

도메인 또는 DNIS 정보 없이 사용자별 VPDN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[RADIUS 서버 구성](#)

[다음을 확인합니다.](#)

[샘플 show 명령 출력](#)

[문제 해결](#)

[문제 해결 명령](#)

[디버그 출력 샘플](#)

[관련 정보](#)

소개

이 문서에서는 도메인 또는 DNIS 정보가 없는 사용자별 VPDN에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.1(4) 이상
- Cisco IOS Software 릴리스 12.1(4)T 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

[표기 규칙](#)

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

[배경 정보](#)

VPDN(Virtual Private Dial-up Network) 시나리오에서 NAS(Network Access Server)(L2TP Access Concentrator 또는 LAC)는 사용자별 정보를 기반으로 LNS(Home Gateway)에 대한 VPDN 터널을 설정합니다. 이 VPDN 터널은 L2F(Level 2 Forwarding) 또는 L2TP(Layer 2 Tunneling Protocol)일 수 있습니다. 사용자가 VPDN 터널을 사용해야 하는지 확인하려면 다음을 확인하십시오.

- 도메인 이름이 사용자 이름의 일부로 포함되는지 여부. 예를 들어, 사용자 이름 tunnelme@cisco.com을 사용하여 NAS는 이 사용자를 cisco.com의 터널로 전달합니다.
- DNIS(Dialed Number Information Service)입니다. 이 번호는 전화를 건 번호에 따라 착신 전환입니다. 즉, NAS는 특정 전화 번호로 모든 통화를 해당 터널로 전달할 수 있습니다. 예를 들어 수신 전화의 번호 5551111이 있는 경우 통화를 VPDN 터널로 전달할 수 있으며 552222로의 통화는 전달되지 않습니다. 이 기능을 사용하려면 Telco 네트워크가 전화 번호 정보를 제공해야 합니다.

VPDN 컨피그레이션에 대한 자세한 내용은 VPDN [이해를 참조하십시오](#).

경우에 따라 VPDN 터널을 사용자 이름 단위로 입력해야 할 수도 있고, 도메인 이름을 전혀 사용하지 않아도 될 수도 있습니다. 예를 들어 사용자 ciscouser는 **cisco.com**으로 터널링할 수 있고 다른 사용자는 NAS에서 로컬로 종료할 수 있습니다.

참고: 이 사용자 이름은 이전 예와 같이 도메인 정보를 포함하지 않습니다.

VPDN 사용자별 컨피그레이션 기능은 라우터가 AAA 서버에 처음 연결할 때 AAA(Authentication, Authorization, and Accounting) 서버에 전체 구조적 사용자 이름을 전송합니다. 이를 통해 Cisco IOS 소프트웨어는 공통 도메인 이름 또는 DNIS를 사용하는 개별 사용자의 터널 특성을 사용자 정의할 수 있습니다.

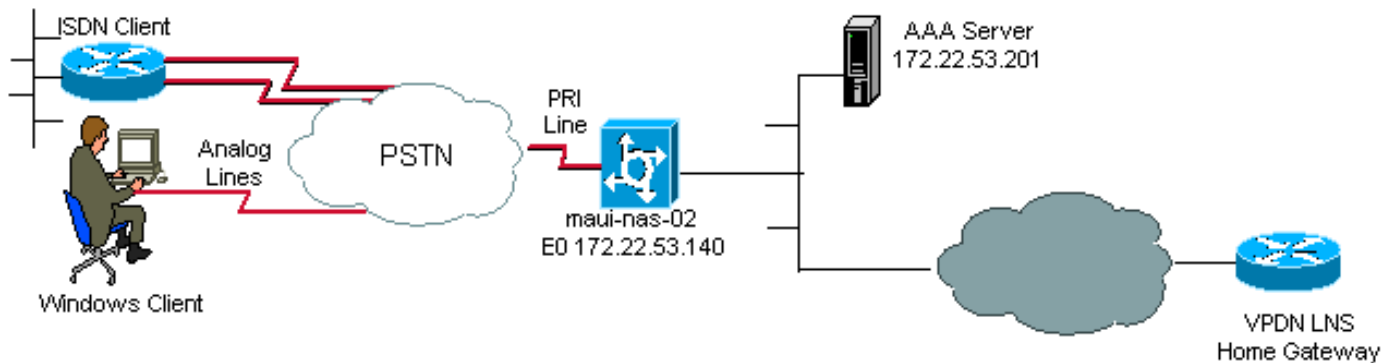
[구성](#)

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구\(등록된 고객만 해당\)](#)를 사용합니다.

[네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

NAS(LAC)에서 사용자별 VPDN을 지원하는 데 필요한 유일한 VPDN 명령은 `vpdn enable` 및 `vpdn authen-before-forward` 전역 구성 명령입니다. `vpdn authen-before-forward` 명령은 전달 결정을 내리기 전에 NAS(LAC)에 전체 사용자 이름을 인증하도록 지시합니다. 그런 다음 이 개별 사용자에게 대해 AAA 서버가 반환한 정보를 기반으로 VPDN 터널이 설정됩니다. AAA 서버에서 반환되는 VPDN 정보가 없으면 사용자가 로컬로 종료됩니다. 이 섹션의 컨피그레이션에는 사용자 이름에 도메인 정보가 없는 터널을 지원하는 데 필요한 명령이 표시됩니다.

참고: 이 구성은 포괄적이지 않습니다. 관련 VPDN, 인터페이스 및 AAA 명령만 포함됩니다.

참고: 이 문서에서는 가능한 모든 터널 프로토콜과 AAA 프로토콜에 대해 설명합니다. 따라서 이 컨피그레이션은 AAA RADIUS 서버가 있는 L2TP 터널을 구현합니다. 여기에서 설명한 원칙과 컨피그레이션을 조정하여 다른 터널 유형 또는 AAA 프로토콜을 구성합니다.

이 문서에서는 다음 구성을 사용합니다.

• VPDN NAS(LAC)

VPDN NAS(LAC)

```

aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.

```

RADIUS 서버 구성

다음은 CSU(Cisco Secure for Unix) RADIUS 서버의 사용자 컨피그레이션입니다.

1. NAS에서 로컬로 종료될 사용자:

```
user1 Password = "cisco"
Service-Type = Framed-User
```

2. VPDN 세션을 설정해야 하는 사용자:

```
user2 Password = "cisco"
Service-Type = Framed-User,
Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
Cisco-AVPair = "vpdn:tunnel-type=l2tp"
```

NAS(LAC)는 Cisco-AVPair VPDN에 지정된 특성을 사용하여 VPDN 터널을 홈 게이트웨이에 삽입합니다. NAS에서 VPDN 터널을 허용하도록 홈 게이트웨이를 구성해야 합니다.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show caller user** - 사용된 TTY 회선, 비동기 인터페이스(shelf, slot 또는 port), DS0 채널 번호, 모뎀 번호, 할당된 IP 주소, PPP 및 PPP 번들 매개변수 등 특정 사용자에게 대한 매개변수를 표시합니다. 사용 중인 버전의 Cisco IOS 소프트웨어가 이 명령을 지원하지 않는 경우 **show user** 명령을 사용합니다.
- **show vpdn** - 활성 L2F 및 L2TP 프로토콜 터널과 VPDN의 메시지 식별자에 대한 정보를 표시합니다.

샘플 show 명령 출력

통화가 연결되면 **show caller user username** 명령 및 **show vpdn** 명령을 사용하여 통화가 성공했는지 확인합니다. 샘플 출력은 다음과 같습니다.

```
maui-nas-02#show caller user vpdn_authen
```

```
User: vpdn_authen, line tty 12, service Async
  Active time 00:09:01, Idle time 00:00:05
Timeouts:
  Absolute Idle Idle
           Session Exec
Limits:    - - 00:10:00
Disconnect in: - - -
TTY: Line 12, running PPP on As12
DS0: (slot/unit/channel)=0/0/5
Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: Ready, Active, No Exit Banner, Async Interface Active
       HW PPP Support Active
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
              Modem Callout, Modem RI is CD,
              Line is permanent async interface, Integrated Modem
Modem State: Ready

User: vpdn_authen, line As12, service PPP
  Active time 00:08:58, Idle time 00:00:05
Timeouts:
  Absolute Idle
```

```

Limits:          -          -
Disconnect in:  -          -
PPP: LCP Open, CHAP (<- AAA)
IP: Local 172.22.53.140
VPDN: NAS , MID 4, MID Unknown
      HGW , NAS CLID 0, HGW CLID 0, tunnel open
!--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no buffer 0 input
errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0 output errors, 0
collisions, 0 interface resets maui-nas-02#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name      State Remote Address  Port  Sessions
6318  3      HGW                est   172.22.53.141   1701  1

LocID RemID TunID Intf          Username      State Last Chg Fastswitch
4      3      6318 As12        vpdn_authen  est   00:09:33 enabled
!--- The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active
PPTP tunnels %No active PPPoE tunnel

```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

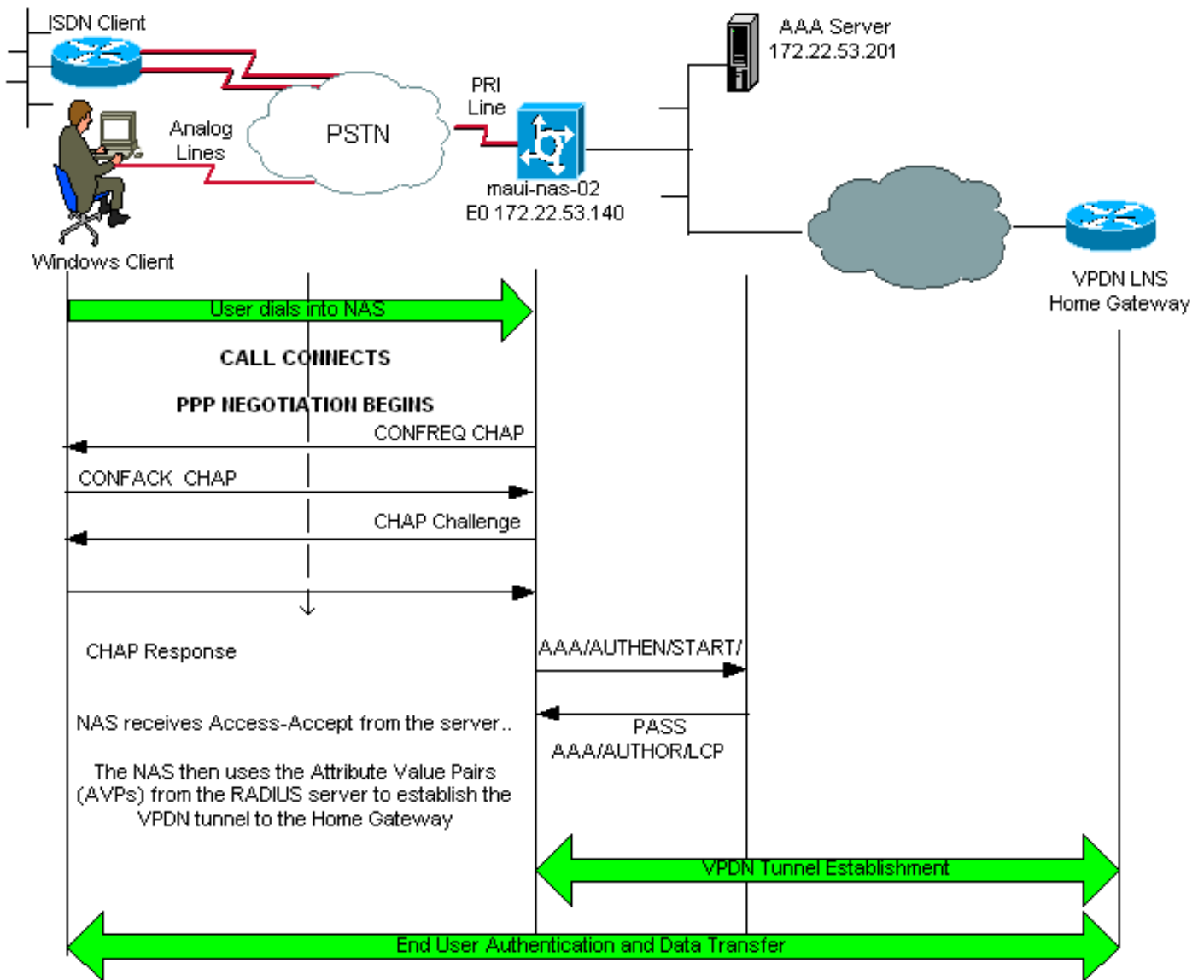
문제 해결 명령

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오.](#)

- **debug ppp authentication**—PPP 인증 프로토콜 메시지를 표시하고 CHAP(Challenge Handshake Authentication Protocol) 패킷 교환 및 PAP>Password Authentication Protocol) 교환을 포함합니다.
- **debug aaa authentication**—AAA/RADIUS 인증에 대한 정보를 표시합니다.
- **debug aaa authorization**—AAA/RADIUS 권한 부여에 대한 정보를 표시합니다.
- **debug radius**—RADIUS와 관련된 자세한 디버깅 정보를 표시합니다. Output Interpreter [틀\(동특된](#) 고객만 해당)을 사용하여 디버그 환경 메시지를 디코딩합니다. 예를 들어 [샘플 디버그 출력](#) 섹션을 참조하십시오. 협상할 특성을 결정하려면 디버그 환경의 정보를 사용합니다.
- **debug tacacs** - TACACS+와 관련된 자세한 디버깅 정보를 표시합니다.
- **debug vpdn event** - VPDN에 대한 일반 터널 설정 또는 종료의 일부인 L2x 오류 및 이벤트를 표시합니다.
- **debug vpdn error** - VPDN 프로토콜 오류를 표시합니다.
- **debug vpdn l2x-event** - VPDN에 대한 일반 터널 설정 또는 종료의 일부인 자세한 L2x 오류 및 이벤트를 표시합니다.
- **debug vpdn l2x-error** - VPDN L2x 프로토콜 오류를 표시합니다.

디버그 출력 샘플

다음은 성공적인 통화에 대한 디버그 출력입니다. 이 예에서는 NAS가 RADIUS 서버에서 VPDN 터널의 특성을 얻습니다.



maui-nas-02#show debug

General OS:

AAA Authentication debugging is on

AAA Authorization debugging is on

PPP:

PPP authentication 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

maui-nas-02#

*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial0:5 is now connected

to N/A N/A

!--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up

*Jan 21 19:07:55.352: As12 PPP: Treating connection as a dedicated line *Jan 21 19:07:55.352:

As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id

1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from

"vpdn_authen"

!--- Incoming CHAP response from user vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12

idb type=10 tty=12 *Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0

adapter=0 port=12 channel=0 *Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1

*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0

channel=5 *Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21

19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12'

```

rem_addr='async/81560' authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): port='Async12' list='' action=LOGIN service=PPP *Jan 21
19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct
sharecount=1 *Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736:      Attribute 4 6 AC16358C
*Jan 21 19:07:55.736:      Attribute 5 6 0000000C
*Jan 21 19:07:55.736:      Attribute 61 6 00000000
*Jan 21 19:07:55.736:      Attribute 1 13 7670646E
*Jan 21 19:07:55.736:      Attribute 30 7 38313536
*Jan 21 19:07:55.736:      Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736:      Attribute 6 6 00000002
*Jan 21 19:07:55.736:      Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740:      Attribute 6 6 00000002
*Jan 21 19:07:55.740:      Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:      Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:      Attribute 26 30 0000000901187670

```

VPDN 터널에 필요한 AVP(특성 값 쌍)는 RADIUS 서버에서 푸시됩니다. 그러나 디버그 반지름은 AVP 및 해당 값을 나타내는 코딩된 출력을 생성합니다. 위의 굵은 글꼴으로 표시된 출력을 [Output Interpreter Tool\(등록된 고객만 해당\)](#)에 붙여넣을 수 있습니다. 굵게 표시된 다음 출력은 도구에서 가져온 디코딩된 출력입니다.

```

Access-Request 172.22.53.201:1645 id 6
Attribute Type 4:  NAS-IP-Address is 172.22.53.140
Attribute Type 5:  NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1:  User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3:  CHAP-Password is (encoded)
Attribute Type 6:  Service-Type is Framed
Attribute Type 7:  Framed-Protocol is PPP
      Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6:  Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
...
...
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
!--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be
authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !---
the VPDN tunnel establishment debug output is omitted.

```

[관련 정보](#)

- [VPDN 이해](#)
- [가상 사설전화 접속 네트워크 구성](#)
- [RADIUS를 사용하여 레이어 2 터널 프로토콜 인증을 구성하는 방법](#)
- [TACACS+를 사용하여 레이어 2 터널 프로토콜 인증을 구성하는 방법](#)
- [액세스 기술 지원 페이지](#)
- [Technical Support - Cisco Systems](#)