

# 使用RADIUS設定第2層通道通訊協定驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[RADIUS伺服器組態](#)

[網路圖表](#)

[LAC RADIUS配置 — Cisco Secure ACS for UNIX](#)

[LNS RADIUS配置 — Cisco Secure ACS for UNIX](#)

[LAC RADIUS配置 — Cisco Secure ACS for Windows](#)

[LNS RADIUS配置 — Cisco Secure ACS for Windows](#)

[LAC RADIUS配置 — Merit RADIUS](#)

[LNS RADIUS配置 — Merit RADIUS](#)

[路由器配置](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[調試輸出](#)

[從LAC路由器進行良好調試](#)

[從LNS路由器進行良好調試](#)

[可能出錯 — 從LAC進行錯誤調試](#)

[可能出現錯誤 — LNS的調試錯誤](#)

[LNS記帳記錄](#)

[相關資訊](#)

## 簡介

本文說明如何使用從RADIUS伺服器下載的通道屬性設定第2層通道通訊協定(L2TP)虛擬專用撥接網路(VPDN)情境。在本示例中，L2TP訪問集中器(LAC)接收傳入連線並聯絡LAC RADIUS伺服器。RADIUS伺服器會尋找使用者網域的通道屬性(例如cisco.com)，並將通道屬性傳遞到LAC。根據這些屬性，LAC發起到L2TP網路伺服器(LNS)的隧道。建立通道後，LNS使用自己的RADIUS伺服器對終端使用者進行身份驗證。

**附註：**本文檔假設NAS(LAC)已配置為常規撥號訪問。有關如何配置撥號的詳細資訊，請參閱[為撥入客戶端配置基本AAA RADIUS](#)。

有關L2TP和VPDN的詳細資訊，請參閱以下文檔：

- [瞭解VPDN](#)

- [配置虛擬專用網路](#)
- [第2層通道通訊協定](#)

## [必要條件](#)

### [需求](#)

本文件沒有特定需求。

### [採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

- 兩台Cisco 2511路由器
- Cisco IOS®軟體版本12.0(2)。T
- Cisco Secure ACS for UNIX、Cisco Secure ACS for Windows或Merit RADIUS

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### [慣例](#)

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

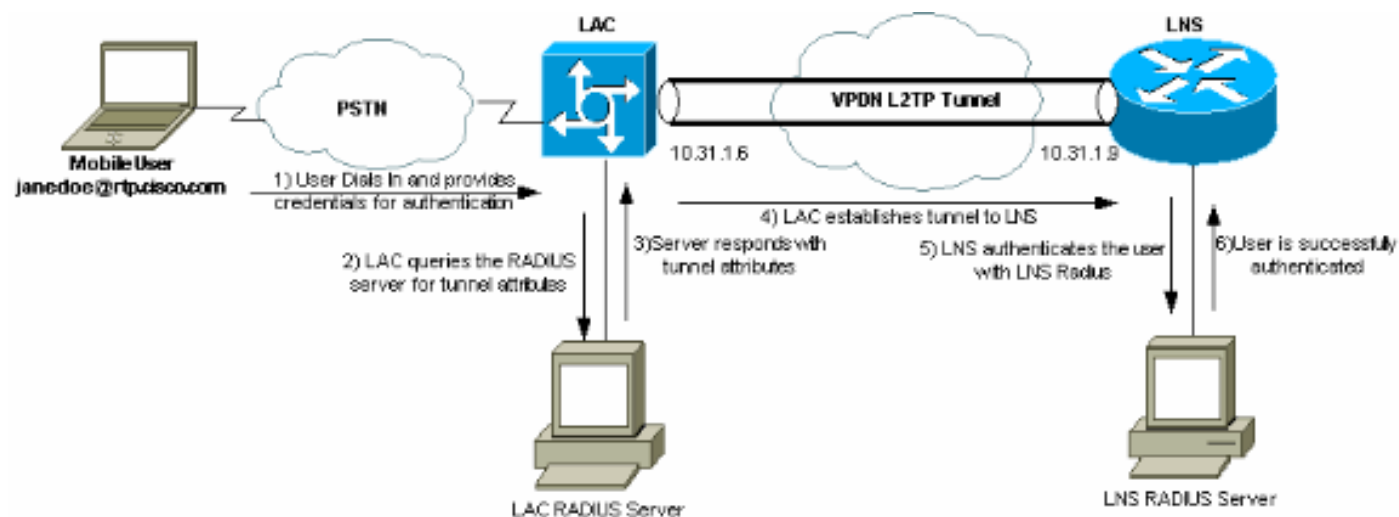
## [RADIUS伺服器組態](#)

本節提供用於設定本文件中所述功能的資訊。

**注意：**要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)（[僅限註冊客戶](#)）。

### [網路圖表](#)

本檔案會使用下圖中所示的網路設定。



## [LAC RADIUS配置 — Cisco Secure ACS for UNIX](#)

LAC RADIUS配置包括使用者「rtp.cisco.com」（客戶端使用的域）。此使用者的密碼必須是 **cisco**。

```
# ./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"
}
}
}
```

有關LAC上RADIUS配置的詳細資訊，請參閱[第2層隧道協定](#)中的[供LAC使用的RADIUS配置](#)部分。

## [LNS RADIUS配置 — Cisco Secure ACS for 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配置 — Cisco Secure ACS for Windows](#)

請完成以下步驟：

1. 在網路配置區域中，設定LAC網路訪問伺服器(NAS)身份驗證以使用RADIUS(Cisco IOS/PIX)。
2. 為使用者「rtp.cisco.com」配置口令 **cisco**，用於明文和CHAP。這是用於通道屬性的使用者名稱。
3. 按一下左側導航欄中的 **Group Setting** 按鈕。選擇使用者所屬的組，然後按一下 **編輯設定**。向下滾動到 **IETF RADIUS** 部分，然後選擇 **Attribute 6 Service-Type** 作為 **Outbound**。如果未顯示所有可選選項，請進入 **Interface Configuration** 並選中各種框，使其顯示在組區域中。
4. 在底部的 Cisco IOS/PIX RADIUS 屬性部分中，選中 **009\001 cisco-av-pair** 覈取方塊，並在框中鍵入以下內容：

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

有關LAC上RADIUS配置的詳細資訊，請參閱[第2層隧道協定](#)中的[供LAC使用的RADIUS配置](#)部分。



## Group Setup

Jump To Access Restrictions

**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 Outbound

[007] Framed-Protocol PPP

[009] Framed-IP-Netmask 0.0.0.0

[010] Framed-IP-Netmask

### [LNS RADIUS配置 — Cisco Secure ACS for Windows](#)

請完成以下步驟：

1. 配置使用者ID `janedoe@rtp.cisco.com`，並輸入任何密碼以使用plain和CHAP。
2. 按一下左欄中的**Group Setup**按鈕。選擇使用者所屬的組，然後按一下**編輯設定**。
3. 在「Internet Engineering Task Force(IETF)RADIUS Attributes」部分，從下拉選單中選擇 **Service-type(attribute 6)= Framed** 和 **Framed-Protocol(attribute 7)=PPP**。注意：還必須按一下選定屬性Service-Type和Framed-Protocol旁邊的**覈取方塊**。

### [LAC RADIUS配置 — Merit RADIUS](#)

**注意：**必須經常修改Livingston和Merit伺服器以支援供應商特定的av對。

```
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"
```

有關LAC上RADIUS配置的詳細資訊，請參閱[第2層隧道協定](#)中的[供LAC使用的RADIUS配置](#)部分。

## [LNS RADIUS配置 — Merit RADIUS](#)

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

## [路由器配置](#)

本檔案會使用這些設定。

- [LAC路由器配置](#)
- [LNS路由器配置](#)

### LAC路由器配置

```
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$9jkyuJR6fJV2JO./Qt0lC1  
enable password ww ! username cse password 0 csecse  
username john password 0 doe ip subnet-zero no ip  
domain-lookup ! jnj00=tfdfv 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
```

## LNS路由器配置

```
LNS#show run
Building configuration...

Current configuration:
!
! Last configuration change at 12:17:54 UTC Sun Feb 7
1999
!==m6knr5yui6yt6egv2wr25nfdlrsion 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 $l$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:l2tp-
tunnel-password !--- configured in the LAC RADIUS
server. 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 matches
the tunnel-id !--- configured in the LAC RADIUS server).
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
```

## 驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- **show vpdn tunnel** — 以摘要樣式格式顯示有關所有活動的第2層轉發和L2TP隧道的資訊。
- **show caller ip** — 顯示您提供的IP地址的呼叫者資訊摘要。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 疑難排解指令

**注意：**發出debug指令之前，請先參閱[有關Debug指令的重要資訊](#)。

- **debug aaa authentication** — 顯示有關AAA/TACACS+身份驗證的資訊。
- **debug aaa authorization** — 顯示有關AAA/TACACS+授權的資訊。
- **debug aaa accounting** — 在發生責任事件時顯示有關這些事件的資訊。此命令顯示的資訊與用於將記帳資訊傳輸到伺服器的記帳協定無關。
- **debug radius** — 顯示與RADIUS關聯的詳細調試資訊。
- **debug vtemplate** — 顯示虛擬訪問介面的克隆資訊，從虛擬模板克隆到呼叫結束時虛擬訪問介面關閉為止。
- **debug vpdn error** — 顯示阻止PPP隧道建立的錯誤或導致已建立的隧道關閉的錯誤。
- **debug vpdn events** — 顯示有關屬於正常PPP隧道建立或關閉部分的事件的消息。
- **debug vpdn l2x-errors** — 顯示阻止第2層建立或阻止其正常操作的第2層協定錯誤。
- **debug vpdn l2x-events** — 顯示有關屬於第2層正常PPP隧道建立或關閉的事件的消息。
- **debug vpdn l2tp-sequencing** — 顯示有關L2TP的消息。

## 調試輸出

有關L2TP調試的詳細說明，請參閱[L2TP隧道設定和拆卸](#)。

### 從LAC路由器進行良好調試

```
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=''
  authn_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: Tnl/C1 51/1 L2TP: Session FS enabled
Feb 7 12:22:17: Tnl/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: Tnl 51 L2TP: SM State idle
Feb 7 12:22:17: Tnl 51 L2TP: O SCCRQ
Feb 7 12:22:17: Tnl 51 L2TP: Tunnel state change
from idle to wait-ctl-reply
Feb 7 12:22:17: Tnl 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: Tnl 51 L2TP: I SCCRP from the_LNS
!--- Tunnel authentication is successful. Feb 7 12:22:17: Tnl 51 L2TP: Got a challenge from
remote
peer, the_LNS
Feb 7 12:22:17: Tnl 51 L2TP: Got a response from remote
peer, the_LNS
Feb 7 12:22:17: Tnl 51 L2TP: Tunnel Authentication
success
Feb 7 12:22:17: Tnl 51 L2TP: Tunnel state change from
wait-ctl-reply to established
Feb 7 12:22:17: Tnl 51 L2TP: O SCCCN to the_LNS tnlid 38
Feb 7 12:22:17: Tnl 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
Asyncl, changed state to up
LAC#
```

## 從LNS路由器進行良好調試

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 tnl 51

Feb 7 12:22:16: Tnl 38 L2TP: New tunnel created for
remote DEFGH, address 10.31.1.6
Feb 7 12:22:16: Tnl 38 L2TP: Got a challenge in SCCRQ,
DEFGH
Feb 7 12:22:16: Tnl 38 L2TP: O SCCRP to DEFGH tnlid 51
Feb 7 12:22:16: Tnl 38 L2TP: Tunnel state change from
idle to wait-ctl-reply
Feb 7 12:22:16: Tnl 38 L2TP: I SCCCN from DEFGH tnl 51
Feb 7 12:22:16: Tnl 38 L2TP: Got a Challenge Response
in SCCCN from DEFGH
Feb 7 12:22:16: Tnl 38 L2TP: Tunnel Authentication
success
Feb 7 12:22:16: Tnl 38 L2TP: Tunnel state change from
wait-ctl-reply to established
Feb 7 12:22:16: Tnl 38 L2TP: SM State established
```

```
Feb  7 12:22:17: Tnl 38 L2TP: I ICRQ from DEFGH tnl 51
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session FS enabled
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change
      from idle to wait-for-tunnel
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: New session created
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: O ICRP to DEFGH 51/1
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change
      from wait-for-tunnel to wait-connect
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: I ICCN from DEFGH tnl
      51, cl 1
Feb  7 12:22:17: Tnl/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-Templatel
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#
```

## 可能出錯 — 從LAC進行錯誤調試

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
```

使用者以janedoe@sj.cisco.com(而不是janedoe@rtp.cisco.com)的身份進入，但LAC RADIUS伺服器無法識別此網域。

```
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
```

以下偵錯顯示收到通道資訊，但通道另一端的IP位址無效的情況。使用者嘗試建立會話，但無法連線。

```
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
```

這些偵錯顯示發生通道密碼不相符的情況。在LNS上，「username the\_LNS password ABCDE」更改為「username the\_LNS password garbage」，因此嘗試進行通道驗證時失敗。

```
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
```

## [可能出現錯誤 — LNS的調試錯誤](#)

```
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#
```

在本示例中，「accept dialing l2tp virtual-template 1 remote DEFGH」更改為「accept dialin l2tp virtual-template 1 remote junk」。LNS無法再找到通道DEFGH（它是「垃圾郵件」）。

```
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記帳記錄

```
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
```

## 相關資訊

- [使用L2TP存取VPDN撥入](#)
- [第2層通道通訊協定](#)
- [RADIUS 支援頁面](#)
- [Cisco Secure ACS for Windows支援頁](#)
- [Cisco Secure ACS for UNIX支援頁](#)
- [要求建議 \(RFC\)](#)
- [技術支援 - Cisco Systems](#)