Configuration de CiscoSecure ACS pour l'authentification PPTP de routeurs Windows

Contenu

Introduction

La prise en charge du protocole PPTP (Point-to-Point Tunnel Protocol) a été ajoutée au logiciel Cisco IOS® Version 12.0.5.XE5 sur les plates-formes Cisco 7100 et 7200 (reportez-vous à PPTP avec Microsoft Point-to-Point Encryption (MPPE) [Logiciel Cisco IOS Version 12.0]). La prise en charge d'autres plates-formes a été ajoutée dans le logiciel Cisco IOS Version 12.1.5.T (reportez-vous à MSCHAP Version 2).

RFC 2637 décrit PPTP. En termes PPTP, selon le RFC, le concentrateur d'accès PPTP (PAC) est le client (le PC, c'est-à-dire l'appelant) et le serveur réseau PPTP (PNS) est le serveur (le routeur, l'appelé).

Ce document suppose que les connexions PPTP au routeur avec l'authentification Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) V1 locale (et éventuellement MPPE, qui nécessite MS-CHAP V1) ont été créées avec l'utilisation de ces documents et sont déjà opérationnelles. RADIUS est requis pour la prise en charge du chiffrement MPPE. TACACS+ fonctionne pour l'authentification, mais pas pour la clé MPPE. La prise en charge de MS-CHAP V2

a été ajoutée au logiciel Cisco IOS Version 12.2(2)XB5 et a été intégrée dans le logiciel Cisco IOS Version 12.2(13)T (voir MSCHAP Version 2), mais MPPE n'est pas encore pris en charge avec MS-CHAP V2.

Cet exemple de configuration montre comment configurer une connexion PC au routeur (à l'adresse 10.66.79.99), qui fournit ensuite l'authentification utilisateur au serveur Cisco Secure Access Control System (ACS) 4.2 pour Windows (à l'adresse 10.66.79.120), avant d'autoriser l'utilisateur à accéder au réseau.

Remarque : le serveur RADIUS n'est généralement pas situé en dehors du routeur, sauf dans un environnement de travaux pratiques.

La prise en charge PPTP a été ajoutée à Cisco Secure ACS 2.5, mais peut ne pas fonctionner avec le routeur en raison de l'ID de bogue Cisco CSCds92266 (clients enregistrés uniquement). ACS 2.6 et versions ultérieures n'ont pas ce problème.

Cisco Secure UNIX ne prend pas en charge MPPE. Microsoft RADIUS et Funk RADIUS sont deux autres applications RADIUS prises en charge par MPPE.

Référez-vous à Configuration du routeur Cisco et des clients VPN à l'aide de PPTP et MPPE pour plus d'informations sur la façon de configurer PPTP et MPPE avec un routeur.

Référez-vous à Configuration du concentrateur VPN 3000 et du protocole PPTP avec Cisco Secure ACS pour l'authentification RADIUS Windows pour plus d'informations sur la configuration du protocole PPTP sur un concentrateur VPN 3000 avec Cisco Secure ACS pour l'authentification RADIUS.

Consultez PIX 6.x : Exemple de configuration de PPTP avec l'authentification Radius afin de configurer les connexions PPTP au PIX.

Conditions préalables

Conditions requises

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure ACS 4.2 pour Windows
- Routeur Cisco 3600
- Logiciel Cisco IOS Version 12.4(3)

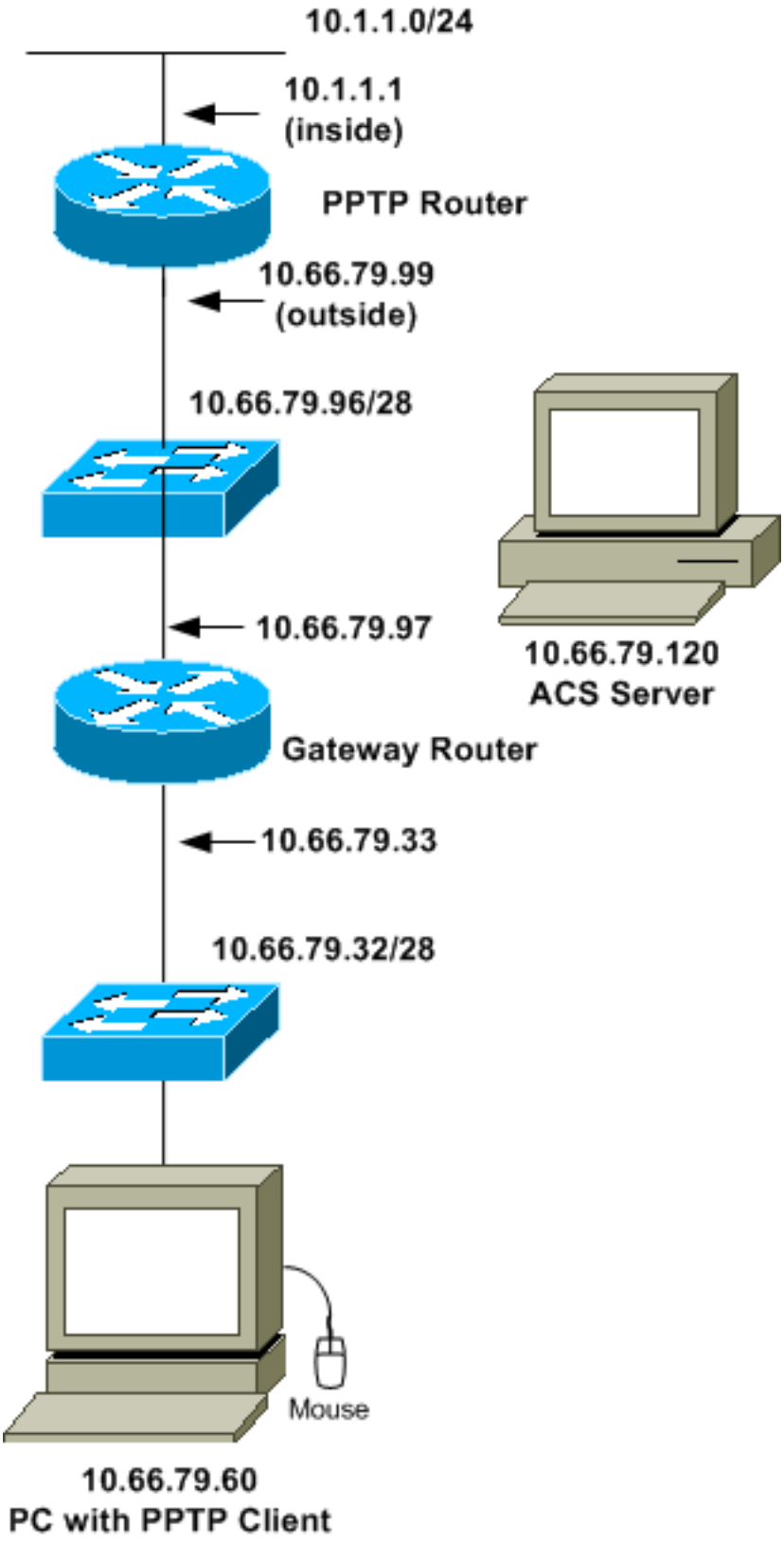
Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous êtes dans un réseau actif, assurez-vous de bien comprendre l'impact potentiel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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration du routeur

Utilisez cette configuration de routeur. L'utilisateur doit être en mesure de se connecter avec "**username john password doe**" même si le serveur RADIUS est inaccessible (ce qui est possible si le serveur n'a pas encore été configuré avec Cisco Secure ACS). Cet exemple suppose que l'authentification locale (et éventuellement le chiffrement) est déjà opérationnelle.

Routeur Cisco 3600

```
Current configuration : 1729 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname moss
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username john password 0 doe
aaa new-model
!

aaa authentication ppp default group radius local

aaa authentication login default local

!--- In order to set authentication, authorization, and
accounting (AAA) authentication !--- at login, use the
aaa authentication login command in global !---
configuration mode as shown above.


aaa authorization network default group radius if-
authenticated
aaa session-id common
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
!--- Default PPTP VPDN group. accept-dialin
protocol pptp
virtual-template 1
!
no ftp-server write-enable
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
!
interface Ethernet0/1
ip address 10.66.79.99 255.255.255.224
half-duplex
!
```

```
interface Virtual-Template1
ip unnumbered Ethernet0/1
peer default ip address pool testpool
ppp authentication ms-chap
!
ip local pool testpool 192.168.1.1 192.168.1.254
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
radius-server host 10.66.79.120 auth-port 1645 acct-port
1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
line aux 0
line vty 0 4
password cisco
!
end
```

Fonctionnalité de secours du serveur RADIUS

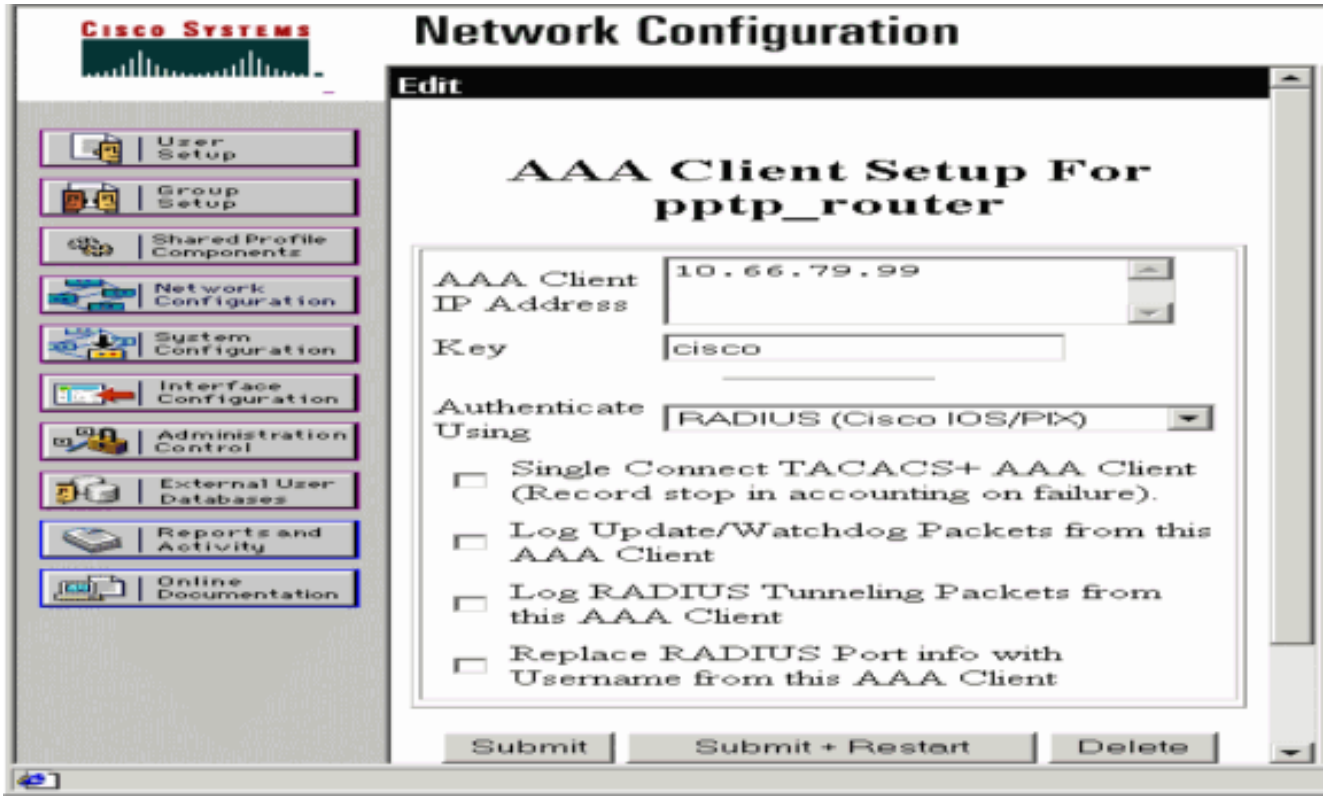
Lorsque le serveur RADIUS principal devient indisponible, le routeur bascule vers le serveur RADIUS de sauvegarde actif suivant. Le routeur continuera à utiliser le serveur RADIUS secondaire pour toujours, même si le serveur principal est disponible. Généralement, le serveur principal est hautes performances et le serveur préféré.

Afin de définir l'authentification AAA (Authentication, Authorization and Accounting) lors de la connexion, utilisez la commande aaa authentication login en mode de configuration globale.

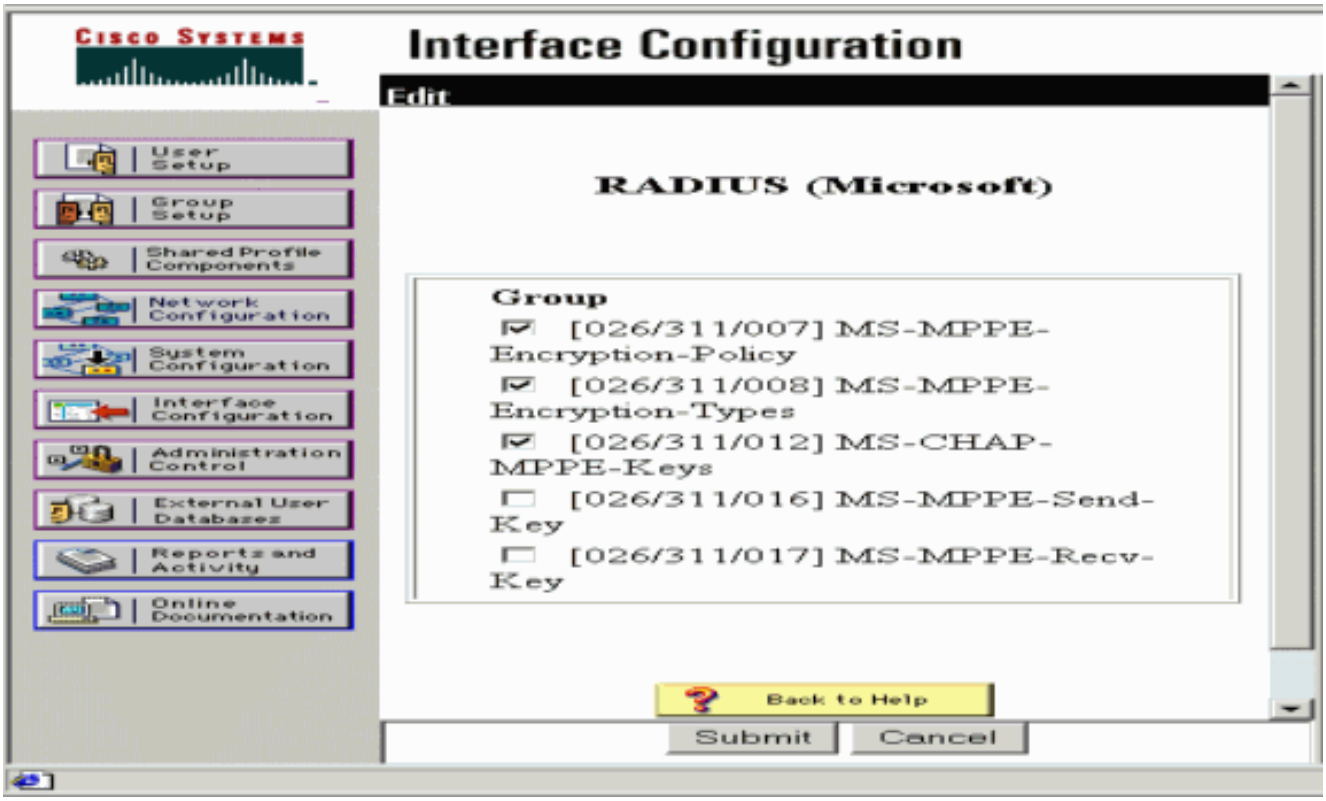
Configuration de Cisco Secure ACS pour Windows

Utilisez cette procédure pour configurer Cisco Secure ACS :

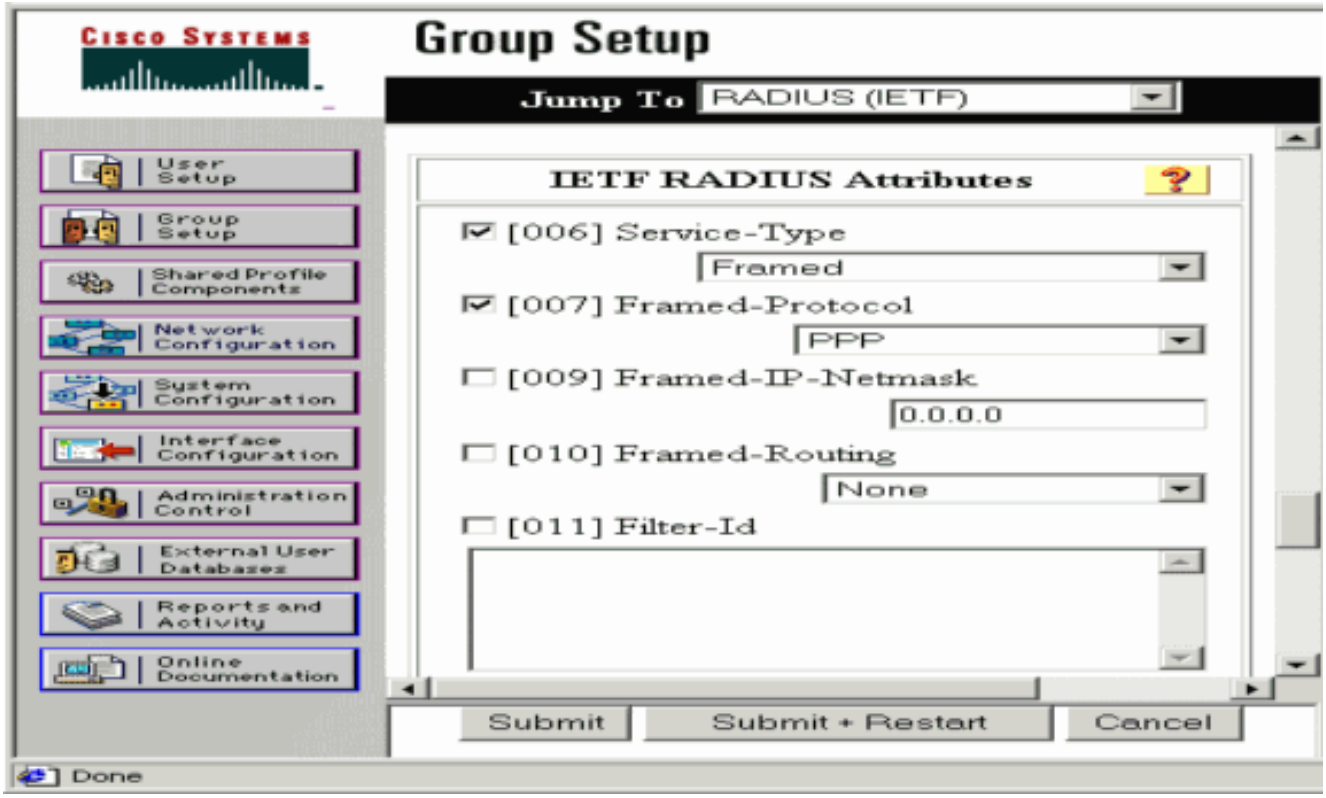
1. Cliquez sur **Configuration réseau**, ajoutez une entrée pour le routeur, puis cliquez sur **Soumettre + Redémarrer** lorsque vous avez terminé.



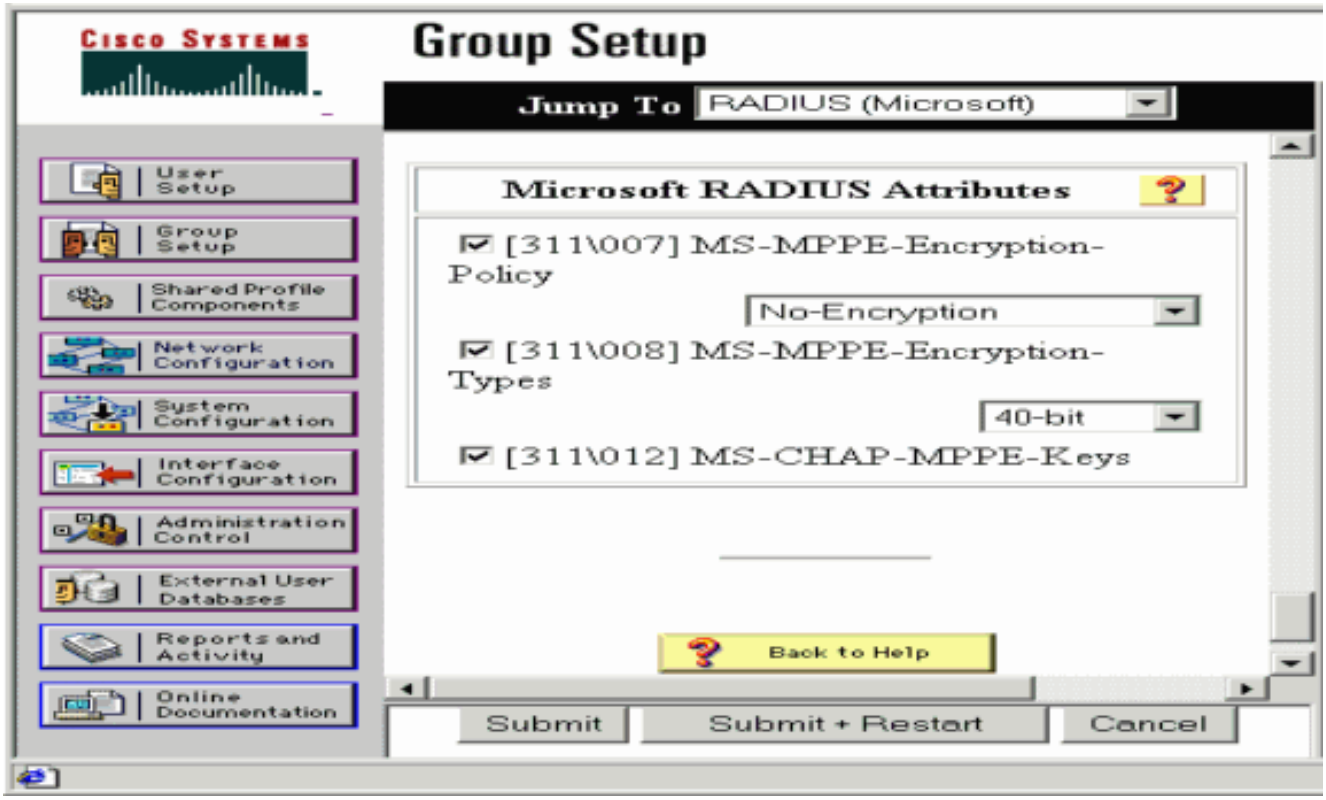
2. Sélectionnez **Interface Configuration > RADIUS (Microsoft)**, puis vérifiez vos attributs MPPE et cliquez sur
Submit.



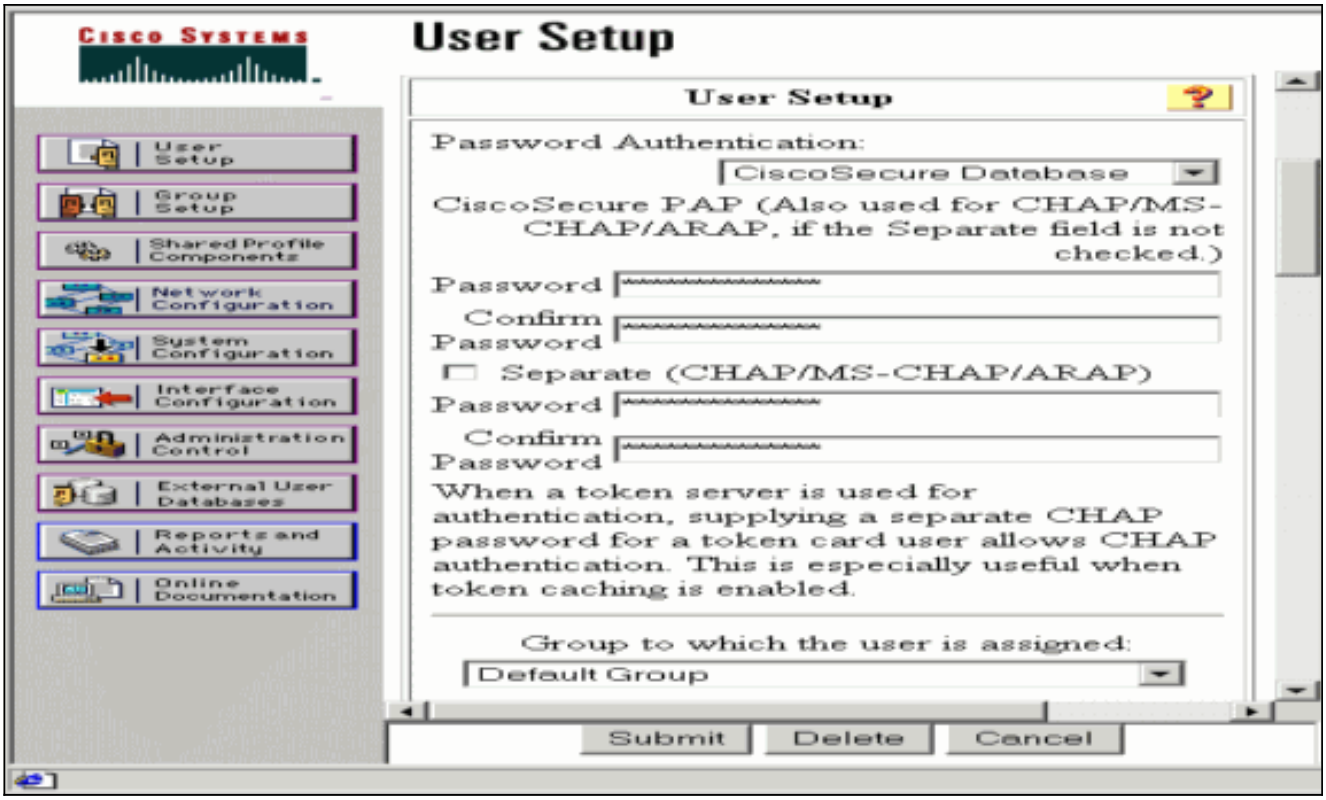
3. Cliquez sur **Configuration du groupe** et, pour Service-Type, sélectionnez **Cadre**. Pour Framed-Protocol, sélectionnez **PPP** et cliquez sur
Submit.



4. Dans **Configuration du groupe**, vérifiez les informations RADIUS MS-MPPE et, lorsque vous avez terminé, cliquez sur **Soumettre + Redémarrer**.



5. Cliquez sur **User Setup**, ajoutez un mot de passe, affectez l'utilisateur au groupe et cliquez sur **Submit**.



6. Testez l'authentification sur le routeur avant d'ajouter le chiffrement. Si l'authentification ne fonctionne pas, consultez la section Dépannage de ce document.

Ajout à la configuration

Ajout du chiffrement

Vous pouvez ajouter le chiffrement MPPE avec cette commande :

```
interface virtual-template 1
(config-if)#ppp encrypt mppe 40|128|auto passive|required|stateful
```

Comme l'exemple suppose que le chiffrement fonctionne avec l'authentification locale (nom d'utilisateur et mot de passe sur le routeur), le PC est configuré correctement. Vous pouvez maintenant ajouter cette commande pour une flexibilité maximale :

```
ppp encrypt mppe auto
```

Attribution d'adresses IP statiques à partir du serveur

Si vous devez attribuer une adresse IP particulière à l'utilisateur, dans Configuration utilisateur ACS, sélectionnez **Affecter une adresse IP statique** et indiquez l'adresse IP.

Ajouter des listes d'accès au serveur

Afin de contrôler ce à quoi l'utilisateur PPTP peut accéder une fois connecté au routeur, vous

pouvez configurer une liste d'accès sur le routeur. Par exemple, si vous émettez cette commande :

```
access-list 101 permit ip any host 10.1.1.2 log
```

et choisissez **Filter-Id (attribut 11)** dans ACS et entrez **101** dans la zone, l'utilisateur PPTP peut accéder à l'hôte 10.1.1.2 mais pas aux autres. Lorsque vous émettez une commande **show ip interface virtual-access** *x, où x* est un nombre que vous pouvez déterminer à partir d'une commande **show user**, la liste d'accès doit s'afficher comme appliquée :

```
Inbound access list is 101
```

Ajoutez la gestion des comptes

Vous pouvez ajouter la comptabilité des sessions à l'aide de cette commande :

```
aaa accounting network default start-stop radius
```

Les enregistrements comptables dans Cisco Secure ACS apparaissent comme le montre ce résultat :

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,
Acct-Status-Type,Acct-Session-Id,Acct-Session-Time,
Service-Type,Framed-Protocol,Acct-Input-Octets,
Acct-Output-Octets,Acct-Input-Packets,Acct-Output-Packets,
Framed-IP-Address,NAS-Port,NAS-IP-Address
09/28/2003,20:58:37,georgia,Default Group,,Start,00000005,,
Framed,PPP,,,,,,5,10.66.79.99
09/28/2000,21:00:38,georgia,Default Group,,Stop,00000005,121,
Framed,PPP,3696,1562,49,
38,192.168.1.1,5,10.66.79.99
```

Remarque : des sauts de ligne ont été ajoutés à l'exemple à des fins d'affichage. Les sauts de ligne dans votre sortie réelle sont différents de ceux affichés ici.

transmission tunnel partagée

Lorsque le tunnel PPTP apparaît sur le PC, le routeur PPTP est installé avec une métrique supérieure à la métrique par défaut précédente, de sorte que vous perdez la connectivité Internet. Afin de remédier à cette situation, étant donné que le réseau à l'intérieur du routeur est 10.1.1.X, exécutez un fichier batch (batch.bat) pour modifier le routage Microsoft afin de supprimer le routage par défaut et de réinstaller la route par défaut (cela nécessite l'adresse IP attribuée au client PPTP ; par exemple, 192.168.1.1) :

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 10.66.79.33 metric 1
route add 10.1.1.0 mask 255.255.255.0 192.168.1.1 metric 1
```

Vérification

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show vpdn session** - Affiche des informations sur le tunnel de protocole L2F (L2F) actif et les identificateurs de message dans un réseau commuté privé virtuel (VPDN).

```
moss#show vpdn session
%No active L2TP tunnels
%No active L2F tunnels

PPTP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf    Username      State   Last Chg Uniq ID
7     32768 7     Vi3     georgia       estabd  00:00:25 6
moss#show vpdn
%No active L2TP tunnels
%No active L2F tunnels

PPTP Tunnel and Session Information Total tunnels 1 sessions 1
LocID Remote Name     State    Remote Address  Port  Sessions VPDN Group
7                     estabd   10.66.79.60     3454  1        1

LocID RemID TunID Intf    Username      State   Last Chg Uniq ID
7     32768 7     Vi3     georgia       estabd  00:00:51 6
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. **Le PC spécifie le chiffrement, mais le routeur ne le spécifie pas.**L'utilisateur du PC voit :
   ```
   The remote computer does not support the required data encryption type.
   ```
2. **Le PC et le routeur spécifient tous deux le chiffrement, mais le serveur RADIUS n'est pas configuré pour envoyer les clés MPPE (celles-ci apparaissent normalement sous l'attribut 26).**L'utilisateur du PC voit :
   ```
   The remote computer does not support the required
   data encryption type.
   ```
3. **Le routeur spécifie le chiffrement (obligatoire), mais le PC n'est pas autorisé.**L'utilisateur du PC voit :
   ```
   The specified port is not connected.
   ```
4. **L'utilisateur entre un nom d'utilisateur ou un mot de passe incorrect.**L'utilisateur du PC voit :
   ```
   Access was denied because the username and/or
   password was invalid on the domain.
   ```
   Le **débogage** du routeur indique :**Remarque :** des sauts de ligne ont été ajoutés à cet exemple à des fins d'affichage. Les sauts de ligne dans votre sortie réelle sont différents de ceux affichés ici.
   ```
   Sep 28 21:34:16.299: RADIUS: Received from id 21645/13 10.66.79.120:1645,
   Access-Reject, len 54
   Sep 28 21:34:16.299: RADIUS: authenticator 37 BA 2B 4F 23 02 44 4D - D4
   A0 41 3B 61 2D 5E 0C
   Sep 28 21:34:16.299: RADIUS:  Vendor, Microsoft   [26]  22
   Sep 28 21:34:16.299: RADIUS:   MS-CHAP-ERROR      [2]   16
   Sep 28 21:34:16.299: RADIUS:   01 45 3D 36 39 31 20 52 3D 30 20 56 3D
   [?E=691 R=0 V=]
   Sep 28 21:34:16.299: RADIUS:  Reply-Message       [18]  12
   ```

```
Sep 28 21:34:16.299: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
```

5. **Le serveur RADIUS n'est pas communicatif.**L'utilisateur du PC voit :
   ```
   Access was denied because the username and/or password
   was invalid on the domain.
   ```
   Le **débogage** du routeur indique :**Remarque :** des sauts de ligne ont été ajoutés à cet exemple à des fins d'affichage. Les sauts de ligne dans votre sortie réelle sont différents de ceux affichés ici.
   ```
   Sep 28 21:46:56.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
   for id 21645/43
   Sep 28 21:47:01.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
   for id 21645/43
   Sep 28 21:47:06.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)
   for id 21645/43
   Sep 28 21:47:11.135: RADIUS: No response from (10.66.79.120:1645,1646)
   for id 21645/43
   Sep 28 21:47:11.135: RADIUS/DECODE: parse response no app start; FAIL
   Sep 28 21:47:11.135: RADIUS/DECODE: parse response; FAIL
   ```

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Si les choses ne fonctionnent pas, les commandes **de débogage** minimales incluent :

- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.
- **debug ppp negotiation** - Affiche les paquets PPP transmis lors du démarrage PPP, où les options PPP sont négociées.
- **debug ppp authentication** - Affiche les messages de protocole d'authentification, qui incluent les échanges de paquets CHAP et les échanges PAP (Password Authentication Protocol).
- **debug radius** : affiche les informations de débogage détaillées associées au RADIUS.

Si l'authentification fonctionne, mais qu'il existe des problèmes avec le chiffrement MPPE, utilisez ces commandes :

- **debug ppp mppe packet** : affiche tout le trafic MPPE entrant et sortant.
- **debug ppp mppe event** : affiche les occurrences MPPE clés.
- **debug ppp mppe detail** : affiche des informations MPPE détaillées.
- **debug vpdn l2x-packets** —Affiche les messages relatifs aux en-têtes et à l'état des protocoles L2F.
- **debug vpdn events** : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel.
- **debug vpdn errors** : affiche les erreurs qui empêchent l'établissement d'un tunnel ou les erreurs qui provoquent la fermeture d'un tunnel établi.
- **debug vpdn packets** —Affiche chaque paquet de protocole échangé. Cette option peut entraîner un grand nombre de messages de débogage et vous ne devez généralement utiliser cette commande que sur un châssis de débogage avec une seule session active.

Vous pouvez également utiliser ces commandes à des fins de dépannage :

- **clear interface virtual-access** *x* : arrête un tunnel spécifié et toutes les sessions dans le tunnel.

Exemple de sortie de débogage correct

Ce débogage montre les événements significatifs de la RFC :

- **SCCRQ** = Start-Control-Connection-Request - octets de code de message 9 et 10 = 0001
- **SCCRP** = Start-Control-Connection-Reply
- **OCRQ** = Appel sortant - Octets de code de message 9 et 10 = 0007
- **OCRP** = Appels sortants-Réponse

Remarque : des sauts de ligne ont été ajoutés à cet exemple à des fins d'affichage. Les sauts de ligne dans votre sortie réelle sont différents de ceux affichés ici.

```
moss#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP protocol negotiation debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
VPN:
  L2X control packets debugging is on
Sep 28 21:53:22.403:  Tnl 23 PPTP:
I 009C00011A2B3C4D000100000100000000000010000...
Sep 28 21:53:22.403:  Tnl 23 PPTP: I SCCRQ
Sep 28 21:53:22.403:  Tnl 23 PPTP: protocol version 100
Sep 28 21:53:22.403:  Tnl 23 PPTP: framing caps 1
Sep 28 21:53:22.403:  Tnl 23 PPTP: bearer caps 1
Sep 28 21:53:22.403:  Tnl 23 PPTP: max channels 0
Sep 28 21:53:22.403:  Tnl 23 PPTP: firmware rev 893
Sep 28 21:53:22.403:  Tnl 23 PPTP: hostname ""
Sep 28 21:53:22.403:  Tnl 23 PPTP: vendor "Microsoft Windows NT"
Sep 28 21:53:22.403:  Tnl 23 PPTP: O SCCRP
Sep 28 21:53:22.407:  Tnl 23 PPTP: I
00A800011A2B3C4D0007000080007C0E0000012C05F5...
Sep 28 21:53:22.407:  Tnl 23 PPTP: CC I OCRQ
Sep 28 21:53:22.407:  Tnl 23 PPTP: call id 32768
Sep 28 21:53:22.411:  Tnl 23 PPTP: serial num 31758
Sep 28 21:53:22.411:  Tnl 23 PPTP: min bps 300
Sep 28 21:53:22.411:  Tnl 23 PPTP: max bps 100000000
Sep 28 21:53:22.411:  Tnl 23 PPTP: bearer type 3
Sep 28 21:53:22.411:  Tnl 23 PPTP: framing type 3
Sep 28 21:53:22.411:  Tnl 23 PPTP: recv win size 64
Sep 28 21:53:22.411:  Tnl 23 PPTP: ppd 0
Sep 28 21:53:22.411:  Tnl 23 PPTP: phone num len 0
Sep 28 21:53:22.411:  Tnl 23 PPTP: phone num ""
Sep 28 21:53:22.411: AAA/BIND(0000001C): Bind i/f Virtual-Template1
Sep 28 21:53:22.415:  Tnl/Sn 23/23 PPTP: CC O OCRP
Sep 28 21:53:22.415: ppp27 PPP: Using vpn set call direction
Sep 28 21:53:22.415: ppp27 PPP: Treating connection as a callin
Sep 28 21:53:22.415: ppp27 PPP: Phase is ESTABLISHING, Passive Open
Sep 28 21:53:22.415: ppp27 LCP: State is Listen
Sep 28 21:53:22.459:  Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
Sep 28 21:53:22.459:  Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.459: ppp27 LCP: I CONFREQ [Listen] id 0 len 44
Sep 28 21:53:22.459: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
```

```
Sep 28 21:53:22.459: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.459: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.459: ppp27 LCP:    Callback 6  (0x0D0306)
Sep 28 21:53:22.459: ppp27 LCP:    MRRU 1614 (0x1104064E)
Sep 28 21:53:22.459: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.459: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.463: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREQ [Listen] id 1 len 15
Sep 28 21:53:22.463: ppp27 LCP:    AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.463: ppp27 LCP:    MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREJ [Listen] id 0 len 11
Sep 28 21:53:22.463: ppp27 LCP:    Callback 6  (0x0D0306)
Sep 28 21:53:22.463: ppp27 LCP:    MRRU 1614 (0x1104064E)
Sep 28 21:53:22.467: ppp27 LCP: I CONFACK [REQsent] id 1 len 15
Sep 28 21:53:22.467: ppp27 LCP:    AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.467: ppp27 LCP:    MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.467: ppp27 LCP: I CONFREQ [ACKrcvd] id 1 len 37
Sep 28 21:53:22.467: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.467: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.467: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: O CONFACK [ACKrcvd] id 1 len 37
Sep 28 21:53:22.471: ppp27 LCP:    MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.471: ppp27 LCP:    PFC (0x0702)
Sep 28 21:53:22.471: ppp27 LCP:    ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP:    EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP:     (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP:     (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: State is Open
Sep 28 21:53:22.471: ppp27 PPP: Phase is AUTHENTICATING, by this end
Sep 28 21:53:22.475: ppp27 MS-CHAP: O CHALLENGE id 1 len 21 from "SV3-2   "
Sep 28 21:53:22.475:  Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
Sep 28 21:53:22.475:  Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 2 len
18 magic 0x377413E2 MSRASV5.00
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 3 len
30 magic 0x377413E2 MSRAS-0-CSCOAPACD12364
Sep 28 21:53:22.479: ppp27 MS-CHAP: I RESPONSE id 1 len 61 from "georgia"
Sep 28 21:53:22.483: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.483: ppp27 PPP: Phase is AUTHENTICATING, Unauthenticated User
Sep 28 21:53:22.483: AAA/AUTHEN/PPP (0000001C): Pick method list 'default'
Sep 28 21:53:22.483: RADIUS:  AAA Unsupported     [152] 14
Sep 28 21:53:22.483: RADIUS:   55 6E 69 71 2D 53 65 73 73 2D 49 44
[Uniq-Sess-ID]
Sep 28 21:53:22.483: RADIUS(0000001C): Storing nasport 27 in rad_db
Sep 28 21:53:22.483: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.483: RADIUS/ENCODE(0000001C): acct_session_id: 38
Sep 28 21:53:22.487: RADIUS(0000001C): sending
Sep 28 21:53:22.487: RADIUS/ENCODE: Best Local IP-Address 10.66.79.99
for Radius-Server 10.66.79.120
Sep 28 21:53:22.487: RADIUS(0000001C): Send Access-Request to
10.66.79.120:1645 id 21645/44, len 133
Sep 28 21:53:22.487: RADIUS:  authenticator 15 8A 3B EE 03 24
0C F0 - 00 00 00 00 00 00 00 00
Sep 28 21:53:22.487: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
Sep 28 21:53:22.487: RADIUS:  User-Name           [1]   9   "georgia"
Sep 28 21:53:22.487: RADIUS:  Vendor, Microsoft   [26]  16
Sep 28 21:53:22.487: RADIUS:   MSCHAP_Challenge   [11]  10
Sep 28 21:53:22.487: RADIUS:   15 8A 3B EE 03 24 0C  [??;??$?]
Sep 28 21:53:22.487: RADIUS:  Vendor, Microsoft   [26]  58
Sep 28 21:53:22.487: RADIUS:   MS-CHAP-Response   [1]   52  *
```

```
Sep 28 21:53:22.487: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Sep 28 21:53:22.487: RADIUS:  NAS-Port            [5]   6   27
Sep 28 21:53:22.487: RADIUS:  Service-Type        [6]   6   Framed                    [2]
Sep 28 21:53:22.491: RADIUS:  NAS-IP-Address      [4]   6   10.66.79.99
Sep 28 21:53:22.515: RADIUS: Received from id 21645/44 10.66.79.120:1645,
Access-Accept, len 141
Sep 28 21:53:22.515: RADIUS:  authenticator ED 3F 8A 08 2D A2 EB 4F - 78
3F 5D 80 58 7B B5 3E
Sep 28 21:53:22.515: RADIUS:  Service-Type        [6]   6   Framed                    [2]
Sep 28 21:53:22.515: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
Sep 28 21:53:22.515: RADIUS:  Filter-Id           [11]  8
Sep 28 21:53:22.515: RADIUS:   31 30 31 2E 69 6E  [101.in]
Sep 28 21:53:22.515: RADIUS:  Vendor, Microsoft   [26]  12
Sep 28 21:53:22.515: RADIUS:   MS-MPPE-Enc-Policy [7]   6
Sep 28 21:53:22.515: RADIUS:   00 00 00          [???]
Sep 28 21:53:22.515: RADIUS:  Vendor, Microsoft   [26]  12
Sep 28 21:53:22.515: RADIUS:   MS-MPPE-Enc-Type   [8]   6
Sep 28 21:53:22.515: RADIUS:   00 00 00          [???]
Sep 28 21:53:22.515: RADIUS:  Vendor, Microsoft   [26]  40
Sep 28 21:53:22.515: RADIUS:   MS-CHAP-MPPE-Keys  [12]  34  *
Sep 28 21:53:22.519: RADIUS:  Framed-IP-Address   [8]   6   192.168.1.1
Sep 28 21:53:22.519: RADIUS:  Class               [25]  31
Sep 28 21:53:22.519: RADIUS:
43 49 53 43 4F 41 43 53 3A 30 30 30 30 30 30 36  [CISCOACS:0000006]
Sep 28 21:53:22.519: RADIUS:
33 2F 30 61 34 32 34 66 36 33 2F 32 37           [3/0a424f63/27]
Sep 28 21:53:22.519: RADIUS(0000001C): Received from id 21645/44
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: service-type
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: Framed-Protocol
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: inacl: Peruser
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: MS-CHAP-MPPE-Keys
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: addr
Sep 28 21:53:22.523: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.523: Vi3 PPP: Phase is DOWN, Setup
Sep 28 21:53:22.527: AAA/BIND(0000001C): Bind i/f Virtual-Access3
Sep 28 21:53:22.531: %LINK-3-UPDOWN: Interface Virtual-Access3,
changed state to up
Sep 28 21:53:22.531: Vi3 PPP: Phase is AUTHENTICATING, Authenticated User
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Author
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Attr: service-type
Sep 28 21:53:22.531: Vi3 MS-CHAP: O SUCCESS id 1 len 4
Sep 28 21:53:22.535: Vi3 PPP: Phase is UP
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/IPCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start IPCP
Sep 28 21:53:22.535: Vi3 IPCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 IPCP:    Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/CCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start CCP
Sep 28 21:53:22.535: Vi3 CCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 CCP: MS-PPC supported bits 0x01000060 (0x120601000060)
Sep 28 21:53:22.535: Vi3 PPP: Process pending packets
Sep 28 21:53:22.539: RADIUS(0000001C): Using existing nas_port 27
Sep 28 21:53:22.539: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.539: RADIUS(0000001C): sending
Sep 28 21:53:22.539: RADIUS/ENCODE: Best Local IP-Address
10.66.79.99 for Radius-Server 10.66.79.120
Sep 28 21:53:22.539: RADIUS(0000001C): Send Accounting-Request
to 10.66.79.120:1646 id 21645/45, len 147
Sep 28 21:53:22.539: RADIUS:  authenticator 1A 76 20 95 95 F8
81 42 - 1F E8 E7 C1 8F 10 BA 94
Sep 28 21:53:22.539: RADIUS:  Acct-Session-Id     [44]  10  "00000026"
Sep 28 21:53:22.539: RADIUS:  Tunnel-Server-Endpoi[67]  13  "10.66.79.99"
Sep 28 21:53:22.539: RADIUS:  Tunnel-Client-Endpoi[66]  13  "10.66.79.60"
Sep 28 21:53:22.543: RADIUS:  Tunnel-Assignment-Id[82]  3   "1"
```

```
Sep 28 21:53:22.543: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Sep 28 21:53:22.543: RADIUS:  Acct-Authentic      [45]  6   RADIUS                      [1]
Sep 28 21:53:22.543: RADIUS:  User-Name           [1]   9   "georgia"
Sep 28 21:53:22.543: RADIUS:  Acct-Status-Type    [40]  6   Start                       [1]
Sep 28 21:53:22.543: RADIUS:  NAS-Port-Type       [61]  6   Virtual                     [5]
Sep 28 21:53:22.543: RADIUS:  NAS-Port            [5]   6   27
Sep 28 21:53:22.543: RADIUS:  Class               [25]  31
Sep 28 21:53:22.543: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30
30 30 36  [CISCOACS:0000006]
Sep 28 21:53:22.543: RADIUS:   33 2F 30 61 34 32 34 66 36 33 2F 32 37
          [3/0a424f63/27]
Sep 28 21:53:22.547: RADIUS:  Service-Type        [6]   6   Framed                      [2]
Sep 28 21:53:22.547: RADIUS:  NAS-IP-Address      [4]   6   10.66.79.99
Sep 28 21:53:22.547: RADIUS:  Acct-Delay-Time     [41]  6   0
Sep 28 21:53:22.547: Vi3 CCP: I CONFREQ [REQsent] id 4 len 10
Sep 28 21:53:22.547: Vi3 CCP:    MS-PPC supported bits 0x010000F1
(0x1206010000F1)
Sep 28 21:53:22.547: Vi3 CCP: O CONFNAK [REQsent] id 4 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000060
(0x120601000060)
Sep 28 21:53:22.551: Vi3 CCP: I CONFNAK [REQsent] id 1 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 CCP: O CONFREQ [REQsent] id 2 len 10
Sep 28 21:53:22.551: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 IPCP: I CONFREQ [REQsent] id 5 len 34
Sep 28 21:53:22.551: Vi3 IPCP:    Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.551: Vi3 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0,
we want 0.0.0.0
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Processing AV inacl
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Processing AV addr
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Authorization succeeded
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0,
we want 192.168.1.1
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary wins
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for seconday dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for seconday wins
Sep 28 21:53:22.555: Vi3 IPCP: O CONFREJ [REQsent] id 5 len 28
Sep 28 21:53:22.555: Vi3 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.555: Vi3 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.555: Vi3 IPCP: I CONFACK [REQsent] id 1 len 10
Sep 28 21:53:22.555: Vi3 IPCP:    Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.563: Vi3 CCP: I CONFREQ [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.563: Vi3 CCP: O CONFACK [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: I CONFACK [ACKsent] id 2 len 10
Sep 28 21:53:22.567: Vi3 CCP:    MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: State is Open
Sep 28 21:53:22.567: Vi3 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
Sep 28 21:53:22.567: Vi3 IPCP:    Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.567: Vi3 IPCP: O CONFNAK [ACKrcvd] id 7 len 10
Sep 28 21:53:22.571: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
```

```
Sep 28 21:53:22.575: Vi3 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: O CONFACK [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:    Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: State is Open
Sep 28 21:53:22.575: AAA/AUTHOR: Processing PerUser AV inacl
Sep 28 21:53:22.583: Vi3 IPCP: Install route to 192.168.1.1
Sep 28 21:53:22.583: Vi3 IPCP: Add link info for cef entry 192.168.1.1
Sep 28 21:53:22.603: RADIUS: Received from id 21645/45 10.66.79.120:1646,
Accounting-response, len 20
Sep 28 21:53:22.603: RADIUS:  authenticator A6 B3 4C 4C 04 1B BE 8E - 6A
BF 91 E2 3C 01 3E CA
Sep 28 21:53:23.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 Virtual-Access3, changed state to up
```

Informations connexes

- Cisco Secure ACS pour la page d'assistance de Windows
- Support et documentation techniques - Cisco Systems