# Virtual Access PPP-Funktionen in Cisco IOS

## Inhalt



## Einführung

Dieses Dokument beschreibt die allgemeine Architektur von Virtual Access PPP-Anwendungen in Cisco IOS®. Weitere Informationen zu einer bestimmten Funktion finden Sie in den Dokumenten am Ende des Glossars.

## Bevor Sie beginnen

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

### Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

## Glossar

Die folgenden Begriffe werden in diesem Dokument verwendet.

- **Zugriffsserver**: Cisco Access Server-Plattformen, einschließlich ISDN und asynchrone Schnittstellen für Remote-Zugriff.
- **L2F**: Layer 2 Forwarding Protocol (Experimental Draft RFC). Dies ist die zugrunde liegende Technologie auf Verbindungsebene für Multichassis MP und Virtual Private Networks (VPN).
- **Link**: Ein Verbindungspunkt, der von einem System bereitgestellt wird. Dabei kann es sich um eine dedizierte Hardware-Schnittstelle (z. B. eine async-Schnittstelle) oder einen Kanal auf einer Multichannel-Hardware-Schnittstelle (z. B. PRI oder BRI) handeln.
- **VA**: Multilink PPP Protocol (siehe RFC 1717)
- **Multichassis-MP**: MP + SGBP + L2F + Vtemplate.
- **PPP**: Point-to-Point-Protokoll (siehe RFC 1331).
- **Rotary Group**: Eine Gruppe physischer Schnittstellen, die zum Wählen oder Empfangen von Anrufen zugewiesen sind. Die Gruppe agiert wie ein Pool, aus dem jede beliebige Verbindung zum Wählen oder Empfangen von Anrufen verwendet werden kann.
- **SGBP**: Stack Group Biding Protocol
- **Stack-Gruppe**: Eine Sammlung von zwei oder mehr Systemen, die für den Betrieb als Gruppe konfiguriert werden und MP-Pakete mit Links auf verschiedenen Systemen unterstützen.
- **VPDN**: Virtuelles privates DFÜ-Netzwerk. Die Weiterleitung von PPP-Verbindungen von einem Internet Service Provider (ISP) an ein Home Gateway.
- **Vorlage**: Virtual Template-Schnittstelle.

**Hinweis:** Informationen zu den in diesem Dokument erwähnten RFCs finden Sie unter RFCs Supported in Cisco IOS Release 11.2, a product bulletin. oder Abrufen von RFCs und anderen Standarddokumenten für einen Link direkt zu InterNIC.

# Übersicht über die Virtual Access Interface

In Cisco IOS Release 11.2F unterstützt Cisco die folgenden DFÜ-Zugriffsfunktionen: VPDN, Multichassis Multilink, VP, Protocol Translation mit Virtual-Access und PPP/ATM. Diese Funktionen verwenden virtuelle Schnittstellen, um PPP auf ihren Zielgeräten zu übertragen.

Eine Virtual Access-Schnittstelle ist eine Cisco IOS-Schnittstelle, genau wie physische Schnittstellen wie eine serielle Schnittstelle. Eine Konfiguration der seriellen Schnittstelle befindet sich in der Konfiguration der seriellen Schnittstelle.

```
#config
  int s0
  ip unnumbered e0
  encap ppp
  :
```

Physische Schnittstellen verfügen über statische, feste Konfigurationen. Virtual Access-Schnittstellen werden jedoch bei Bedarf dynamisch erstellt (die verschiedenen Verwendungsmöglichkeiten werden im nächsten Abschnitt dieses Dokuments erläutert). Sie werden auch dann freigelassen, wenn sie nicht mehr benötigt werden. Daher muss die **Konfigurationsquelle** der Virtual Access-Schnittstellen auf andere Weise verankert sein.

Die verschiedenen Methoden, mit denen ein virtueller Zugriff seine Konfiguration erhält, sind die Schnittstelle **Virtual Template** und/oder RADIUS- und TACAC+-Datensätze, die sich auf einem Authentifizierungsserver befinden. Die letztgenannte Methode wird *pro Benutzer als* **virtuelle Profile** bezeichnet. Da Virtual Access-Schnittstellen mithilfe einer globalen virtuellen Vorlage konfiguriert werden können, können Virtual Access-Schnittstellen für verschiedene Benutzer identische Konfigurationen von einer Virtual Template-Schnittstelle erben. Beispielsweise kann der Netzwerkadministrator eine gemeinsame PPP-Authentifizierungsmethode (CHAP) für alle Virtual Access-Benutzer des Systems definieren. Für **spezifische benutzerspezifische** Konfigurationen kann der Netzwerkadministrator Schnittstellenkonfigurationen definieren, z. B. die PAP-Authentifizierung, die für den Benutzer im virtuellen Profil spezifisch sind. Kurz gesagt, das allgemeine bis spezifische Konfigurationsschema, das den Virtual Access-Schnittstellen zur Verfügung steht, ermöglicht es dem Netzwerkadministrator, die für alle Benutzer gemeinsamen Schnittstellenkonfigurationen und/oder individuelle Anpassungen an den Benutzer vorzunehmen.

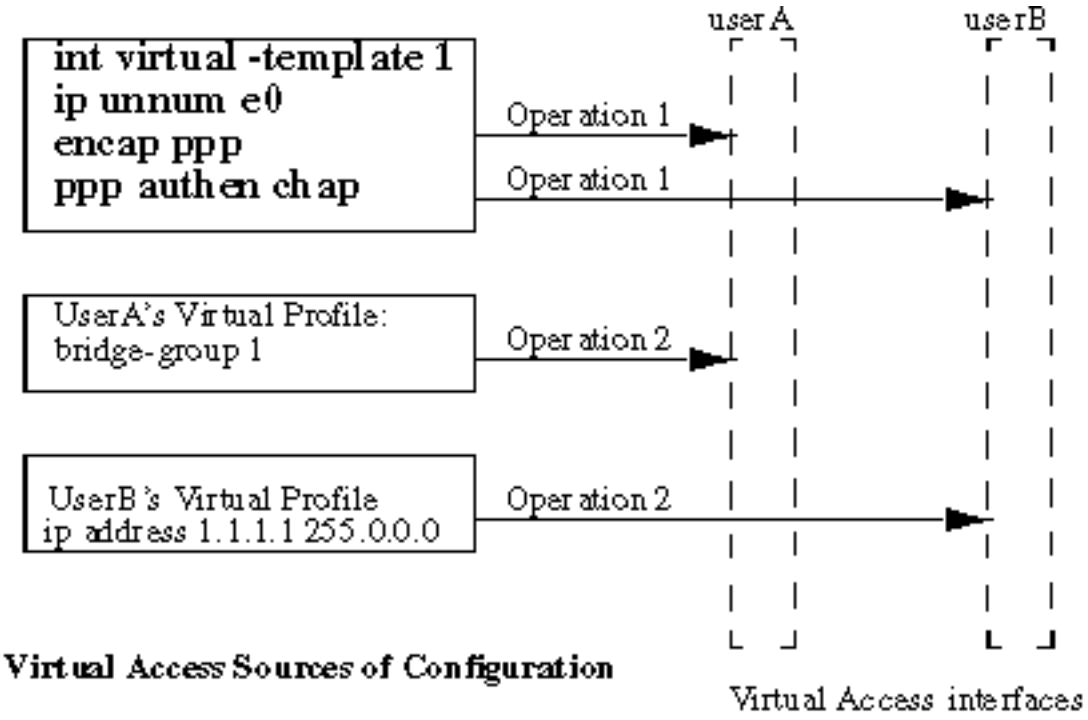


**Figure 1. Virtual Access Sources of Configuration**

Abbildung 1 oben zeigt zwei der Virtual Access-Schnittstellen für Benutzer A und Benutzer B. Operation 1 kennzeichnet die Anwendung der Schnittstellenkonfiguration von einer **globalen** Virtual Template-Schnittstelle auf die beiden Virtual Access-Schnittstellen. Operation 2 kennzeichnet die Anwendung von Schnittstellenkonfigurationen pro Benutzer von **unterschiedlichen** virtuellen Profilen auf die beiden Virtual Access-Schnittstellen.

## Anwendungen der Virtual Access Interfaces

In diesem Abschnitt werden die verschiedenen Methoden beschrieben, wie Cisco IOS Virtual Access-Schnittstellen verwendet.

Sie sehen ein wiederkehrendes Design jeder Anwendung: Sie ermöglichen eine allgemeine virtuelle Vorlage für die Anwendung (Vorgang 1). Pro Benutzer werden dann virtuelle Profile pro Benutzer angewendet (Vorgang 2)

### Multilink PPP

Multilink PPP verwendet die Virtual Access-Schnittstelle als Paketschnittstelle, um über einzelne Links empfangene Pakete neu zusammenzufügen und Pakete zu fragmentieren, die über einzelne Links versendet wurden. Die Paketschnittstelle erhält ihre Konfiguration von der virtuellen Vorlage für Multilink PPP. Wenn der Netzwerkadministrator virtuelle Profile aktiviert, wird die Konfiguration der virtuellen Profile für jeden Benutzernamen auf die Paketschnittstelle für diesen Benutzer angewendet.

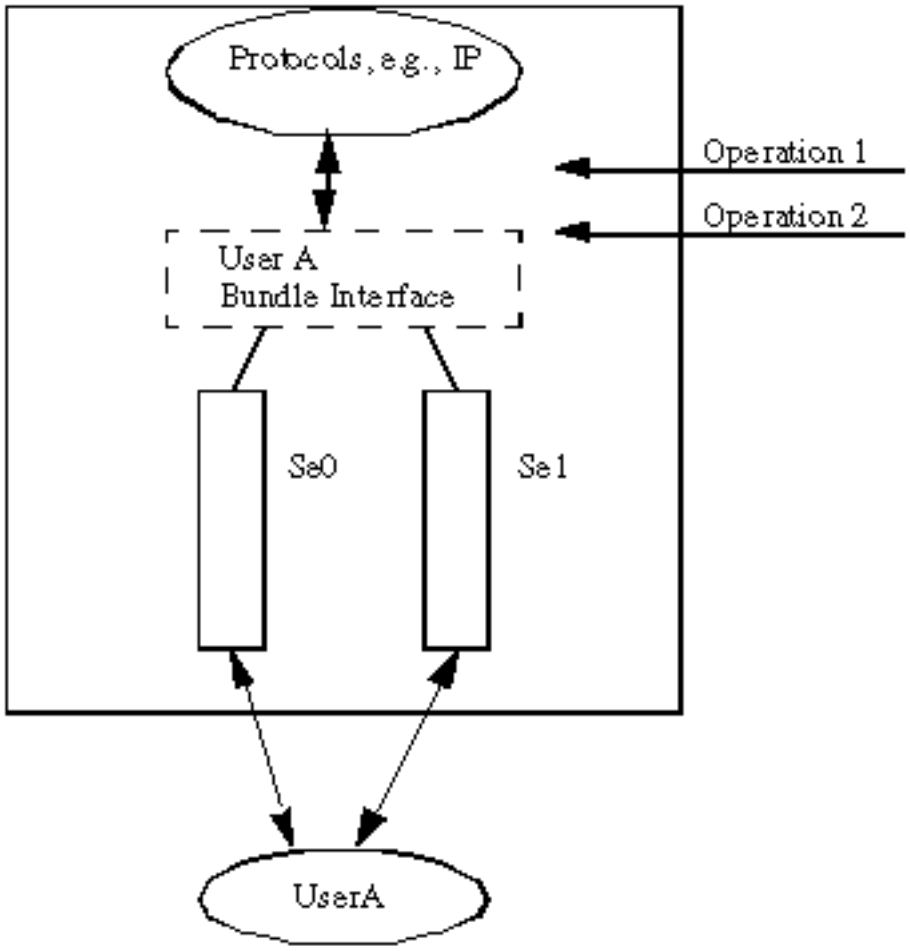


**Figure 2. Multilink PPP Bundle Interface**

Abbildung 2 zeigt die Verwendung von Multilink PPP für serielle Schnittstellen. Da es keine Dialer-Schnittstelle gibt, wird eine Virtual Template-Schnittstelle wie folgt definiert:

```
multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp chap authen
```

Die optionale Konfiguration des virtuellen Profils pro Benutzername wird dann auf die Paketschnittstelle angewendet. Wenn die Dialer-Schnittstelle beteiligt ist, ist die Bündelschnittstelle eine passive Schnittstelle. Eine virtuelle Vorlagenschnittstelle ist nicht erforderlich.

Abbildung 3 unten zeigt beispielsweise ein PRI se0:23, das für die Unterstützung von Multilink PPP konfiguriert ist.

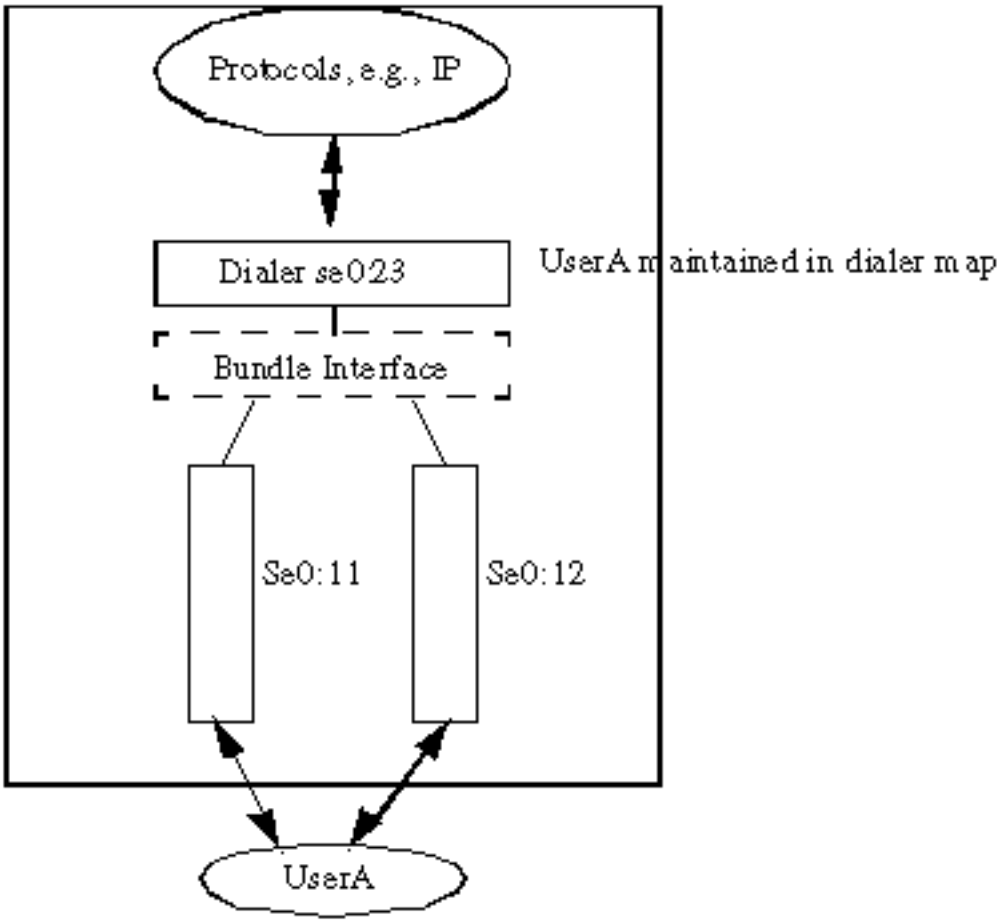


**Figure 3. Multilink PPP Interface (Passive)**

Wenn Virtual Profile (Virtuelles Profil) aktiviert ist, wird das Schema umgekehrt, wie in Abbildung 2 dargestellt. Das heißt, wenn ein eingehender Anruf auf einer Dialer-Schnittstelle empfangen wird und Virtual Profile (Virtuelles Profil) aktiviert ist, wird die Konfiguration nicht mehr vom Wähler übernommen. Stattdessen ist die Paketschnittstelle (siehe Abbildung 2) die "aktive" Schnittstelle, auf die alle Protokolle gelesen oder geschrieben werden. Die Konfigurationsquelle ist zunächst die Virtual Template-Schnittstelle und dann das Virtual Profile für einen bestimmten Benutzer.

## L2F

Mit der Layer-2-Weiterleitung auf Verbindungsebene (L2F) kann PPP an einem Remote-Ziel terminiert werden. Normalerweise befindet sich PPP ohne L2F zwischen dem gewählten Client und dem NAS, der den eingehenden Anruf entgegennimmt. Mit L2F wird das PPP auf einen Zielknoten projiziert. Der Kunde "denkt", dass er über PPP mit dem Zielknoten verbunden ist. Das NAS wird im Prinzip zu einem einfachen PPP-Frame Forwarder. In der L2F-Terminologie wird der Zielknoten als **Home-Gateway** bezeichnet.

Am Home-Gateway wird die Virtual Access-Schnittstelle zum Beenden der PPP-Verbindung verwendet. Auch hier wird eine virtuelle Vorlage als Konfigurationsquelle verwendet. Wenn Virtual Profile (Virtuelles Profil) definiert ist, wird die Konfiguration pro Benutzer auf die Virtual-Access-Schnittstelle angewendet.

Der L2F-Tunnel wird derzeit über UDP/IP propagiert.

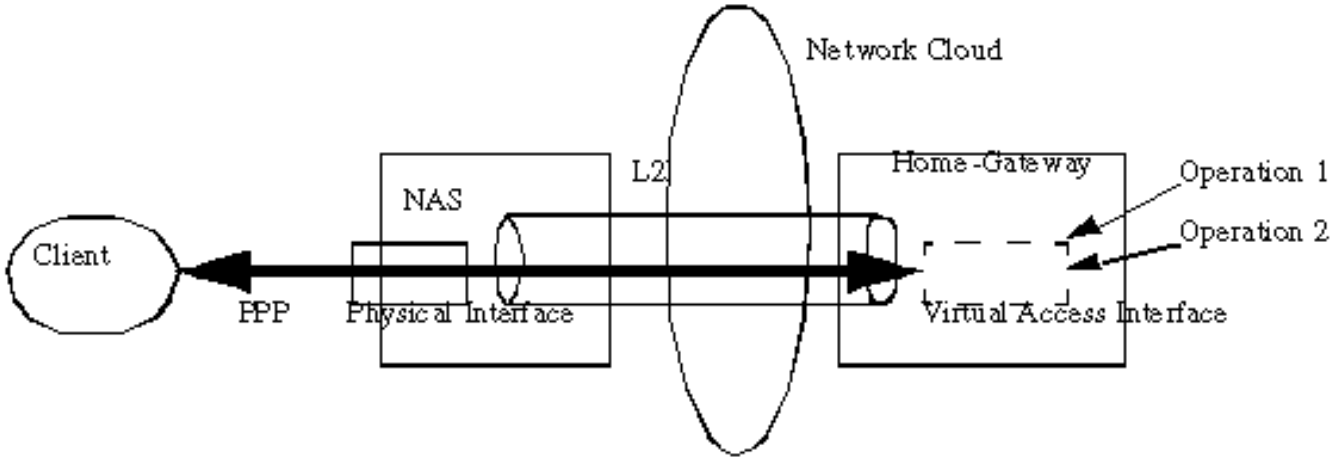


**Figure 4. Client PPP to the Home-Gateway via a L2F Tunnel**

Die L2F-Tunneling-Technologie wird derzeit in zwei Cisco IOS 11.2-Funktionen verwendet: **VPDN** (Virtual Private Dialup Network) und **Multichassis Multilink PPP** (MMP).

## VPDN

**VPDN** ermöglicht den privaten Netzwerken die direkte Verbindung vom Client zum Home Gateway der Wahl. So möchten beispielsweise mobile Benutzer (z. B. Vertriebsmitarbeiter) von HP jederzeit und überall eine Verbindung zum HP Home-Gateway ihrer Wahl herstellen können. HP würde Verträge über ISPs abschließen, die PDN unterstützen. Diese ISPs werden so konfiguriert, dass das NAS-Gerät automatisch an das HP Home-Gateway weiterleitet, wenn sich **jsmith@hp.com** bei einer von dem ISP bereitgestellten Nummer einwählt. Der ISP kann somit die IP-Adressen, das Routing und andere Funktionen von HP-Benutzern, die an die Benutzerbasis von HP gebunden sind, nicht mehr verwalten. Die IP-Konnektivitätsprobleme des HP-Home-Gateways werden auf die Administrationsfunktion des ISP reduziert.

### NAS: ISP

```
  vpdn outgoing hp.com isp ip 1.1.1.2
```

### Home-Gateway: HP-Gateway

```
int virtual-template 1
  ip unnum e0
  encap ppp
  ppp chap authen

  vpdn incoming isp hp-gateway virtual-template 1
```

### Multi-Chassis

PPP Multilink bietet Benutzern zusätzliche Bandbreite bei Bedarf, wobei Pakete über eine logische Leitung (Bündel) aufgeteilt und neu kombiniert werden können, die aus mehreren Verbindungen besteht. Dadurch wird die Übertragungslatenz über die langsamen WAN-Verbindungen verringert, und es wird auch die maximale Empfangseinheit erhöht. Multilink wird in einer einzigen Access Server-Umgebung unterstützt.

So möchten ISPs z. B. mehreren PRIs über mehrere Access Server eine einzige Rufnummer zuweisen, die skalierbar und flexibel an ihre geschäftlichen Anforderungen angepasst ist.

Bei Multichassis Multilink können mehrere Multilink-Verbindungen desselben Clients an unterschiedlichen Access-Servern enden. Zwar können einzelne MP-Verbindungen desselben Pakets tatsächlich an unterschiedlichen Access-Servern enden, doch was den MP-Client betrifft, so ist dies so, als würde er an einem einzigen Access-Server enden. Wenn Komponenten mit denen von VPDN verglichen werden, unterscheidet sich MultiChassis nur durch ein zusätzliches StackGroup Bidding Protocol (SGBP), um die Gebotsbildung und das Schiedsverfahren für Multilink-Pakete zu erleichtern. Sobald die Ziel-IP-Adresse des Gewinners der Stack Group über SGBP festgelegt wurde, verwendet Multichassis L2F, um vom NAS auf das andere NAS zu projizieren, das wiederum der Gewinner der Stack Group ist.

Beispielsweise ruft eine Stack-Gruppe **Stackq** von zwei NASs auf: **Nasenbluten** und **Nasenbluten**.

### Nasa:

```
  username stackq password hello
  multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  sgbp stack stackq
  sgbp member nasb 1.1.1.2
```

### nasb:

```
username stackq password hello
  multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  sgbp stack stackq
  sgbp member nasb 1.1.1.2
```

### Protokollübersetzung

Bei der Protokoll-Übersetzung kann gekapselter PPP-Datenverkehr über ein Gateway (z. B. X.25/TCP) als Virtual Access Interface (zweistufige Übersetzung) terminiert werden. Die Virtual Access-Schnittstelle wird auch in einer einstufigen Übersetzung unterstützt.

### Beispiel für die Protokollübersetzung in zwei Schritten:

```
  int virtual-template 1
  ip unnum e0
```

```
  encap ppp
  ppp authen chap

  vty-async virtual-template 1
```

### Beispiel für eine Protokollübersetzung in einem Schritt:

```
int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  translate tcp 1.1.1.1 virtual-template 1
```

### PPP über ATM

Diese Funktion ermöglicht die Terminierung mehrerer PPP-Verbindungen an einer ATM-Schnittstelle des Routers, wenn die Daten gemäß der Kapselung von Frame Forwarding (StrataCom) von Cisco formatiert sind. Das PPP-Protokoll wird auf dem Router beendet, als ob es von einer typischen seriellen PPP-Schnittstelle empfangen wurde. Jede PPP-Verbindung wird in einem separaten ATM VC gekapselt. VCs, die andere Kapselungstypen verwenden, können auch auf derselben Schnittstelle konfiguriert werden.

```
interface Virtual-Template1
  ip unnumbered e0/0
  ppp authentication chap

  interface ATM2/0.2 point-to-point
  atm pvc 34 34 34 aal5ppp virtual-template 1
```

### Virtuelle Profile

Virtual Profiles ist eine eindeutige PPP-Anwendung, die Konfigurationsinformationen für Benutzer definiert und anwendet, die sich bei einem Router anmelden. Virtuelle Profile ermöglichen die Anwendung benutzerspezifischer Konfigurationsinformationen unabhängig von den Medien, die für den Einwahlanruf verwendet werden. Die Konfigurationsinformationen für virtuelle Profile können je nach Konfiguration des Routers und des AAA-Servers aus einer Vorlage für virtuelle Schnittstellen, aus Konfigurationsdaten für jeden Benutzer, die auf einem AAA-Server gespeichert sind, oder aus beidem stammen. Die Anwendung virtueller Profile kann in einer Einzelkomponentenumgebung, in einem VPDN Home-Gateway oder in einer Multichassis-Umgebung erfolgen.

So definieren Sie eine virtuelle Vorlage als Konfigurationsquelle für virtuelles Profil:

```
virtual-profile virtual-template 1
  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap
  :
```

So definieren Sie AAA als Konfigurationsquelle für das virtuelle Profil:

```
virtual-profile aaa
```

In diesem Beispiel beschließt der Systemadministrator, die an John gesendeten Routen zu filtern und Zugriffslisten auf Rick's Einwahlverbindungen anzuwenden. Wenn sich John oder Rick über die Schnittstelle S1 oder BRI 0 einwählt und sich authentifiziert, wird ein virtuelles Profil erstellt: Routingfilter werden auf John angewendet, und Zugriffslisten werden auf Rick angewendet.

AAA-Konfiguration für die Benutzer John und Rick:

```
john Password = ``welcome''
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
           cisco-avpair = ``ip:rte-fltr-out#0=router igrp 60'',
           cisco-avpair = ``ip:rte-fltr-out#3=deny 171.0.0.0 0.255.255.255'',
           cisco-avpair = ``ip:rte-fltr-out#4=deny 172.0.0.0 0.255.255.255'',
           cisco-avpair = ``ip:rte-fltr-out#5=permit any''
  rick Password = ``emoclew''
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
           cisco-avpair = ``ip:inacl#3=permit ip any any precedence immediate'',
           cisco-avpair = ``ip:inacl#4=deny igrp 0.0.1.2 255.255.0.0 any'',
           cisco-avpair = ``ip:outacl#2=permit ip any any precedence immediate'',
           cisco-avpair = ``ip:outacl#3=deny igrp 0.0.9.10 255.255.0.0 any''
```

Kurz gesagt enthalten die AAA **cisco-avpair-**Befehle von Cisco IOS pro Schnittstelle, die für einen bestimmten Benutzer angewendet werden.