Configuración de clientes del software IOS de Cisco y Windows 2000 para PPTP por medio de Microsoft IAS

Contenido

Introducción

El soporte del Point-to-Point Tunnel Protocol (PPTP) fue agregado a la versión 12.0.5.XE5 del Cisco IOS ® Software en las Plataformas del Cisco 7100 y 7200 Router. El soporte de más plataformas se agregó en Cisco IOS Software Release 12.1.5.T.

La Solicitud de comentarios (RFC) 2637 describe el PPTP. Según este RFC, el PPTP Access Concentrator (PAC) es el cliente (es decir, el PC o el llamador) y el PPTP Network Server (PNS) es el servidor (es decir, el router o el dispositivo que es llamado).

prerrequisitos

Requisitos

Este documento asume que usted ha configurado las conexiones PPTP al router con la autenticación local V1 del protocolo microsoft-challenge handshake authentication (MS-CHAP) (y opcionalmente el [MPPE] del Microsoft Point-to-Point Encryption que requiere MS-CHAP V1) usando estos documentos, y que él está trabajando ya. El Remote Authentication Dial-In User Service (RADIUS) se requiere para el soporte de encripción de MPPE; El TACACS+ trabaja para la autenticación, pero no para la codificación MPPE.

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- El componente opcional del Microsoft IAS instaló en un Advanced Server de Microsoft 2000 con el Active Directory.
- Un Cisco 3600 Router.
- C3640-io3s56i-mz.121-5.T de la versión de Cisco IOS Software.

Esta configuración utiliza el Microsoft IAS instalado en un Advanced Server del Windows 2000 como el servidor de RADIUS.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Teoría Precedente

Esta configuración de muestra demuestra cómo configurar un PC para conectar con el router (en el direccionamiento 10.200.20.2), que entonces autentica al usuario al Internet Authentication Server de Microsoft (IAS) (en 10.200.20.245) antes de permitir al usuario en la red. El soporte PPTP está disponible con la versión 2.5 del Cisco Secure Access Control Server (ACS) para Windows. Sin embargo, puede no trabajar con el router debido al Id. de bug Cisco CSCds92266. Si usted está utilizando Cisco seguro, recomendamos usando la versión 2.6 o posterior segura de Cisco. Cisco UNIX seguro no soporta el MPPE. Dos otras aplicaciones de RADIUS con el soporte de MPPC son Microsoft RADIUS y tienen miedo de RADIUS.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento,

use la herramienta IOS Command Lookup

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.

Agrupación IP para los clientes de dial up:

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

Aunque la configuración antedicha utilice a un cliente de dial up para conectar con el router del Proveedor de servicios de Internet (ISP) vía la terminal de marcado manual, el usted puede conectarse el PC y el router de gateway vía cualquier media, tal como un LAN.

Configuración de Windows 2000 Advanced Server para Microsoft IAS

Esta sección muestra cómo configurar el Advanced Server del Windows 2000 para el Microsoft IAS:

1. Asegúrese de que el Microsoft IAS esté instalado. Para instalar el Microsoft IAS, inicie sesión como administrador. Bajo **servicios de red**, verifique que todas las casillas de verificación estén borradas. Seleccione la casilla de verificación del Internet Authentication Server y después haga clic la **AUTORIZACIÓN**.
2. En el **Asistente de componentes de Windows**, haga clic **después**. Si está indicado, inserte el CD del Windows 2000.
3. Después de que los archivos necesarios hayan sido clic en Finalizar copiado y entonces cierre todas las ventanas. Usted no necesita reiniciar.

Configuración de clientes Radius

Esta sección muestra los pasos para configurar a los clientes RADIUS:

1. **De las herramientas administrativas**, abra la **consola del servidor de autenticación de Internet** y haga clic en a los **clientes**.
2. En el cuadro del **nombre descriptivo**, teclee la dirección IP del servidor de acceso a la red (NAS).
3. Haga clic en el **uso esta opción IP**.
4. En el cuadro del menú desplegable de **Client Vendedor**, asegúrese de que la opción de la **norma RADIUS** esté seleccionada.
5. En el **secreto compartido** y **confirme los** cuadros del **secreto compartido**, teclee la contraseña y entonces el clic en Finalizar.
6. En el árbol de la consola, haga clic con el botón derecho del ratón en el **Internet Authentication Service**, y después haga clic el **comienzo**.
7. Cierre la consola.

Configuración de usuarios en IAS

A diferencia de Cisco seguro, el Windows 2000 base de datos del usuario RADIUS está limitado

firmemente a la base de datos de usuario de Windows. En caso de que un **Active Directory** esté instalado en su Windows 2000 Server, cree a sus nuevos usuarios de marcación manual de los **usuarios de directorio activo y computadora**. Si el **Active Directory** no está instalado, utilice los **usuarios locales y a los grupos de las herramientas administrativas** para crear a los usuarios nuevos.

Configurar a los usuarios en el Active Directory

Esta sección muestra los pasos para configurar a los usuarios en el Active Directory:

1. En los **usuarios de directorio activo y computadora** consuele, amplíe su dominio. Haga clic con el botón derecho del ratón a los **usuarios**. Navegue para seleccionar al **usuario nuevo**. Cree a un usuario nuevo llamado **tac**.
2. Teclee una contraseña en la **contraseña** y **confirme los cuadros de diálogo de contraseña**.
3. Borre al **usuario debe cambiar la contraseña en el** campo **siguiente del inicio** y hacer clic **después**.
4. Abra el cuadro de las **propiedades tac del usuario**. Switch al **dial-in tab**. Bajo el **Permiso de acceso remoto (dial-in o VPN)**, el tecleo permite el acceso, después hace clic la **AUTORIZACIÓN**.

Configurar a los usuarios si no se instala ningún Active Directory

Esta sección muestra los pasos para configurar a los usuarios si no se instala ningún Active Directory:

1. **De las herramientas administrativas** seccione, haga clic en la **administración de la computadora**. Amplíe la **consola de administración de la computadora** y haga clic en los **usuarios locales y a los grupos**. Haga clic con el botón derecho del ratón en la barra de desplazamiento de los **usuarios** para seleccionar al **usuario nuevo**. Cree a un usuario nuevo llamado **tac**.
2. Teclee una contraseña en la **contraseña** y **confirme los cuadros de diálogo de contraseña**.
3. Borre al **usuario debe cambiar la contraseña en la** opción **siguiente del inicio** y hacer clic **después**.
4. Abra al usuario nuevo llamado el cuadro de las **propiedades tac**. Switch al **dial-in tab**. Bajo el **Permiso de acceso remoto (dial-in o VPN)**, el tecleo **permite el acceso**, después hace clic la **AUTORIZACIÓN**.

Aplicación de política de acceso remoto al usuario de Windows

Esta sección muestra los pasos para aplicar una política de acceso remoto al usuario de Windows:

1. **De las herramientas administrativas**, abra la **consola del servidor de autenticación de Internet** y haga clic en las **políticas de acceso remoto**.
2. Haga clic el **botón Add** en **Specify las condiciones para hacer juego**, y agregue el **tipo de servicio**. Elija el tipo disponible como **Framed** y agreguelo a la lista de los **tipos seleccionados**. Presione **OK**.
3. Haga clic el **botón Add** en **Specify las condiciones para hacer juego** y para agregar el

protocolo entramado. Elija el tipo disponible como **ppp** y agreguelo a la lista de los **tipos seleccionados**. Presione **OK**.

4. Haga clic el **botón Add** en **Specify las condiciones para hacer juego** y agregar a los Windows-**grupos** para agregar al grupo de Windows el usuario pertenece a. Elija al grupo y agreguelo a los **tipos seleccionados** y presione **OK**.
5. En el **acceso de la permit si el permiso de dial in es Enabled Properties**, seleccione el **Grant remote Access permission**.
6. Cierre la consola.

Configuración de Windows 2000 Client para PPTP

La sección abajo muestra los pasos para configurar al cliente del Windows 2000 para el PPTP:

1. Desde el principio menú, **configuraciones** selectas, entonces cualquiera:**Panel de control** y **red y conexiones por línea telefónica**, o**Make New Connection de la red y de las conexiones por línea telefónica** entonces.Utilice al **Asisitente** para crear una conexión llamada **PPTP**. Esta conexión conecta con una red privada a través de Internet. Usted también necesita especificar la dirección IP o el nombre del PPTP Network Server (PNS).
2. La nueva conexión aparece en la ventana de la **red y de las conexiones por línea telefónica** bajo el **panel de control**.De aquí, haga clic en el botón derecho del mouse para editar sus propiedades. Conforme a la **ficha de interconexión de redes**, aseegurese que el campo del **Type of Server I Am Calling** está fijado al PPTP. Si usted planea afectar un aparato a una dirección interna dinámica a este cliente del gateway, vía una agrupación local o el Protocolo de configuración dinámica de host (DHCP), seleccionar el **protocolo TCP/IP**, y aseegurarse configuran al cliente para obtener una dirección IP automáticamente. Usted puede también publicar la información DNS automáticamente.**El botón Advanced** permite que usted defina el Windows Internet Naming Service estático (TRIUNFOS) y la información DNS.La lengueta de las **opciones** permite que usted apague el IPSec o que asigne una diversa directiva a la conexión.
3. Conforme a la **ficha de seguridad**, usted puede definir los parámetros de autenticación de usuario. Por ejemplo, PAP, GRIETA o MS-CHAP, o inicio del Dominio de Windows. Una vez que se configura la conexión, usted puede doblar la hace clic en para visualizar a la pantalla de inicio de sesión y después para conectar.

Configuraciones

Usando la configuración del router siguiente, el usuario puede conectar con nombre de usuario tac y contraseña admin incluso si el servidor de RADIUS es inasequible (esto es posible cuando el Microsoft IAS debe todavía ser configurado). El siguiente ejemplo delinea los comandos required para L2tp sin el 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta del Output Interpreter soportan a los ciertos comandos show, que permite que usted vea una análisis de la salida del comando show.

- **vpdn de la demostración** - Información de las visualizaciones sobre el túnel de protocolo y los identificadores de mensajes activos del Level 2 Forwarding (L2F) en un VPDN.

¿Usted puede también utilizar el **vpdn de la demostración?** para ver otros **comandos show VPDN-** específicos.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta del Output Interpreter soportan a los ciertos comandos show, que permite que usted vea una análisis de la salida del comando show.

Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

- **haga el debug de la autenticación aaa** - Visualiza la información sobre la autenticación AAA/TACACS+.
- **debug aaa authorization** - Visualiza la información sobre la autorización AAA/TACACS+.
- **negociación ppp del debug** - Visualiza los paquetes PPP transmitidos durante el inicio de

PPP, donde se negocian las opciones PPP.

- debug ppp authentication - Muestra los mensajes del protocolo de autenticación, incluidos el intercambio de paquetes del Protocolo de autenticación por desafío mutuo (CHAP) y los intercambios del Protocolo de autenticación de contraseña (PAP).
- debug radius - Muestra información detallada de depuración asociada con el RADIUS. Si la autenticación trabaja, pero hay problemas con la encripción MPPE, utilice uno de los comandos debug abajo.
- debug ppp mppe packet - Muestra todo el tráfico MPPE entrante y saliente.
- **debug ppp mppe event** - Acontecimientos dominantes de las visualizaciones MPPE.
- debug ppp mppe detailed - Muestra información de MPPE verboso.
- **debug vpdn l2x-packets** - Mensajes de las visualizaciones sobre las encabezados y el estatus de protocolo L2F.
- debug vpdn events - Muestra mensajes acerca de eventos que forman parte del cierre normal o del establecimiento del túnel.
- debug vpdn errors - Muestra errores que evitan que se establezca un túnel o errores que provocan que un túnel establecido se cierre.
- debug vpdn packets - Muestra cada paquete de protocolo intercambiado. Esta opción puede resultar en un gran número de mensajes de depuración y, generalmente, debería utilizarse sólo con un chasis de depuración con una sola sesión activa.

Tunelización dividida

Asumamos al router de gateway es un router del ISP. Cuando el túnel PPTP sube en el PC, la ruta PPTP está instalada con un métrico más alto que el valor por defecto anterior, así que perdemos la conectividad a Internet. Para remediar esto, modificar el Microsoft Routing para borrar el valor por defecto y reinstalar la ruta predeterminado (esto requiere saber que se haya asignado la dirección IP el cliente PPTP; para el ejemplo actual, éste era 172.16.10.1):

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

Si el cliente no está configurado para encripción

Conforme a la **ficha de seguridad** en la conexión por línea telefónica usada para la sesión PPTP, usted puede definir los parámetros de autenticación de usuario. Por ejemplo, éste puede ser PAP, GRIETA, MS-CHAP, o inicio del Dominio de Windows. Si usted ha elegido el **no encryption no prohibido** (las desconexiones del servidor si requiere el cifrado) la opción en la sección de **propiedades de la** conexión VPN, usted puede ver un mensaje de error PPTP en el 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
```

Si el cliente está configurado para encripción y el router no

Podemos ver el siguiente mensaje en el PC:

```
Registering your computer on the network..
Errror 742: The remote computer doesnot support the required data
encryption type.
On the Router:
*Mar  9 01:06:00.868: Vi2 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar  9 01:06:00.868: Vi2 CCP:    MS-PPC supported bits 0x010000B1
(0x1206010000B1)
*Mar  9 01:06:00.868: Vi2 LCP: O PROTREJ [Open] id 18 len 16 protocol CCP
(0x80FD0105000A1206010000B1)
*Mar  9 01:06:00.876: Vi2 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar  9 01:06:00.876: Vi2 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV service=ppp
```

```
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#1
1Z1`1k1}111
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 IPCP: Pool returned 172.16.10.1
*Mar  9 01:06:00.880: Vi2 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.884: Vi2 IPCP: I CONFACK [REQsent] id 8 len 10
*Mar  9 01:06:00.884: Vi2 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  9 01:06:01.024: Vi2 LCP: I TERMREQ [Open] id 7 len 16
(0x79127FBE003CCD74000002E6)
*Mar  9 01:06:01.024: Vi2 LCP: O TERMACK [Open] id 7 len 4
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: ClearReq -> state change
estabd to terminal
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: Destroying session, trace
follows:
*Mar  9 01:06:01.152: -Traceback= 60C4A150 60C4AE48 60C49F68 60C4B2CC
60C4B558 60C485E0 60C486E0 60C48AB8 6040DE0C 6040DDF8
*Mar  9 01:06:01.156: Vi2 Tnl/Cl 38/38 PPTP: Releasing idb for tunnel 38
session 38
*Mar  9 01:06:01.156: Vi2 VPDN: Reset
*Mar  9 01:06:01.156: Tnl 38 PPTP: no-sess -> state change estabd to
wt-stprp
*Mar  9 01:06:01.160: %LINK-3-UPDOWN: Interface Virtual-Access2, changed
state to down
*Mar  9 01:06:01.160: Vi2 LCP: State is Closed
*Mar  9 01:06:01.160: Vi2 IPCP: State is Closed
*Mar  9 01:06:01.160: Vi2 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  9 01:06:01.160: Vi2 VPDN: Cleanup
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: AAA/MEMORY: free_user (0x6273D528) user='tac' ruser=''
port='Virtual-Access2' rem_addr='' authen_type=MSCHAP service=PPP priv=1
*Mar  9 01:06:01.324: Tnl 38 PPTP: StopCCRQ -> state change wt-stprp to wt-stprp
*Mar  9 01:06:01.324: Tnl 38 PPTP: Destroy tunnel
*Mar  9 01:06:02.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to down
```

Desactivación de MS-CHAP cuando la PC está configurada para encripción

Podemos ver el siguiente mensaje en el PC:

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

Si el usuario especifica un nombre de usuario incorrecto o una contraseña, podemos ver el producto siguiente.

En el PC:

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

En el 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
```

Cuando el Servidor Radius no establece comunicación

Podemos ver el producto siguiente en el router:

```
*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
```

Información Relacionada

- PPTP con MPPE
- Página de tecnología PPTP
- Introducción a VPDN'
- Comprensión del radio
- Configuración de CiscoSecure ACS para la autenticación PPTP de router de Windows
- Soporte Técnico y Documentación - Cisco Systems