

Funzioni PPP di accesso virtuale in Cisco IOS

Sommario

[Introduzione](#)

[Operazioni preliminari](#)

[Convenzioni](#)

[Prerequisiti](#)

[Componenti usati](#)

[Glossario](#)

[Panoramica dell'interfaccia di accesso virtuale](#)

[Applicazioni delle interfacce di accesso virtuale](#)

[Multilink PPP](#)

[L2F](#)

[VPDN](#)

[Introduzione](#)

Questo documento descrive l'architettura generale delle applicazioni PPP di Virtual Access in Cisco IOS®. Per ulteriori informazioni su una particolare funzione, consultare i documenti elencati alla fine del glossario.

[Operazioni preliminari](#)

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Prerequisiti](#)

Non sono previsti prerequisiti specifici per questo documento.

[Componenti usati](#)

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Glossario

Di seguito vengono riportati i termini che verranno visualizzati nel documento.

- **Server di accesso:** Piattaforme Cisco Access Server, incluse ISDN e interfacce asincrone per fornire accesso remoto.
- **L2F:** Protocollo RFC (Layer 2 Forwarding Protocol) (Bozza sperimentale di RFC). Questa è la tecnologia sottostante a livello di collegamento per Multicassis MP e Virtual Private Network (VPN).
- **Collegamento:** Punto di connessione fornito da un sistema. Può trattarsi di un'interfaccia hardware dedicata (ad esempio un'interfaccia asincrona) o di un canale su un'interfaccia hardware multicanale (ad esempio PRI o BRI).
- **MP:** Protocollo Multilink PPP (vedere RFC 1717).
- **MP multicassis:** MP + SGBP + L2F + Vtemplate.
- **PPP:** Protocollo Point-to-Point (vedere RFC 1331).
- **Gruppo rotante:** Gruppo di interfacce fisiche allocate per la chiamata in uscita o la ricezione di chiamate. Il gruppo funziona come un pool da cui qualsiasi collegamento può essere utilizzato per comporre o ricevere chiamate.
- **SGBP:** Protocollo di offerta Stack Group
- **Gruppo stack:** Insieme di due o più sistemi che verranno configurati per funzionare come gruppo e supportare bundle MP con collegamenti su sistemi diversi.
- **VPDN:** Virtual Private Dialup Network. Inoltro di collegamenti PPP da un provider di servizi Internet (ISP) a un gateway locale.
- **Vtemplate:** Interfaccia del modello virtuale.

Nota: per informazioni sulle RFC a cui si fa riferimento nel presente documento, vedere [le RFC supportate in Cisco IOS versione 11.2](#), un bollettino sul prodotto; o [ottenere RFC e altri documenti relativi agli standard](#) per un collegamento diretto a InterNIC.

Panoramica dell'interfaccia di accesso virtuale

In Cisco IOS versione 11.2F, Cisco supporta le seguenti funzionalità di accesso remoto: VPDN, Multicassis Multilink, VP, Protocol Translation con Virtual-Access e PPP/ATM. Queste funzionalità utilizzano interfacce virtuali per trasportare il protocollo PPP sui computer di destinazione.

Un'interfaccia di accesso virtuale è un'interfaccia Cisco IOS, proprio come le interfacce fisiche come un'interfaccia seriale. La configurazione di un'interfaccia seriale risiede nella configurazione dell'interfaccia seriale.

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

Le interfacce fisiche hanno configurazioni statiche fisse. Le interfacce di accesso virtuale, tuttavia, vengono create dinamicamente su richiesta (i vari utilizzi sono descritti nella sezione successiva di questo documento). Sono anche liberati quando non sono più necessari. Pertanto, l'**origine della configurazione** delle interfacce di accesso virtuale deve essere ancorata in altro modo.

I vari metodi con cui un accesso virtuale ottiene la configurazione sono l'interfaccia del **modello virtuale** e/o i record RADIUS e TACAC+ che risiedono su un server di autenticazione. Quest'ultimo metodo è denominato **Profili virtuali per utente**. Poiché le interfacce di accesso virtuale possono essere configurate utilizzando un modello virtuale globale, le interfacce di accesso virtuale per vari utenti possono ereditare configurazioni identiche da un'interfaccia di modello virtuale. Ad esempio, l'amministratore di rete può scegliere di definire un metodo di autenticazione PPP (CHAP) comune per tutti gli utenti di Accesso virtuale del sistema. Per configurazioni personalizzate **specifiche per utente**, l'amministratore di rete può definire configurazioni di interfaccia specifiche dell'utente nel profilo virtuale, ad esempio l'autenticazione PAP. In breve, lo schema di configurazione generale e specifico disponibile per le interfacce di accesso virtuale consente all'amministratore di rete di personalizzare le configurazioni dell'interfaccia comuni a tutti gli utenti e/o personalizzate singolarmente per l'utente.

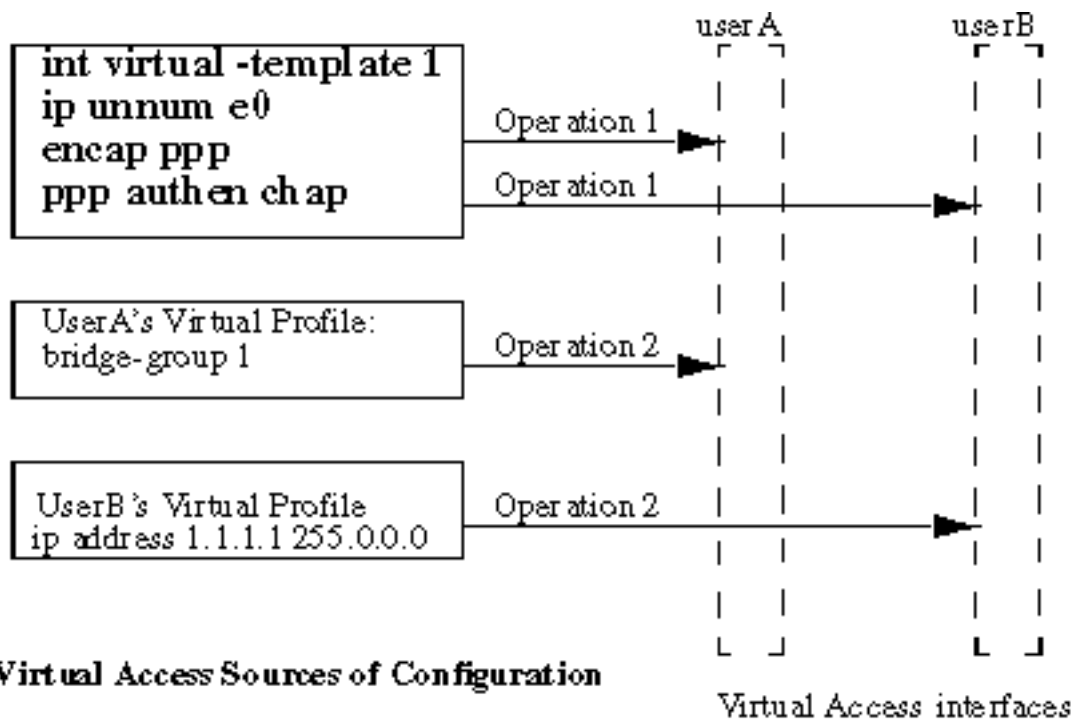


Figure 1. Virtual Access Sources of Configuration

Nella figura 1 sono illustrate due interfacce di accesso virtuale per l'utente A e l'utente B. L'operazione 1 indica l'applicazione della configurazione dell'interfaccia da un'interfaccia di modello virtuale **globale** alle due interfacce di accesso virtuale. L'operazione 2 indica l'applicazione di configurazioni di interfacce per utente da **diversi** profili virtuali alle due interfacce di accesso virtuale.

[Applicazioni delle interfacce di accesso virtuale](#)

In questa sezione vengono descritti i vari modi in cui Cisco IOS utilizza le interfacce di accesso virtuale.

Si noterà un tema ricorrente di ogni applicazione - consentono un modello virtuale generale specifico per l'applicazione (operazione 1). I profili virtuali per utente vengono quindi applicati per utente (operazione 2)

[Multilink PPP](#)

Multilink PPP utilizza l'interfaccia di accesso virtuale come interfaccia di bundle per ricomporre i

pacchetti ricevuti sui singoli collegamenti e per frammentare i pacchetti inviati sui singoli collegamenti. L'interfaccia del bundle ottiene la configurazione dal modello virtuale specifico di Multilink PPP. Se l'amministratore di rete sceglie di abilitare i profili virtuali, la configurazione dell'interfaccia Profilo virtuale per nome utente viene applicata all'interfaccia del bundle per tale utente.

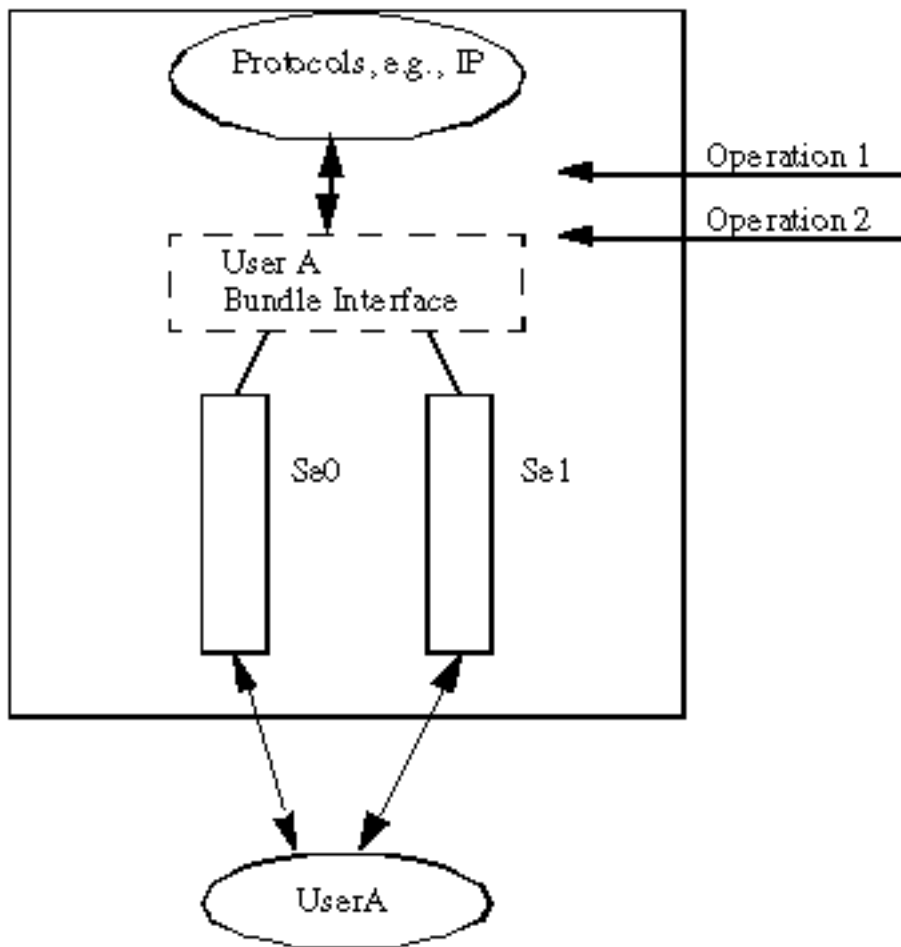


Figure 2. Multilink PPP Bundle Interface

Nella figura 2 viene illustrato l'utilizzo del protocollo Multilink PPP per le interfacce seriali. Poiché non esiste un'interfaccia Dialer, un'interfaccia di modello virtuale è definita da:

```

multilink virtual-template 1

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

La configurazione opzionale del profilo virtuale per nome utente viene quindi applicata all'interfaccia del bundle. Quando è coinvolta l'interfaccia dialer, l'interfaccia bundle è un'interfaccia passiva - non è richiesta alcuna interfaccia di modello virtuale.

Ad esempio, la Figura 3 seguente mostra un PRI se0:23 configurato per supportare Multilink PPP.

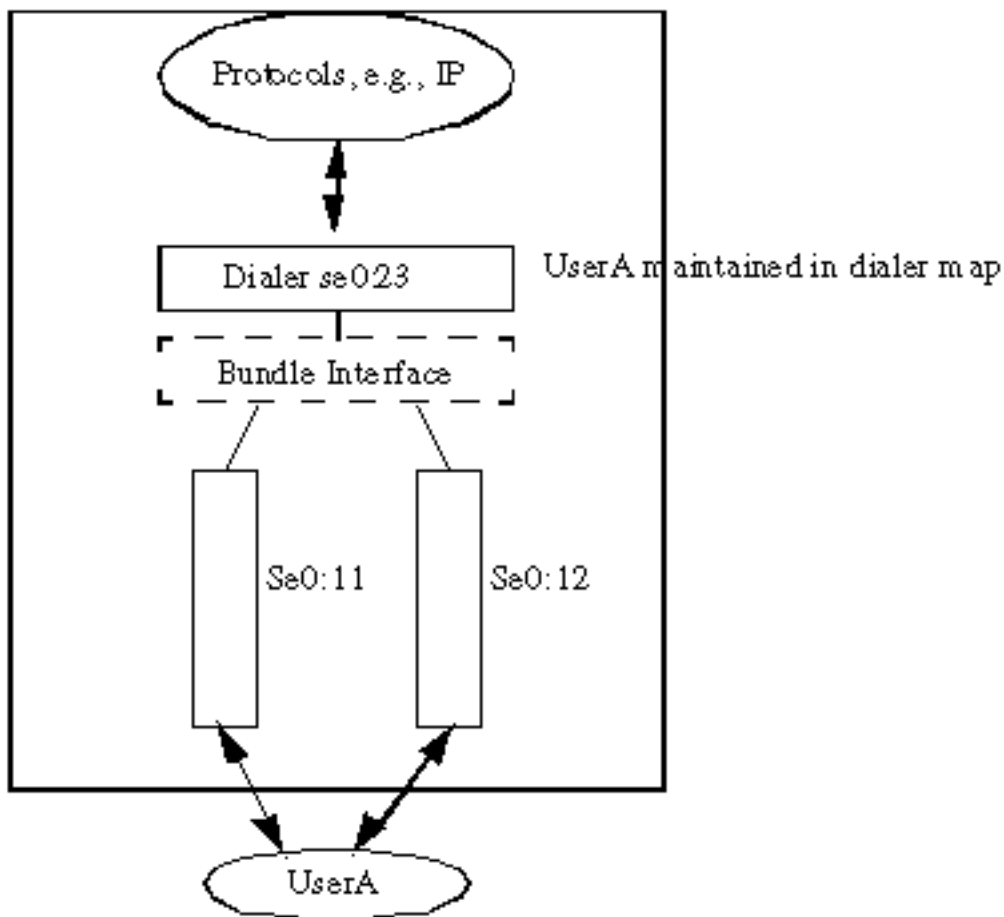


Figure 3. Multilink PPP Interface (Passive)

Se il profilo virtuale è abilitato, lo schema viene ripristinato come mostrato nella Figura 2. In altre parole, se si riceve una chiamata in arrivo su un'interfaccia dialer e il profilo virtuale è abilitato, l'origine della configurazione non sarà più quella della connessione. L'interfaccia Bundle (vedere la Figura 2) è invece l'interfaccia "attiva" su cui verranno letti o scritti tutti i protocolli. L'origine della configurazione è innanzitutto l'interfaccia del modello virtuale, quindi il profilo virtuale di un utente specifico.

L2F

L'inoltro L2F (Link-Level Layer 2 Forwarding) consente di terminare il protocollo PPP su una destinazione remota. In genere, senza L2F, il protocollo PPP è tra il client che ha effettuato la connessione e il server NAS che ha risposto alla chiamata in arrivo. Con L2F, il PPP viene proiettato su un nodo di destinazione. Per quanto riguarda il client, "pensa" di essere collegato al nodo di destinazione tramite PPP. Il NAS, in effetti, diventa un semplice frame forwarder PPP. Nella terminologia L2F, il nodo di destinazione è denominato **Home-Gateway**.

Nel gateway locale, l'interfaccia di accesso virtuale viene utilizzata per terminare il collegamento PPP. Anche in questo caso viene utilizzato un modello virtuale come origine della configurazione. Se è definito il profilo virtuale, la configurazione dell'interfaccia per utente viene applicata all'interfaccia di accesso virtuale.

Il tunnel L2F è attualmente propagato su UDP/IP.

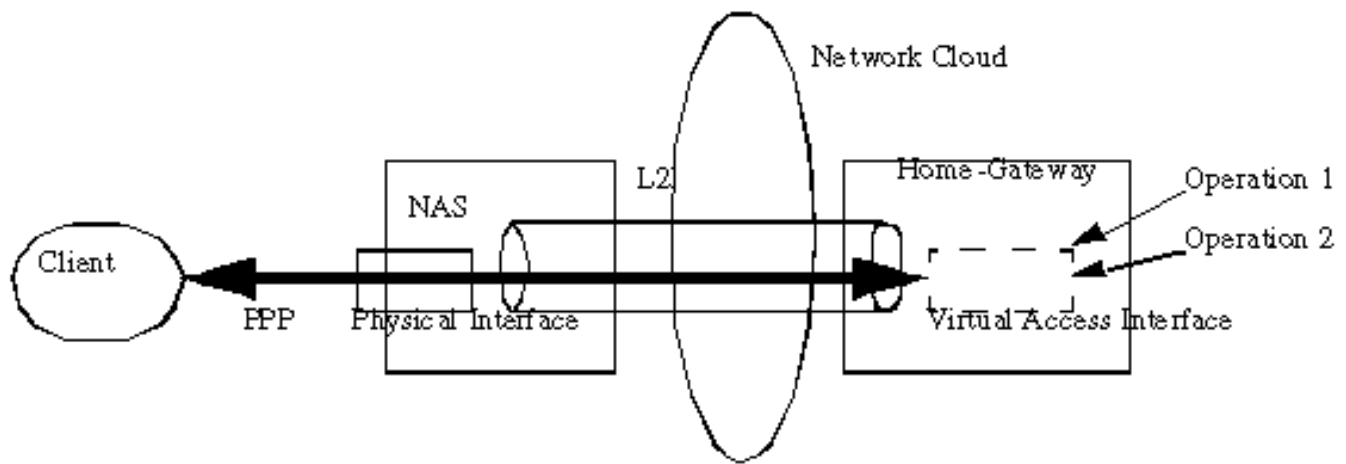


Figure 4. Client PPP to the Home-Gateway via a L2F Tunnel

La tecnologia di tunneling L2F è attualmente utilizzata in due funzionalità di Cisco IOS 11.2: **VPDN** (Virtual Private Dialup Network) e **Multilink PPP** (MMP) multicassis.

VPDN

La **VPDN** consente alle reti private di estendersi dal client direttamente al gateway principale scelto. Ad esempio, gli utenti mobili (ad esempio, i responsabili delle vendite) di HP desiderano poter sempre connettersi al gateway HP Home in qualsiasi momento e in qualsiasi luogo. HP stipulerebbe un contratto per gli ISP che supportano la PDN. Questi ISP sarebbero configurati in modo tale che, se **jsmith@hp.com** compone uno dei numeri forniti dall'ISP, il NAS inoltri automaticamente al gateway HP Home. L'ISP è quindi libero dall'amministrare gli indirizzi IP degli utenti HP, il routing e altre funzioni legate alla base di utenti HP. L'amministrazione ISP di HP viene ridotta ai problemi di connettività IP per HP Home-Gateway.

NAS: isp

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

Home-Gateway: hp-gateway

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

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

Multicassis

PPP Multilink fornisce agli utenti una larghezza di banda aggiuntiva su richiesta, con la possibilità di dividere e ricombinare i pacchetti su una pipe logica (bundle) formata da più collegamenti. Ciò riduce la latenza di trasmissione sui collegamenti WAN lenti e fornisce anche un metodo per aumentare l'unità di ricezione massima. Multilink è supportato in un singolo ambiente Access Server.

Gli ISP, ad esempio, vorrebbero assegnare in modo conveniente un singolo numero rotante a più PRI su più server di accesso, scalabili e flessibili in base alle loro esigenze aziendali.

Con Multicassis Multilink, più collegamenti Multilink dallo stesso client possono terminare in server di accesso diversi. Mentre i singoli collegamenti MP dello stesso bundle possono in realtà terminare su server di accesso diversi, per quanto riguarda il client MP, è come se terminasse su un singolo server di accesso. Quando i componenti vengono confrontati con quelli della VPDN, Mutichassis differisce solo per un protocollo SGBP (Stack Group Bidding Protocol) aggiuntivo per facilitare la licitazione e l'arbitraggio dei bundle Multilink. Una volta che l'indirizzo IP di destinazione del vincitore dello Stack Group è stato stabilito sopra SGBP, Multicassis utilizza L2F per proiettare dal NAS all'altro NAS, che è il vincitore dello Stack Group.

Ad esempio, su uno Stack Group viene chiamato **stackq** di due NAS: **nasa** e **nasb**.

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
```

Traslazione di protocollo

Protocol Translation consente al traffico PPP incapsulato attraverso un gateway, ad esempio X.25/TCP, di terminare come interfaccia di accesso virtuale (traduzione in due passaggi). L'interfaccia di accesso virtuale è supportata oltre alla traduzione in un unico passaggio.

Esempio di traduzione del protocollo in due passaggi:

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

```
ppp authen chap

vty-async virtual-template 1
```

Esempio di traduzione del protocollo in un unico passaggio:

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

translate tcp 1.1.1.1 virtual-template 1
```

PPP over ATM

Questa funzione fornisce il supporto per la terminazione di più connessioni PPP su un'interfaccia ATM del router quando i dati sono formattati in base all'incapsulamento Frame Forwarding di Cisco (StrataCom). Il protocollo PPP viene terminato sul router come se fosse stato ricevuto da un'interfaccia seriale PPP tipica. Ogni connessione PPP verrà incapsulata in un VC ATM separato. Sulla stessa interfaccia possono essere configurati anche i VC che utilizzano altri tipi di incapsulamento.

```
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
```

Profili virtuali

Profili virtuali è un'applicazione PPP univoca che definisce e applica le informazioni di configurazione per utente per gli utenti che si connettono a un router. I profili virtuali consentono l'applicazione di informazioni di configurazione specifiche dell'utente indipendentemente dal supporto utilizzato per la chiamata in ingresso. Le informazioni di configurazione per i profili virtuali possono provenire da un modello di interfaccia virtuale, da informazioni di configurazione per utente memorizzate su un server AAA o da entrambi, a seconda della configurazione del router e del server AAA. L'applicazione dei profili virtuali può essere in un ambiente a scatola singola, in un VPDN Home-Gateway o in un ambiente a più chassis.

Per definire un modello virtuale come origine della configurazione per il profilo virtuale:

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

Per definire il server AAA come origine della configurazione del profilo virtuale:


```
virtual-profile aaa
```

In questo esempio, l'amministratore di sistema decide di filtrare le route annunciate a John e di applicare elenchi di accesso alle connessioni remote di Rick. Quando John o Rick effettuano la chiamata tramite l'interfaccia S1 o BRI 0 e procedono all'autenticazione, viene creato un profilo virtuale: I filtri route vengono applicati a John e gli elenchi access a Rick.

Configurazione AAA per utenti John e 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``
```

In breve, le **coppie AAA/cisco** contengono i comandi per interfaccia di Cisco IOS da applicare per un particolare utente.