

# Cisco IOS のバーチャルアクセス PPP 機能

## 内容

[概要](#)

[はじめに](#)

[表記法](#)

[前提条件](#)

[使用するコンポーネント](#)

[用語集](#)

[仮想アクセスインターフェイスの概要](#)

[仮想アクセスインターフェイスのアプリケーション](#)

[マルチリンク PPP](#)

[L2F](#)

[VPDN](#)

## 概要

このドキュメントでは、Cisco IOS® のバーチャル アクセス PPP アプリケーション全体のアーキテクチャについて説明します。特定の機能の詳細については、「用語集」の終わりの一覧にあるドキュメントを参照してください。

## [はじめに](#)

### [表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

### [前提条件](#)

このドキュメントに関しては個別の前提条件はありません。

### [使用するコンポーネント](#)

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

## 用語集

このドキュメント内で使用されている用語は次のとおりです。

- **アクセス サーバ** : リモート アクセスのための Cisco アクセス サーバのプラットフォーム ( ISDN および非同期インターフェイスなど )。
- **L2F** : L2F プロトコル ( RFC の Experimental Draft )。マルチシャーシ MP ( MMP )、およびバーチャルプライベート ネットワーク ( VPN ) 双方の基礎となるリンクレベル テクノロジーです。
- **リンク** : システムの接続ポイント。専用のハードウェア インターフェイス ( 非同期インターフェイスなど )、あるいは、マルチチャンネル ハードウェア インターフェイスのチャンネル ( PRI や BRI など ) です。
- **MP** : マルチリンク PPP プロトコル。RFC 1717 を参照してください。
- **マルチシャーシ MP** : MP + SGBP + L2F + Vtemplate。
- **PPP**:Point-to-Point Protocol ( PPP; ポイントツーポイント プロトコル )。RFC 1331 を参照してください。
- **ロータリー グループ** : 外部へのダイヤルやコールの受信に割り当てられた物理インターフェイスのグループ。このグループは、外部にダイヤルしたりコールを受信したりするためのリンクのプールのような役割を果たします。
- **SGBP** : Stack Group Bidding プロトコル。
- **スタック グループ** : 2 つ以上のシステムの集まり。グループとして動作するように設定され、他のシステムからのリンクの MP バンドルをサポートします。
- **VPDN**:バーチャルプライベートダイヤルアップネットワーク。Internet Service Provider ( ISP; インターネット サービス プロバイダー ) からホーム ゲートウェイへの PPP リンクを転送します。
- **Vtemplate** : バーチャル テンプレート インターフェイス。

注 : このドキュメントで参照されるRFCの詳細については、製品速報の「[Cisco IOSリリース 11.2でサポートされるRFC](#)」を参照してください。または[InterNICへのリンクに関するRFCおよびその他の標準文書の取得](#)

## 仮想アクセスインターフェイスの概要

Cisco IOS リリース 11.2F でサポートされるダイヤルアップアクセス機能は、VPDN、マルチシャーシ マルチリンク、VP、バーチャル アクセスによるプロトコル変換、および PPP/ATM です。これらの機能では、バーチャル インターフェイスを使用して、目的のマシンへ PPP を伝送します。

バーチャル アクセス インターフェイスは Cisco IOS のインターフェイスで、シリアル インターフェイスのような物理インターフェイスです。シリアル インターフェイスの設定は、シリアル インターフェイス コンフィギュレーションにあります。

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

物理インターフェイスには、スタティックな固定設定があります。それに対して、バーチャル アクセス インターフェイスは、必要に応じて動的に作成されます ( この文書の次のセクションでさ

さまざまな使用法について説明します)。また、必要がなくなると解放されます。したがって、バーチャルアクセスインターフェイスのコンフィギュレーションソースは、他の方法で繋ぎとめておく必要があります。

バーチャルアクセスでは、その構成が、バーチャル テンプレート インターフェイス、RADIUS、および認証サーバの TACAC+ レコードなどを介したさまざまな方法で取得されます。後者の方法は、ユーザごとのバーチャル プロファイルと呼ばれるものです。バーチャルアクセスインターフェイスは、グローバルなバーチャル テンプレートを使用して構成できるため、1つのバーチャル テンプレート インターフェイスから同一の設定を、さまざまなユーザのバーチャルアクセスインターフェイスに継承できます。たとえば、ネットワーク管理者は、システム上のバーチャルアクセスの全ユーザに共通の PPP 認証方法 (CHAP) を定義できます。特定のユーザごとの設定には、ネットワーク管理者が仮想プロファイル内のユーザーに固有のインターフェイス設定 (PAP 認証など) を定義できます。バーチャルアクセスインターフェイスでは、一般的なコンフィギュレーション スキームも特定のコンフィギュレーション スキームも利用できるため、ネットワーク管理者は、インターフェイス コンフィギュレーションをすべてのユーザ共通に設定することも、個別のユーザごとに設定することも可能です。

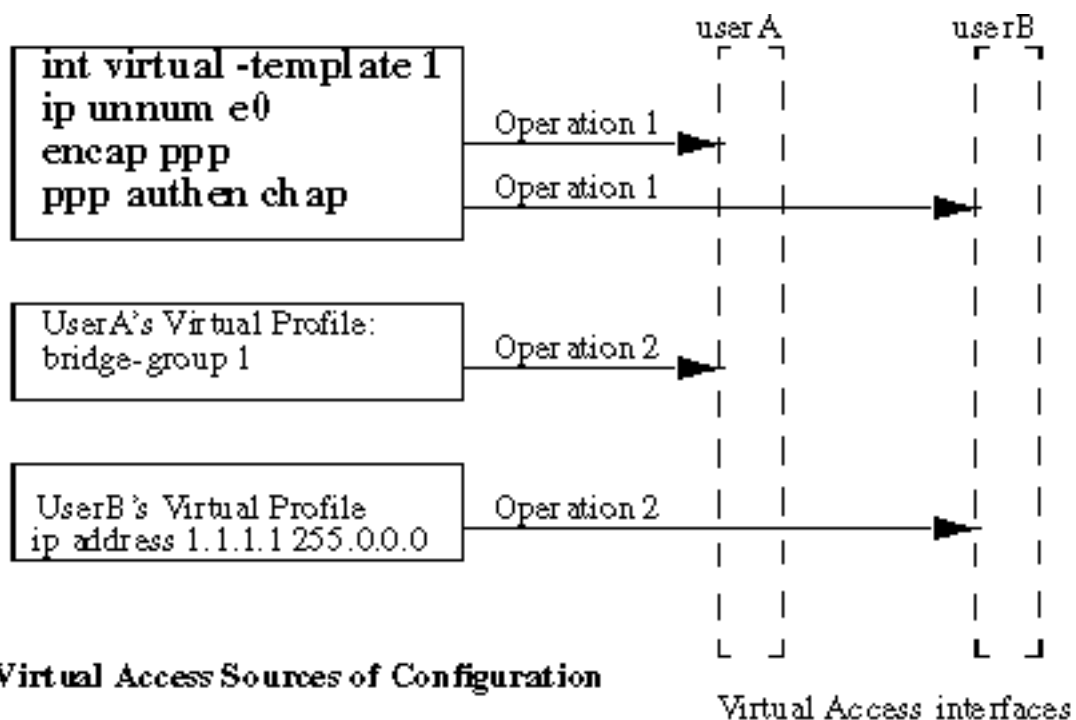


Figure 1. Virtual Access Sources of Configuration

図 1 に、userA と userB が使用する 2 種類のバーチャルアクセスインターフェイスについて説明しています。Operation 1 は、グローバルなバーチャル テンプレート インターフェイスから 2 つのバーチャルアクセスインターフェイスへのインターフェイス コンフィギュレーションの適用を示しています。Operation 2 は、個別のバーチャル プロファイルから 2 つのバーチャルアクセスインターフェイスへの、ユーザごとのインターフェイス コンフィギュレーションの適用を示しています。

## 仮想アクセスインターフェイスのアプリケーション

このセクションでは、Cisco IOS でバーチャルアクセスインターフェイスを使用するさまざまな方法を説明します。

各アプリケーションのテーマが繰り返し表示されます。アプリケーションに固有の一般的な仮想テンプレート (操作1) を使用できます。Operation 2 は、ユーザごとのバーチャルプロファイルが各ユーザに適用されています)。

## マルチリンク PPP

マルチリンク PPP では、各リンクで受信したパケットを再構成したり、各リンクから送信するパケットを断片化するためのバンドル インターフェイスとして、バーチャル アクセス インターフェイスを使用します。バンドル インターフェイスは、そのコンフィギュレーションをマルチリンク PPP 用のバーチャル テンプレートから入手します。ネットワーク管理者がバーチャル プロファイルをイネーブルにすると、ユーザ名ごとのバーチャル プロファイルのインターフェイス コンフィギュレーションがユーザのバンドル インターフェイスに適用されます。

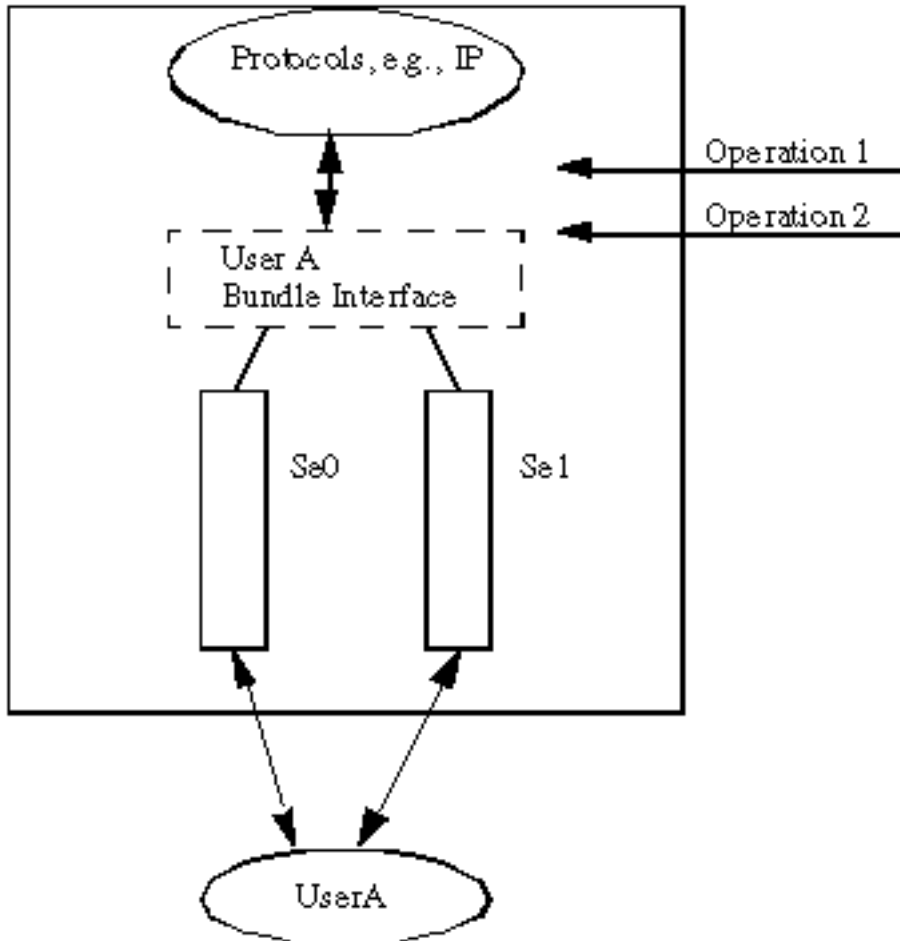


Figure 2. Multilink PPP Bundle Interface

図 2 は、シリアル インターフェイスでマルチリンク PPP を使用した場合は示しています。ダイヤラインターフェイスがないので、次のようにバーチャル テンプレート インターフェイスを定義します。

```
multilink virtual-template 1

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

任意で設定されたユーザ名ごとのバーチャル プロファイルのコンフィギュレーションが、バンドル インターフェイスに適用されます。ダイヤラインターフェイスが関係している場合、バンドル インターフェイスはパッシブインターフェイスです。仮想テンプレートインターフェイスは必要ありません。

たとえば、図 3 では、マルチリンク PPP をサポートするように PRI se0:23 が構成されています。

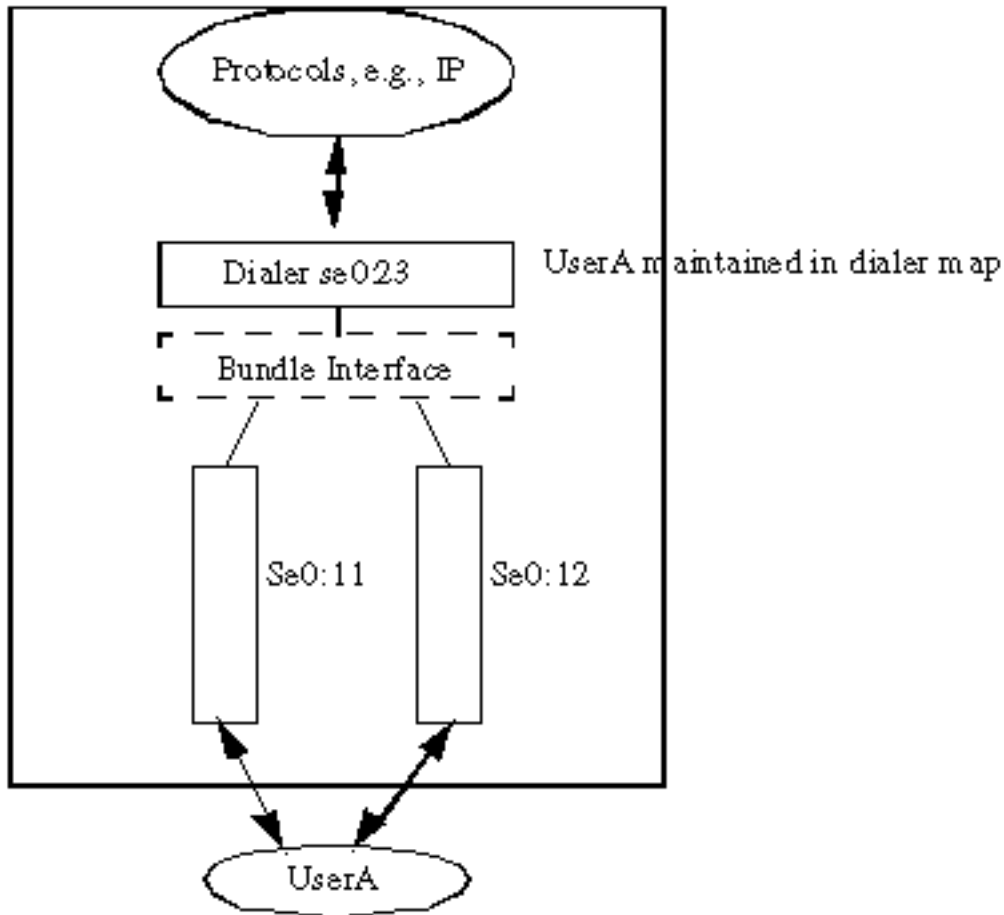


Figure 3. Multilink PPP Interface (Passive)

バーチャルプロファイルがイネーブルな場合は、スキームが図 2 に戻ることにご注意ください。つまり、着信コールがダイヤラ インターフェイスで受信され、バーチャルプロファイルがイネーブルになっている場合、ダイヤラからのコンフィギュレーションソースは使用されません。代わりにバンドル インターフェイスがアクティブ インターフェイスになり (図 2 を参照してください)、ここですべてのプロトコルが読み書きされます。まずバーチャル テンプレート インターフェイスが、次に特定ユーザのバーチャル プロファイルがコンフィギュレーション ソースとなります。

## L2F

リンクレベルのレイヤ 2 送信 (L2F) では、PPP をリモートの宛先で終端させることができます。通常、L2F を使用しない場合、ダイヤルしたクライアントと着信コールに回答した NAS 間では PPP が使用されます。L2F を使用すると、宛先ノードに PPP が投影されます。クライアントでは、PPP を介して宛先ノードに接続していると認識されています。実際には、NAS が PPP フレームを転送しています。L2F の用語では、宛先ノードはホームゲートウェイと呼ばれます。

ホームゲートウェイでは、バーチャル アクセス インターフェイスを使用して PPP リンクを終端させます。コンフィギュレーション ソースとしてバーチャル テンプレートが使用されます。バーチャルプロファイルが定義されている場合は、バーチャル アクセス インターフェイスにユーザごとのインターフェイス コンフィギュレーションが適用されます。

一般的に、L2F トンネルは UDP/IP で伝搬されます。

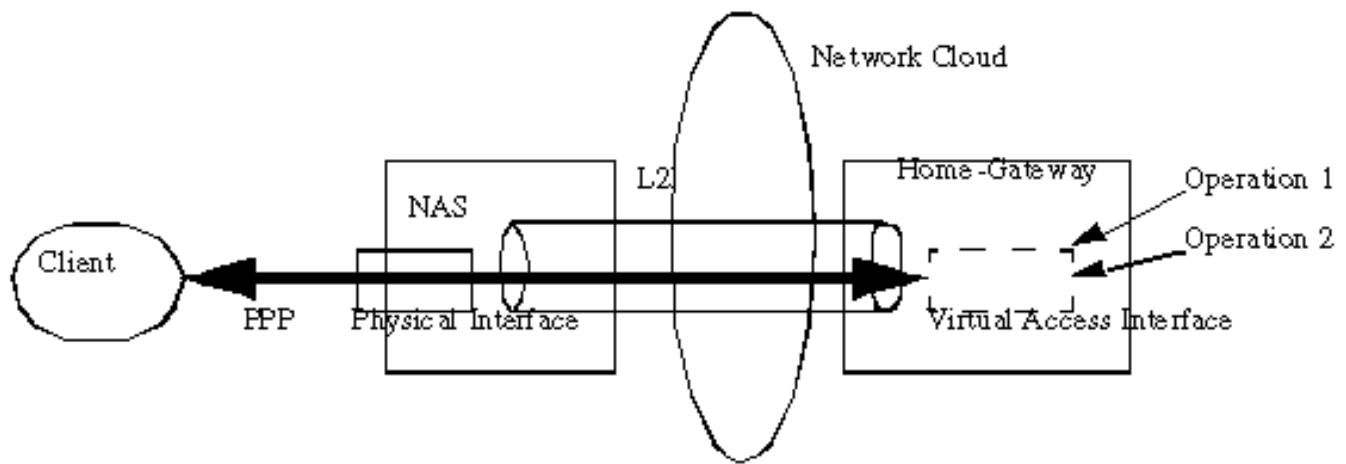


Figure 4. Client PPP to the Home-Gateway via a L2F Tunnel

L2F トンネリング テクノロジーは、現在 Cisco IOS 11.2 の次の 2 つの機能に使用されています。これらの機能は VPDN (バーチャルプライベートダイヤルアップネットワーク) とマルチシャーシマルチリンク PPP (MMP) です。

## VPDN

VPDN では、クライアントから、直接、選択したホームゲートウェイにまで、プライベートネットワークを広げることができます。たとえば、HP のモバイル ユーザ (営業担当者など) は、常にどこでも、選択した HP のホームゲートウェイに接続できる状態である必要があります。HP は、ISP に PDN をサポートしてもらう契約をします。ISP では、jsmith@hp.com が ISP が提供した番号にダイヤルすると、自動的に NAS が HP のホームゲートウェイに転送するように設定します。これによって、ISP は、HP ユーザの IP アドレス、ルーティング、その他 HP ユーザに密接した機能を管理する必要がなくなります。そして、ISP の HP 管理者では、HP ホームゲートウェイへの IP 接続の問題が軽減されます。

## NAS : isp

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

## ホームゲートウェイ : hp-gateway

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

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

## マルチシャーシ

PPP マルチリンクでは、複数のリンクから形成されている論理パイプ (バンドル) でパケットを分割したり再構成することによって、必要な帯域幅を増やすことができます。これによって、低速の WAN リンクでの転送遅延が軽減され、最大受信ユニットを増やすことができます。マルチリンクは、アクセスサーバが 1 つの環境でサポートされます。

たとえば、ISP では、効率良く 1 つのロータリー番号を複数のアクセスサーバ上の複数の PRI に割り当てるため、柔軟性と拡張性が求められます。

マルチシャーシ マルチリンクでは、同一クライアントからの複数のマルチリンクを異なるアクセスサーバで終端させることができます。同一バンドルの各 MP リンクを異なるアクセスサーバで終端できますが、MP クライアントから見ると、1 つのアクセスサーバで終端しているかのように見えます。マルチシャーシと VPDN のコンポーネントの違いは、マルチリンクバンドルをビIDDINGおよび調停するために追加する StackGroup Bidding プロトコル ( SGBP ) だけです。SGBP でスタックグループの宛先 IP アドレスが決定すると、マルチシャーシでは、L2F を使用して、その NAS からスタックグループの宛先になった他方の NAS へ投影します。

たとえば、スタックグループでは次の 2 つの NAS の stackq を呼び出します。nasa と nasb です。

**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
```

## プロトコル変換

プロトコル変換により、X.25/TCPなどのゲートウェイを経由するPPPカプセル化トラフィックを仮想アクセスインターフェイス ( 2ステップ変換 ) として終端させることができます。バーチャルアクセスインターフェイスは、ワンステップ変換でもサポートされます。

**ツーステップのプロトコル変換例 :**

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

```
ppp authen chap

vty-async virtual-template 1
```

## ワンステップのプロトコル変換例：

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

translate tcp 1.1.1.1 virtual-template 1
```

## PPP over ATM

この機能により、データがシスコの ( StrataCom ) フレーム転送カプセル化の形式になっている場合、ルータ ATM インターフェイスで複数の PPP 接続を終端させることができます。PPP プロトコルは、一般的な PPP シリアル インターフェイスから受信した場合と同様に、ルータで終端します。各 PPP 接続は、個別の ATM VC でカプセル化されます。別のタイプのカプセル化を使用する VC も同じインターフェイスに設定できます。

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

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

## 仮想プロフィール

バーチャルプロフィールは、独特の PPP アプリケーションで、ルータにダイヤルするユーザごとにコンフィギュレーション情報を定義して適用します。バーチャルプロフィールでは、コールのダイヤルに使用されたメディアの種類に関係なく、ユーザ特定のコンフィギュレーション情報が適用されます。バーチャルプロフィールのコンフィギュレーション情報は、バーチャルインターフェイス テンプレートが AAA サーバに格納されたユーザごとのコンフィギュレーション情報、またはその両方から取得されます。これは、ルータと AAA サーバの設定方法によって異なります。バーチャルプロフィールのアプリケーションは、VPDN ホームゲートウェイ、またはマルチシャーシ環境内のシングルボックス環境にあります。

バーチャルプロフィールのコンフィギュレーション ソースとしてバーチャル テンプレートを定義する手順は次のとおりです。

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

バーチャルプロフィールのコンフィギュレーション ソースとして AAA を定義する手順は次のとおりです。



```
virtual-profile aaa
```

この例では、システム管理者が John にアドバタイズされるルートをフィルタリングすることと、Rick のダイヤルイン接続にアクセス リストを適用することを決定しています。John または Rick がインターフェイス S1 または BRI 0 でダイヤルして認証すると、バーチャル プロファイルが作成されます。ルート フィルタが John に適用され、アクセス リストが Rick に適用されます。

John と Rick の AAA 構成 :

```
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''
```

AAA cisco-avpairs に、特定のユーザに適用される Cisco IOS のインターフェイスごとのコマンドが含まれています。