt die Gültigkeitsdauer im Bereich von 60 bis 86400 Sekunden für eine IKE-Security-Association (SA) an.

Schritt 7	**exit**
	
	Beispiel:
	`Router(config-isakmp)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für IKE-Richtlinien beendet und der globale Konfigurationsmodus aufgerufen.

Konfigurieren von Gruppenrichtlinieninformationen

Führen Sie die folgenden Schritte aus, um die Gruppenrichtlinie zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	
	Beispiel:
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird eine IKE-Richtliniengruppe erstellt, in der Attribute enthalten sind, die auf den entfernten Client heruntergeladen werden sollen.
		
		Außerdem wird der Konfigurationsmodus für ISAKMP-Richtlinien (Internet Security Association Key Management Protocol) aufgerufen.

Schritt 2	**key** *Name*
	
	Beispiel:
	`Router(config-isakmp-group)# key secret-password`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird der IKE-Preshared-Key für die Gruppenrichtlinie angegeben.

Schritt 3	**dns** *primärer-Server*
	
	Beispiel:
	`Router(config-isakmp-group)# dns 10.50.10.1`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird der primäre DNS-Server (Domain Name Service) für die Gruppe angegeben.
		
		Hinweis Mit dem Befehl **wins** können Sie außerdem WINS-Server (Windows Internet Naming Service) für die Gruppe angeben.

	Befehl oder Aktion	Zweck

Schritt 4	**domain** *Name*
	
	Beispiel:
	`Router(config-isakmp-group)# domain company.com`
	`Router(config-isakmp-group)#`
		Mit diesem Befehl wird die Zugehörigkeit der Gruppe zu einer Domäne angegeben.

Schritt 5	**exit**
	
	Beispiel:
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für IKE-Gruppenrichtlinien beendet und der globale Konfigurationsmodus aufgerufen.

Schritt 6	**ip local pool** {**default** | *Poolname*} [*IP-Anfangsadresse* [*IP-Endadresse*]]
	
	Beispiel:
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		Mit diesem Befehl wird ein lokaler Adresspool für die Gruppe angegeben.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Aktivieren des Richtlinien-Lookup

Führen Sie die folgenden Schritte aus, um Richtlinien-Lookup über AAA zu aktivieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**aaa new-model**
	
	Beispiel:
	`Router(config)# aaa new-model`
	`Router(config)#`
		Mit diesem Befehl wird das AAA-Zugriffssteuerungsmodell aktiviert.

Schritt 2	**aaa authentication login** {**default** | *Listenname*} *Methode1* [*Methode2...*]
	
	Beispiel:
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		Mit diesem Befehl wird die AAA-Authentifizierung ausgewählter Benutzer bei der Anmeldung festgelegt und die verwendete Methode angegeben.
		
		In diesem Beispiel wird eine lokale Authentifizierungsdatenbank verwendet. Sie könnten hierfür auch einen RADIUS-Server verwenden. Genauere Informationen finden Sie im *Cisco IOS Security Configuration Guide* und in der *Cisco IOS Security Command Reference*.

	Befehl oder Aktion	Zweck

Schritt 3	**aaa authorization** {**network** | **exec** | **commands** *Ebene* | **reverse-access** | **configuration**} {**default** | *Listenname*} [*Methode1* [*Methode2...*]]
	
	Beispiel:
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		In diesem Schritt wird für alle netzwerkbezogenen Dienstanforderungen, einschließlich PPP, die AAA-Autorisierung sowie die hierfür verwendete Methode festgelegt.
		
		In diesem Beispiel wird eine lokale Autorisierungsdatenbank verwendet. Sie könnten hierfür auch einen RADIUS-Server verwenden. Genauere Informationen finden Sie im *Cisco IOS Security Configuration Guide* und in der *Cisco IOS Security Command Reference*.

Schritt 4	**username** *Name* {**nopassword** | **password** *Kennwort* | **password** *Verschlüsselungstyp verschlüsseltes-Kennwort*}
	
	Beispiel:
	`Router(config)# username cisco password 0 cisco`
	`Router(config)#`
		In diesem Schritt wird ein benutzernamenbasiertes Authentifizierungssystem eingerichtet.
		
		In diesem Beispiel wird der Benutzername *cisco* mit dem verschlüsselten Kennwort *cisco* implementiert.

Konfigurieren von IPSec-Transformationen und Protokollen

Ein Transformationssatz stellt eine bestimmte Kombination von Sicherheitsprotokollen und -algorithmen dar. Während der IKE-Verhandlung wird zwischen den Peers vereinbart, einen bestimmten Transformationssatz zum Schutz des Datenflusses zu verwenden.

Bei den IKE-Verhandlungen suchen die Peers in mehreren Transformationssätzen nach einer bei beiden Peers identischen Transformation. Wird ein derartiger Transformationssatz gefunden, wird er ausgewählt und auf den geschützten Datenverkehr als Bestandteil der Konfigurationen beider Peers angewendet.

Führen Sie die folgenden Schritte aus, um die IPSec-Transformationssätze und -Protokolle anzugeben (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto ipsec transform-set** *Transformationssatzname Transformation1* [*Transformation2*] [*Transformation3*] [*Transformation4*]
	
	Beispiel:
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		Mit diesem Befehl wird ein Transformationssatz, eine zulässige Kombination aus IPSec-Sicherheitsprotokollen und Algorithmen, definiert.
		
		Ausführliche Informationen zu gültigen Transformationen und Kombinationen finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 2	**crypto ipsec security-association lifetime** {**seconds** *Sekunden* | **kilobytes** *Kilobytes*}
	
	Beispiel:
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		Mit diesem Befehl werden die Werte für die globale Gültigkeitsdauer festgelegt, die bei der Verhandlung der IPSec-Security-Associations verwendet werden.
		
		Ausführliche Informationen finden Sie in der *Cisco IOS Security Command Reference*.

Hinweis Bei manuell eingerichteten Security-Associations erfolgt keine Verhandlung mit dem Peer, und beide Seiten müssen jeweils denselben Transformationssatz angeben.

Konfigurieren der IPSec-Verschlüsselungsmethode und -Parameter

Durch eine dynamische Crypto-Map-Richtlinie werden Verhandlungsanforderungen für neue Security-Associations von entfernten IPSec-Peers verarbeitet, selbst wenn der Router nicht alle Crypto-Map-Parameter kennt (z. B. die IP-Adresse).

Führen Sie die folgenden Schritte aus, um die IPSec-Verschlüsselungsmethode zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**crypto dynamic-map** *dynamischer-Map-Name dynamische-Seq-Num*
	
	Beispiel:
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		Mit diesem Befehl wird ein Eintrag für eine dynamische Crypto-Map erstellt und der Crypto-Map-Konfigurationsmodus aufgerufen.
		
		Ausführliche Informationen zu diesem Befehl finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 2	**set transform-set** *Transformationssatzname* [*Transformationssatzname2 ... Transformationssatzname6*]
	
	Beispiel:
	`Router(config-crypto-map)# set transform-set vpn1`
	`Router(config-crypto-map)#`
		Mit diesem Befehl wird festgelegt, welche Transformationssätze mit dem Crypto-Map-Eintrag verwendet werden können.

Schritt 3	**reverse-route**
	
	Beispiel:
	`Router(config-crypto-map)# reverse-route`
	`Router(config-crypto-map)#`
		Mit diesem Befehl werden Quellproxyinformationen für den Crypto-Map-Eintrag erstellt.
		
		Ausführliche Informationen finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 4	**exit**
	
	Beispiel:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 5	**crypto map** *Map-Name Seq-Num* [**ipsec-isakmp**] [**dynamic** *dynamischer-Map-Name*] [**discover**] [**profile** *Profilname*]
	
	Beispiel:
	`Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`
	`Router(config)#`
		Mit diesem Befehl wird ein Crypto-Map-Profil erstellt.

Anwenden der Crypto-Map auf die physische Schnittstelle

Die Crypto-Maps müssen auf jede einzelne Schnittstelle angewendet werden, über die IPSec-Datenverkehr fließt. Durch Anwendung der Crypto-Map auf die physische Schnittstelle wird der Router angewiesen, den gesamten Datenverkehr anhand der Security-Association-Datenbank zu evaluieren. Mit den Standardkonfigurationen bietet der Router eine sichere Konnektivität, da der zwischen den entfernten Standorten gesendete Datenverkehr verschlüsselt wird. Die öffentliche Schnittstelle gestattet jedoch auch die Durchleitung des übrigen Datenverkehrs und stellt eine Verbindung mit dem Internet bereit.

Führen Sie die folgenden Schritte aus, um eine Crypto-Map auf eine Schnittstelle anzuwenden (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die Schnittstelle aufgerufen, auf die Sie die Crypto-Map anwenden möchten.

Schritt 2	**crypto map** *Map-Name*
	
	Beispiel:
	`Router(config-if)# crypto map static-map`
	`Router (config-if)#`
		Mit diesem Befehl wird die Crypto-Map auf die Schnittstelle angewendet.
		
		Ausführliche Informationen zu diesem Befehl finden Sie in der *Cisco IOS Security Command Reference*.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Konfigurieren eines GRE-Tunnels

Führen Sie die folgenden Schritte aus, um einen GRE-Tunnel zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface tunnel 1`
	`Router (config-if)#`
		Mit diesem Befehl wird eine Tunnelschnittstelle erstellt und der Schnittstellen-Konfigurationsmodus aufgerufen.

Schritt 2	**ip address** *IP-Adresse Maske*
	
	Beispiel:
	`Router(config-if)# 10.62.1.193 255.255.255.252`
	`Router (config-if)#`
		Mit diesem Befehl wird dem Tunnel eine Adresse zugewiesen.

Schritt 3	**tunnel source** *Schnittstellentyp Nummer*
	
	Beispiel:
	`Router(config-if)# tunnel source fastethernet 0`
	`Router (config-if)#`
		Mit diesem Befehl wird der Quellen-Endpunkt des Routers für den GRE-Tunnel angegeben.

Schritt 4	**tunnel destination** *Standard-Gateway-IP-Adresse*
	
	Beispiel:
	`Router(config-if)# tunnel destination 192.168.101.1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Ziel-Endpunkt des Routers für den GRE-Tunnel angegeben.

Schritt 5	**crypto map** *Map-name*
	
	Beispiel:
	`Router(config-if)# crypto map static-map`
	`Router (config-if)#`
		Mit diesem Befehl wird dem Tunnel eine Crypto-Map zugewiesen.
		
		Hinweis Konnektivität zwischen den Standorten kann nur hergestellt werden, wenn dynamisches Routing oder statische Routen zu der Tunnelschnittstelle konfiguriert sind. Ausführliche Informationen finden Sie im *Cisco IOS Security Configuration Guide*.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus beendet und erneut der globale Konfigurationsmodus aufgerufen.

	Befehl oder Aktion	Zweck

Schritt 7	**ip access-list** {**standard** | **extended**} *Access-Listenname*
	
	Beispiel:
	`Router(config)# ip access-list extended vpnstatic1`
	`Router(config-acl)#`
		Mit diesem Befehl wird der ACL-Konfigurationsmodus für die benannte ACL aufgerufen, die von der Crypto-Map verwendet wird.

Schritt 8	**permit** *protocol Quelle Quellenplatzhalter Ziel Zielplatzhalter*
	
	Beispiel:
	`Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`
	`Router(config-acl)#`
		Mit diesem Befehl wird angegeben, dass nur GRE-Datenverkehr auf der ausgehenden Schnittstelle zulässig ist.

Schritt 9	**exit**
	
	Beispiel:
	`Router(config-acl)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Konfigurationsbeispiel

Im nachstehenden Konfigurationsbeispiel ist ein Auszug aus der entsprechenden Konfigurationsdatei für ein VPN-Szenario mit GRE-Tunnel aufgeführt, das in den vorhergehenden Abschnitten beschrieben wurde.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username cisco password 0 cisco
!
interface tunnel 1
    ip address 10.62.1.193 255.255.255.252

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
```

```
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Definiert die Schlüsselzuordnung und Authentifizierung für IPSec-Tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Definiert die Verschlüsselung und den Transformationssatz für den IPSec-Tunnel.
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
! Ordnet alle Crypto-Werte und die Peering-Adresse für den IPSec-Tunnel zu.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
! VLAN 1 ist das interne Heimnetz.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Prüfung untersucht ausgehenden Datenverkehr.
 crypto map static-map
 no cdp enable
!
! FE4 ist die äußere bzw. dem Internet zugewandte Schnittstelle.
interface fastethernet 4
 ip address 210.110.101.21 255.255.255.0
 ! ACL 103 ermöglicht IPSec-Datenverkehr vom Unternehmensrouter und
 ! sperrt den Zugang für aus dem Internet stammenden Datenverkehr.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Mit diesem Befehl wird der IPSec-Tunnel auf die äußere
Schnittstelle angewendet.
!
! Verwenden Sie NAT-Overload, um die
! vom ISP bereitgestellte einzelne Adresse optimal zu nutzen.
ip nat inside source list 102 interface Dialer0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
!
```

```
! ACL 102 zugeordnete Adressen werden für NAT verwendet.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
! ACL 103 definiert zulässigen Datenverkehr vom Peer für den IPSec-Tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! ICMP wird zum Debugging zugelassen, sollte jedoch aufgrund von Sicherheitsaspekten
! deaktiviert sein.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Verhindert eingehenden Datenverkehr, der im Internet
initiiert wurde.
! ACL 105 entspricht den Adressen für den IPSec-Tunnel zu bzw. vom Unternehmensnetz.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
```

Konfigurieren einer einfachen Firewall

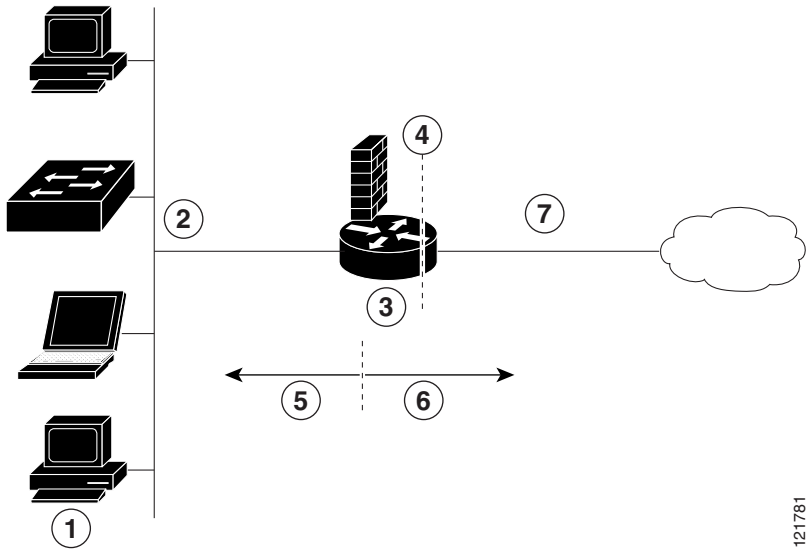
Die Router der Cisco 850-Serie und der Cisco 870-Serie unterstützen die Filterung von Netzwerkdatenverkehr mittels Access-Listen. Die Router bieten außerdem Unterstützung für die Paketprüfung und dynamische temporäre Access-Listen durch kontextbasierte Zugriffssteuerung (CBAC, Context-Based Access Control).

Die grundlegende Datenverkehrsfilterung beschränkt sich auf konfigurierte Access-Listenimplementierungen, durch die Pakete auf der Netzwerkschicht oder bestenfalls in der Transportschicht untersucht werden, wobei dann die Durchleitung der einzelnen Pakete durch die Firewall gestattet oder verweigert wird. Die Verwendung von Prüfregeln in CBAC ermöglicht jedoch die Erstellung und Nutzung dynamischer temporärer Access-Listen. Mit diesen dynamischen Listen können temporäre Öffnungen in den konfigurierten Access-Listen an Firewall-Schnittstellen geschaffen werden. Diese Öffnungen werden erstellt, wenn Datenverkehr für eine festgelegte Benutzersitzung das interne Netzwerk durch die Firewall verlässt. Durch die Öffnungen wird dem zurückkehrenden Datenverkehr (der normalerweise blockiert worden wäre) für die festgelegte Sitzung die Durchleitung durch die Firewall gestattet.

Ausführlichere Informationen zur Filterung von Datenverkehr und zu Firewalls finden Sie im *Cisco IOS Security Configuration Guide, Release 12.3*.

In Abbildung 8-1 ist ein Netzwerkszenario dargestellt, bei dem PPPoE bzw. PPPoA mit NAT und einer Firewall verwendet wird.

Abbildung 8-1 Router mit konfigurierter Firewall



1	Mehrere vernetzte Geräte – Desktop- und Laptop-PCs, Switches
2	Fast-Ethernet-LAN-Schnittstelle (die innere Schnittstelle für NAT)
3	PPPoE- oder PPPoA-Client-und-Firewall-Implementierung – Zugangsrouter der Cisco 851/871-Serie oder der Cisco 857/876/877/878-Serie
4	Punkt, an dem NAT erfolgt
5	Geschütztes Netzwerk
6	Ungeschütztes Netzwerk
7	Fast-Ethernet- oder ATM-WAN-Schnittstelle (äußere Schnittstelle für NAT)

Im folgenden Konfigurationsbeispiel wird die Firewall auf die äußere WAN-Schnittstelle (FE4) auf dem Cisco 851 oder Cisco 871 angewendet. Die Firewall schützt das Fast-Ethernet-LAN auf FE0 durch Filterung und Prüfung des gesamten Datenverkehrs, der an der Fast-Ethernet-WAN-Schnittstelle FE4 in den Router eintritt. Beachten Sie, dass in diesem Beispiel der aus dem Unternehmensnetz mit der Netzwerkadresse 10.1.1.0 stammende Netzwerkdatenverkehr als sicher angesehen und somit nicht gefiltert wird.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren von Access-Listen
- Konfigurieren von Prüfregeln
- Anwenden von Access-Listen und Prüfregeln auf Schnittstellen

Ein Konfigurationsbeispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 8-5.

Hinweis Bei den in diesem Kapitel beschriebenen Anleitungen wird davon ausgegangen, dass Sie die grundlegenden Routerfunktionen sowie PPPoE oder PPPoA mit NAT bereits konfiguriert haben. Falls Sie diese Konfigurationsschritte noch nicht ausgeführt haben, finden Sie die entsprechenden Informationen für Ihren Router in Kapitel 1, „Grundlegende Routerkonfiguration“,, Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“, und Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“. Möglicherweise haben Sie außerdem DHCP, VLANs und sichere Tunnel konfiguriert.

Konfigurieren von Access-Listen

Führen Sie die folgenden Schritte aus, um Access-Listen für die Firewall zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**access-list** *Access-Listenummer* {**deny** | **permit**} *Protokoll Quelle Quellenplatzhalter* [**operator** [*Port*]] *Ziel*
	
	Beispiel:
	`Router(config)# access-list 103 deny ip any any`
	`Router(config)# access-list 103 permit host 200.1.1.1 eq isakmp any`
	`Router(config)#`
		Mit diesem Befehl wird eine Access-Liste erstellt, die verhindert, dass aus dem Internet stammender Datenverkehr das lokale (innere) Netzwerk des Routers erreicht, und die die Quell- und Zielports miteinander vergleicht.
		
		Ausführliche Informationen finden Sie in der *Cisco IOS IP Command Reference, Band 1 von 4: Addressing and Services*.

Schritt 2	**access-list** *Access-Listennummer* {**deny** | **permit**} *Protokoll Quelle Quellenplatzhalter Ziel Zielplatzhalter*
	
	Beispiel:
	`Router(config)# access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255`
	`Router(config)#`
		Mit diesem Befehl wird eine Access-Liste erstellt, die die freie Durchleitung von Netzwerkdatenverkehr zwischen dem Unternehmensnetz und den lokalen Netzwerken über den konfigurierten VPN-Tunnel gestattet.

Konfigurieren von Prüfregeln

Führen Sie die folgenden Schritte aus, um Firewall-Prüfregeln für den gesamten TCP- und UDP-Datenverkehr zu konfigurieren und spezielle Anwendungsprotokolle gemäß Definition durch die Sicherheitsrichtlinie festzulegen (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**ip inspect name** *Prüfungsname Protokoll*
	
	Beispiel:
	`Router(config)# ip inspect name firewall tcp`
	`Router(config)#`
		Mit diesem Befehl wird eine Prüfregel für ein bestimmtes Protokoll definiert.

Schritt 2	**ip inspect name** *Prüfungsname Protokoll*
	
	Beispiel:
	`Router(config)# ip inspect name firewall rtsp`
	`Router(config)# ip inspect name firewall h323`
	`Router(config)# ip inspect name firewall netshow`
	`Router(config)# ip inspect name firewall ftp`
	`Router(config)# ip inspect name firewall sqlnet`
	`Router(config)#`
		Führen Sie diesen Befehl für jede zu verwendende Prüfregel erneut aus.

Anwenden von Access-Listen und Prüfregeln auf Schnittstellen

Führen Sie die folgenden Schritte aus, um die Access-Listen und Prüfregeln auf die Netzwerkschnittstellen anzuwenden (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface vlan 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die innere Netzwerkschnittstelle des Routers aufgerufen.

Schritt 2	**ip inspect** *Prüfungsname* {***in*** | ***out***}
	
	Beispiel:
	`Router(config-if)# ip inspect firewall in`
	`Router (config-if)#`
		Mit diesem Befehl wird die Gruppe der Firewall-Prüfregeln auf die innere Schnittstelle des Routers angewendet.

	Befehl	Zweck

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Schritt 4	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface fastethernet 4`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die äußere Netzwerkschnittstelle des Routers aufgerufen.

Schritt 5	**ip access-group** {*Access-Listennummer* | *Access-Listenname*}{**in** | **out**}
	
	Beispiel:
	`Router(config-if)# ip access-group 103 in`
	`Router (config-if)#`
		Mit diesem Befehl werden die definierten Access-Listen der äußeren Schnittstelle des Routers zugewiesen.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird wieder der globale Konfigurationsmodus aufgerufen.

Konfigurationsbeispiel

Einem Telearbeiter wird mit IPSec-Tunneling ein sicherer Zugang zu einem Unternehmensnetz gewährt. Sicherheit für das Heimnetzwerk wird durch die Firewall-Prüfung gewährleistet. Die zulässigen Protokolle sind TCP, UDP, RTSP, H.323, NetShow, FTP und SQLNet. Es befinden sich keine Server im Heimnetzwerk. Daher wird auch kein von außen initiierter Datenverkehr zugelassen. Mit IPSec-Tunneling wird die Verbindung des Heim-LANs mit dem Unternehmensnetzwerk gesichert.

Wie bei der Internet-Firewall-Richtlinie muss HTTP nicht angegeben werden, da eine Java-Blockierung nicht notwendig ist. Durch Angabe der TCP-Prüfung können Einkanalprotokolle, z. B. Telnet und HTTP, verwendet werden. UDP wird für DNS festgelegt.

In dem nachstehenden Konfigurationsbeispiel ist ein Teil der Konfigurationsdatei für das einfache Firewall-Szenario aufgeführt, das in den vorhergehenden Abschnitten beschrieben wurde.

```
!
! Firewallüberprüfung für jeglichen TCP- und UDP-Verkehr und
! spezielle Anwendungsprotokolle gemäß der Definition durch die Sicherheitsrichtlinie
! eingerichtet.
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
```

```
interface vlan 1 ! Dies ist das interne Netzwerk.
ip inspect firewall in ! Prüfung untersucht ausgehenden Datenverkehr.
    no cdp enable
!
interface fastethernet 4! FE4 ist die äußere bzw. dem Internet zugewandte Schnittstelle.
! ACL 103 ermöglicht IPSec-Datenverkehr vom Unternehmensrouter
! und sperrt den Zugang für aus dem Internet stammenden Datenverkehr.
ip access-group 103 in
    ip nat outside
    no cdp enable
!
! ACL 103 definiert zulässigen Datenverkehr vom Peer für den IPSec-Tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! ICMP wird zum Debugging zugelassen, sollte jedoch aufgrund von Sicherheitsaspekten
! deaktiviert sein.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Verhindert eingehenden Datenverkehr, der im Internet
! initiiert wurde.
! ACL 105 entspricht den Adressen für den IPSec-Tunnel zu bzw. vom Unternehmensnetz.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
!
```

Konfigurieren einer Wireless-LAN-Verbindung

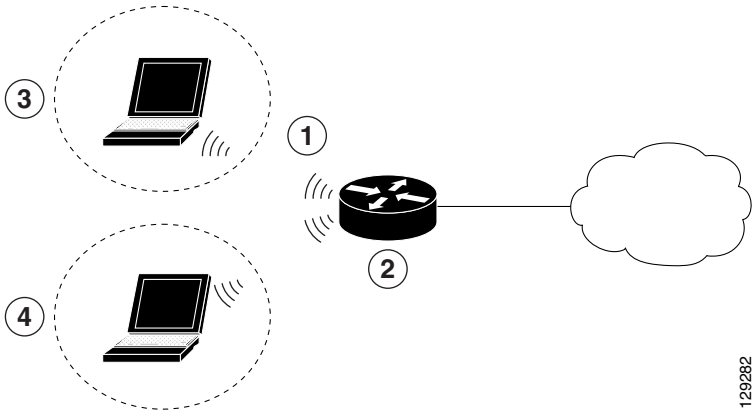
Die Router der Cisco 850-Serie und der Cisco 870-Serie unterstützen eine sichere, kostengünstige und benutzerfreundliche Wireless-LAN-Lösung, durch die Mobilität und Flexibilität mit den leistungsfähigen Funktionen verbunden werden, die für Netzwerkadministratoren unabdingbar sind. Mit einem auf der Cisco IOS-Software basierenden Verwaltungssystem fungieren Cisco-Router als Zugangspunkte und stellen Wi-Fi-zertifizierte, IEEE 802.11a/b/g-konforme Wireless-LAN-Transceiver dar.

Sie können die Router mit einer Befehlszeilenschnittstelle, der so genannten Command Line Interface (CLI), oder einem browserbasierten Verwaltungssystem bzw. per SNMP (Simple Network Management Protocol) konfigurieren und überwachen. In diesem Kapitel wird beschrieben, wie Sie den Router mit der CLI konfigurieren können. Geben Sie im globalen Konfigurationsmodus den CLI-Befehl **interface dot11radio** ein, um das Gerät in den Funkkonfigurationsmodus zu schalten.

Ausführliche Informationen zum Konfigurieren dieser Cisco-Router in einer Wireless-LAN-Anwendung finden Sie im *Cisco Access Router Wireless Configuration Guide*.

In Abbildung 9-1 ist ein Einsatzszenario in einem Wireless (drahtlosen) Netzwerk dargestellt.

Abbildung 9-1 Wireless (drahtlose) Verbindung zum Cisco-Router



1	Wireless-LAN (mit mehreren vernetzten Geräten)
2	Zugangsrouter der Cisco 850-Serie oder der Cisco 870-Serie, verbunden mit dem Internet
3	VLAN 1
4	VLAN 2

Im folgenden Konfigurationsbeispiel greift ein entfernter Benutzer über eine drahtlose Verbindung auf den Zugangsrouter der Cisco 850-Serie oder der Cisco 870-Serie zu. Jeder entfernte Benutzer verfügt jeweils über ein eigenes VLAN.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um dieses Netzwerkszenario zu konfigurieren:

- Konfigurieren der Basisfunkstation
- Konfigurieren von Bridging in VLANs
- Konfigurieren von Funkstation-Subschnittstellen

Ein Konfigurationsbeispiel, bei dem die Ergebnisse dieser Konfigurationsaufgaben verdeutlicht werden, finden Sie unter „Konfigurationsbeispiel“ auf Seite 9-7.

Hinweis Bei den in diesem Kapitel beschriebenen Anleitungen wird davon ausgegangen, dass Sie die grundlegenden Routerfunktionen sowie PPPoE oder PPPoA mit NAT bereits konfiguriert haben. Falls Sie diese Konfigurationsschritte noch nicht ausgeführt haben, finden Sie die entsprechenden Informationen für Ihren Router in Kapitel 1, „Grundlegende Routerkonfiguration“,, Kapitel 3, „Konfigurieren von PPP über Ethernet mit NAT“, und Kapitel 4, „Konfigurieren von PPP über ATM mit NAT“. Möglicherweise haben Sie außerdem DHCP, VLANs und sichere Tunnel konfiguriert.

Konfigurieren der Basisfunkstation

Führen Sie die folgenden Schritte aus, um die Basisfunkstation für ein Wireless-LAN zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Name Nummer*
	
	Beispiel:
	`Router(config)# interface dot11radio 0`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die Funkschnittstelle aufgerufen.

Schritt 2	**broadcast-key** [**vlan** *VLAN-ID*] **change** *Sekunden*
	
	Beispiel:
	`Router(config-if)# broadcast-key vlan 1 change 45`
	`Router (config-if)#`
		Mit diesem Befehl wird das Intervall in Sekunden festgelegt, das jeweils den Zeitraum zwischen dem Wechsel des Broadcast-Verschlüsselungsschlüssels angibt, der für Clients verwendet wird.
		
		Hinweis Clientgeräte, die statisches WEP (Wired Equivalent Privacy) verwenden, können den Zugangspunkt nicht nutzen, wenn Sie den Wechsel der Broadcast-Schlüssel aktivieren – der Zugangspunkt ist dann nur für Clientgeräte mit Funkmodul mit 802.1x-Authentifizierung (z. B. Light Extensible Authentication Protocol [LEAP], Extensible Authentication Protocol-Transport Layer Security [EAP-TLS] oder Protected Extensible Authentication Protocol [PEAP]) nutzbar.
		
		Hinweis Dieser Befehl wird auf Bridges nicht unterstützt.
		
		Weitere Informationen finden Sie unter *Cisco IOS Commands for Access Points and Bridges*.

Schritt 3	**encryption** *Methode Algorithmus Schlüssel*
	
	Beispiel:
	`Router(config-if)# encryption vlan 1 mode ciphers tkip`
	`Router (config-if)#`
		Mit diesem Befehl werden die Verschlüsselungsmethode sowie der Verschlüsselungsalgorithmus und der Schlüssel für den Zugang zur drahtlosen Schnittstelle angegeben.
		
		In diesem Beispiel wird das VLAN mit der optionalen Verschlüsselungsmethode „Data Ciphers“ verwendet.

	Befehl	Zweck

Schritt 4	**ssid** *Name*
	
	Beispiel:
	`Router(config-if)# ssid cisco`
	`Router(config-if-ssid)#`
		Mit diesem Befehl wird eine Serversatz-ID (SSID), der öffentliche Name eines drahtlosen Netzwerks, erstellt.
		
		Hinweis Sämtliche Geräte mit Funkmodul in einem WLAN müssen dieselbe SSID verwenden, um miteinander kommunizieren zu können.

Schritt 5	**vlan** *Nummer*
	
	Beispiel:
	`Router(config-if-ssid)# vlan 1`
	`Router(config-if-ssid)#`
		Mit diesem Befehl wird die SSID an ein VLAN gebunden.

Schritt 6	**authentication** *Typ*
	
	Beispiel:
	`Router(config-if-ssid)# authentication open`
	`Router(config-if-ssid)# authentication network-eap eap_methods`
	`Router(config-if-ssid)# authentication key-management wpa`
		Mit diesem Befehl werden die zugelassenen Authentifizierungsmethoden für Benutzer festgelegt, die versuchen, auf das Wireless-LAN zuzugreifen.
		
		Wie im Beispiel dargestellt, können auch mehrere Methoden angegeben werden.

Schritt 7	**exit**
	
	Beispiel:
	`Router(config-if-ssid)# exit`
	`Router (config-if)#`
		Mit diesem Befehl wird der SSID-Konfigurationsmodus beendet und der Schnittstellen-Konfigurationsmodus für die Funkschnittstelle aufgerufen.

Schritt 8	**speed** *Rate*
	
	Beispiel:
	`Router(config-if)# basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0`
	`Router (config-if)#`
		(Optional) Mit diesem Befehl werden die erforderlichen und zulässigen Datenraten in Mbit/s für Datenverkehr angegeben, der über die drahtlose Verbindung übertragen wird.

Schritt 9	**rts** [**retries** | **threshold**]
	
	Beispiel:
	`Router(config-if)# rts threshold 2312`
	`Router (config-if)#`
		(Optional) Mit diesem Befehl wird ein RTS-Schwellenwert (Request to Send, Sendeanforderung) oder die Anzahl der Sendeversuche für eine Anforderung festgelegt. Wenn dieser Schwellenwert erreicht ist bzw. diese Sendeversuche nicht erfolgreich sind, gilt ein Wireless-LAN als nicht erreichbar.

	Befehl	Zweck

Schritt 10	**power** [**client** | **local**] [**cck** [*Nummer* | **maximum**] | **ofdm** [*Nummer* | **maximum**]]
	
	Beispiel:
	`Router(config-if)# power local cck 50`
	`Router(config-if)# power local ofdm 30`
	`Router (config-if)#`
		(Optional) Mit diesem Befehl wird die Leistungsstufe des Funksenders angegeben.
		
		Informationen zu den verfügbaren Leistungsstufenwerten finden Sie im *Cisco Access Router Wireless Configuration Guide*.

Schritt 11	**channel** [*Nummer* | **least-congested**]
	
	Beispiel:
	`Router(config-if)# channel 2462`
	`Router (config-if)#`
		(Optional) Mit diesem Befehl wird der Kommunikationskanal angegeben.
		
		Informationen zu den verfügbaren Kanalnummern finden Sie im *Cisco Access Router Wireless Configuration Guide*.

Schritt 12	**station-role** [**repeater** | **root**]
	
	Beispiel:
	`Router(config-if)# station-role root`
	`Router (config-if)#`
		(Optional) Mit diesem Befehl wird die Rolle dieser Funkschnittstelle angegeben.
		
		Sie müssen mindestens eine Root-Schnittstelle angeben.

Schritt 13	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus beendet und der globale Konfigurationsmodus aufgerufen.

Konfigurieren von Bridging in VLANs

Führen Sie die folgenden Schritte aus, um integriertes Routing und Bridging in VLANs zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl oder Aktion	Zweck

Schritt 1	**bridge** [*Nummer* | **crb** | **irb** |**mac-address-table**]
	
	Beispiel:
	`Router(config)# bridge irb`
	`Router(config)#`
		Mit diesem Befehl wird der Bridging-Typ angegeben.
		
		In diesem Beispiel wird integriertes Routing und Bridging verwendet.

Schritt 2	**interface** *Name Nummer*
	
	Beispiel:
	`Router(config)# interface vlan 1`
	`Router(config)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus aufgerufen.
		
		Da in unserem Fall Bridging in den VLANs eingerichtet werden soll, wird im Beispiel der VLAN-Schnittstellen-Konfigurationsmodus aufgerufen.

	Befehl oder Aktion	Zweck

Schritt 3	**bridge-group** *Nummer*
	
	Beispiel:
	`Router(config)# bridge-group 1`
	`Router(config)#`
		Mit diesem Befehl wird der Schnittstelle eine Bridge-Gruppe zugewiesen.

Schritt 4	**bridge-group** *Parameter*
	
	Beispiel:
	`Router(config)# bridge-group spanning-disabled`
	`Router(config)#`
		Mit diesem Befehl werden andere Parameter für die Bridging-Schnittstelle festgelegt.

Schritt 5	**interface** *Name Nummer*
	
	Beispiel:
	`Router(config)# interface bvi 1`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die virtuelle Bridge-Schnittstelle aufgerufen.

Schritt 6	**ip address** *Adresse Maske*
	
	Beispiel:
	`Router(config)# ip address 10.0.1.1 255.255.255.0`
	`Router(config)#`
		Mit diesem Befehl wird die Adresse für die virtuelle Bridge-Schnittstelle angegeben.

Wiederholen Sie Schritt 2 bis Schritt 6 für jedes VLAN, das eine drahtlose Schnittstelle benötigt.

Konfigurieren von Funkstation-Subschnittstellen

Führen Sie die folgenden Schritte aus, um Subschnittstellen für jede Basisstation zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface dot11radio 0,1`
	`Router(config-subif)#`
		Mit diesem Befehl wird der Subschnittstellen-Konfigurationsmodus für die Schnittstelle der Basisstation aufgerufen.

Schritt 2	**description** *Zeichenfolge*
	
	Beispiel:
	`Router(config-subif)# description Cisco open`
	`Router(config-subif)#`
		Mit diesem Befehl wird eine Beschreibung der Subschnittstelle für den administrativen Benutzer angegeben.

	Befehl	Zweck

Schritt 3	**encapsulation dot1q** *vlanID* [**native** | **second-dot1q**]
	
	Beispiel:
	`Router(config-subif)# encapsulation dot1q 1 native`
	`Router(config-subif)#`
		Mit diesem Befehl wird angegeben, dass IEEE 802.1Q (Dot1Q)-Kapselung auf der betreffenden Subschnittstelle verwendet wird.

Schritt 4	**no cdp enable**
	
	Beispiel:
	`Router(config-subif)# no cdp enable`
	`Router(config-subif)#`
		Mit diesem Befehl wird CDP (Cisco Discovery Protocol) auf der drahtlosen Schnittstelle deaktiviert.

Schritt 5	**bridge-group** *Nummer*
	
	Beispiel:
	`Router(config-subif)# bridge-group 1`
	`Router(config-subif)#`
		Mit diesem Befehl wird der Subschnittstelle eine Bridge-Gruppe zugewiesen.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-subif)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Subschnittstellen-Konfigurationsmodus beendet und der globale Konfigurationsmodus aufgerufen.

Wiederholen Sie ggf. diese Schritte, um weitere Subschnittstellen zu konfigurieren.

Konfigurationsbeispiel

Im nachstehenden Konfigurationsbeispiel ist ein Auszug aus der Konfigurationsdatei für das Wireless-LAN-Szenario dargestellt, das in den vorhergehenden Abschnitten beschrieben wurde.

```
!
bridge irb
!
interface Dot11Radio0
 no ip address
 !
 broadcast-key vlan 1 change 45
 !
 !
 encryption vlan 1 mode ciphers tkip
 !
 ssid cisco
    vlan 1
    authentication open
    authentication network-eap eap_methods
    authentication key-management wpa
 !
```

```
 ssid ciscowep
    vlan 2
    authentication open
 !
 ssid ciscowpa
    vlan 3
    authentication open
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 2312
 power local cck 50
 power local ofdm 30
 channel 2462
 station-role root
!
interface Dot11Radio0.1
 description Cisco Open
 encapsulation dot1Q 1 native
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 spanning-disabled
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 spanning-disabled
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface Vlan1
 no ip address
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Vlan2
 no ip address
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Vlan3
 no ip address
 bridge-group 3
 bridge-group 3 spanning-disabled
!
interface BVI1
 ip address 10.0.1.1 255.255.255.0
!
```

```
interface BVI2
 ip address 10.0.2.1 255.255.255.0
!
interface BVI3
 ip address 10.0.3.1 255.255.255.0
!
```

Beispielkonfiguration

In diesem Kapitel sind die Ergebnisse der Konfiguration der Ethernet-WAN-, DHCP-, VLAN-, Easy VPN-Schnittstelle sowie der Wireless-Schnittstelle zusammengefasst, die in den vorherigen Kapiteln vorgenommen wurde. So können Sie sich anhand von Beispiel 10-1 in übersichtlicher Form mit der Grundkonfiguration des Routers vertraut machen, die in diesem Handbuch beschrieben wird.

Hinweis Durch „(**default**)“ gekennzeichnete Befehle werden jeweils automatisch generiert, sobald Sie den Befehl **show running-config** ausführen.

Beispiel 10-1 Beispielkonfiguration

```
Router# show running-config
Building configuration...

Current configuration : 3781 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname retail
!
boot-start-marker
boot-end-marker
!
enable password cisco123
!
username jsomeone password 0 cg6#107X
aaa new-model
!
aaa group server radius rad_eap
    server 10.0.1.1 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
ip subnet-zero
ip cef
!
vpdn enable
    vpdn-group 1
    request-dialin
    protocol pppoe
!
```

```
interface dialer 1
    ip address negotiated
    ppp authentication chap
    dialer pool 1
    dialer-group 1
!
dialer-list 1 protocol ip permit
    ip nat inside source list 1 interface dialer 0 overload
    ip classless (default)
    ip route 10.10.25.2 0.255.255.255 dialer 0
!
ip dhcp excluded-address 10.0.1.1 10.0.1.10
ip dhcp excluded-address 10.0.2.1 10.0.2.10
ip dhcp excluded-address 10.0.3.1 10.0.3.10
!
ip dhcp pool vlan1
   network 10.0.1.0 255.255.255.0
   default-router 10.0.1.1
!
ip dhcp pool vlan2
   network 10.0.2.0 255.255.255.0
   default-router 10.0.2.1
!
ip dhcp pool vlan3
   network 10.0.3.0 255.255.255.0
   default-router 10.0.3.1
!
ip ips po max-events 100
no ftp-server write-enable
!
bridge irb
!
interface FastEthernet0
    no ip address
!
interface FastEthernet1
    no ip address
!
interface FastEthernet2
    no ip address
!
interface FastEthernet3
    switchport mode trunk
    no ip address
!
interface FastEthernet4
    ip address 192.168.12.2 255.255.255.0
    no ip directed-broadcast (default)
    speed auto
    ip nat outside
    ip access-group 103 in
    no cdp enable
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
```

```
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!
interface Dot11Radio0
    no ip address
    !
    broadcast-key vlan 1 change 45
    !
    encryption vlan 1 mode ciphers tkip
    !
    ssid cisco
        vlan 1
        authentication open
        authentication network-eap eap_methods
        authentication key-management wpa optional
    !
    ssid ciscowep
        vlan 2
        authentication open
        !
    ssid ciscowpa
        vlan 3
        authentication open
    !
    speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
    rts threshold 2312
    power local cck 50
    power local ofdm 30
    channel 2462
    station-role root
!
interface Dot11Radio0.1
    description Cisco Open
    encapsulation dot1Q 1 native
    no cdp enable
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 spanning-disabled
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
!
```

```
interface Dot11Radio0.2
    encapsulation dot1Q 2
    bridge-group 2
    bridge-group 2 subscriber-loop-control
    bridge-group 2 spanning-disabled
    bridge-group 2 block-unknown-source
    no bridge-group 2 source-learning
    no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
    encapsulation dot1Q 3
    bridge-group 3
    bridge-group 3 subscriber-loop-control
    bridge-group 3 spanning-disabled
    bridge-group 3 block-unknown-source
    no bridge-group 3 source-learning
    no bridge-group 3 unicast-flooding
!
interface Vlan1
    ip address 192.168.1.1 255.255.255.0
    no ip directed-broadcast (default)
    ip nat inside
    crypto ipsec client ezvpn ezvpnclient inside
    ip inspect firewall in
    no cdp enable
    bridge-group 1
    bridge-group 1 spanning-disabled
!
interface Vlan2
    no ip address
    bridge-group 2
    bridge-group 2 spanning-disabled
!
interface Vlan3
    no ip address
    bridge-group 3
    bridge-group 3 spanning-disabled
!
interface BVI1
    ip address 10.0.1.1 255.255.255.0
!
interface BVI2
    ip address 10.0.2.1 255.255.255.0
!
interface BVI3
    ip address 10.0.3.1 255.255.255.0
!
ip classless
!
ip http server
no ip http secure-server
!
radius-server local
    nas 10.0.1.1 key 0 cisco123
    group rad_eap
!
user jsomeone nthash 7 0529575803696F2C492143375828267C7A760E1113734624452725707C010B065B
user AMER\jsomeone nthash 7
0224550C29232E041C6A5D3C5633305D5D560C09027966167137233026580E0B0D
!
radius-server host 10.0.1.1 auth-port 1812 acct-port 1813 key cisco123
!
control-plane
!
```

```
bridge 1 route ip
bridge 2 route ip
bridge 3 route ip
!
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
access-list 103 permit icmp any any
access-list 103 deny ip any any
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
!
line con 0
    password cisco123
    no modem enable
    transport preferred all
    transport output all
line aux 0
    transport preferred all
    transport output all
line vty 0 4
    password cisco123
    transport preferred all
    transport input all
    transport output all
!
```

Teil 3

Konfigurieren zusätzlicher Funktionen und Fehlerbehebung

Weitere Konfigurationsoptionen

In diesem Teil des Software-Konfigurationshandbuchs werden zusätzliche Konfigurationsmöglichkeiten und Tipps zur Fehlerbehebung für Router der Cisco 850-Serie (Cisco 851 und Cisco 857) sowie Router der Cisco 870-Serie (Cisco 871, Cisco 876, Cisco 877 und Cisco 878) beschrieben.

Folgende Konfigurationsoptionen werden in diesem Teil des Handbuchs erläutert:

- Kapitel 12, „Konfigurieren von Sicherheitsfunktionen“
- Kapitel 13, „Konfigurieren von Reserve-Wählleitung und Remoteverwaltung“
- Kapitel 14, „Fehlerbehebung“

Die in diesen Kapiteln enthaltenen Beschreibungen behandeln nicht alle Konfigurationsfragen oder Hinweise zur Fehlersuche. Weitere Informationen finden Sie in den entsprechenden Konfigurationshandbüchern und Befehlsreferenzen der Cisco IOS-Software.

Hinweis Wenn Sie überprüfen möchten, ob eine bestimmte Funktion mit Ihrem Router kompatibel ist, verwenden Sie das Software Advisor-Tool. Sie können auf dieses Tool unter www.cisco.com **> Technical Support & Documentation > Tools & Resources** mit Ihrem Cisco-Benutzernamen und dem entsprechenden Kennwort zugreifen.

Konfigurieren von Sicherheitsfunktionen

In diesem Kapitel erhalten Sie einen Überblick über Authentifizierung, Autorisierung und Abrechnung (AAA), den grundlegenden Funktionalitätsrahmen von Cisco für die Implementierung ausgewählter Sicherheitsfunktionen, die auf den Zugangsroutern der Cisco 850-Serie und Cisco 870-Serie konfiguriert werden können.

Hinweis Unter Umständen wird von einzelnen Routermodellen nicht jede in diesem Handbuch beschriebene Funktion unterstützt. Funktionen, die von einem bestimmten Routermodell nicht unterstützt werden, wurden daher nach Möglichkeit gekennzeichnet.

Dieses Kapitel ist in folgende Abschnitte unterteilt:

- Authentifizierung, Autorisierung und Abrechnung (AAA)
- Konfigurieren von AutoSecure
- Konfigurieren von Access-Listen
- Konfigurieren einer CBAC-Firewall
- Konfigurieren des Cisco IOS Firewall-IDS
- Konfigurieren von VPNs

Jeder Abschnitt enthält ein Konfigurationsbeispiel und ggf. Schritte zur Überprüfung.

Authentifizierung, Autorisierung und Abrechnung (AAA)

AAA-Netzwerksicherheitsdienste stellen die primäre Grundlage für die Einrichtung der Zugriffssteuerung auf dem Router dar. Die Authentifizierung bietet eine Methode zur Identifizierung von Benutzern, z. B. Anmelde- und Kennwortdialog, Abfrage und Antwort, Messaging-Unterstützung sowie in Abhängigkeit vom gewählten Sicherheitsprotokoll die Verschlüsselung. Die Autorisierung ermöglicht eine Fernzugriffssteuerung, einschließlich folgender Funktionen: einmalige Autorisierung oder Autorisierung für jeden einzelnen Dienst, benutzerbasierte Kontoliste und Profil, Unterstützung von Benutzergruppen, IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA) und Telnet. Die Abrechnungsfunktion bietet eine Methode zum Erfassen und Senden von Sicherheitsserverinformationen, die für Rechnungsstellungs-, Prüfungs- und Berichterstellungszwecke verwendet werden, z. B. Benutzeridentitäten, Start- und Stoppzeiten, ausgeführte Befehle (z. B. PPP), Anzahl der Pakete und Anzahl der Bytes.

AAA verwendet Protokolle wie RADIUS, TACACS+ oder Kerberos zur Verwaltung von Sicherheitsfunktionen. Falls Ihr Router als Netzzugangsserver fungiert, wird die Kommunikation zwischen dem Netzzugangsserver und dem RADIUS-, TACACS+- oder Kerberos-Sicherheitsserver über AAA hergestellt.

Informationen zum Konfigurieren von AAA-Diensten und den unterstützten Sicherheitsprotokollen finden Sie in folgenden Abschnitten des *Cisco IOS Security Configuration Guide*:

- Konfigurieren der Authentifizierung
- Konfigurieren der Autorisierung
- Konfigurieren der Abrechnung
- Konfigurieren von RADIUS
- Konfigurieren von TACACS+
- Konfigurieren von Kerberos

Konfigurieren von AutoSecure

Durch die AutoSecure-Funktion werden allgemeine IP-Dienste deaktiviert, die bei Netzwerkangriffen Schwachstellen darstellen. Zugleich werden bestimmte IP-Dienste und Funktionen zur Verteidigung eines angegriffenen Netzwerks durch AutoSecure aktiviert. Diese IP-Dienste werden jeweils gleichzeitig mit einem einzigen Befehl deaktiviert oder aktiviert, so dass die Sicherheitskonfiguration für Ihren Router erheblich vereinfacht wird. Eine umfassende Beschreibung der AutoSecure-Funktion finden Sie im Dokument *AutoSecure*.

Konfigurieren von Access-Listen

Durch Access-Listen (ACLs) wird Netzwerkdatenverkehr über eine Schnittstelle anhand bestimmter IP-Quelladressen, IP-Zieladressen oder Protokolle entweder zugelassen oder verweigert. Access-Listen können standardmäßig oder erweitert konfiguriert werden. Durch eine standardmäßige Access-Liste wird die Durchleitung von Paketen von einer bestimmten Quelle gestattet oder verweigert. Mit einer erweiterten Access-Liste hingegen besteht die Möglichkeit, außer den Quellen auch bestimmte Ziele sowie einzelne Protokolle festzulegen, deren Datenverkehr für die Durchleitung zugelassen oder abgelehnt wird. Eine Access-Liste besteht aus einer Reihe von Befehlen, die mit einem gemeinsamen Tag untereinander verbunden sind. Dieses Tag kann eine Zahl oder ein Name sein. In Tabelle 12-1 sind die zum Konfigurieren von Access-Listen verwendeten Befehle aufgeführt.

Tabelle 12-1 Konfigurationsbefehle für Access-Listen

ACL-Typ	Konfigurationsbefehle
Bezeichnung per Nummer	
Standard	**access-list** {**1-99**} {**permit** | **deny**} *Quelladresse* [*Quellmaske*]
Erweitert	**access-list** {**100-199**} {**permit** | **deny**} *Protokoll Quelladresse* [*Quellmaske*] *Zieladresse* [*Zielmaske*]

Tabelle 12-1 Konfigurationsbefehle für Access-Listen (continued)

ACL-Typ	Konfigurationsbefehle
Bezeichnung per Namen	
Standard	**ip access-list standard** *Name* gefolgt von **deny** {*Quelle* | *Quellenplatzhalter* | **any**}
Erweitert	**ip access-list extended** *Name* gefolgt von {**permit** | **deny**} *Protokoll* {*Quelladresse*[*Quellmaske*] | **any**}{*Zieladresse* [*Zielmaske*] | **any**}

Access-Gruppen

Eine Reihe von Access-Listendefinitionen, die durch einen gemeinsamen Namen oder eine Nummer miteinander verbunden sind, wird als Access-Gruppe bezeichnet. Eine Access-Gruppe wird während der Schnittstellenkonfiguration mit folgendem Befehl für eine Schnittstelle aktiviert:

ip access-group {*Access-Listennummer* | *Access-Listenname*}{**in** | **out**}

Hierbei wird durch die Schlüsselwörter **in** | **out** die Übertragungsrichtung der gefilterten Pakete bezeichnet.

Richtlinien zum Erstellen von Access-Gruppen

Beachten Sie beim Erstellen von Access-Gruppen die folgenden Richtlinien.

- Die Reihenfolge der Access-Listendefinitionen ist wichtig. Ein Paket wird jeweils mit der ersten Access-Liste in der Reihe verglichen. Falls sich dabei keine Übereinstimmung ergibt (d. h. das Paket wird weder explizit zugelassen noch verweigert), wird das Paket mit der nächsten Access-Liste verglichen usw.
- Bevor ein Paket zugelassen oder verweigert wird, muss eine Übereinstimmung aller Parameter mit einer Access-Liste vorliegen.
- Am Ende der gesamten Vergleichssequenz erfolgt eine implizite „Verweigerung für alle“.

Ausführliche Informationen zum Erstellen von Access-Listen finden Sie im Abschnitt Access Control Lists: Overview and Guidelines des *Cisco IOS Release 12.3 Security Configuration Guide*.

Konfigurieren einer CBAC-Firewall

Mit der kontextbasierten Zugriffssteuerung (CBAC, Context-Based Access Control) können Sie eine statusbetonte Firewall konfigurieren, durch die Pakete intern geprüft werden und der Status von Netzwerkverbindungen überwacht wird. Diese Verfahrensweise bietet im Vergleich zu statischen Access-Listen eine höhere Sicherheit, da Access-Listen Datenverkehr nur anhand einzelner Pakete, jedoch nicht basierend auf Paketströmen zulassen oder verweigern können. Da mit CBAC Pakete außerdem geprüft werden, können Entscheidungen für eine Zulassung oder Zurückweisung von Datenverkehr mittels einer Untersuchung von Daten auf der Anwendungsschicht getroffen werden. Bei statischen Access-Listen ist dies hingegen nicht möglich.

Legen Sie zum Konfigurieren einer CBAC-Firewall durch Eingabe des folgenden Befehls im Schnittstellen-Konfigurationsmodus fest, welche Protokolle untersucht werden sollen:

ip inspect name *Prüfungsname Protokoll* **timeout** *Sekunden*

Wenn bei der Prüfung festgestellt wird, dass Datenverkehr mit dem angegebenen Protokoll die Firewall durchläuft, wird eine dynamische Access-Liste erstellt, um die Durchleitung des zurückkehrenden Datenverkehrs zu gestatten. Mit dem Parameter **timeout** wird die Zeitspanne angegeben, während der die betreffende dynamische Access-Liste im aktiven Zustand verbleibt, ohne dass zurückkehrender Datenverkehr durch den Router geleitet wird. Nach Erreichen des festgelegten Timeout-Wertes wird die dynamische Access-Liste entfernt, so dass nachfolgende (möglicherweise auch gültige) Pakete dann nicht mehr zugelassen werden.

Verwenden Sie jeweils den gleichen Prüfungsnamen in mehreren Anweisungen, um diese zu einer Regelgruppe zusammenzufassen. Sie können eine solche Regelgruppe dann an anderer Stelle in der Konfiguration aktivieren, indem Sie beim Konfigurieren einer Schnittstelle an der Firewall den Befehl **ip inspect** *Prüfungsname* **in** | **out** eingeben.

Eine entsprechende Beispielkonfiguration finden Sie in Kapitel 8, „Konfigurieren einer einfachen Firewall“. Weitere Informationen zum Konfigurieren einer CBAC-Firewall finden Sie im Abschnitt Configuring Context-Based Access Control des *Cisco IOS Release 12.3 Security Configuration Guide*.

Konfigurieren des Cisco IOS Firewall-IDS

Durch Cisco IOS Firewall-IDS-Technologie (Intrusion Detection System, System zur Erkennung von Angriffen bzw. Eindringlingen) wird der Schutz durch Perimeterfirewalls verbessert, indem geeignete Maßnahmen für Pakete und Datenflüsse ergriffen werden können, die eine Sicherheitsrichtlinie verletzen oder eine böswillige Netzwerkaktivität darstellen.

Durch Cisco IOS Firewall-IDS können 59 der häufigsten Angriffe anhand von „Signaturen“ erkannt werden, mit denen sich bestimmte Missbrauchsmuster im Netzwerkdatenverkehr feststellen lassen. IDS agiert als Intrusionsmeldesensor am Netzeingang, der Pakete und Sitzungen während des Datenflusses durch den Router überwacht und jeweils nach den speziellen IDS-Signaturen durchsucht. Wenn eine verdächtige Aktivität erkannt wird, reagiert die IDS-Firewall, bevor die Netzwerksicherheit gefährdet wird. Das Ereignis wird sofort protokolliert, und abhängig von der jeweiligen Konfiguration wird eine Warnung gesendet. Außerdem werden die verdächtigen Pakete verworfen, oder die TCP-Verbindung wird zurückgesetzt.

Weitere Informationen zum Konfigurieren von Cisco IOS Firewall-IDS finden Sie im Abschnitt Configuring Cisco IOS Firewall Intrusion Detection System im *Cisco IOS Release 12.3 Security Configuration Guide*.

Konfigurieren von VPNs

Eine VPN-Verbindung (virtuelles privates Netzwerk) ist eine sichere Verbindung zwischen zwei Netzwerken über ein öffentlich zugängliches Netz, z. B. das Internet. Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie unterstützen Standort-zu-Standort-VPNs mit IPSec-Tunneln (IP Security) und GRE (Generic Routing Encapsulation). Ständige VPN-Verbindungen zwischen zwei Peers oder dynamische VPNs mit EZVPN oder DMVPN, bei denen VPN-Verbindungen je nach Bedarf erstellt oder beendet werden, können konfiguriert werden. In Kapitel 6, „Konfigurieren eines VPN mit Easy VPN und einem IPSec-Tunnel“, und Kapitel 7, „Konfigurieren von VPNs mit einem IPSec-Tunnel und Generic Routing Encapsulation“, sind Beispiele für die Konfiguration des Routers mit diesen Funktionen enthalten. Weitere Informationen zur IPSec- und GRE-Konfiguration finden Sie im Kapitel Configuring IPSec Network Security des *Cisco IOS Release 12.3 Security Configuration Guide*.

Informationen zu weiteren VPN-Konfigurationen, die von den Zugangsroutern der Cisco 850-Serie und der Cisco 870-Serie unterstützt werden, finden Sie in den folgenden Dokumenten:

- *VPN Access Control Using 802.1X Authentication* – Durch 802.1X-Authentifizierung können Unternehmensmitarbeiter von zu Hause aus auf das Netzwerk in ihrem Unternehmen zugreifen, während anderen Angehörigen des betreffenden Haushalts nur der Zugang zum Internet gewährt wird.
- *EZVPN Server* – Router der Cisco 850-Serie und der Cisco 870-Serie können als EZVPN-Server konfiguriert werden und entsprechend autorisierten EZVPN-Clients gestatten, dynamische VPN-Tunnel zu den verbundenen Netzwerken einzurichten.
- *Dynamic Multipoint VPN (DMVPN)* – Mit der DMVPN-Funktion können VPN-Tunnel je nach Bedarf zwischen mehreren Routern in einer Mehrpunktkonfiguration erstellt werden. Der Vorteil: Die Konfiguration wird vereinfacht, und es werden keine ständigen Punkt-zu-Punkt-VPN-Tunnel mehr benötigt.

Konfigurieren von Reserve-Wählleitung und Remoteverwaltung

Zugangsrouter der Cisco 800-Serie unterstützen Funktionen zum Einwählen (für Remoteverwaltung) und Hinauswählen (für Reserve-Wählleitung). Durch die Möglichkeit der Konfiguration einer Reserveverbindung über eine Modemleitung bieten Zugangsrouter der Cisco 800-Serie Schutz vor WAN-Ausfällen. Die Reserve-Wählleitung ist standardmäßig deaktiviert und muss daher per Konfiguration aktiviert werden.

Die Funktionen für die Reserve-Wählleitung werden folgendermaßen konfiguriert:

- An allen Routern der Cisco 870-Serie über den Zusatzanschluss
- Am Router Cisco 876 über den ISDN S/T-Anschluss mit erweitertem Enterprise-Abbild (c870-adventerprisek9-mz)

Die Funktionen für die Remoteverwaltung werden folgendermaßen konfiguriert:

- An allen Routern der Cisco 850- und Cisco 870-Serie über den Zusatzanschluss
- An den Routern Cisco 876 und Cisco 878 jeweils über den ISDN S/T-Anschluss

Hinweis Der Konsolenanschluss und der Zusatzanschluss (Aux-Port) befinden sich in der Cisco IOS-Softwarekonfiguration am selben physischen RJ-45-Anschluss. Daher können beide Anschlüsse nicht gleichzeitig aktiviert werden. Die Aktivierung der gewünschten Funktion muss über die CLI (Command-Line Interface) vorgenommen werden.

Dieses Kapitel ist in folgende Themen unterteilt:

Aktivierungsmethoden für die Reserve-Wählleitungsfunktion

Zur Aktivierung der Reserve-Wählleitungsfunktion können drei Verfahren genutzt werden:

- Reserveschnittstellen
- Statische Floating-Routen
- Dialer-Überwachung

Reserveschnittstellen

Sobald der Router die Meldung erhält, dass die Hauptleitung außer Betrieb ist, wird eine Reserveschnittstelle aktiviert. Sie können die Reserveschnittstelle so konfigurieren, dass sie wieder deaktiviert wird, wenn die primäre Verbindung wiederhergestellt und für eine bestimmte Zeitspanne in Betrieb ist.

Dieses Verhalten lässt sich mit der so genannten DDR-Funktion (Dial-on-Demand Routing) erreichen. Sobald diese Funktion konfiguriert ist, wird durch den entsprechend festgelegten Datenverkehr ein Reserveanruf ausgelöst.

Hinweis Selbst wenn diese Reserveschnittstelle aus dem Standby-Modus heraus eingeschaltet (aktiviert) wird, löst der Router den Reserveanruf erst dann aus, wenn der in der Konfiguration festgelegte Datenverkehr für diese Reserveschnittstelle vom Router empfangen wird.

Konfigurieren der Reserveschnittstellen

Führen Sie die folgenden Schritte aus, um den Router mit einer Reserveschnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface atm 0`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus für die Schnittstelle aufgerufen, für die Sie eine Reservefunktion konfigurieren möchten.
		
		Hierbei kann es sich um eine serielle, asynchrone oder eine ISDN-Schnittstelle handeln.
		
		In diesem Beispiel ist die Vorgehensweise zur Konfiguration einer Reserveschnittstelle für eine ATM-WAN-Verbindung dargestellt.

Schritt 2	**backup interface** *Schnittstellentyp Schnittstellennummer*
	
	Beispiel:
	`Router(config-if)#backup interface bri 0`
	`Router (config-if)#`
		Mit diesem Befehl wird eine Schnittstelle als sekundäre Schnittstelle bzw. Reserveschnittstelle zugewiesen.
		
		Hierbei kann es sich um eine serielle oder asynchrone Schnittstelle handeln. Beispielsweise kann die Schnittstelle „serial 1“ als Reserveschnittstelle für die Schnittstelle „serial 0“ konfiguriert werden.
		
		In unserem Beispiel wird ein Basisanschluss (Basic Rate Interface) als Reserveschnittstelle für die Schnittstelle „ATM 0“ konfiguriert.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Statische Floating-Routen

Statische Floating-Routen (Floating Static Routes) sind alternative Routen für den Datenverkehr. Diese statischen Routen werden nur dann aktiviert, wenn ein DDR-Reserveanruf durch den für eine Reserveschnittstelle entsprechend festgelegten Datenverkehr ausgelöst wurde.

Statische Floating-Routen sind vom Leitungsprotokollstatus unabhängig. Dies ist ein wichtiger Aspekt für Frame-Relay-Schaltungen, da das Leitungsprotokoll nicht ausfallen kann, wenn der DLCI (Data-Link Connection Identifier) inaktiv ist. Statische Floating-Routen sind außerdem kapselungsunabhängig.

Hinweis Wenn statische Routen konfiguriert sind, muss das primäre Schnittstellenprotokoll ausfallen, damit die statische Floating-Route aktiviert werden kann.

Konfigurieren von statischen Floating-Routen

Statische Floating-Routen bestehen aus zwei Komponenten: aus statischen und dynamischen Routen. Führen Sie die folgenden Schritte aus, um die statischen und dynamischen Routen auf dem Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]}
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		Mit diesem Befehl wird die primäre statische Route zugewiesen.

Schritt 2	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]} [*Distanz*]
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		Mit diesem Befehl wird der untere Wert der administrativen Distanz für die Reserveschnittstellen-Route zugewiesen. 192.168.2.2 ist die Peer-IP-Adresse der Reserveschnittstellen.

Schritt 3	**router rip**
	
	Beispiel:
	`Router(config)#router rip`
	`Router(config)#`
		Mit diesem Befehl wird RIP-Routing aktiviert.

Schritt 4	**network** *IP-Adresse*
	
	Beispiel:
	`Router(config)#network 22.0.0.0`
	`Router(config)#`
		Mit diesem Befehl wird das Netzwerk für die primäre Schnittstelle definiert. 22.0.0.0 ist der Netzwerkwert der primären Schnittstelle.

Schritt 5	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]} [*Distanz*]
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		Mit diesem Befehl wird der untere Wert der administrativen Distanz für die Reserveschnittstellen-Route zugewiesen. 192.168.2.2 ist die Peer-IP-Adresse der Reserveschnittstellen.

Hinweis Wenn dynamische Routen verwendet werden, ist die für die Aktivierung einer statischen Floating-Route erforderliche Zeit von den Konvergenzzeiten des Routingprotokolls abhängig.

Dialer-Überwachung

Die Dialer-Überwachungsmethode (Dialer Watch) unterstützt nur dynamische Verbindungsstatus-Routingprotokolle des Typs EIGRP (Extended Interior Gateway Routing Protocol).

Konfigurieren der Dialer-Überwachung

Führen Sie die folgenden Schritte aus, um eine Dialer-Überwachung auf dem Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface dialer 2`
	`Router (config-if)#`
		Mit diesem Schritt wird der Konfigurationsmodus für die Einwahl-Reserveschnittstelle aufgerufen.

Schritt 2	**dialerwatch-group** *Gruppennummer*
	
	Beispiel:
	`Router(config-if)# dialer watch-group 2`
	`Router (config-if)#`
		Mit diesem Befehl wird die Gruppennummer für die Überwachungsliste angegeben.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 4	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]}
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		Mit diesem Befehl wird die primäre Route zugewiesen. 22.0.0.2 ist die Peer-IP-Adresse der primären Schnittstellen.

	Befehl	Zweck

Schritt 5	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]} [*Distanz*]
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		Mit diesem Befehl wird der untere Wert der administrativen Distanz für die Reserveschnittstellen-Route zugewiesen. 192.168.2.2 ist die Peer-IP-Adresse der Reserveschnittstellen.

Schritt 6	**dialerwatch-list** *Gruppennummer* {**ip** *IP-Adresse Adressenmaske* | **delay route-check initial** *Sekunden*}
	
	Beispiel:
	`Router(config)# dialer watch-list 2 ip 22.0.0.2 255.255.255.255`
	`Router(config)#`
		Mit diesem Befehl wird der Überwachungsliste eine IP-Adresse zugewiesen.
		
		Wenn die Verbindung auf der primären Schnittstelle verloren geht und die IP-Adresse auf dem Router nicht verfügbar ist, wird auf der Reserveschnittstelle die Dial-out-Funktion (zum Hinauswählen) aktiviert. 22.0.0.2 ist die Peer-IP-Adresse der primären Schnittstellen.

Beschränkungen der Reserve-Wählleitungsfunktion

Für die Reserve-Wählleitungsfunktion gelten folgende Beschränkungen:

- Bridging wird über die Reserveschnittstellen am Konsolen- oder Zusatzanschluss nicht unterstützt.
- Der Router des Typs Cisco 851 unterstützt nur die Einwahlfunktion (Dial-in).
- Der Router Cisco 871 verfügt nur über eine begrenzte Unterstützung für die Reserve-Wählleitungsfunktion, da die Ethernet-WAN-Schnittstelle immer in Betrieb ist, selbst wenn keine ISP-Verbindung auf der anderen Seite des Modems besteht, das mit dem Cisco 871 verbunden ist. Der Router muss sich in einer PPPoE-Umgebung befinden, wobei die Dialer-Überwachungsfunktion aktiviert sein muss. Die IP-Adressen des Peers müssen in der Dialer-Überwachung und den Befehlen für statische Routen angegeben werden, damit die Reserve-Wählleitung bei einem Ausfall der primären Leitung aktiviert werden kann.

In Tabelle 13-1 finden Sie eine Zusammenfassung der unterstützten Merkmale und Beschränkungen in Bezug auf die Reserve-Wählleitung für Zugangsrouter der Cisco 800-Serie.

Tabelle 13-1 Übersicht – Unterstützung und Beschränkungen für Reserve-Wählleitung

WAN-Kapselungstyp	Reserve-Wählleitung möglich?	Methode der Reserve-Wählleitung	Beschränkungen
Cisco 851 oder 871			
PPPoE	Ja	Dialer-Überwachung	Bridging wird bei langsamen Schnittstellen, z. B. einem Zusatzanschluss (Aux-Port), nicht unterstützt. Die Peer-IP-Adresse des Internet-Service-Providers (ISP) wird für die Konfiguration des Befehls **dialerwatch** sowie der statischen IP-Route benötigt.

Tabelle 13-1 Übersicht – Unterstützung und Beschränkungen für Reserve-Wählleitung (Fortsetzung)

WAN-Kapselungstyp	Reserve-Wählleitung möglich?	Methode der Reserve-Wählleitung	Beschränkungen
Normales IP bei Kabelmodem-Szenario	Nein	Dialer-Überwachung	Die IP-Adressen der Peers werden benötigt, um eine ordnungsgemäße Funktionsweise der Dialer-Überwachung zu gewährleisten. Falls eine durch DHCP erhaltene Lease-Zeit nicht niedrig genug eingestellt ist (1 oder 2 Minuten), wird keine Reserve-Wählleitung unterstützt.
Cisco 876, 877 oder 878			
PPP über ATM PPP über Ethernet	Ja	Reserveschnittstellen Floating Static Routes Dialer-Überwachung	Für die Funktionen Floating Static Route und Dialer-Überwachung muss auf dem Router ein Routingprotokoll ausgeführt werden. Durch die Dialer-Überwachung wird bei einem Ausfall der Primärleitung die Reserveschnittstelle aktiviert. Die Reserveschnittstelle wird wieder deaktiviert, sobald der Dialer-Timeout erreicht und die primäre Schnittstelle wieder eingeschaltet ist. Der Router überprüft die primäre Schnittstelle erst nach Ablauf des Dialer-Timeouts. Die Reserveschnittstelle verbleibt bis zum Erreichen des Dialer-Timeouts in aktiviertem Zustand, auch wenn die primäre Schnittstelle in Betrieb ist. Wenn die IP-Adresse des Peers bekannt ist, muss für die Dialer-Überwachung kein Routingprotokoll auf dem Router ausgeführt werden.
RFC 1483 (AAL5, SNAP und MUX)	Ja	Reserveschnittstellen Floating Static Routes Dialer-Überwachung	Wenn Bridging über die WAN-Schnittstelle erfolgt, wird diese Funktion über den Zusatzanschluss nicht unterstützt.

Konfigurationsbeispiel

In den folgenden drei Beispielen sind Beispielkonfigurationen für die drei Reserveverbindungsmethoden dargestellt.

Beispiel 13-1 Konfigurieren der Reserve-Wählleitung mit Reserveschnittstellen

```
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
! Mit diesem Befehl wird der ISDN-Switchtyp angegeben.
isdn switch-type basic-net3
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
```

```
! ISDN-Schnittstelle, die als Reserveschnittstelle dienen soll.
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 backup interface BRI0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
 encapsulation aal5snap
 pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Reserveschnittstelle für Wählleitung, die der physikalischen Schnittstelle BRI0
! zugeordnet ist.
! Dialer-Pool 1 ordnet sie dem Dialer-Pool-Mitglied 1 von BRI0 zu.
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer-group 1
!
! Primäre Schnittstelle, die der physikalischen Schnittstelle von ATM0 zugeordnet ist.
! Dialer-Pool 2 ordnet sie dem Dialer-Pool 2 von ATM0 zu.
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 no cdp enable
!
ip classless
! Primäre und Reserveschnittstelle werden mit Routing-Angaben versehen.
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
! Gibt verdächtigen Datenverkehr an, der den Reserve-ISDN-Datenverkehr auslösen soll.
dialer-list 1 protocol ip permit
```

Beispiel 13-2 Konfigurieren der Reserve-Wählleitung mit Floating Static Routes

```
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
! Mit diesem Befehl wird der ISDN-Switchtyp angegeben.
isdn switch-type basic-net3
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
```

```
!
! ISDN-Schnittstelle, die als Reserveschnittstelle dienen soll.
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
 encapsulation aal5snap
 pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Reserveschnittstelle für Wählleitung, die der physikalischen Schnittstelle BRI0
! zugeordnet ist.
! Dialer-Pool 1 ordnet sie dem Dialer-Pool-Mitglied 1 von BRI0 zu
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer-group 1
!
! Primäre Schnittstelle, die der physikalischen Schnittstelle von ATM0 zugeordnet ist.
! Dialer-Pool 2 ordnet sie dem Dialer-Pool 2 von ATM0 zu.
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
!
ip classless
no cdp enable
! Primäre und Reserveschnittstelle werden mit Routing-Angaben versehen. (In diesem
! Beispiel werden statische Routen verwendet.
! Das Leitungsprotokoll "atm0" muss daher deaktiviert werden, damit die
! Reserveschnittstelle funktioniert.)
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 150
ip http server
!
! Gibt verdächtigen Datenverkehr an, der den Reserve-ISDN-Datenverkehr auslösen soll.
dialer-list 1 protocol ip permit
```

Beispiel 13-3 Konfigurieren der Reserve-Wählleitung mit Dialer-Überprüfung

```
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
!
! Mit diesem Befehl wird der ISDN-Switchtyp angegeben.
isdn switch-type basic-net3
!
```

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 hold-queue 100 out
!
! ISDN-Schnittstelle, die als Reserveschnittstelle dienen soll.
interface BRI0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
 encapsulation aal5snap
 pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Reserveschnittstelle für Wählleitung, die der physikalischen Schnittstelle BRI0
! zugeordnet ist.
! Dialer-Pool 1 ordnet sie dem Dialer-Pool-Mitglied 1 von BRI0 zu.
! Beachten Sie, dass "dialer watch-group 1" eine Überwachungsliste mit dem entsprechenden
! Befehl
! "dialer watch-list" verbindet.
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 30
 dialer string 384040
 dialer watch-group 1
 dialer-group 1
!
! Primäre Schnittstelle, die der physikalischen Schnittstelle von ATM0 zugeordnet ist.
! Dialer-Pool 2 ordnet sie dem Dialer-Pool 2 von ATM0 zu.
interface Dialer2
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 no cdp enable
!
ip classless
!
! Primäre und Reserveschnittstelle werden mit Routing-Angaben versehen.
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
! Auf verdächtigen Datenverkehr überwachen.
dialer watch-list 1 ip 22.0.0.2 255.255.255.255

! Gibt verdächtigen Datenverkehr an, der den Reserve-ISDN-Datenverkehr auslösen soll.
dialer-list 1 protocol ip permit
!
```

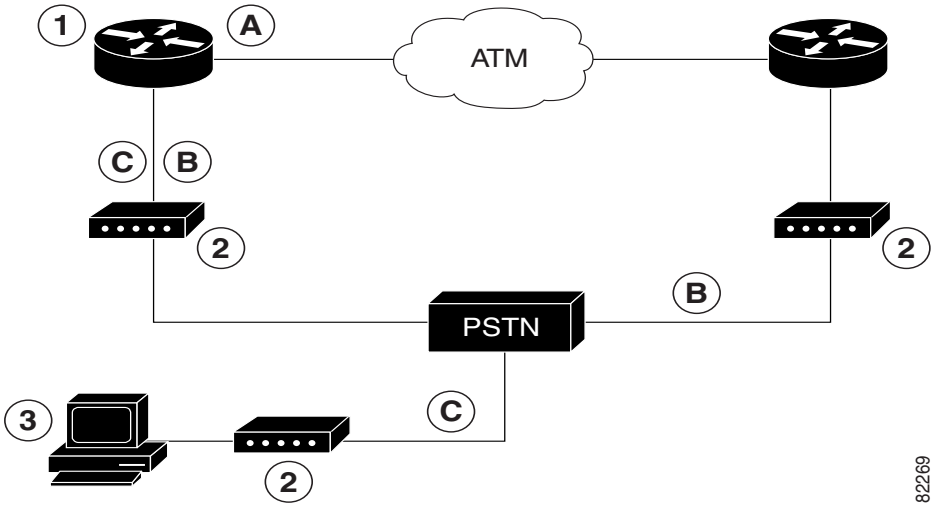
Konfigurieren von Reserve-Wählleitung und Remoteverwaltung über den Konsolen-/Zusatzanschluss

Wenn am Kundenstandort befindliche Geräte, z. B. ein Cisco 850 oder Cisco 870, mit einem ISP verbunden werden, wird dem jeweiligen Router dynamisch eine IP-Adresse zugewiesen. Es ist ebenfalls möglich, dass die IP-Adresse durch den Peer über eine zentral gesteuerte Funktion zugewiesen wird. Die Reserve-Wählleitungsfunktion kann zusätzlich eingerichtet werden, um eine Failover-Route für den Fall eines Ausfalls der Primärleitung bereitzustellen. Die Router des Typs Cisco 850 und Cisco 870 verwenden den Zusatzanschluss für die Reserve-Wählleitung und Remoteverwaltung.

Hinweis Eine Kabelmodemumgebung wird derzeit nicht unterstützt.

In Abbildung 13-1 ist die Netzwerkkonfiguration für einen Zugang per Remoteverwaltung und die Bereitstellung einer Reserveverbindung für die primäre WAN-Leitung dargestellt.

Abbildung 13-1 Reserve-Wählleitung und Remoteverwaltung über den Zusatzanschluss



1	Router der Cisco 850- oder Cisco 870-Serie	**A**	WAN-Hauptverbindung; primäre Verbindung mit dem Internet-Service-Provider
2	Modem	**B**	Reserve-Wählleitung; dient als Failover-Verbindung für den Router Cisco 870, falls die Primärleitung ausfallen sollte
3	PC	**C**	Remoteverwaltung; dient zum Zugriff per Einwahl, um Änderungen oder Aktualisierungen an den Cisco IOS-Konfigurationen vorzunehmen

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um die Funktionen Reserve-Wählleitung und Remoteverwaltung für diese Router zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**ip name-server** *Serveradresse*
	
	Beispiel:
	`Router(config)# ip name-server 192.168.28.12`
	`Router(config)#`
		Mit diesem Befehl wird die DNS-IP-Adresse Ihres Internet-Service-Providers eingegeben.
		
		Tipp Sie können gegebenenfalls auch mehrere Serveradressen angeben.

Schritt 2	**ip dhcp pool** *Name*
	
	Beispiel:
	`Router(config)#ip dhcp pool 1`
	`Router(config-dhcp)#`
		Mit diesem Befehl wird ein DHCP-Adresspool auf dem Router erstellt und der Konfigurationsmodus für „DHCP Pool“ aufgerufen. Das Argument *Name* kann eine Zeichenfolge oder ein ganzzahliger Wert sein.
		
		• Konfigurieren Sie den DHCP-Adresspool. Beispiele für Befehle, die Sie im Konfigurationsmodus für „DHCP Pool“ verwenden können, finden Sie unter „Konfigurationsbeispiel“ auf Seite 13-15.

Schritt 3	**exit**
	
	Beispiel:
	`Router(config-dhcp)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 4	**chat-script** *Skriptname erwartete-Sendung*
	
	Beispiel:
	`Router(config)#chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102 T" TIMEOUT 45 CONNECT \c`
	`Router(config)#`
		In diesem Schritt wird ein Chatskript konfiguriert, das bei Dial-on-Demand-Routing (DDR) verwendet wird. Damit können Befehle zur Anwahl eines Modems und zur Anmeldung bei Remotesystemen erteilt werden. Mit dem definierten Skript wird ein Anruf über ein Modem getätigt.

Schritt 5	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)#interface Async 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die asynchrone Schnittstelle erstellt und aufgerufen.
		
		• Konfigurieren Sie die asynchrone Schnittstelle. Beispiele für Befehle, die Sie im Konfigurationsmodus für die asynchrone Schnittstelle verwenden können, finden Sie unter „Konfigurationsbeispiel“ auf Seite 13-15.

	Befehl	Zweck

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 7	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)#interface Dialer 3`
	`Router (config-if)#`
		Mit diesem Befehl wird der Schnittstellen-Konfigurationsmodus aufgerufen.

Schritt 8	**dialer watch-group** *Gruppennummer*
	
	Beispiel:
	`Router(config-if)# dialer watch-group 1`
	`Router (config-if)#`
		Mit diesem Befehl wird die Gruppennummer für die Überwachungsliste angegeben.

Schritt 9	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 10	**ip nat inside source** {**list** *Access-Listenummer*} {**interface** *Typ Nummer* | **pool** *Name*} [**overload**] **Beispiel:** `Router(config)#ip nat inside source list 101 interface Dialer 3 overload`	Mit diesem Befehl wird die dynamische Übersetzung von Adressen auf der inneren Schnittstelle aktiviert.

Schritt 11	**ip route** *Präfixmaske* {*IP-Adresse* | *Schnittstellentyp Schnittstellennummer* [*IP-Adresse*]}
	
	Beispiel:
	`Router(config)#ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		Mit diesem Befehl wird die IP-Route so festgelegt, dass sie auf die Dialer-Schnittstelle als Standardgateway verweist.

Schritt 12	**access-list** *Access-Listennummer* {**deny** | **permit**} *Quelle* [*Quellenplatzhalter*] **Beispiel:** `Router(config)#access-list 1 permit 192.168.0.0 0.0.255.255 any`	In diesem Schritt wird eine erweiterte Access-Liste definiert, durch die angegeben wird, welche Adressen übersetzt werden sollen.

	Befehl	Zweck

Schritt 13	**dialerwatch-list** *Gruppennummer* {**ip** *IP-Adresse Adressenmaske* | **delay route-check initial** *Sekunden*}
	
	Beispiel:
	`Router(config)# dialer watch-list 1 ip 22.0.0.2 255.255.255.255`
	`Router(config)#`
		In diesem Schritt wird der Status der Primärleitung anhand vorhandener Routen zum Peer ausgewertet. 22.0.0.2 ist die Peer-IP-Adresse des ISP.

Schritt 14	**line** [**aux** | **console** | **tty** | **vty**] *Leitungsnummer* [*Endleitungsnummer*]
	
	Beispiel:
	`Router(config)# line console 0`
	`Router (config- line)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Leitungsschnittstelle aufgerufen.

Schritt 15	**modem enable**
	
	Beispiel:
	`Router(config-line)# modem enable`
	`Router (config- line)#`
		Mit diesem Befehl wird die Anschlussfunktion vom Konsolen- auf den Zusatzanschluss umgeschaltet.

Schritt 16	**exit**
	
	Beispiel:
	`Router(config-line)#exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 17	**line** [**aux** | **console** | **tty** | **vty**] *Leitungsnummer* [*Endleitungsnummer*]
	
	Beispiel:
	`Router(config)# line aux 0`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus für die Zusatzschnittstelle aufgerufen.

Schritt 18	**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}
	
	Beispiel:
	`Router(config)# flowcontrol hardware`
	`Router(config)#`
		Mit diesem Befehl wird die Hardware-Signalflusskontrolle aktiviert.

Konfigurationsbeispiel

Im folgenden Konfigurationsbeispiel wird eine IP-Adresse für die ATM-Schnittstelle über PPP/IPCP-Adressenverhandlung sowie eine Reserve-Wählleitung über den Konsolenanschluss festgelegt.

```
!
ip name-server 192.168.28.12
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool 1
 import all
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
! Korrekte Telefonnummer des eigenen Internet Service Providers muss angegeben werden.
modemcap entry MY-USER_MODEM:MSC=&F1S0=1
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102\T"
TIMEOUT 45 CONNECT \c
!
!
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
! Reserve-Wählleitung und physikalische Schnittstelle für Remoteverwaltung.
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 async default routing
 async dynamic routing
 async mode dedicated
 ppp authentication pap callin
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
 pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
! Primäre WAN-Leitung.
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username account password 7 pass
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
```

```
! Logische Backup-Schnittstelle für Dialer.
interface Dialer3
 ip address negotiated
 ip nat outside
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool 3
 dialer idle-timeout 60
 dialer string 5555102 modem-script Dialout
 dialer watch-group 1
!
! IP-Adresse des PCs für die Remoteverwaltung.
peer default ip address 192.168.2.2
no cdp enable
!
! Eigenes Internet Service Provider-Konto und Passwort müssen angegeben werden.
ppp pap sent-username account password 7 pass
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
! IP-NAT über Dialer-Schnittstelle unter Verwendung des Befehls route-map.
ip nat inside source route-map main interface Dialer1 overload
ip nat inside source route-map secondary interface Dialer3 overload
ip classless
!
! Wenn die Primärleitung wieder aktiviert ist, wird der Distanzwert 80 außer Kraft gesetzt
! und durch den Wert 50 ersetzt, wenn kein Timeout der Reserve-Wählleitung
! aufgetreten ist. Verwendet mehrere Routen, da Peer-IP-Adressen abgewechselt werden,
! wenn Endgerät angeschlossen wird.
ip route 0.0.0.0 0.0.0.0 64.161.31.254 50
ip route 0.0.0.0 0.0.0.0 66.125.91.254 50
ip route 0.0.0.0 0.0.0.0 64.174.91.254 50
ip route 0.0.0.0 0.0.0.0 63.203.35.136 80
ip route 0.0.0.0 0.0.0.0 63.203.35.137 80
ip route 0.0.0.0 0.0.0.0 63.203.35.138 80
ip route 0.0.0.0 0.0.0.0 63.203.35.139 80
ip route 0.0.0.0 0.0.0.0 63.203.35.140 80
ip route 0.0.0.0 0.0.0.0 63.203.35.141 80
ip route 0.0.0.0 0.0.0.0 Dialer1 150
no ip http server
ip pim bidir-enable
!
! IP-Adresse des PCs hinter dem Endgerät.
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 103 permit ip 192.168.0.0 0.0.255.255 any
!
! Überwachung mehrerer IP-Adressen, da Peers abgewechselt werden,
! wenn Endgerät angeschlossen wird.
dialer watch-list 1 ip 64.161.31.254 255.255.255.255
dialer watch-list 1 ip 64.174.91.254 255.255.255.255
dialer watch-list 1 ip 64.125.91.254 255.255.255.255
!
! Reserve-Wählleitung wird aktiviert, wenn die Primärleitung
! 5 Minuten nach dem Hochfahren des Endgeräts nicht verfügbar ist.
dialer watch-list 1 delay route-check initial 300
dialer-list 1 protocol ip permit
!
! Datenverkehr nur dann an eine Schnittstelle weiterleiten, wenn dem Dialer eine
! IP-Adresse zugewiesen wird.
route-map main permit 10
 match ip address 101
 match interface Dialer1
```

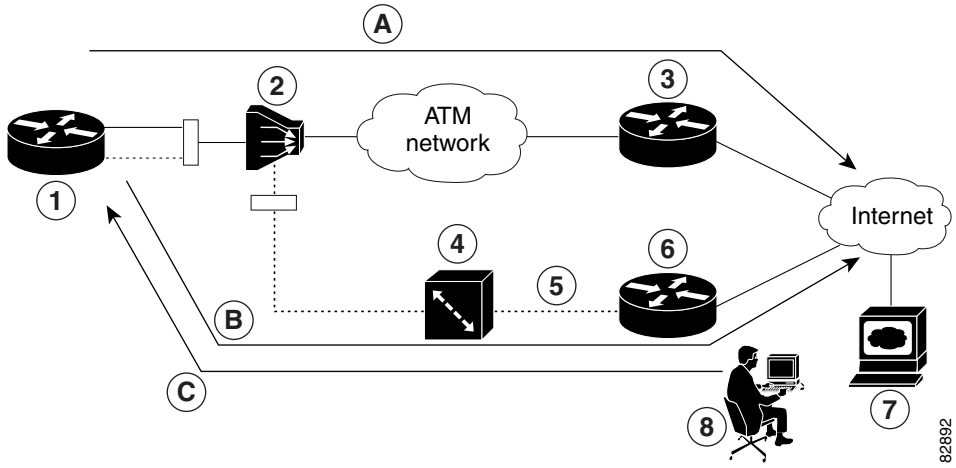
```
!
route-map secondary permit 10
 match ip address 103
 match interface Dialer3
!
! Umschalten von Konsolen- auf Zusatzanschlussfunktion (Aux).
line con 0
 exec-timedout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 ! Zur Aktivierung und ordnungsgemäßen Kommunikation mit dem externen Modem.
 script dialer Dialout
 modem InOut
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
scheduler max-task-time 5000
end
```

Konfigurieren von Reserve-Wählleitung und Remoteverwaltung über den ISDN S/T-Anschluss

Die Router des Typs Cisco 876 und Cisco 878 verwenden den ISDN S/T-Anschluss für die Remoteverwaltung. Mit einem erweiterten Enterprise-Abbild (c870-adventerprisek9-mz) kann ein Router des Typs Cisco 876 den ISDN S/T-Anschluss auch für die Reserve-Wählleitung verwenden.

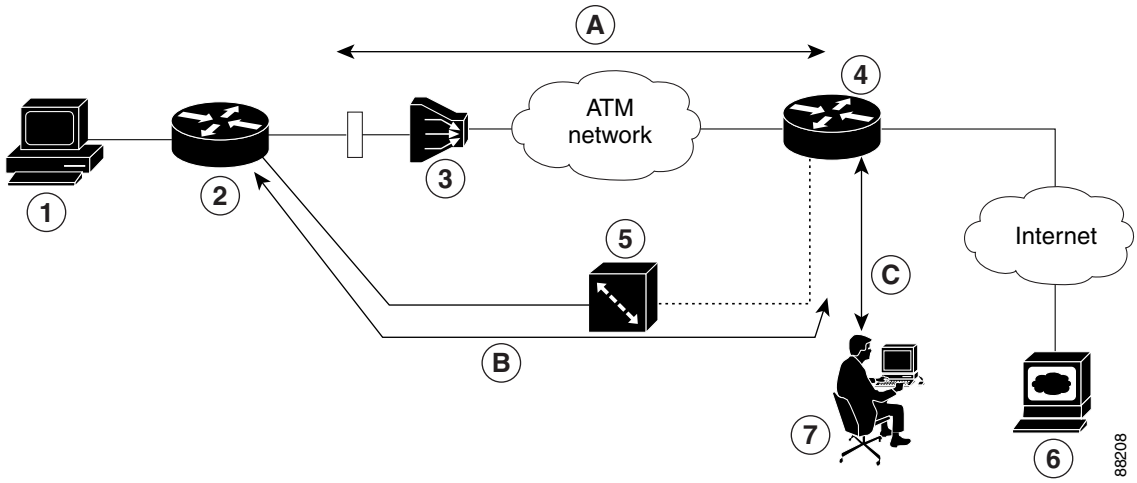
In Abbildung 13-2 und Abbildung 13-3 sind zwei typische Netzwerkkonfigurationen zum Zugriff per Remoteverwaltung und zur Bereitstellung einer Reserveverbindung für die primäre WAN-Leitung dargestellt. In Abbildung 13-2 führt die Verbindung der Reserve-Wählleitung über einen CPE-Splitter (Customer Premises Equipment), DSLAM (Digital Subscriber Line Access Multiplexer) und CO-Splitter (Central Office), bevor sie an den ISDN-Switch angeschlossen wird. In Abbildung 13-3 wird die Reserve-Wählleitung direkt vom Cisco-Router zum ISDN-Switch geführt.

Abbildung 13-2 Reserve-Wählleitung über CPE-Splitter, DSLAM und CO-Splitter



1	Router der Cisco 876- oder Cisco 878-Serie	**A**	Primäre DSL-Schnittstelle
2	DSLAM	**B**	Reserve-Wählleitung und Remoteverwaltung über ISDN-Schnittstelle (ISDN S/T-Anschluss); dient als Failover-Verbindung, falls die Primärleitung ausfallen sollte
3	ATM-Aggregator		
4	ISDN-Switch		
5	ISDN	**C**	Remoteverwaltung durch Administrator über ISDN-Schnittstelle bei Ausfall der primären DSL-Verbindung; dient als Einwählzugang, um Änderungen oder Aktualisierungen der Cisco IOS-Konfiguration zu ermöglichen
6	ISDN-Peer-Router		
7	Webserver		
8	Administrator	—	—

Abbildung 13-3 Reserve-Wählleitung direkt vom Router zum ISDN-Switch



1	PC	**A**	Primäre DSL-Schnittstelle
2	Cisco 876-Router	**B**	Reserve-Wählleitung und Remoteverwaltung über ISDN-Schnittstelle (ISDN S/T-Anschluss); dient als Failover-Verbindung, falls die Primärleitung ausfallen sollte
3	DSLAM		
4	Aggregator		
5	ISDN-Switch	**C**	Remoteverwaltung durch Administrator über ISDN-Schnittstelle bei Ausfall der primären DSL-Verbindung; dient als Einwählzugang, um Änderungen oder Aktualisierungen der Cisco IOS-Konfiguration zu ermöglichen
6	Webserver		
7	Administrator		

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um die Reserve-Wählleitung und Remoteverwaltung über den ISDN-S/T-Anschluss des Routers zu konfigurieren:

- Konfigurieren von ISDN-Einstellungen
- Konfigurieren des Aggregators und ISDN-Peer-Routers

Konfigurieren von ISDN-Einstellungen

Hinweis Der gesuchte Datenverkehr muss vorhanden sein, damit die ISDN-Reserveleitung über die Reserveschnittstelle und mittels Floating Static Routes aktiviert werden kann. Der gesuchte Datenverkehr ist nicht erforderlich, wenn die ISDN-Reserveleitung durch die Dialer-Überwachung aktiviert werden soll.

Führen Sie die folgenden Schritte aus, um die ISDN-Schnittstelle des Routers als Reserveschnittstelle zu konfigurieren (zu Beginn befindet sich der Router im globalen Konfigurationsmodus):

	Befehl	Zweck

Schritt 1	**isdn switch-type** *Switchtyp*
	
	Beispiel:
	`Router(config)# isdn switch-type basic-net3`
	`Router(config)#`
		Mit diesem Befehl wird der ISDN-Switchtyp angegeben.
		
		In unserem Beispiel wird ein in Australien, Kontinentaleuropa und Großbritannien gebräuchlicher Switchtyp angegeben. Informationen zu anderen unterstützten Switchtypen finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Schritt 2	**interface** *Typ Nummer*
	
	Beispiel:
	`Router(config)# interface bri 0`
	`Router (config-if)#`
		Mit diesem Befehl wird der Konfigurationsmodus für den ISDN-Basisanschluss (BRI) aufgerufen.

	Befehl	Zweck

Schritt 3	**encapsulation** *Kapselungstyp*
	
	Beispiel:
	`Router(config-if)#encapsulation ppp`
	`Router (config-if)#`
		Mit diesem Befehl wird der Kapselungstyp für die Schnittstelle „BRI0“ festgelegt.

Schritt 4	**dialer pool-member** *Nummer*
	
	Beispiel:
	`Router(config-if)#dialer pool-member 1`
	`Router (config-if)#`
		Mit diesem Befehl wird die Zugehörigkeit zu einem Dialer-Pool angegeben.

Schritt 5	**isdn switch-type** *Switchtyp*
	
	Beispiel:
	`Router(config-if)# idsn switch-type basic-net3`
	`Router (config-if)#`
		Mit diesem Befehl wird der ISDN-Switchtyp angegeben.

Schritt 6	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.

Schritt 7	**interface dialer** *dialer-rotary-group-Nummer*
	
	Beispiel:
	`Router(config)# interface dialer 0`
	`Router (config-if)#`
		Mit diesem Befehl wird eine Dialer-Schnittstelle (mit einer Nummer zwischen 0 und 255) erstellt und der Schnittstellen-Konfigurationsmodus aufgerufen.

Schritt 8	**ip address negotiated**
	
	Beispiel:
	`Router(config-if)#ip address negotiated`
	`Router (config-if)#`
		In diesem Schritt wird angegeben, dass die IP-Adresse für die Schnittstelle über die PPP/IPCP-Adressenverhandlung (IP Control Protocol) bezogen wird. Die IP-Adresse wird vom Peer erhalten.

Schritt 9	**encapsulation** *Kapselungstyp*
	
	Beispiel:
	`Router(config-if)#encapsulation ppp`
	`Router (config-if)#`
		Mit diesem Befehl wird der Kapselungstyp für die Schnittstelle auf PPP gesetzt.

Schritt 10	**dialer pool** *Nummer*
	
	Beispiel:
	`Router(config-if)#dialer pool 1`
	`Router (config-if)#`
		Mit diesem Befehl wird der zu verwendende Dialer-Pool angegeben.
		
		In diesem Beispiel wird durch die Einstellung „Dialer pool 1“ die Schnittstelle „Dialer 0“ der Schnittstelle „BRI0“ zugeordnet, da der Wert „dialer pool-member“ für BRI0 „1“ beträgt.

	Befehl	Zweck

Schritt 11	**dialer string** *Wählstring*[**:***ISDN-Subadresse*]
	
	Beispiel:
	`Router(config-if)#dialer string 384040`
	`Router (config-if)#`
		Mit diesem Befehl wird die zu wählende Telefonnummer angegeben.

Schritt 12	**dialer-group** *Gruppennummer*
	
	Beispiel:
	`Router(config-if)#dialer group 1`
	`Router (config-if)#`
		Mit diesem Befehl wird die Dialer-Schnittstelle einer Dialer-Gruppe (1 - 10) zugewiesen.

Schritt 13	**exit**
	
	Beispiel:
	`Router(config-if)# exit`
	`Router(config)#`
		Mit diesem Befehl wird der Konfigurationsmodus der Schnittstelle „Dialer 0“ beendet und der globale Konfigurationsmodus aufgerufen.

Schritt 14	**dialer-list** *Dialer-Gruppe* **protocol** *Protokollname* {**permit** | **deny** | **list** *Access-Listennummer* | *Access-Gruppen*}
	
	Beispiel:
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		Mit diesem Schritt wird eine Dialer-Liste für gesuchte Pakete erstellt, die über die festgelegte Schnittstellen-Dialer-Gruppe weitergeleitet werden soll.
		
		In diesem Beispiel entspricht „dialer-list 1“ der Gruppe „dialer-group 1“.
		
		Ausführliche Informationen über diesen Befehl und weitere einstellbare Parameter finden Sie in der *Cisco IOS Dial Technologies Command Reference*.

Konfigurieren des Aggregators und ISDN-Peer-Routers

Der Aggregator ist in der Regel ein Konzentrator-Router, an dem der ATM-PVC des Cisco-Routers endet. Im nachstehend aufgeführten Konfigurationsbeispiel wird der Aggregator als PPPoE-Server konfiguriert, der dem in diesem Kapitel enthaltenen Konfigurationsbeispiel für den Router des Typs Cisco 876 entsprechen soll.

Der ISDN-Peer-Router ist ein beliebiger Router, der über eine ISDN-Schnittstelle verfügt und über ein öffentliches ISDN-Netz mit der ISDN-Schnittstelle des Cisco-Routers kommunizieren kann. Der ISDN-Peer-Router stellt bei Ausfallzeiten des ATM-Netzes einen Internetzugang für Ihren Cisco-Router bereit.

```
! In diesem Abschnitt des Beispiels wird der Aggregator konfiguriert.
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
 protocol pppoe
 virtual-template 1
```

```
!
interface Ethernet3
 description "4700ref-1"
 ip address 40.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Ethernet4
 ip address 30.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Virtual-Template1
 ip address 22.0.0.2 255.255.255.0
 ip mtu 1492
 peer default ip address pool adsl
!
interface ATM0
 no ip address
 pvc 1/40
 encapsulation aal5snap
 protocol pppoe
!
no atm limi-keepalive
!
ip local pool adsl 22.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 22.0.0.1 50
ip route 0.0.0.0 0.0.0.0 30.1.1.2.80

! In diesem Abschnitt des Beispiels wird der ISDN-Peer konfiguriert.
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 30.1.1.2 255.0.0.0
!
interface BRI0
 description "to 836-dialbackup"
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface Dialer0
 ip address 192.168.2.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer string 384020
 dialer-group 1
 peer default ip address pool isdn
!
ip local pool isdn 192.168.2.1
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip route 40.0.0.0 255.0.0.0 30.1.1.1
!
dialer-list 1 protocol ip permit
!
```

Fehlerbehebung

Mithilfe der in diesem Kapitel enthaltenen Informationen können Sie möglicherweise auftretende Probleme besser eingrenzen oder den Router als Ursache des Problems ggf. ausschließen. Dieses Kapitel ist in folgende Abschnitte unterteilt:

Erste Schritte

Bevor Sie ein Softwareproblem beheben können, müssen Sie ein Terminal oder einen PC an den hellblauen Konsolenanschluss des Routers anschließen. (Informationen darüber, wie Sie diese Verbindung herstellen können, finden Sie in der unter "Verwandte Dokumente" section on page xiv aufgeführten Dokumentation.) Mit einem verbundenen Terminal oder PC können Sie die Statusmeldungen vom Router anzeigen und die Befehle für die Fehlerbehebung eingeben.

Sie können ebenfalls per Fernzugriff oder mit Telnet auf die Schnittstelle (Ethernet, ADSL oder Telefon) zugreifen. Für die Verwendung von Telnet wird vorausgesetzt, dass die Schnittstelle aktiv und in Betrieb ist.

Bevor Sie sich an Cisco oder Ihren Vertragshändler wenden

Falls Sie die Ursache eines Problems nicht finden können, wenden Sie sich an Ihren Vertragshändler vor Ort, um Unterstützung zu erhalten. Wenn Sie den Händler anrufen, sollten Sie folgende Angaben bereithalten:

- Gehäusetyp und Seriennummer
- Wartungsvertrag oder Angaben zur Garantie
- Bezeichnung der Software und Versionsnummer

- Datum, an dem Sie das Gerät erhalten haben
- Kurzbeschreibung des Problems
- Kurzbeschreibung der Schritte, die Sie zur Eingrenzung des Problems bereits unternommen haben

ADSL-Fehlerbehebung

Falls im Zusammenhang mit der ADSL-Verbindung Probleme auftreten, vergewissern Sie sich, dass folgende Bedingungen erfüllt sind:

- Die ADSL-Leitung ist angeschlossen und belegt die Pins 3 und 4. Weitere Informationen zur ADSL-Verbindung finden Sie im Hardwarehandbuch des betreffenden Routers.
- Die LED „ADSL CD“ leuchtet. Andernfalls ist der Router möglicherweise nicht an den DSL-Access-Multiplexer (DSLAM) angeschlossen. Weitere Informationen zu den ADSL-LEDs finden Sie im Hardware-Installationshandbuch für den betreffenden Router.
- Der richtige VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) für den asynchronen Transfermodus (ATM) wird verwendet.
- Der DSLAM unterstützt DMT, Ausgabe 2 (Discrete Multi-Tone, Mehrfrequenzübertragung).
- Das ADSL-Kabel, das an den Cisco-Router angeschlossen wird, muss ein ungeschirmtes Twisted-Pair-Kabel (UTP) des Typs 10BASE-T, Kategorie 5 sein. Bei Verwendung normaler Telefonkabel können Leitungsfehler auftreten.

SHDSL-Fehlerbehebung

SHDSL (Symmetrical High-data-rate Digital Subscriber Line) ist auf den Routermodellen Cisco 878 und Cisco 1803 verfügbar. Falls im Zusammenhang mit der SHDSL-Verbindung Probleme auftreten, vergewissern Sie sich, dass folgende Bedingungen erfüllt sind:

- Die SHDSL-Leitung ist angeschlossen und belegt die Pins 3 und 4. Weitere Informationen zur G.SHDSL-Verbindung finden Sie im Hardwarehandbuch des betreffenden Routers.
- Die LED „G.SHDSL“ leuchtet. Andernfalls ist der Router möglicherweise nicht an den DSL-Access-Multiplexer (DSLAM) angeschlossen. Weitere Informationen zu der G.SHDSL-LED finden Sie im Hardware-Installationshandbuch für den betreffenden Router.
- Der richtige VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) für den asynchronen Transfermodus (ATM) wird verwendet.
- Der DSLAM unterstützt das G.SHDSL-Signalisierungsprotokoll.

Geben Sie im EXEC-Modus den Befehl **show controllers dsl 0** ein, um die SHDSL-Konfiguration anzuzeigen.

Befehle zur ATM-Fehlerbehebung

Verwenden Sie die folgenden Befehle, um Fehler an der ATM-Schnittstelle zu beheben.

- Der Befehl „ping atm interface“
- Der Befehl „show interface“
- Der Befehl „show atm interface“
- debug atm-Befehle

Der Befehl „ping atm interface“

Mit dem Befehl **ping atm interface** können Sie feststellen, ob ein bestimmter PVC verwendet wird. Für die Verwendung dieses Befehls muss der PVC nicht auf dem Router konfiguriert sein. In Beispiel 14-1 ist dargestellt, wie mit diesem Befehl bestimmt werden kann, ob PVC 8/35 genutzt wird.

Beispiel 14-1 Feststellen des Nutzungsstatus eines PVC

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

Dieser Befehl sendet fünf OAM F5-Loopback-Pakete an den DSLAM (Abschnitt OAM-Pakete). Falls der PVC am DSLAM konfiguriert wurde, ist die ping-Abfrage erfolgreich.

Um zu testen, ob der Aggregator den PVC verwendet, geben Sie folgenden Befehl ein:

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

Dieser Befehl sendet End-to-End-OAM F5-Pakete, die vom Aggregator als Echo zurückgegeben werden.

Der Befehl „show interface“

Mit dem Befehl **show interface** können Sie den Status aller physischen Anschlüsse (Ethernet und ATM) sowie der logischen Schnittstellen am Router anzeigen. In Tabelle 14-1 sind Beschreibungen für die Meldungen der Befehlsausgabe enthalten.

Beispiel 14-2 Anzeigen des Status ausgewählter Schnittstellen

```
Router# show interface atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 14.0.0.16/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
```

```
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out

Router# show interface fastethernet 0
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.0c13.a4db
(bia0010.9181.1281)
Internet address is 170.1.4.101/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255., txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)

Router# show interface dialer 1
Dialer 1 is up, line protocol is up
    Hardware is Dialer interface
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
        255/255. txload 1/255, rxload 1/255
    Encapsulation PPP, loopback not set
    Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

In Tabelle 14-1 ist eine mögliche Ausgabe für den Befehl **show interface** beschrieben.

Tabelle 14-1Beschreibung der Ausgabe für den Befehl „show interface"

Ausgabe	Ursache
Für ATM-Schnittstellen	
ATM 0 is up, line protocol is up	Die ATM-Leitung ist aktiv und funktioniert fehlerfrei.
ATM 0 is down, line protocol is down	• Die ATM-Schnittstelle wurde mit dem Befehl **shutdown** deaktiviert. oder • Die ATM-Leitung ist nicht in Betrieb. Dies kann darauf zurückzuführen sein, dass das ADSL-Kabel entfernt wurde oder ein ungeeignetes Kabel an den ATM-Port angeschlossen ist.
ATM 0.*n* is up, line protocol is up	Die angegebene ATM-Subschnittstelle ist aktiv und funktioniert fehlerfrei.

Tabelle 14-1Beschreibung der Ausgabe für den Befehl „show interface“ (Fortsetzung)

Ausgabe	Ursache
ATM 0.*n* is administratively down, line protocol is down	Die angegebene ATM-Subschnittstelle wurde mit dem Befehl **shutdown** deaktiviert.
ATM 0.*n* is down, line protocol is down	Die angegebene ATM-Subschnittstelle ist außer Betrieb, da möglicherweise die ATM-Verbindung unterbrochen wurde (durch den Service-Provider).
Für Fast-Ethernet-Schnittstellen	
Fast Ethernet *n* is up, line protocol is up	Die angegebene Fast-Ethernet-Schnittstelle ist mit dem Netzwerk verbunden und funktioniert fehlerfrei.
Fast Ethernet *n* is up, line protocol is down	Die angegebene Fast-Ethernet-Schnittstelle wurde ordnungsgemäß konfiguriert und aktiviert, jedoch ist das Ethernet-Kabel möglicherweise vom LAN getrennt.
Fast Ethernet *n* is administratively down, line protocol is down	Die angegebene Fast-Ethernet-Schnittstelle wurde mit dem Befehl **shutdown** deaktiviert, und die Verbindung mit der Schnittstelle wurde getrennt.
Für Dialer-Schnittstellen	
Dialer *n* is up, line protocol is up	Die angegebene Dialer-Schnittstelle ist aktiv und funktioniert fehlerfrei.
Dialer *n* is down, line protocol is down	• Dies ist eine Standardmeldung, die unter Umständen auch dann angezeigt wird, wenn kein Fehler in der Konfiguration vorliegt. oder • Diese Meldung kann jedoch bei Problemen mit der angegebenen Dialer-Schnittstelle ebenfalls bedeuten, dass diese Schnittstelle nicht funktionsfähig ist, da sie möglicherweise mit dem Befehl **shutdown** deaktiviert wurde oder die ADSL-Kabelverbindung getrennt wurde.

Der Befehl „show atm interface“

Wenn Sie ATM-bezogene Informationen zu einer ATM-Schnittstelle anzeigen möchten, geben Sie im privilegierten EXEC-Modus den Befehl **show atm interface atm 0** ein, wie in Beispiel 14-3 dargestellt.

Beispiel 14-3 Anzeigen von Informationen zu einer ATM-Schnittstelle

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0

Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
```

```
Avail bw = 640
Config. is ACTIVE
```

In Tabelle 14-2 sind Beschreibungen für einige Felder der Befehlsausgabe enthalten.

Tabelle 14-2Beschreibung der Ausgabe für den Befehl „show atm interface“

Feld	Beschreibung
ATM interface	Nummer der Schnittstelle. Dieser Wert ist bei den Zugangsroutern der Cisco 850-Serie und der Cisco 870-Serie stets 0.
AAL enabled	Typ der aktivierten AAL (ATM-Adaptionsschicht). Die Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie unterstützen AAL5.
Maximum VCs	Die von dieser Schnittstelle unterstützte maximale Anzahl virtueller Verbindungen.
Current VCCs	Anzahl aktiver Virtual Channel Connections (VCCs, virtuelle Kanalanschlüsse).
Maximum Transmit Channels	Maximale Anzahl der Sendekanäle.
Max Datagram Size	Der konfigurierte Wert für die maximale Anzahl von Bytes, die im größten Datagramm enthalten sein können.
PLIM Type	Typ des Bitübertragungsschicht-Schnittstellenmoduls (PLIM, Physical Layer Interface Module).

debug atm-Befehle

Mithilfe der **debug**-Befehle können Sie Konfigurationsprobleme beheben, die unter Umständen in Ihrem Netzwerk auftreten können. Durch Eingabe der **debug**-Befehle lassen sich umfassende und hilfreiche Informationen anzeigen, die Sie bei der Ursachenforschung für eventuelle Probleme unterstützen.

Richtlinien für die Verwendung von Debugging-Befehlen

Lesen Sie vor dem Einsatz von Debugging-Befehlen die folgenden Richtlinien, damit gewährleistet ist, dass mit den Befehlen die gewünschten Ergebnisse erzielt werden.

- Alle Debugging-Befehle müssen im privilegierten EXEC-Modus eingegeben werden.
- Geben Sie zum Anzeigen der Debugging-Meldungen auf einer Konsole den Befehl **logging console debug** ein.
- Die meisten **debug**-Befehle werden ohne Argumente eingegeben.
- Zum Deaktivieren des Debugging geben Sie den Befehl **undebug all** ein.
- Um **debug**-Befehle während einer Telnet-Sitzung verwenden zu können, müssen Sie den Befehl **terminal monitor** eingeben.

Caution Dem Debugging wird eine hohe Priorität im CPU-Prozess Ihres Routers zugewiesen, so dass der Router als Folge des Debugging unter Umständen funktionsuntüchtig wird. Setzen Sie aus diesem Grund die **debug**-Befehle nur ein, um besondere Probleme zu beheben. Am besten sollte das Debugging daher in Zeiten mit geringem Netzwerkdatenverkehr durchgeführt werden, so dass andere Aktivitäten im Netzwerk nicht beeinträchtigt werden.

Weitere Informationen und Dokumente zu den **debug**-Befehlen finden Sie in der *Cisco IOS Debug Command Reference*.

Der Befehl „debug atm errors“

Mit dem Befehl **debug atm errors** können ATM-Fehler angezeigt werden. Durch ein dem Befehl vorangestelltes **no** wird die Debugging-Ausgabe deaktiviert. In Beispiel 14-4 ist eine Beispielausgabe dargestellt.

Beispiel 14-4 Anzeigen von ATM-Fehlern

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

Der Befehl „debug atm events“

Mit dem Befehl **debug atm events** können im ATM-Schnittstellenprozessor auftretende Ereignisse angezeigt und Probleme in einem ATM-Netz diagnostiziert werden. Sie können sich dadurch einen Gesamtüberblick über die Stabilität des Netzwerks verschaffen. Durch ein dem Befehl vorangestelltes **no** wird die Debugging-Ausgabe deaktiviert.

Falls die Schnittstelle erfolgreich mit dem DSLAM (Digital Subscriber Line Access Multiplexer) beim Telefonunternehmen kommuniziert, ist der Modemstatus 0x10. Wenn die Schnittstelle nicht mit dem DSLAM kommuniziert, ist der Modemstatus 0x8. In Beispiel 14-5 ist eine ADSL-Verbindung dargestellt, die aktiv ist und erfolgreich einen Test durchläuft. In Beispiel 14-6 ist eine ADSL-Verbindung dargestellt, die nicht ordnungsgemäß kommuniziert. Beachten Sie, dass der Modemstatus nicht zu 0x10 übergeht.

Beispiel 14-5 Anzeigen von Ereignissen des ATM-Schnittstellenprozessors – Erfolg

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
```

```
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

Beispiel 14-6 Anzeigen von Ereignissen des ATM-Schnittstellenprozessors – Fehler

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

Der Befehl „debug atm packet“

Mit dem Befehl **debug atm packet** können Sie alle ATM-Pakete auf Prozessebene für ausgehende und eingehende Pakete anzeigen. Durch die Ausgabe werden Informationen online gemeldet, sobald ein Paket empfangen oder ein Sendeversuch unternommen wird. Durch ein dem Befehl vorangestelltes **no** wird die Debugging-Ausgabe deaktiviert.

Caution Da durch den Befehl **debug atm packet** für jedes verarbeitete Paket eine beträchtliche Informationsmenge als Ausgabe generiert wird, sollten Sie den Befehl nur in verkehrsschwachen Zeiten des Netzwerks verwenden, damit andere Systemaktivitäten nicht beeinträchtigt werden.

Es gilt folgende Befehlssyntax:

debug atm packet [**interface atm** *Nummer* [**vcd** *VCD-Nummer*][**vc** *VPI/VCI Nummer*]]

no debug atm packet [**interface atm** *Nummer* [**vcd** *VCD-Nummer*][**vc** *VPI/VCI Nummer*]]

Die entsprechenden Schlüsselwörter sind hierbei folgendermaßen definiert:

interface atm *Nummer*	(Optional) Nummer der ATM-Schnittstelle oder -Subschnittstelle.
vcd *VCD-Nummer*	(Optional) Nummer des Virtual Circuit Designators (VCD).
vc *VPI/VCI-Nummer*	Der VPI/VCI-Wert des ATM-PVC.

In Beispiel 14-7 ist eine Beispielausgabe für den Befehl **debug atm packet** enthalten.

Beispiel 14-7 Anzeigen einer ATM-Paketverarbeitung

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

In Tabelle 14-3 sind Beschreibungen für einige Felder der Ausgabe des Befehls **debug atm packet** enthalten.

Tabelle 14-3Beschreibung der Ausgabe für den Befehl „debug atm packet“

Feld	Beschreibung
ATM0	Schnittstelle, die das Paket generiert.
(O)	Ausgabepaket. (I) würde Empfangspaket bedeuten.
VCD: 0x*n*	Diesem Paket zugeordneter Virtual Circuit; *n* steht hierbei für einen bestimmten Wert.
VPI: 0x*n*	Virtual Path Identifier für dieses Paket; *n* steht hierbei für einen bestimmten Wert.
DM: 0x*n*	Deskriptormodus-Bits; *n* steht hierbei für einen bestimmten Wert.
Length: *n*	Gesamtlänge des Pakets (in Bytes), einschließlich der ATM-Header.

Methoden zum Aktualisieren der Software

Die Aktualisierung der Software auf den Zugangsroutern der Cisco 850-Serie und der Cisco 870-Serie kann auf verschiedene Weise vorgenommen werden:

- Kopieren Sie das neue Softwareabbild über das LAN oder WAN in den Flash-Speicher, während das bisherige Cisco IOS-Softwareabbild noch ausgeführt wird.
- Kopieren Sie das neue Softwareabbild über das LAN in den Flash-Speicher, während das Bootabbild (ROM Monitor) ausgeführt wird.
- Kopieren Sie das neue Softwareabbild im ROM Monitor-Modus über den Konsolenanschluss.
- Booten Sie den Router im ROM Monitor-Modus von einem Softwareabbild, das auf einen TFTP-Server geladen wurde. Dazu muss sich der TFTP-Server im selben LAN wie der Router befinden.

Wiederherstellen eines gelöschten Kennworts

So stellen Sie ein gelöschtes Aktivierungskennwort (enable) oder geheimes Aktivierungskennwort (enable-secret) wieder her:

1. Ändern des Konfigurationsregisters
2. Zurücksetzen des Routers
3. Zurücksetzen des Kennworts und Speichern der Änderungen (nur für enable-secret-Kennwörter)
4. Zurücksetzen des Konfigurationsregisterwerts

Hinweis Ein gelöschtes Kennwort kann nur wiederhergestellt werden, wenn Sie über den Konsolenanschluss mit dem Router verbunden sind. Die folgenden Schritte können in einer Telnet-Sitzung nicht ausgeführt werden.

Tipp Weitere Informationen zum Ersetzen von geheimen Aktivierungskennwörtern finden Sie im Bereich „Hot Tips“ auf der Website Cisco.com.

Ändern des Konfigurationsregisters

Führen Sie folgende Schritte aus, um ein Konfigurationsregister zu ändern:

Schritt 1 Verbinden Sie ein ASCII-Terminal oder einen PC mit einem Terminal-Emulationsprogramm mit dem Konsolenanschluss (CONSOLE) an der Rückseite des Routers.

Schritt 2 Konfigurieren Sie das Terminal mit folgenden Einstellungen: 9600 Baud, 8 Datenbit, keine Parität und 1 Stoppbit.

Schritt 3 Geben Sie an der Eingabeaufforderung des privilegierten EXEC-Modus (*Routername* #) den Befehl **show version** ein, um den aktuellen Konfigurationsregisterwert anzuzeigen (in der untersten Zeile dieses Ausgabebeispiels angegeben):

```
Router# show version
Cisco IOS Software, C870 Software (C870-ADVENTERPRISEK9-M), Version 12.3(nightly
.PCBU_WIRELESS041110) NIGHTLY BUILD, synced to haw_t_pi1_pcbu HAW_T_PI1_PCBU_200
40924
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Nov-04 03:37 by jsomebody

ROM: System Bootstrap, Version 1.0.0.6(20030916:100755) [jsomebody],
 DEVELOPMENT SOFTWARE

Router uptime is 2467 minutes
System returned to ROM by power-on
System image file is "flash:c870-adventerprisek9-mz.pcbu_wireless.041110"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
use. Delivery of Cisco cryptographic products does not imply
```

```
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 877 (MPC8272) processor (revision 0x00) with 59392K/6144K bytes of memory.

Processor board ID
MPC8272 CPU Rev: Part Number 0xC, Mask Number 0x10
4 FastEthernet interfaces
1 ATM interface
1 802.11 Radio
128K bytes of non-volatile configuration memory.
20480K bytes of processor board System flash (Intel Strataflash)

Configuration register is 0x2102
```

Schritt 4 Notieren Sie sich die Einstellung des Konfigurationsregisters.

Schritt 5 Um die Break-Einstellung (Unterbrechung) zu aktivieren (wird durch den Wert von Bit 8 im Konfigurationsregister angegeben), müssen Sie den Befehl **config-register 0x01** im privilegierten EXEC-Modus eingeben.

- Break aktiviert – Bit 8 ist auf 0 gesetzt.
- Break deaktiviert (Standardeinstellung) – Bit 8 ist auf 1 gesetzt.

Zurücksetzen des Routers

Führen Sie die folgenden Schritte aus, um den Router zurückzusetzen:

Schritt 1 Bei aktivierter Break-Einstellung setzen Sie den Vorgang mit Schritt 2 fort. Bei deaktivierter Break-Einstellung schalten Sie den Router aus (O), warten 5 Sekunden und schalten ihn dann wieder ein (|). Drücken Sie dann innerhalb von 60 Sekunden die Taste **Untbr**. Auf dem Terminal wird die ROM Monitor-Eingabeaufforderung angezeigt. Setzen Sie den Vorgang mit Schritt 3 fort.

Hinweis Manche Terminal-Tastaturen sind mit einer Taste *Untbr* ausgestattet. Falls an Ihrer Tastatur eine solche Unterbrechungstaste nicht vorhanden ist, schlagen Sie in der Dokumentation des Terminals nach, um herauszufinden, wie Sie einen Unterbrechungsbefehl (Break) senden können.

Schritt 2 Drücken Sie die Taste **Untbr**. Auf dem Terminal wird folgende Eingabeaufforderung angezeigt:

```
rommon 2>
```

Schritt 3 Geben Sie **confreg 0x142** ein, um das Konfigurationsregister zurückzusetzen:

```
rommon 2> confreg 0x142
```

Schritt 4 Initialisieren Sie den Router, indem Sie den Befehl **reset** eingeben:

```
rommon 2> reset
```

Der Router führt einen Einschaltzyklus durch, und das Konfigurationsregister wird auf „0x142“ gesetzt. Der Router verwendet das Boot-ROM-Systemabbild, das im Systemkonfigurationsdialog angezeigt wird:

```
--- System Configuration Dialog ---
```

Schritt 5 Geben Sie als Antwort auf die folgenden Eingabeaufforderungen **no** ein, bis folgende Meldung erscheint:

```
Press RETURN to get started.
```

Schritt 6 Drücken Sie die **Eingabetaste**. Daraufhin wird folgende Eingabeaufforderung angezeigt:

```
Router>
```

Schritt 7 Geben Sie den Befehl **enable** ein, um den Aktivierungsmodus aufzurufen. Konfigurationsänderungen sind nur im Aktivierungsmodus möglich:

```
Router> enable
```

Die Eingabeaufforderung wechselt zur Eingabeaufforderung des privilegierten EXEC-Modus:

```
Router#
```

Schritt 8 Geben Sie den Befehl **show startup-config** ein, um ein enable-Kennwort (Aktivierungskennwort) in der Konfigurationsdatei anzuzeigen:

```
Router# show startup-config
```

Führen Sie die Schritte im folgenden Abschnitt “Zurücksetzen des Kennworts und Speichern der Änderungen” nicht aus, falls Sie ein enable-Kennwort wiederherstellen. Schließen Sie stattdessen den Vorgang zur Kennwortwiederherstellung ab, indem Sie die Schritte im Abschnitt “Zurücksetzen des Konfigurationsregisterwerts” ausführen.

Falls Sie ein enable-secret-Kennwort wiederherstellen, wird dieses Kennwort in der Ausgabe des Befehls **show startup-config** nicht angezeigt. Schließen Sie den Vorgang zur Kennwortwiederherstellung ab, indem Sie die Schritte im nächsten Abschnitt “Zurücksetzen des Kennworts und Speichern der Änderungen” ausführen.

Zurücksetzen des Kennworts und Speichern der Änderungen

Führen Sie die folgenden Schritte aus, um Ihr Kennwort zurückzusetzen und die Änderungen zu speichern:

Schritt 1 Geben Sie den Befehl **configure terminal** ein, um den globalen Konfigurationsmodus aufzurufen:

```
Router# configure terminal
```

Schritt 2 Geben Sie den Befehl **enable secret** ein, um das geheime Aktivierungskennwort im Router zurückzusetzen:

```
Router(config)# enable secret Kennwort
```

Schritt 3 Geben Sie **exit** ein, um den globalen Konfigurationsmodus zu beenden:

```
Router(config)# exit
```

Schritt 4 Speichern Sie Ihre Konfigurationsänderungen:

```
Router# copy running-config startup-config
```

Zurücksetzen des Konfigurationsregisterwerts

Führen Sie die folgenden Schritte aus, um den Konfigurationsregisterwert zurückzusetzen, nachdem Sie ein Kennwort wiederhergestellt oder neu konfiguriert haben:

Schritt 1 Geben Sie den Befehl **configure terminal** ein, um den globalen Konfigurationsmodus aufzurufen:

```
Router# configure terminal
```

Schritt 2 Geben Sie den Befehl **configure register** sowie den ursprünglichen Konfigurationsregisterwert ein, den Sie sich notiert hatten.

```
Router(config)# config-reg Wert
```

Schritt 3 Geben Sie **exit** ein, um den Konfigurationsmodus zu beenden:

```
Router(config)# exit
```

Hinweis Wenn Sie zu der Konfiguration zurückkehren möchten, die vor der Wiederherstellung des Aktivierungskennworts verwendet wurde, verzichten Sie auf die Speicherung der Konfigurationsänderungen, bevor Sie den Router neu booten.

Schritt 4 Booten Sie den Router neu, und geben Sie das wiederhergestellte Kennwort ein.

Verwalten des Routers mit SDM

Das Cisco SDM-Tool ist ein kostenloses Dienstprogramm zur Softwarekonfiguration, das die Zugangsrouter der Cisco 850-Serie und der Cisco 870-Serie unterstützt. Dieses Tool umfasst eine webbasierte Benutzeroberfläche, die folgende Funktionen bzw. Leistungsmerkmale zur Verfügung stellt:

- Vereinfachtes Setup
- Erweiterte Konfiguration
- Routersicherheit
- Routerüberwachung

Teil 4

Referenzinformationen

Grundlegende Fertigkeiten für die Arbeit mit der Cisco IOS-Software

Benutzer, die im Umgang mit der Cisco IOS-Software vertraut sind, können bei der Konfiguration des Routers viel Zeit sparen. Falls Sie Ihre diesbezüglichen Kenntnisse auffrischen möchten, nehmen Sie sich einige Minuten Zeit und lesen diesen Anhang.

Dieser Anhang ist in folgende Abschnitte unterteilt:

- Konfigurieren des Routers von einem PC aus
- Informationen über Befehlsmodi
- Anzeigen der Hilfe
- Verschlüsselte und nicht verschlüsselte Aktivierungskennwörter
- Aufrufen des globalen Konfigurationsmodus
- Verwenden von Befehlen
- Speichern von Konfigurationsänderungen
- Zusammenfassung
- Weitere Vorgehensweise

Wenn Sie bereits mit der Cisco IOS-Software vertraut sind, lesen Sie eines der folgenden Kapitel:

- Kapitel 1, „Grundlegende Routerkonfiguration“
- Kapitel 2, „Beispiele für den Netzwerkeinsatz“
- Ein Kapitel zum Thema Konfiguration in Teil 3.

Konfigurieren des Routers von einem PC aus

Sie können den Router über einen PC konfigurieren, der mit dem Konsolenanschluss verbunden ist und auf dem eine *Terminal-Emulationssoftware* ausgeführt wird. Der PC sendet mit dieser Software die entsprechenden Befehle an den Router. In Tabelle A-1 sind einige gebräuchliche Typen dieser Software aufgeführt, die auf dem jeweils verwendeten PC-Typ basieren.

Tabelle A-1 Terminal-Emulationssoftware

PC-Betriebssystem	Software
Windows 95, Windows 98, Windows 2000, Windows NT, Windows XP	HyperTerm (in Windows-Software integriert), ProComm Plus
Windows 3.1	Terminal (in Windows-Software integriert)
Macintosh	ProComm, VersaTerm (gesondert erhältlich)

Mit der Terminal-Emulationssoftware können Sie die Einstellungen für den am PC angeschlossenen Gerätetyp ändern, d. h. in diesem Fall für einen Router. Konfigurieren Sie die Software mit den folgenden standardmäßigen VT-100-Emulationseinstellungen, um eine Kommunikation zwischen PC und Router zu ermöglichen:

- 9.600 Baud
- 8 Datenbit
- Keine Parität
- 1 Stoppbit
- Keine Flusskontrolle

Diese Einstellungen sollten mit den Standardeinstellungen des Routers übereinstimmen. Zum Ändern der Baudrate sowie der Einstellungen für Datenbit, Parität oder Stoppbit müssen Sie die Parameter im Dienstprogramm ROM-Monitor neu konfigurieren. Weitere Informationen finden Sie in Anhang C, „ROM Monitor“. Wenn Sie die Flusskontrolleinstellungen des Routers ändern möchten, geben Sie den Befehl für die Leitungskonfiguration **flowcontrol** ein.

Informationen darüber, wie Sie den globalen Konfigurationsmodus aufrufen und dann Ihren Router konfigurieren können, finden Sie im Abschnitt „Aufrufen des globalen Konfigurationsmodus“ in diesem Kapitel.

Informationen über Befehlsmodi

In diesem Abschnitt wird die Struktur des Cisco IOS-Befehlsmodus beschrieben. Jeder Befehlsmodus unterstützt bestimmte Cisco IOS-Befehle. Beispielsweise kann der Befehl **interface** *Typ Nummer* nur im globalen Konfigurationsmodus eingegeben werden.

Die folgenden Cisco IOS-Befehlsmodi sind hierarchisch strukturiert. Zu Beginn einer Routersitzung befinden Sie sich im EXEC-Benutzermodus.

- EXEC-Benutzermodus
- Privilegierter EXEC-Modus
- Globale Konfiguration

In Tabelle A-2 sind die in diesem Handbuch verwendeten Befehlsmodi, die Schritte zum Aufrufen jedes einzelnen Modus, die im jeweiligen Modus angezeigte Eingabeaufforderung sowie die Schritte zum Beenden eines Modus oder zum Aufrufen des nächsten Modus aufgeführt. Da in jedem Modus unterschiedliche Routerelemente konfiguriert werden, müssen Sie die Modi unter Umständen relativ häufig wechseln, d. h. einen Modus beenden und einen neuen Modus aufrufen. Durch Eingabe eines Fragezeichens (?) an der Eingabeaufforderung wird eine Liste der verfügbaren Befehle für einen bestimmten Modus angezeigt. Eine Beschreibung der einzelnen Befehle, einschließlich der entsprechenden Befehlssyntax, finden Sie in der Dokumentation zu Cisco IOS Release 12.3.

Tabelle A-2 Übersicht über Befehlsmodi

Modus	Zugriffsmethode	Eingabeaufforderung	Methode zum Beenden und Aufrufen	Informationen über den Modus
EXEC-Benutzermodus	Starten Sie eine Routersitzung.	`Router>`	Zum Beenden einer Routersitzung geben Sie den Befehl **logout** ein.	Verwenden Sie diesen Modus für folgende Aufgaben: • Ändern von Terminaleinstellungen; • Durchführen von grundlegenden Tests; • Anzeigen von Systeminformationen.
Privilegierter EXEC-Modus	Geben Sie im EXEC-Benutzermodus den Befehl **enable** ein.	`Router#`	• Geben Sie zum Beenden des EXEC-Benutzermodus den Befehl **disable** ein. • Geben Sie zum Aufrufen des globalen Konfigurationsmodus den Befehl **configure** ein.	Verwenden Sie diesen Modus für folgende Aufgaben: • Konfigurieren der Betriebsparameter des Routers; • Durchführen der in diesem Handbuch beschriebenen Schritte zur Überprüfung. Um unbefugte Änderungen an einer Routerkonfiguration zu verhindern, sollte der Zugriff auf diesen Modus entsprechend der Beschreibung im Abschnitt „Verschlüsselte und nicht verschlüsselte Aktivierungskennwörter“ dieses Kapitels mit einem Kennwort geschützt werden.
Globale Konfiguration	Geben Sie im privilegierten EXEC-Modus den Befehl **configure** ein.	`Router(config)#`	• Geben Sie zum Beenden des privilegierten EXEC-Modus den Befehl **exit** oder **end** ein, oder drücken Sie die Tastenkombination **Strg-Z**. • Wenn Sie den Schnittstellen-Konfigurationsmodus aufrufen möchten, geben Sie den Befehl **interface** ein.	In diesem Modus können Sie Parameter konfigurieren, die auf den Router global angewendet werden. Sie können ebenfalls auf die folgenden Modi zugreifen, die weiter unten in dieser Tabelle beschrieben sind: • Schnittstellenkonfiguration • Routerkonfiguration • Leitungskonfiguration

Tabelle A-2 Übersicht über Befehlsmodi (Fortsetzung)

Modus	Zugriffsmethode	Eingabeaufforderung	Methode zum Beenden und Aufrufen	Informationen über den Modus
Schnittstellenkonfiguration	Geben Sie im globalen Konfigurationsmodus den Befehl **interface** (mit der Angabe einer bestimmten Schnittstelle, z. B. **interface atm 0**) ein.	`Router (config-if)#`	• Geben Sie zum Beenden des globalen Konfigurationsmodus den Befehl **exit** ein. • Zum Beenden des privilegierten EXEC-Modus geben Sie den Befehl **end** ein oder drücken die Tastenkombination **Strg-Z**. • Wenn Sie den Konfigurationsmodus für eine Subschnittstelle aufrufen möchten, geben Sie mit dem Befehl **interface** die gewünschte Subschnittstelle an.	Mit diesem Modus können Parameter für die Ethernet-Schnittstelle sowie die seriellen Schnittstellen oder Subschnittstellen des Routers konfiguriert werden.
Routerkonfiguration	Geben Sie im globalen Konfigurationsmodus einen Routerbefehl (**router**) gefolgt von dem entsprechenden Schlüsselwort ein, beispielsweise **router rip**.	`Router(config-router)#`	• Geben Sie zum Beenden des globalen Konfigurationsmodus den Befehl **exit** ein. • Zum Beenden des privilegierten EXEC-Modus geben Sie den Befehl **end** ein oder drücken die Tastenkombination **Strg-Z**.	In diesem Modus können Sie das IP-Routingprotokoll konfigurieren.
Leitungskonfiguration	Geben Sie im globalen Konfigurationsmodus den Befehl **line** mit der gewünschten Leitungsnummer, z. B. **line 0**, und dem Leitungstyp (optional) ein.	`Router (config-line)#`	• Geben Sie zum Beenden des globalen Konfigurationsmodus den Befehl **exit** ein. • Zum Beenden des privilegierten EXEC-Modus geben Sie den Befehl **end** ein oder drücken die Tastenkombination **Strg-Z**.	In diesem Modus können Sie Parameter für die Terminalleitung konfigurieren.

Anzeigen der Hilfe

Die Verwendung der Befehle wird durch eine Hilfefunktion unterstützt, die Sie durch Eingabe eines Fragezeichens (?) und durch Navigation mit den Pfeiltasten aufrufen bzw. nutzen können.

Wenn Sie eine Liste der im jeweiligen Befehlsmodus verfügbaren Befehle anzeigen möchten, geben Sie ein Fragezeichen ein:

```
Router> ?
access-enable  Create a temporary access-list entry
access-profile Apply user-profile to interface
clear          Reset functions
...
```

Um einen vollständigen Befehl anzuzeigen, geben Sie die ersten bekannten Zeichen des gewünschten Befehls und ein Fragezeichen ein (ohne Leerzeichen):

```
Router> s?
* s=show set show slip systat
```

Wenn Sie eine Liste der Befehlsvariablen anzeigen möchten, geben Sie den Befehl ein, gefolgt von einem Leerzeichen und einem Fragezeichen:

```
Router> show ?
...
clock      Display the system clock
dialer     Dialer parameters and statistics
exception  exception information
...
```

Um einen zuvor eingegebenen Befehl erneut anzuzeigen, drücken Sie die **Nach-oben**-Taste. Um noch weitere vorherige Befehle anzuzeigen, müssen Sie die **Nach-oben**-Taste lediglich gedrückt halten.

Verschlüsselte und nicht verschlüsselte Aktivierungskennwörter

Der Router wird standardmäßig ohne Kennwortschutz ausgeliefert. Da jedoch mit vielen Befehlen im privilegierten EXEC-Modus Betriebsparameter eingestellt werden können, sollten Sie diese Befehle mit einem Kennwortschutz versehen, um eine Verwendung durch unbefugte Benutzer auszuschließen.

Zum Festlegen eines Kennworts stehen Ihnen die folgenden zwei Befehle zur Verfügung:

- **enable secret** *Kennwort* – Ein sehr sicheres verschlüsseltes Kennwort.
- **enable** *Kennwort* – Ein lokales, nicht verschlüsseltes Kennwort, das eine geringere Sicherheitsstufe bietet.

Mit beiden Kennwörtern, d. h. mit dem Befehl **enable** und mit dem Befehl **enable secret**, kann der Zugriff auf verschiedene Berechtigungsstufen (0 bis 15) gesteuert werden. Das **enable**-Kennwort (Aktivierungskennwort) ist zur Verwendung auf dem lokalen System bestimmt und daher nicht verschlüsselt. Hingegen ist das **enable secret**-Kennwort (geheimes Aktivierungskennwort) für den Einsatz im Netzwerk vorgesehen, d. h. in Umgebungen, in denen ein Kennwort im Netzwerk übertragen oder auf einem TFTP-Server gespeichert wird. Um Zugriff auf die Befehle des privilegierten EXEC-Modus zu erhalten, müssen Sie ein **enable secret**- oder **enable**-Kennwort mit der Berechtigungsstufe 1 eingeben.

Zur Gewährleistung eines größtmöglichen Sicherheitsniveaus sollten diese beiden Kennwörter jeweils unterschiedlich sein. Falls Sie während der Einrichtung ein und dasselbe Kennwort für beide Kennwortbefehle eingeben, übernimmt der Router diese Kennwörter, weist Sie jedoch in einer Warnmeldung darauf hin, dass diese nicht identisch sein sollten.

Ein **enable secret**-Kennwort kann aus 1 bis 25 alphanumerischen Zeichen in Groß- und Kleinschreibung bestehen. Ein **enable**-Kennwort kann aus einer beliebigen Anzahl alphanumerischer Zeichen in Groß- und Kleinschreibung bestehen. In beiden Fällen darf das erste Zeichen jedoch keine Zahl sein. Leerzeichen sind ebenfalls zulässige Zeichen in Kennwörtern; z. B. wäre *zwei Wörter* ein gültiges Kennwort. Vorangestellte Leerzeichen werden ignoriert, Leerzeichen am Wortende hingegen werden erkannt.

Aufrufen des globalen Konfigurationsmodus

Um Konfigurationsänderungen an Ihrem Router vornehmen zu können, müssen Sie sich im globalen Konfigurationsmodus befinden. In diesem Abschnitt wird beschrieben, wie Sie bei Verwendung eines am Router-Konsolenanschluss angeschlossenen Terminals oder PCs den globalen Konfigurationsmodus aufrufen können.

Führen Sie die folgenden Schritte aus, um den globalen Konfigurationsmodus aufzurufen:

Schritt1 Geben Sie nach dem Booten des Router den **enable**- oder **enable secret**-Befehl ein:

```
Router> enable
```

Schritt2 Wenn Sie den Router mit einem Aktivierungskennwort konfiguriert haben, geben Sie dieses Kennwort bei entsprechender Aufforderung ein.

Das Aktivierungskennwort wird bei der Eingabe nicht auf dem Bildschirm angezeigt. Im folgenden Beispiel ist die Verfahrensweise zum Aufrufen des privilegierten EXEC-Modus dargestellt:

```
Password: enable_password
Router#
```

Der privilegierte EXEC-Modus wird durch das Zeichen „#“ in der Eingabeaufforderung angezeigt. Bei Bedarf können Sie jetzt Änderungen an der Routerkonfiguration vornehmen.

Schritt3 Geben Sie den Befehl **configure terminal** ein, um den globalen Konfigurationsmodus aufzurufen:

```
Router# configure terminal
Router(config)#
```

Sie können jetzt Änderungen an der Konfiguration des Routers vornehmen.

Verwenden von Befehlen

In diesem Abschnitt finden Sie einige Tipps zur Eingabe von Cisco IOS-Befehlen über die Befehlszeilenschnittstelle (CLI, Command-Line Interface).

Abkürzen von Befehlen

Bei der Befehlseingabe müssen lediglich einige wenige Zeichen eines gewünschten Befehls eingegeben werden, die es jedoch dem Router ermöglichen müssen, einen eindeutigen Befehl zu erkennen. Im folgenden Beispiel ist die Verfahrensweise zur Eingabe des Befehls **show version** dargestellt:

```
Router # sh v
```

Rückgängigmachen von Befehlen

Um eine Funktion zu deaktivieren oder einen eingegebenen Befehl zu widerrufen, d. h. rückgängig zu machen, können Sie durch Eingabe des vorangestellten Schlüsselworts **no** die meisten Befehle außer Kraft setzen, z. B. **no ip routing**.

CLI-Fehlermeldungen

In Tabelle A-3 werden einige Fehlermeldungen aufgeführt, die bei Verwendung der CLI zum Konfigurieren des Routers unter Umständen auftreten können.

Tabelle A-3 Allgemeine CLI-Fehlermeldungen

Fehlermeldung	Bedeutung	Aufrufen der Hilfefunktion
`% Ambiguous command: „show con"`	Sie haben nicht genügend Zeichen eingegeben, daher wurde der Befehl vom Router nicht erkannt.	Geben Sie den Befehl erneut ein, gefolgt von einem Fragezeichen (**?**), wobei zwischen dem Befehl und dem Fragezeichen jedoch kein Leerzeichen stehen darf. Die möglichen Schlüsselwörter, die Sie für die betreffenden Befehle eingeben können, werden dann angezeigt.

Tabelle A-3 Allgemeine CLI-Fehlermeldungen (Fortsetzung)

Fehlermeldung	Bedeutung	Aufrufen der Hilfefunktion
`% Incomplete command.`	Sie haben nicht alle für diesen Befehl erforderlichen Schlüsselwörter oder Werte eingegeben.	Geben Sie den Befehl erneut ein, gefolgt von einem Fragezeichen (**?**), wobei zwischen dem Befehl und dem Fragezeichen jedoch kein Leerzeichen stehen darf. Die möglichen Schlüsselwörter, die Sie für die betreffenden Befehle eingeben können, werden dann angezeigt.
`% Invalid input detected at '^' marker.`	Sie haben den betreffenden Befehl falsch eingegeben. Die fehlerhafte Stelle wird durch das Auslassungszeichen (^) gekennzeichnet.	Geben Sie ein Fragezeichen (**?**) ein, um alle Befehle anzuzeigen, die in diesem speziellen Befehlsmodus verfügbar sind.

Speichern von Konfigurationsänderungen

Wenn Sie die von Ihnen vorgenommenen Konfigurationsänderungen im nichtflüchtigen RAM-Speicher (NVRAM) speichern möchten, damit diese beim Neuladen des Systems oder bei einem Stromausfall nicht gelöscht werden, geben Sie den Befehl **copy running-config startup-config** ein. Im folgenden Beispiel ist die Verfahrensweise zum Speichern der Änderungen mit diesem Befehl verdeutlicht:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

Drücken Sie die **Eingabetaste**, um den standardmäßigen Zieldateinamen (destination filename) *startup-config* zu übernehmen, oder geben Sie einen gewünschten Dateinamen als Ziel ein, und drücken Sie die **Eingabetaste**.

Unter Umständen dauert es ein bis zwei Minuten, bis die Konfiguration im NVRAM gespeichert ist. Nach dem Speichern der Konfiguration wird folgende Meldung angezeigt:

```
Building configuration...
Router#
```

Zusammenfassung

Nachdem Ihnen in diesem Kapitel einige Grundkenntnisse über die Cisco IOS-Software vermittelt wurden, können Sie mit der Konfiguration des Routers beginnen. Beachten Sie jedoch folgende Hinweise:

- Durch Eingabe eines Fragezeichens (**?**) und durch Navigation mit den Pfeiltasten können Sie eine Hilfefunktion aufrufen, die Sie bei der Eingabe der gewünschten Befehle unterstützt.
- In jedem Befehlsmodus gelten Beschränkungen, nach denen nur die Eingabe einer bestimmten Gruppe von Befehlen zulässig ist. Falls bei der Eingabe eines Befehls Probleme auftreten, überprüfen Sie die Eingabeaufforderung, und geben Sie dann ein Fragezeichen (**?**) ein, um eine Liste der verfügbaren Befehle anzuzeigen. Möglicherweise befinden Sie sich im falschen Befehlsmodus, oder Sie haben eine falsche Befehlssyntax verwendet.
- Wenn Sie eine Funktion deaktivieren möchten, geben Sie das Schlüsselwort **no** vor dem entsprechenden Befehl ein, z. B. **no ip routing**.
- Speichern Sie Ihre Konfigurationsänderungen im nichtflüchtigen RAM-Speicher (NVRAM), damit diese beim Neuladen des Systems oder bei einem Stromausfall nicht gelöscht werden.

Weitere Vorgehensweise

Wenn Sie den Router jetzt konfigurieren möchten, lesen Sie Kapitel 1, „Grundlegende Routerkonfiguration“, und Kapitel 2, „Beispiele für den Netzwerkeinsatz“.

Konzepte

Dieser Anhang enthält Erläuterungen und Definitionen von Schlüsselbegriffen, die Internetdienstanbietern oder Netzwerkadministratoren bei der Konfiguration von Cisco-Routern als Referenz dienen können. Einige typische Netzwerkszenarios sind in folgendem Kapitel dargestellt: Kapitel 2, „Beispiele für den Netzwerkeinsatz“. Informationen zu weiteren Details oder Konfigurationsfragen finden Sie in Kapitel 11, „Weitere Konfigurationsoptionen“.

Dieser Anhang enthält die folgenden Themen:

- ADSL
- SHDSL
- Netzwerkprotokolle
- Routingprotokolloptionen
- PPP-Authentifizierungsprotokolle
- TACACS+
- Netzwerkschnittstellen
- Reserve-Wählleitung
- NAT
- Easy IP (Phase 1)
- Easy IP (Phase 2)
- QoS
- Access-Listen

ADSL

ADSL ist eine Technologie, die eine Übertragung von Daten und Sprachsignalen über ein und dieselbe Leitung ermöglicht. ADSL ist eine paketbasierte Netzwerktechnologie. Sie ermöglicht Hochgeschwindigkeitsübertragungen über eine gewöhnliche verdrillte Teilnehmeranschluss-Kupferleitung (Twisted Pair-Kabel) zwischen der Ortsvermittlungsstelle eines Network-Service-Providers (NSP, Anbieter von Telefondiensten) und dem Endnutzer („letzte Meile“) bzw. über Teilnehmeranschlussleitungen, die in einem Gebäude oder auf dem Gelände einer Organisation eingerichtet wurden.

Der Vorteil von ADSL gegenüber einer seriellen Datenübertragungsleitung oder einer Wählleitung besteht darin, dass ADSL stets aktiviert und verbunden ist und, verglichen mit einer Wähl- oder Standleitung, bei ADSL eine höhere Bandbreite zur Verfügung steht sowie geringere Kosten verursacht werden. Durch die ADSL-Technologie werden Daten asymmetrisch, d. h. unterschiedlich schnell übertragen. Die Bandbreite auf der Strecke von der Vermittlungsstelle des NSP zum Kunden ist somit größer als die Bandbreite, die für Übertragungen vom Kunden zur Vermittlungsstelle verfügbar ist. Durch diese Asymmetrie, verbunden mit der Fähigkeit einer dauerhaften Verbindung (kein Verbindungsaufbau nötig), ist ADSL ideal für das Surfen im Internet und in Intranets, für Video-on-Demand-Dienste sowie für den Remote-LAN-Zugriff geeignet.

SHDSL

SHDSL ist eine auf G.SHDSL (G.991.2)-Standard aufbauende Technologie, die Übertragungen von Daten und Sprachsignalen über ein und dieselbe Leitung ermöglicht. SHDSL ist ebenfalls eine paketbasierte Netzwerktechnologie, die Hochgeschwindigkeitsübertragungen über eine verdrillte Teilnehmeranschluss-Kupferleitung zwischen der Ortsvermittlungsstelle eines Network-Service-Providers (NSP) und dem Endnutzer ermöglicht bzw. über Teilnehmeranschlussleitungen, die in einem Gebäude oder auf dem Gelände einer Organisation eingerichtet wurden.

Mit G.SHDSL-Geräten kann die Reichweite von Vermittlungsstellen und Fernterminals bei einer symmetrischen Datenübertragungsrate von 72 kbit/s auf bis zu 2,3 Mbit/s gesteigert werden (Reichweite ca. 7.925 m). Darüber hinaus kann die Leitung bei geringeren Geschwindigkeiten gebündelt werden, so dass der Reichweite kaum Grenzen gesetzt sind.

SHDSL-Technologie wird als symmetrisch bezeichnet, da die Bandbreite in beiden Richtungen, d. h. von der Vermittlungsstelle zum Endnutzer und umgekehrt, jeweils gleich ist. Aufgrund dieser Symmetrie bei der Übertragung, verbunden mit einer ständigen Verfügbarkeit der Verbindung (kein Verbindungsaufbau erforderlich), ist SHDSL für den LAN-Zugang hervorragend geeignet.

Netzwerkprotokolle

Netzwerkprotokolle ermöglichen es dem Netzwerk, Daten über LAN- oder WAN-Verbindungen von der Datenquelle zu einem bestimmten Ziel weiterzuleiten. In den Netzwerkprotokollen sind Routingadresstabellen enthalten, die jeweils den günstigsten Weg für die Durchleitung der Daten durch das Netzwerk angeben.

IP

IP ist das gebräuchlichste und bekannteste Protokoll der TCP/IP-Protokollgruppe (Transmission Control Protocol/Internet Protocol, Protokoll für die Übertragungskontrolle/Internetprotokoll) auf der Netzverbundschicht und bietet einen grundlegenden Paketübertragungsdienst für alle TCP/IP-Netzwerke. Zusätzlich zu den Adressen physischer Knoten wird durch das IP-Protokoll ein System logischer Hostadressen implementiert, die als IP-Adressen bezeichnet werden. Diese IP-Adressen werden durch die Netzverbundschicht und höhere Schichten zur Identifizierung von Geräten und zur Ausführung des netzüberschreitenden Routing verwendet. Mithilfe des Adressauflösungsprotokolls (ARP, Address Resolution Protocol) kann IP die physische Adresse für eine bestimmte IP-Adresse ermitteln.

IP wird von allen Protokollen in den darüber und darunter liegenden Netzwerkschichten zur Übertragung von Daten verwendet. Dies bedeutet, dass alle TCP/IP-Daten unabhängig von ihrem Bestimmungsort beim Senden und Empfangen das IP-Protokoll durchlaufen.

IP ist ein verbindungsloses Protokoll, d. h. IP tauscht vor der Verbindungsherstellung und der Datenübertragung keine Steuerungsinformationen (*Handshake*) aus. Im Gegensatz dazu werden bei einem verbindungsorientierten Protokoll Steuerungsinformationen mit dem Remotecomputer ausgetauscht, um vor dem Senden von Daten zu überprüfen, ob dieser Computer zum Empfang der Daten bereit ist. Nach erfolgreichem Abschluss des Handshake-Vorgangs ist zwischen den Computern eine Verbindung hergestellt. Falls verbindungsorientierte Protokolle erforderlich sind, stützt sich IP bei der Verbindungsherstellung auf Protokolle in anderen Schichten.

IPX (Internet Packet Exchange) verwendet zum Austausch von Routinginformationen das Protokoll RIP (Routing Information Protocol), ein dynamisches Routingprotokoll mit Distance-Vector-Algorithmus. RIP wird in den folgenden Abschnitten ausführlich beschrieben.

Routingprotokolloptionen

Folgende Protokolle sind Routingprotokolle:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)

Die Unterschiede zwischen RIP und Enhanced IGRP sind in Tabelle B-1 erläutert.

Tabelle B-1 Vergleich zwischen RIP und Enhanced IGRP

Protokoll	Ideale Topologie	Metrik	Routing-Updates
RIP	Geeignet für Topologien mit höchstens 15 Hops.	Zahl der Hops. Die maximale Anzahl von Hops beträgt 15. Als beste Route gilt die mit der geringsten Hop-Zahl.	Standardmäßig alle 30 Sekunden. Sie können diesen Wert neu konfigurieren und außerdem gesteuerte RIP-Erweiterungen verwenden.
Enhanced IGRP	Geeignet für große Topologien mit 16 oder mehr Hops bis zum Ziel.	Entfernungsinformationen. Basierend auf einem Nachfolger, d. h. einem benachbarten Router, der über einen Least-Cost-Pfad zu einem Ziel verfügt, das mit Sicherheit nicht Bestandteil einer Routingschleife ist.	Hello-Pakete werden alle 5 Sekunden gesendet; inkrementelle Updates werden gesendet, wenn sich der Zustand eines Ziels ändert.

RIP

RIP ist ein IP zugeordnetes Protokoll, welches das Routing von Protokolldatenverkehr über das Internet regelt. RIP ist ein Routingprotokoll mit Distance-Vector-Algorithmus, d. h. dass die Entfernung (Zahl der Hops) als Metrik für die Routenauswahl verwendet wird. Die *Zahl der Hops* bezeichnet die Anzahl der Router, die ein Datenpaket bis zum entsprechenden Ziel durchlaufen muss. Wenn beispielsweise auf einer bestimmten Route die Zahl der Hops 2 beträgt, muss ein Paket durch zwei Router geleitet werden, um sein Ziel zu erreichen.

Standardmäßig werden RIP-Routing-Updates alle 30 Sekunden per Broadcast gesendet. Sie können das Intervall neu konfigurieren, mit dem Routing-Updates gesendet werden. Sie können ebenfalls gesteuerte Erweiterungen für RIP konfigurieren, so dass Routing-Updates nur dann gesendet werden, wenn die Routingdatenbank aktualisiert wird. Weitere Informationen über gesteuerte Erweiterungen für RIP finden Sie in der Dokumentation zu Cisco IOS Release 12.3.

Enhanced IGRP

Enhanced IGRP ist ein erweitertes proprietäres Distance-Vector- und Verbindungsstatus-Routingprotokoll von Cisco, d. h. zur Routenauswahl wird eine komplexere Metrik als die Entfernung (Zahl der Hops) verwendet. Die von Enhanced IGRP angewendete Metrik basiert auf einem Nachfolger, d. h. einem benachbarten Router, der einen Least-Cost-Pfad zu einem Ziel bereitstellt, das mit Sicherheit nicht Bestandteil einer Routingschleife ist. Falls ein Nachfolger für ein bestimmtes Ziel nicht vorhanden ist, jedoch benachbarte Router das Ziel ankündigen, muss der Router eine Route neu berechnen.

Jeder Router, auf dem das Protokoll Enhanced IGRP ausgeführt wird, sendet alle 5 Sekunden so genannte Hello-Pakete, um benachbarten Routern die eigene Funktionsfähigkeit zu signalisieren. Falls ein bestimmter Router innerhalb eines vorgeschriebenen Zeitraums kein Hello-Paket sendet, nimmt Enhanced IGRP an, dass sich der Zustand eines Ziels geändert hat, und sendet daher ein inkrementelles Update.

Da Enhanced IGRP Unterstützung für IP bietet, brauchen Sie nur ein Routingprotokoll für Mehrprotokoll-Netzwerkumgebungen einzusetzen und können somit die Größe der Routingtabellen sowie den Umfang der Routinginformationen minimieren.

PPP-Authentifizierungsprotokolle

Durch das Point-to-Point-Protokoll (PPP) werden Netzwerkschicht-Protokollinformationen über Punkt-zu-Punkt-Verbindungen gekapselt.

PPP wurde ursprünglich als Kapselungsprotokoll zur Übertragung von IP-Datenverkehr über Punkt-zu-Punkt-Verbindungen konzipiert. Durch PPP wurde ebenfalls ein Standard für die Zuweisung und Verwaltung von IP-Adressen, asynchrone (Start/Stopp) und bitorientierte synchrone Kapselung, Netzwerkprotokoll-Multiplexing, Verbindungskonfiguration, Verbindungsqualitätsprüfung, Fehlererkennung und Optionsaushandlung für Funktionen begründet, wie z. B. die Netzwerkschicht-Adressenverhandlung und Datenkomprimierungsverhandlung. PPP unterstützt diese Funktionen durch Bereitstellung des erweiterbaren Protokolls LCP (Link Control Protocol) und einer Gruppe von NCPs (Network Control Protocols) zur Aushandlung optionaler Konfigurationsparameter und -funktionen.

Die aktuelle PPP-Implementierung unterstützt zwei Sicherheitsauthentifizierungsprotokolle zur Authentifizierung einer PPP-Sitzung:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

PPP mit PAP- oder CHAP-Authentifizierung wird häufig eingesetzt, um den zentralen Standort darüber zu informieren, mit welchen Remote-Routern er verbunden ist.

PAP

PAP verwendet ein bidirektionales Handshake-Verfahren, um die Kennwörter von Routern zu überprüfen. Zur Verdeutlichung der Funktionsweise von PAP müssen Sie sich eine Netzwerktopologie vorstellen, in der ein Cisco-Router an einem entfernten Standort mit einem Cisco-Router im zentralen Büro des Unternehmens verbunden ist. Nachdem die PPP-Verbindung hergestellt ist, sendet der Router am entfernten Standort einen konfigurierten Benutzernamen und ein festgelegtes Kennwort, bis der Router im Unternehmensbüro die Authentifizierung akzeptiert.

PAP bietet folgende Merkmale:

- Der Kennwortteil der Authentifizierung wird in der Verbindung als Klartext übertragen (nicht per Scrambling vermischt oder verschlüsselt).
- PAP bietet keinen Schutz vor Playback- oder wiederholten Trial-and-Error-Angriffen.
- Der Router am entfernten Standort steuert die Frequenz und den zeitlichen Ablauf der Authentifizierungsversuche.

CHAP

CHAP verwendet ein dreiseitiges Handshake-Verfahren zur Kennwortverifizierung. Stellen Sie sich zur Verdeutlichung der Funktionsweise von CHAP eine Netzwerktopologie vor, in der ein Cisco-Router an einem entfernten Standort mit einem Cisco-Router im Büro des Unternehmens verbunden ist.

Nachdem die PPP-Verbindung hergestellt wurde, sendet der Router am Unternehmenssitz eine Abfragemeldung an den am entfernten Standort befindlichen Router. Der Router am entfernten Standort beantwortet diese Abfrage mit einem Variablenwert. Der Router im Büro des Unternehmens überprüft diese Antwort anhand einer eigenen Berechnung des Wertes. Wenn diese beiden Werte übereinstimmen, übernimmt der Router im Unternehmensbüro die Authentifizierung. Der Authentifizierungsvorgang kann nach Herstellung der Verbindung jederzeit wiederholt werden.

CHAP bietet folgende Merkmale:

- Beim Authentifizierungsvorgang wird kein Kennwort, sondern ein variabler Abfragewert verwendet.
- CHAP bietet mit diesem variablen Abfragewert Schutz vor Playback-Angriffen, da der Wert eindeutig und nicht im Voraus bestimmbar ist. Durch wiederholte Abfragen wird die Zeitspanne begrenzt, während der eine mögliche Gefährdung durch Angriffe besteht.
- Der Router im Büro am Unternehmensstandort steuert die Frequenz und den zeitlichen Ablauf der Authentifizierungsversuche.

Hinweis Cisco empfiehlt die Verwendung von CHAP, da dieses Protokoll ein höheres Sicherheitsniveau als PAP bietet.

TACACS+

Router der Cisco 850-Serie und Cisco 870-Serie unterstützen das Protokoll TACACS+ (Terminal Access Controller Access Control System Plus) über Telnet. TACACS+ ist ein von Cisco entwickeltes Authentifizierungsprotokoll, das eine Authentifizierung per Remotezugriff sowie diesbezügliche Netzwerksicherheitsdienste ermöglicht, z. B. die Ereignisprotokollierung. Benutzerkennwörter werden nicht in den einzelnen Routern, sondern in einer zentralen Datenbank verwaltet. TACACS+ bietet darüber hinaus Unterstützung für separate, modulare Authentifizierungs-, Autorisierungs- und Abrechnungsfunktionen (AAA), die auf den einzelnen Routern konfiguriert werden.

Netzwerkschnittstellen

In diesem Abschnitt werden die Netzwerkschnittstellenprotokolle beschrieben, die von den Routern der Cisco 850-Serie und Cisco 870-Serie unterstützt werden. Folgende Netzwerkschnittstellenprotokolle werden unterstützt:

- Ethernet
- ATM for DSL

Ethernet

Ethernet ist ein LAN-Basisbandprotokoll, das Daten- und Sprachpakete mit CSMA/CD (Carrier Sense Multiple Access/Collision Detection, Trägermessung bei Mehrfachzugriff mit Kollisionserkennung) an die WAN-Schnittstelle überträgt. Dieser Begriff ist mittlerweile sehr gebräuchlich und wird häufig in Bezug auf alle CSMA/CD-LANs verwendet. Ethernet war zunächst für den Einsatz in Netzwerken mit sporadischen, gelegentlich hohen Datenverkehrsanforderungen konzipiert. Die IEEE 802.3-Spezifikation wurde dann 1980 auf Grundlage der ursprünglichen Ethernet-Technologie entwickelt.

Unter dem Ethernet CSMA/CD-Medienzugriffsprozess kann jeder Host in einem CSMA/CD-LAN jederzeit auf das Netzwerk zugreifen. Vor dem Senden von Daten überwachen CSMA/CD-Hosts das Netzwerk in Bezug auf Datenverkehr. Ein Host, der Daten senden möchte, wartet mit dem Sendevorgang, bis kein Datenverkehr festgestellt wird. Ethernet gestattet jedem Host im Netzwerk, Daten zu übermitteln, sobald das Netzwerk frei ist. Zu einer so genannten Kollision kommt es, wenn zwei Hosts den Datenverkehr abhören und bei einer Pause im Datenverkehr gleichzeitig senden. In dieser Situation sind beide Übertragungen beschädigt, so dass die Hosts ihre Sendungen zu einem späteren Zeitpunkt wiederholen müssen. Durch spezielle Algorithmen wird bestimmt, wann die kollidierenden Hosts ihre Daten erneut senden sollten.

ATM for DSL

ATM (Asynchroner Transfer-Modus) ist ein Multiplexing- und Switching-Protokoll für Hochgeschwindigkeitsübertragungen, das mehrere Datenverkehrstypen unterstützt, z. B. Sprache, Daten, Video und Imaging.

ATM ist aus Zellen mit fester Länge zusammengesetzt, durch die alle Informationen für das Netzwerk per Switching und Multiplexing vermittelt werden. Eine ATM-Verbindung wird verwendet, um Datenbits an einen Zielrouter oder -host zu übertragen. Ein ATM-Netzwerk wird als LAN mit hoher

verfügbarer Bandbreite angesehen. Im Unterschied zu einem verbindungslosen LAN sind für ATM bestimmte Leistungsmerkmale erforderlich, damit eine LAN-Umgebung für Benutzer bereitgestellt werden kann.

Jeder ATM-Knoten muss eine separate Verbindung mit jedem einzelnen Knoten im ATM-Netzwerk herstellen, mit dem kommuniziert werden muss. Alle derartigen Verbindungen werden über einen Permanent Virtual Circuit (PVC, feste virtuelle Verbindung) hergestellt.

PVC

Ein Permanent Virtual Circuit (PVC) ist eine Verbindung zwischen Remotehosts und Routern. Ein PVC wird für jeden ATM-Endknoten hergestellt, mit dem der Router kommuniziert. Die beim Erstellen des PVC eingerichteten Kenndaten werden durch die ATM-Adaptionsschicht (AAL, ATM Adaptation Layer) und den Kapselungstyp bestimmt. Eine AAL definiert die Konvertierung der Benutzerinformationen in Zellen. Durch die AAL werden Informationen der oberen Schicht am Sender in Zellen segmentiert; diese Zellen werden am Empfänger wieder zu Informationen zusammengesetzt.

Cisco-Router unterstützen das AAL5-Format, das einen optimierten Datentransportdienst bietet. Vorteile dieses Dienstes sind ein geringerer Verwaltungsaufwand und bessere Fehlererkennungs- und -korrekturfunktionen im Vergleich zu AAL3/4. AAL5 wird in der Regel VBR-Datenverkehr (Variable Bit Rate) und UBR-Datenverkehr (Unspecified Bit Rate) zugeordnet.

ATM-Kapselung bezeichnet das Verpacken von Daten in einem bestimmten Protokollheader. Der Typ des Routers, mit dem Sie eine Verbindung herstellen, bestimmt den Typ der ATM-PVC-Kapselung.

Die Router unterstützen die folgenden Kapselungstypen für ATM-PVCs:

- LLC/SNAP (RFC 1483)
- VC-MUX (RFC 1483)
- PPP (RFC 2364)

Jeder Permanent Virtual Circuit (PVC) wird als eine vollständige und separate Verbindung mit einem Zielknoten betrachtet. Benutzer können Daten je nach Bedarf über die Verbindung kapseln. Die Dateninhalte werden vom ATM-Netz ignoriert. Als einzige Anforderung gilt, dass die Daten in einer Art und Weise an das ATM-Subsystem des Routers gesendet werden müssen, die dem jeweiligen AAL-Format entspricht.

Dialer-Schnittstelle

Durch eine Dialer-Schnittstelle werden PPP-Funktionen (z. B. Authentifizierung und IP-Adresszuweisungsmethode) einem PVC zugewiesen. Dialer-Schnittstellen werden bei der Konfiguration von PPP über ATM verwendet.

Dialer-Schnittstellen können unabhängig von physischen Schnittstellen konfiguriert und je nach Bedarf dynamisch angewendet werden.

Reserve-Wählleitung

Die Funktion der Reserve-Wählleitung bietet Schutz vor WAN-Ausfallzeiten, indem es Benutzern ermöglicht wird, eine Modemverbindung als Reserveleitung zu konfigurieren. In den folgenden Themen sind die verschiedenen Verfahren zum Aufrufen der Funktion für die Reserve-Wählleitung in der Cisco IOS-Software erläutert:

- Reserveschnittstelle
- Statische Floating-Routen
- Dialer-Überwachung

Reserveschnittstelle

Eine Reserveschnittstelle ist eine Schnittstelle, die im Ruhezustand verbleibt, bis bestimmte Umstände eintreten, z. B. Ausfall des WANs, die zur Aktivierung dieser Schnittstelle führen. Die Reserveschnittstelle kann eine physische Schnittstelle, z. B. ein ISDN-Basisanschluss (Basic Rate Interface, BRI), oder eine zugewiesene Reserve-Dialer-Schnittstelle sein, die in einem Dialer-Pool verwendet wird. Bei aktiver Primärleitung befindet sich die Reserveschnittstelle im Standby-Modus. Im Standby-Modus ist die Reserveschnittstelle effektiv abgeschaltet, bis sie wieder aktiviert wird. Der Reserveschnittstelle zugeordnete Routen werden in der Routingtabelle nicht angezeigt.

Da der Befehl für die Reserveschnittstelle von der Fähigkeit des Routers zur Erkennung des ausgeschalteten Zustands abhängt, wird diese Schnittstelle häufig zur Sicherung von ISDN-BRI-Verbindungen, asynchronen Verbindungen sowie Standleitungen eingesetzt. Die Schnittstellen mit derartigen Verbindungen werden beim Ausfall der Hauptleitung deaktiviert. Von der Reserveschnittstelle werden diese Ausfälle schnell erkannt.

Statische Floating-Routen

Statische Floating-Routen (Floating Static Routes) sind statische Routen, bei denen die administrative Distanz größer ist als bei dynamischen Routen. Administrative Distanzen können auf einer statischen Route konfiguriert werden, so dass diese statische Route im Vergleich zur dynamischen Route ungünstiger ist. Somit wird die statische Route nicht genutzt, wenn die entsprechende dynamische Route verfügbar ist. Bei einem Verlust der dynamischen Route kann jedoch die statische Route aktiviert werden, so dass der Datenverkehr dann über diese alternative Route gesendet werden kann. Falls diese alternative Route eine DDR-Schnittstelle (Dial-on-Demand Routing) verwendet, kann diese Schnittstelle als Reservefunktion dienen.

Dialer-Überwachung

Die Dialer-Überwachung (Dialer Watch) ist eine Sicherungsfunktion, die zur Integration der Reserve-Wählleitung in Routingfunktionen dient. Die Dialer-Überwachung bietet eine zuverlässige Verbindung, ohne dass der gesuchte Datenverkehr definiert werden muss, durch den ausgehende Anrufe am zentralen Router ausgelöst werden. Die Dialer-Überwachung kann daher als reguläres Dial-on-Demand-Routing angesehen werden, bei dem keine Anforderungen bezüglich des gesuchten Datenverkehrs gelten. Wenn Sie eine Gruppe überwachter Routen zur Definition der primären Schnittstelle konfigurieren, können Sie den Status der primären Schnittstelle überwachen und verfolgen, während überwachte Routen hinzugefügt und gelöscht werden.

Wenn eine überwachte Route gelöscht wird, sucht die Dialer-Überwachung mindestens eine gültige Route für jede der überwachten IP-Adressen oder Netzwerke. Falls keine gültige Route vorhanden ist, wird die primäre Leitung als ausgefallen und nicht verwendbar angesehen. Falls eine gültige Route für mindestens eines der überwachten IP-Netzwerke definiert ist und die Route nicht auf die für die Dialer-Überwachung als Reserveschnittstelle konfigurierte, sondern eine andere Schnittstelle verweist, wird die primäre Leitung als funktionsfähig angesehen. Folglich wird in diesem Fall die Reserveverbindung durch die Dialer-Überwachung nicht aktiviert.

NAT

Die Netzadress-Übersetzung (NAT, Network Address Translation) bietet einen Mechanismus, mit dem Zugriffe aus einem privat adressierten Netzwerk auf registrierte Netzwerke, z. B. das Internet, ausgeführt werden können, ohne dass eine registrierte Subnetzadresse erforderlich ist. Durch diesen Mechanismus entfällt die nötige Neunummerierung von Hosts, so dass ein und derselbe IP-Adressbereich in mehreren Intranets verwendet werden kann.

NAT wird auf dem Router konfiguriert, der sich an der Grenze eines *inneren Netzwerks* (ein Netzwerk, das nicht registrierte IP-Adressen verwendet) und eines *äußeren Netzwerks* (ein Netzwerk, das global eindeutige IP-Adressen verwendet; in diesem Fall das Internet) befindet. Durch NAT werden die lokalen inneren Adressen (nicht registrierte IP-Adressen, die Hosts im inneren Netzwerk zugewiesen sind) in global eindeutige IP-Adressen übersetzt, bevor Pakete an das äußere Netzwerk gesendet werden.

Mit NAT können im inneren Netzwerk weiterhin die bestehenden privaten oder veralteten Adressen verwendet werden. Diese Adressen werden vor der Weiterleitung von Paketen an das äußere Netzwerk in zulässige Adressen umgewandelt. Diese Übersetzungsfunktion ist mit dem Standardrouting kompatibel und nur auf Routern erforderlich, die ein inneres Netzwerk mit einer externen Domäne verbinden.

Übersetzungen können statisch oder dynamisch erfolgen. Eine statische Adressübersetzung stellt eine Eins-zu-Eins-Zuordnung (eineindeutig) zwischen dem inneren Netzwerk und der äußeren Domäne her. Dynamische Adressübersetzungen werden definiert, indem die für die Übersetzung bestimmten lokalen Adressen und der Adressenpool beschrieben werden, aus dem die externen Adressen zugewiesen werden sollen. Die Zuordnung erfolgt in numerischer Reihenfolge. Es können auch mehrere Pools benachbarter Adressblöcke definiert werden.

Durch den NAT-Mechanismus entfällt die ansonsten nötige Neuadressierung sämtlicher Hosts, die einen externen Zugriff benötigen, so dass Zeit und Kosten eingespart werden. Adressen können durch Multiplexing auf Anwendungsebene beibehalten werden. Mit NAT können interne Hosts eine einzelne registrierte IP-Adresse jeweils für alle externen Datenverbindungen gemeinsam nutzen. Bei diesem Konfigurationstyp werden nur eine relativ geringe Anzahl externer Adressen zur Unterstützung vieler interner Hosts benötigt, so dass zugeordnete IP-Adressen beibehalten werden können.

Da das Adressierungsschema im internen Netzwerk unter Umständen mit den im Internet bereits zugewiesenen registrierten Adressen in Konflikt gerät, kann NAT einen separaten Adresspool für sich überschneidende Netzwerke unterstützen und Adressen dementsprechend übersetzen.

Easy IP (Phase 1)

Die Funktion Easy IP (Phase 1) verbindet Network Address Translation (NAT) mit PPP/Internet Protocol Control Protocol (IPCP). Mit dieser Funktion kann ein Cisco-Router automatisch eine eigene registrierte IP-Adresse für die WAN-Schnittstelle von einem zentralen Server beziehen. Alle Remotehosts können dann mit dieser registrierten IP-Adresse auf das Internet zugreifen. Da Easy IP (Phase 1) die vorhandene Multiplex-NAT-Funktionalität auf Portebene aus der Cisco IOS-Software nutzt, sind die IP-Adressen im Remote-LAN für das Internet nicht sichtbar.

Die Funktion Easy IP (Phase 1) kombiniert NAT und PPP/IPCP. Mit NAT übersetzt der Router die von LAN-Geräten verwendeten, nicht registrierten IP-Adressen in eine global eindeutige IP-Adresse, die von der Dialer-Schnittstelle verwendet wird. Die Funktion zur Nutzung einer global eindeutigen IP-Adresse durch mehrere LAN-Geräte wird als *Overloading* bezeichnet. NAT wird auf dem Router konfiguriert, der sich an der Grenze eines inneren Netzwerks (Netzwerk, das nicht registrierte IP-Adressen verwendet) und eines äußeren Netzwerks (Netzwerk, das global eindeutige IP-Adressen verwendet; in diesem Fall das Internet) befindet.

Mit PPP/IPCP können Cisco-Router automatisch eine global eindeutige (registrierte) IP-Adresse für die Dialer-Schnittstelle aushandeln und vom ISP-Router beziehen.

Easy IP (Phase 2)

Die Funktion Easy IP (Phase 2) kombiniert DHCP-Server und -Relay (Dynamic Host Configuration Protocol). DHCP ist ein Client-Server-Protokoll, das es Geräten in einem IP-Netzwerk (den DHCP-Clients) ermöglicht, Konfigurationsinformationen von einem DHCP-Server abzufragen. DHCP weist die Netzwerkadressen je nach Bedarf aus einem zentralen Pool zu. Mit DHCP lassen sich IP-Adressen Hosts zuweisen, die nur vorübergehend mit dem Netzwerk verbunden sind. Darüber hinaus kann mit DHCP ein begrenzter Pool mit IP-Adressen von verschiedenen Hosts, die keine ständigen IP-Adressen benötigen, gemeinsam genutzt werden.

Mit DHCP müssen Sie nicht mehr jedem einzelnen Client eine IP-Adresse manuell zuweisen.

DHCP konfiguriert den Router zur Weiterleitung von UDP-Broadcasts, einschließlich IP-Adressanforderungen, von DHCP-Clients. Durch folgende Merkmale ermöglicht DHCP einen höheren Automatisierungsgrad und sorgt für weniger Probleme bei der Netzwerkverwaltung:

- Es ist keine manuelle Konfiguration einzelner Computer, Drucker und freigegebener Dateisysteme mehr erforderlich.
- Die gleichzeitige Verwendung einer IP-Adresse durch zwei Clients wird verhindert.
- Konfiguration von einem zentralen Standort aus ist möglich.

QoS

In diesem Abschnitt werden die folgenden QoS-Parameter (Quality of Service, Dienstgüte) beschrieben:

- IP-Vorrang
- PPP-Fragmentierung und -Verschachtelung
- CBWFQ
- RSVP
- Low Latency Queuing

Der Begriff „Quality of Service“ (QoS, Dienstgüte) bezieht sich auf die Fähigkeit eines Netzwerks zur Bereitstellung eines optimierten Dienstes für ausgewählten Netzwerkdatenverkehr über verschiedene Technologien. Hierzu zählen beispielsweise ATM-, Ethernet- und IEEE 802.1-Netzwerke sowie Netzwerke mit IP-Routing, die eine oder alle dieser grundlegenden Technologien nutzen. Zu den Hauptzielen von QoS gehören eine fest zugeordnete Bandbreite, Jitter- und Latenzkontrolle (in manchen Fällen für Echtzeit- und interaktiven Datenverkehr erforderlich) sowie eine verbesserte Verlustcharakteristik. QoS-Technologien sind die Grundbausteine für zukünftige Geschäftsanwendungen in Unternehmens-, WAN- und Service-Provider-Netzwerken.

Zur Verbesserung der Sprachübertragungsleistung im Netz muss QoS im gesamten Netzwerk konfiguriert sein, nicht nur auf dem Router, auf dem VoIP ausgeführt wird. Jedoch sind nicht alle QoS-Verfahren für alle Netzwerkrouter geeignet. Edge-Router und Backbone-Router in Ihrem Netzwerk haben nicht unbedingt dieselbe Funktion. Die von diesen Routern ausgeführten QoS-Aufgaben können daher unter Umständen ebenfalls unterschiedlich sein. Um ein IP-Netzwerk für Echtzeit-Spachdatenübertragungen zu konfigurieren, müssen Sie somit die Funktionen der in Ihrem Netzwerk befindlichen Edge- und Backbone-Router berücksichtigen.

Mit QoS-Software werden komplexe Netzwerke in die Lage versetzt, verschiedenste vernetzte Anwendungen und Datenverkehrstypen zu steuern und prädiktiv zu bedienen. Nahezu jedes Netzwerk kann von QoS profitieren und eine Effizienzsteigerung im Netzwerkbetrieb erreichen, unabhängig davon, ob es sich um ein kleines Unternehmensnetz, einen Internetdienstanbieter oder ein konzernweites Netzwerk handelt.

IP-Vorrang

Mit IP-Vorrang (IP Precedence) lässt sich Datenverkehr in max. sechs Dienstklassen unterteilen (zwei weitere Klassen sind für den internen Gebrauch im Netzwerk reserviert). Durch Warteschlangenverfahren im Netzwerk kann mithilfe dieses Signals dann die Verarbeitung beschleunigt werden.

Mittels anderer Funktionen, z. B. durch regelbasiertes Routing und Committed Access Rate (CAR), kann eine Vorrangstellung bzw. Priorität auf Grundlage einer erweiterten Access-Listenklassifizierung festgelegt werden. Dies ermöglicht eine erhebliche Flexibilität für die Zuweisung einer Priorität, beispielsweise der Zuweisung durch die Anwendung oder den Benutzer bzw. der Zuweisung nach Ziel- und Quell-Subnetz usw. Normalerweise wird diese Funktionalität möglichst nah am Rand eines Netzwerks (oder der administrativen Domäne) eingesetzt, so dass jedes nachfolgende Netzwerkelement seine Dienste basierend auf der festgelegten Regel bereitstellen kann.

IP-Vorrang kann ebenfalls auf dem Host oder Netzwerkclient festgelegt werden, wobei die Signalisierung optional verwendet werden kann. Mit IP-Vorrang können Dienstklassen mithilfe von Netzwerkwarteschlangen-Mechanismen (wie z. B. Class-Based Weighted Fair Queueing [CBWFQ]) eingerichtet werden, wobei keine Änderungen an vorhandenen Anwendungen vorgenommen werden müssen und keine komplizierten Netzwerkanforderungen gelten.

PPP-Fragmentierung und -Verschachtelung

Mit Multiclass-Multilink-PPP-Interleaving lassen sich große Datenpakete in Mehrfachübermittlungsabschnitte kapseln und in kleinere Pakete fragmentieren, so dass die Verzögerungsanforderungen von Echtzeit-Datenverkehr erfüllt werden. Kleine Echtzeitpakete, die nicht in Mehrfachübermittlungsabschnitten gekapselt sind, werden zwischen den Fragmenten der größeren Pakete übertragen. Die Verschachtelungsfunktion stellt ebenfalls eine spezielle Übermittlungswarteschlange für die kleineren, verzögerungssensitiven Pakete bereit, so dass diese früher als die anderen Datenströme übermittelt werden können. Durch Interleaving werden die Verzögerungsgrenzen für verzögerungssensitive Pakete auf einer langsamen Verbindung bereitgestellt, die für sonstigen Best-Effort-Datenverkehr verwendet wird.

Im Allgemeinen wird Multilink-PPP mit Interleaving in Verbindung mit CBWFQ und RSVP oder IP-Vorrang eingesetzt, um die Übertragung von Sprachpaketen sicherzustellen. Verwenden Sie Multilink-PPP mit Interleaving und CBWFQ, um die Art und Weise der Datenverarbeitung zu definieren. Verwenden Sie Resource Reservation Protocol (RSVP) oder IP-Vorrang, um den Sprachpaketen eine höhere Priorität zuzuweisen.

CBWFQ

Im Allgemeinen wird Class-based Weighted Fair Queuing (CBWFQ) in Verbindung mit Multilink-PPP und Interleaving sowie RSVP oder IP-Vorrang verwendet, um die Übertragung von Sprachpaketen sicherzustellen. Durch die kombinierte Verwendung von CBWFQ und Multilink-PPP wird festgelegt, auf welche Weise Daten verwaltet werden sollen. RSVP oder IP-Vorrang dient der Prioritätszuweisung für Sprachdatenpakete.

Es gibt zwei Ebenen von Warteschlangen: ATM-Warteschlangen und Cisco IOS-Warteschlangen. CBWFQ wird auf Cisco IOS-Warteschlangen angewendet. Bei Erstellung eines PVC wird in Cisco IOS automatisch eine FIFO-Warteschlange (First-in-First-out) erstellt. Falls Sie zur Erstellung von Klassen CBWFQ verwenden und diese Klassen an ein PVC anhängen, wird eine Warteschlange für jede einzelne Klasse erstellt.

Durch CBWFQ wird sichergestellt, dass die Warteschlangen über eine ausreichende Bandbreite verfügen und der Datenverkehr einen berechenbaren Dienst erhält. Datenverkehrsströme mit geringem Umfang werden bevorzugt. Sehr umfangreiche Datenverkehrsströme teilen sich die verbleibende Kapazität und erhalten jeweils die gleiche oder eine proportionale Bandbreite.

RSVP

Mit RSVP können Router genügend Bandbreite auf einer Schnittstelle reservieren, um einen zuverlässigen und leistungsfähigen Betrieb in guter Qualität zu gewährleisten. Endsysteme können mit RSVP einen bestimmten QoS vom Netzwerk anfordern. Für Echtzeit-Datenverkehr ist ein konsistentes Netzwerk erforderlich. Ohne eine konsistente QoS-Funktionalität können bei Echtzeit-Datenverkehr unter Umständen Jitter, unzureichende Bandbreite, Laufzeitschwankungen oder Informationsverluste auftreten. RSVP funktioniert im Zusammenwirken mit den derzeitigen Warteschlangenmechanismen. Ob eine Reservierung implementiert wird, hängt vom Warteschlangenmechanismus der Schnittstelle ab (wie z. B. CBWFQ).

RSVP funktioniert bei PPP- und HDLC-Schnittstellen sowie ähnlichen Schnittstelle für eine bitserielle Datenübertragung reibungslos. In Multi-Access-LANs ist die einwandfreie Funktionsweise von RSVP nicht gewährleistet. RSVP kann einer dynamischen Access-Liste für Paketflüsse gleichgesetzt werden.

Sie sollten RSVP konfigurieren, um die Funktion von QoS zu gewährleisten, falls die nachstehend genannten Bedingungen auf Ihr Netzwerk zutreffen:

- Implementierung eines Sprachdatennetzes kleiner Größe;
- Verbindungen langsamer als 2 Mbit/s;
- Verbindungen weisen hohe Auslastung auf;
- Bestmögliche Sprachqualität wird benötigt.

Low Latency Queuing

Low Latency Queuing (LLQ) stellt eine Prioritätswarteschlange für die Übermittlung mit geringer Latenzzeit für Echtzeit-Datenverkehr bereit. Durch eine streng nach Priorität geordnete Warteschlangeneinreihung können verzögerungssensitive Daten aus der Warteschlange entfernt und zuerst gesendet werden (bevor die Pakete aus den anderen Warteschlangen entfernt werden). Auf diese Weise können solche verzögerungssensitiven Daten vor sonstigem Datenverkehr bevorzugt behandelt werden.

Access-Listen

Mit grundlegenden standardmäßigen und statischen erweiterten Access-Listen können Sie die Sitzungsfilterung annähernd definieren. Verwenden Sie dazu das mit dem Befehl **permit** eingerichtete Schlüsselwort. Mit diesem festgelegten Schlüsselwort werden TCP-Pakete nach eventuell gesetzten ACK- oder RST-Bits gefiltert. (Gesetzte ACK- oder RST-Bits geben an, dass das betreffende Paket nicht an erster Stelle in einer Sitzung steht und daher zu einer bereits bestehenden Sitzung gehört.) Dieses Filterkriterium wäre Bestandteil einer Access-Liste, die dauerhaft auf eine Schnittstelle angewendet wird.

ROM Monitor

Die Firmware ROM Monitor wird ausgeführt, wenn der Router eingeschaltet oder zurückgesetzt wird. Diese Firmware unterstützt die Initialisierung der Prozessorhardware und den Bootvorgang der Betriebssystemsoftware. Mit ROM Monitor lassen sich bestimmte Konfigurationsaufgaben ausführen, beispielsweise können Sie mit diesem Dienstprogramm ein Kennwort wiederherstellen oder Software über den Konsolenanschluss herunterladen. Falls auf einem Router kein Cisco IOS-Softwareabbild geladen ist, wird ROM Monitor auf diesem Router ausgeführt.

Dieser Anhang ist in folgende Abschnitte unterteilt:

Aufrufen von ROM Monitor

Zur Verwendung von ROM Monitor müssen Sie auf einem Terminal oder PC arbeiten, der über den Konsolenanschluss mit dem Router verbunden ist.

Führen Sie die folgenden Schritte aus, um den Router so zu konfigurieren, dass dieser beim nächsten Booten im ROM Monitor-Modus gestartet wird.

	Befehl	Zweck
Schritt 1	**enable**	Aktiviert den privilegierten EXEC-Modus. Geben Sie Ihr Kennwort ein, wenn Sie dazu aufgefordert werden.
Schritt 2	**configure terminal**	Mit diesem Befehl wird der globale Konfigurationsmodus aufgerufen.
Schritt 3	**config-reg 0x0**	Mit diesem Befehl wird das Konfigurationsregister zurückgesetzt.

	Befehl	Zweck
Schritt 4	**exit**	Mit diesem Befehl wird der globale Konfigurationsmodus beendet.
Schritt 5	**reload**	Durch Eingabe dieses Befehls wird der Router mit dem neuen Konfigurationsregisterwert neu gebootet. Der Router verbleibt im ROM Monitor-Modus, so dass die Cisco IOS-Software nicht gebootet wird. Wenn als Konfigurationswert 0x0 festgelegt ist, müssen Sie das Betriebssystem manuell über die Konsole starten. Weitere Informationen zum Befehl **boot** finden Sie im Abschnitt „Befehlsbeschreibungen“ in diesem Anhang. Nach dem erneuten Booten des Routers verbleibt dieser im ROM Monitor-Modus. Die Zahl in der Eingabeaufforderung erhöht sich mit jeder neuen Zeile.

Zeitersparnis Nach einem Neustart des Routers erfolgt stets eine Unterbrechung (Systemunterbrechung) mit einer Dauer von 60 Sekunden, unabhängig davon, ob diese Einstellung (Break) im Konfigurationsregister aktiviert oder deaktiviert ist. Während dieses 60-Sekunden-Zeitfensters können Sie durch Drücken der Pause-Taste zur ROM Monitor-Eingabeaufforderung wechseln.

ROM Monitor-Befehle

Geben Sie an der ROM Monitor-Eingabeaufforderung **?** oder **help** ein, um die nachstehend abgebildete Liste mit den verfügbaren Befehlen und Optionen anzuzeigen:

```
rommon 1 > ?
alias              set and display aliases command
boot               boot up an external process
break              set/show/clear the breakpoint
confreg            configuration register utility
cont               continue executing a downloaded image
context            display the context of a loaded image
cookie             display contents of cookie PROM in hex
copy               Copy a file-copy [-b <buffer_size>] <src_file> <dst_file>
delete             Delete file(s)-delete <filenames ...>
dir                List files in directories-dir <directory>
dis                display instruction stream
dnld               serial download a program module
format             Format a filesystem-format <filessystem>
frame              print out a selected stack frame
fsck               Check filesystem consistency-fsck <filesystem>
help               monitor builtin command help
history            monitor command history
meminfo            main memory information
mkdir              Create dir(s)-mkdir <dirnames ...>
more               Concatenate (type) file(s)-cat <filenames ...>
rename             Rename a file-rename <old_name> <new_name>
repeat             repeat a monitor command
reset              system reset
rmdir              Remove a directory
set                display the monitor variables
stack              produce a stack trace
sync               write monitor environment to NVRAM
sysret             print out info from last system return
tftpdnld           tftp image download
```

```
unalias            unset an alias
unset              unset a monitor variable
xmodem             x/ymodem image download
```

Bei der Eingabe der Befehle muss die Groß- und Kleinschreibung beachtet werden. Sie können jeden Befehl durch Drücken der Pause-Taste auf einem Terminal stoppen. Bei Verwendung eines PCs können Befehle in den meisten Terminal-Emulationsprogrammen durch gleichzeitiges Drücken der Strg-Taste und der Pause-Taste angehalten werden. Falls Sie eine andere Art von Terminal-Emulator oder Terminal-Emulationssoftware verwenden, schlagen Sie in der Dokumentation des betreffenden Produkts nach, wie Sie einen Unterbrechungsbefehl senden können.

Befehlsbeschreibungen

In Tabelle C-1 sind die gebräuchlichsten ROM Monitor-Befehle beschrieben.

Tabelle C-1 Häufig verwendete ROM Monitor-Befehle

Befehl	Beschreibung
help oder **?**	Mit diesem Befehl wird eine Übersicht über alle verfügbaren ROM Monitor-Befehle angezeigt.

-?	Mit diesem Befehl werden Informationen zur Befehlssyntax angezeigt. Beispiel:
	`rommon 16 > dis -?`
	`usage: dis [addr] [length]`
	
	Die Ausgabe für diesen Befehl ist in Verbindung mit dem Download-Befehl **xmodem** etwas anders:
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

reset oder **i**	Mit diesem Befehl wird der Router zurückgesetzt und initialisiert, ähnlich einem Neustart.

dir *device***:**	Mit diesem Befehl werden die Dateien auf dem benannten Gerät aufgelistet, z. B. Dateien im Flash-Speicher:
	`rommon 4 > dir flash:`
	`Directory of flash:/`
	`2 -rwx 10283208 <date> c870-advsecurityk9-mz`
	`9064448 bytes available (10289152 bytes used)`

Boot-Befehle	Weitere Informationen über Boot-Befehle in ROM Monitor finden Sie im *Cisco IOS Configuration Fundamentals and Network Management Guide*.
b	Mit diesem Befehl wird das erste Speicherabbild im Flash-Speicher gebootet.
b flash: [*Dateiname*]	Mit diesem Befehl wird das Speicherabbild direkt von der ersten Partition des Flash-Speichers gebootet. Wenn Sie keinen Dateinamen eingeben, wird durch diesen Befehl das erste Abbild im Flash-Speicher gebootet.

Notfallwiederherstellung mit TFTP-Download

Bei der standardmäßigen Verfahrensweise zum Laden neuer Software auf den Router wird im privilegierten EXEC-Modus der Befehl **copy tftp flash** über die Befehlszeilenschnittstelle (CLI) der Cisco IOS-Software eingegeben. Wenn der Router jedoch die Cisco IOS-Software nicht booten kann, können Sie neue Software auch im ROM Monitor-Modus laden.

In diesem Abschnitt wird beschrieben, wie die Cisco IOS-Software von einem TFTP-Remote-Server in den Flash-Speicher des Routers geladen werden kann. Verwenden Sie den Befehl **tftpdnld** nur zur Wiederherstellung bei Notfällen, da durch diesen Befehl alle vorhandenen Daten im Flash-Speicher gelöscht werden, bevor ein neues Softwareabbild auf den Router heruntergeladen wird.

TFTP-Download-Befehlsvariablen

In diesem Abschnitt werden die Systemvariablen beschrieben, die im ROM Monitor-Modus festgelegt werden können und die beim TFTP-Downloadvorgang verwendet werden. Hierbei wird zwischen obligatorischen und optionalen Variablen unterschieden.

Hinweis Die Befehle in diesem Abschnitt müssen genau in der Schreibweise eingegeben werden, in der sie aufgeführt sind, d. h. die vorgegebene Groß- oder Kleinschreibung muss übernommen werden.

Vorgeschriebene Variablen

Folgende Variablen müssen mit den entsprechend aufgeführten Befehlen festgelegt werden, bevor der Befehl **tftpdnld** verwendet wird:

Variable	Befehl
IP-Adresse des Routers.	**IP_ADDRESS=** *IP_Adresse*
Subnetzmaske des Routers.	**IP_SUBNET_MASK=** *IP_Adresse*
IP-Adresse des Standard-Gateways des Routers.	**DEFAULT_GATEWAY=** *IP_Adresse*
IP-Adresse des TFTP-Servers, von dem die Software heruntergeladen wird.	**TFTP_SERVER=** *IP_Adresse*
Der Name der Datei, die auf den Router heruntergeladen wird.	**TFTP_FILE=** *Dateiname*

Optionale Variablen

Folgende Variablen müssen mit den entsprechend aufgeführten Befehlen festgelegt werden, bevor der Befehl **tftpdnld** verwendet werden kann:

Variable	Befehl
Durch diese Variable wird festgelegt, wie der Router den Fortschritt, d. h. den aktuellen Status des Dateidownloads anzeigt. 0 – Es wird kein Downloadstatus angezeigt. 1 – Der Status des Dateidownloads wird durch Ausrufezeichen (!!!) angezeigt. Dies ist die Standardeinstellung. 2 – Während des Dateidownloads wird jeweils ein detaillierter Status angezeigt. Beispiel: • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *Einstellung*
Anzahl der ARP- und TFTP-Downloadversuche des Routers. Die Standardeinstellung ist 7.	**TFTP_RETRY_COUNT=** *Anzahl_der_Wiederholungen*
Dauer in Sekunden, bis der Downloadvorgang aufgrund einer Zeitüberschreitung (Timeout) abgebrochen wird. Die Standardeinstellung ist 2.400 Sekunden (40 Minuten).	**TFTP_TIMEOUT=** *Dauer*
Mit dieser Variable wird festgelegt, ob der Router eine Prüfsummenkontrolle für das heruntergeladene Softwareabbild durchführt: 1 – Prüfsummenkontrolle wird ausgeführt. 0 – Es wird keine Prüfsummenkontrolle ausgeführt.	**TFTP_CHECKSUM=***Einstellung*

Verwenden des TFTP-Downloadbefehls

Führen Sie die folgenden Schritte im ROM Monitor-Modus aus, um eine Datei über TFTP herunterzuladen.

Schritt1 Geben Sie gemäß der Beschreibung in den vorhergehenden Abschnitten alle vorgeschriebenen Variablen und ggf. optionale Variablen mit den entsprechenden Befehlen ein.

Schritt2 Geben Sie den Befehl **tftpdnld** in folgender Syntax ein:

```
rommon 1 > tftpdnld -r
```

Hinweis Die Variable **-r** ist optional. Durch Eingabe dieser Variable wird die neue Software heruntergeladen und gebootet, jedoch nicht im Flash-Speicher gespeichert. Sie können dann bei der nächsten Eingabe des Befehls **reload** das im Flash-Speicher enthaltene Softwareabbild verwenden.

Die als Ausgabe angezeigten Daten sollten dem nachfolgenden Beispiel in etwa ähneln:

```
IP_ADDRESS: 10.3.6.7
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 10.3.0.1
TFTP_SERVER: 192.168.254.254
TFTP_FILE: c870-advsecurityk9-mz
Do you wish to continue? y/n:  [n]:
```

Schritt3 Wenn Sie sicher sind, dass Sie den Vorgang fortsetzen möchten, geben Sie als Antwort auf die an dieser Stelle angezeigte Frage **y** ein:

```
Do you wish to continue? y/n:  [n]:y
```

Der Router beginnt jetzt mit dem Herunterladen der neuen Datei.

Falls Sie irrtümlicherweise mit „y“ (Ja) geantwortet haben, können Sie die Übertragung durch Drücken der Tasten **Strg-C** oder **Pause** abbrechen, bevor der Flash-Speicher gelöscht wird.

Konfigurationsregister

Das virtuelle Konfigurationsregister befindet sich im nichtflüchtigen RAM-Speicher (NVRAM) und besitzt die gleiche Funktionalität wie bei anderen Cisco-Routern. Sie können das virtuelle Konfigurationsregister in ROM Monitor oder in der Betriebssystemsoftware anzeigen und bearbeiten. In ROM Monitor können Sie das Konfigurationsregister ändern, indem Sie den Registerwert im Hexadezimalformat eingeben oder indem Sie ROM Monitor jeweils eine Eingabeaufforderung für die Einstellung jedes Bit anzeigen lassen.

Manuelles Bearbeiten des Konfigurationsregisters

Zum manuellen Ändern des virtuellen Konfigurationsregisters in ROM Monitor geben Sie den Befehl **confreg** ein, gefolgt von dem neuen Wert des betreffenden Registers im Hexadezimalformat, wie im nachstehenden Beispiel dargestellt:

```
rommon 1 > confreg 0x2101


Damit die neue Konfiguration wirksam wird, müssen Sie den Router zurücksetzen bzw. aus-
und wieder einschalten.
rommon 2 >
```

Der Eingabewert wird stets als Hexadezimalwert interpretiert. Der neue virtuelle Konfigurationsregisterwert wird in den NVRAM geschrieben, ist jedoch erst nach dem Zurücksetzen oder erneuten Booten des Routers wirksam.

Bearbeiten des Konfigurationsregisters über Eingabeaufforderungen

Bei Eingabe des Befehls **confreg** ohne Argumente wird der Inhalt des virtuellen Konfigurationsregisters und eine Eingabeaufforderung zum Ändern des Inhalts mit einer Beschreibung für jedes Bit angezeigt.

In jedem Fall wird der neue virtuelle Konfigurationsregisterwert zwar in den NVRAM geschrieben, jedoch erst nach dem Zurücksetzen oder erneuten Booten des Routers wirksam.

Im folgenden Beispiel wird die Konfiguration mit dem Befehl **confreg** dargestellt:

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


Damit die neue Konfiguration wirksam wird, müssen Sie den Router zurücksetzen bzw. aus-
und wieder einschalten.
```

Konsolendownload

Mit dem Konsolendownload, einer ROM Monitor-Funktion, kann ein Softwareabbild oder eine Konfigurationsdatei über den Konsolenanschluss des Routers heruntergeladen werden. Nach dem Herunterladen wird die Datei im Mini-Flash-Speichermodul oder im Hauptspeicher zur Ausführung gespeichert (nur für Image-Dateien, d. h. Dateien des Softwareabbilds).

Verwenden Sie die Konsolendownloadfunktion, wenn kein Zugang zu einem TFTP-Server verfügbar ist.

Hinweis Wenn Sie ein Softwareabbild oder eine Konfigurationsdatei über den Konsolenanschluss auf den Router herunterladen möchten, müssen Sie hierzu den ROM Monitor-Befehl **dnld** verwenden.

Hinweis Falls Sie mit einem PC ein Abbild der Cisco IOS-Software über den Konsolenanschluss des Routers mit 115.200 Bit/s herunterladen, müssen Sie sicherstellen, dass der serielle Anschluss am PC einen 16550 UART (universell-asynchronen Receiver-Transmitter) verwendet. Falls am seriellen PC-Anschluss kein 16550 UART verwendet wird, sollten Sie beim Herunterladen des Cisco IOS-Softwareabbilds über den Konsolenanschluss eine Datenübertragungsgeschwindigkeit von 38.400 Bit/s oder eine geringere Datenrate einstellen.

Befehlsbeschreibung

Im nachstehenden Abschnitt werden die Syntax und Beschreibungen für den Konsolendownloadbefehl **xmodem** aufgeführt:

xmodem [-cyrx] *Zieldateiname*

c	Optional. Mit diesem Parameter wird der Downloadvorgang mit einer zyklischen 16-Bit-Blockprüfung (CRC-16) durchgeführt, die als Fehlerprüfung bei der Validierung von Paketen dient. Standardmäßig wird lediglich eine 8-Bit-CRC-Prüfung ausgeführt.
y	Optional. Mit diesem Parameter wird festgelegt, dass der Router den Downloadvorgang mit dem Protokoll „YModem“ ausführt. Standardmäßig wird jedoch das Protokoll „XModem“ verwendet. Die Protokolle unterscheiden sich wie folgt: • XModem unterstützt Übertragungen mit 128-Byte-Blockgröße. YModem hingegen unterstützt Übertragungen mit einer Blockgröße von 1.024 Byte. • YModem verwendet die Fehlerprüfmethode CRC-16 zur Validierung jedes Pakets. Je nachdem, von welchem Gerät die Software heruntergeladen wird, kann es vorkommen, dass diese Funktion durch XModem nicht unterstützt wird.
r	Optional. Bei Eingabe dieses Parameters wird das Abbild zur Ausführung in den DRAM-Speicher geladen. Standardmäßig wird das Abbild jedoch in den Flash-Speicher geladen.
x	Optional. Bei Eingabe dieses Parameters wird das Abbild in den DRAM-Speicher geladen, jedoch nicht ausgeführt.
Zieldateiname	Name der Systemabbilddatei oder der Systemkonfigurationsdatei. Damit der Router diese Datei erkennt, muss der Name der Konfigurationsdatei mit *router_confg* identisch sein.

Führen Sie die folgenden Schritte aus, um den Befehl „Xmodem“ auszuführen:

Schritt1 Verschieben Sie die Abbilddatei auf das lokale Laufwerk, auf dem „Xmodem“ ausgeführt werden soll.

Schritt2 Geben Sie den Befehl **xmodem** ein.

Fehlermeldungen

Da beim ROM Monitor-Konsolendownload die Konsole für die Datenübertragung verwendet wird, werden beim Auftreten von Fehlern während eines Datenübertragungsvorgangs die entsprechenden Fehlermeldungen erst nach Abschluss der Übertragung auf der Konsole angezeigt.

Wenn Sie anstelle der standardmäßigen Datenübertragungsrate eine andere Baudrate eingestellt haben, wird nach der Fehlermeldung eine weitere Meldung angezeigt, in der Sie aufgefordert werden, die im Konfigurationsregister angegebene Baudrate auf dem Terminal wiederherzustellen.

Debugging-Befehle

Die meisten ROM Monitor-Debugging-Befehle funktionieren nur bei einem Absturz der Cisco IOS-Software bzw. wenn die Ausführung der Software unterbrochen wurde. Wenn Sie einen Debugging-Befehl eingeben und keine Cisco IOS-Absturzinformationen verfügbar sind, wird folgende Fehlermeldung angezeigt:

```
"xxx: kernel context state is invalid, can not proceed."
```

Folgende Debugging-Befehle sind in ROM Monitor verfügbar:

- **stack** oder **k** – Generiert eine Stapelverfolgung (Stack Trace). Beispiel:

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context** – Zeigt den jeweiligen Prozessorkontext an. Beispiel:

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame** – Zeigt einen einzelnen Stapelframe an.
- **sysret** – Zeigt Rückgabeinformationen vom zuletzt gebooteten Systemabbild an. Diese Informationen umfassen den Grund für die Beendigung des Abbilds, einen Stapel-Speicherauszug von bis zu acht Frames und, sofern es sich um einen Ausnahmefehler handelt, die Speicheradresse, bei der dieser Ausnahmefehler aufgetreten ist. Beispiel:

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
```

```
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo** – Zeigt die Größe in Bytes, die Anfangsadresse, den verfügbaren Bereich des Hauptspeichers, den Anfangspunkt und die Größe des Paketspeichers sowie die NVRAM-Größe an. Beispiel:

```
rommon 9> meminfo
Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
IO (packet) memory size: 5 percent of main memory.
NVRAM size: 32KB
```

Beenden von ROM Monitor

Sie müssen das Konfigurationsregister für den Router auf einen Wert von 0x2 bis 0xF setzen, damit ein Cisco IOS-Abbild beim Start oder Neuladen aus dem Flash-Speicher gebootet wird.

Im folgenden Beispiel ist dargestellt, wie das Konfigurationsregister zurückgesetzt wird, so dass der Router ein im Flash-Speicher enthaltenes Cisco IOS-Abbild bootet:

```
rommon 1 > confreg 0x2101
```

Damit die neue Konfiguration wirksam wird, müssen Sie den Router zurücksetzen bzw. aus- und wieder einschalten:

```
rommon 2 > boot
```

Der Router bootet dann das Cisco IOS-Abbild im Flash-Speicher. Im Konfigurationsregister wird beim nächsten Zurücksetzen bzw. beim nächsten Aus- und Einschalten des Routers der neue Wert 0x2101 übernommen.

Allgemeine Portzuweisungen

In Tabelle D-1 sind die aktuell zugewiesenen TCP-Portnummern (Transmission Control Protocol) aufgeführt. Soweit dies möglich ist, werden dieselben Nummern auch von UDP (User Datagram Protocol) verwendet.

Tabelle D-1 Aktuell zugewiesene TCP- und UDP-Portnummern

Port	Schlüsselwort	Beschreibung
0	—	Reserviert
1–4	—	Nicht zugewiesen
5	RJE	Auftragsferneingabe
7	ECHO	Echo
9	DISCARD	Verwerfen
11	USERS	Aktive Benutzer
13	DAYTIME	Tageszeit
15	NETSTAT	Wer ist aktiv oder NETSTAT
17	QUOTE	Quote des Tages
19	CHARGEN	Zeichengenerator
20	FTP-DATA	File-Transfer-Protokoll (Daten)
21	FTP	File-Transfer-Protokoll
23	TELNET	Terminalverbindung
25	SMTP	Simple-Mail-Transport-Protokoll
37	TIME	Zeit
39	RLP	Resource-Location-Protokoll
42	NAMESERVER	Hostnamenserver
43	NICNAME	Who-is-Abfrage
49	LOGIN	Login-Host-Protokoll
53	DOMAIN	Domänennamenserver
67	BOOTPS	Bootstrap-Protokoll-Server
68	BOOTPC	Bootstrap-Protokoll-Client
69	TFTP	Trivial-File-Transfer-Protokoll

Tabelle D-1 Aktuell zugewiesene TCP- und UDP-Portnummern (Fortsetzung)

Port	Schlüsselwort	Beschreibung
75	—	Beliebiger privater Dial-out-Dienst
77	—	Beliebiger privater RJE-Dienst
79	FINGER	Finger
95	SUPDUP	SUPDUP-Protokoll
101	HOST NAME	Netzwerkkarte, Hostnamenserver
102	ISO-TSAP	ISO-Transport Service Access Point (TSAP, Transportdienst-Zugangspunkt)
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	Sun Microsystems Remote Procedure Call (Sun Microsystems-Remote-Prozedurauf ruf)
113	AUTH	Authentifizierungsdienst
117	UUCP-PATH	UNIX-zu-UNIX-Copy-Protokoll-Pf addienst (UUCP-Pfaddienst)
119	NNTP	Usenet-Network-News-Transfer-Pr otokoll
123	NTP	Network-Time-Protokoll
126	SNMP	Simple-Network-Management-Prot okoll
137	NETBIOS-NS	NetBIOS-Namensdienst
138	NETBIOS-DGM	NetBIOS-Datagrammdienst
139	NETBIOS-SSN	NetBIOS-Sitzungsdienst
161	SNMP	Simple-Network-Management-Prot okoll
162	SNMP-TRAP	Simple-Network-Management-Prot okoll-Traps
512	rexec	UNIX-Remote-Ausführung (Steuerung)
513	TCP – rlogin UDP – rwho	TCP – UNIX-Remote-Anmeldung UDP – UNIX-Broadcast-Namensdienst
514	TCP – rsh UDP – syslog	TCP – UNIX-Remote-Shell UDP – Systemprotokoll
515	Printer	UNIX-Remote-Spoolbetrieb für Zeilendrucker
520	RIP	Routing-Information-Protokoll
525	Timed	Zeit-Server

Symbole

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z