Configuration du logiciel Cisco IOS et de Windows 2000 pour PPTP à l'aide de Microsoft IAS

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 de routeurs Cisco 7100 et 7200. La prise en charge d'autres plates-formes a été ajoutée dans le logiciel Cisco IOS Version 12.1.5.T.

Le document Request for Comments (RFC) 2637 décrit PPTP. Selon cette RFC, le concentrateur d'accès PPTP (PAC) est le client (c'est-à-dire le PC ou l'appelant) et le serveur réseau PPTP (PNS) est le serveur (c'est-à-dire le routeur ou le périphérique appelé).

Conditions préalables

Conditions requises

Ce document suppose que vous avez configuré des connexions PPTP au routeur avec l'authentification Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) V1 locale (et éventuellement Microsoft Point-to-Point Encryption [MPPE] qui nécessite MS-CHAP V1) en utilisant ces documents, et qu'ils fonctionnent déjà. Le service RADIUS (Remote Authentication Dial-In User Service) est requis pour la prise en charge du chiffrement MPPE ; TACACS+ fonctionne pour l'authentification, mais pas pour la clé MPPE.

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Composant optionnel Microsoft IAS installé sur un serveur avancé Microsoft 2000 avec Active Directory.
- Un routeur Cisco 3600.
- Logiciel Cisco IOS Version c3640-io3s56i-mz.121-5.T.

Cette configuration utilise Microsoft IAS installé sur un serveur avancé Windows 2000 comme serveur RADIUS.

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.

Conventions

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

Théorie générale

Cet exemple de configuration montre comment configurer un PC pour se connecter au routeur (à l'adresse 10.200.20.2), qui authentifie ensuite l'utilisateur sur le serveur d'authentification Internet (IAS) de Microsoft (à 10.200.20.245) avant d'autoriser l'utilisateur à accéder au réseau. La prise en charge PPTP est disponible avec Cisco Secure Access Control Server (ACS) version 2.5 pour Windows. Cependant, il peut ne pas fonctionner avec le routeur en raison de l'ID de bogue Cisco CSCds92266. Si vous utilisez Cisco Secure, nous vous recommandons d'utiliser Cisco Secure version 2.6 ou ultérieure. Cisco Secure UNIX ne prend pas en charge MPPE. Microsoft RADIUS et Funk RADIUS sont deux autres applications RADIUS prenant en charge MPPE.

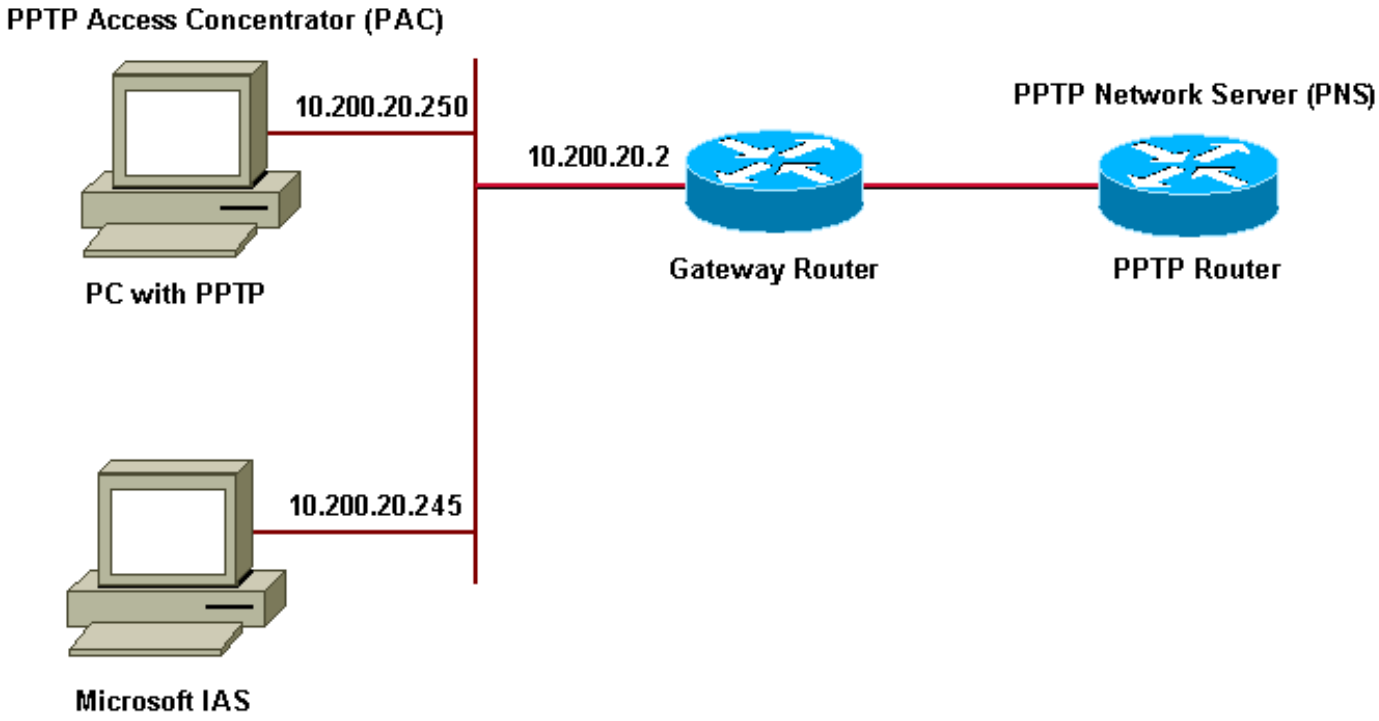
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'outil de recherche de commandes IOS

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Pool IP pour les clients commutés :

- Routeur de passerelle : 192.168.1.2 ~ 192.168.1.254
- LNS : 172.16.10.1 ~ 172.16.10.10

Bien que la configuration ci-dessus utilise un client d'accès commuté pour se connecter au routeur du fournisseur d'accès à Internet (FAI) via une connexion commutée, vous pouvez connecter le PC et le routeur de passerelle via n'importe quel support, tel qu'un réseau local.

Configuration de Windows 2000 Advanced Server pour Microsoft IAS

Cette section explique comment configurer le serveur avancé Windows 2000 pour Microsoft IAS :

1. Vérifiez que Microsoft IAS est installé. Pour installer Microsoft IAS, connectez-vous en tant qu'administrateur. Sous **Services réseau**, vérifiez que toutes les cases à cocher sont désactivées. Activez la case à cocher Internet Authentication Server, puis cliquez sur **OK**.
2. Dans l'assistant **Composants Windows**, cliquez sur **Suivant**. Si vous y êtes invité, insérez le CD Windows 2000.
3. Après avoir copié les fichiers requis, cliquez sur **Terminer**, puis fermez toutes les fenêtres. Vous n'avez pas besoin de redémarrer.

Configuration des clients Radius

Cette section présente les étapes de configuration des clients radius :

1. Dans **Outils d'administration**, ouvrez la console **Internet Authentication Server** et cliquez sur **Clients**.

2. Dans la zone **Nom convivial**, saisissez l'adresse IP du serveur d'accès au réseau (NAS).
3. Cliquez sur l'option **Utiliser cette adresse IP**.
4. Dans la liste déroulante **Client-Fournisseur**, assurez-vous que l'option **RADIUS Standard** est sélectionnée.
5. Dans les zones **Secret partagé** et **Confirmer le secret partagé**, tapez le mot de passe, puis cliquez sur **Terminer**.
6. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Internet Authentication Service**, puis cliquez sur **Start**.
7. Fermez la console.

Configuration des utilisateurs sur IAS

Contrairement à Cisco Secure, la base de données utilisateur Windows 2000 RADIUS est étroitement liée à la base de données utilisateur Windows. Si un **Active Directory** est installé sur votre serveur Windows 2000, créez vos nouveaux utilisateurs à distance à partir d'**Utilisateurs et ordinateurs Active Directory**. Si **Active Directory** n'est pas installé, utilisez **Utilisateurs et groupes locaux** des **outils d'administration** pour créer de nouveaux utilisateurs.

Configuration des utilisateurs dans Active Directory

Cette section présente les étapes à suivre pour configurer les utilisateurs dans le répertoire actif :

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, développez votre domaine. Cliquez avec le bouton droit sur **Utilisateurs**. Faites défiler la liste pour sélectionner **Nouvel utilisateur**. Créez un nouvel utilisateur appelé **tac**.
2. Tapez un mot de passe dans les boîtes de dialogue **Mot de passe** et **Confirmer le mot de passe**.
3. Effacez le champ **L'utilisateur doit changer de mot de passe à l'ouverture de session suivante** et cliquez sur **Suivant**.
4. Ouvrez la zone **User tac Properties. Passez à l'onglet Composer. Sous Autorisation d'accès à distance (accès commuté ou VPN), cliquez sur Autoriser l'accès, puis sur OK.**

Configuration des utilisateurs si aucun Active Directory n'est installéCette section présente les étapes à suivre pour configurer les utilisateurs si aucun répertoire actif n'est installé :

1. **Dans la section Outils d'administration, cliquez sur Gestion de l'ordinateur. Développez la console Gestion de l'ordinateur et cliquez sur Utilisateurs et groupes locaux. Cliquez avec le bouton droit sur la barre de défilement Utilisateurs pour sélectionner Nouvel utilisateur. Créez un nouvel utilisateur appelé tac.**
2. **Tapez un mot de passe dans les boîtes de dialogue Mot de passe et Confirmer le mot de passe.**
3. **Effacez l'option L'utilisateur doit changer de mot de passe lors de la prochaine connexion et cliquez sur Suivant.**
4. **Ouvrez la zone des propriétés de tac, nouvel utilisateur. Passez à l'onglet Composer. Sous Autorisation d'accès à distance (accès commuté ou VPN), cliquez sur Autoriser l'accès, puis sur OK.**

Application d'une stratégie d'accès à distance à l'utilisateur WindowsCette section présente les étapes à suivre pour appliquer une stratégie d'accès à distance à l'utilisateur Windows :

1. **Dans Outils d'administration, ouvrez la console Internet Authentication Server et cliquez sur Remote Access Policies.**

2. Cliquez sur le bouton Ajouter dans Spécifier les conditions à respecter, puis ajoutez Service-Type. Choisissez le type disponible en tant que Cadre et ajoutez-le à la liste Types sélectionnés. Appuyez sur OK.
3. Cliquez sur le bouton Ajouter sur Spécifier les conditions à respecter et ajouter le protocole encadré. Choisissez le type disponible en tant que ppp et ajoutez-le à la liste Types sélectionnés. Appuyez sur OK.
4. Cliquez sur le bouton Ajouter dans Spécifier les conditions à respecter et ajouter Windows-Groups pour ajouter le groupe Windows auquel appartient l'utilisateur. Choisissez le groupe et ajoutez-le aux types sélectionnés et appuyez sur OK.
5. Dans les propriétés Allow Access if Dial-in Permission is Enabled, sélectionnez Grant remote Access autorisation.
6. Fermez la console.

Configuration du client Windows 2000 pour PPTP

La section ci-dessous présente les étapes de configuration du client Windows 2000 pour PPTP :

1. Dans le menu Démarrer, sélectionnez Paramètres, puis :Panneau de configuration et Connexions réseau et accès à distance, ouConnexions réseau et accès à distance, puis Nouvelle connexion.Utilisez l'Assistant pour créer une connexion appelée PPTP. Cette connexion se connecte à un réseau privé via Internet. Vous devez également spécifier l'adresse IP ou le nom du serveur réseau PPTP (PNS).
2. La nouvelle connexion apparaît dans la fenêtre Connexions réseau et accès à distance sous Panneau de configuration.Àpartir de là, cliquez sur le bouton droit de la souris pour modifier ses propriétés. Sous l'onglet Réseau, assurez-vous que le champ Type de serveur que j'appelle est PPTP. Si vous prévoyez d'allouer une adresse interne dynamique à ce client à partir de la passerelle, soit via un pool local, soit via le protocole DHCP (Dynamic Host Configuration Protocol), sélectionnez TCP/IP, et assurez-vous que le client est configuré pour obtenir automatiquement une adresse IP. Vous pouvez également émettre des informations DNS automatiquement.Le bouton Avancé vous permet de définir des informations WINS (Windows Internet Naming Service) et DNS statiques.L'onglet Options vous permet de désactiver IPSec ou d'affecter une autre stratégie à la connexion.
3. Sous l'onglet Sécurité, vous pouvez définir les paramètres d'authentification de l'utilisateur. Par exemple, PAP, CHAP ou MS-CHAP, ou ouverture de session de domaine Windows. Une fois la connexion configurée, vous pouvez double-cliquer dessus pour afficher l'écran de connexion, puis vous connecter.

Configurations

Àl'aide de la configuration de routeur suivante, l'utilisateur peut se connecter avec le nom d'utilisateur tac et le mot de passe admin même si le serveur RADIUS n'est pas disponible (ceci est possible lorsque Microsoft IAS n'est pas encore configuré). L'exemple de configuration suivant présente les commandes requises pour L2tp sans IPSec.

angela

```
angela#show running-config
Building configuration...
Current configuration : 1606 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname angela
```

```
!
logging rate-limit console 10 except errors
!---Enable AAA services here aaa new-model aaa
authentication login default group radius local aaa
authentication login console none aaa authentication ppp
default group radius local aaa authorization network
default group radius local enable password ! username
tac password 0 admin memory-size iomem 30 ip subnet-zero
! ! no ip finger no ip domain-lookup ip host rund
172.17.247.195 ! ip audit notify log ip audit po max-
events 100 ip address-pool local !---Enable VPN/Virtual
Private Dialup Network (VPDN) services !---and define
groups and their respective parameters. vpdn enable no
vpdn logging ! ! vpdn-group PPTP_WIN2KClient !---Default
PPTP VPDN group !---Allow the router to accept incoming
Requests accept-dialin protocol pptp virtual-template 1
! ! ! call rsvp-sync ! ! ! ! ! ! controller E1 2/0 ! !
interface Loopback0 ip address 172.16.10.100
255.255.255.0 ! interface Ethernet0/0 ip address
10.200.20.2 255.255.255.0 half-duplex ! interface
Virtual-Template1 ip unnumbered Loopback0 peer default
ip address pool default !--- The following encryption
command is optional !--- and could be added later. ppp
encrypt mppe 40 ppp authentication ms-chap ! ip local
pool default 172.16.10.1 172.16.10.10 ip classless ip
route 0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ! end angela#show debug
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
PPP:
MPPE Events debugging is on
PPP protocol negotiation debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
Radius protocol debugging is on

angela#
*Mar  7 04:21:07.719: L2X: TCP connect reqd from
0.0.0.0:2000
*Mar  7 04:21:07.991: Tnl 29 PPTP: Tunnel created; peer
initiated
*Mar  7 04:21:08.207: Tnl 29 PPTP: SCCRQ-ok ->
state change wt-sccrq to estabd
*Mar  7 04:21:09.267: VPDN: Session vaccess task running
*Mar  7 04:21:09.267: Vi1 VPDN: Virtual interface
created
*Mar  7 04:21:09.267: Vi1 VPDN: Clone from Vtemplate 1
*Mar  7 04:21:09.343: Tnl/Cl 29/29 PPTP: VAccess created
*Mar  7 04:21:09.343: Vi1 Tnl/Cl 29/29 PPTP: vacc-ok ->
#state change wt-vacc to estabd
*Mar  7 04:21:09.343: Vi1 VPDN: Bind interface
direction=2
*Mar  7 04:21:09.347: %LINK-3-UPDOWN: Interface Virtual-
Access1, changed
```

```
state to up
*Mar  7 04:21:09.347: Vi1 PPP: Using set call direction
*Mar  7 04:21:09.347: Vi1 PPP: Treating connection as a
callin
*Mar  7 04:21:09.347: Vi1 PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load]
*Mar  7 04:21:09.347: Vi1 LCP: State is Listen
*Mar  7 04:21:10.347: %LINEPROTO-5-UPDOWN: Line protocol
on Interface
Virtual-Access1, changed state to up
*Mar  7 04:21:11.347: Vi1 LCP: TIMEout: State Listen
*Mar  7 04:21:11.347: Vi1 AAA/AUTHOR/FSM: (0): LCP
succeeds trivially
*Mar  7 04:21:11.347: Vi1 LCP: O CONFREQ [Listen] id 7
len 15
*Mar  7 04:21:11.347: Vi1 LCP:    AuthProto MS-CHAP
(0x0305C22380)
*Mar  7 04:21:11.347: Vi1 LCP:    MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar  7 04:21:11.635: Vi1 LCP: I CONFACK [REQsent] id 7
len 15
*Mar  7 04:21:11.635: Vi1 LCP:    AuthProto MS-CHAP
(0x0305C22380)
*Mar  7 04:21:11.635: Vi1 LCP:    MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar  7 04:21:13.327: Vi1 LCP: I CONFREQ [ACKrcvd] id 1
len 44
*Mar  7 04:21:13.327: Vi1 LCP:    MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar  7 04:21:13.327: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.327: Vi1 LCP:    ACFC (0x0802)
*Mar  7 04:21:13.327: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar  7 04:21:13.327: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar  7 04:21:13.327: Vi1 LCP:    EndpointDisc 1 Local
*Mar  7 04:21:13.327: Vi1 LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar  7 04:21:13.331: Vi1 LCP:     (0xB9182600000008)
*Mar  7 04:21:13.331: Vi1 LCP: O CONFREJ [ACKrcvd] id 1
len 34
*Mar  7 04:21:13.331: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar  7 04:21:13.331: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar  7 04:21:13.331: Vi1 LCP:    EndpointDisc 1 Local
*Mar  7 04:21:13.331: Vi1 LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar  7 04:21:13.331: Vi1 LCP:     (0xB9182600000008)
*Mar  7 04:21:13.347: Vi1 LCP: TIMEout: State ACKrcvd
*Mar  7 04:21:13.347: Vi1 LCP: O CONFREQ [ACKrcvd] id 8
len 15
*Mar  7 04:21:13.347: Vi1 LCP:    AuthProto MS-CHAP
(0x0305C22380)
*Mar  7 04:21:13.347: Vi1 LCP:    MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar  7 04:21:13.647: Vi1 LCP: I CONFREQ [REQsent] id 2
len 14
*Mar  7 04:21:13.651: Vi1 LCP:    MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar  7 04:21:13.651: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.651: Vi1 LCP:    ACFC (0x0802)
*Mar  7 04:21:13.651: Vi1 LCP: O CONFACK [REQsent] id 2
len 14
*Mar  7 04:21:13.651: Vi1 LCP:    MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar  7 04:21:13.651: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.651: Vi1 LCP:    ACFC (0x0802)
```

```
*Mar  7 04:21:13.723: Vi1 LCP: I CONFACK [ACKsent] id 8
len 15
*Mar  7 04:21:13.723: Vi1 LCP:    AuthProto MS-CHAP
(0x0305C22380)
*Mar  7 04:21:13.723: Vi1 LCP:    MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar  7 04:21:13.723: Vi1 LCP: State is Open
*Mar  7 04:21:13.723: Vi1 PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load]
*Mar  7 04:21:13.723: Vi1 MS-CHAP: O CHALLENGE id 20 len
21 from "angela "
*Mar  7 04:21:14.035: Vi1 LCP: I IDENTIFY [Open] id 3
len 18 magic
0x35BE1CB0 MSRASV5.00
*Mar  7 04:21:14.099: Vi1 LCP: I IDENTIFY [Open] id 4
len 24 magic
0x35BE1CB0 MSRAS-1-RSHANMUG
*Mar  7 04:21:14.223: Vi1 MS-CHAP: I RESPONSE id 20 len
57 from "tac"
*Mar  7 04:21:14.223: AAA: parse name=Virtual-Access1
idb type=21 tty=-1
*Mar  7 04:21:14.223: AAA: name=Virtual-Access1
flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar  7 04:21:14.223: AAA/MEMORY: create_user
(0x62740E7C) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925):
port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925):
using "default" list
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925):
Method=radius (radius)
*Mar  7 04:21:14.223: RADIUS: ustruct sharecount=0
*Mar  7 04:21:14.223: RADIUS: Initial Transmit Virtual-
Access1 id 116
10.200.20.245:1645, Access-Request, len 129
*Mar  7 04:21:14.227:         Attribute 4 6 0AC81402
*Mar  7 04:21:14.227:         Attribute 5 6 00000001
*Mar  7 04:21:14.227:         Attribute 61 6 00000005
*Mar  7 04:21:14.227:         Attribute 1 5 7461631A
*Mar  7 04:21:14.227:         Attribute 26 16
000001370B0AFD11
*Mar  7 04:21:14.227:         Attribute 26 58
0000013701341401
*Mar  7 04:21:14.227:         Attribute 6 6 00000002
*Mar  7 04:21:14.227:         Attribute 7 6 00000001
*Mar  7 04:21:14.239: RADIUS: Received from id 116
10.200.20.245:1645,
Access-Accept, len 116
*Mar  7 04:21:14.239:         Attribute 7 6 00000001
*Mar  7 04:21:14.239:         Attribute 6 6 00000002
*Mar  7 04:21:14.239:         Attribute 25 32 64080750
*Mar  7 04:21:14.239:         Attribute 26 40
000001370C223440
*Mar  7 04:21:14.239:         Attribute 26 12
000001370A06144E
*Mar  7 04:21:14.239: AAA/AUTHEN (2474402925): status =
PASS
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
Port='Virtual-Access1' list='' service=NET
```

```
*Mar  7 04:21:14.243: AAA/AUTHOR/LCP: Vi1 (2434357606)
user='tac'
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
send AV service=ppp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
send AV protocol=lcp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
found list "default"
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
Method=radius
(radius)
*Mar  7 04:21:14.243: RADIUS: unrecognized Microsoft VSA
type 10
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR (2434357606): Post
authorization
status = PASS_REPL
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:14.243: Vi1 MS-CHAP: O SUCCESS id 20 len 4
*Mar  7 04:21:14.243: Vi1 PPP: Phase is UP [0 sess, 0
load]
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0): Can we
start IPCP?
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:14.247: AAA/AUTHOR/FSM: Vi1 (1553311212)
user='tac'
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
send AV service=ppp
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
send AV protocol=ip
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
found list "default"
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
Method=radius
(radius)
*Mar  7 04:21:14.247: RADIUS: unrecognized Microsoft VSA
type 10
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR (1553311212): Post
authorization
status = PASS_REPL
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: We can start
IPCP
*Mar  7 04:21:14.247: Vi1 IPCP: O CONFREQ [Not
negotiated] id 4 len 10
*Mar  7 04:21:14.247: Vi1 IPCP:    Address 172.16.10.100
(0x0306AC100A64)
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0): Can we
start CCP?
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (3663845178):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:14.251: AAA/AUTHOR/FSM: Vi1 (3663845178)
user='tac'
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178):
send AV service=ppp
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178):
send AV protocol=ccp
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178):
found list "default"
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178):
Method=radius
```

```
(radius)
*Mar  7 04:21:14.251: RADIUS: unrecognized Microsoft VSA
type 10
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR (3663845178): Post
authorization
status = PASS_REPL
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM: We can start
CCP
*Mar  7 04:21:14.251: Vi1 CCP: O CONFREQ [Closed] id 3
len 10
*Mar  7 04:21:14.251: Vi1 CCP:    MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar  7 04:21:14.523: Vi1 CCP: I CONFREQ [REQsent] id 5
len 10
*Mar  7 04:21:14.523: Vi1 CCP:    MS-PPC supported bits
0x010000F1
(0x1206010000F1)
*Mar  7 04:21:14.523: Vi1 MPPE: don't understand all
options, NAK
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Processing AV
service=ppp
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  7 04:21:14.523: Vi1 CCP: O CONFNAK [REQsent] id 5
len 10
*Mar  7 04:21:14.523: Vi1 CCP:    MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar  7 04:21:14.607: Vi1 IPCP: I CONFREQ [REQsent] id 6
len 34
*Mar  7 04:21:14.607: Vi1 IPCP:    Address 0.0.0.0
(0x030600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryDNS 0.0.0.0
(0x810600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryWINS 0.0.0.0
(0x820600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    SecondaryDNS 0.0.0.0
(0x830600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    SecondaryWINS 0.0.0.0
(0x840600000000)
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  7 04:21:14.607: Vi1 IPCP: Pool returned
172.16.10.1
*Mar  7 04:21:14.607: Vi1 IPCP: O CONFREJ [REQsent] id 6
len 28
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryDNS 0.0.0.0
(0x810600000000)
*Mar  7 04:21:14.611: Vi1 IPCP:    PrimaryWINS 0.0.0.0
(0x820600000000)
```

```
*Mar  7 04:21:14.611: Vi1 IPCP:    SecondaryDNS 0.0.0.0
(0x830600000000)
*Mar  7 04:21:14.611: Vi1 IPCP:    SecondaryWINS 0.0.0.0
(0x840600000000)
*Mar  7 04:21:14.675: Vi1 IPCP: I CONFACK [REQsent] id 4
len 10
*Mar  7 04:21:14.675: Vi1 IPCP:    Address 172.16.10.100
(0x0306AC100A64)
*Mar  7 04:21:14.731: Vi1 CCP: I CONFACK [REQsent] id 3
len 10
*Mar  7 04:21:14.731: Vi1 CCP:    MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar  7 04:21:14.939: Vi1 CCP: I CONFREQ [ACKrcvd] id 7
len 10
*Mar  7 04:21:14.939: Vi1 CCP:    MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Processing AV
service=ppp
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  7 04:21:14.939: Vi1 CCP: O CONFACK [ACKrcvd] id 7
len 10
*Mar  7 04:21:14.939: Vi1 CCP:    MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar  7 04:21:14.943: Vi1 CCP: State is Open
*Mar  7 04:21:14.943: Vi1 MPPE: Generate keys using
RADIUS data
*Mar  7 04:21:14.943: Vi1 MPPE: Initialize keys
*Mar  7 04:21:14.943: Vi1 MPPE: [40 bit encryption]
[stateless mode]
*Mar  7 04:21:14.991: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8
len 10
*Mar  7 04:21:14.991: Vi1 IPCP:    Address 0.0.0.0
(0x030600000000)
*Mar  7 04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  7 04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  7 04:21:14.995: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8
len 10
*Mar  7 04:21:14.995: Vi1 IPCP:    Address 172.16.10.1
(0x0306AC100A01)
*Mar  7 04:21:15.263: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9
len 10
*Mar  7 04:21:15.263: Vi1 IPCP:    Address 172.16.10.1
(0x0306AC100A01)
*Mar  7 04:21:15.263: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 172.16.10.1, we want 172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
Port='Virtual-Access1' list='' service=NET
```

```
*Mar  7 04:21:15.267: AAA/AUTHOR/IPCP: Vi1 (2052567766)
user='tac'
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
send AV service=ppp
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
send AV protocol=ip
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
send AV
addr*172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
found list
"default"
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
Method=radius
(radius)
*Mar  7 04:21:15.267: RADIUS: unrecognized Microsoft VSA
type 10
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR (2052567766): Post
authorization
status = PASS_REPL
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Reject
172.16.10.1, using
172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV
addr*172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 172.16.10.1, we want 172.16.10.1
*Mar  7 04:21:15.271: Vi1 IPCP: O CONFACK [ACKrcvd] id 9
len 10
*Mar  7 04:21:15.271: Vi1 IPCP:    Address 172.16.10.1
(0x0306AC100A01)
*Mar  7 04:21:15.271: Vi1 IPCP: State is Open
*Mar  7 04:21:15.271: Vi1 IPCP: Install route to
172.16.10.1
*Mar  7 04:21:22.571: Vi1 LCP: I ECHOREP [Open] id 1 len
12 magic
0x35BE1CB0
*Mar  7 04:21:22.571: Vi1 LCP: Received id 1, sent id 1,
line up
*Mar  7 04:21:30.387: Vi1 LCP: I ECHOREP [Open] id 2 len
12 magic
0x35BE1CB0
*Mar  7 04:21:30.387: Vi1 LCP: Received id 2, sent id 2,
line up

angela#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
29                    estabd   192.168.1.47    2000  1
LocID RemID TunID Intf    Username      State   Last Chg
29    32768 29    Vi1     tac           estabd  00:00:31
%No active PPPoE tunnels
angela#
```

```
*Mar  7 04:21:40.471: Vi1 LCP: I ECHOREP [Open] id 3 len
12 magic
0x35BE1CB0
*Mar  7 04:21:40.471: Vi1 LCP: Received id 3, sent id 3,
line up
*Mar  7 04:21:49.887: Vi1 LCP: I ECHOREP [Open] id 4 len
12 magic
0x35BE1CB0
*Mar  7 04:21:49.887: Vi1 LCP: Received id 4, sent id 4,
line up

angela#ping 192.168.1.47
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.47, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 484/584/732 ms

*Mar  7 04:21:59.855: Vi1 LCP: I ECHOREP [Open] id 5 len
12 magic
0x35BE1CB0
*Mar  7 04:21:59.859: Vi1 LCP: Received id 5, sent id 5,
line up
*Mar  7 04:22:06.323: Tnl 29 PPTP: timeout -> state
change estabd to estabd
*Mar  7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> state
change estabd to estabd
*Mar  7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> echo state
change Idle to Idle
*Mar  7 04:22:09.879: Vi1 LCP: I ECHOREP [Open] id 6 len
12 magic
0x35BE1CB0
*Mar  7 04:22:09.879: Vi1 LCP: Received id 6, sent id 6,
line up

angela#ping 172.16.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 584/707/1084 ms

*Mar  7 04:22:39.863: Vi1 LCP: I ECHOREP [Open] id 7 len
12 magic
0x35BE1CB0
*Mar  7 04:22:39.863: Vi1 LCP: Received id 7, sent id 7,
line up

angela#clear vpdn tunnel pptp tac
Could not find specified tunnel

angela#show vpdn tunnel
%No active L2TP tunnels
%No active L2F tunnels
PPTP Tunnel Information Total tunnels 1 sessions 1
LocID Remote Name     State    Remote Address  Port
Sessions
29                    estabd   192.168.1.47    2000  1
%No active PPPoE tunnels

angela#
```

```
*Mar  7 04:23:05.347: Tnl 29 PPTP: timeout -> state
change estabd to estabd

angela#
*Mar  7 04:23:08.019: Tnl 29 PPTP: EchoRQ -> state
change estabd to estabd
*Mar  7 04:23:08.019: Tnl 29 PPTP: EchoRQ -> echo state
change Idle to Idle

angela#
*Mar  7 04:23:09.887: Vi1 LCP: I ECHOREP [Open] id 10
len 12 magic 0x35BE1CB0
*Mar  7 04:23:09.887: Vi1 LCP: Received id 10, sent id
10, line up
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.certaines commandes show sont prises en charge par l'outil Interpréteur de sortie, qui vous permet d'afficher une analyse de la sortie de la commande show.

- show vpdn - Affiche des informations sur le tunnel de protocole L2F (Level 2 Forwarding) actif et les identificateurs de message dans un VPDN.

Vous pouvez également utiliser show vpdn ? pour voir d'autres commandes show spécifiques à VPDN.

Dépannage

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

Dépannage des commandes

certaines commandes show sont prises en charge par l'outil Interpréteur de sortie, qui vous permet d'afficher une analyse de la sortie de la commande show.Note : Avant d'émettre des commandes debug, consultez Informations importantes sur les commandes de débogage.

- 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, y compris les échanges de paquets CHAP (Challenge Authentication Protocol) 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 y a des problèmes avec le chiffrement MPPE, utilisez l'une des commandes de débogage ci-dessous.
- debug ppp mppe packet - Affiche tout le trafic MPPE sortant entrant.
- 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 ne doit généralement être utilisée que sur un châssis de débogage avec une seule session active.

transmission tunnel partagée

Supposons que le routeur de passerelle est un routeur ISP. Lorsque le tunnel PPTP apparaît sur le PC, la route PPTP est installée avec une métrique plus

élevée que la métrique par défaut précédente, de sorte que nous perdons la connectivité Internet. Pour y remédier, modifiez le routage Microsoft afin de supprimer le routage par défaut et réinstallez le routage par défaut (cela nécessite de connaître l'adresse IP attribuée au client PPTP ; pour l'exemple actuel, il s'agissait de 172.16.10.1) :

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

Si le client n'est pas configuré pour le chiffrementSous l'onglet Sécurité de la connexion commutée utilisée pour la session PPTP, vous pouvez définir les paramètres d'authentification utilisateur. Par exemple, il peut s'agir d'une connexion au domaine PAP, CHAP, MS-CHAP ou Windows. Si vous avez choisi l'option No Encryption Allowed (le serveur se déconnecte s'il nécessite un chiffrement) dans la section Properties de la connexion VPN, vous pouvez voir un message d'erreur PPTP sur le client :

```
Registering your computer on the network..
Error 734:  The PPP link control protocol was terminated.
Debugs on the  router:
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV protocol=ccp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  8 22:38:52.500: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar  8 22:38:52.500: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  8 22:38:52.500: Vi1 CCP: State is Open
*Mar  8 22:38:52.500: Vi1 MPPE: RADIUS keying material missing
*Mar  8 22:38:52.500: Vi1 CCP: O TERMREQ [Open] id 5 len 4
*Mar  8 22:38:52.524: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  8 22:38:52.640: Vi1 CCP: I TERMACK [TERMsent] id 5 len 4
*Mar  8 22:38:52.640: Vi1 CCP: State is Closed
*Mar  8 22:38:52.640: Vi1 MPPE: Required encryption not negotiated
*Mar  8 22:38:52.640: Vi1 IPCP: State is Closed
*Mar  8 22:38:52.640: Vi1 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  8 22:38:52.640: Vi1 LCP: O TERMREQ [Open] id 13 len 4
*Mar  8 22:38:52.660: Vi1 IPCP: LCP not open, discarding packet
*Mar  8 22:38:52.776: Vi1 LCP: I TERMACK [TERMsent] id 13 len 4
*Mar  8 22:38:52.776: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar  8 22:38:52.780: Vi1 LCP: State is Closed
*Mar  8 22:38:52.780: Vi1 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  8 22:38:52.780: Vi1 VPDN: Cleanup
*Mar  8 22:38:52.780: Vi1 VPDN: Reset
*Mar  8 22:38:52.780: Vi1
Tnl/Cl 33/33 PPTP: close -> state change estabd to terminal
*Mar  8 22:38:52.780: Vi1 Tnl/Cl 33/33 PPTP:
Destroying session, trace follows:
*Mar  8 22:38:52.780: -Traceback= 60C4A150 60C4AE48 60C49F68 60C4B5AC
60C30450 60C18B10 60C19238 60602CC4 605FC380 605FB730 605FD614 605F72A8
6040DE0C 6040DDF8
*Mar  8 22:38:52.784: Vi1 Tnl/Cl 33/33 PPTP:
Releasing idb for tunnel 33 session 33
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
```

```
*Mar  8 22:38:52.784: Tnl 33 PPTP:
no-sess -> state change estabd to wt-stprp
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
```

Si le client est configuré pour le chiffrement et que le routeur n'est pasLe message suivant s'affiche sur le PC :

```
Registering your computer on the network..
Errror 742: The remote computer doesnot support the required data
encryption type.
On the Router:
*Mar  9 01:06:00.868: Vi2 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar  9 01:06:00.868: Vi2 CCP:    MS-PPC supported bits 0x010000B1
(0x1206010000B1)
*Mar  9 01:06:00.868: Vi2 LCP: O PROTREJ [Open] id 18 len 16 protocol CCP
(0x80FD0105000A1206010000B1)
*Mar  9 01:06:00.876: Vi2 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar  9 01:06:00.876: Vi2 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#1
1Z1`1k1}111
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 IPCP: Pool returned 172.16.10.1
*Mar  9 01:06:00.880: Vi2 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.884: Vi2 IPCP: I CONFACK [REQsent] id 8 len 10
*Mar  9 01:06:00.884: Vi2 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  9 01:06:01.024: Vi2 LCP: I TERMREQ [Open] id 7 len 16
(0x79127FBE003CCD74000002E6)
*Mar  9 01:06:01.024: Vi2 LCP: O TERMACK [Open] id 7 len 4
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: ClearReq -> state change
estabd to terminal
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: Destroying session, trace
follows:
*Mar  9 01:06:01.152: -Traceback= 60C4A150 60C4AE48 60C49F68 60C4B2CC
60C4B558 60C485E0 60C486E0 60C48AB8 6040DE0C 6040DDF8
*Mar  9 01:06:01.156: Vi2 Tnl/Cl 38/38 PPTP: Releasing idb for tunnel 38
session 38
*Mar  9 01:06:01.156: Vi2 VPDN: Reset
*Mar  9 01:06:01.156: Tnl 38 PPTP: no-sess -> state change estabd to
wt-stprp
*Mar  9 01:06:01.160: %LINK-3-UPDOWN: Interface Virtual-Access2, changed
state to down
*Mar  9 01:06:01.160: Vi2 LCP: State is Closed
*Mar  9 01:06:01.160: Vi2 IPCP: State is Closed
*Mar  9 01:06:01.160: Vi2 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  9 01:06:01.160: Vi2 VPDN: Cleanup
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
```

```
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: AAA/MEMORY: free_user (0x6273D528) user='tac' ruser=''
port='Virtual-Access2' rem_addr='' authen_type=MSCHAP service=PPP priv=1
*Mar  9 01:06:01.324: Tnl 38 PPTP: StopCCRQ -> state change wt-stprp to wt-stprp
*Mar  9 01:06:01.324: Tnl 38 PPTP: Destroy tunnel
*Mar  9 01:06:02.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to down
```

Désactivation de MS-CHAP lorsque le PC est configuré pour le chiffrement

Le message suivant s'affiche sur le PC :

```
The current encryption selection requires EAP or some version of
MS-CHAP logon security methods.
```

Si l'utilisateur spécifie un nom d'utilisateur ou un mot de passe incorrect, le résultat suivant s'affiche.Sur le PC :

```
Verifying Username and Password..
Error 691: Access was denied because the username and/or password
was invalid on the domain.
```

Sur le routeur :

```
*Mar  9 01:13:43.192: RADIUS: Received from id 139 10.200.20.245:1645,
Access-Reject, len 42
*Mar  9 01:13:43.192: Attribute 26 22 0000013702101545
*Mar  9 01:13:43.192: AAA/AUTHEN (608505327): status = FAIL
*Mar  9 01:13:43.192: Vi2 CHAP: Unable to validate Response. Username tac:
Authentication failure
*Mar  9 01:13:43.192: Vi2 MS-CHAP: O FAILURE id 21 len 13 msg is "E=691 R=0"
*Mar  9 01:13:43.192: Vi2 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  9 01:13:43.192: Vi2 LCP: O TERMREQ [Open] id 20 len 4
*Mar  9 01:13:43.196: AAA/MEMORY: free_user (0x62740E7C) user='tac'
ruser='' port='Virtual-Access2' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
```

Lorsque le serveur Radius n'est pas communicatif

Le résultat suivant s'affiche sur le routeur :

```
*Mar  9 01:18:32.944: RADIUS: Retransmit id 141
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No valid server found. Trying any viable server
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No response for id 141
*Mar  9 01:18:42.944: Radius: No response from server
*Mar  9 01:18:42.944: AAA/AUTHEN (374484072): status = ERROR
```

Informations connexes

- PPTP avec MPPE
- Page Technologie PPTP
- Présentation de VPDN
- Comprendre le rayon
- Configuration de CiscoSecure ACS pour l'authentification PPTP de routeurs Windows
- Support et documentation techniques - Cisco Systems