Configurazione del software Cisco IOS e di Windows 2000 per PPTP con Microsoft IAS

Sommario

Introduzione

Il supporto PPTP (Point-to-Point Tunnel Protocol) è stato aggiunto al software Cisco IOS® versione 12.0.5.XE5 sulle piattaforme dei router Cisco 7100 e 7200. Il supporto per più piattaforme è stato aggiunto nel software Cisco IOS versione 12.1.5.T.

Request for Comments (RFC) 2637 descrive PPTP. In base a questa RFC, il PPTP Access Concentrator (PAC) è il client (ossia il PC o il chiamante) e il PPTP Network Server (PNS) è il server (ossia il router o il dispositivo chiamato).

Prerequisiti

Requisiti

In questo documento si presume che le connessioni PPTP al router siano state configurate con l'autenticazione V1 Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) locale (e, facoltativamente, Microsoft Point-to-Point Encryption [MPPE] che richiede MS-CHAP V1) utilizzando questi documenti e che stiano già funzionando. Per il supporto della crittografia MPPE è necessario il servizio RADIUS (Remote Authentication Dial-In User Service). TACACS+ funziona per l'autenticazione, ma non per la generazione di chiavi MPPE.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Componente facoltativo di Microsoft IAS installato in un server avanzato Microsoft 2000 con Active Directory.
- Un router Cisco 3600.
- Software Cisco IOS release c3640-io3s56i-mz.121-5.T.

In questa configurazione viene utilizzato Microsoft IAS installato in un server avanzato Windows 2000 come server RADIUS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Nozioni di base

In questa configurazione di esempio viene illustrato come configurare un PC per la connessione al router (all'indirizzo 10.200.20.2), che quindi autentica l'utente in Microsoft Internet Authentication Server (IAS) (alla posizione 10.200.245) prima di consentire l'accesso dell'utente alla rete. Il supporto PPTP è disponibile con Cisco Secure Access Control Server (ACS) versione 2.5 per Windows. Tuttavia, potrebbe non funzionare con il router a causa dell'ID bug Cisco CSCds92266. Se si usa Cisco Secure, si consiglia di usare Cisco Secure versione 2.6 o successive. Cisco Secure UNIX non supporta MPPE. Altre due applicazioni RADIUS supportate da MPPE sono Microsoft RADIUS e Funk RADIUS.

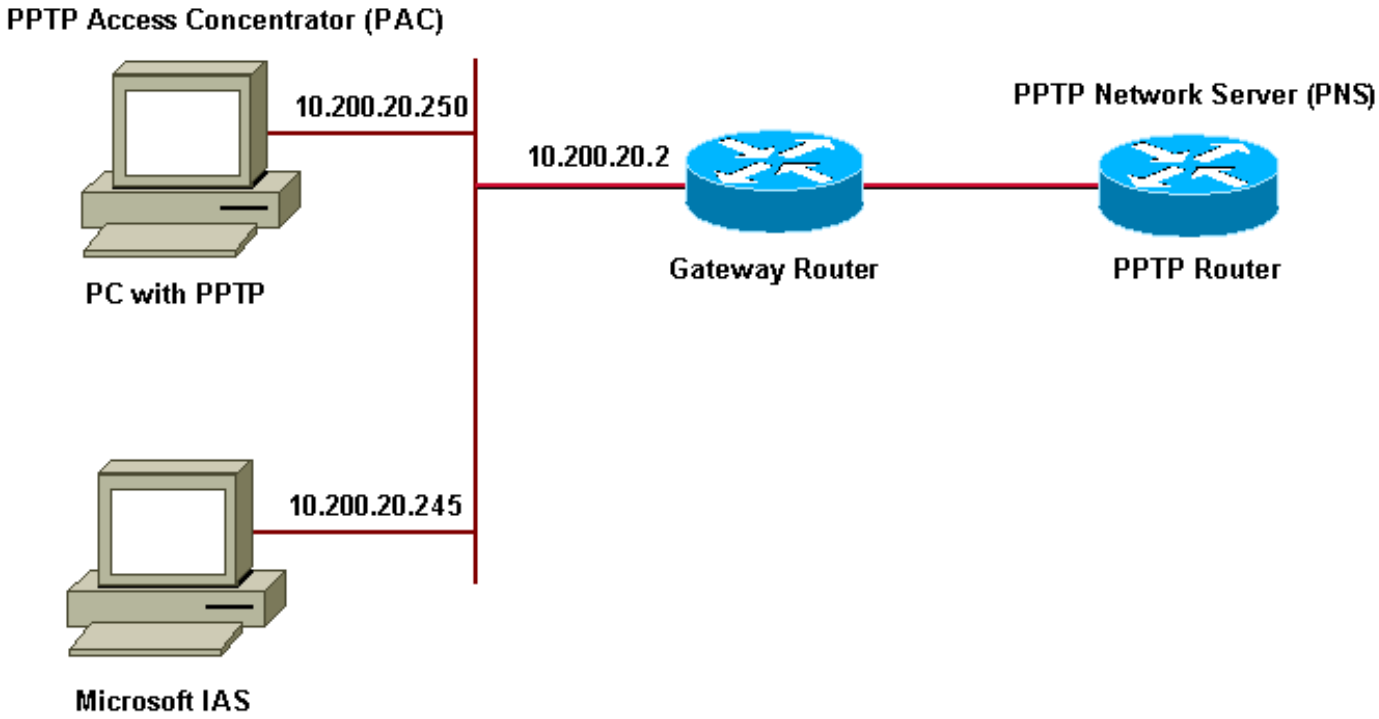
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi di IOS

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Pool IP per client remoti:

- Router gateway: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.10

Sebbene la configurazione sopra descritta utilizzi un client di connessione remota per connettersi al router del provider di servizi Internet (ISP) tramite connessione remota, è possibile connettere il PC e il router gateway tramite qualsiasi supporto, ad esempio una LAN.

Configurazione di Windows 2000 Advanced Server per Microsoft IAS

Questa sezione illustra come configurare il server avanzato di Windows 2000 per Microsoft IAS:

1. Verificare che Microsoft IAS sia installato. Per installare Microsoft IAS, accedere come amministratore. In **Servizi di rete** verificare che tutte le caselle di controllo siano deselezionate. Selezionare la casella di controllo Server di autenticazione Internet e quindi fare clic su **OK**.
2. Nella Creazione guidata **Componenti di Windows** fare clic su **Avanti**. Se richiesto, inserire il CD di Windows 2000.
3. Dopo aver copiato i file richiesti, fare clic su **Fine** e chiudere tutte le finestre. Non è necessario riavviare il sistema.

Configurazione dei client Radius

In questa sezione vengono illustrati i passaggi per configurare i client radius:

1. Da **Strumenti di amministrazione**, aprire la console **Internet Authentication Server** e fare clic su **Client**.
2. Nella casella **Nome descrittivo** digitare l'indirizzo IP del server di accesso alla rete (NAS).

3. Fare clic sull'opzione **Use this IP**.
4. Nella casella di riepilogo a discesa **Client-Vendor**, verificare che l'opzione **RADIUS Standard** sia selezionata.
5. Nelle caselle **Segreto condiviso** e **Conferma segreto condiviso** digitare la password e quindi fare clic su **Fine**.
6. Nell'albero della console fare clic con il pulsante destro del mouse su **Internet Authentication Service** e quindi scegliere **Avvia**.
7. Chiudere la console.

Configurazione degli utenti su IAS

A differenza di Cisco Secure, il database utenti RADIUS di Windows 2000 è strettamente associato al database utenti di Windows. Se nel server Windows 2000 è installato **Active Directory**, creare i nuovi utenti remoti da **Utenti e computer di Active Directory**. Se **Active Directory** non è installato, utilizzare **Utenti e gruppi locali** da **Strumenti di amministrazione** per creare nuovi utenti.

Configurazione degli utenti in Active Directory

Questa sezione illustra la procedura per configurare gli utenti in Active Directory:

1. Nella console **Utenti e computer di Active Directory** espandere il dominio. Fare clic con il pulsante destro del mouse su **Utenti**. Scorrere fino a selezionare **Nuovo utente**. Creare un nuovo utente denominato **tac**.
2. Digitare una password nelle finestre di dialogo **Password** e **Conferma password**.
3. Deselezionare il campo **Cambiamento obbligatorio password all'accesso successivo** e fare clic su **Avanti**.
4. Aprire la casella **User tac Properties. Passare alla scheda Dial-In. In Autorizzazioni di accesso remoto (chiamate in ingresso o VPN) fare clic su Consenti accesso e quindi su OK.**

Configurazione degli utenti se non è installato Active DirectoryIn questa sezione vengono illustrati i passaggi per configurare gli utenti se non è installato Active Directory:

1. **Dalla sezione Strumenti di amministrazione, fare clic su Gestione computer. Espandere la console Gestione computer e fare clic su Utenti e gruppi locali. Fare clic con il pulsante destro del mouse sulla barra di scorrimento Utenti per selezionare Nuovo utente. Creare un nuovo utente denominato tac.**
2. **Digitare una password nelle finestre di dialogo Password e Conferma password.**
3. **Deselezionare l'opzione Cambiamento obbligatorio password all'accesso successivo e fare clic su Avanti.**
4. **Aprire la casella Proprietà tac del nuovo utente. Passare alla scheda Connessione remota. In Autorizzazioni di accesso remoto (chiamate in ingresso o VPN) fare clic su Consenti accesso, quindi su OK.**

Applicazione di un criterio di accesso remoto all'utente di WindowsIn questa sezione vengono illustrati i passaggi per applicare un criterio di accesso remoto all'utente Windows:

1. **Da Strumenti di amministrazione, aprire la console Internet Authentication Server e fare clic su Criteri di accesso remoto.**
2. **Fare clic sul pulsante Add (Aggiungi) in Specify the Conditions to Match (Specifica le condizioni da soddisfare), quindi aggiungere Service-Type (Tipo di servizio). Scegliete il tipo disponibile Framed e aggiungetelo all'elenco Selected Types. Premere OK.**

3. Fare clic sul pulsante Add (Aggiungi) in Specify the Conditions to Match (Specifica le condizioni da soddisfare) e aggiungere Framed Protocol. Scegliere il tipo disponibile come ppp e aggiungerlo all'elenco Tipi selezionati. Premere OK.
4. Fare clic sul pulsante Add (Aggiungi) in Specify the Conditions to Match (Specifica le condizioni da soddisfare) e aggiungere Windows-Groups (Gruppi di Windows) per aggiungere il gruppo di Windows a cui appartiene l'utente. Selezionate il gruppo e aggiungetelo ai tipi selezionati e premete OK.
5. Nella finestra di dialogo Consenti accesso se l'autorizzazione di connessione remota è abilitata, selezionare Concedi autorizzazione di accesso remoto.
6. Chiudere la console.

Configurazione del client Windows 2000 per PPTP

Nella sezione seguente vengono illustrati i passaggi per configurare il client Windows 2000 per PPTP:

1. Dal menu Start, selezionare Impostazioni, quindi:Pannello di controllo e Rete e connessioni remote, oppureRete e connessioni remote, quindi Crea nuova connessione.Utilizzare la procedura guidata per creare una connessione denominata PPTP. La connessione si connette a una rete privata tramite Internet. È inoltre necessario specificare l'indirizzo IP o il nome del server di rete PPTP (PNS).
2. La nuova connessione verrà visualizzata nella finestra Rete e connessioni remote nel Pannello di controllo.Fare clic con il pulsante destro del mouse per modificarne le proprietà. Nella scheda Rete verificare che il campo Tipo di server che si sta chiamando sia impostato su PPTP. Se si intende allocare un indirizzo interno dinamico al client dal gateway, tramite un pool locale o il protocollo DHCP (Dynamic Host Configuration Protocol), selezionare il protocollo TCP/IP e verificare che il client sia configurato per ottenere automaticamente un indirizzo IP. È inoltre possibile rilasciare automaticamente le informazioni DNS.Il pulsante Avanzate consente di definire informazioni statiche WINS (Windows Internet Naming Service) e DNS.La scheda Opzioni consente di disattivare IPSec o assegnare un criterio diverso alla connessione.
3. Nella scheda Protezione è possibile definire i parametri di autenticazione dell'utente. Ad esempio, PAP, CHAP o MS-CHAP o accesso al dominio Windows. Una volta configurata la connessione, è possibile fare doppio clic su di essa per visualizzare la schermata di accesso e quindi connettersi.

Configurazioni

Utilizzando la seguente configurazione del router, l'utente è in grado di connettersi con il nome utente tac e la password admin anche se il server RADIUS non è disponibile (ciò è possibile quando Microsoft IAS non è ancora stato configurato). Nella configurazione di esempio seguente vengono illustrati i comandi necessari per L2tp senza 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.Alcuni comandi show sono supportati dallo strumento Output Interpreter, che consente di visualizzare un'analisi dell'output del comando show.

- show vpdn: visualizza le informazioni sul tunnel del protocollo L2F (Level 2 Forwarding) attivo e gli identificatori di messaggio in una VPDN.

È possibile usare anche il comando show vpdn? per visualizzare altri comandi show specifici della VPDN.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi show sono supportati dallo strumento Output Interpreter, che consente di visualizzare un'analisi dell'output del comando show.Nota: prima di usare i comandi di debug, consultare le informazioni importanti sui comandi di debug.

- debug aaa authentication: visualizza le informazioni sull'autenticazione AAA/TACACS+.
- debug aaa authorization: visualizza le informazioni sull'autorizzazione AAA/TACACS+.
- debug ppp negotiation: visualizza i pacchetti PPP trasmessi durante l'avvio del protocollo PPP, dove le opzioni PPP vengono negoziate.
- debug ppp authentication: visualizza i messaggi del protocollo di autenticazione, inclusi gli scambi di pacchetti Challenge Authentication Protocol (CHAP) e gli scambi PAP (Password Authentication Protocol).
- debug radius: visualizza informazioni di debug dettagliate associate a RADIUS. Se l'autenticazione funziona ma si verificano problemi con la crittografia MPPE, utilizzare uno dei comandi di debug riportati di seguito.
- debug ppp mppe packet: visualizza tutto il traffico MPPE in entrata in uscita.
- debug ppp mppe event: visualizza le occorrenze principali di MPPE.
- debug ppp mppe detail - Visualizza informazioni dettagliate su MPPE.
- debug vpdn l2x-packets: visualizza i messaggi relativi alle intestazioni e allo stato del protocollo L2F.
- debug vpdn events: visualizza i messaggi relativi agli eventi che fanno parte della normale creazione del tunnel o del processo di arresto.
- debug vpdn errors: visualizza gli errori che impediscono di stabilire un tunnel o gli errori che provocano la chiusura di un tunnel stabilito.
- debug vpdn packets: visualizza tutti i pacchetti del protocollo scambiati. Questa opzione può generare un numero elevato di messaggi di debug e in genere deve essere utilizzata solo su uno chassis di debug con una singola sessione attiva.

Tunneling ripartito

Si supponga che il router gateway sia un router ISP. Quando sul PC viene visualizzato il tunnel PPTP, il percorso PPTP viene installato con una metrica superiore a quella predefinita, pertanto la connettività Internet viene interrotta. Per risolvere questo problema, modificare il routing Microsoft in modo da eliminare il routing predefinito e reinstallare il route predefinito (è necessario conoscere l'indirizzo IP assegnato al client PPTP; nell'esempio corrente, questo valore è 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
```

Se il client non è configurato per la crittografiaNella scheda Protezione della connessione remota utilizzata per la sessione PPTP è possibile definire i parametri di autenticazione utente. Può trattarsi ad esempio di un accesso al dominio PAP, CHAP, MS-CHAP o Windows. Se è stata selezionata l'opzione No Encryption Allowed (il server si disconnette se richiede la crittografia) nella sezione Proprietà della connessione VPN, è possibile che venga visualizzato un messaggio di errore PPTP sul 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
```

Se il client è configurato per la crittografia e il router non èSul PC viene visualizzato il seguente messaggio:

```
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
```

Disattivazione di MS-CHAP quando il PC è configurato per la crittografiaSul PC viene visualizzato il seguente messaggio:

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

Se l'utente specifica un nome utente o una password errati, viene visualizzato l'output seguente.Sul PC:

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

Sul 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
```

Quando il server Radius non è comunicativoSul router è possibile visualizzare l'output seguente:

```
*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
```

Informazioni correlate

- PPTP con MPPE
- Pagina sulla tecnologia PPTP
- Informazioni sulla VPDN
- Informazioni sul raggio
- Configurazione di Cisco Secure ACS per l'autenticazione PPTP del router Windows
- Documentazione e supporto tecnico – Cisco Systems