

Microsoft IAS를 사용하여 PPTP용 Cisco IOS 소프트웨어 및 Windows 2000 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 이론](#)

[구성](#)

[네트워크 다이어그램](#)

[Microsoft IAS용 Windows 2000 Advanced Server 구성](#)

[RADIUS 클라이언트 구성](#)

[IAS에서 사용자 구성](#)

[PPTP용 Windows 2000 클라이언트 구성](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[스플릿 터널링](#)

[클라이언트가 암호화용으로 구성되지 않은 경우](#)

[클라이언트가 암호화에 대해 구성되어 있고 라우터가 구성되지 않은 경우](#)

[PC가 암호화를 위해 구성된 경우 MS-CHAP 비활성화](#)

[RADIUS 서버가 통신할 수 없는 경우](#)

[관련 정보](#)

소개

PPTP(Point-to-Point Tunnel Protocol) 지원이 Cisco 7100 및 7200 라우터 플랫폼의 Cisco IOS® Software Release 12.0.5.XE5에 추가되었습니다. Cisco IOS Software 릴리스 12.1.5.T에 더 많은 플랫폼에 대한 지원이 추가되었습니다.

RFC(Request for Comments) 2637에서는 PPTP를 설명합니다. 이 RFC에 따르면 PPTP PAC(Access Concentrator)는 클라이언트(즉, PC 또는 호출자)이고 PPTP PNS(Network Server)는 서버(즉, 호출되는 라우터 또는 디바이스)입니다.

[사전 요구 사항](#)

[요구 사항](#)

이 문서에서는 이러한 문서를 사용하여 로컬 Microsoft-CHAP(Challenge Handshake Authentication Protocol) V1 인증(및 MS-CHAP V1이 필요한 Microsoft MPPE[Point-to-Point Encryption](선택 사항)을 사용하여 라우터에 대한 PPTP 연결을 설정하고 이미 작동하고 있다고 가정합니다. MPPE 암호화 지원을 위해서는 RADIUS(Remote Authentication Dial-In User Service)가 필요합니다. TACACS+는 인증에 작동하지만 MPPE 키잉에는 작동하지 않습니다.

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Active Directory가 있는 Microsoft 2000 고급 서버에 설치된 Microsoft IAS 선택적 구성 요소입니다.
- Cisco 3600 라우터.
- Cisco IOS 소프트웨어 릴리스 c3640-io3s56i-mz.121-5.T.

이 구성에서는 Windows 2000 고급 서버에 설치된 Microsoft IAS를 RADIUS 서버로 사용합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

배경 이론

이 샘플 컨피그레이션에서는 라우터에 연결하기 위해 PC를 설정하는 방법(10.200.20.2 주소)을 보여 줍니다. 이 방법을 통해 사용자가 네트워크에 연결되도록 허용하기 전에 Microsoft의 IAS(Internet Authentication Server)에 사용자를 인증합니다(10.200.20.245). PPTP는 Windows용 Cisco ACS(Secure Access Control Server) 버전 2.5에서 지원됩니다. 그러나 Cisco Bug ID CSCds92266 때문에 라우터에서 작동하지 않을 수 있습니다. Cisco Secure를 사용하는 경우 Cisco Secure Version 2.6 이상을 사용하는 것이 좋습니다. Cisco Secure UNIX는 MPPE를 지원하지 않습니다. MPPE를 지원하는 다른 두 RADIUS 애플리케이션은 Microsoft RADIUS와 Funk RADIUS입니다.

구성

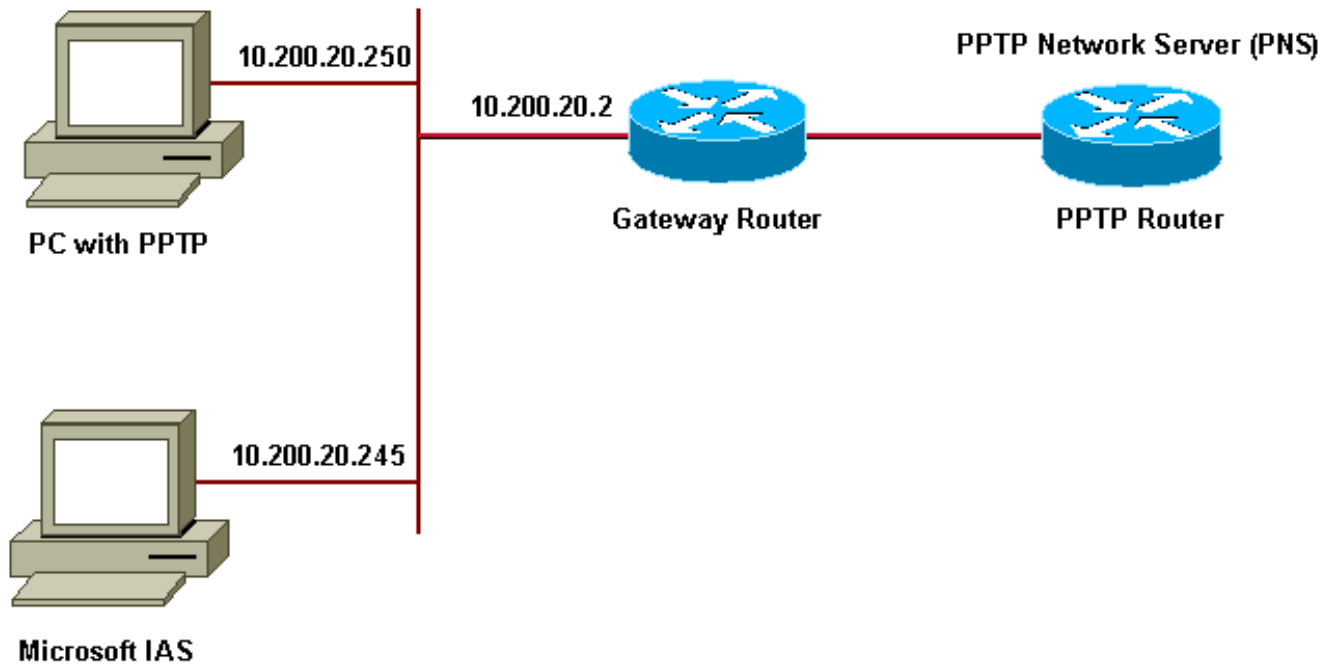
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에서 사용되는 명령에 대한 추가 정보를 찾으려면 IOS 명령 조회 도구를 사용하십시오.

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.

PPTP Access Concentrator (PAC)



전화 접속 클라이언트용 IP 풀:

- 게이트웨이 라우터: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.10

위 설정에서 전화 접속 클라이언트를 사용하여 전화 접속을 통해 인터넷 서비스 공급자(ISP) 라우터에 연결하는 경우에도 LAN과 같은 미디어를 통해 PC 및 게이트웨이 라우터를 연결할 수 있습니다.

[Microsoft IAS용 Windows 2000 Advanced Server 구성](#)

이 섹션에서는 Microsoft IAS용 Windows 2000 고급 서버를 구성하는 방법을 보여줍니다.

1. Microsoft IAS가 설치되어 있는지 확인합니다. Microsoft IAS를 설치하려면 관리자로 로그인합니다. Network Services(네트워크 서비스)에서 모든 확인란이 선택되었는지 확인합니다. 인터넷 인증 서버 확인란을 선택한 다음 **확인**을 클릭합니다.
2. **Windows 구성 요소** 마법사에서 다음을 클릭합니다. 메시지가 표시되면 Windows 2000 CD를 넣습니다.
3. 필요한 파일을 복사한 후 **마침**을 클릭하고 모든 창을 닫습니다. 재부팅할 필요가 없습니다.

[RADIUS 클라이언트 구성](#)

이 섹션에서는 radius 클라이언트를 구성하는 단계를 보여줍니다.

1. 관리 도구에서 **인터넷 인증 서버** 콘솔을 열고 **클라이언트**를 클릭합니다.
2. **Friendly Name**(식별 이름) 상자에 NAS(네트워크 액세스 서버)의 IP 주소를 입력합니다.
3. **Use this IP** 옵션을 클릭합니다.
4. **Client-Vendor** 드롭다운 목록 상자에서 **RADIUS Standard** 옵션이 선택되었는지 확인합니다.
5. **Shared Secret**(공유 암호) 및 **Confirm Shared Secret**(공유 암호 확인) 상자에 암호를 입력하고 **Finish**(마침)를 클릭합니다.
6. 콘솔 트리에서 **인터넷 인증 서비스**를 마우스 오른쪽 단추로 클릭한 다음 **시작**을 클릭합니다.

7. 콘솔을 닫습니다.

IAS에서 사용자 구성

Cisco Secure와 달리 Windows 2000 RADIUS 사용자 데이터베이스는 Windows 사용자 데이터베이스에 긴밀하게 바인딩됩니다. Windows 2000 서버에 **Active Directory**가 설치된 경우 **Active Directory 사용자 및 컴퓨터**에서 새 전화 접속 사용자를 만듭니다. **Active Directory**가 설치되어 있지 않은 경우 관리 도구의 로컬 사용자 및 그룹을 사용하여 새 사용자를 생성합니다.

Active Directory에서 사용자 구성

이 섹션에서는 Active Directory에서 사용자를 구성하는 단계를 보여줍니다.

1. **Active Directory 사용자 및 컴퓨터** 콘솔에서 도메인을 확장합니다. 사용자를 마우스 오른쪽 단추로 클릭합니다. 스크롤하여 새 사용자를 선택합니다. tac이라는 새 사용자를 생성합니다.
2. Password(비밀번호) 및 Confirm Password(비밀번호 확인) 대화 상자에 비밀번호를 입력합니다.
3. User Must Change Password at Next Logon(다음 로그인 시 사용자가 반드시 비밀번호를 변경해야 함) 필드를 지우고 Next(다음)를 클릭합니다.
4. User tac Properties(사용자 tac 속성) 상자를 엽니다. 전화 접속 탭으로 전환합니다. Remote Access Permission (Dial-in or VPN)(원격 액세스 권한(전화 접속 또는 VPN))에서 Allow Access(액세스 허용)를 클릭한 다음 OK(확인)를 클릭합니다.

Active Directory가 설치되지 않은 경우 사용자 구성이 섹션에서는 Active Directory가 설치되지 않은 경우 사용자를 구성하는 단계를 보여줍니다.

1. 관리 도구 섹션에서 컴퓨터 관리를 클릭합니다. 컴퓨터 관리 콘솔을 확장하고 로컬 사용자 및 그룹을 클릭합니다. Users(사용자) 스크롤 막대를 마우스 오른쪽 버튼으로 클릭하여 New User(새 사용자)를 선택합니다. tac이라는 새 사용자를 생성합니다.
2. Password(비밀번호) 및 Confirm Password(비밀번호 확인) 대화 상자에 비밀번호를 입력합니다.
3. User Must Change Password at Next Logon(다음 로그인 시 사용자가 반드시 비밀번호를 변경해야 함) 옵션의 선택을 취소하고 Next(다음)를 클릭합니다.
4. tac의 속성 상자라는 새 사용자를 엽니다. 전화 접속 탭으로 전환합니다. Remote Access Permission (Dial-in or VPN)(원격 액세스 권한(전화 접속 또는 VPN))에서 Allow Access(액세스 허용)를 클릭한 다음 OK(확인)를 클릭합니다.

Windows 사용자에게 원격 액세스 정책 적용이 섹션에서는 Windows 사용자에게 원격 액세스 정책을 적용하는 단계를 보여줍니다.

1. 관리 도구에서 인터넷 인증 서버 콘솔을 열고 원격 액세스 정책을 클릭합니다.
2. Specify the Conditions to Match and add Service-Type(일치시킬 조건 지정 및 서비스 유형 추가)에서 Add(추가) 버튼을 클릭합니다. 사용 가능한 유형을 프레임드(Framed)로 선택하고 선택된 유형 목록에 추가합니다. 확인을 누릅니다.
3. Specify the Conditions to Match and add Framed Protocol에서 Add(추가) 버튼을 클릭합니다. 사용 가능한 유형을 ppp로 선택하고 Selected Types 목록에 추가합니다. 확인을 누릅니다.
4. Specify the Conditions to Match and add Windows-Groups(일치시킬 조건 지정에서 추가 버튼을 클릭하여 사용자가 속한 Windows 그룹을 추가합니다. 그룹을 선택하고 Selected Types(선택한 유형)에 추가하고 OK(확인)를 누릅니다.
5. 전화 접속 권한이 활성화된 경우 액세스 허용 속성에서 원격 액세스 권한 부여를 선택합니다.
6. 콘솔을 닫습니다.

PPTP용 Windows 2000 클라이언트 구성 아래 섹션에서는 PPTP용 Windows 2000 클라이언트를 구성하는 단계를 보여줍니다.

1. 시작 메뉴에서 설정을 선택한 다음 중 하나를 선택합니다. 제어판 및 네트워크 및 전화 접속 연결 또는 네트워크 및 전화 접속 연결을 다시 연결합니다. 마법사를 사용하여 PPTP라는 연결을 생성합니다. 이 연결은 인터넷을 통해 사설 네트워크에 연결됩니다. 또한 PPTP PNS(Network Server) IP 주소 또는 이름을 지정해야 합니다.
2. 새 연결이 제어판의 네트워크 및 전화 접속 연결 창에 나타납니다. 여기서 마우스 오른쪽 버튼을 클릭하여 속성을 편집합니다. Networking(네트워킹) 탭에서 Type of Server I Am Calling(서버 I am Calling) 필드가 PPTP로 설정되어 있는지 확인합니다. 로컬 폴 또는 DHCP(Dynamic Host Configuration Protocol)를 통해 게이트웨이에서 이 클라이언트에 동적 내부 주소를 할당하려는 경우 TCP/IP 프로토콜을 선택하고 클라이언트가 IP 주소를 자동으로 가져오도록 구성되었는지 확인합니다. DNS 정보를 자동으로 발급할 수도 있습니다. Advanced(고급) 버튼을 사용하면 고정 WINS(Windows Internet Naming Service) 및 DNS 정보를 정의할 수 있습니다. Options 탭을 사용하면 IPsec을 끄거나 연결에 다른 정책을 할당할 수 있습니다.
3. Security 탭 아래에서 사용자 인증 매개변수를 정의할 수 있습니다. 예를 들어 PAP, CHAP 또는 MS-CHAP 또는 Windows 도메인 로그인과 같이 하십시오. 연결이 구성되면 두 번 클릭하여 로그인 화면을 표시한 다음 연결할 수 있습니다.

구성 사용자는 다음 라우터 컨피그레이션을 사용하여 RADIUS 서버를 사용할 수 없는 경우에도 사용자 이름 tac 및 비밀번호 관리자와 연결할 수 있습니다(Microsoft IAS를 아직 구성하지 않은 경우 가능). 다음 샘플 컨피그레이션에서는 IPsec 없이 L2tp에 필요한 명령을 간략하게 설명합니다.

```
안젤라

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-Templat1 ip unnumbered Loopback0 peer default
ip address pool default !--- The following encryption
command is optional !--- and could be added later. ppp
```

```
encrypt mppe 40 ppp authentication ms-chap ! ip local
pool default 172.16.10.1 172.16.10.10 ip classless ip
route 0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ! end angela#show debug
```

General OS:

AAA Authentication debugging is on

AAA Authorization debugging is on

PPP:

MPPE Events debugging is on

PPP protocol negotiation debugging is on

VPN:

L2X protocol events debugging is on

L2X protocol errors debugging is on

VPDN events debugging is on

VPDN errors debugging is on

Radius protocol debugging is on

angela#

*Mar 7 04:21:07.719: L2X: TCP connect reqd from
0.0.0.0:2000

*Mar 7 04:21:07.991: Tnl 29 PPTP: Tunnel created; peer
initiated

*Mar 7 04:21:08.207: Tnl 29 PPTP: SCCRQ-ok ->
state change wt-sccrq to estabd

*Mar 7 04:21:09.267: VPDN: Session vaccess task running

*Mar 7 04:21:09.267: Vil VPDN: Virtual interface
created

*Mar 7 04:21:09.267: Vil VPDN: Clone from Vtemplate 1

*Mar 7 04:21:09.343: Tnl/Cl 29/29 PPTP: VAccess created

*Mar 7 04:21:09.343: Vil Tnl/Cl 29/29 PPTP: vacc-ok ->
#state change wt-vacc to estabd

*Mar 7 04:21:09.343: Vil VPDN: Bind interface
direction=2

*Mar 7 04:21:09.347: %LINK-3-UPDOWN: Interface Virtual-
Access1, changed

state to up

*Mar 7 04:21:09.347: Vil PPP: Using set call direction

*Mar 7 04:21:09.347: Vil PPP: Treating connection as a
callin

*Mar 7 04:21:09.347: Vil PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load]

*Mar 7 04:21:09.347: Vil LCP: State is Listen

*Mar 7 04:21:10.347: %LINEPROTO-5-UPDOWN: Line protocol
on Interface

Virtual-Access1, changed state to up

*Mar 7 04:21:11.347: Vil LCP: TIMEout: State Listen

*Mar 7 04:21:11.347: Vil AAA/AUTHOR/FSM: (0): LCP
succeeds trivially

*Mar 7 04:21:11.347: Vil LCP: O CONFREQ [Listen] id 7
len 15

*Mar 7 04:21:11.347: Vil LCP: AuthProto MS-CHAP
(0x0305C22380)

*Mar 7 04:21:11.347: Vil LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F)

*Mar 7 04:21:11.635: Vil LCP: I CONFACK [REQsent] id 7
len 15

*Mar 7 04:21:11.635: Vil LCP: AuthProto MS-CHAP
(0x0305C22380)

```
*Mar 7 04:21:11.635: Vil LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.327: Vil LCP: I CONFREQ [ACKrcvd] id 1
len 44
*Mar 7 04:21:13.327: Vil LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.327: Vil LCP: PFC (0x0702)
*Mar 7 04:21:13.327: Vil LCP: ACFC (0x0802)
*Mar 7 04:21:13.327: Vil LCP: Callback 6 (0x0D0306)
*Mar 7 04:21:13.327: Vil LCP: MRRU 1614 (0x1104064E)
*Mar 7 04:21:13.327: Vil LCP: EndpointDisc 1 Local
*Mar 7 04:21:13.327: Vil LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar 7 04:21:13.331: Vil LCP: (0xB9182600000008)
*Mar 7 04:21:13.331: Vil LCP: O CONFREQ [ACKrcvd] id 1
len 34
*Mar 7 04:21:13.331: Vil LCP: Callback 6 (0x0D0306)
*Mar 7 04:21:13.331: Vil LCP: MRRU 1614 (0x1104064E)
*Mar 7 04:21:13.331: Vil LCP: EndpointDisc 1 Local
*Mar 7 04:21:13.331: Vil LCP:
(0x1317016AC616B006CC4281A1CA941E39)
*Mar 7 04:21:13.331: Vil LCP: (0xB91826000000008)
*Mar 7 04:21:13.347: Vil LCP: TIMEout: State ACKrcvd
*Mar 7 04:21:13.347: Vil LCP: O CONFREQ [ACKrcvd] id 8
len 15
*Mar 7 04:21:13.347: Vil LCP: AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:13.347: Vil LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.647: Vil LCP: I CONFREQ [REQsent] id 2
len 14
*Mar 7 04:21:13.651: Vil LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.651: Vil LCP: PFC (0x0702)
*Mar 7 04:21:13.651: Vil LCP: ACFC (0x0802)
*Mar 7 04:21:13.651: Vil LCP: O CONFACK [REQsent] id 2
len 14
*Mar 7 04:21:13.651: Vil LCP: MagicNumber 0x35BE1CB0
(0x050635BE1CB0)
*Mar 7 04:21:13.651: Vil LCP: PFC (0x0702)
*Mar 7 04:21:13.651: Vil LCP: ACFC (0x0802)
*Mar 7 04:21:13.723: Vil LCP: I CONFACK [ACKsent] id 8
len 15
*Mar 7 04:21:13.723: Vil LCP: AuthProto MS-CHAP
(0x0305C22380)
*Mar 7 04:21:13.723: Vil LCP: MagicNumber 0x3050EB1F
(0x05063050EB1F)
*Mar 7 04:21:13.723: Vil LCP: State is Open
*Mar 7 04:21:13.723: Vil PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load]
*Mar 7 04:21:13.723: Vil MS-CHAP: O CHALLENGE id 20 len
21 from "angela "
*Mar 7 04:21:14.035: Vil LCP: I IDENTIFY [Open] id 3
len 18 magic
0x35BE1CB0 MSRASV5.00
*Mar 7 04:21:14.099: Vil LCP: I IDENTIFY [Open] id 4
len 24 magic
0x35BE1CB0 MSRAS-1-RSHANMUG
*Mar 7 04:21:14.223: Vil MS-CHAP: I RESPONSE id 20 len
57 from "tac"
*Mar 7 04:21:14.223: AAA: parse name=Virtual-Access1
idb type=21 tty=-1
*Mar 7 04:21:14.223: AAA: name=Virtual-Access1
flags=0x11 type=5 shelf=0
```

```
slot=0 adapter=0 port=1 channel=0
*Mar 7 04:21:14.223: AAA/MEMORY: create_user
(0x62740E7C) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1
*Mar 7 04:21:14.223: AAA/AUTHEN/START (2474402925):
port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 7 04:21:14.223: AAA/AUTHEN/START (2474402925):
using "default" list
*Mar 7 04:21:14.223: AAA/AUTHEN/START (2474402925):
Method=radius (radius)
*Mar 7 04:21:14.223: RADIUS: ustruct sharecount=0
*Mar 7 04:21:14.223: RADIUS: Initial Transmit Virtual-
Access1 id 116
10.200.20.245:1645, Access-Request, len 129
*Mar 7 04:21:14.227: Attribute 4 6 0AC81402
*Mar 7 04:21:14.227: Attribute 5 6 00000001
*Mar 7 04:21:14.227: Attribute 61 6 00000005
*Mar 7 04:21:14.227: Attribute 1 5 7461631A
*Mar 7 04:21:14.227: Attribute 26 16
000001370B0AFD11
*Mar 7 04:21:14.227: Attribute 26 58
0000013701341401
*Mar 7 04:21:14.227: Attribute 6 6 00000002
*Mar 7 04:21:14.227: Attribute 7 6 00000001
*Mar 7 04:21:14.239: RADIUS: Received from id 116
10.200.20.245:1645,
Access-Accept, len 116
*Mar 7 04:21:14.239: Attribute 7 6 00000001
*Mar 7 04:21:14.239: Attribute 6 6 00000002
*Mar 7 04:21:14.239: Attribute 25 32 64080750
*Mar 7 04:21:14.239: Attribute 26 40
000001370C223440
*Mar 7 04:21:14.239: Attribute 26 12
000001370A06144E
*Mar 7 04:21:14.239: AAA/AUTHEN (2474402925): status =
PASS
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP: Authorize LCP
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP (2434357606):
Port='Virtual-Access1' list='' service=NET
*Mar 7 04:21:14.243: AAA/AUTHOR/LCP: V11 (2434357606)
user='tac'
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP (2434357606):
send AV service=ppp
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP (2434357606):
send AV protocol=lcp
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP (2434357606):
found list "default"
*Mar 7 04:21:14.243: V11 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: V11 AAA/AUTHOR (2434357606): Post
authorization
status = PASS_REPL
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP: Processing AV
service=ppp
*Mar 7 04:21:14.243: V11 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar 7 04:21:14.243: V11 MS-CHAP: O SUCCESS id 20 len 4
*Mar 7 04:21:14.243: V11 PPP: Phase is UP [0 sess, 0
```



```
load]
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM: (0): Can we
start IPCP?
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM (1553311212):
Port='Virtual-Access1' list='' service=NET
*Mar 7 04:21:14.247: AAA/AUTHOR/FSM: V1 (1553311212)
user='tac'
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM (1553311212):
send AV service=ppp
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM (1553311212):
send AV protocol=ip
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM (1553311212):
found list "default"
*Mar 7 04:21:14.247: V1 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: V1 AAA/AUTHOR (1553311212): Post
authorization
status = PASS_REPL
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM: We can start
IPCP
*Mar 7 04:21:14.247: V1 IPCP: O CONFREQ [Not
negotiated] id 4 len 10
*Mar 7 04:21:14.247: V1 IPCP: Address 172.16.10.100
(0x0306AC100A64)
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM: (0): Can we
start CCP?
*Mar 7 04:21:14.247: V1 AAA/AUTHOR/FSM (3663845178):
Port='Virtual-Access1' list='' service=NET
*Mar 7 04:21:14.251: AAA/AUTHOR/FSM: V1 (3663845178)
user='tac'
*Mar 7 04:21:14.251: V1 AAA/AUTHOR/FSM (3663845178):
send AV service=ppp
*Mar 7 04:21:14.251: V1 AAA/AUTHOR/FSM (3663845178):
send AV protocol=ccp
*Mar 7 04:21:14.251: V1 AAA/AUTHOR/FSM (3663845178):
found list "default"
*Mar 7 04:21:14.251: V1 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: V1 AAA/AUTHOR (3663845178): Post
authorization
status = PASS_REPL
*Mar 7 04:21:14.251: V1 AAA/AUTHOR/FSM: We can start
CCP
*Mar 7 04:21:14.251: V1 CCP: O CONFREQ [Closed] id 3
len 10
*Mar 7 04:21:14.251: V1 CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.523: V1 CCP: I CONFREQ [REQsent] id 5
len 10
*Mar 7 04:21:14.523: V1 CCP: MS-PPC supported bits
0x010000F1
(0x1206010000F1)
*Mar 7 04:21:14.523: V1 MPPE: don't understand all
options, NAK
*Mar 7 04:21:14.523: V1 AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar 7 04:21:14.523: V1 AAA/AUTHOR/FSM: Processing AV
```

```
service=ppp
*Mar 7 04:21:14.523: Vil AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1kl}
111
*Mar 7 04:21:14.523: Vil AAA/AUTHOR/FSM: Succeeded
*Mar 7 04:21:14.523: Vil CCP: O CONFNAK [REQsent] id 5
len 10
*Mar 7 04:21:14.523: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.607: Vil IPCP: I CONFREQ [REQsent] id 6
len 34
*Mar 7 04:21:14.607: Vil IPCP: Address 0.0.0.0
(0x030600000000)
*Mar 7 04:21:14.607: Vil IPCP: PrimaryDNS 0.0.0.0
(0x810600000000)
*Mar 7 04:21:14.607: Vil IPCP: PrimaryWINS 0.0.0.0
(0x820600000000)
*Mar 7 04:21:14.607: Vil IPCP: SecondaryDNS 0.0.0.0
(0x830600000000)
*Mar 7 04:21:14.607: Vil IPCP: SecondaryWINS 0.0.0.0
(0x840600000000)
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1kl}
111
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar 7 04:21:14.607: Vil AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar 7 04:21:14.607: Vil IPCP: Pool returned
172.16.10.1
*Mar 7 04:21:14.607: Vil IPCP: O CONFREQ [REQsent] id 6
len 28
*Mar 7 04:21:14.607: Vil IPCP: PrimaryDNS 0.0.0.0
(0x810600000000)
*Mar 7 04:21:14.611: Vil IPCP: PrimaryWINS 0.0.0.0
(0x820600000000)
*Mar 7 04:21:14.611: Vil IPCP: SecondaryDNS 0.0.0.0
(0x830600000000)
*Mar 7 04:21:14.611: Vil IPCP: SecondaryWINS 0.0.0.0
(0x840600000000)
*Mar 7 04:21:14.675: Vil IPCP: I CONFACK [REQsent] id 4
len 10
*Mar 7 04:21:14.675: Vil IPCP: Address 172.16.10.100
(0x0306AC100A64)
*Mar 7 04:21:14.731: Vil CCP: I CONFACK [REQsent] id 3
len 10
*Mar 7 04:21:14.731: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.939: Vil CCP: I CONFREQ [ACKrcvd] id 7
len 10
*Mar 7 04:21:14.939: Vil CCP: MS-PPC supported bits
0x01000020
(0x120601000020)
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM: Processing AV
service=ppp
*Mar 7 04:21:14.939: Vil AAA/AUTHOR/FSM: Processing AV
```

```
mschap_mppe_keys*1p1T11=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: Vll AAA/AUTHOR/IPCP: Processing AV
service=ppp
*Mar 7 04:21:15.267: Vll AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=lv101~11a1W11151\1V1M1#11Z1`1k1}
111
*Mar 7 04:21:15.267: Vll AAA/AUTHOR/IPCP: Processing AV
addr*172.16.10.1
*Mar 7 04:21:15.267: Vll AAA/AUTHOR/IPCP: Authorization
succeeded
*Mar 7 04:21:15.267: Vll AAA/AUTHOR/IPCP: Done.
Her address 172.16.10.1, we want 172.16.10.1
*Mar 7 04:21:15.271: Vll IPCP: O CONFACK [ACKrcvd] id 9
len 10
*Mar 7 04:21:15.271: Vll IPCP: Address 172.16.10.1
(0x0306AC100A01)
*Mar 7 04:21:15.271: Vll IPCP: State is Open
*Mar 7 04:21:15.271: Vll IPCP: Install route to
172.16.10.1
*Mar 7 04:21:22.571: Vll LCP: I ECHOREP [Open] id 1 len
12 magic
0x35BE1CB0
*Mar 7 04:21:22.571: Vll LCP: Received id 1, sent id 1,
line up
*Mar 7 04:21:30.387: Vll LCP: I ECHOREP [Open] id 2 len
12 magic
0x35BE1CB0
*Mar 7 04:21:30.387: Vll 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 Vll tac estabd 00:00:31
%No active PPPoE tunnels
angela#

*Mar 7 04:21:40.471: Vll LCP: I ECHOREP [Open] id 3 len
12 magic
0x35BE1CB0
*Mar 7 04:21:40.471: Vll LCP: Received id 3, sent id 3,
line up
*Mar 7 04:21:49.887: Vll LCP: I ECHOREP [Open] id 4 len
12 magic
0x35BE1CB0
*Mar 7 04:21:49.887: Vll 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: Vll LCP: I ECHOREP [Open] id 5 len
12 magic
0x35BE1CB0

```

```

*Mar 7 04:21:59.859: Vll 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: Vll LCP: I ECHOREP [Open] id 6 len
12 magic
0x35BE1CB0
*Mar 7 04:22:09.879: Vll 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: Vll LCP: I ECHOREP [Open] id 7 len
12 magic
0x35BE1CB0
*Mar 7 04:22:39.863: Vll 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: Vll LCP: I ECHOREP [Open] id 10
len 12 magic 0x35BE1CB0
*Mar 7 04:23:09.887: Vll LCP: Received id 10, sent id
10, line up

```

다음을 확인합니다. 이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다. 특정 show 명령은 show 명령 출력의 분석을 볼 수 있는 출력 인터프리터 도구에서 지원됩니다.

- show vpdn - VPDN의 활성 L2F(Level 2 Forwarding) 프로토콜 터널 및 메시지 식별자에 대한 정보를 표시합니다.

show vpdn을 사용할 수도 있습니다. 다른 VPDN별 show 명령을 확인합니다. **문제 해결**이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. **문제 해결 명령** 특정 show 명령은 show 명령 출력의 분석을 볼 수 있는 출력 인터프리터 도구에서 지원됩니다. 참고: debug 명령을 실행하기 전에 **디버그 명령에 대한 중요 정보를 참조하십시오**.

- debug aaa authentication - AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- debug aaa authorization - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.
- debug ppp negotiation - PPP 시작 중에 전송된 PPP 패킷을 표시합니다. 여기서 PPP 옵션은 협상됩니다.
- debug ppp authentication - CHAP(Challenge Authentication Protocol) 패킷 교환 및 PAP(Password Authentication Protocol) 교환을 비롯한 인증 프로토콜 메시지를 표시합니다.
- debug radius - RADIUS와 관련된 자세한 디버깅 정보를 표시합니다. 인증이 작동하지만 MPPE 암호화에 문제가 있는 경우 아래 debug 명령 중 하나를 사용합니다.
- debug ppp mppe packet - 모든 수신 발신 MPPE 트래픽을 표시합니다.
- debug ppp mppe event - 키 MPPE 발생을 표시합니다.
- debug ppp mppe detailed - 자세한 MPPE 정보를 표시합니다.
- debug vpdn l2x-packets - L2F 프로토콜 헤더 및 상태에 대한 메시지를 표시합니다.
- debug vpdn events - 일반 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- debug vpdn errors - 터널이 설정되지 않도록 하는 오류 또는 설정된 터널을 닫도록 하는 오류를 표시합니다.
- debug vpdn packets - 교환된 각 프로토콜 패킷을 표시합니다. 이 옵션을 사용하면 디버그 메시지가 많이 발생할 수 있으며 일반적으로 단일 활성 세션이 있는 디버그 새시에서만 사용해야 합니다.

스플릿 터널링 게이트웨이 라우터가 ISP 라우터라고 가정하겠습니다. PC에서 PPTP 터널이 나타나면 PPTP 경로가 이전 기본값보다 높은 메트릭으로 설치되므로 인터넷 연결이 끊어집니다. 이를 해결하려면 Microsoft 라우팅을 수정하여 기본값을 삭제하고 기본 경로를 다시 설치합니다(PPTP 클라이언트가 할당된 IP 주소를 알아야 합니다. 현재 예에서는 172.16.10.1입니다).

```
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
```

클라이언트가 암호화용으로 구성되지 않은 경우 PPTP 세션에 사용된 전화 접속 연결의 Security(보안) 탭 아래에서 사용자 인증 매개변수를 정의할 수 있습니다. 예를 들어 PAP, CHAP, MS-CHAP 또는 Windows 도메인 로그인 가능합니다. VPN 연결의 Properties 섹션에서 No Encryption Allowed(암호화가 필요한 경우 서버 연결 해제) 옵션을 선택한 경우 클라이언트에 PPTP 오류 메시지가 표시될 수 있습니다.

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
클라이언트가 암호화에 대해 구성되어 있고 라우터가 구성되지 않은 경우 PC에서 다음
메시지를 확인할 수 있습니다.
Registering your computer on the network..
Error 742: The remote computer doesnot support the required data
encryption type.
On the Router:
*Mar 9 01:06:00.868: Vi2 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar 9 01:06:00.868: Vi2 CCP: MS-PPC supported bits 0x010000B1
(0x1206010000B1)
*Mar 9 01:06:00.868: Vi2 LCP: O PROTREQ [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 CONFREQ [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
establd 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 establd 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

```

[PC가 암호화를 위해 구성된 경우 MS-CHAP 비활성화](#) PC에서 다음 메시지를 확인할 수 있습니다.

```

The current encryption selection requires EAP or some version of
MS-CHAP logon security methods.
사용자가 잘못된 사용자 이름 또는 비밀번호를 지정하면 다음 출력이 표시됩니다.PC:
Verifying Username and Password..
Error 691: Access was denied because the username and/or password
was invalid on the domain.

```

라우터에서:

```

*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

```

[RADIUS 서버가 통신할 수 없는 경우](#) 라우터에서 다음 출력을 볼 수 있습니다.

```

*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
```

관련 정보

- [PPTP\(MPPE 포함\)](#)
- [PPTP 기술 페이지](#)
- [VPDN 이해](#)
- [반지름 이해](#)
- [Windows 라우터 PPTP 인증을 위한 CiscoSecure ACS 구성](#)
- [기술 지원 및 문서 - Cisco Systems](#)