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

Contenu

Introduction

Le support point par point de Protocol de tunnel (PPTP) a été ajouté à la version de logiciel 12.0.5.XE5 de Cisco IOS® sur le Cisco 7100 et 7200 Plateformes (référez-vous à PPTP avec le chiffrement point par point de Microsoft (MPPE) [version du logiciel Cisco IOS 12.0]). Le soutien de plus de Plateformes a été ajouté dans la version du logiciel Cisco IOS 12.1.5.T (référez-vous à la version MSCHAP 2).

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

Ce document suppose que des connexions PPTP au routeur avec l'authentification V1 de Microsoft Challenge Handshake Authentication Protocol de gens du pays (MS-CHAP) (et sur option le MPPE, qui exige MS-CHAP V1) ont été créées avec l'utilisation de ces documents et sont déjà opérationnelles. Le RAYON est exigé pour le support de chiffrement MPPE. TACACS+ fonctionne pour l'authentification, mais pas la génération de clés MPPE. Le support MS-CHAP V2

a été ajouté à la version du logiciel Cisco IOS 12.2(2)XB5 et a été intégré dans le Logiciel Cisco IOS version 12.2(13)T (référez-vous à la version MSCHAP 2), cependant, le MPPE n'est pas pris en charge avec MS-CHAP V2 en date d'encore.

Cette configuration d'échantillon explique comment installer une connexion par PC au routeur (à 10.66.79.99), qui fournit alors l'authentification de l'utilisateur au Système de contrôle d'accès sécurisé Cisco (ACS) 4.2 pour des Windows Server (à 10.66.79.120), avant que vous permettiez l'utilisateur dans le réseau.

Remarque: Le serveur de RAYON n'est pas habituellement en dehors du routeur excepté dans un environnement de travaux pratiques.

Le support PPTP a été ajouté au Cisco Secure ACS 2.5, mais peut ne pas fonctionner avec le routeur dû à l'ID de bogue Cisco CSCds92266 (clients enregistrés seulement). ACS 2.6 et plus tard n'ont pas ce problème.

Cisco Secure UNIX ne prend en charge pas le MPPE. Deux autres applications de RAYON avec le support MPPE incluent le RAYON de Microsoft et se dégonflent RAYON.

Référez-vous à configurer le routeur et les clients vpn de Cisco utilisant PPTP et MPPE pour plus d'informations sur la façon configurer PPTP et MPPE avec un routeur.

Référez-vous à configurer le concentrateur VPN 3000 et le PPTP avec le Cisco Secure ACS pour l'authentification de RAYON de Windows pour plus d'informations sur la façon configurer PPTP sur un concentrateur VPN 3000 avec le Cisco Secure ACS pour Windows pour l'authentification de RAYON.

Consultez PIX 6.x : PPTP avec l'exemple de configuration d'authentification de rayon afin de configurer des connexions PPTP au PIX.

Conditions préalables

Conditions requises

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

Composants utilisés

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 de Cisco 3600
- Logiciel Cisco IOS version 12.4(3)

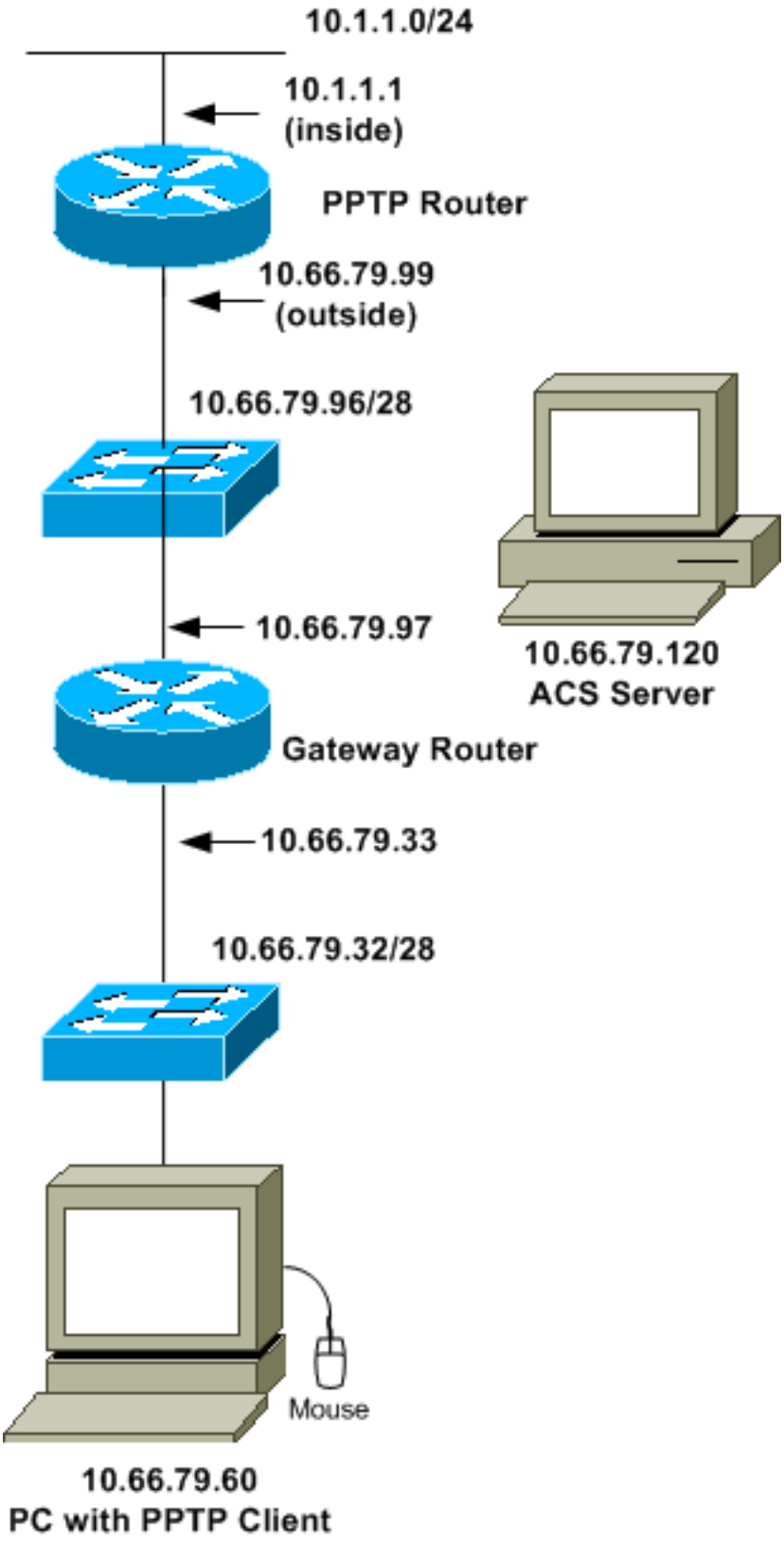
Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous êtes dans un réseau vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande avant que vous l'utilisiez.

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 devrait pouvoir se connecter « à la **daine de mot de passe de John de nom d'utilisateur** » même si le serveur de RAYON est inaccessible (qui est possible si le serveur n'était pas configuré avec le Cisco Secure ACS pourtant). Cet exemple suppose que cette authentification locale (et, sur option, cryptage) est déjà opérationnel.

Routeur de 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
```

Caractéristique de retour de serveur de RAYON

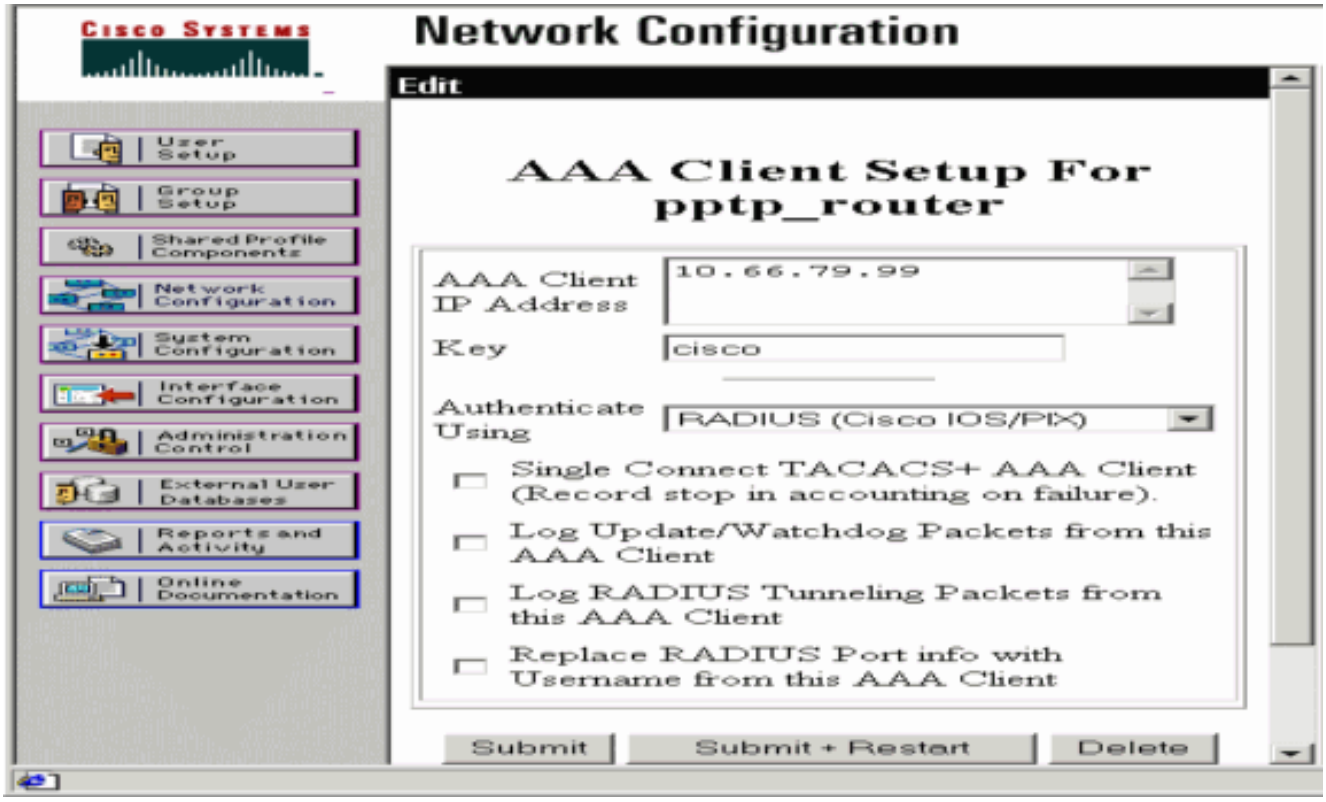
Quand le serveur primaire de RAYON devient indisponible, le routeur Basculement au prochain serveur de sauvegarde actif de RAYON. Le routeur continuera à utiliser le serveur secondaire de RAYON pour toujours même si le serveur primaire est disponible. Habituellement le serveur primaire est les hautes performances et le serveur préféré.

Afin de placer l'authentification d'Authentification, autorisation et comptabilité (AAA) à la procédure de connexion, utilisez la commande d'authentication login d'AAA en mode de configuration globale.

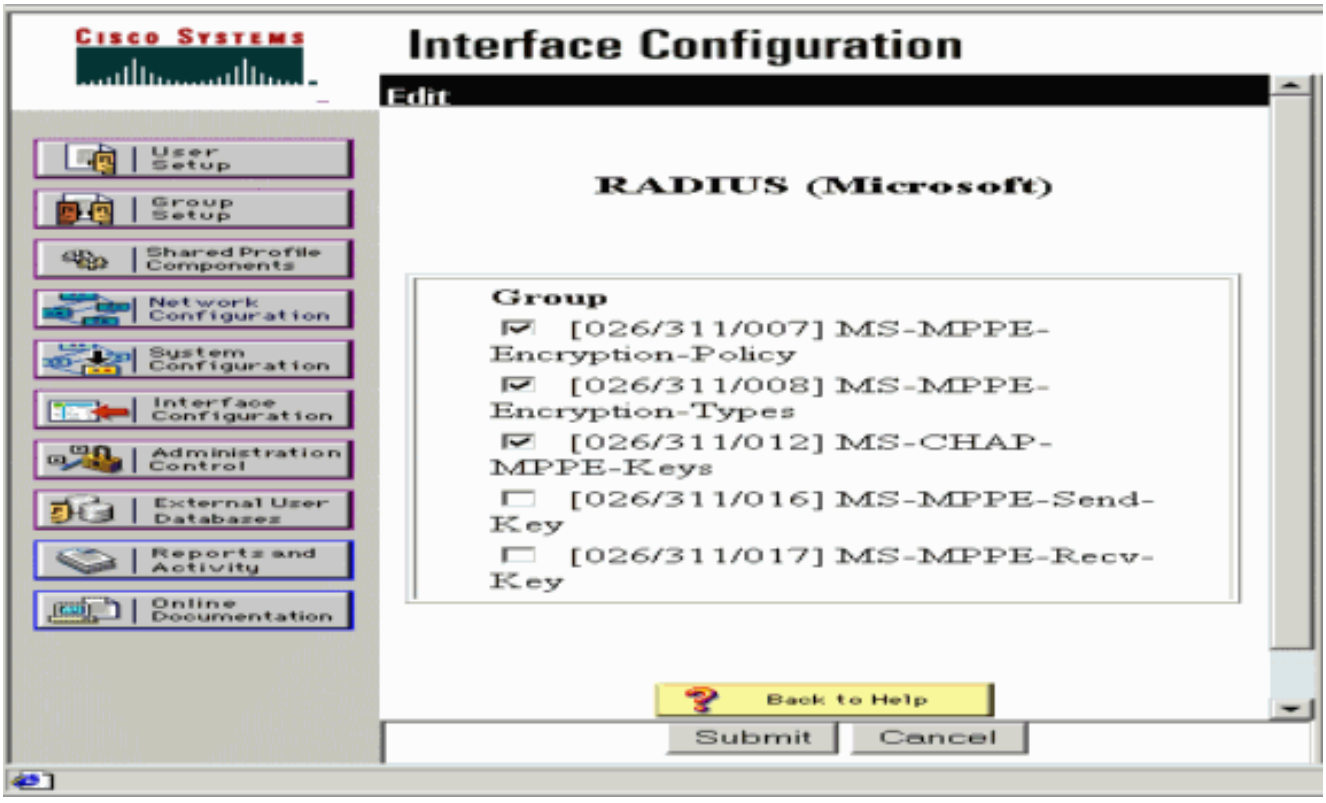
Cisco Secure ACS pour la configuration de Windows

Employez cette procédure pour configurer le Cisco Secure ACS :

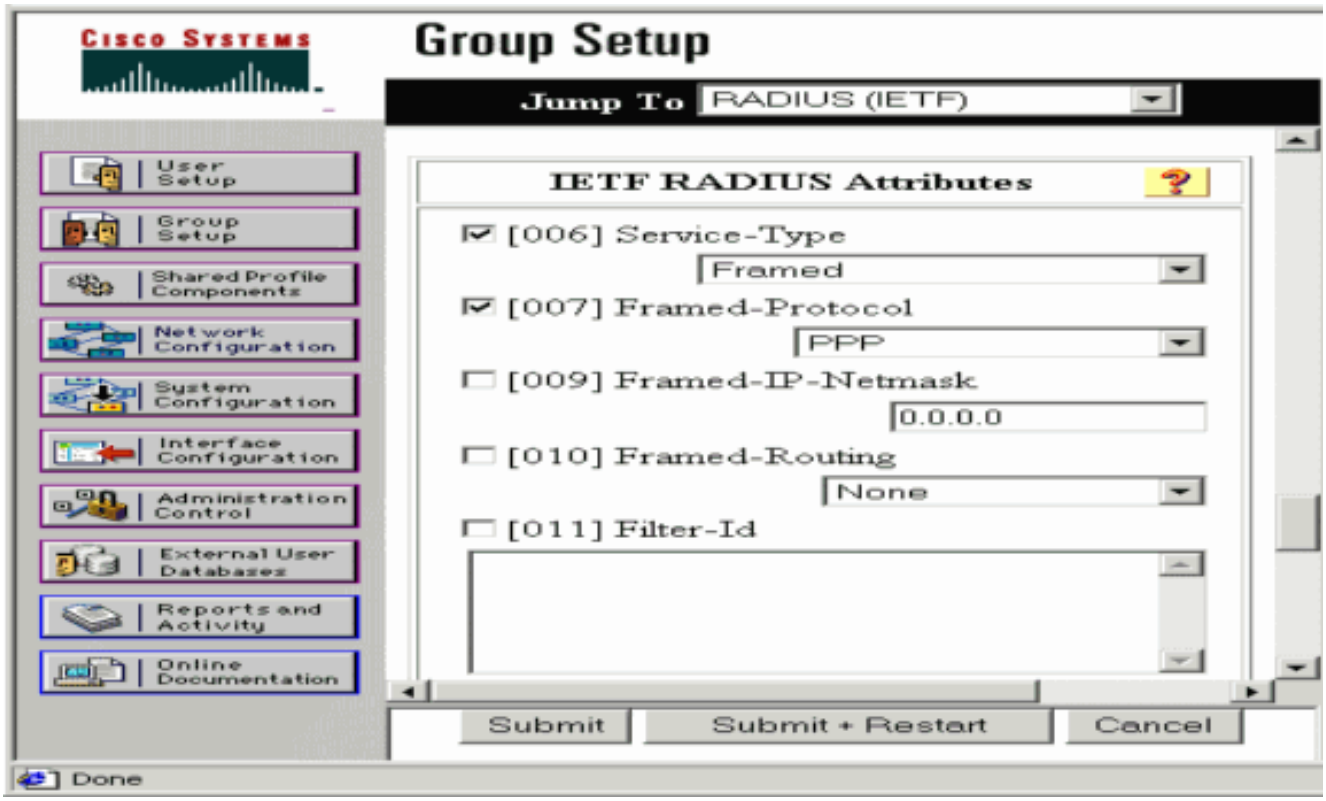
1. Cliquez sur Network Configuration, ajoutez une entrée pour le routeur, et cliquez sur Submit **+ reprise** quand vous êtes de
finition.



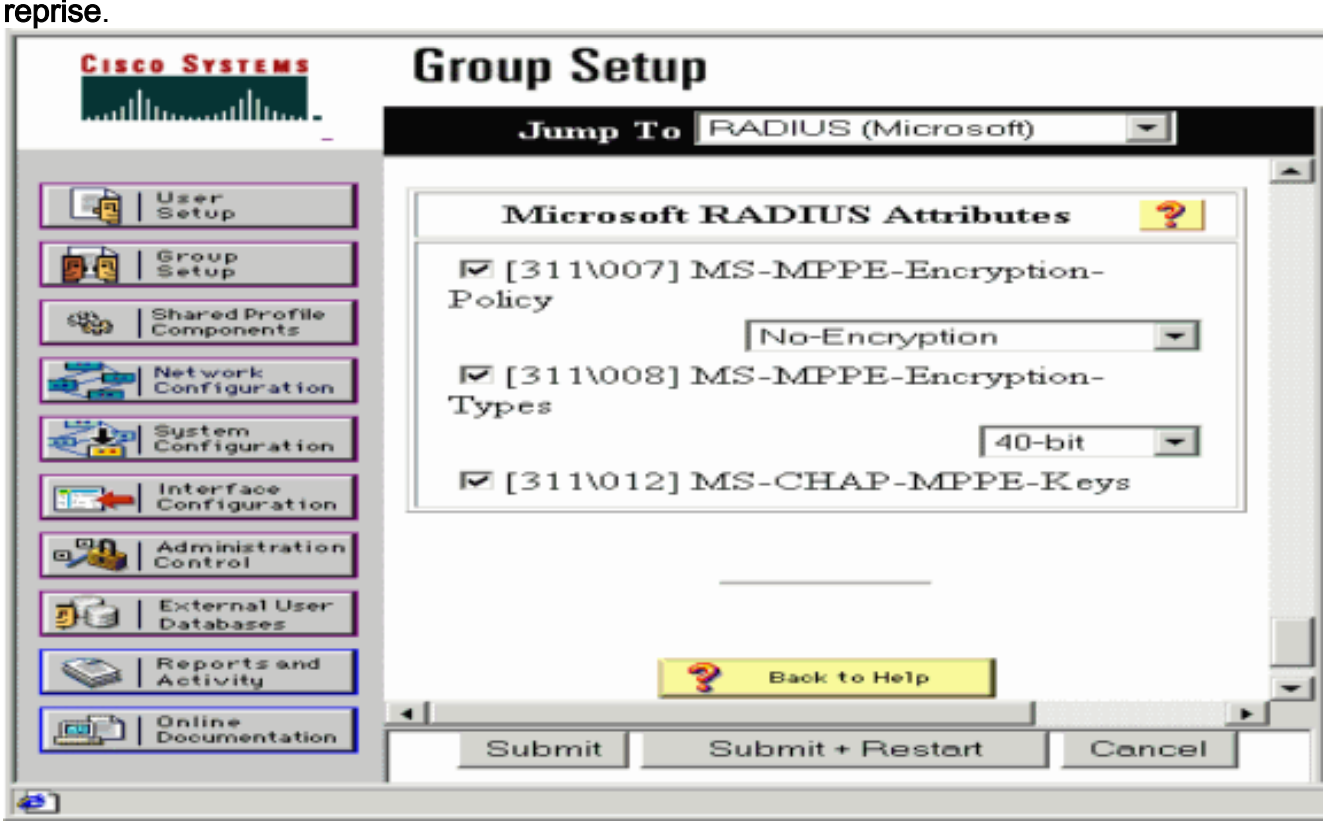
2. **La configuration d'interface** > le **RAYON** choisis **(Microsoft)**, alors vérifient vos attributs MPPE et cliquent sur
Submit.



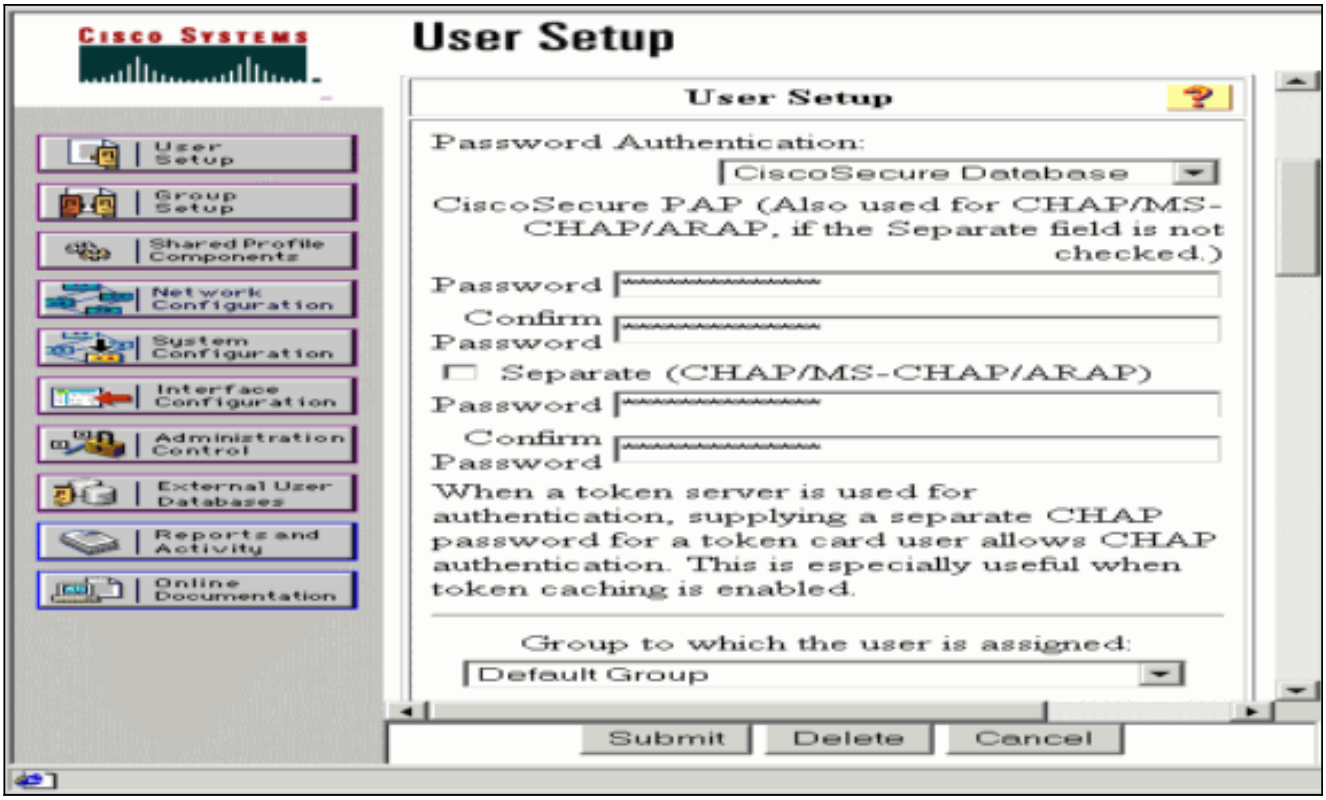
3. Cliquez sur le **Group Setup** et pour le type de service, choisi **vue**. Pour le protocole tramé, le **PPP** choisi et cliquent sur
Submit.



4. Dans le **Group Setup**, vérifiez les informations de RAYON MS-MPPE et quand vous êtes fait, cliquez sur Submit **+**
reprise.



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



6. Test d'authentification au routeur avant que vous ajoutiez le cryptage. Si l'authentification ne fonctionne pas, voyez la section de dépannage de ce document.

Ajouter à la configuration

Ajouter le cryptage

Vous pouvez ajouter le chiffrement MPPE avec cette commande :

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

Puisque l'exemple suppose que le cryptage 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 de permettre la flexibilité maximale :

```
ppp encrypt mppe auto
```

Affectation d'adresse IP statique de serveur

Si vous devez assigner une adresse IP particulière à l'utilisateur, dans l'installation utilisateur ACS, choisie **assignez l'adresse IP statique** et complétez l'adresse IP.

Ajoutez les Listes d'accès au serveur

Afin de contrôler ce que l'utilisateur PPTP peut accéder à une fois l'utilisateur est connecté au routeur, vous peut 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 le Filtre-**id (attribut 11)** dans ACS et écrivez **101** dans la case, l'utilisateur PPTP peut accéder à l'hôte mais pas d'autres de 10.1.1.2. Quand vous émettez une commande du **show ip interface virtual-access** *X*, où *x* est un nombre que vous pouvez déterminer à partir d'un ordre d'**utilisateur d'exposition**, la liste d'accès devrait afficher comme appliqué :

```
Inbound access list is 101
```

Ajoutez la gestion des comptes

Vous pouvez ajouter expliquer des sessions avec cette commande :

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

Les enregistrements des comptes dans le Cisco Secure ACS apparaissent pendant que cette sortie affiche :

```
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: La ligne ruptures ont été ajoutées à l'exemple pour l'affichage. La ligne ruptures dans votre sortie réelle sont différente de ceux affichées ici.

transmission tunnel partagée

Quand le tunnel PPTP monte sur le PC, le routeur PPTP est installé avec une mesure plus élevée que le par défaut précédent, ainsi vous perdez la connexion Internet. Afin de remédier à de ceci, étant donné que le réseau à l'intérieur du routeur est 10.1.1.X, exécutez un fichier batch (batch.bat) pour modifier Microsoft conduisant pour supprimer le par défaut et pour réinstaller le default route (ceci exige l'adresse IP que le client PPTP est assigné ; pour l'exemple, c'est 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
```

Vérifiez

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 au sujet de tunnel et d'identificateurs de message de protocole de l'expédition du niveau actif 2 (L2F) dans un Réseau privé virtuel à accès commuté (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
```

Dépannez

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

1. **Le PC spécifie le cryptage, mais le routeur ne fait pas.**L'utilisateur sur PC voit :`The remote computer does not support the required data encryption type.`
2. **Le PC et le routeur spécifient le cryptage, mais le serveur de RAYON n'est pas configuré pour envoyer en bas des clés MPPE (ceux-ci apparaissent normalement en tant qu'attribut 26).**L'utilisateur sur PC voit :`The remote computer does not support the required data encryption type.`
3. **Le routeur spécifie le cryptage (requis), mais le PC ne fait pas (non laissé).**L'utilisateur sur PC voit :`The specified port is not connected.`
4. **L'utilisateur entre le nom d'utilisateur incorrect ou le mot de passe.**L'utilisateur sur PC voit :`Access was denied because the username and/or password was invalid on the domain.`Le routeur **mettent au point des** expositions :**Remarque:** La ligne ruptures ont été ajoutées à cet exemple pour l'affichage. La ligne ruptures dans votre sortie réelle sont différente de ceux affichées 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 de RAYON est non communicatif.**L'utilisateur sur PC voit :`Access was denied because the username and/or password was invalid on the domain.`Le routeur **mettent au point des** expositions :**Remarque:** La ligne ruptures ont été ajoutées à cet exemple pour l'affichage. La ligne ruptures dans votre sortie réelle sont différente de ceux affichées 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: Référez-vous aux informations importantes 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 au sujet de l'authentification AAA/TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.
- **debug ppp negotiation** — Paquets PPP d'affichages transmis pendant le startup de PPP, où des options PPP sont négociées.
- **debug ppp authentication** — Affiche les messages du protocole d'authentification, qui incluent des échanges de paquet de CHAP et des échanges de Password Authentication Protocol (PAP).
- **debug radius** — Affiche les informations de débogage détaillées associées avec le RAYON.

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

- **paquet de mppe de debug ppp** — Affiche tout le trafic entrant et sortant MPPE.
- **événement de mppe de debug ppp** — Occurrences principales des affichages MPPE.
- **mppe de debug ppp détaillé** — Affiche les informations MPPE détaillées.
- **debug vpdn l2x-packets** — Messages d'affichages au sujet des en-têtes et d'état de protocole L2F.
- **événements de debug vpdn** — Affiche des messages au sujet des événements qui sont partie de l'établissement normal d'un tunnel ou arrêt.
- **erreurs de debug vpdn** — Affiche les erreurs qui empêchent un tunnel d'être établi ou les erreurs qui causent un tunnel établi d'être fermé.
- **paquets de debug vpdn** — Affiche chaque paquet de protocole permuté. Cette option peut avoir comme conséquence un grand nombre de messages de débogage, et vous devriez généralement seulement utiliser cette commande sur un châssis de débogage avec une session active simple.

Vous pouvez également utiliser ces commandes pour dépannage des buts :

- **clear interface virtual-access** *X* — Arrêtent un tunnel spécifié et tous sessions dans le tunnel.

Bon exemple de sortie de débogage

Ceci mettent au point des événements significatifs d'expositions du RFC :

- **SCCRQ** = Commencement-Contrôle-Connexion-demande - octets 9 et 10 = 0001 de code de message
- **SCCRP** = Commencement-Contrôle-Connexion-réponse
- **OCRQ** = Sortant-Appel-demande - octets 9 et 10 = 0007 de code de message
- **OCRP** = Sortant-Appel-réponse

Remarque: La ligne ruptures ont été ajoutées à cet exemple pour l'affichage. La ligne ruptures dans votre sortie réelle sont différente de ceux affichées 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