

# Configurando o CiscoSecure ACS para a autenticação PPTP do roteador Windows

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Diagrama de Rede](#)

[Configuração do roteador](#)

[Recurso de Fallback do Servidor RADIUS](#)

[Configuração do Cisco Secure ACS para Windows](#)

[Adicionando à configuração](#)

[Adicionando criptografia](#)

[Atribuição de endereço IP estático do servidor](#)

[Adicionar listas de acesso ao servidor](#)

[Adicionar relatório](#)

[Encapsulamento dividido](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Exemplo de saída de boa depuração](#)

[Informações Relacionadas](#)

## [Introduction](#)

O suporte a Point-to-Point Tunnel Protocol (PPTP) foi adicionado ao Cisco IOS® Software Release 12.0.5.XE5 nas plataformas Cisco 7100 e 7200 (consulte PPTP com Microsoft Point-to-Point Encryption (MPPE) [Cisco IOS Software Release 12.0]). O suporte a outras plataformas foi adicionado no Cisco IOS Software Release 12.1.5.T (consulte MSCHAP Versão 2).

[O RFC 2637](#) descreve o PPTP. Nos termos do PPTP, de acordo com a RFC, o Concentrador de acessos do PPTP (PAC) é o cliente (o PC, isto é, o chamador) e o Servidor de rede do PPTP (PNS) é o servidor (o roteador é o que foi chamado).

Este documento pressupõe que as conexões PPTP com o roteador com a autenticação V1 do Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP) (e, opcionalmente, MPPE, que requer MS-CHAP V1) foram criadas com o uso desses documentos e já estão operacionais. RADIUS é necessário para suporte à criptografia MPPE. TACACS+ funciona para autenticação, mas não para chaveamento MPPE. O suporte a MS-CHAP V2 foi adicionado ao Cisco IOS Software Release 12.2(2)XB5 e foi integrado ao Cisco IOS Software Release 12.2(13)T (consulte

[MSCHAP Versão 2](#)), entretanto, o MPPE ainda não é suportado com MS-CHAP V2.

Este exemplo de configuração demonstra como configurar uma conexão de PC com o roteador (em 10.66.79.99), que, em seguida, fornece autenticação de usuário ao Cisco Secure Access Control System (ACS) 4.2 para o servidor Windows (em 10.66.79.120), antes de permitir que o usuário entre na rede.

**Observação:** o servidor RADIUS geralmente não está fora do roteador, exceto em um ambiente de laboratório.

O suporte PPTP foi adicionado ao Cisco Secure ACS 2.5, mas pode não funcionar com o roteador devido à ID de bug da Cisco [CSCds92266](#) (somente clientes [registrados](#)). O ACS 2.6 e posterior não têm esse problema.

O Cisco Secure UNIX não é compatível com a MPPE. Dois outros aplicativos RADIUS com suporte a MPPE incluem Microsoft RADIUS e Funk RADIUS.

Consulte [Configurando o Roteador Cisco e Clientes VPN Usando PPTP e MPPE](#) para obter mais informações sobre como configurar PPTP e MPPE com um roteador.

Consulte [Configuração do VPN 3000 Concentrador e PPTP com Cisco Secure ACS for Windows RADIUS Authentication](#) para obter mais informações sobre como configurar o PPTP em um VPN 3000 Concentrador com a autenticação Cisco Secure ACS for Windows for RADIUS.

Consulte o [PIX 6.x: Exemplo de Configuração de PPTP com Autenticação Radius](#) para configurar conexões PPTP com o PIX.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure ACS 4.2 para Windows
- Cisco 3600 Router
- Software Cisco IOS versão 12.4(3)

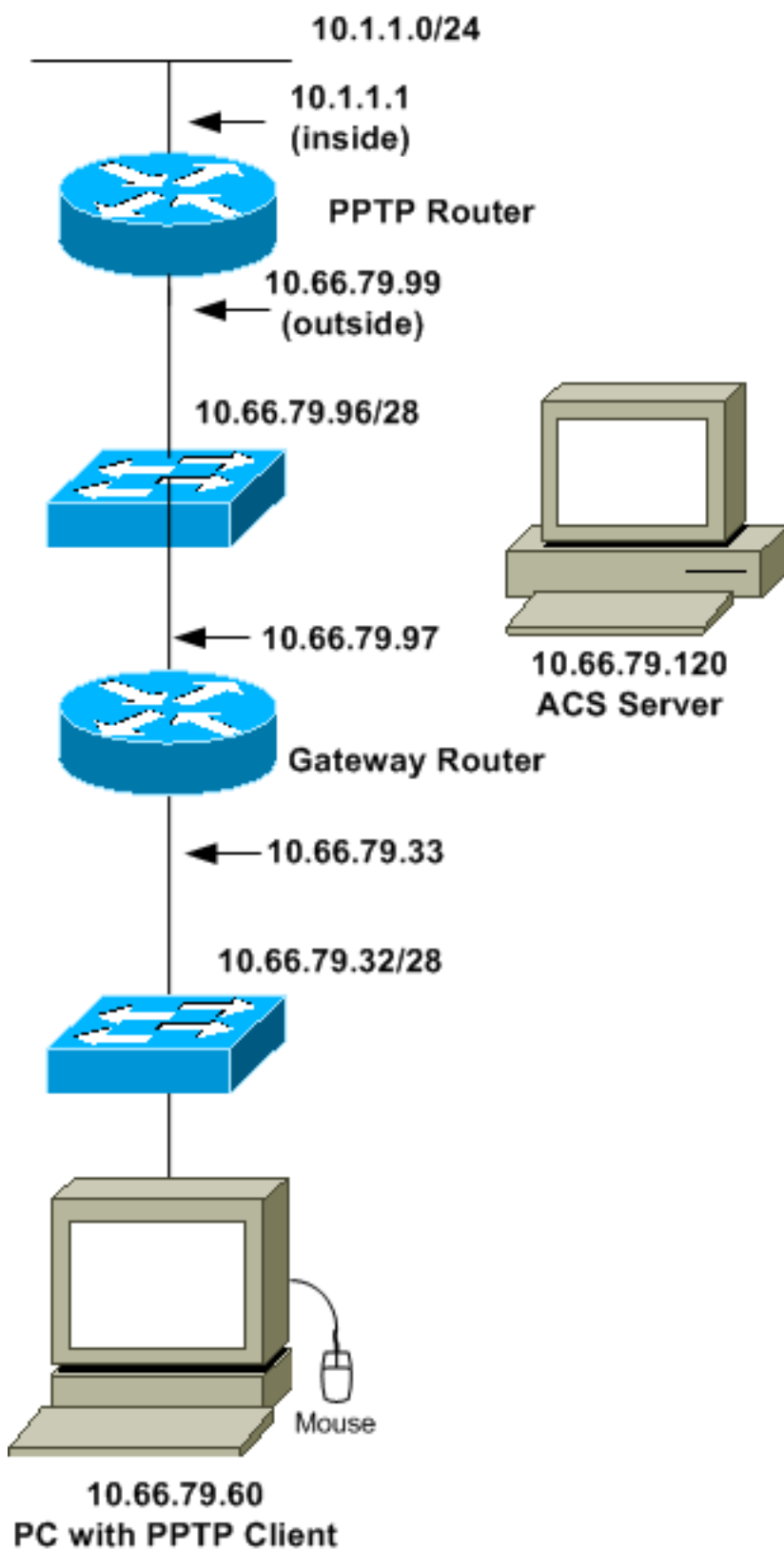
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver em uma rede ativa, certifique-se de entender o impacto potencial de qualquer comando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

### Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



## Configuração do roteador

Use esta configuração de roteador. O usuário deve ser capaz de se conectar com "username john password doe" mesmo que o servidor RADIUS não esteja acessível (o que é possível se o

servidor ainda não tiver sido configurado com o Cisco Secure ACS). Este exemplo pressupõe que a autenticação local (e, opcionalmente, a criptografia) já está operacional.

## 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 ptp
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
```

## [Recurso de Fallback do Servidor RADIUS](#)

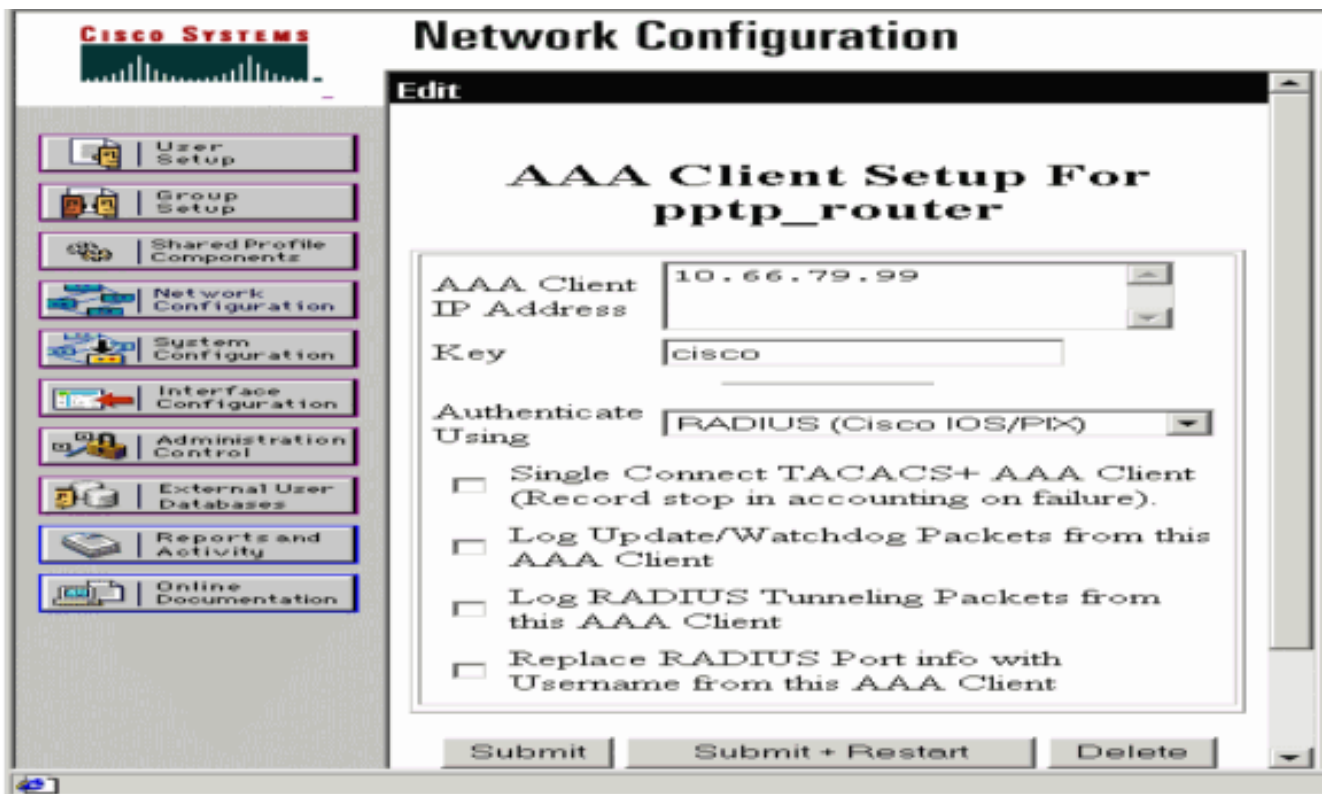
Quando o servidor RADIUS primário se tornar indisponível, o roteador realizará failover para o próximo servidor RADIUS de backup ativo. O roteador continuará a usar o servidor RADIUS secundário para sempre, mesmo que o servidor primário esteja disponível. Geralmente, o servidor primário é de alto desempenho e o preferido.

Para definir a autenticação de autenticação, autorização e contabilização (AAA) no login, use o comando [aaa authentication login](#) no modo de configuração global.

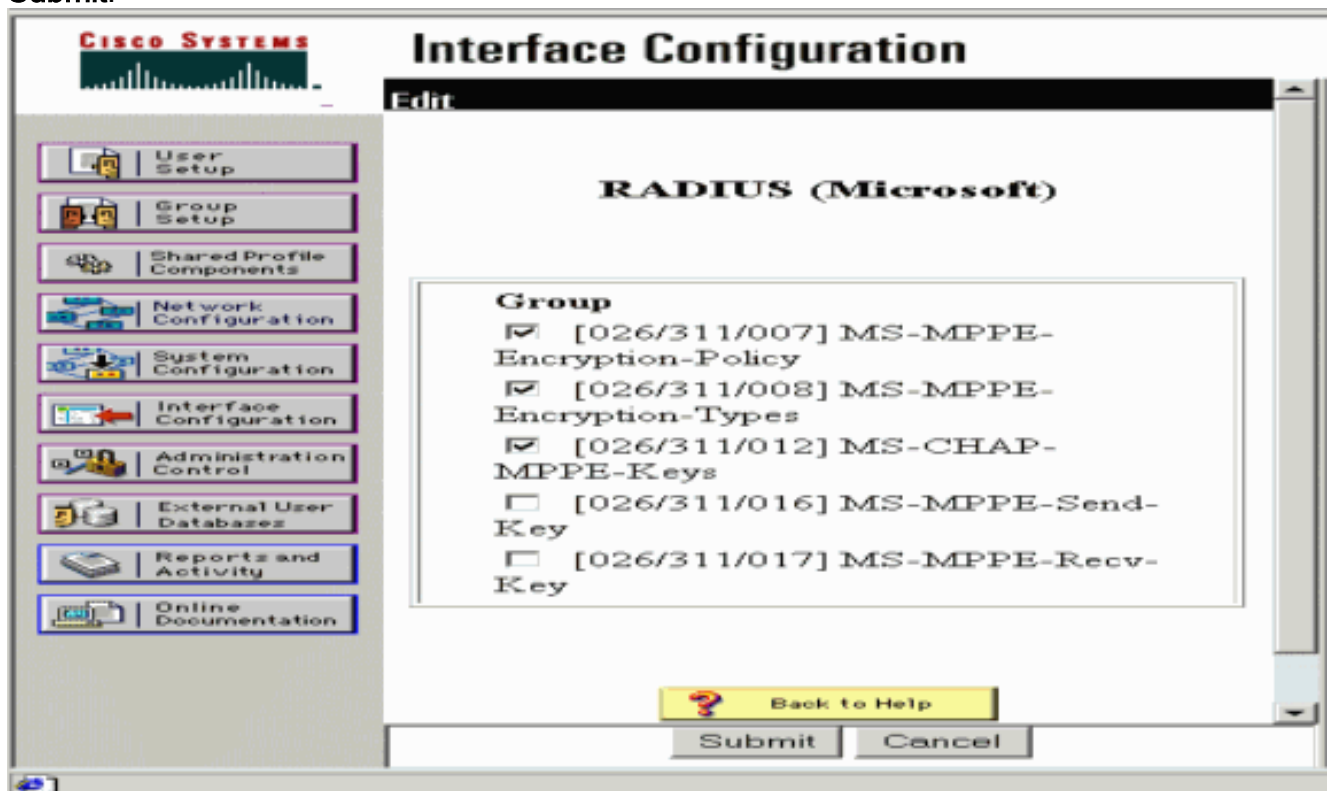
## [Configuração do Cisco Secure ACS para Windows](#)

Use este procedimento para configurar o Cisco Secure ACS:

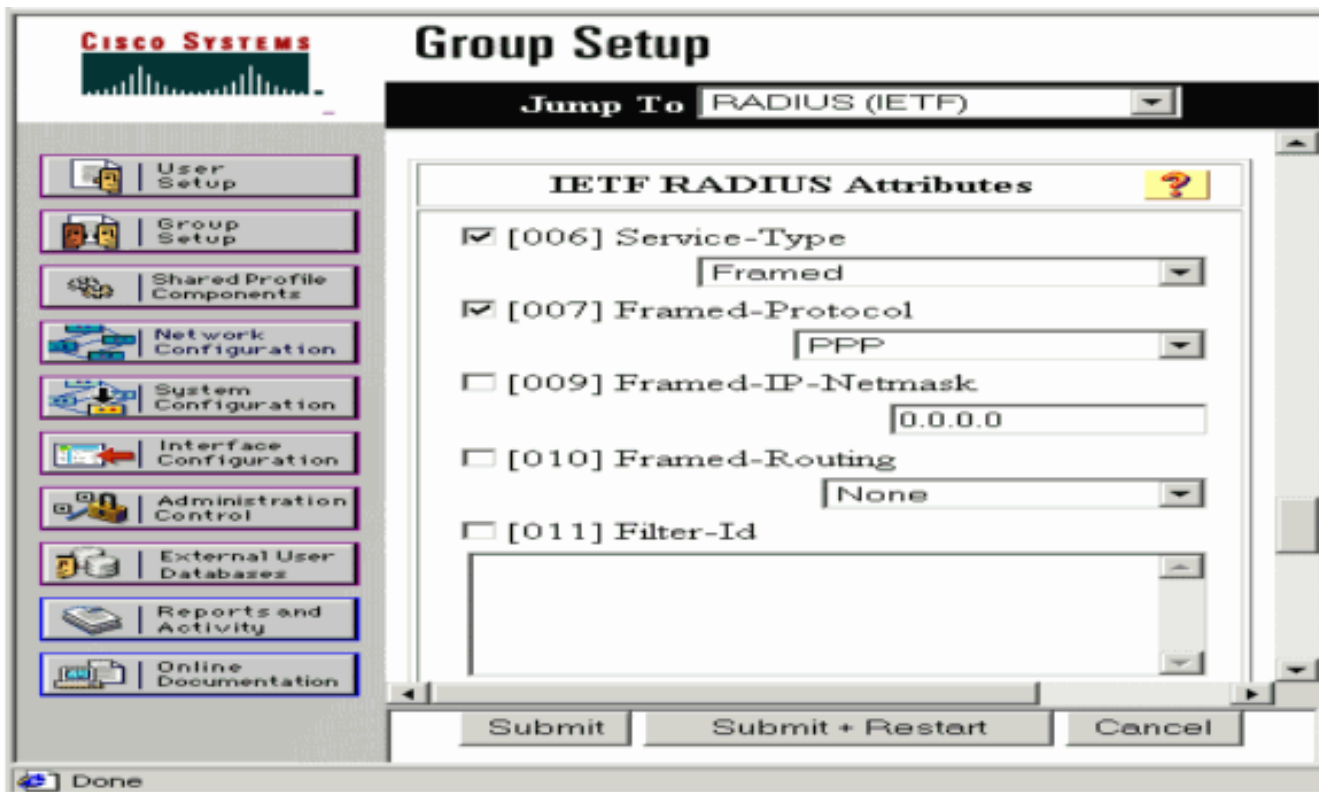
1. Clique em **Network Configuration**, adicione uma entrada para o roteador e clique em **Submit + Restart** quando terminar.



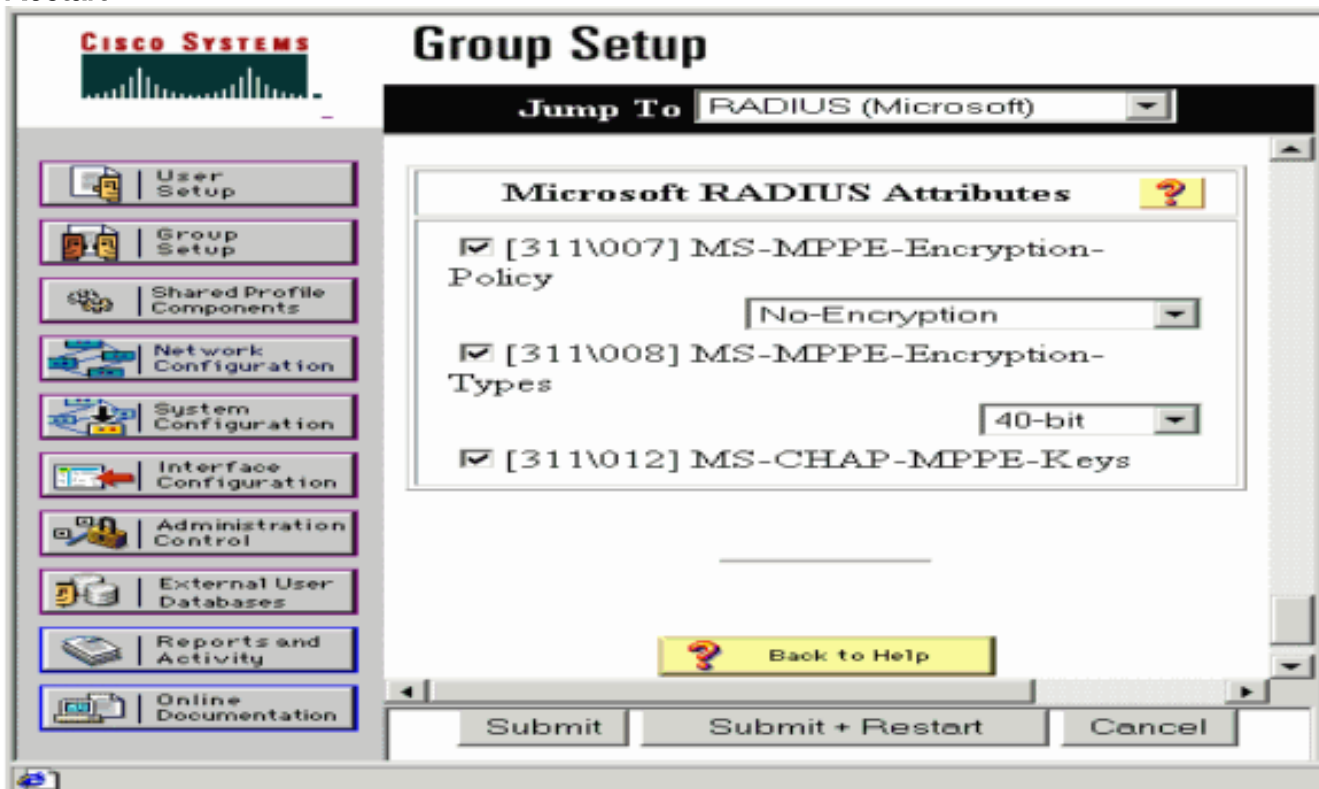
2. Selecione **Interface Configuration > RADIUS (Microsoft)**, marque seus atributos MPPE e clique em **Submit**.



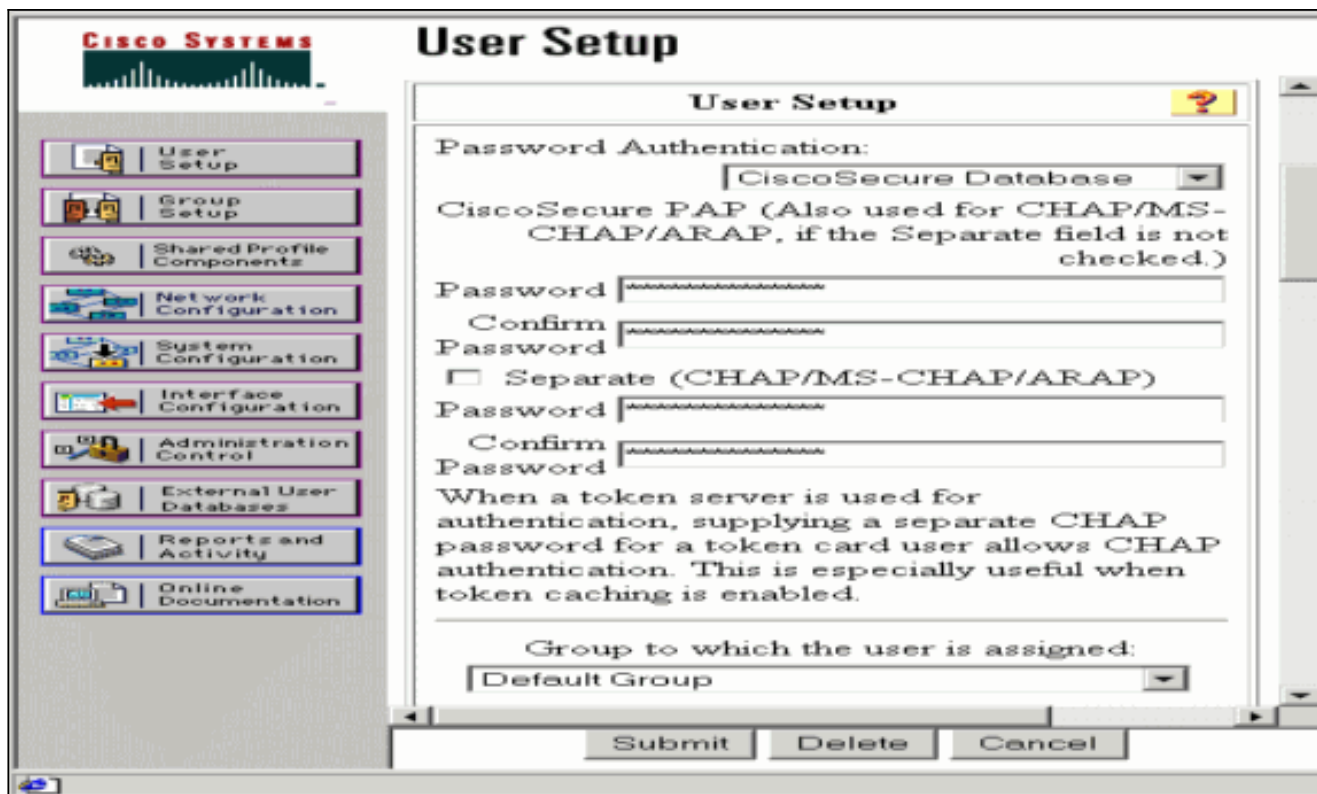
3. Clique em **Group Setup** e, em Service-Type, selecione **Framed**. Para Framed-Protocol, selecione **PPP** e clique em **Submit**.



4. Em **Group Setup**, verifique as informações do MS-MPPE RADIUS e, quando terminar, clique em **Submit + Restart**.



5. Clique em **User Setup**, adicione uma senha, atribua o usuário ao grupo e clique em **Submit**.



6. Teste a autenticação no roteador antes de adicionar criptografia. Se a autenticação não funcionar, consulte a seção [Solução de problemas](#) deste documento.

## [Adicionando à configuração](#)

### [Adicionando criptografia](#)

Você pode adicionar criptografia MPPE com este comando:

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

Como o exemplo presume que a criptografia funciona com autenticação local (nome de usuário e senha no roteador), o PC está configurado corretamente. Agora você pode adicionar este comando para permitir máxima flexibilidade:

```
ppp encrypt mppe auto
```

### [Atribuição de endereço IP estático do servidor](#)

Se precisar atribuir um endereço IP específico ao usuário, em Configuração do usuário ACS, selecione **Atribuir endereço IP estático** e preencha o endereço IP.

### [Adicionar listas de acesso ao servidor](#)

Para controlar o que o usuário PPTP pode acessar quando estiver conectado ao roteador, você



pode configurar uma lista de acesso no roteador. Por exemplo, se você emitir este comando:

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

e escolha **Filter-Id (atributo 11)** no ACS e digite **101** na caixa, o usuário PPTP pode acessar o host 10.1.1.2, mas não outros. Quando você emite um comando **show ip interface virtual-access x**, onde **x** é um número que você pode determinar a partir de um **show user**, a lista de acesso deve mostrar conforme aplicado:

```
Inbound access list is 101
```

## [Adicionar relatório](#)

Você pode adicionar a contabilização de sessões com este comando:

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

Os registros de contabilidade no Cisco Secure ACS são exibidos conforme mostrado na saída:

```
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
```

**Observação:** quebras de linha foram adicionadas ao exemplo para fins de exibição. As quebras de linha na sua saída real são diferentes das mostradas aqui.

## [Encapsulamento dividido](#)

Quando o túnel PPTP é ativado no PC, o roteador PPTP é instalado com uma métrica mais alta do que o padrão anterior, de modo que você perde a conectividade com a Internet. Para corrigir isso, considerando que a rede dentro do roteador é 10.1.1.X, execute um arquivo de lote (batch.bat) para modificar o roteamento da Microsoft para excluir o padrão e reinstalar a rota padrão (isso requer o endereço IP que o cliente PPTP está atribuído; por exemplo, 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
```

## [Verificar](#)

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

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados comandos `show`. Use a OIT para exibir uma análise da saída do comando `show`.

- **show vpdn session** — Exibe informações sobre o túnel de protocolo L2F (L2F) ativo e identificadores de mensagem em uma VPDN (Virtual Private Dialup Network).

```
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](#)

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

1. **O PC especifica a criptografia, mas o roteador não.**O usuário do PC vê:  
The remote computer does not support the required data encryption type.
2. **Tanto o PC quanto o roteador especificam a criptografia, mas o servidor RADIUS não está configurado para enviar as chaves MPPE (normalmente aparecem como atributo 26).**O usuário do PC vê:  
The remote computer does not support the required data encryption type.
3. **O roteador especifica a criptografia (obrigatório), mas o PC não (não permitido).**O usuário do PC vê:  
The specified port is not connected.
4. **O usuário digita o nome de usuário ou a senha incorretos.**O usuário do PC vê:  
Access was denied because the username and/or password was invalid on the domain.

A **depuração** do roteador mostra: **Observação:** quebras de linha foram adicionadas a este exemplo para fins de exibição. As quebras de linha na sua saída real são diferentes das mostradas aqui.

```
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. O servidor RADIUS não é comunicativo. O usuário do PC vê:

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

A depuração do roteador mostra: **Observação:** quebras de linha foram adicionadas a este exemplo para fins de exibição. As quebras de linha na sua saída real são diferentes das mostradas aqui.

```
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 Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados comandos `show`. Use a OIT para exibir uma análise da saída do comando `show`.

**Nota:** Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos `debug`.

Se as coisas não funcionarem, os comandos **debug** mínimos incluem:

- **debug aaa authentication** — Exibe informações sobre autenticação AAA/TACACS+
- **debug aaa authorization** — Exibe informações sobre autorização AAA/TACACS+.
- **debug ppp negotiation** — Exibe os pacotes PPP transmitidos durante a inicialização do PPP, onde as opções do PPP são negociadas.
- **debug ppp authentication** — Exibe mensagens do protocolo de autenticação, que incluem trocas de pacotes CHAP e trocas PAP (Password Authentication Protocol).
- **debug radius** — Exibe informações de debug detalhadas associadas ao RADIUS.

Se a autenticação funcionar, mas houver problemas com a criptografia MPPE, use estes comandos:

- **debug ppp mppe packet** — Exibe todo o tráfego MPPE de entrada e saída.
- **debug ppp mppe event** — Exibe as principais ocorrências de MPPE.
- **debug ppp mppe detailed** — Exibe informações de MPPE detalhadas.
- **debug vpdn l2x-packets** — Exibe mensagens sobre os cabeçalhos e o status do protocolo L2F.
- **debug vpdn events** — Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal de túneis.
- **debug vpdn errors** — Exibe erros que impedem que um túnel seja estabelecido ou erros que fazem com que um 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 você deve geralmente usar esse comando apenas em um chassi de depuração com uma única sessão ativa.

Você também pode usar estes comandos para fins de solução de problemas:

- **clear interface virtual-access x** — Desliga um túnel especificado e todas as sessões dentro do túnel.

## Exemplo de saída de boa depuração

Esta depuração mostra eventos significativos do RFC:

- **SCCRQ = Start-Control-Connection-Request** – código de mensagem bytes 9 e 10 = 0001
- **SCCRP = Start-Control-Connection-Reply**
- **OCRQ = Outgoing-Call-Request** - código de mensagem bytes 9 e 10 = 0007
- **OCRP = Outgoing-Call-Reply**

**Observação:** quebras de linha foram adicionadas a este exemplo para fins de exibição. As quebras de linha na sua saída real são diferentes das mostradas aqui.

```

moss#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
00A800011A2B3C4D0007000080007C0E0000012C05F5...
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: rcv 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
001800011A2B3C4D000F000000170000FFFFFFFFFFFFFFFF
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
```

## [Informações Relacionadas](#)

- [Cisco Secure ACS para página de suporte do Windows](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)