

Layer 2 Tunnel-protocolverificatie configureren met RADIUS

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[RADIUS-serverconfiguratie](#)

[Netwerkdigram](#)

[LAC RADIUS-configuratie - Cisco Secure ACS voor UNIX](#)

[LAN RADIUS-configuratie - Cisco Secure ACS voor UNIX](#)

[LAC RADIUS-configuratie - Cisco Secure ACS voor Windows](#)

[LAN RADIUS-configuratie - Cisco Secure ACS voor Windows](#)

[LAC RADIUS-configuratie - Merit RADIUS](#)

[LNS RADIUS-configuratie - Merit RADIUS](#)

[Routerconfiguraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Debug uitvoer](#)

[Good Debug van LAC router](#)

[Good Debug van LNS-router](#)

[Wat kan er mis gaan - Slechte Debug van LAC](#)

[Wat kan er mis gaan - Slechte Debug van LNS](#)

[LNS-boekhoudingsgegevens](#)

[Gerelateerde informatie](#)

Inleiding

Dit document laat zien hoe u een Layer 2 Tunnel Protocol (L2TP) Virtual Private Dialup Network (VPDN)-scenario kunt configureren met behulp van tunnelkenmerken die van een RADIUS-server zijn gedownload. In dit voorbeeld ontvangt de L2TP Access Concentrator (LAC) de inkomende verbinding en neemt deze contact op met de LAC RADIUS-server. De RADIUS-server kijkt de tunnelkenmerken op voor het domein van de gebruiker (bijvoorbeeld cisco.com) en geeft de tunnelkenmerken door aan de LAC. Gebaseerd op deze kenmerken start de LAC een tunnel naar de L2TP Network Server (LNS). Zodra de tunnel is opgezet, verifieert de LNS de eindgebruiker via zijn eigen RADIUS-server.

Opmerking: dit document gaat ervan uit dat de NAS (LAC) is geconfigureerd voor algemene

kiestoegang. Zie [Basis AAA RADIUS voor inbelclients configureren voor](#) meer informatie over [het configureren van inbelclients](#).

Raadpleeg voor meer informatie over L2TP en VPDN's deze documenten:

- [VPDN begrijpen](#)
- [Virtual Private Networks configureren](#)
- [Layer 2-tunnelprotocol](#)

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Twee Cisco 2511 routers
- Cisco IOS®-softwarerelease 12.0(2)T
- Cisco Secure ACS voor UNIX, Cisco Secure ACS voor Windows of Merit RADIUS

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

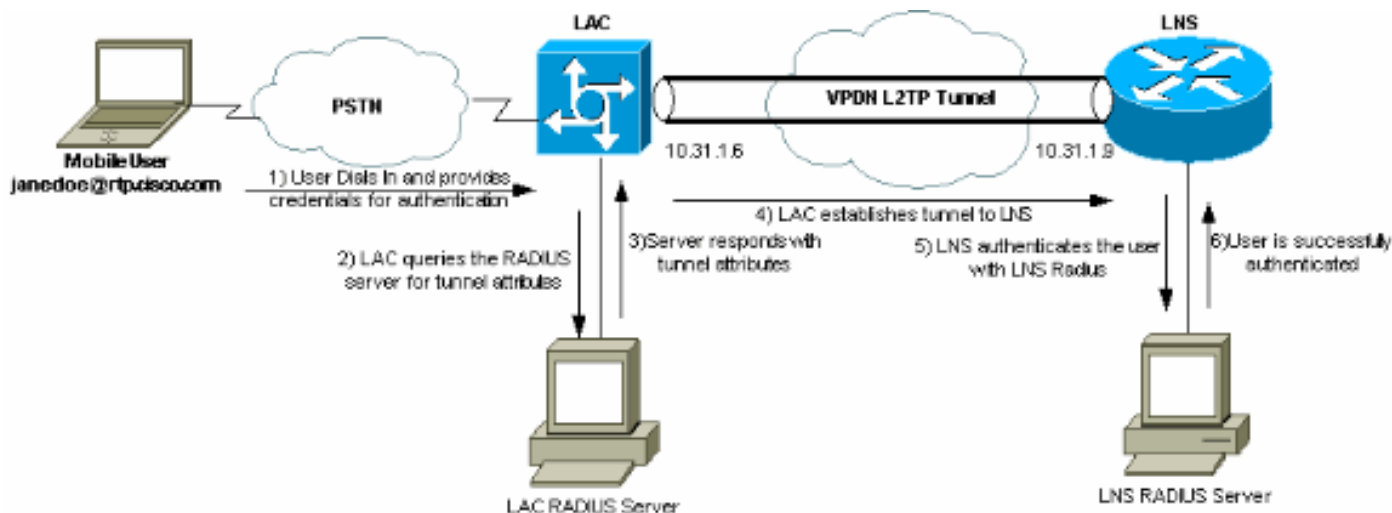
RADIUS-serverconfiguratie

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik [Command Lookup Tool](#) (alleen voor [geregistreeerde](#) klanten) voor meer informatie over de opdrachten die in dit document worden gebruikt.

Netwerkdigram

Dit document gebruikt de netwerkinstallatie die in dit diagram wordt getoond.



LAC RADIUS-configuratie - Cisco Secure ACS voor UNIX

De LAC RADIUS-configuratie bevat de gebruiker "rtp.cisco.com" (dat is het domein dat door de client wordt gebruikt). Het wachtwoord voor deze gebruiker moet cisco zijn.

```
# ./ViewProfile -p 9900 -u rtp.cisco.com
user = rtp.cisco.com{
radius=Cisco {
check_items= {
2="cisco"
}
reply_attributes= {
6=5
9,1="vpdn:tunnel-id=DEFGH"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.31.1.9"
9,1="vpdn:l2tp-tunnel-password=ABCDE"
}
}
}
```

Raadpleeg voor meer informatie over RADIUS-configuratie op de LAC het [RADIUS-profiel voor gebruik in de LAC](#)-sectie binnen het [Layer 2-tunnelprotocol](#).

LAN RADIUS-configuratie - Cisco Secure ACS voor UNIX

```
# ./ViewProfile -p 9900 -u janedoe@rtp.cisco.com
user = janedoe@rtp.cisco.com{
radius=Cisco {
check_items= {
2="rtp"
}
reply_attributes= {
6=2
7=1
}
}
```

}

}

LAC RADIUS-configuratie - Cisco Secure ACS voor Windows

Voer de volgende stappen uit:

1. Stel in het gedeelte Network Configuration de verificatie voor LAC Network Access Server (NAS) in om RADIUS (Cisco IOS/PIX) te gebruiken.
2. Configureer de gebruiker 'rtp.cisco.com' met wachtwoord cisco voor zowel eenvoudig als CHAP. Dit is de gebruikersnaam die wordt gebruikt voor de tunnelkenmerken.
3. Klik op de knop Groepsinstelling in de linkernavigatiebalk. Selecteer de groep waartoe de gebruiker behoort en klik op Instellingen bewerken. Blader naar beneden naar het gedeelte IETF RADIUS en selecteer Attriboot 6 Service-Type als Uitgaand. .

Als niet alle opties die ingeschakeld kunnen worden worden weergegeven, gaat u naar Interface Configuration (Interfaceconfiguratie) en schakelt u de verschillende vakjes in om deze in het groeps gedeelte te laten verschijnen.

4. In het gedeelte Cisco IOS/PIX RADIUS-kenmerken onderaan kruist u het vakje 009\001 cisco-av-paar aan en typt u dit in het vak:


```
vpdn:tunnel-id=DEFGH  
vpdn:tunnel-type=l2tp  
vpdn:ip-addresses=10.31.1.9  
vpdn:l2tp-tunnel-password=ABCDE
```

Raadpleeg voor meer informatie over RADIUS-configuratie op de LAC het [RADIUS-profiel voor gebruik in de LAC](#)-sectie binnen [Layer 2 Tunnel Protocol](#).




Group Setup

Jump To

Cisco IOS/PIX RADIUS Attributes 

[009\001] cisco-av-pair

```
vpdn:tunnel-id=DEFGH
vpdn:tunnel-type=l2tp
vpdn:ip-addresses=10.31.1.9
vpdn:l2tp-tunnel-
password=ABCDE
```

IETF RADIUS Attributes 

[006] Service-Type

[007] Framed-Protocol

[009] Framed-IP-Netmask

[010] Framed-IP-Netmask

LAN RADIUS-configuratie - Cisco Secure ACS voor Windows

Voer de volgende stappen uit:

1. Configureer de gebruikersidentificatie janedoe@rtp.cisco.com en voer een willekeurig wachtwoord in voor Sprint en CHAP.
2. Klik op de knop Group Setup in de linkerbalk. Selecteer de groep waartoe de gebruiker behoort en klik op Instellingen bewerken.
3. In de sectie voor Internet Engineering Task Force (IETF) RADIUS-kenmerken selecteert u Service-type (kenmerk 6) = framed en framed-protocol (kenmerk 7)=PPP in het vervolgkeuzemenu.

Opmerking: u moet ook op het selectievakje naast de geselecteerde kenmerken Service-

Type en Framed-Protocol klikken.

LAC RADIUS-configuratie - Merit RADIUS

Opmerking: Livingston- en Merit-servers moeten vaak worden aangepast om leverancierspecifieke av-paren te ondersteunen.

```
rtp.cisco.com Password = "cisco"  
    Service-Type = Outbound-User,  
    cisco-avpair = "vpdn:tunnel-id=DEFGH",  
    cisco-avpair = "vpdn:tunnel-type=l2tp",  
    cisco-avpair = "vpdn:ip-addresses=10.31.1.9",  
    cisco-avpair = "vpdn:l2tp-tunnel-password=ABCDE"
```

Raadpleeg voor meer informatie over RADIUS-configuratie op de LAC het [RADIUS-profiel voor gebruik in de LAC](#)-sectie binnen [Layer 2 Tunnel Protocol](#).

LNS RADIUS-configuratie - Merit RADIUS

```
janedoe@rtp.cisco.com Password = "rtp",  
    Service-Type = Framed,  
    Framed-Protocol = PPP
```

Routerconfiguraties

Dit document gebruikt de volgende configuraties.

- [Configuratie van LAC-router](#)
- [Configuratie van LAN-router](#)

Configuratie van LAC-router

```
<#root>  
LAC#  
show run  
Building configuration...  
Current configuration:  
!  
version 12.0  
service timestamps debug datetime  
service timestamps log uptime
```

```
no service password-encryption
!
hostname LAC
!
!--- AAA commands needed to authenticate the user and obtain !--- VPDN tunnel information.

aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed radius
aaa authorization network default radius
aaa accounting exec default start-stop radius
aaa accounting network default start-stop radius
enable secret level 7 5 $1$Dj3K$9jkyuJR6fJV2J0./Qt01C1
enable password ww
!
username cse password 0 csecse
username john password 0 doe
ip subnet-zero
no ip domain-lookup
!
jnj00=tfdftr

vpdn enable

!
!--- VPDN tunnel authorization is based on the domain name !--- (the default is DNIS).

vpdn search-order domain
!
!
!
interface Loopback0
 no ip address
 no ip directed-broadcast
!
interface Ethernet0
 ip address 10.31.1.6 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Async1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 ip tcp header-compression passive
 encapsulation ppp
 async mode dedicated
 peer default ip address pool async
 no cdp enable
 ppp authentication chap
!
```

```
interface Group-Async1
  physical-layer async
  no ip address
  no ip directed-broadcast
!
ip local pool default 10.5.5.5 10.5.5.50
ip local pool async 10.7.1.1 10.7.1.5
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!
!--- RADIUS server host and key.

radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
  transport input none
line 1
  session-timeout 20
  exec-timeout 0 0
  password ww
  autoselect during-login
  autoselect ppp
  modem InOut
  transport preferred none
  transport output none
  stopbits 1
  speed 38400
  flowcontrol hardware
line 2 16
  modem InOut
  transport input all
  speed 38400
  flowcontrol hardware
line aux 0
line vty 0 4
  password ww
!
end
```

Configuratie van LAN-router

```
<#root>
LNS#
show run
Building configuration...

Current configuration:
!
! Last configuration change at 12:17:54 UTC Sun Feb 7 1999
! ==m6knr5yui6yt6egv2wr25nfd1rsion 12.0=4rservice exec-callback
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
```



```
!  
hostname LNS  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication ppp default radius local  
aaa authorization network default radius local  
aaa accounting exec default start-stop radius  
aaa accounting network default start-stop radius  
enable secret 5 $1$pnYM$B.FveZjZpgA3C9ZPq/cma/  
enable password ww  
!  
username john password 0 doe  
  
!--- User the_LNS is used to authenticate the tunnel. !--- The password used here must match the vpdn:  
  
username the_LNS password 0 ABCDE  
  
ip subnet-zero  
!  
  
!--- Enable VPDN on the LNS.  
  
vpdn enable  
!  
  
!--- VPDN group for connection from the LAC.  
  
vpdn-group 1  
  
!--- This command specifies that the router uses !--- virtual-template 1 for tunnel-id DEFGH (which ma  
  
accept dialin l2tp virtual-template 1 remote DEFGH  
  
!--- The username used to authenticate this tunnel !--- is the_LNS (configured above).  
  
local name the_LNS  
!  
interface Ethernet0  
 ip address 10.31.1.9 255.255.255.0  
 no ip directed-broadcast  
!  
  
!--- Virtual-template that is used for the incoming connection.  
  
interface Virtual-Template1  
  
 ip unnumbered Ethernet0  
 no ip directed-broadcast  
 peer default ip address pool default  
 ppp authentication chap  
!  
interface Serial0  
 no ip address  
 no ip directed-broadcast
```

```
no ip mroute-cache
shutdown
no fair-queue
!
interface Serial1
no ip address
no ip directed-broadcast
shutdown
!
interface Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
async mode interactive
peer default ip address pool async
ppp authentication chap
!
ip local pool default 10.6.1.1 10.6.1.5
ip local pool async 10.8.100.100 10.8.100.110
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!
!--- RADIUS server host and key information.

radius-server host 171.68.120.194 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
transport input none
line 1
session-timeout 20
exec-timeout 5 0
password ww
autoselect during-login
autoselect ppp
modem InOut
transport input all
escape-character BREAK
stopbits 1
speed 38400
flowcontrol hardware
line 2 8
line aux 0
line vty 0 4
password ww
!
end
```

Verifiëren

Deze sectie bevat informatie die u kunt gebruiken om te controleren of uw configuratie correct werkt.

Bepaalde opdrachten met show worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met show

genereren.

- toon vpdn tunnel-Vertoningen informatie over alle actieve Layer 2 Forwarding en L2TP tunnels in summiere stijl formaat.
- IP-weergaven van de beller een overzicht van de belleninformatie voor het IP-adres dat u opgeeft.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Opmerking: Voordat u debug-opdrachten uitvoert, raadpleegt u [Belangrijke informatie over debug-opdrachten](#).

- debug aaa verificatie—Hier wordt informatie over AAA/TACACS+ verificatie weergegeven.
- debug aaa-autorisatie—Hier wordt informatie weergegeven over AAA/TACACS+ autorisatie.
- debug aaa accounting—Hier wordt informatie weergegeven over verantwoordelijke gebeurtenissen wanneer deze zich voordoen. De informatie die in deze opdracht wordt weergegeven, is onafhankelijk van het boekhoudprotocol dat wordt gebruikt om de boekhoudingsinformatie naar een server over te dragen.
- debug radius—Hier wordt gedetailleerde debugging-informatie weergegeven die aan de RADIUS is gekoppeld.
- debug vtemplate—Hier wordt informatie over klonen voor een virtuele toegangsinterface weergegeven vanaf het moment dat de interface wordt gekloond van een virtuele sjabloon tot het moment waarop de virtuele toegangsinterface neerkomt wanneer de oproep eindigt.
- debug vpdn fout—Hier worden fouten weergegeven die verhinderen dat een PPP-tunnel wordt gemaakt of fouten die ervoor zorgen dat een ingestelde tunnel wordt gesloten.
- debug vpdn gebeurtenissen—Hier worden berichten weergegeven over gebeurtenissen die deel uitmaken van de normale PPP-tunnelinstelling of -sluiting.
- debug vpdn l2x-fouten—Hier wordt Layer 2-protocolfouten weergegeven die Layer 2-vestiging voorkomen of de normale werking ervan verhinderen.
- debug vpdn l2x-events—Hier worden berichten weergegeven over gebeurtenissen die deel uitmaken van de normale PPP-tunnelinstelling of afsluiten voor Layer 2.
- debug vpdn l2tp-sequencing—Hier worden berichten over L2TP weergegeven.

Debug uitvoer

Raadpleeg voor een gedetailleerde beschrijving van de L2TP-debuggs [L2TP Tunnel Setup en Teardown](#).

Good Debug van LAC router

```
<#root>
```

```
LAC#
```

```
show debug
```

```
General OS:
```

```
AAA Authentication debugging is on  
AAA Authorization debugging is on  
AAA Accounting 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  
L2TP data sequencing debugging is on
```

```
VTEMPLATE:
```

```
Virtual Template debugging is on  
Radius protocol debugging is on
```

```
LAC#
```

```
Feb 7 12:22:16: As1 AAA/AUTHOR/FSM: (0):  
LCP succeeds trivially
```

```
2d18h: %LINK-3-UPDOWN: Interface Async1,  
changed state to up
```

```
Feb 7 12:22:17: As1 VPDN: Looking for tunnel  
-- rtp.cisco.com --
```

```
Feb 7 12:22:17: AAA: parse name=Async1 idb  
type=10 tty=1
```

```
Feb 7 12:22:17: AAA: name=Async1 flags=0x11  
type=4 shelf=0 slot=0  
adapter=0 port=1 channel=0
```

```
Feb 7 12:22:17: AAA/AUTHEN: create_user (0x25BA84)  
user='rtp.cisco.com' ruser='' port='Async1' rem_addr=''  
authen_type=NONE service=LOGIN priv=0
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN (6239469):  
Port='Async1' list='default' service=NET
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469)  
user='rtp.cisco.com'
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469)  
send AV service=ppp
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469)  
send AV protocol=vpdn
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN (6239469)  
found list "default"
```

```
Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469) Method=RADIUS
```

```
Feb 7 12:22:17: RADIUS: authenticating to get author data
```

```
Feb 7 12:22:17: RADIUS: ustruct sharecount=2
```

```
Feb 7 12:22:17: RADIUS: Initial Transmit Async1 id 66  
171.68.118.101:1645, Access-Request, len 77
```

```
Feb 7 12:22:17: Attribute 4 6 0A1F0106
```

```
Feb 7 12:22:17: Attribute 5 6 00000001
```

```
Feb 7 12:22:17: Attribute 61 6 00000000
```

```
Feb 7 12:22:17: Attribute 1 15 7274702E
```

```
Feb 7 12:22:17: Attribute 2 18 6AB5A2B0
```

```
Feb 7 12:22:17: Attribute 6 6 00000005
```

```
Feb 7 12:22:17: RADIUS: Received from id 66
171.68.118.101:1645, Access-Accept, len 158
Feb 7 12:22:17: Attribute 6 6 00000005
Feb 7 12:22:17: Attribute 26 28 0000000901167670
Feb 7 12:22:17: Attribute 26 29 0000000901177670
Feb 7 12:22:17: Attribute 26 36 00000009011E7670
Feb 7 12:22:17: Attribute 26 39 0000000901217670
Feb 7 12:22:17: RADIUS: saved authorization data for user
25BA84 at 24C488
```

!--- RADIUS server supplies the VPDN tunnel attributes.

```
Feb 7 12:22:17: RADIUS: cisco AVPair
"vpdn:tunnel-id=DEFGH"
Feb 7 12:22:17: RADIUS: cisco AVPair
"vpdn:tunnel-type=l2tp"
Feb 7 12:22:17: RADIUS: cisco AVPair
"vpdn:ip-addresses=10.31.1.9,"
Feb 7 12:22:17: RADIUS: cisco AVPair
"vpdn:l2tp-tunnel-password=ABCDE"

Feb 7 12:22:17: AAA/AUTHOR (6239469): Post
authorization status = PASS_ADD
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing
AV service=ppp
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing
AV protocol=vpdn
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing
AV tunnel-id=DEFGH
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing
AV tunnel-type=l2tp
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV
ip-addresses=10.31.1.9,
Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV
l2tp-tunnel-password=ABCDE
Feb 7 12:22:17: As1 VPDN: Get tunnel info for
rtp.cisco.com with LAC DEFGH, IP 10.31.1.9
Feb 7 12:22:17: AAA/AUTHEN: free_user (0x25BA84)
user='rtp.cisco.com' ruser='' port='Async1' rem_addr=''
authen_type=NONE service=LOGIN priv=0

Feb 7 12:22:17: As1 VPDN: Forward to address 10.31.1.9

Feb 7 12:22:17: As1 VPDN: Forwarding...
Feb 7 12:22:17: AAA: parse name=Async1 idb
type=10 tty=1
Feb 7 12:22:17: AAA: name=Async1 flags=0x11 type=4
shelf=0 slot=0 adapter=0 port=1 channel=0
Feb 7 12:22:17: AAA/AUTHEN: create_user (0xB7918)
user='janedoe@rtp.cisco.com' ruser='' port='Async1'
rem_addr='async' authen_type=CHAP service=PPP priv=1
Feb 7 12:22:17: As1 VPDN: Bind interface direction=1
Feb 7 12:22:17: Tn1/C1 51/1 L2TP: Session FS enabled
Feb 7 12:22:17: Tn1/C1 51/1 L2TP: Session state change
from idle to wait-for-tunnel
Feb 7 12:22:17: As1 51/1 L2TP: Create session
Feb 7 12:22:17: Tn1 51 L2TP: SM State idle
Feb 7 12:22:17: Tn1 51 L2TP: 0 SCCRQ
Feb 7 12:22:17: Tn1 51 L2TP: Tunnel state change
from idle to wait-ctl-reply
Feb 7 12:22:17: Tn1 51 L2TP: SM State wait-ctl-reply

Feb 7 12:22:17: As1 VPDN: janedoe@rtp.cisco.com
```

is forwarded

Feb 7 12:22:17: Tn1 51 L2TP: I SCCRP from the_LNS

!--- Tunnel authentication is successful.

Feb 7 12:22:17: Tn1 51 L2TP: Got a challenge from remote peer, the_LNS

Feb 7 12:22:17: Tn1 51 L2TP: Got a response from remote peer, the_LNS

Feb 7 12:22:17: Tn1 51 L2TP: Tunnel Authentication success

Feb 7 12:22:17: Tn1 51 L2TP: Tunnel state change from wait-ctl-reply to established

Feb 7 12:22:17: Tn1 51 L2TP: O SCCN to the_LNS tn1id 38

Feb 7 12:22:17: Tn1 51 L2TP: SM State established

Feb 7 12:22:17: As1 51/1 L2TP: O ICRQ to the_LNS 38/0

Feb 7 12:22:17: As1 51/1 L2TP: Session state change from wait-for-tunnel to wait-reply

Feb 7 12:22:17: As1 51/1 L2TP: O ICCN to the_LNS 38/1

Feb 7 12:22:17: As1 51/1 L2TP: Session state change from wait-reply to established

2d18h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up

LAC#

Good Debug van LNS-router

<#root>

LNS#

show debug

General OS:

AAA Authentication debugging is on

AAA Authorization debugging is on

AAA Accounting 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

L2TP data sequencing debugging is on

VTEMPLATE:

Virtual Template debugging is on

Radius protocol debugging is on

LNS#

Feb 7 12:22:16: L2TP: I SCCRQ from DEFGH tn1 51

Feb 7 12:22:16: Tn1 38 L2TP: New tunnel created for remote DEFGH, address 10.31.1.6

Feb 7 12:22:16: Tn1 38 L2TP: Got a challenge in SCCRQ, DEFGH

Feb 7 12:22:16: Tn1 38 L2TP: O SCCRP to DEFGH tn1id 51

Feb 7 12:22:16: Tn1 38 L2TP: Tunnel state change from

```
idle to wait-ctl-reply
Feb 7 12:22:16: Tn1 38 L2TP: I SCCCN from DEFGH tn1 51
Feb 7 12:22:16: Tn1 38 L2TP: Got a Challenge Response
in SCCCN from DEFGH
Feb 7 12:22:16: Tn1 38 L2TP: Tunnel Authentication
success
Feb 7 12:22:16: Tn1 38 L2TP: Tunnel state change from
wait-ctl-reply to established
Feb 7 12:22:16: Tn1 38 L2TP: SM State established
Feb 7 12:22:17: Tn1 38 L2TP: I ICRQ from DEFGH tn1 51
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: Session FS enabled
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: Session state change
from idle to wait-for-tunnel
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: New session created
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: O ICRP to DEFGH 51/1
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: Session state change
from wait-for-tunnel to wait-connect
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: I ICCN from DEFGH tn1
51, cl 1
Feb 7 12:22:17: Tn1/Cl 38/1 L2TP: Session state change
from wait-connect to established
Feb 7 12:22:17: Vi1 VTEMPLATE: Reuse Vi1, recycle
queue size 0
Feb 7 12:22:17: Vi1 VTEMPLATE: Hardware address
00e0.1e68.942c
```

!--- Use Virtual-template 1 for this user.

```
Feb 7 12:22:17: Vi1 VPDN: Virtual interface created for
janedoe@rtp.cisco.com
Feb 7 12:22:17: Vi1 VPDN: Set to Async interface
Feb 7 12:22:17: Vi1 VPDN: Clone from Vtemplate 1
filterPPP=0 blocking

Feb 7 12:22:17: Vi1 VTEMPLATE: Has a new cloneblk vtemplate,
now it has vtemplate
Feb 7 12:22:17: Vi1 VTEMPLATE: ***** CLONE
VACCESS1 *****
Feb 7 12:22:17: Vi1 VTEMPLATE: Clone from
Virtual-Template1
interface Virtual-Access1
default ip address
no ip address
encap ppp
ip unnum eth 0
no ip directed-broadcast
peer default ip address pool default
ppp authen chap
end

Feb 7 12:22:18: janedoe@rtp.cisco.com 38/1 L2TP: Session
with no hwidb
02:23:59: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
trivially
Feb 7 12:22:19: Vi1 VPDN: Bind interface direction=2
Feb 7 12:22:19: Vi1 VPDN: PPP LCP accepted rcv CONFACK
Feb 7 12:22:19: Vi1 VPDN: PPP LCP accepted sent CONFACK
Feb 7 12:22:19: Vi1 L2X: Discarding packet because of
no mid/session
Feb 7 12:22:19: AAA: parse name=Virtual-Access1 idb
```

```
type=21 tty=-1
Feb 7 12:22:19: AAA: name=Virtual-Access1 flags=0x11
type=5 shelf=0 slot=0 adapter=0 port=1 channel=0
Feb 7 12:22:19: AAA/AUTHEN: create_user (0x2462A0)
user='janedoe@rtp.cisco.com' ruser='' port='Virtual-Access1'
rem_addr='' authen_type=CHAP service=PPP priv=1
Feb 7 12:22:19: AAA/AUTHEN/START (2229277178):
port='Virtual-Access1' list='' action=LOGIN
service=PPP
Feb 7 12:22:19: AAA/AUTHEN/START (2229277178):
using "default" list
Feb 7 12:22:19: AAA/AUTHEN/START (2229277178):
Method=RADIUS
Feb 7 12:22:19: RADIUS: ustruct sharecount=1
Feb 7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
id 78 171.68.120.194:1645, Access-Request, len 92
Feb 7 12:22:19: Attribute 4 6 0A1F0109
Feb 7 12:22:19: Attribute 5 6 00000001
Feb 7 12:22:19: Attribute 61 6 00000005
Feb 7 12:22:19: Attribute 1 23 6464756E
Feb 7 12:22:19: Attribute 3 19 34A66389
Feb 7 12:22:19: Attribute 6 6 00000002
Feb 7 12:22:19: Attribute 7 6 00000001
Feb 7 12:22:19: RADIUS: Received from id 78
171.68.120.194:1645, Access-Accept, len 32
Feb 7 12:22:19: Attribute 6 6 00000002
Feb 7 12:22:19: Attribute 7 6 00000001
Feb 7 12:22:19: AAA/AUTHEN (2229277178): status = PASS
Feb 7 12:22:19: Vi1 AAA/AUTHOR/LCP: Authorize LCP
Feb 7 12:22:19: AAA/AUTHOR/LCP Vi1 (1756915964):
Port='Virtual-Access1' list='' service=NET
Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
user='janedoe@rtp.cisco.com'
Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
send AV service=ppp
Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
send AV protocol=lcp
Feb 7 12:22:19: AAA/AUTHOR/LCP (1756915964) found
list "default"
Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
Method=RADIUS
Feb 7 12:22:19: AAA/AUTHOR (1756915964): Post
authorization status = PASS_REPL
Feb 7 12:22:19: Vi1 AAA/AUTHOR/LCP: Processing
AV service=ppp
Feb 7 12:22:19: AAA/ACCT/NET/START User
janedoe@rtp.cisco.com, Port Virtual-Access1, List ""
Feb 7 12:22:19: AAA/ACCT/NET: Found list "default"
Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): Can we
start IPCP?
Feb 7 12:22:19: AAA/AUTHOR/FSM Vi1 (1311872588):
Port='Virtual-Access1' list='' service=NET
Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
user='janedoe@rtp.cisco.com'
Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
send AV service=ppp
Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
send AV protocol=ip
Feb 7 12:22:19: AAA/AUTHOR/FSM (1311872588)
found list "default"
Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
Method=RADIUS
```



```
Feb 7 12:22:19: AAA/AUTHOR (1311872588): Post
authorization status = PASS_REPL
Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: We can start
IPCP
Feb 7 12:22:19: RADIUS: ustruct sharecount=2
Feb 7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
id 79 171.68.120.194:1646, Accounting-Request, len 101
Feb 7 12:22:19: Attribute 4 6 0A1F0109
Feb 7 12:22:19: Attribute 5 6 00000001
Feb 7 12:22:19: Attribute 61 6 00000005
Feb 7 12:22:19: Attribute 1 23 6464756E
Feb 7 12:22:19: Attribute 40 6 00000001
Feb 7 12:22:19: Attribute 45 6 00000001
Feb 7 12:22:19: Attribute 6 6 00000002
Feb 7 12:22:19: Attribute 44 10 30303030
Feb 7 12:22:19: Attribute 7 6 00000001
Feb 7 12:22:19: Attribute 41 6 00000000
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start. Her
address 0.0.0.0, we want 0.0.0.0
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
AV service=ppp
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done. Her
address 0.0.0.0, we want 0.0.0.0
Feb 7 12:22:19: RADIUS: Received from id 79
171.68.120.194:1646, Accounting-response,
len 20
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 10.6.1.1
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
AV service=ppp
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 10.6.1.1
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 10.6.1.1, we want 10.6.1.1
Feb 7 12:22:19: AAA/AUTHOR/IPCP Vi1 (2909132255):
Port='Virtual-Access1' list='' service=NET
Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
user='janedoe@rtp.cisco.com'
Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
send AV service=ppp
Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
send AV protocol=ip
Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
send AV addr*10.6.1.1
Feb 7 12:22:19: AAA/AUTHOR/IPCP (2909132255)
found list "default"
Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
Method=RADIUS
Feb 7 12:22:19: AAA/AUTHOR (2909132255): Post
authorization status = PASS_REPL
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Reject
10.6.1.1, using 10.6.1.1
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
AV service=ppp
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
AV addr*10.6.1.1
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
succeeded
```

```
Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.  
Her address 10.6.1.1, we want 10.6.1.1  
02:24:00: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Virtual-Access1, changed state to up  
LNS#
```

Wat kan er mis gaan - Slechte Debug van LAC

```
<#root>
```

```
LAC#
```

```
show debug
```

```
General OS:
```

```
AAA Authentication debugging is on  
AAA Authorization debugging is on  
AAA Accounting 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  
L2TP data sequencing debugging is on
```

```
VTEMPLATE:
```

```
Virtual Template debugging is on  
Radius protocol debugging is on
```

De gebruiker komt binnen als janedoe@sj.cisco.com (in plaats van janedoe@rtp.cisco.com), maar de server van de RADIUS van LAC herkent dit domein niet.

```
<#root>
```

```
Feb 7 13:26:48: RADIUS: Received from id 86  
171.68.118.101:1645, Access-Reject, len 46  
Feb 7 13:26:48: Attribute 18 26 41757468  
Feb 7 13:26:48: RADIUS: failed to get  
authorization data: authen status = 2  
%VPDN-6-AUTHORFAIL: L2F NAS LAC, AAA authorization  
failure for As1 user janedoe@sj.cisco.com
```

Deze debugs tonen een situatie waar de tunnelinformatie wordt ontvangen, maar met een ongeldig IP adres voor het andere eind van de tunnel. De gebruiker probeert een sessie te starten, maar kan geen verbinding maken.

```
<#root>
```

```
Feb 7 13:32:45: As1 VPDN: Forward to  
address 1.1.1.1  
Feb 7 13:32:45: As1 VPDN: Forwarding...
```

```
Feb 7 13:32:45: Tnl 56 L2TP: Tunnel state
change from idle to wait-ctl-reply
Feb 7 13:32:46: As1 56/1 L2TP: Discarding data
packet because tunnel is not open
```

Deze debugs tonen een situatie wanneer er een tunnelwachtwoordwanverhouding is. In het LNS, "username the_LNS password ABCDE" wordt veranderd in "username the_LNS password garbage" zodat tunnelverificatie mislukt wanneer geprobeerd.

```
<#root>
```

```
Feb 7 13:39:35: Tnl 59 L2TP: Tunnel Authentication
fails for the_LNS
Feb 7 13:39:35: Tnl 59 L2TP: Expected
E530DA13B826685C678589250C0BF525
Feb 7 13:39:35: Tnl 59 L2TP: Got
E09D90E8A91CF1014C91D56F65BDD052
Feb 7 13:39:35: Tnl 59 L2TP: O StopCCN
to the_LNS tnlid 44
Feb 7 13:39:35: Tnl 59 L2TP: Tunnel state
change from wait-ctl-reply to shutting-down
Feb 7 13:39:35: Tnl 59 L2TP: Shutdown tunnel
```

Wat kan er mis gaan - Slechte Debug van LNS

```
<#root>
```

```
LNS#
```

```
show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting 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
L2TP data sequencing debugging is on
```

```
VTEMPLATE:
```

```
Virtual Template debugging is on
Radius protocol debugging is on
LNS#
```

In dit voorbeeld, "accepteer het draaien l2tp virtual-template 1 Remote DEFGH" is veranderd in "accepteer dialin l2tp virtual-template 1 remote junk". De LNS kan de tunnel DEFGH niet meer vinden (in plaats daarvan is het "junk").

<#root>

```
Feb  7 13:45:32: L2TP: I SCCRQ from
      DEFGH tnl 62
Feb  7 13:45:32: L2X: Never heard of
      DEFGH
Feb  7 13:45:32: L2TP: Could not find info
      block for DEFGH
```

LNS-boekhoudingsgegevens

```
10.31.1.9 janedoe@rtp.cisco.com 1 - start
  server=rtp-cherry time=09:23:53
  date=02/ 6/1999 task_id=0000001C
Sat Feb  6 12:23:53 1999
  Client-Id = 10.31.1.9
  Client-Port-Id = 1
  NAS-Port-Type = Virtual
  User-Name = "janedoe@rtp.cisco.com"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  User-Service-Type = Framed-User
  Acct-Session-Id = "0000001C"
  Framed-Protocol = PPP
  Acct-Delay-Time = 0
```

```
10.31.1.9 janedoe@rtp.cisco.com 1 - stop
  server=rtp-cherry time=09:24:46
  date=02/ 6/1999 task_id=0000001C
Sat Feb  6 12:24:46 1999
  Client-Id = 10.31.1.9
  Client-Port-Id = 1
  NAS-Port-Type = Virtual
  User-Name = "janedoe@rtp.cisco.com"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  User-Service-Type = Framed-User
  Acct-Session-Id = "0000001C"
  Framed-Protocol = PPP
  Framed-Address = 10.6.1.1
  Acct-Terminate-Cause = Lost-Carrier
  Acct-Input-Octets = 678
  Acct-Output-Octets = 176
  Acct-Input-Packets = 17
  Acct-Output-Packets = 10
  Acct-Session-Time = 53
  Acct-Delay-Time = 0
```

Gerelateerde informatie

- [Access VPDN inbellen met L2TP](#)
- [Layer 2-tunnelprotocol](#)

- [Pagina voor RADIUS-ondersteuning](#)
- [Cisco Secure ACS voor Windows-ondersteuningspagina](#)
- [Cisco Secure ACS voor UNIX-ondersteuningspagina](#)
- [Requests for Comments \(RFC's\)](#)
- [Technische ondersteuning – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.