Fonctions PPP d'accès virtuel dans Cisco IOS

Contenu

Introduction

Ce document décrit l'architecture globale des applications PPP d'accès virtuel dans Cisco IOS®. Pour plus de renseignements sur une fonction précise, référez-vous aux documents répertoriés à la fin du glossaire.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Glossaire

Les termes suivants apparaîtront dans ce document.

- **Serveur d'accès** : Plates-formes Cisco Access Server, y compris les interfaces RNIS et asynchrones, pour fournir un accès à distance.
- **L2F** : Protocole de transfert de couche 2 (projet expérimental de RFC). Il s'agit de la technologie de niveau de liaison sous-jacente pour les réseaux MP multichâssis et VPN (Virtual Private Networks).
- **Lien** : Point de connexion fourni par un système. Il peut s'agir d'une interface matérielle dédiée (telle qu'une interface asynchrone) ou d'un canal sur une interface matérielle multicanal (telle qu'une interface PRI ou BRI).
- **MP** : Protocole PPP multiliaison (voir RFC 1717).
- **MP multichâssis** : MP + SGBP + L2F + Vtemplate.
- **PPP** : Protocole point à point (voir RFC 1331).
- **Groupe Rotary** : Groupe d'interfaces physiques allouées pour la composition ou la réception d'appels. Le groupe agit comme un pool à partir duquel n'importe quelle liaison peut être utilisée pour composer ou recevoir des appels.
- **SGBP** : Protocole de soumission de groupe de piles
- **Groupe de piles** : Ensemble de deux systèmes ou plus qui seront configurés pour fonctionner en tant que groupe et prendre en charge les ensembles MP avec des liaisons sur différents systèmes.
- **VPDN** : Réseau commuté privé virtuel. Transfert de liaisons PPP d'un fournisseur d'accès à Internet (FAI) vers une passerelle domestique.
- **Vtemplate** : Interface de modèle virtuel.

Remarque : Pour plus d'informations sur les RFC référencées dans ce document, consultez RFC pris en charge dans Cisco IOS version 11.2, un bulletin produit ; ou Obtention de documents RFC et autres documents de normes pour une liaison directe à InterNIC.

Présentation de l'interface d'accès virtuel

Dans la version 11.2F de Cisco IOS, Cisco prend en charge les fonctions d'accès à distance suivantes : VPDN, Multichassis Multilink, VP, Traduction de protocole à l'aide de l'accès virtuel et PPP/ATM. Ces fonctions utilisent des interfaces virtuelles pour transporter le protocole PPP sur leurs machines cibles.

Une interface d'accès virtuel est une interface Cisco IOS, tout comme des interfaces physiques telles qu'une interface série. Une configuration d'interface série se trouve dans la configuration d'interface série.

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

Les interfaces physiques ont des configurations fixes et statiques. Cependant, les interfaces d'accès virtuel sont créées dynamiquement à la demande (les différentes utilisations sont abordées dans la section suivante de ce document). Ils sont également libérés lorsqu'ils ne sont

plus nécessaires. Par conséquent, la **source de configuration** des interfaces d'accès virtuel doit être ancrée par d'autres moyens.

Les différentes méthodes par lesquelles un accès virtuel gagne sa configuration sont via l'interface **Virtual Template** et/ou les enregistrements RADIUS et TACAC+ qui résident sur un serveur d'authentification. Cette dernière méthode est appelée **Profils virtuels** *par utilisateur*. Comme les interfaces d'accès virtuel peuvent être configurées à l'aide d'un modèle virtuel global, les interfaces d'accès virtuel pour différents utilisateurs peuvent hériter de configurations identiques à partir d'une interface de modèle virtuel. Par exemple, l'administrateur réseau peut choisir de définir une méthode d'authentification PPP commune (CHAP) pour tous les utilisateurs d'accès virtuel du système. Pour **des** configurations personnalisées **spécifiques par utilisateur**, l'administrateur réseau peut définir des configurations d'interface, telles que l'authentification PAP, spécifiques à l'utilisateur dans le profil virtuel. En bref, le schéma de configuration général à spécifique disponible pour les interfaces d'accès virtuel permet à l'administrateur réseau d'adapter les configurations d'interface communes à tous les utilisateurs et/ou individuellement adaptées à l'utilisateur.

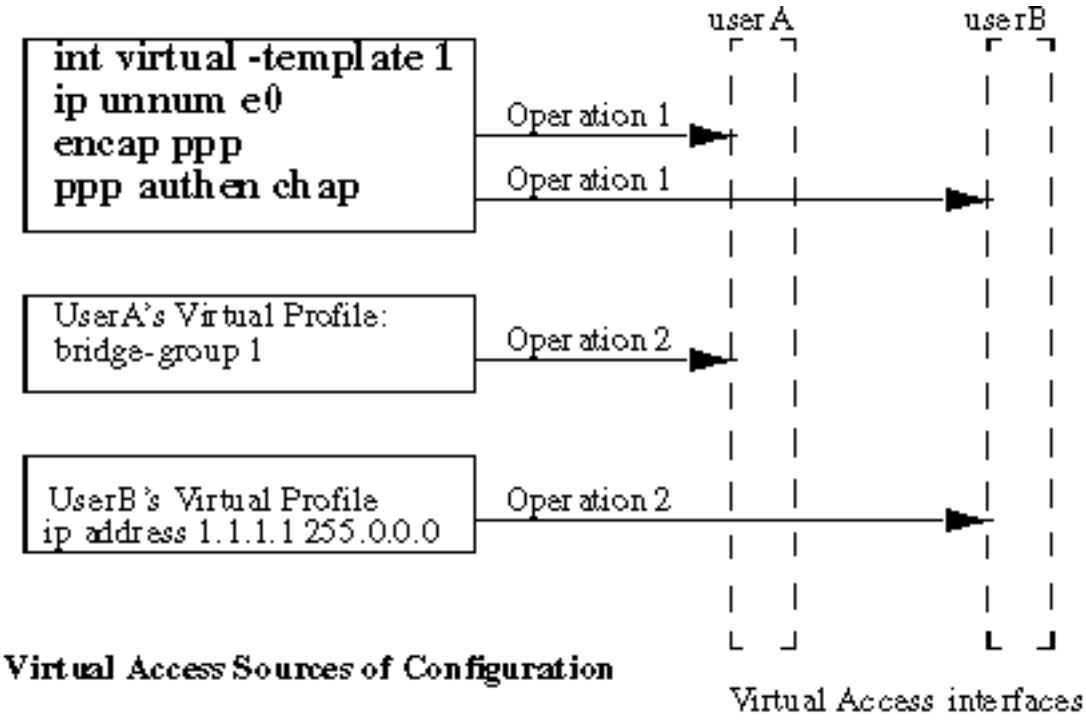

Figure 1. Virtual Access Sources of Configuration

La figure 1 ci-dessus illustre deux des interfaces d'accès virtuel pour l'utilisateur A et l'utilisateur B. L'opération 1 indique l'application de la configuration d'interface d'une interface de modèle virtuel **globale** aux deux interfaces d'accès virtuel. L'opération 2 indique l'application de configurations d'interface par utilisateur de **différents** profils virtuels aux deux interfaces d'accès virtuel.

Applications des interfaces d'accès virtuel

Cette section décrit les différentes manières dont Cisco IOS utilise les interfaces d'accès virtuel.

Vous remarquerez un thème récurrent de chaque application : ils autorisent un modèle virtuel général spécifique à l'application (opération 1). Les profils virtuels par utilisateur sont ensuite appliqués par utilisateur (opération 2)

Multilink PPP

Le protocole PPP multiliaison utilise l’interface d’accès virtuel comme interface d’ensemble pour réassembler les paquets reçus sur des liaisons individuelles et pour fragmenter les paquets envoyés sur des liaisons individuelles. L'interface du bundle obtient sa configuration du modèle virtuel spécifique au protocole PPP multiliaison. Si l'administrateur réseau choisit d'activer les profils virtuels, la configuration de l'interface de profil virtuel par nom d'utilisateur est ensuite appliquée à l'interface de l'ensemble pour cet utilisateur.

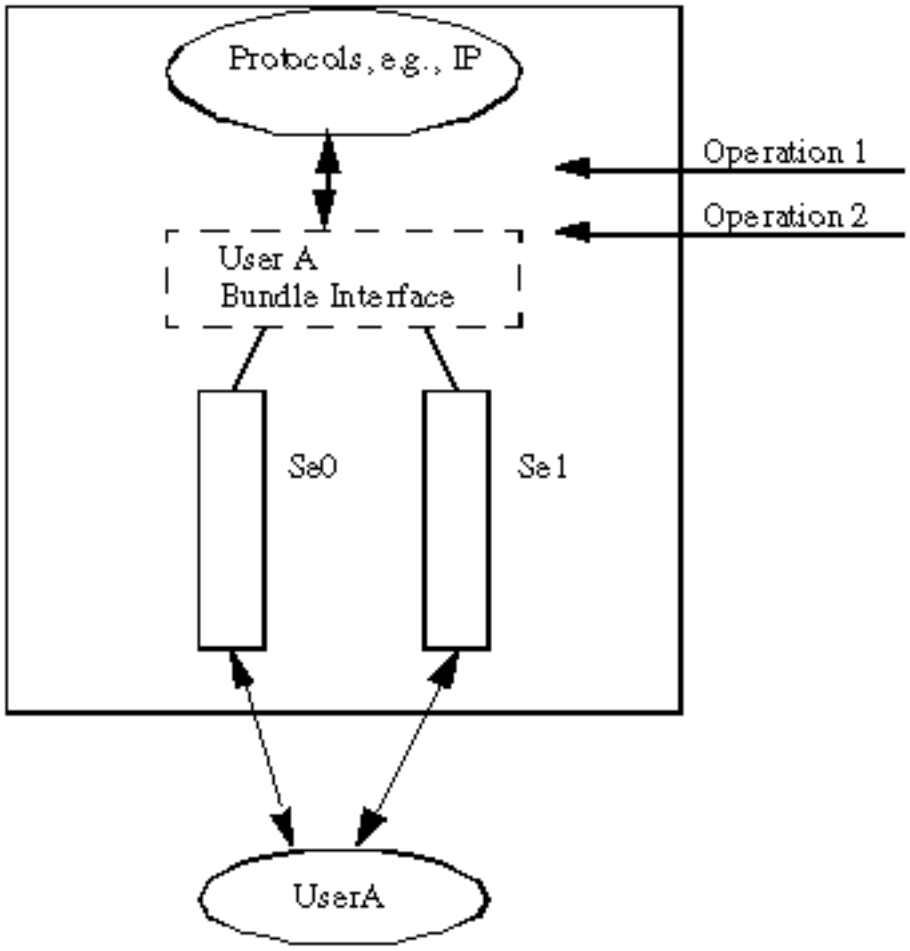

Figure 2. Multilink PPP Bundle Interface

La Figure 2 illustre l'utilisation du protocole PPP multiliaison des interfaces série. Comme il n'y a pas d'interface de numérotation, une interface de modèle virtuel est définie par :

```
multilink virtual-template 1

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

La configuration facultative par nom d'utilisateur Virtual Profile est ensuite appliquée à l'interface de l'offre groupée. Lorsque l'interface de numérotation est impliquée, l'interface de l'offre groupée est une interface passive - aucune interface de modèle virtuel n'est requise.

Par exemple, la Figure 3 ci-dessous illustre un PRI se0:23 configuré pour prendre en charge le protocole PPP multiliaison.

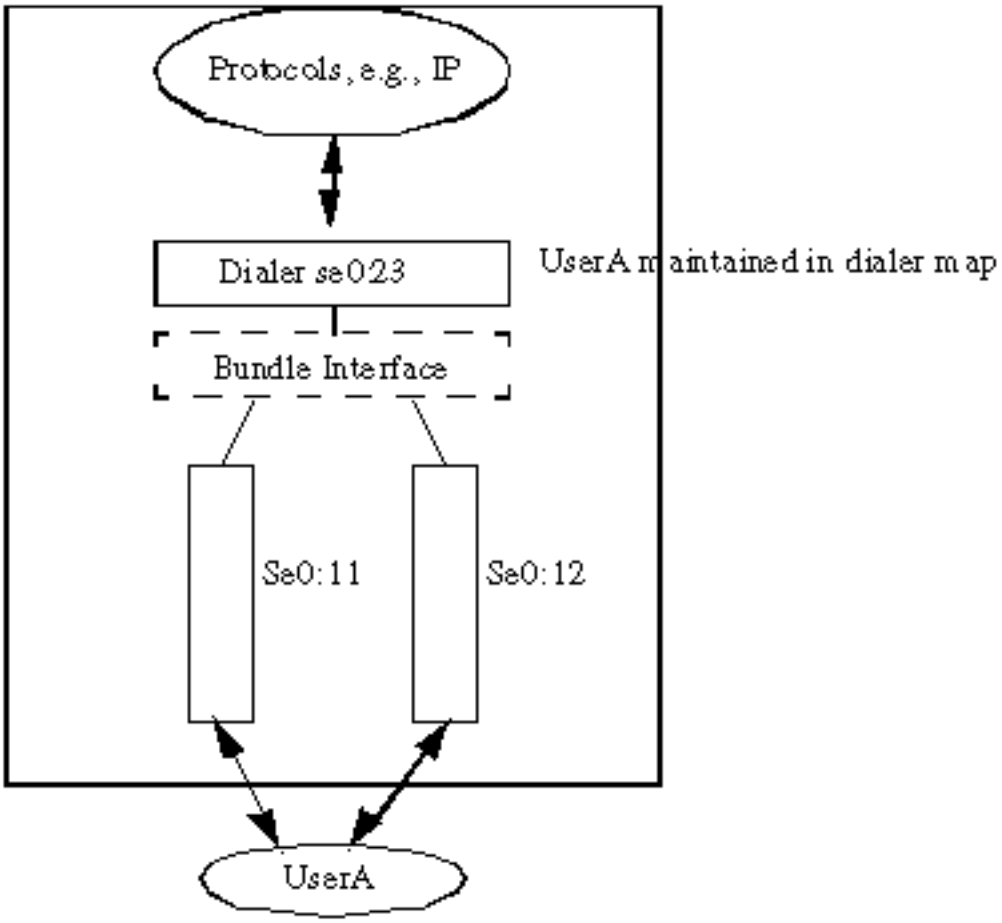

Figure 3. Multilink PPP Interface (Passive)

Notez que si Virtual Profile est activé, le schéma est rétabli comme illustré à la Figure 2. En d'autres termes, si un appel entrant est reçu sur une interface de numérotation et si Virtual Profile est activé, la source de configuration n'est plus celle du numéroteur. Au lieu de cela, l'interface Bundle (voir Figure 2) est l'interface active à laquelle tous les protocoles liront ou seront écrits. La source de configuration est d'abord l'interface Modèle virtuel, puis le profil virtuel pour un utilisateur particulier.

L2F

Le transfert de couche 2 au niveau de la liaison, ou L2F, permet de terminer le protocole PPP sur une destination distante. Normalement, sans L2F, le protocole PPP se situe entre le client connecté et le NAS qui a répondu à l'appel entrant. Avec L2F, le protocole PPP est projeté vers un noeud de destination. En ce qui concerne le client, il « pense » qu'il est connecté au noeud de destination via PPP. En effet, le NAS devient un simple redirecteur de trame PPP. Dans la terminologie L2F, le noeud de destination est appelé **Home-Gateway**.

Au niveau de Home-Gateway, l'interface d'accès virtuel est utilisée pour mettre fin à la liaison PPP. Là encore, un modèle virtuel est utilisé comme source de configuration. Si Virtual Profile est défini, la configuration de l'interface par utilisateur est appliquée à l'interface d'accès virtuel.

Le tunnel L2F est actuellement propagé sur UDP/IP.

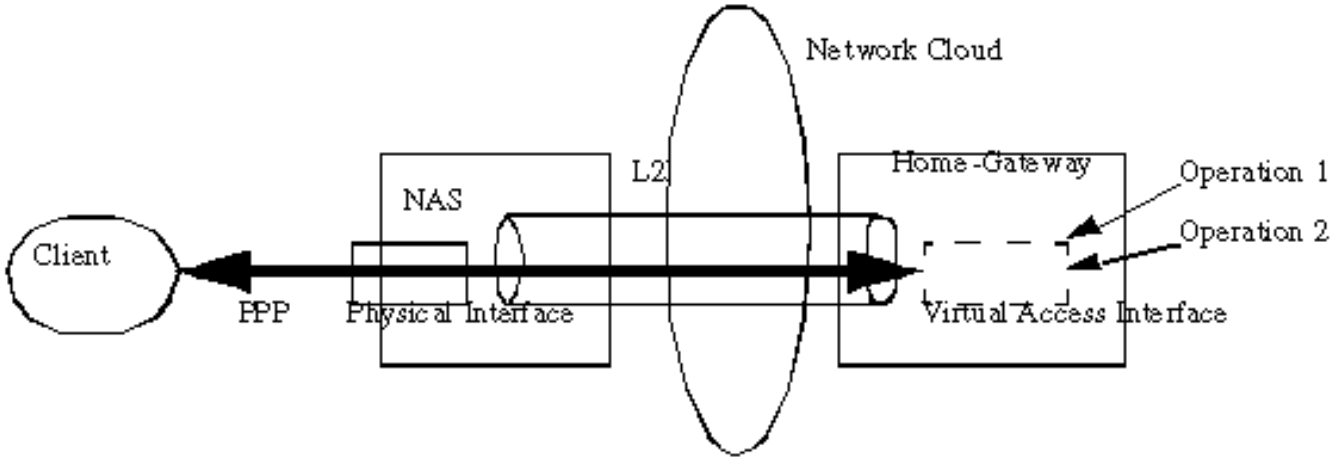

Figure 4. Client PPP to the Home-Gateway via a L2F Tunnel

La technologie de tunnellisation L2F est actuellement utilisée dans deux fonctions de Cisco IOS 11.2 : **VPDN** (Virtual Private Dialup Network) et **Multichassis Multilink PPP** (MMP).

VPDN

VPDN permet aux réseaux privés de s'étendre directement du client à la passerelle domestique de votre choix. Par exemple, les utilisateurs mobiles (les commerciaux, par exemple) de HP souhaitent pouvoir toujours se connecter à HP Home-Gateway de leur choix n'importe où, n'importe quand. HP s'engagerait pour des FAI qui prendraient en charge PDN. Ces FAI seraient configurés de sorte que, si **jsmith@hp.com** compose un numéro fourni par le FAI, le NAS transfère automatiquement vers la passerelle HP Home-Gateway. Le FAI est ainsi libéré de l'administration des adresses IP, du routage et d'autres fonctions des utilisateurs HP liées à la base d'utilisateurs HP. L'administration HP du FAI est réduite aux problèmes de connectivité IP pour la passerelle 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
  encap ppp
  ppp chap authen

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

Multichâssis

PPP Multilink fournit aux utilisateurs une bande passante supplémentaire à la demande, avec la possibilité de fractionner et de recombiner des paquets sur un canal logique (bundle) formé par plusieurs liaisons. Cela réduit la latence de transmission sur les liaisons WAN lentes et fournit également une méthode d'augmentation de l'unité de réception maximale. La multiliaison est prise en charge sur un seul environnement de serveur d'accès.

Les FAI, par exemple, voudraient facilement attribuer un numéro rotatif unique à plusieurs PRI sur plusieurs serveurs d'accès, évolutifs et flexibles pour répondre à leurs besoins métier.

Avec Multichassis Multilink, plusieurs liaisons Multilink du même client peuvent se terminer sur différents serveurs d'accès. Bien que les liaisons MP individuelles d'un même bundle puissent effectivement se terminer sur différents serveurs d'accès, dans la mesure où le client MP est concerné, c'est comme s'il se terminait sur un seul serveur d'accès. Lorsque les composants sont comparés à ceux du VPDN, Mutichassis ne diffère que par un protocole d'enchère StackGroup supplémentaire (SGBP) pour faciliter l'appel d'offres et l'arbitrage des offres multiliaison. Une fois que l'adresse IP de destination du gagnant du groupe de piles est décidée sur SGBP, Multichassis utilise L2F pour projeter du NAS vers l'autre NAS, lequel est le gagnant du groupe de piles.

Par exemple, sur un groupe de piles, appelle **la pile** de deux NAS : **nasa** et **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
```

Traduction de protocole

La traduction de protocoles permet au trafic encapsulé PPP sur une passerelle (par exemple X.25/TCP) de se terminer en tant qu'interface d'accès virtuel (traduction en deux étapes). L'interface d'accès virtuel est également prise en charge sur la traduction en une étape.

Exemple de traduction de protocole en deux étapes :

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

```
  ppp authen chap

  vty-async virtual-template 1
```

Exemple de traduction de protocole en une étape :

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

  translate tcp 1.1.1.1 virtual-template 1
```

PPP sur ATM

Cette fonctionnalité permet de mettre fin à plusieurs connexions PPP sur une interface ATM de routeur lorsque les données sont formatées conformément à l'encapsulation de transfert de trames de Cisco (StrataCom). Le protocole PPP s’arrête sur le routeur comme s’il avait été reçu d’une interface série PPP classique. Chaque connexion PPP est encapsulée dans un circuit virtuel ATM distinct. Les circuits virtuels utilisant d’autres types d’encapsulation peuvent également être configurés sur la même interface.

```
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
```

Profils virtuels

Virtual Profiles est une application PPP unique qui définit et applique les informations de configuration par utilisateur aux utilisateurs qui se connectent à un routeur. Les profils virtuels permettent d'appliquer des informations de configuration spécifiques à l'utilisateur quel que soit le support utilisé pour l'appel entrant. Les informations de configuration des profils virtuels peuvent provenir d'un modèle d'interface virtuelle, d'informations de configuration par utilisateur stockées sur un serveur AAA, ou les deux, selon la configuration du routeur et du serveur AAA. L'application de profils virtuels peut se trouver dans un environnement unique, dans une passerelle résidentielle VPDN ou dans un environnement multichâssis.

Pour définir un modèle virtuel comme source de configuration pour le profil virtuel :

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

Pour définir AAA comme source de configuration pour Virtual Profile :

```
virtual-profile aaa
```

Dans cet exemple, l'administrateur système décide de filtrer les routes annoncées à John et d'appliquer des listes d'accès aux connexions commutées de Rick. Lorsque John ou Rick se connecte via l'interface S1 ou BRI 0 et s'authentifie, un profil virtuel est créé : les filtres de route sont appliqués à John et les listes d'accès à Rick.

Configuration AAA pour les utilisateurs John et 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''
```

En résumé, l'AAA cisco-avpair contient des commandes Cisco IOS par interface à appliquer à un utilisateur particulier.