Konfigurieren der Cisco IOS Software und Windows 2000 für PPTP mithilfe von Microsoft IAS

Inhalt

Einführung

Die PPTP-Unterstützung (Point-to-Point Tunnel Protocol) wurde der Cisco IOS® Softwareversion 12.0.5.XE5 auf den Cisco Router-Plattformen 7100 und 7200 hinzugefügt. Die Unterstützung für weitere Plattformen wurde in Version 12.1.5.T der Cisco IOS-Software hinzugefügt.

Request for Comments (RFC) 2637 beschreibt PPTP. Laut RFC ist der PPTP Access Concentrator (PAC) der Client (d. h. der PC oder der Anrufer), und der PPTP Network Server (PNS) ist der Server (d. h. der Router oder das Gerät, das bzw. das aufgerufen wird).

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie PPTP-Verbindungen zum Router mit der lokalen Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) V1-Authentifizierung (und optional Microsoft Point-to-Point Encryption [MPPE], die MS-CHAP V1 erfordert) unter Verwendung dieser Dokumente eingerichtet haben und dass diese bereits funktionieren. Zur Unterstützung der MPPE-Verschlüsselung ist ein RADIUS (Remote Authentication Dial-In User Service) erforderlich. TACACS+ funktioniert für die Authentifizierung, jedoch nicht für die MPPE-Keying.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Microsoft IAS optionale Komponente, die auf einem erweiterten Microsoft 2000-Server mit Active Directory installiert ist.
- Ein Cisco Router der Serie 3600.
- Cisco IOS Softwareversion c3640-io3s56i-mz.121-5.T.

Bei dieser Konfiguration wird Microsoft IAS auf einem erweiterten Windows 200-Server als RADIUS-Server installiert.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundtheorie

In dieser Beispielkonfiguration wird veranschaulicht, wie ein PC für die Verbindung mit dem Router eingerichtet wird (unter der Adresse 10.200.20.2), der dann den Benutzer mit dem Microsoft Internet Authentication Server (IAS) (unter 10.200.20.245) authentifiziert, bevor der Benutzer in das Netzwerk eindringen kann. PPTP-Unterstützung ist mit Cisco Secure Access Control Server (ACS) Version 2.5 für Windows verfügbar. Aufgrund der Cisco Bug-ID CSCds92266 funktioniert sie jedoch möglicherweise nicht mit dem Router. Wenn Sie Cisco Secure verwenden, empfehlen wir die Verwendung von Cisco Secure Version 2.6 oder höher. MPPE wird von Cisco Secure UNIX nicht unterstützt. Zwei weitere RADIUS-Anwendungen mit MPPE-Unterstützung sind Microsoft RADIUS und Funk RADIUS.

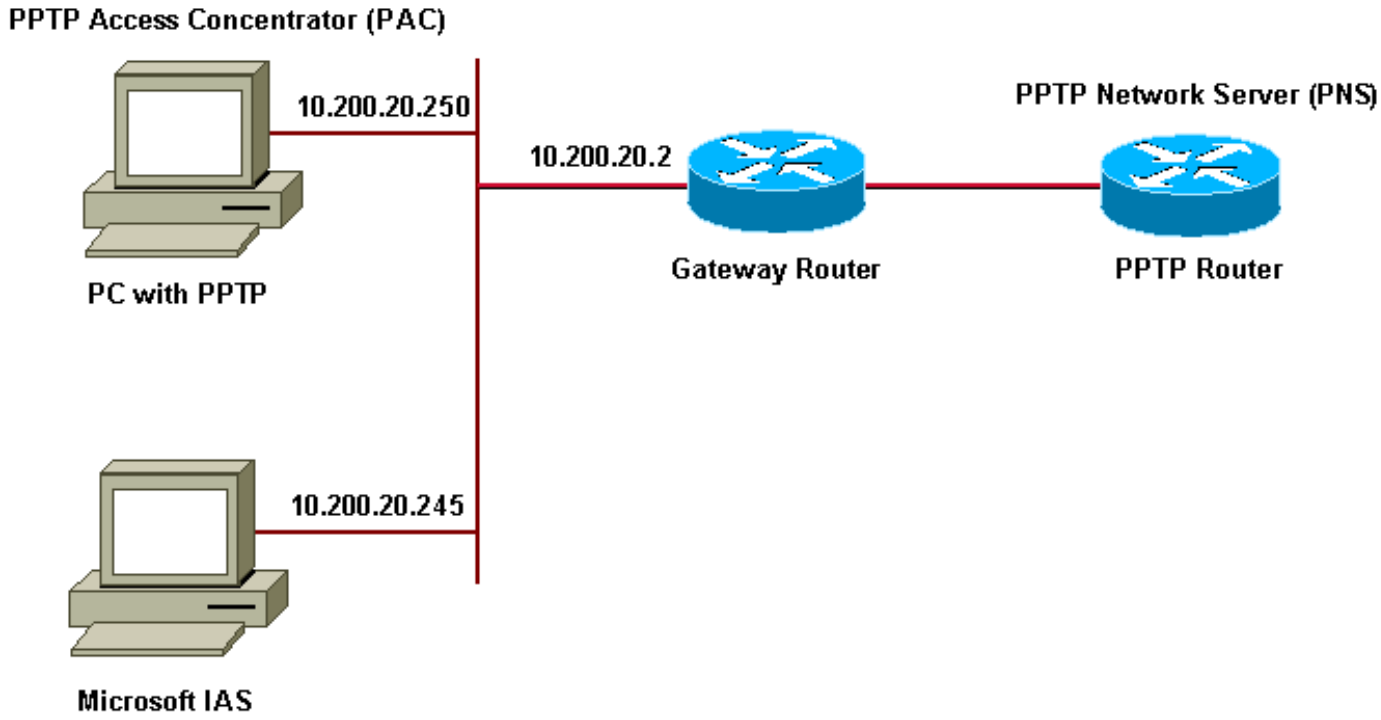
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das IOS-Befehlssuche-Tool.

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



IP-Pool für DFÜ-Clients:

- Gateway-Router: 192.168.1.2 - 192.168.1.254
- LNS: 172,16,10,1 - 172,16,10,10

Obwohl bei der oben beschriebenen Einrichtung ein DFÜ-Client für die Verbindung mit dem ISP-Router (Internet Service Provider) verwendet wird, können Sie den PC und den Gateway-Router über beliebige Medien, wie z. B. ein LAN, verbinden.

Konfigurieren des Windows 2000 Advanced Server für Microsoft IAS

In diesem Abschnitt wird gezeigt, wie der erweiterte Windows 2000-Server für Microsoft IAS konfiguriert wird:

1. Stellen Sie sicher, dass Microsoft IAS installiert ist. Um Microsoft IAS zu installieren, melden Sie sich als Administrator an. Überprüfen Sie unter **Netzwerkdienste**, ob alle Kontrollkästchen deaktiviert sind. Aktivieren Sie das Kontrollkästchen Internet Authentication Server (Internet-Authentifizierungsserver), und klicken Sie dann auf **OK**.
2. Klicken Sie im Assistenten **Windows-Komponenten** auf **Weiter**. Legen Sie die Windows 2000-CD ein, wenn Sie dazu aufgefordert werden.
3. Nachdem die erforderlichen Dateien kopiert wurden, klicken Sie auf **Fertig stellen** und schließen Sie dann alle Fenster. Sie müssen nicht neu starten.

Konfigurieren von RADIUS-Clients

In diesem Abschnitt werden die Schritte zum Konfigurieren von Radius-Clients beschrieben:

1. Öffnen Sie unter **Verwaltung** die **Internet Authentication Server** Console, und klicken Sie auf **Clients**.
2. Geben Sie im Feld **Freundlicher Name** die IP-Adresse des Netzwerkzugriffsservers (NAS) ein.
3. Klicken Sie auf **Diese IP-**Option **verwenden**.
4. Stellen Sie sicher, dass im Dropdown-Listenfeld **Client-Anbieter** die **RADIUS Standard-**Option aktiviert ist.
5. Geben Sie in die Felder **Freier geheimer** und **geheimer geheimer Schlüssel bestätigen** das Kennwort ein und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Internet Authentication Service**, und klicken Sie dann auf **Start**.
7. Schließen Sie die Konsole.

Konfigurieren von Benutzern in IAS

Im Gegensatz zu Cisco Secure ist die Windows 2000 RADIUS-Benutzerdatenbank eng mit der Windows-Benutzerdatenbank verknüpft. Falls ein **Active Directory** auf Ihrem Windows 2000-Server installiert ist, erstellen Sie Ihre neuen DFÜ-Benutzer von **Active Directory-Benutzern und -Computern**. Wenn **Active Directory** nicht installiert ist, können Sie mithilfe der **Verwaltungstools Lokale Benutzer und Gruppen** neue Benutzer erstellen.

Konfigurieren von Benutzern im Active Directory

In diesem Abschnitt werden die Schritte zum Konfigurieren von Benutzern im aktiven Verzeichnis beschrieben:

1. Erweitern Sie in der Konsole **Active Directory-Benutzer und -Computer** Ihre Domäne. Klicken Sie mit der rechten Maustaste auf **Benutzer**. Navigieren Sie zu **Neuer Benutzer**. Erstellen Sie einen neuen Benutzer mit dem Namen **tac**.
2. Geben Sie ein Kennwort in die Dialogfelder **Kennwort** und **Kennwort bestätigen ein**.
3. Löschen Sie das Feld **Benutzer muss Kennwort bei Nächster Anmeldung ändern**, und klicken Sie auf **Weiter**.
4. Öffnen Sie das Feld **Benutzer-TAC-Eigenschaften. Wechseln Sie zur Registerkarte Einwählen. Klicken Sie unter Remotezugriffsberechtigung (Einwahl oder VPN) auf Zugriff zulassen, und klicken Sie dann auf OK.**

Konfigurieren von Benutzern, wenn kein Active Directory installiert istIn diesem Abschnitt werden die Schritte zum Konfigurieren von Benutzern beschrieben, wenn kein Active Directory installiert ist:

1. **Klicken Sie im Abschnitt "Verwaltung" auf Computerverwaltung. Erweitern Sie die Konsole Computerverwaltung, und klicken Sie auf Lokale Benutzer und Gruppen. Klicken Sie mit der rechten Maustaste auf die Bildlaufleiste Benutzer, um Neuer Benutzer auszuwählen. Erstellen Sie einen neuen Benutzer mit dem Namen tac.**
2. **Geben Sie ein Kennwort in die Dialogfelder Kennwort und Kennwort bestätigen ein.**
3. **Deaktivieren Sie die Option Benutzer muss Kennwort bei Nächster Anmeldung ändern, und klicken Sie auf Weiter.**
4. **Öffnen Sie das Feld Eigenschaften des neuen Benutzers. Wechseln Sie zur Registerkarte**

Einwählen. Klicken Sie unter Remotezugriffsberechtigung (Einwahl oder VPN) auf Zugriff zulassen und klicken Sie anschließend auf OK.

Anwenden einer Richtlinie für den Remote-Zugriff auf den Windows-BenutzerIn diesem Abschnitt werden die Schritte zum Anwenden einer Remotezugriffsrichtlinie auf den Windows-Benutzer beschrieben:

1. Öffnen Sie unter Verwaltung die Internet Authentication Server-Konsole, und klicken Sie auf Remote Access Policies (Remote-Zugriffsrichtlinien).
2. Klicken Sie auf die Schaltfläche Hinzufügen unter Zuzuordnende Bedingungen angeben, und fügen Sie Servicetyp hinzu. Wählen Sie den verfügbaren Typ als Framed aus, und fügen Sie ihn der Liste Ausgewählte Typen hinzu. Drücken Sie OK.
3. Klicken Sie unter Zuzuordnende Bedingungen angeben auf die Schaltfläche Hinzufügen und fügen Sie Framed-Protokoll hinzu. Wählen Sie den verfügbaren Typ als ppp aus, und fügen Sie ihn der Liste Ausgewählte Typen hinzu. Drücken Sie OK.
4. Klicken Sie auf die Schaltfläche Hinzufügen unter Zuzuordnende Bedingungen angeben, und fügen Sie Windows-Gruppen hinzu, um die Windows-Gruppe hinzuzufügen, der der Benutzer angehört. Wählen Sie die Gruppe aus, fügen Sie sie den ausgewählten Typen hinzu und drücken Sie OK.
5. Wählen Sie in den Eigenschaften Zugriff zulassen, wenn die DFÜ-Berechtigung aktiviert ist, die Option Remotezugriffsberechtigung gewähren aus.
6. Schließen Sie die Konsole.

Konfigurieren des Windows 2000-Clients für PPTPIm folgenden Abschnitt werden die Schritte zum Konfigurieren des Windows 2000-Clients für PPTP beschrieben:

1. Wählen Sie im Start-Menü Einstellungen und dann entweder:Systemsteuerung, Netzwerk- und DFÜ-Verbindungen oderNetzwerk- und DFÜ-Verbindungen stellen dann eine neue Verbindung her.Verwenden Sie den Assistenten, um eine Verbindung mit dem Namen PPTP zu erstellen. Diese Verbindung stellt über das Internet eine Verbindung zu einem privaten Netzwerk her. Sie müssen auch die IP-Adresse oder den IP-Namen des PPTP-Netzwerkservers (PNS) angeben.
2. Die neue Verbindung wird im Fenster Netzwerk- und DFÜ-Verbindungen unter Systemsteuerung angezeigt.Klicken Sie hier auf die rechte Maustaste, um die Eigenschaften zu bearbeiten. Stellen Sie unter der Registerkarte "Netzwerk" sicher, dass das Feld Servertyp I Am Anruf auf PPTP festgelegt ist. Wenn Sie planen, diesem Client entweder über einen lokalen Pool oder ein Dynamic Host Configuration Protocol (DHCP) eine dynamische interne Adresse vom Gateway zuzuweisen, wählen Sie TCP/IP-Protokoll, und stellen Sie sicher, dass der Client so konfiguriert ist, dass er automatisch eine IP-Adresse erhält. Sie können DNS-Informationen auch automatisch ausgeben.Mit der Schaltfläche Erweitert können Sie statische Windows Internet Naming Service (WINS)- und DNS-Informationen definieren.Mit dem Register Optionen können Sie IPSec deaktivieren oder der Verbindung eine andere Richtlinie zuweisen.
3. Auf der Registerkarte Sicherheit können Sie die Parameter für die Benutzerauthentifizierung festlegen. Beispiel: Anmeldung bei PAP, CHAP oder MS-CHAP oder Windows-Domäne. Wenn die Verbindung konfiguriert ist, können Sie auf sie doppelklicken, um den Anmeldebildschirm anzuzeigen und dann eine Verbindung herzustellen.

KonfigurationenMithilfe der folgenden Router-Konfiguration kann der Benutzer eine Verbindung mit dem Benutzernamen TAC und dem Kennwort admin herstellen, selbst wenn der RADIUS-Server nicht verfügbar ist (dies ist möglich, wenn die Microsoft IAS noch konfiguriert werden muss). In der folgenden Beispielkonfiguration werden die für L2tp ohne IPSec erforderlichen Befehle beschrieben.

Engel

```
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
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.Bestimmte show-Befehle werden vom Tool Output Interpreter unterstützt, mit dem Sie eine Analyse der Ausgabe des Befehls show anzeigen können.

- show vpdn - Zeigt Informationen über den L2F-Protokolltunnel (Active Level 2 Forwarding) und die Meldungsbezeichner in einem VPDN an.

Sie können auch show vpdn verwenden? um weitere VPDN-spezifische show-Befehle anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte show-Befehle werden vom Tool Output Interpreter unterstützt, mit dem Sie eine Analyse der Ausgabe des Befehls show anzeigen können.Hinweis: Bevor Sie Debugbefehle ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- debug aaa authentication: Zeigt Informationen über die AAA/TACACS+-Authentifizierung an.
- debug aaa autorization - Zeigt Informationen zur AAA/TACACS+-Autorisierung an.
- debug ppp negotiation - Zeigt PPP-Pakete an, die während des PPP-Starts übertragen werden und über die PPP-Optionen ausgehandelt werden.
- debug ppp authentication: Zeigt Authentifizierungsprotokollmeldungen an, einschließlich CHAP-Paketaustausch (Challenge Authentication Protocol) und PAP-Austausch (Password Authentication Protocol).
- Debug-Radius - Zeigt detaillierte Debuginformationen an, die dem RADIUS zugeordnet sind. Wenn die Authentifizierung funktioniert, aber Probleme mit der MPPE-Verschlüsselung auftreten, verwenden Sie einen der folgenden Debugbefehle.
- debug ppp mppe packet - Zeigt den gesamten eingehenden MPPE-Datenverkehr an.
- debug ppp mppe event - Zeigt die MPPE-Schlüsselereignisse an.
- debug ppp mppe detail - Zeigt ausführliche MPPE-Informationen an.
- debug vpdn l2x-pakete - Zeigt Meldungen über L2F-Protokollheader und -Status an.

- debug vpdn events - Zeigt Meldungen über Ereignisse an, die Teil der normalen Tunneleinrichtung oder -abschaltung sind.
- debug vpdn errors - Zeigt Fehler an, die verhindern, dass ein Tunnel erstellt wird, oder Fehler, die das Schließen eines etablierten Tunnels verursachen.
- debug vpdn pakete - Zeigt jedes ausgetauschte Protokollpaket an. Diese Option kann zu einer großen Anzahl von Debug-Meldungen führen und sollte im Allgemeinen nur in einem Debug-Chassis mit einer einzigen aktiven Sitzung verwendet werden.

Split TunnelingNehmen wir an, der Gateway-Router ist ein ISP-Router. Wenn der PPTP-Tunnel auf dem PC hochgefahren wird, wird die PPTP-Route mit einer höheren Metrik als die vorherige Standardeinstellung installiert, sodass die Internetverbindung unterbrochen wird. Um dies zu beheben, ändern Sie das Microsoft-Routing, um den Standardwert zu löschen, und installieren Sie die Standardroute neu (hierzu muss die IP-Adresse bekannt sein, der der PPTP-Client zugewiesen wurde. für das aktuelle Beispiel war dies 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
```

Wenn der Client nicht für die Verschlüsselung konfiguriert istAuf der Registerkarte Sicherheit der für die PPTP-Sitzung verwendeten DFÜ-Verbindung können Sie die Parameter für die Benutzerauthentifizierung festlegen. Dies kann z. B. PAP-, CHAP-, MS-CHAP- oder Windows-Domänenanmeldung sein. Wenn Sie die Option Keine Verschlüsselung zulässig (Server trennt, wenn Verschlüsselung erforderlich ist) im Abschnitt Eigenschaften der VPN-Verbindung ausgewählt haben, wird möglicherweise eine PPTP-Fehlermeldung auf dem Client angezeigt:

```
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
```

Wenn der Client für die Verschlüsselung konfiguriert ist und der Router nicht Die folgende Meldung wird auf dem PC angezeigt:

```
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
```

Deaktivieren von MS-CHAP, wenn der Computer für die Verschlüsselung konfiguriert istDie folgende Meldung wird auf dem PC angezeigt:

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

Wenn der Benutzer einen falschen Benutzernamen oder ein falsches Kennwort angibt, wird folgende Ausgabe angezeigt.Auf dem PC:

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

Auf dem Router:

```
*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
```

Wenn der RADIUS-Server nicht kommuniziertDie folgende Ausgabe wird auf dem Router angezeigt:

```
*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
```

Zugehörige Informationen

- PPTP mit MPPE
- PPTP-Technologie-Seite
- VPDN im Überblick
- Radius
- Konfigurieren von CiscoSecure ACS für PPTP-Authentifizierung des Windows-Routers
- Technischer Support und Dokumentation - Cisco Systems