

VPDN에 대한 TACACS+ 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[TACACS+ 서버 구성](#)

[라우터 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[샘플 디버그 출력](#)

[관련 정보](#)

소개

VPDN(Virtual Private Dial-Up Network)을 사용하면 프라이빗 네트워크 다이얼인 서비스가 원격 액세스 서버(LAC[L2TP Access Concentrator])로 정의됩니다. PPP(Point-to-Point Protocol) 클라이언트가 LAC에 전화를 걸 때 LAC는 해당 클라이언트의 L2TP 네트워크 서버(LNS)에 해당 PPP 세션을 전달해야 한다고 결정하며, 이 경우 사용자를 인증하고 PPP 협상을 시작합니다. PPP 설정이 완료되면 모든 프레임이 LAC를 통해 클라이언트와 LNS로 전송됩니다.

이 샘플 컨피그레이션을 사용하면 VPDN(Virtual Private Dial-Up Networks)과 함께 TACACS+ 인증을 사용할 수 있습니다. LAC는 TACACS+ 서버를 쿼리하고, 사용자를 전달할 LNS를 결정하고, 적절한 터널을 설정합니다.

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

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 Secure ACS for UNIX 버전 2.x.x 이상 또는 TACACS+ 프리웨어
- Cisco IOS® Software 릴리스 11.2 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 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 필요한 정보를 제공합니다.

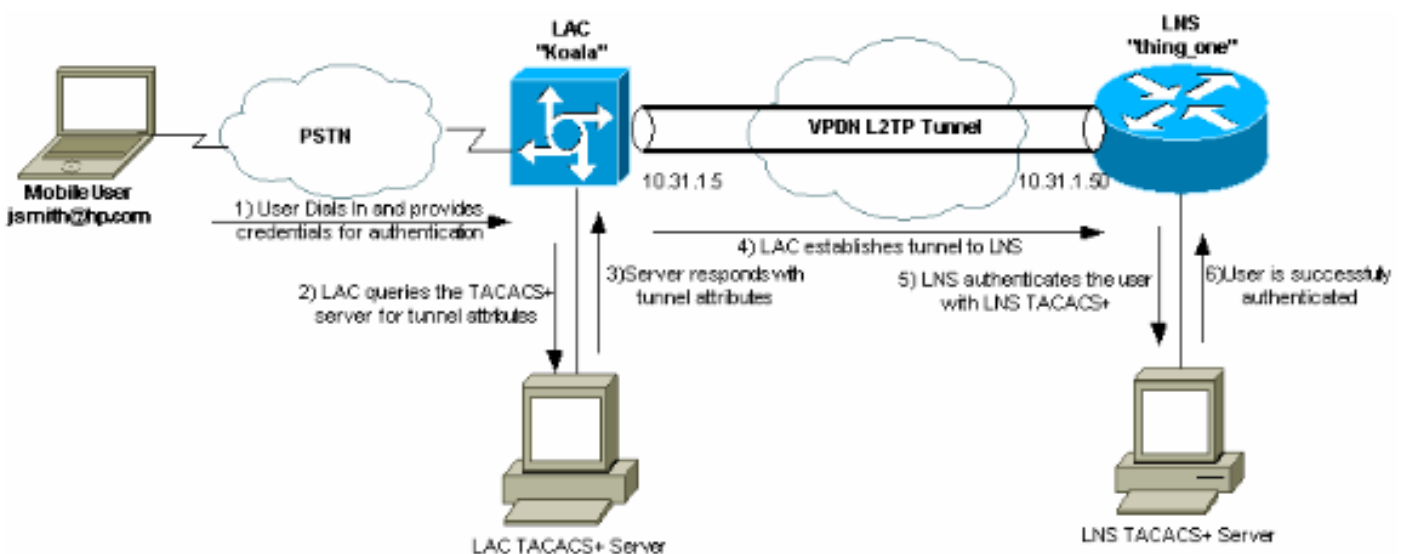
이 예에서는 "test"라는 비밀번호가 있는 "jsmith@hp.com"입니다. "jsmith@hp.com"이 ISP 라우터로 전화를 걸면 ISP 라우터는 "hp.com" 사용자 ID를 ISP TACACS+ 서버로 전송합니다. ISP 서버는 "hp.com" 사용자 ID를 찾아 터널 ID("isp"), 홈 게이트웨이(HGW) 라우터의 IP 주소(10.31.1.50), 네트워크 액세스 서버(NAS) 비밀번호("hello"), 게이트웨이 비밀번호("there")를 ISP 라우터로 다시 보냅니다.

ISP 라우터는 터널을 시작하고 HGW 라우터에 연결합니다. 이 라우터는 사용자 ID "hp-gw"("there") 및 사용자 ID "isp"("hello")의 비밀번호를 HGW TACACS+ 서버로 전달합니다. 터널이 설정되면 ISP 라우터는 전화를 거는 사용자의 사용자 ID("jsmith@hp.com") 및 비밀번호("test")를 HGW 라우터로 전달합니다. 이 사용자는 HGW 서버에서 인증됩니다. 이 문서의 샘플 컨피그레이션에서는 ISP 라우터 호스트 이름이 "코알라"이고 HGW 라우터 호스트 이름은 "thing_one"입니다.

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

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



TACACS+ 서버 구성

이 문서에서는 여기에 표시된 서버 구성을 사용합니다.

- [TACACS+ 프리웨어](#)
- [UNIX 2.x.x용 Cisco Secure ACS](#)

[TACACS+ 프리웨어](#)

```
!--- This user is on the ISP TACACS+ server. !--- The profile includes the Tunnel ID ("isp"),
the IP address !--- of the Peer (10.31.1.50), !--- and the passwords used to authenticate the
tunnel. !--- The ISP uses these attributes to establish the tunnel. user = hp.com { service = ppp
protocol = vpdn { tunnel-id = isp ip-addresses = "10.31.1.50" nas-password = "hello" gw-password
= "there" } } !--- The next three users are on the HGW server. user = isp { chap = cleartext
"hello" service = ppp protocol = ip { default attribute = permit } } user = hp-gw { chap =
cleartext "there" service = ppp protocol = ip { default attribute = permit } } user =
jsmith@hp.com { chap = cleartext "test" service = ppp protocol = ip { default attribute = permit
} }
```

[UNIX 2.x.x용 Cisco Secure ACS](#)

```
!--- This user is on the ISP server. # ./ViewProfile -p 9900 -u hp.com User Profile Information
user = hp.com{ profile_id = 83 profile_cycle = 1 service=ppp { protocol=vpdn { set tunnel-id=isp
set ip-addresses="10.31.1.50" set nas-password="hello" set gw-password="there" } protocol=lcp {
} } } !--- The next three users are on the HGW server. !--- The next two usernames are used to
authenticate the LAC !--- during tunnel initialization. # ./ViewProfile -p 9900 -u isp User
Profile Information user = isp{ profile_id = 84 profile_cycle = 1 password = chap "*****"
service=ppp { protocol=ip { default attribute=permit } protocol=lcp { } } } # ./ViewProfile -p
9900 -u hp-gw User Profile Information user = hp-gw{ profile_id = 82 profile_cycle = 1 password
= chap "*****" service=ppp { protocol=ip { default attribute=permit } protocol=lcp { } } } !-
-- This username is used to authenticate the end user !--- after the tunnel is established. #
./ViewProfile -p 9900 -u jsmith@hp.com User Profile Information user = jsmith@hp.com{ profile_id
= 85 profile_cycle = 1 password = chap "*****" service=ppp { protocol=ip { default
attribute=permit } protocol=lcp { } } }
```

[라우터 컨피그레이션](#)

이 문서에서는 여기에 표시된 구성을 사용합니다.

- [ISP 라우터](#)
- [HGW 라우터](#)

ISP 라우터 컨피그레이션

```
koala#show running config
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname koala
!
```

```
aaa new-model
aaa authentication ppp default tacacs+ none
aaa authorization network tacacs+ none
aaa accounting network start-stop tacacs+

enable password ww
!
!--- VPDN is enabled. vpdn enable
!
interface Ethernet0
ip address 10.31.1.5 255.255.255.0
!
interface Serial0
shutdown
!
interface Serial1
shutdown
!
interface Async1
ip unnumbered Ethernet0
encapsulation ppp
async mode dedicated
no cdp enable
ppp authentication chap
!
ip default-gateway 10.31.1.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!
!--- Specify the TACACS server information on the NAS.
tacacs-server host 171.68.120.194
tacacs-server key cisco
no tacacs-server directed-request
snmp-server community public RW
snmp-server enable traps config
!
line con 0
password ww
line 1 16
password ww
autoselect ppp
modem InOut
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
line aux 0
line vty 0 4
exec-timeout 0 0
password ww
!
end
```

HGW 라우터 컨피그레이션

```
thing_one#show running config
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
```

```

no service udp-small-servers
no service tcp-small-servers
!
hostname thing_one
!
aaa new-model
aaa authentication ppp default tacacs+ none
aaa authorization network tacacs+ none
enable password ww
!
!--- Enable VPDN. vpdn enable
!--- Specify the remote host ("isp" on the network
access server) !--- and the local name ("hp-gw" on the
home gateway) to use to authenticate. !--- Also specify
the virtual template to use. !--- The local name and the
remote host name must match !--- the ones in the TACACS
server. vpdn incoming isp hp-gw virtual-template 1
!
interface Loopback0
shutdown
!
interface Ethernet0
ip address 10.31.1.50 255.255.255.0
!
interface Virtual-Template1
!--- Create a virtual template interface. ip unnumbered
Ethernet0
!--- Un-number the Virtual interface to an available LAN
interface. peer default ip address pool async
!--- Use the pool "async" to assign the IP address for
incoming connections. ppp authentication chap
!--- Use CHAP authentication for the incoming
connection. ! interface Serial0 shutdown ! interface
Serial1 shutdown ! ip local pool async 15.15.15.15 no ip
classless ip route 0.0.0.0 0.0.0.0 10.31.1.1 ! tacacs-
server host 171.68.118.101
no tacacs-server directed-request
tacacs-server key cisco
!--- Specify the TACACS+ server information on the NAS.
! line con 0 exec-timeout 0 0 line 1 8 line aux 0 line
vty 0 4 ! end

```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

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 aaa authentication** - AAA(authentication, authorization, and accounting)/TACACS+ 인 증에 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 tacacs+**—TACACS+와 관련된 자세한 디버깅 정보를 표시합니다.
- **debug vpdn errors** - PPP 터널이 설정되지 않도록 하는 오류 또는 설정된 터널이 닫히는 오류를 표시합니다.
- **debug vpdn events** - 일반 PPP 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- **debug vpdn l2f-errors** - 레이어 2 설정을 방지하거나 정상적인 작동을 방지하는 레이어 2 프로토콜 오류를 표시합니다.
- **debug vpdn l2f-events** - Layer 2에 대한 일반 PPP 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- **debug vpdn l2f-packets** - Layer 2 Forwarding 프로토콜 헤더 및 상태에 대한 메시지를 표시합니다.
- **debug vpdn packets** - VPDN에 대한 일반 터널 설정 또는 종료의 일부인 L2TP(Layer 2 Tunnel Protocol) 오류 및 이벤트를 표시합니다.
- **debug vtemplate** - 가상 액세스 인터페이스가 가상 템플릿에서 복제될 때부터 통화가 종료될 때 가상 액세스 인터페이스가 중단될 때까지 가상 액세스 인터페이스에 대한 복제 정보를 표시합니다.

샘플 디버그 출력

이러한 디버그는 참조용으로 제공됩니다.

- [ISP 라우터 정상 디버그](#)
- [HGW 라우터 정상 디버그](#)
- [ISP 라우터에서 연결 실패 디버깅](#)
- [HGW 라우터의 실패한 연결에 대한 디버깅](#)

ISP 라우터 정상 디버그

```

koala#show debug
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
VPN events debugging is on
VPN errors debugging is on
koala#
%LINK-3-UPDOWN: Interface Async1, changed state to up
15:04:47: VPDN: Looking for tunnel -- hp.com --
15:04:47: AAA/AUTHEN: create_user (0x15FA80) user='hp.com' ruser=''
      port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): user='hp.com'
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): send AV service=ppp
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): send AV protocol=vpdn
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): Method=TACACS+
15:04:47: AAA/AUTHOR/TAC+: (2445181346): user=hp.com
15:04:47: AAA/AUTHOR/TAC+: (2445181346): send AV service=ppp
15:04:47: AAA/AUTHOR/TAC+: (2445181346): send AV protocol=vpdn
15:04:47: TAC+: (2445181346): received author response status = PASS_ADD

```

```
15:04:47: AAA/AUTHOR (2445181346): Post authorization status = PASS_ADD
15:04:47: AAA/AUTHOR/VPDN: Processing AV service=ppp
15:04:47: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
15:04:47: AAA/AUTHOR/VPDN: Processing AV tunnel-id=isp
15:04:47: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.50
15:04:47: AAA/AUTHOR/VPDN: Processing AV nas-password=hello
15:04:47: AAA/AUTHOR/VPDN: Processing AV gw-password=there
15:04:47: VPDN: Get tunnel info with NAS isp GW hp.com, IP 10.31.1.50
!--- The TACACS+ server returns the attributes the !--- NAS should use for the tunnel. !--- The
tunnel-id is "ISP" and the IP address of HGW is 10.31.1.50. 15:04:47: AAA/AUTHEN: free_user
(0x15FA80) user='hp.com' ruser='' port='Async1' rem_addr='' authen_type=NONE service=LOGIN
priv=0 15:04:47: VPDN: Forward to address 10.31.1.50 15:04:47: As1 VPDN: Forwarding... 15:04:47:
AAA/AUTHEN: create_user (0x118008) user='jsmith@hp.com' ruser='' port='Async1' rem_addr='async'
authen_type=CHAP service=PPP priv=1 15:04:47: As1 VPDN: Bind interface direction=1 15:04:47: As1
VPDN: jsmith@hp.com is forwarded
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
15:04:49: AAA/ACCT: NET acct start. User jsmith@hp.com, Port Async1: Async1
!--- User finishes and disconnects. %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to down %LINK-5-CHANGED: Interface Async1, changed state to reset 15:05:27: As1
VPDN: Cleanup 15:05:27: As1 VPDN: Reset 15:05:27: As1 VPDN: Reset 15:05:27: As1 VPDN: Unbind
interface 15:05:27: AAA/ACCT: Network acct stop. User jsmith@hp.com, Port Async1: task_id=2
timezone=UTC service=vpdn bytes_in=1399 bytes_out=150 paks_in=27 paks_out=9 elapsed_time=38
%LINK-3-UPDOWN: Interface Async1, changed state to down 15:05:30: AAA/AUTHEN: free_user
(0x118008) user='jsmith@hp.com' ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1 koala#
```

HGW 라우터 정상 디버그

```
thing_one#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
AAA Accounting debugging is on
```

```
VPN:
```

```
VPN events debugging is on
```

```
VPN errors debugging is on
```

```
VTEMPLATE:
```

```
Virtual Template debugging is on
```

```
thing_one#
```

```
15:04:46: AAA/AUTHEN: create_user (0x15E6E0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: TAC+: ver=192 id=969200103 received AUTHEN status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15E6E0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN (3252085483): status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15CBEC) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN: create_user (0x15F1B8) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN/START (3897539709): port='' list='default'
action=LOGIN service=PPP
15:04:46: AAA/AUTHEN/START (3897539709): found list default
15:04:46: AAA/AUTHEN/START (3897539709): Method=TACACS+
15:04:46: TAC+: send AUTHEN/START packet ver=193 id=3897539709
15:04:46: TAC+: ver=192 id=3897539709 received AUTHEN status = GETPASS
15:04:46: AAA/AUTHEN: create_user (0x15E6F0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: TAC+: ver=192 id=2306139011 received AUTHEN status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15E6F0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN (3897539709): status = PASS
15:04:46: VPDN: Chap authentication succeeded for isp
```

```
!--- The LAC ("ISP") is succesfully authenticated. 15:04:46: AAA/AUTHEN: free_user (0x15F1B8)
user='isp' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1 15:04:46: Vi1
VTEMPLATE: Reuse Vi1, recycle queue size 0 15:04:46: Vi1 VTEMPLATE: Set default settings with no
ip address 15:04:47: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c 15:04:47: Vi1 VPDN: Virtual
interface created for jsmith@hp.com 15:04:47: Vi1 VPDN: Set to Async interface 15:04:47: Vi1
VPDN: Clone from Vtemplate 1 filterPPP=0 blocking 15:04:47: Vi1 VTEMPLATE: Has a new cloneblk
vtemplate, now it has vtemplate 15:04:47: Vi1 VTEMPLATE: Undo default settings 15:04:47: Vi1
VTEMPLATE: ***** CLONE VACCESS1 ***** 15:04:47: Vi1 VTEMPLATE: Clone from
vtemplate1 interface Virtual-Access1 no ip address encap ppp ip unnum eth 0 peer default ip
address pool async ppp authen chap end %LINK-3-UPDOWN: Interface Virtual-Access1, changed state
to up 15:04:48: Vi1 VPDN: Bind interface direction=2 15:04:48: Vi1 VPDN: PPP LCP accepted sent &
rcv CONFACK 15:04:48: Vi1 VPDN: Virtual interface iteration 15:04:48: AAA/AUTHEN: create_user
(0x161688) user='jsmith@hp.com' ruser='' port='Virtual-Access1' rem_addr='async'
authen_type=CHAP service=PPP priv=1 15:04:48: AAA/AUTHEN/START (580760432): port='Virtual-
Access1' list='' action=LOGIN service=PPP 15:04:48: AAA/AUTHEN/START (580760432): using
"default" list 15:04:48: AAA/AUTHEN/START (580760432): Method=TACACS+ 15:04:48: TAC+: send
AUTHEN/START packet ver=193 id=580760432 15:04:48: Vi1 VPDN: Virtual interface iteration
15:04:49: TAC+: ver=192 id=580760432 received AUTHEN status = GETPASS !--- Authenticate user
jsmith@hp.com with the TACACS+ server. 15:04:49: AAA/AUTHEN: create_user (0x1667C0)
user='jsmith@hp.com' ruser=''
port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:49: TAC+: ver=192 id=2894253624 received AUTHEN status = PASS
15:04:49: AAA/AUTHEN: free_user (0x1667C0) user='jsmith@hp.com' ruser=''
port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:49: AAA/AUTHEN (580760432): status = PASS
15:04:49: AAA/AUTHOR/LCP Vi1: Authorize LCP
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): user='jsmith@hp.com'
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): send AV service=ppp
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): send AV protocol=lcp
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): Method=TACACS+
15:04:49: AAA/AUTHOR/TAC+: (687698354): user=jsmith@hp.com
15:04:49: AAA/AUTHOR/TAC+: (687698354): send AV service=ppp
15:04:49: AAA/AUTHOR/TAC+: (687698354): send AV protocol=lcp
15:04:49: TAC+: (687698354): received author response status = PASS_ADD
15:04:49: AAA/AUTHOR (687698354): Post authorization status = PASS_ADD
15:04:49: AAA/ACCT: NET acct start. User jsmith@hp.com, Port Virtual-Access1:
Virtual-Access1
15:04:49: AAA/AUTHOR/FSM Vi1: (0): Can we start IPCP?
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): user='jsmith@hp.com'
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): send AV service=ppp
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): send AV protocol=ip
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): Method=TACACS+
15:04:49: AAA/AUTHOR/TAC+: (3562892028): user=jsmith@hp.com
15:04:49: AAA/AUTHOR/TAC+: (3562892028): send AV service=ppp
15:04:49: AAA/AUTHOR/TAC+: (3562892028): send AV protocol=ip
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
15:04:49: TAC+: (3562892028): received author response status = PASS_ADD
15:04:49: AAA/AUTHOR (3562892028): Post authorization status = PASS_ADD
!--- IPCP negotiation begins. 15:04:49: AAA/AUTHOR/FSM Vi1: We can start IPCP 15:04:50:
AAA/AUTHOR/ICP Vi1: Start. Her address 0.0.0.0, we want 0.0.0.0 15:04:50: AAA/AUTHOR/ICP Vi1:
Processing AV service=ppp 15:04:50: AAA/AUTHOR/ICP Vi1: Processing AV protocol=ip 15:04:50:
AAA/AUTHOR/ICP Vi1: Authorization succeeded 15:04:50: AAA/AUTHOR/ICP Vi1: Done. Her address
0.0.0.0, we want 0.0.0.0 15:04:51: AAA/AUTHOR/ICP Vi1: Start. Her address 0.0.0.0, we want
15.15.15.15 15:04:51: AAA/AUTHOR/ICP Vi1: Processing AV service=ppp 15:04:51: AAA/AUTHOR/ICP
Vi1: Processing AV protocol=ip 15:04:51: AAA/AUTHOR/ICP Vi1: Authorization succeeded 15:04:51:
AAA/AUTHOR/ICP Vi1: Done. Her address 0.0.0.0, we want 15.15.15.15 15:04:51: AAA/AUTHOR/ICP
Vi1: Start. Her address 15.15.15.15, we want 15.15.15.15 15:04:51: AAA/AUTHOR/ICP: Virtual-
Access1: (3193852847): user='jsmith@hp.com' 15:04:51: AAA/AUTHOR/ICP: Virtual-Access1:
(3193852847): send AV service=ppp 15:04:51: AAA/AUTHOR/ICP: Virtual-Access1: (3193852847): send
AV protocol=ip 15:04:51: AAA/AUTHOR/ICP: Virtual-Access1: (3193852847): send AV
addr*15.15.15.15 15:04:51: AAA/AUTHOR/ICP: Virtual-Access1: (3193852847): Method=TACACS+
15:04:51: AAA/AUTHOR/TAC+: (3193852847): user=jsmith@hp.com 15:04:51: AAA/AUTHOR/TAC+:
(3193852847): send AV service=ppp 15:04:51: AAA/AUTHOR/TAC+: (3193852847): send AV protocol=ip
```



```
15:04:51: AAA/AUTHOR/TAC+: (3193852847): send AV addr*15.15.15.15 15:04:51: TAC+: (3193852847):
received author response status = PASS_ADD 15:04:51: AAA/AUTHOR (3193852847): Post authorization
status = PASS_ADD 15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV service=ppp 15:04:51:
AAA/AUTHOR/IPCP Vi1: Processing AV protocol=ip 15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV
addr*15.15.15.15 15:04:51: AAA/AUTHOR/IPCP Vi1: Authorization succeeded 15:04:51:
AAA/AUTHOR/IPCP Vi1: Done. Her address 15.15.15.15, we want 15.15.15.15 !--- User finishes and
disconnects. 15:05:24: Vi1 VPDN: Reset 15:05:24: Vi1 VPDN: Reset %LINK-3-UPDOWN: Interface
Virtual-Access1, changed state to down 15:05:24: Vi1 VPDN: Cleanup 15:05:24: Vi1 VPDN: Reset
15:05:24: Vi1 VPDN: Reset 15:05:24: Vi1 VPDN: Unbind interface 15:05:24: Vi1 VTEMPLATE: Free
vaccess 15:05:24: Vi1 VPDN: Reset 15:05:24: Vi1 VPDN: Reset 15:05:24: AAA/ACCT: Network acct
stop. User jsmith@hp.com, Port Virtual-Access1: task_id=2 timezone=UTC service=ppp protocol=ip
addr=15.15.15.15 bytes_in=564 bytes_out=142 paks_in=15 paks_out=8 elapsed_time=35 15:05:24:
AAA/AUTHEN: free_user (0x161688) user='jsmith@hp.com' ruser='' port='Virtual-Access1'
rem_addr='async' authen_type=CHAP service=PPP priv=1 %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access1, changed state to down 15:05:25: VTEMPLATE: Clean up dirty vaccess
queue, size 1 15:05:25: Vi1 VTEMPLATE: Found a dirty vaccess clone with vtemplate 15:05:25: Vi1
VTEMPLATE: ***** UNCLONE VACCESS1 ***** 15:05:25: Vi1 VTEMPLATE: Unclone to-be-
freed command#5 interface Virtual-Access1 default ppp authen chap default peer default ip
address pool async default ip unnum eth 0 default encaps ppp default ip address end 15:05:26: Vi1
VTEMPLATE: Set default settings with no ip address 15:05:26: Vi1 VTEMPLATE: Remove cloneblk
vtemplate with vtemplate 15:05:26: Vi1 VTEMPLATE: Add vaccess to recycle queue, queue size=1
thing_one#
```

ISP 라우터에서 연결 실패 디버깅

```
koala#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
AAA Accounting debugging is on
```

```
VPN:
```

```
VPN events debugging is on
```

```
VPN errors debugging is on
```

```
koala#
```

```
!--- Problem 1: !--- The ISP TACACS+ server is down. !--- There is no output on the HGW router
!--- because the call has not gone that far.
```

```
AAA/AUTHOR (3015476150): Post authorization status = ERROR
```

```
AAA/AUTHOR/VPDN: : (3015476150): Method=NOT_SET
```

```
AAA/AUTHOR/VPDN: : (3015476150): no methods left to try
```

```
AAA/AUTHOR (3015476150): Post authorization status = ERROR
```

```
VPDN: (hp.com) Authorization failed, could not talk to AAA server or
local tunnel problem
```

```
!--- Problem 2: !--- Userid hp.com is not in the ISP server. !--- There is no output on the
Gateway router !--- because the call has not gone that far.
```

```
TAC+: (894828802): received author response status = PASS_ADD
```

```
AAA/AUTHOR (894828802): Post authorization status = PASS_ADD
```

```
VPDN: (hp.com) Authorization failed, had talked to AAA server;
but both Tunnel ID and IP address are missing
```

```
AAA/AUTHEN: free_user (0x16A6E4) user='hp.com' ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
```

```
AAA/AUTHEN: create_user (0x16CA8C) user='jsmith@hp.com' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
```

```
AAA/AUTHEN/START (1904487288): port='Async1' list=''
action=LOGIN service=PPP
```

```
AAA/AUTHEN/START (1904487288): using "default" list
```

```
AAA/AUTHEN (1904487288): status = UNKNOWN
```

```
AAA/AUTHEN/START (1904487288): Method=TACACS+
```

```
TAC+: send AUTHEN/START packet ver=193 id=1904487288
```

```
TAC+: ver=193 id=1904487288 received AUTHEN status = FAIL
```

```
AAA/AUTHEN (1904487288): status = FAIL
```

HGW 라우터의 실패한 연결에 대한 디버깅

```
thing_one#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
AAA Accounting debugging is on
```

```
VPN:
```

```
VPN events debugging is on
```

```
VPN errors debugging is on
```

```
VTEMPLATE:
```

```
Virtual Template debugging is on
```

```
thing_one#
```

```
!--- Problem 1: !--- The problem is in the tunnel definition on HGW router. !--- In the HGW configuration, vpdn incoming hp-gw isp virtual-template 1 !--- is inserted instead of vpdn incoming isp hp-gw virtual-template 1 !--- The debug vpdn l2f-errors command displays.
```

```
L2F: Couldn't find tunnel named isp
```

```
L2F: Couldn't find tunnel named isp
```

```
!--- Problem 2: !--- This message appears when User hp-gw is not in the HGW server.
```

```
TAC+: ver=192 id=1920941753 received AUTHEN status = FAIL
```

```
AAA/AUTHEN: free_user (0x138C34) user='hp-gw' ruser=''
```

```
port='' rem_addr='' authen_type=CHAP service=PPP priv=1
```

```
AAA/AUTHEN (3006335673): status = FAIL
```

```
VPDN: authentication failed, couldn't find user information for hp-gw
```

```
!--- Problem 3: !--- This appears when user isp is not in the HGW server.
```

```
TAC+: ver=192 id=1917558147 received AUTHEN status = FAIL
```

```
AAA/AUTHEN: free_user (0x15F20C) user='isp' ruser=''
```

```
port='' rem_addr='' authen_type=CHAP service=PPP priv=1
```

```
AAA/AUTHEN (1949507921): status = FAIL
```

```
VPDN: authentication failed, couldn't find user information for isp
```

```
!--- Problem 4: !--- This message appears when User jsmith@hp.com is !--- not in the HGW server:
```

```
TAC+: ver=192 id=755036341 received AUTHEN status = FAIL
```

```
AAA/AUTHEN: free_user (0x15F89C) user='jsmith@hp.com' ruser=''
```

```
port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
```

```
AAA/AUTHEN (2606986667): status = FAIL
```

관련 정보

- [UNIX용 Cisco Secure ACS 지원 페이지](#)
- [TACACS+ 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)