

Configuring Cisco IOS Software and Windows 2000 for PPTP Using Microsoft IAS

(Configurando o software Cisco IOS e o Windows 2000 para PPTP usando o Microsoft IAS)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Material de Suporte](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurando o Windows 2000 Advanced Server para Microsoft IAS](#)

[Configuração dos clientes RADIUS](#)

[Configurando usuários em IAS](#)

[Configurando o cliente Windows 2000 para PPTP](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Encapsulamento dividido](#)

[Se o cliente não está configurado para criptografia](#)

[Se o cliente estiver configurado para criptografia e o roteador não estiver](#)

[Desativando o MS-CHAP quando o PC é configurado para criptografia](#)

[Quando o servidor Radius não estiver comunicativo](#)

[Informações Relacionadas](#)

[Introduction](#)

O suporte ao Point-to-Point Tunnel Protocol (PPTP) foi adicionado ao Cisco IOS® Software Release 12.0.5.XE5 nas plataformas do roteador Cisco 7100 e 7200. O suporte a mais plataformas foi adicionado ao Cisco IOS Software Release 12.1.5.T.

A Solicitação de Comentários (RFC, Request for Comments) 2637 descreve o PPTP. De acordo com esta RFC, o Concentrador de Acesso PPTP (PAC, PPTP Access Concentrator) é o cliente

(isto é, o PC ou chamador), e o Servidor de Rede PPTP (PNS, PPTP Network Server) é o servidor (isto é, o roteador ou o dispositivo sendo chamado).

Prerequisites

Requirements

Este documento pressupõe que, usando seu conteúdo, você instalou as conexões PPTP no roteador com a autenticação do Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) e opcionalmente com a Criptografia Ponto a Ponto da Microsoft (MPPE, Microsoft Point-to-Point Encryption), que requer MS-CHAP V1, e que as conexões já estão funcionando. O Serviço de Usuário de Discagem de Autenticação Remota (RADIUS, Remote Authentication Dial-In User Service) é necessário para o suporte à criptografia MPPE; O TACACS+ funciona para autenticação, mas não para chaveamento de MPPE.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Componente opcional do Microsoft IAS instalado em um servidor avançado do Microsoft 2000 com Active Directory.
- Um Cisco Router 3600.
- Cisco IOS Software Release c3640-io3s56i-mz.121-5.T.

Essa configuração usa o Microsoft IAS instalado em um servidor avançado do Windows 2000 como o servidor RADIUS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Material de Suporte

Essa configuração de exemplo demonstra como configurar um PC para se conectar ao roteador (no endereço 10.200.20.2), que autentica então o usuário para o Internet Authentication Server (IAS) da Microsoft (em 10.200.20.245) antes de permitir que o usuário faça login na rede. O suporte ao PPTP está disponível com o Cisco Secure Access Control Server (ACS) Version 2.5 for Windows. Contudo, poderá não funcionar com o roteador devido ao ID de bug CSCds92266 da Cisco. Se você estiver usando o Cisco Secure, recomendamos que use a versão 2.6 ou posterior. O Cisco Secure UNIX não é compatível com a MPPE. Outros dois aplicativos RADIUS com suporte para MPPE são o Microsoft RADIUS e o Funk RADIUS.

Configurar

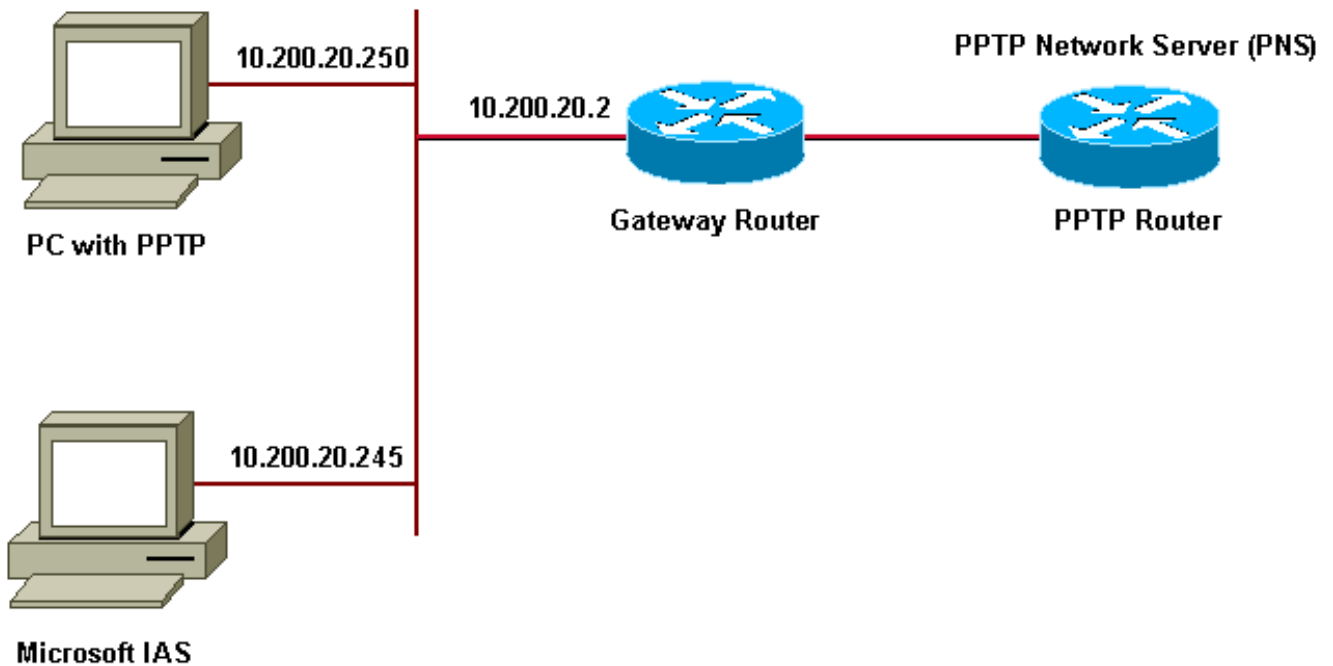
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta IOS Command Lookup

[Diagrama de Rede](#)

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

PPTP Access Concentrator (PAC)



Conjunto de IP para clientes dial-up:

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

Embora a configuração acima use um cliente dial-up para conectar ao provedor de Internet (ISP, Internet Service Provider) via dial-up, você pode conectar o PC e o roteador gateway por meio de qualquer mídia, como uma LAN.

[Configurando o Windows 2000 Advanced Server para Microsoft IAS](#)

Esta seção mostra como configurar o servidor avançado do Windows 2000 para Microsoft IAS:

1. Certifique-se de que o Microsoft IAS esteja instalado. Para instalar o Microsoft IAS, faça login como um administrador. Em **Network Services**, verifique se todas as caixas de seleção estão desmarcadas. Marque a caixa de seleção Internet Authentication Server e clique em **OK**.
2. No **Windows Components wizard**, clique em **Next**. Se solicitado, insira o CD do Windows 2000.
3. Depois que os arquivos necessários tiverem sido copiados, clique em **Finish** e feche todas as janelas. Não é preciso reinicializar.

[Configuração dos clientes RADIUS](#)

Esta seção mostra os passos para configurar clientes RADIUS:

1. Em **Administrative Tools**, abra o Internet Authentication Server Console e clique em Clients.
2. Na caixa **Friendly Name**, digite o endereço IP do servidor de acesso à rede (**NAS, network access server**).
3. Clique em **Use this IP option**.
4. Na caixa da lista suspensa **Client-Vendor**, certifique-se de que a opção **RADIUS Standard** esteja selecionada.
5. Nas caixas **Shared Secret** e **Confirm Shared Secret**, digite a senha e clique em **Finish**.
6. Na árvore de console, clique com o botão direito em **Internet Authentication Service** e clique em **Start**.
7. Feche a console.

[Configurando usuários em IAS](#)

Diferentemente do Cisco Secure, o banco de dados do RADIUS do Windows 2000 é estreitamente ligado ao banco de dados de usuário do Windows. Caso haja um **Active Directory** instalado em seu servidor do Windows 2000, crie seus novos usuários dial-up em **Active Directory Users and Computers**. Se o **Active Directory** não estiver instalado, use **Local Users and Groups** em **Administrative tools** para criar novos usuários.

[Configuração de Usuários no Active Directory](#)

Esta seção mostra os passos para configurar usuários no Active Directory:

1. Na console **Active Directory Users and Computers**, expanda seu domínio. Clique com o botão direito em **Users**. Mova a barra de rolagem para selecionar **New User**. Crie um novo usuário chamado **tac**.
2. Digite a senha nas caixas de diálogo **Password** e **Confirm Password**.
3. Desmarque o campo **User Must Change Password at Next Logon** e clique em **Next**.
4. Abra a caixa **User tac Properties**. Altere para a guia **Dial-In**. Em **Remote Access Permission (Dial-in or VPN)**, clique em **Allow Access** e depois em **OK**.

Configuração de Usuários se o Active Directory Não Estiver Instalado

Esta seção mostra os passos para configurar usuários se o Active Directory não estiver instalado:

1. Na seção **Administrative Tools**, clique em **Computer Management**. Expand a console do **Computer Management** e clique em **Local Users and Groups**. Clique com o botão direito na barra de rolagem **Users** para selecionar **New User**. Crie um novo usuário chamado **tac**.
2. Digite a senha nas caixas de diálogo **Password** e **Confirm Password**.
3. Desmarque a opção **User Must Change Password at Next Logon** e clique em **Next**.
4. Abra a caixa do novo usuário chamada **tac's Properties**. Altere para a guia **Dial-In**. Em **Remote Access Permission (Dial-in or VPN)**, clique em **Allow Access** e depois em **OK**.

[Aplicando uma política de acesso remoto ao usuário Windows](#)

Esta seção mostra os passos para aplicar uma política de acesso remoto ao usuário do Windows:

1. Em **Administrative Tools**, abra a console do Internet Authentication Server e clique em Remote Access Policies.
2. Clique no botão **Add**, em **Specify the Conditions to Match**, e adicione **Service-Type**. Escolha o tipo disponível como **Framed** e adicione-o à lista **Selected Types**. Pressione **OK**.
3. Clique no botão **Add**, em **Specify the Conditions to Match**, e adicione **Framed Protocol**. Escolha o tipo disponível como **ppp** e adicione-o à lista **Selected Types**. Pressione **OK**.
4. Clique no botão **Add**, em **Specify the Conditions to Match**, e adicione **Windows-Groups** para adicionar o grupo do Windows ao qual o usuário pertence. Escolha o grupo, adicione-o a **Selected Types** e pressione **OK**.
5. Nas propriedades **Allow Access if Dial-in Permission is Enabled**, selecione **Grant remote Access permission**.
6. Feche a console.

[Configurando o cliente Windows 2000 para PPTP](#)

A seção abaixo mostra os passos para configurar o cliente do Windows 2000 para PPTP:

1. No menu **Start**, selecione **Settings** e então: **Control Panel** e **Network and Dial-up Connections** ou **Network and Dial-up Connections** e **Make New Connection**. Use o Wizard para criar uma conexão chamada **PPTP**. Essa conexão conecta a uma rede privada através da Internet. Você também precisa especificar o endereço IP ou o nome do Servidor de Rede PPTP (PNS, PPTP Network Server).
2. A nova conexão aparece na janela **Network and Dial-up Connections no Control Panel**. Então clique com o botão direito do mouse para editar suas propriedades. Na guia **Networking**, verifique se o campo **Type of Server I Am Calling** está configurado como **PPTP**. Se você pretende atribuir um endereço interno dinâmico a esse cliente a partir do gateway através de um conjunto local ou de um Dynamic Host Configuration Protocol (DHCP), selecione **TCP/IP protocol** e certifique-se de que o cliente esteja configurado para obter um endereço IP automaticamente. Você também pode enviar informações do DNS automaticamente. O botão **Advanced** permite que você defina informações estáticas do Serviço de Cadastramento na Internet do Windows (WINS, Windows Internet Naming Service) e do DNS. A guia **Options** permite que você desative o IPsec ou atribua uma política diferente à conexão.
3. Na guia **Security**, você pode definir os parâmetros de autenticação de usuário. Por exemplo, PAP, CHAP ou MS-CHAP, ou login de domínio do Windows. Depois que a conexão for configurada, você pode clicar duas vezes nela para exibir a tela de login e então fazer a conexão.

[Configurações](#)

Usando a configuração de roteador a seguir, o usuário pode conectar-se com o nome de usuário **tac** e a senha **admin**, mesmo se o servidor RADIUS não estiver disponível (isso é possível quando o Microsoft IAS ainda não foi configurado). O exemplo de configuração a seguir descreve os comandos necessários para L2tp sem 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: Vil VPDN: Virtual interface
created
*Mar 7 04:21:09.267: Vil VPDN: Clone from Vtemplate 1
*Mar 7 04:21:09.343: Tnl/Cl 29/29 PPTP: VAccess created
*Mar 7 04:21:09.343: Vil Tnl/Cl 29/29 PPTP: vacc-ok ->
#state change wt-vacc to estabd
*Mar 7 04:21:09.343: Vil 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: Vil PPP: Using set call direction
*Mar 7 04:21:09.347: Vil PPP: Treating connection as a
callin
*Mar 7 04:21:09.347: Vil PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load]
*Mar 7 04:21:09.347: Vil 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: Vil LCP: TIMEout: State Listen
*Mar 7 04:21:11.347: Vil AAA/AUTHOR/FSM: (0): LCP
succeeds trivially
*Mar 7 04:21:11.347: Vil LCP: O CONFREQ [Listen] id 7
len 15
*Mar 7 04:21:11.347: Vil LCP:      AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:11.347: Vil LCP:      MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:11.635: Vil LCP: I CONFACK [REQsent] id 7
len 15
*Mar 7 04:21:11.635: Vil LCP:      AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:11.635: Vil LCP:      MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.327: Vil LCP: I CONFREQ [ACKrcvd] id 1
len 44
*Mar 7 04:21:13.327: Vil LCP:      MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.327: Vil LCP:      PFC (0x0702)
*Mar 7 04:21:13.327: Vil LCP:      ACFC (0x0802)
*Mar 7 04:21:13.327: Vil LCP:      Callback 6 (0x0D0306)
*Mar 7 04:21:13.327: Vil LCP:      MRRU 1614 (0x1104064E)
*Mar 7 04:21:13.327: Vil LCP:      EndpointDisc 1 Local
*Mar 7 04:21:13.327: Vil LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar 7 04:21:13.331: Vil LCP:      (0xB9182600000008)
*Mar 7 04:21:13.331: Vil LCP: O CONFREQ [ACKrcvd] id 1
len 34
*Mar 7 04:21:13.331: Vil LCP:      Callback 6 (0x0D0306)
*Mar 7 04:21:13.331: Vil LCP:      MRRU 1614 (0x1104064E)
*Mar 7 04:21:13.331: Vil LCP:      EndpointDisc 1 Local
*Mar 7 04:21:13.331: Vil LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar 7 04:21:13.331: Vil LCP:      (0xB9182600000008)
*Mar 7 04:21:13.347: Vil LCP: TIMEout: State ACKrcvd
*Mar 7 04:21:13.347: Vil LCP: O CONFREQ [ACKrcvd] id 8
len 15
*Mar 7 04:21:13.347: Vil LCP:      AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:13.347: Vil LCP:      MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.647: Vil LCP: I CONFREQ [REQsent] id 2
```

```
len 14
*Mar 7 04:21:13.651: Vil LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.651: Vil LCP: PFC (0x0702)
*Mar 7 04:21:13.651: Vil LCP: ACFC (0x0802)
*Mar 7 04:21:13.651: Vil LCP: O CONFACK [REQsent] id 2
len 14
*Mar 7 04:21:13.651: Vil LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.651: Vil LCP: PFC (0x0702)
*Mar 7 04:21:13.651: Vil LCP: ACFC (0x0802)
*Mar 7 04:21:13.723: Vil LCP: I CONFACK [ACKsent] id 8
len 15
*Mar 7 04:21:13.723: Vil LCP: AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:13.723: Vil LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.723: Vil LCP: State is Open
*Mar 7 04:21:13.723: Vil PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load]
*Mar 7 04:21:13.723: Vil MS-CHAP: O CHALLENGE id 20 len
21 from "angela "
*Mar 7 04:21:14.035: Vil LCP: I IDENTIFY [Open] id 3
len 18 magic
0x35BE1CB0 MSRASV5.00
*Mar 7 04:21:14.099: Vil LCP: I IDENTIFY [Open] id 4
len 24 magic
0x35BE1CB0 MSRAS-1-RSHANMUG
*Mar 7 04:21:14.223: Vil 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=lv101~11a1W11151\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=1v101~11a1W11151\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=1v101~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar 7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Authorization
```

```
succeeded
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar 7 04:21:14.607: Vil IPCP: Pool returned
172.16.10.1
*Mar 7 04:21:14.607: Vil IPCP: O CONFREJ [REQsent] id 6
len 28
*Mar 7 04:21:14.607: Vil IPCP: PrimaryDNS 0.0.0.0
(0x810600000000)
*Mar 7 04:21:14.611: Vil IPCP: PrimaryWINS 0.0.0.0
(0x820600000000)
*Mar 7 04:21:14.611: Vil IPCP: SecondaryDNS 0.0.0.0
(0x830600000000)
*Mar 7 04:21:14.611: Vil IPCP: SecondaryWINS 0.0.0.0
(0x840600000000)
*Mar 7 04:21:14.675: Vil IPCP: I CONFACK [REQsent] id 4
len 10
*Mar 7 04:21:14.675: Vil IPCP: Address 172.16.10.100
(0x0306AC100A64)
*Mar 7 04:21:14.731: Vil CCP: I CONFACK [REQsent] id 3
len 10
*Mar 7 04:21:14.731: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.939: Vil CCP: I CONFREQ [ACKrcvd] id 7
len 10
*Mar 7 04:21:14.939: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM: Processing AV
service=ppp
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM: Succeeded
*Mar 7 04:21:14.939: Vil CCP: O CONFACK [ACKrcvd] id 7
len 10
*Mar 7 04:21:14.939: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.943: Vil CCP: State is Open
*Mar 7 04:21:14.943: Vil MPPE: Generate keys using
RADIUS data
*Mar 7 04:21:14.943: Vil MPPE: Initialize keys
*Mar 7 04:21:14.943: Vil MPPE: [40 bit encryption]
[stateless mode]
*Mar 7 04:21:14.991: Vil IPCP: I CONFREQ [ACKrcvd] id 8
len 10
*Mar 7 04:21:14.991: Vil IPCP: Address 0.0.0.0
(0x030600000000)
*Mar 7 04:21:14.991: Vil AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar 7 04:21:14.991: Vil AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar 7 04:21:14.995: Vil AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar 7 04:21:14.995: Vil AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar 7 04:21:14.995: Vil AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar 7 04:21:14.995: Vil 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=1v101~11a1W11151\1V1M1#11Z1`1kl}
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: Vil LCP: I ECHOREP [Open] id 10
len 12 magic 0x35BE1CB0
*Mar  7 04:23:09.887: Vil LCP: Received id 10, sent id
10, line up
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

Determinados comandos show são suportados pela Ferramenta Output Interpreter, que permite que você veja uma análise do resultado do comando show.

- **show vpdn** - Exibe informações sobre os túneis do Level 2 Forwarding (L2F) Protocol ativo e identificadores de mensagem em uma VPDN.

Você também pode usar **show vpdn ?** para ver outros comandos **show** específicos para VPDN.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Determinados comandos show são suportados pela Ferramenta Output Interpreter, que permite que você veja uma análise do resultado do comando show.

Observação: antes de emitir comandos **debug**, consulte [Informações importantes sobre comandos debug](#).

- **debug aaa authentication** - Exibe informações sobre a autenticação AAA/TACACS+.
- **debug aaa authorization** - Exibe informações sobre a autorização AAA/TACACS+.
- **debug ppp negotiation** - Exibe pacotes PPP transmitidos durante a inicialização de PPP, em

que as opções de PPP são negociadas.

- **debug ppp authentication** Exibe mensagens de protocolo de autenticação, incluindo intercâmbios de pacote de Protocolo de Autenticação de Desafio (CHAP) e intercâmbios de Protocolo de Autenticação de Senha (PAP).
- **debug radius** - Exibe informações detalhadas de depuração associadas ao RADIUS. Se a autenticação funcionar, mas houver problemas com a criptografia MPPE, use um dos comandos de depuração.
- **debug ppp mppe packet** - Exibe todo o tráfego MPPE de entrada e de saída.
- **debug ppp mppe event** - Exibe as principais ocorrências de MPPE.
- **debug ppp mppe detailed** - Exibe informações detalhadas de MPPE.
- **debug vpdn l2x-packets** - Exibe mensagens sobre os cabeçalhos e de protocolo e o status de L2F.
- **debug vpdn events** - Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal de túnel.
- **debug vpdn errors** - Exibe erros que impedem que um túnel seja estabelecido ou erros que fazem com que o túnel estabelecido seja fechado.
- **debug vpdn packets** - Exibe cada pacote de protocolo trocado. Essa opção pode resultar em um grande número de mensagens de depuração e normalmente deve ser usada somente em um chassi de depuração com uma única sessão ativa.

Encapsulamento dividido

Suponhamos que o roteador gateway seja um roteador ISP. Quando o túnel PPTP é ativado no PC, a rota PPTP é instalada com uma métrica maior do que o padrão anterior, então a conectividade com a Internet é perdida. Para resolver o problema, modifique o roteamento da Microsoft para excluir o padrão e reinstalar a rota padrão (para isso, é necessário saber o endereço IP atribuído ao cliente PPTP; no exemplo atual, é 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 o cliente não está configurado para criptografia

Na guia **Security** na conexão dial-up usada para a sessão PPTP, você pode definir os parâmetros de autenticação do usuário. Por exemplo, podem ser PAP, CHAP, MS-CHAP, ou login de domínio do Windows. Se você escolheu a opção **No Encryption Allowed** (o servidor desconecta se precisar de criptografia) na seção **Properties** da conexão VPN, uma mensagem de erro PPTP poderá ser exibida no cliente:

```
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 o cliente estiver configurado para criptografia e o roteador não estiver](#)

A seguinte mensagem é exibida no PC:

Registering your computer on the network..

Error 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=lv1O1~11a1W11151\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

```

[Desativando o MS-CHAP quando o PC é configurado para criptografia](#)

A seguinte mensagem é exibida no PC:

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

Se o usuário especificar um nome de usuário ou uma senha incorretos, veremos a seguinte saída.

No PC:

Verifying Username and Password..

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

No roteador:

```
*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 o servidor Radius não estiver comunicativo](#)

Podemos ver a seguinte saída no roteador:

```
*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
```

[Informações Relacionadas](#)

- [PPTP com MPPE](#)
- [Página Tecnologia de PPTP](#)
- [Entendendo o VPDN](#)
- [Entendendo o RADIUS](#)
- [Configurando o CiscoSecure ACS para a autenticação PPTP do roteador Windows](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)