

Configuración de CiscoSecure ACS para la autenticación PPTP de router de Windows

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configuración del router](#)

[Función RADIUS Server Fallback](#)

[Configuración de Cisco Secure ACS para Windows](#)

[Agregar a la configuración](#)

[Adición de cifrado](#)

[Asignación de dirección IP estática desde el servidor](#)

[Agregar listas de acceso al servidor](#)

[Agregar contabilidad](#)

[Tunelización dividida](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Ejemplo de Salida de debug Correcta](#)

[Información Relacionada](#)

[Introducción](#)

El soporte de Point-to-Point Tunnel Protocol (PPTP) se agregó a Cisco IOS® Software Release 12.0.5.XE5 en las plataformas Cisco 7100 y 7200 (consulte el PPTP sobre Microsoft Point-to-Point Encryption (MPPE) [Cisco IOS Software Release 12.0]). El soporte para más plataformas se agregó en Cisco IOS Software Release 12.1.5.T (consulte MSCHAP Version 2).

[RFC 2637](#) describe PPTP. En términos PPTP, de acuerdo con el RFC, el PPTP Access Concentrator (PAC) es el cliente (la PC, es decir el caller) y el PPTP Network Server (PNS) es el servidor(el router, el callee).

Este documento asume que las conexiones PPTP al router con autenticación V1 del protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP) local (y opcionalmente MPPE, que requiere MS-CHAP V1) se han creado con el uso de estos documentos y ya están operativas. RADIUS es necesario para el soporte de cifrado MPPE. TACACS+ funciona para la autenticación, pero no para la codificación MPPE. El soporte MS-CHAP V2 se agregó a Cisco IOS Software Release 12.2(2)XB5 y se integró en Cisco IOS Software Release 12.2(13)T (consulte [MSCHAP](#)

[Version 2](#)); sin embargo, MPPE no se soporta con MS-CHAP V2 hasta ahora.

Esta configuración de ejemplo muestra cómo configurar una conexión de PC al router (en 10.66.79.99), que luego proporciona autenticación de usuario al Cisco Secure Access Control System (ACS) 4.2 para el servidor Windows (en 10.66.79.120), antes de permitir que el usuario entre en la red.

Nota: El servidor RADIUS no suele estar fuera del router excepto en un entorno de laboratorio.

El soporte PPTP se agregó a Cisco Secure ACS 2.5, pero es posible que no funcione con el router debido al Id. de error de Cisco [CSCds92266 \(sólo clientes registrados\)](#). ACS 2.6 y posteriores no tienen este problema.

Cisco Secure UNIX no admite MPPE. Otras dos aplicaciones RADIUS con soporte MPPE incluyen Microsoft RADIUS y Funk RADIUS.

Consulte [Configuración del Router Cisco y de los Clientes VPN Usando PPTP y MPPE](#) para obtener más información sobre cómo configurar PPTP y MPPE con un router.

Refiérase a [Configuración del Concentrador VPN 3000 y PPTP con Cisco Secure ACS para la Autenticación RADIUS de Windows](#) para obtener más información sobre cómo configurar PPTP en un Concentrador VPN 3000 con Cisco Secure ACS para Windows para la autenticación RADIUS.

Consulte [PIX 6.x: Ejemplo de Configuración de PPTP con Autenticación Radius](#) para configurar conexiones PPTP al PIX.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

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

- Cisco Secure ACS 4.2 para Windows
- Cisco 3600 router
- Versión 12.4(3) del software Cisco IOS

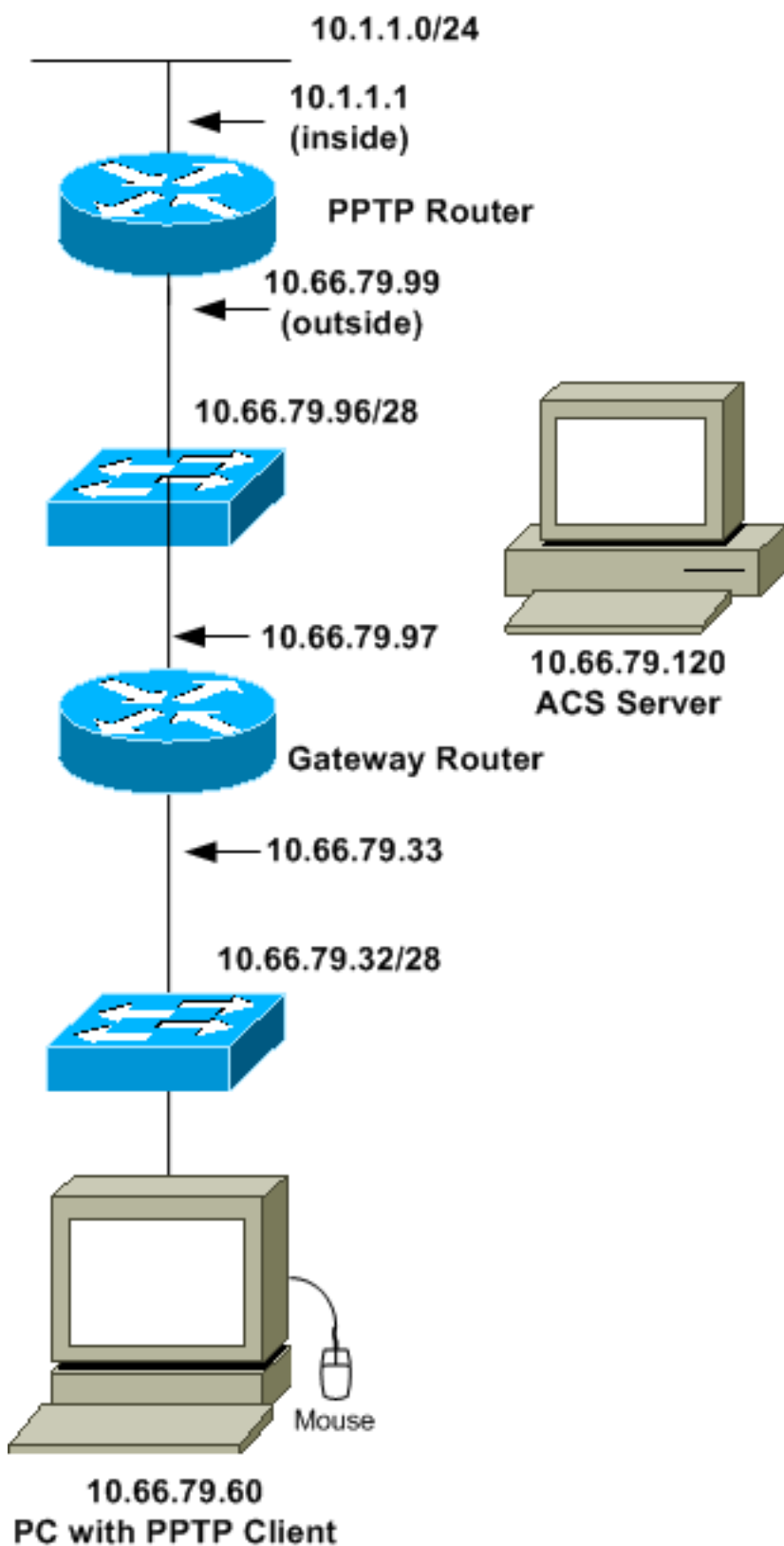
La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si se encuentra en una red activa, asegúrese de comprender el impacto potencial de cualquier comando antes de utilizarlo.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración del router

Utilice esta configuración del router. El usuario debería poder conectarse con "username john password doe" incluso si el servidor RADIUS es inalcanzable (lo que es posible si el servidor aún

no se ha configurado con Cisco Secure ACS). Este ejemplo supone que la autenticación local (y, opcionalmente, el cifrado) ya está operativa.

Cisco 3600 Router

```
Current configuration : 1729 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname moss
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username john password 0 doe
aaa new-model
!
aaa authentication ppp default group radius local
aaa authentication login default local
!
!--- In order to set authentication, authorization, and
accounting (AAA) authentication !--- at login, use the
aaa authentication login command in global !---
configuration mode as shown above.
!
aaa authorization network default group radius if-
authenticated
aaa session-id common
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
vpdn-group 1
!--- Default PPTP VPDN group. accept-dialin
protocol pptp
virtual-template 1
!
no ftp-server write-enable
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
!
interface Ethernet0/1
ip address 10.66.79.99 255.255.255.224
half-duplex
!
interface Virtual-Template1
ip unnumbered Ethernet0/1
```

```
peer default ip address pool testpool
ppp authentication ms-chap
!
ip local pool testpool 192.168.1.1 192.168.1.254
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
radius-server host 10.66.79.120 auth-port 1645 acct-port
1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
line aux 0
line vty 0 4
password cisco
!
end
```

[Función RADIUS Server Fallback](#)

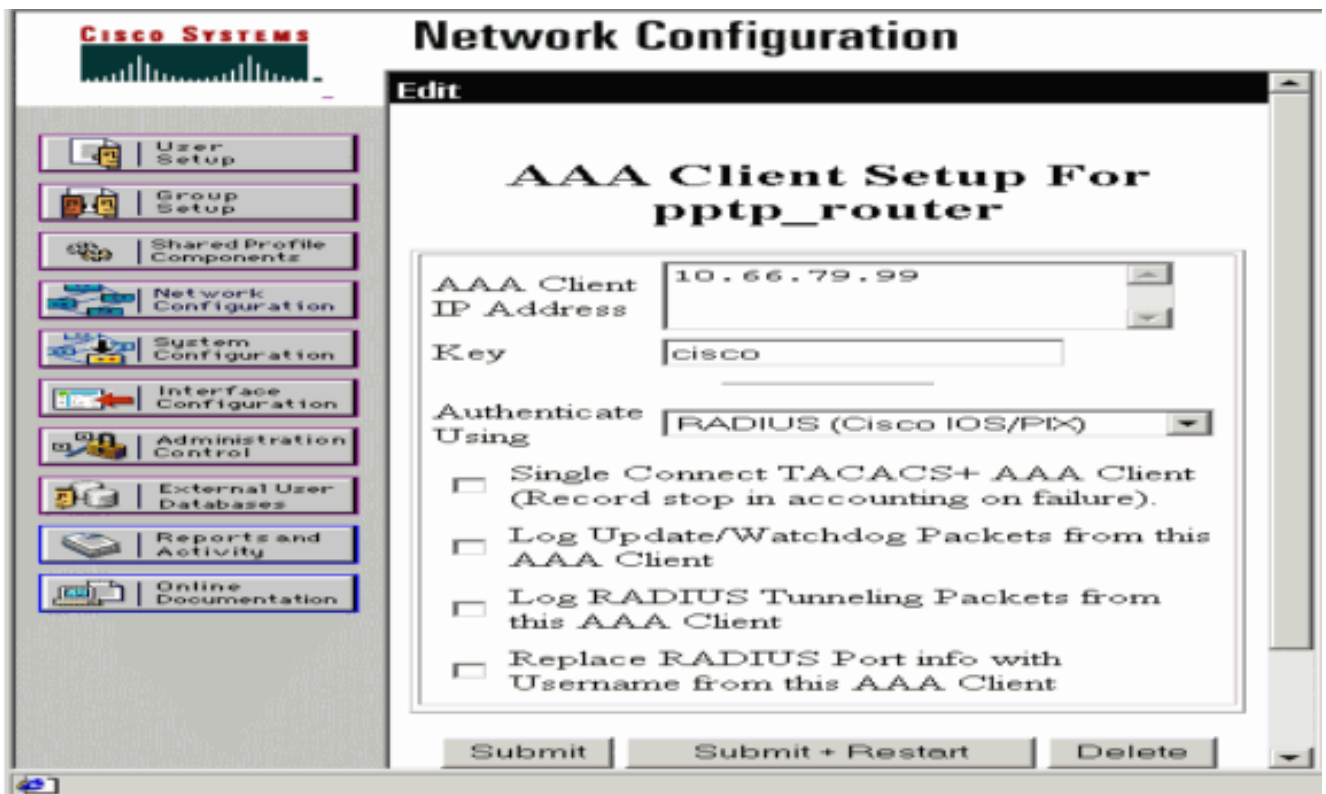
Cuando el servidor RADIUS primario deja de estar disponible, el router conmutará por error al siguiente servidor RADIUS de respaldo activo. El router continuará utilizando el servidor RADIUS secundario para siempre incluso si el servidor primario está disponible. Por lo general, el servidor principal es de alto rendimiento y el servidor preferido.

Para configurar la autenticación de autenticación, autorización y contabilidad (AAA) al iniciar sesión, utilice el comando [aaa authentication login](#) en el modo de configuración global.

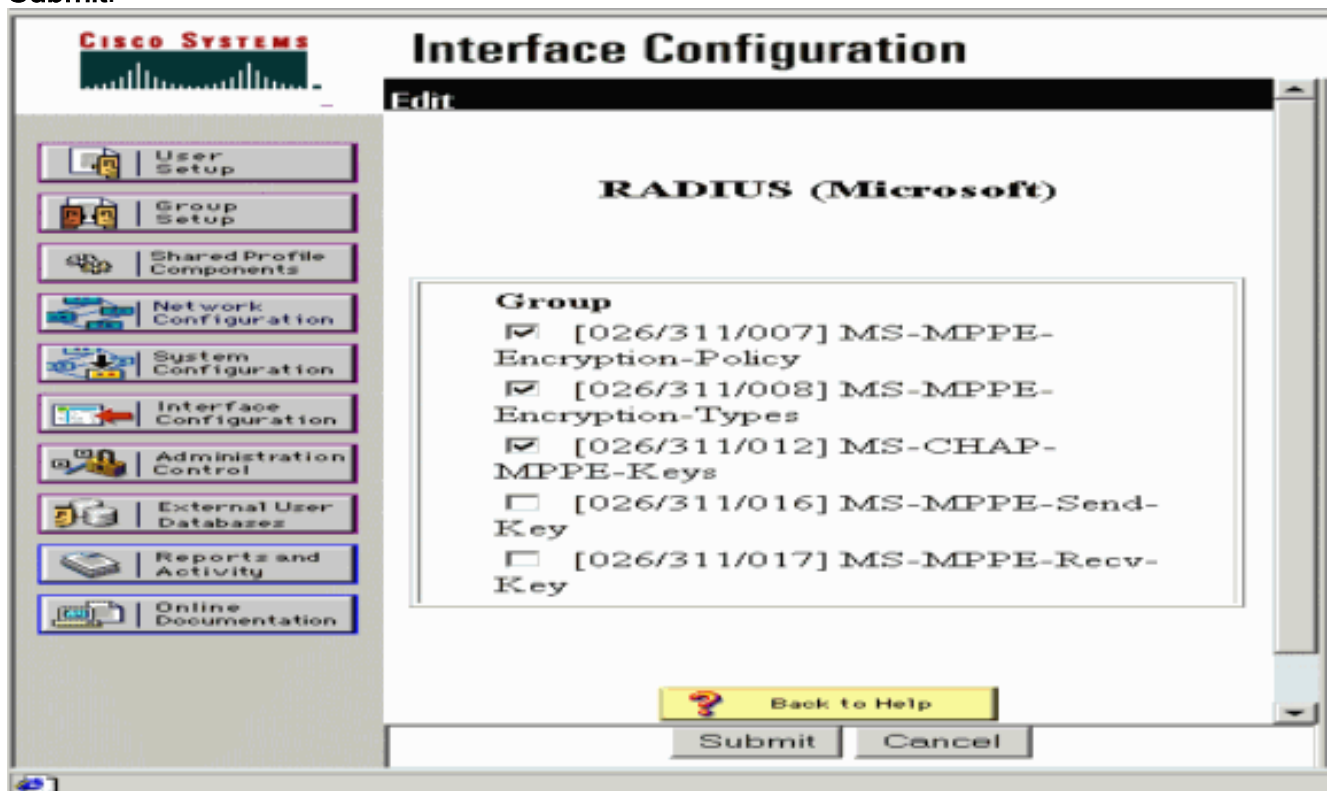
[Configuración de Cisco Secure ACS para Windows](#)

Utilice este procedimiento para configurar Cisco Secure ACS:

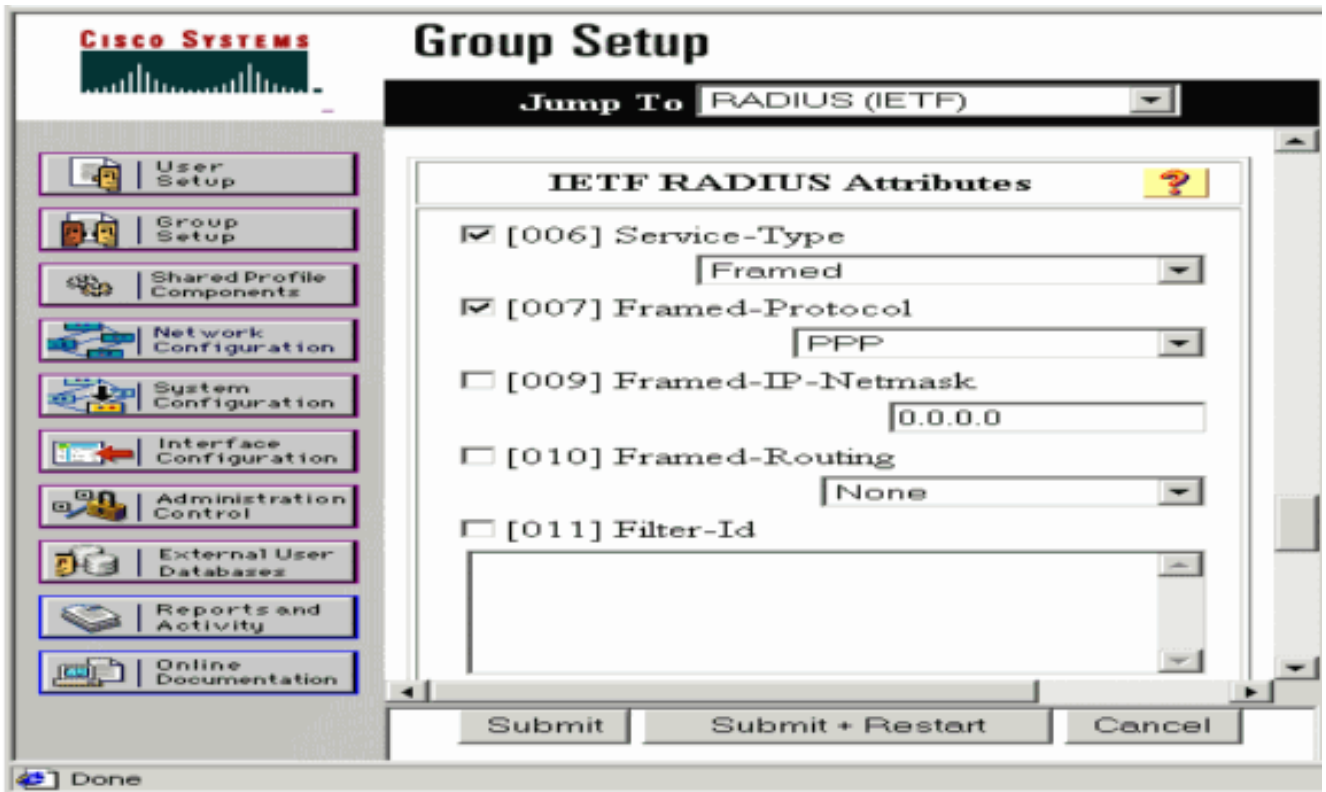
1. Haga clic en **Configuración de red**, agregue una entrada para el router y haga clic en **Enviar + Reiniciar** cuando termine.



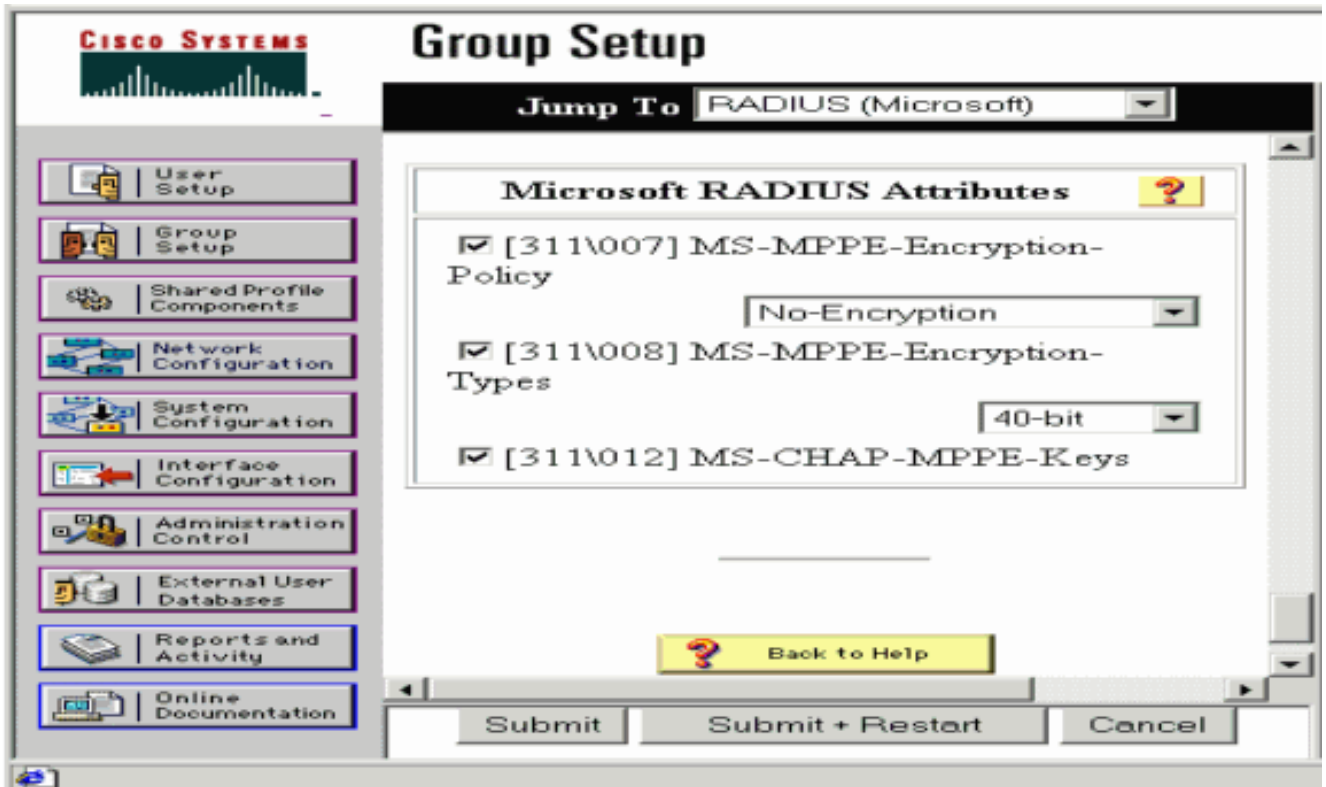
2. Seleccione **Interface Configuration > RADIUS (Microsoft)**, luego verifique sus atributos MPPE y haga clic en **Submit**.



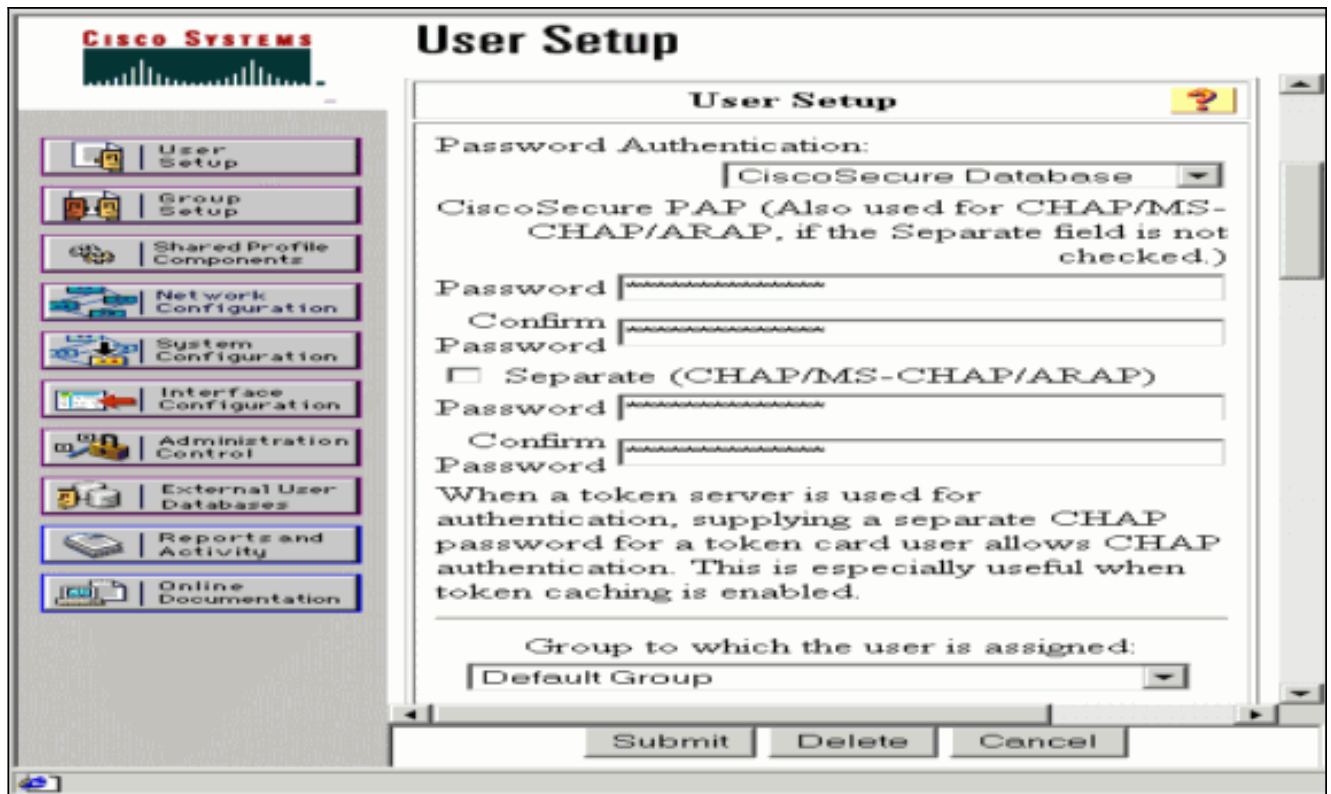
3. Haga clic en **Group Setup** y, para Service-Type, seleccione **Framed**. Para el protocolo entrado, seleccione **PPP** y haga clic en **Enviar**.



4. En **Group Setup**, verifique la información RADIUS de MS-MPPE y, cuando haya terminado, haga clic en **Submit + Restart**.



5. Haga clic en **User Setup**, agregue una contraseña, asigne el usuario al grupo y haga clic en **Submit**.



6. Pruebe la autenticación al router antes de agregar el cifrado. Si la autenticación no funciona, vea la sección [Solución de problemas](#) de este documento.

[Agregar a la configuración](#)

[Adición de cifrado](#)

Puede agregar cifrado MPPE con este comando:

```
interface virtual-template 1
(config-if)#ppp encrypt mppe 40|128|auto passive|required|stateful
```

Dado que el ejemplo supone que el cifrado funciona con la autenticación local (nombre de usuario y contraseña en el router), el PC se configura correctamente. Ahora puede agregar este comando para permitir la máxima flexibilidad:

```
ppp encrypt mppe auto
```

[Asignación de dirección IP estática desde el servidor](#)

Si necesita asignar una dirección IP específica al usuario, en ACS User Setup, seleccione **Assign static IP Address** (Asignar dirección IP estática) y rellene la dirección IP.

[Agregar listas de acceso al servidor](#)

Para controlar a qué puede acceder el usuario PPTP una vez que el usuario está conectado al

router, puede configurar una lista de acceso en el router. Por ejemplo, si ejecuta este comando:

```
access-list 101 permit ip any host 10.1.1.2 log
```

y elija **Filter-Id (atributo 11)** en ACS y escriba **101** en el cuadro, el usuario PPTP puede acceder al host 10.1.1.2 pero no a otros. Cuando ejecuta un comando **show ip interface virtual-access x**, donde x es un número que puede determinar desde un comando *show user*, la lista de acceso debe mostrarse como se aplica:

```
Inbound access list is 101
```

[Agregar contabilidad](#)

Puede agregar contabilidad para las sesiones con este comando:

```
aaa accounting network default start-stop radius
```

Los registros contables en Cisco Secure ACS aparecen como muestra este resultado:

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,
Acct-Status-Type,Acct-Session-Id,Acct-Session-Time,
Service-Type,Framed-Protocol,Acct-Input-Octets,
Acct-Output-Octets,Acct-Input-Packets,Acct-Output-Packets,
Framed-IP-Address,NAS-Port,NAS-IP-Address
09/28/2003,20:58:37,georgia,Default Group,,Start,00000005,,
Framed,PPP,,,,,5,10.66.79.99
09/28/2000,21:00:38,georgia,Default Group,,Stop,00000005,121,
Framed,PPP,3696,1562,49,
38,192.168.1.1,5,10.66.79.99
```

Nota: Los saltos de línea se agregaron al ejemplo con fines de visualización. Los saltos de línea en la salida real son diferentes de los que se muestran aquí.

[Tunelización dividida](#)

Cuando se activa el túnel PPTP en el PC, el router PPTP se instala con una métrica más alta que la predeterminada anterior, por lo que se pierde la conectividad a Internet. Para remediar esto, dado que la red dentro del router es 10.1.1.X, ejecute un archivo por lotes (batch.bat) para modificar el ruteo de Microsoft para eliminar el valor predeterminado y reinstalar la ruta predeterminada (esto requiere la dirección IP que se asigna al cliente PPTP; por ejemplo, es 192.168.1.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 10.66.79.33 metric 1
route add 10.1.1.0 mask 255.255.255.0 192.168.1.1 metric 1
```

[Verificación](#)

En esta sección encontrará información que puede utilizar para comprobar que su configuración

funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show vpdn session:** muestra información sobre el túnel de protocolo de reenvío de nivel 2 activo (L2F) y los identificadores de mensaje en una red de marcado privado virtual (VPDN).

```
moss#show vpdn session
%No active L2TP tunnels
%No active L2F tunnels
```

```
PPTP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf Username State Last Chg Uniq ID
7 32768 7 Vi3 georgia estabd 00:00:25 6
```

```
moss#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 VPDN Group
7 estabd 10.66.79.60 3454 1 1
```

```
LocID RemID TunID Intf Username State Last Chg Uniq ID
7 32768 7 Vi3 georgia estabd 00:00:51 6
```

Troubleshoot

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

1. **El PC especifica el cifrado, pero el router no.** El usuario del PC verá:
The remote computer does not support the required data encryption type.
2. **Tanto el PC como el router especifican el cifrado, pero el servidor RADIUS no está configurado para enviar las claves MPPE (normalmente aparecen como atributo 26).** El usuario del PC verá:
The remote computer does not support the required data encryption type.
3. **El router especifica el cifrado (obligatorio), pero el PC no (no permitido).** El usuario del PC verá:
The specified port is not connected.
4. **El usuario ingresa el nombre de usuario o la contraseña incorrectos.** El usuario del PC verá:
Access was denied because the username and/or password was invalid on the domain.

El debug del router muestra: Nota: Los saltos de línea se agregaron a este ejemplo con fines de visualización. Los saltos de línea en la salida real son diferentes de los que se muestran aquí.

```
Sep 28 21:34:16.299: RADIUS: Received from id 21645/13 10.66.79.120:1645,
Access-Reject, len 54
Sep 28 21:34:16.299: RADIUS: authenticator 37 BA 2B 4F 23 02 44 4D - D4
A0 41 3B 61 2D 5E 0C
Sep 28 21:34:16.299: RADIUS: Vendor, Microsoft [26] 22
Sep 28 21:34:16.299: RADIUS: MS-CHAP-ERROR [2] 16
Sep 28 21:34:16.299: RADIUS: 01 45 3D 36 39 31 20 52 3D 30 20 56 3D
[?E=691 R=0 V=]
Sep 28 21:34:16.299: RADIUS: Reply-Message [18] 12
```

```
Sep 28 21:34:16.299: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D  
[Rejected??]
```

5. El servidor RADIUS no se comunica. El usuario del PC verá:

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

El **debug** del router muestra: **Nota:** Los saltos de línea se agregaron a este ejemplo con fines de visualización. Los saltos de línea en la salida real son diferentes de los que se muestran aquí.

```
Sep 28 21:46:56.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)  
for id 21645/43  
Sep 28 21:47:01.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)  
for id 21645/43  
Sep 28 21:47:06.135: RADIUS: Retransmit to (10.66.79.120:1645,1646)  
for id 21645/43  
Sep 28 21:47:11.135: RADIUS: No response from (10.66.79.120:1645,1646)  
for id 21645/43  
Sep 28 21:47:11.135: RADIUS/DECODE: parse response no app start; FAIL  
Sep 28 21:47:11.135: RADIUS/DECODE: parse response; FAIL
```

Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

Si las cosas no funcionan, los comandos **debug** mínimos incluyen:

- **debug aaa authentication** — Muestra información sobre autenticación de AAA/TACACS+.
- **debug aaa authorization**—Muestra información sobre la autorización AAA/TACACS+.
- **debug ppp negotiation** — Muestra los paquetes PPP transmitidos durante el inicio PPP, durante el cual se negocian las opciones PPP.
- **debug ppp authentication**: muestra los mensajes del protocolo de autenticación, que incluyen intercambios de paquetes CHAP e intercambios de protocolo de autenticación de contraseña (PAP).
- **debug radius**: muestra información detallada de depuración asociada con el RADIUS.

Si la autenticación funciona, pero hay problemas con el cifrado MPPE, utilice estos comandos:

- **debug ppp mppe packet**—Muestra todo el tráfico MPPE entrante y saliente.
- **debug ppp mppe event**—Muestra las ocurrencias clave de MPPE.
- **debug ppp mppe detailed**—Muestra información detallada de MPPE.
- **debug vpdn l2x-packets**—Muestra mensajes acerca de los encabezados y del estado del protocolo L2F.
- **debug vpdn events**: muestra mensajes sobre eventos que forman parte del establecimiento o cierre normal 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 dar como resultado un gran número de mensajes de depuración, y por lo general debe utilizar este comando sólo en un chasis de depuración con una sola sesión activa.

También puede utilizar estos comandos para solucionar problemas:

- **clear interface virtual-access x** : cierra un túnel especificado y todas las sesiones dentro del túnel.

Ejemplo de Salida de debug Correcta

Esta depuración muestra eventos significativos del RFC:

- **SCCRQ = Start-Control-Connection-Request - message code bytes 9 and 10 = 0001**
- **SCCRP = Inicio-Control-Conexión-Respuesta**
- **OCRQ = Outgoing-Call-Request - bytes de código de mensaje 9 y 10 = 0007**
- **OCRP = Respuesta de llamada saliente**

Nota: Los saltos de línea se agregaron a este ejemplo con fines de visualización. Los saltos de línea en la salida real son diferentes de los que se muestran aquí.

```

mos#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP protocol negotiation debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
VPN:
  L2X control packets debugging is on
Sep 28 21:53:22.403: Tnl 23 PPTP:
I 009C00011A2B3C4D0001000001000000000000010000...
Sep 28 21:53:22.403: Tnl 23 PPTP: I SCCRQ
Sep 28 21:53:22.403: Tnl 23 PPTP: protocol version 100
Sep 28 21:53:22.403: Tnl 23 PPTP: framing caps 1
Sep 28 21:53:22.403: Tnl 23 PPTP: bearer caps 1
Sep 28 21:53:22.403: Tnl 23 PPTP: max channels 0
Sep 28 21:53:22.403: Tnl 23 PPTP: firmware rev 893
Sep 28 21:53:22.403: Tnl 23 PPTP: hostname ""
Sep 28 21:53:22.403: Tnl 23 PPTP: vendor "Microsoft Windows NT"
Sep 28 21:53:22.403: Tnl 23 PPTP: O SCCRP
Sep 28 21:53:22.407: Tnl 23 PPTP: I
00A800011A2B3C4D000700080007C0E0000012C05F5...
Sep 28 21:53:22.407: Tnl 23 PPTP: CC I OCRQ
Sep 28 21:53:22.407: Tnl 23 PPTP: call id 32768
Sep 28 21:53:22.411: Tnl 23 PPTP: serial num 31758
Sep 28 21:53:22.411: Tnl 23 PPTP: min bps 300
Sep 28 21:53:22.411: Tnl 23 PPTP: max bps 100000000
Sep 28 21:53:22.411: Tnl 23 PPTP: bearer type 3
Sep 28 21:53:22.411: Tnl 23 PPTP: framing type 3
Sep 28 21:53:22.411: Tnl 23 PPTP: recv win size 64
Sep 28 21:53:22.411: Tnl 23 PPTP: ppd 0
Sep 28 21:53:22.411: Tnl 23 PPTP: phone num len 0
Sep 28 21:53:22.411: Tnl 23 PPTP: phone num ""
Sep 28 21:53:22.411: AAA/BIND(0000001C): Bind i/f Virtual-Template1
Sep 28 21:53:22.415: Tnl/Sn 23/23 PPTP: CC O OCRP
Sep 28 21:53:22.415: ppp27 PPP: Using vpn set call direction
Sep 28 21:53:22.415: ppp27 PPP: Treating connection as a callin
Sep 28 21:53:22.415: ppp27 PPP: Phase is ESTABLISHING, Passive Open
Sep 28 21:53:22.415: ppp27 LCP: State is Listen
Sep 28 21:53:22.459: Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFF
Sep 28 21:53:22.459: Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.459: ppp27 LCP: I CONFREQ [Listen] id 0 len 44

```

```

Sep 28 21:53:22.459: ppp27 LCP: MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.459: ppp27 LCP: PFC (0x0702)
Sep 28 21:53:22.459: ppp27 LCP: ACFC (0x0802)
Sep 28 21:53:22.459: ppp27 LCP: Callback 6 (0x0D0306)
Sep 28 21:53:22.459: ppp27 LCP: MRRU 1614 (0x1104064E)
Sep 28 21:53:22.459: ppp27 LCP: EndpointDisc 1 Local
Sep 28 21:53:22.459: ppp27 LCP: (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.463: ppp27 LCP: (0x2D0E8100000016)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREQ [Listen] id 1 len 15
Sep 28 21:53:22.463: ppp27 LCP: AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.463: ppp27 LCP: MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.463: ppp27 LCP: O CONFREQ [Listen] id 0 len 11
Sep 28 21:53:22.463: ppp27 LCP: Callback 6 (0x0D0306)
Sep 28 21:53:22.463: ppp27 LCP: MRRU 1614 (0x1104064E)
Sep 28 21:53:22.467: ppp27 LCP: I CONFACK [REQsent] id 1 len 15
Sep 28 21:53:22.467: ppp27 LCP: AuthProto MS-CHAP (0x0305C22380)
Sep 28 21:53:22.467: ppp27 LCP: MagicNumber 0xD0B06B2C (0x0506D0B06B2C)
Sep 28 21:53:22.467: ppp27 LCP: I CONFREQ [ACKrcvd] id 1 len 37
Sep 28 21:53:22.467: ppp27 LCP: MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.467: ppp27 LCP: PFC (0x0702)
Sep 28 21:53:22.467: ppp27 LCP: ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP: EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP: (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP: (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: O CONFACK [ACKrcvd] id 1 len 37
Sep 28 21:53:22.471: ppp27 LCP: MagicNumber 0x377413E2 (0x0506377413E2)
Sep 28 21:53:22.471: ppp27 LCP: PFC (0x0702)
Sep 28 21:53:22.471: ppp27 LCP: ACFC (0x0802)
Sep 28 21:53:22.471: ppp27 LCP: EndpointDisc 1 Local
Sep 28 21:53:22.471: ppp27 LCP: (0x1317010D046656E8C7445895763667BB)
Sep 28 21:53:22.471: ppp27 LCP: (0x2D0E8100000016)
Sep 28 21:53:22.471: ppp27 LCP: State is Open
Sep 28 21:53:22.471: ppp27 PPP: Phase is AUTHENTICATING, by this end
Sep 28 21:53:22.475: ppp27 MS-CHAP: O CHALLENGE id 1 len 21 from "SV3-2 "
Sep 28 21:53:22.475: Tnl 23 PPTP: I
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
Sep 28 21:53:22.475: Tnl/Sn 23/23 PPTP: CC I SLI
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 2 len
18 magic 0x377413E2 MSRASV5.00
Sep 28 21:53:22.479: ppp27 LCP: I IDENTIFY [Open] id 3 len
30 magic 0x377413E2 MSRAS-0-CSCOAPACD12364
Sep 28 21:53:22.479: ppp27 MS-CHAP: I RESPONSE id 1 len 61 from "georgia"
Sep 28 21:53:22.483: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.483: ppp27 PPP: Phase is AUTHENTICATING, Unauthenticated User
Sep 28 21:53:22.483: AAA/AUTHEN/PPP (0000001C): Pick method list 'default'
Sep 28 21:53:22.483: RADIUS: AAA Unsupported [152] 14
Sep 28 21:53:22.483: RADIUS: 55 6E 69 71 2D 53 65 73 73 2D 49 44
[Uniq-Sess-ID]
Sep 28 21:53:22.483: RADIUS(0000001C): Storing nasport 27 in rad_db
Sep 28 21:53:22.483: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.483: RADIUS/ENCODE(0000001C): acct_session_id: 38
Sep 28 21:53:22.487: RADIUS(0000001C): sending
Sep 28 21:53:22.487: RADIUS/ENCODE: Best Local IP-Address 10.66.79.99
for Radius-Server 10.66.79.120
Sep 28 21:53:22.487: RADIUS(0000001C): Send Access-Request to
10.66.79.120:1645 id 21645/44, len 133
Sep 28 21:53:22.487: RADIUS: authenticator 15 8A 3B EE 03 24
0C F0 - 00 00 00 00 00 00 00 00
Sep 28 21:53:22.487: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 28 21:53:22.487: RADIUS: User-Name [1] 9 "georgia"
Sep 28 21:53:22.487: RADIUS: Vendor, Microsoft [26] 16
Sep 28 21:53:22.487: RADIUS: MSCHAP_Challenge [11] 10
Sep 28 21:53:22.487: RADIUS: 15 8A 3B EE 03 24 0C [??;??$?]
Sep 28 21:53:22.487: RADIUS: Vendor, Microsoft [26] 58

```

```

Sep 28 21:53:22.487: RADIUS: MS-CHAP-Response [1] 52 *
Sep 28 21:53:22.487: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 28 21:53:22.487: RADIUS: NAS-Port [5] 6 27
Sep 28 21:53:22.487: RADIUS: Service-Type [6] 6 Framed [2]
Sep 28 21:53:22.491: RADIUS: NAS-IP-Address [4] 6 10.66.79.99
Sep 28 21:53:22.515: RADIUS: Received from id 21645/44 10.66.79.120:1645,
Access-Accept, len 141
Sep 28 21:53:22.515: RADIUS: authenticator ED 3F 8A 08 2D A2 EB 4F - 78
3F 5D 80 58 7B B5 3E
Sep 28 21:53:22.515: RADIUS: Service-Type [6] 6 Framed [2]
Sep 28 21:53:22.515: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 28 21:53:22.515: RADIUS: Filter-Id [11] 8
Sep 28 21:53:22.515: RADIUS: 31 30 31 2E 69 6E [101.in]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft [26] 12
Sep 28 21:53:22.515: RADIUS: MS-MPPE-Enc-Policy [7] 6
Sep 28 21:53:22.515: RADIUS: 00 00 00 [???]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft [26] 12
Sep 28 21:53:22.515: RADIUS: MS-MPPE-Enc-Type [8] 6
Sep 28 21:53:22.515: RADIUS: 00 00 00 [???]
Sep 28 21:53:22.515: RADIUS: Vendor, Microsoft [26] 40
Sep 28 21:53:22.515: RADIUS: MS-CHAP-MPPE-Keys [12] 34 *
Sep 28 21:53:22.519: RADIUS: Framed-IP-Address [8] 6 192.168.1.1
Sep 28 21:53:22.519: RADIUS: Class [25] 31
Sep 28 21:53:22.519: RADIUS:
43 49 53 43 4F 41 43 53 3A 30 30 30 30 30 30 36 [CISCOACS:0000006]
Sep 28 21:53:22.519: RADIUS:
33 2F 30 61 34 32 34 66 36 33 2F 32 37 [3/0a424f63/27]
Sep 28 21:53:22.519: RADIUS(0000001C): Received from id 21645/44
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: service-type
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: Framed-Protocol
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: inacl: Peruser
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: MS-CHAP-MPPE-Keys
Sep 28 21:53:22.523: ppp27 PPP/AAA: Check Attr: addr
Sep 28 21:53:22.523: ppp27 PPP: Phase is FORWARDING, Attempting Forward
Sep 28 21:53:22.523: Vi3 PPP: Phase is DOWN, Setup
Sep 28 21:53:22.527: AAA/BIND(0000001C): Bind i/f Virtual-Access3
Sep 28 21:53:22.531: %LINK-3-UPDOWN: Interface Virtual-Access3,
changed state to up
Sep 28 21:53:22.531: Vi3 PPP: Phase is AUTHENTICATING, Authenticated User
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Author
Sep 28 21:53:22.531: Vi3 AAA/AUTHOR/LCP: Process Attr: service-type
Sep 28 21:53:22.531: Vi3 MS-CHAP: O SUCCESS id 1 len 4
Sep 28 21:53:22.535: Vi3 PPP: Phase is UP
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/PCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start IPCP
Sep 28 21:53:22.535: Vi3 IPCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 IPCP: Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/CCP: FSM authorization not needed
Sep 28 21:53:22.535: Vi3 AAA/AUTHOR/FSM: We can start CCP
Sep 28 21:53:22.535: Vi3 CCP: O CONFREQ [Closed] id 1 len 10
Sep 28 21:53:22.535: Vi3 CCP: MS-PPC supported bits 0x01000060 (0x120601000060)
Sep 28 21:53:22.535: Vi3 PPP: Process pending packets
Sep 28 21:53:22.539: RADIUS(0000001C): Using existing nas_port 27
Sep 28 21:53:22.539: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Sep 28 21:53:22.539: RADIUS(0000001C): sending
Sep 28 21:53:22.539: RADIUS/ENCODE: Best Local IP-Address
10.66.79.99 for Radius-Server 10.66.79.120
Sep 28 21:53:22.539: RADIUS(0000001C): Send Accounting-Request
to 10.66.79.120:1646 id 21645/45, len 147
Sep 28 21:53:22.539: RADIUS: authenticator 1A 76 20 95 95 F8
81 42 - 1F E8 E7 C1 8F 10 BA 94
Sep 28 21:53:22.539: RADIUS: Acct-Session-Id [44] 10 "00000026"
Sep 28 21:53:22.539: RADIUS: Tunnel-Server-Endpoi[67] 13 "10.66.79.99"
Sep 28 21:53:22.539: RADIUS: Tunnel-Client-Endpoi[66] 13 "10.66.79.60"

```

```

Sep 28 21:53:22.543: RADIUS: Tunnel-Assignment-Id[82] 3 "1"
Sep 28 21:53:22.543: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 28 21:53:22.543: RADIUS: Acct-Authentic [45] 6 RADIUS [1]
Sep 28 21:53:22.543: RADIUS: User-Name [1] 9 "georgia"
Sep 28 21:53:22.543: RADIUS: Acct-Status-Type [40] 6 Start [1]
Sep 28 21:53:22.543: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 28 21:53:22.543: RADIUS: NAS-Port [5] 6 27
Sep 28 21:53:22.543: RADIUS: Class [25] 31
Sep 28 21:53:22.543: RADIUS: 43 49 53 43 4F 41 43 53 3A 30 30 30 30
30 30 36 [CISCOACS:0000006]
Sep 28 21:53:22.543: RADIUS: 33 2F 30 61 34 32 34 66 36 33 2F 32 37
[3/0a424f63/27]
Sep 28 21:53:22.547: RADIUS: Service-Type [6] 6 Framed [2]
Sep 28 21:53:22.547: RADIUS: NAS-IP-Address [4] 6 10.66.79.99
Sep 28 21:53:22.547: RADIUS: Acct-Delay-Time [41] 6 0
Sep 28 21:53:22.547: Vi3 CCP: I CONFREQ [REQsent] id 4 len 10
Sep 28 21:53:22.547: Vi3 CCP: MS-PPC supported bits 0x010000F1
(0x1206010000F1)
Sep 28 21:53:22.547: Vi3 CCP: O CONFNAK [REQsent] id 4 len 10
Sep 28 21:53:22.551: Vi3 CCP: MS-PPC supported bits 0x01000060
(0x120601000060)
Sep 28 21:53:22.551: Vi3 CCP: I CONFNAK [REQsent] id 1 len 10
Sep 28 21:53:22.551: Vi3 CCP: MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 CCP: O CONFREQ [REQsent] id 2 len 10
Sep 28 21:53:22.551: Vi3 CCP: MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.551: Vi3 IPCP: I CONFREQ [REQsent] id 5 len 34
Sep 28 21:53:22.551: Vi3 IPCP: Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.551: Vi3 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.551: Vi3 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.551: Vi3 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.551: Vi3 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0,
we want 0.0.0.0
Sep 28 21:53:22.551: Vi3 AAA/AUTHOR/IPCP: Processing AV inacl
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Processing AV addr
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Authorization succeeded
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0,
we want 192.168.1.1
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for primary wins
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for secondday dns
Sep 28 21:53:22.555: Vi3 AAA/AUTHOR/IPCP: no author-info for secondday wins
Sep 28 21:53:22.555: Vi3 IPCP: O CONFREJ [REQsent] id 5 len 28
Sep 28 21:53:22.555: Vi3 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
Sep 28 21:53:22.555: Vi3 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
Sep 28 21:53:22.555: Vi3 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
Sep 28 21:53:22.555: Vi3 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
Sep 28 21:53:22.555: Vi3 IPCP: I CONFACK [REQsent] id 1 len 10
Sep 28 21:53:22.555: Vi3 IPCP: Address 10.66.79.99 (0x03060A424F63)
Sep 28 21:53:22.563: Vi3 CCP: I CONFREQ [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP: MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.563: Vi3 CCP: O CONFACK [REQsent] id 6 len 10
Sep 28 21:53:22.563: Vi3 CCP: MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: I CONFACK [ACKsent] id 2 len 10
Sep 28 21:53:22.567: Vi3 CCP: MS-PPC supported bits 0x01000040
(0x120601000040)
Sep 28 21:53:22.567: Vi3 CCP: State is Open
Sep 28 21:53:22.567: Vi3 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
Sep 28 21:53:22.567: Vi3 IPCP: Address 0.0.0.0 (0x030600000000)
Sep 28 21:53:22.567: Vi3 IPCP: O CONFNAK [ACKrcvd] id 7 len 10

```

```
Sep 28 21:53:22.571: Vi3 IPCP:      Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:      Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: O CONFACK [ACKrcvd] id 8 len 10
Sep 28 21:53:22.575: Vi3 IPCP:      Address 192.168.1.1 (0x0306C0A80101)
Sep 28 21:53:22.575: Vi3 IPCP: State is Open
Sep 28 21:53:22.575: AAA/AUTHOR: Processing PerUser AV inacl
Sep 28 21:53:22.583: Vi3 IPCP: Install route to 192.168.1.1
Sep 28 21:53:22.583: Vi3 IPCP: Add link info for cef entry 192.168.1.1
Sep 28 21:53:22.603: RADIUS: Received from id 21645/45 10.66.79.120:1646,
Accounting-response, len 20
Sep 28 21:53:22.603: RADIUS:  authenticator A6 B3 4C 4C 04 1B BE 8E - 6A
BF 91 E2 3C 01 3E CA
Sep 28 21:53:23.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access3, changed state to up
```

[Información Relacionada](#)

- [Página de soporte de Cisco Secure ACS para Windows](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)