

# 配置使用 RADIUS 认证的第二层隧道协议

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[RADIUS 服务器配置](#)

[网络图](#)

[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](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[调试输出](#)

[LAC 路由器的正确调试](#)

[LNS 路由器的正常调试](#)

[可能的出错原因 - LAC 的错误调试](#)

[可能的出错原因 - LNS 的错误调试](#)

[LNS计费记录](#)

[相关信息](#)

## 简介

本文档描述如何使用从 RADIUS 服务器下载的隧道属性配置第二层隧道协议 (L2TP) 虚拟专用拨号网络 (VPDN) 方案。在本示例中，L2TP 接入集中器 (LAC) 收到传入连接并与 LAC RADIUS 服务器联系。RADIUS 服务器查找用户域 (例如 cisco.com) 的隧道属性并将隧道属性传送给 LAC。LAC 基于这些属性启动连接 L2TP 网络服务器 (LNS) 的隧道。隧道建立后，LNS 使用其自己的 RADIUS 服务器对最终用户进行身份验证。

**注意：**本文档假设已针对一般拨号访问对 NAS (LAC) 进行了配置。有关如何配置拨号的详细信息，请参阅[为拨入客户端配置基本 AAA RADIUS](#)。

有关 L2TP 和 VPDN 的详细信息，请参阅以下文档：

- [了解 VPDN](#)

- [配置虚拟专用网络](#)
- [第二层隧道协议](#)

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 两个 Cisco 2511 路由器
- Cisco IOS® 软件版本 12.0(2).T
- Cisco Secure ACS for UNIX、Cisco Secure ACS for Windows 或 Merit RADIUS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

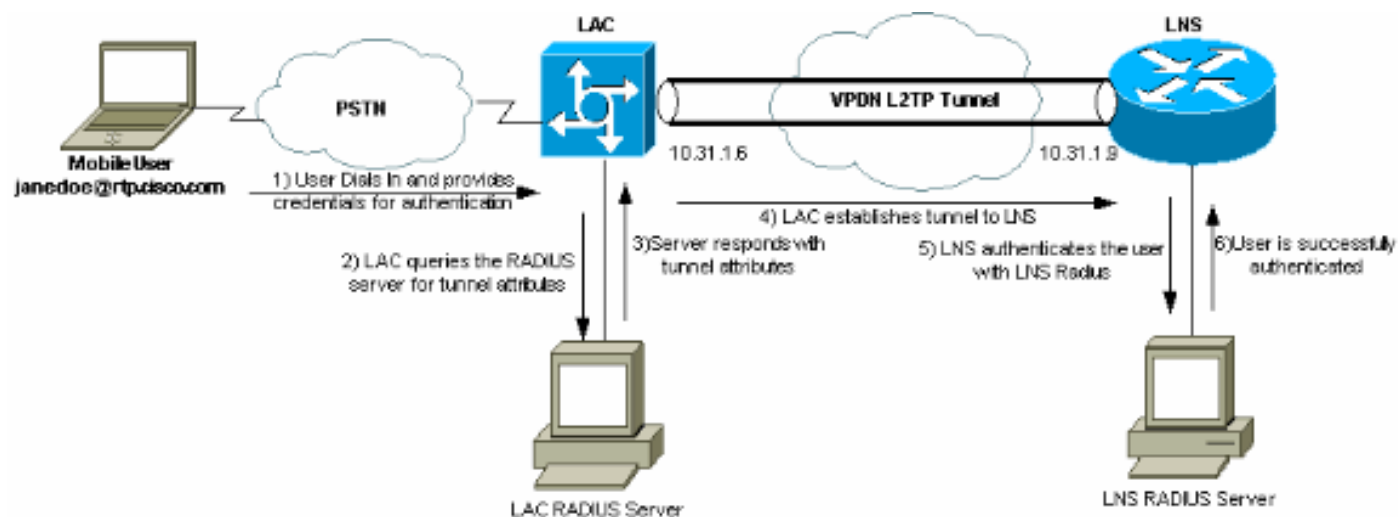
## [RADIUS 服务器配置](#)

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

### [网络图](#)

本文档使用此图所示的网络设置。



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

LAC RADIUS 配置包括用户“rtp.cisco.com”（这是客户端使用的域）。此用户的口令必须是 **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"
}
}
}
```

有关 LAC 上 RADIUS 配置的详细信息，请参阅[第二层隧道协议](#)中的[供 LAC 使用的 RADIUS 配置文件](#)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](#)

完成这些步骤：

1. 在 Network Configuration 区域中，设置 LAC 网络接入服务器 (NAS) 身份验证以使用 **RADIUS (Cisco IOS/PIX)**。
  2. 配置用户‘rtp.cisco.com’用bothplain和CHAP的密码cisco。这是用于隧道属性的用户名。
  3. 单击左侧导航栏上的 **Group Setting** 按钮。选择用户所属的组并单击 **Edit Settings**。向下滚动到 **IETF RADIUS** 部分并选择属性 6 Service-Type 作为 Outbound。如果未显示所有可选中的选项，请转到 **Interface Configuration** 并选中各个框以使它们显示在组区域中。
  4. 在底部的 Cisco IOS/PIX RADIUS 属性部分中，选中 **009\001 cisco-av-pair** 的框，并在框中键入以下内容：  
vpdn:tunnel-id=DEFGH  
vpdn:tunnel-type=l2tp  
vpdn:ip-addresses=10.31.1.9  
vpdn:l2tp-tunnel-password=ABCDE
- 有关 LAC 上 RADIUS 配置的详细信息，请参阅[第二层隧道协议](#)中的[供 LAC 使用的 RADIUS 配置文件](#)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](#)

完成这些步骤：

1. 为 plain 和 CHAP 身份验证配置用户 ID `janedoe@rtp.cisco.com` 并输入任何口令。
2. 单击左侧栏上的 **Group Setup** 按钮。选择用户所属的组并单击 **Edit Settings**。
3. 在 Internet 工程任务组 (IETF) RADIUS 属性部分中，从下拉菜单中选择 **Service-type (attribute 6) = Framed** 和 Framed-Protocol (attribute 7)=PPP。注意：还必须单击位于所选属性 **Service-Type** 和 Framed-Protocol 旁边的复选框。

### [LAC RADIUS 配置 - Merit RADIUS](#)

**注意：** 必须经常修改 Livingston 和 Merit 服务器以支持供应商特定的 av 对。

```
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"
```

有关 LAC 上 RADIUS 配置的详细信息，请参阅[第二层隧道协议](#)中的[供 LAC 使用的 RADIUS 配置文件](#)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](#)

本文档使用以下配置。

- [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./Qt0lCl enable
password ww ! username cse password 0 csecse username
john password 0 doe ip subnet-zero no ip domain-lookup !
jn100=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 !=m6knr5yui6yt6eqv2wr25nfdlrsion
l2.0=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 $1$pnYMSB.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
```

## 验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令，使用此工具可以查看对 **show** 命令输出的分析。

- **show vpdn tunnel** - 以概要风格的格式显示有关所有活动第二层转发和 L2TP 隧道的信息。
- **show caller ip** - 显示您提供的 IP 地址的呼叫方信息概要。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

### 故障排除命令

**注意：** 在发出 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- `debug aaa authentication` - 显示 AAA/TACACS+ 身份验证的信息。
- `debug aaa authorization` - 显示有关 AAA/TACACS+ 授权的信息。
- `debug aaa accounting` - 在可记帐事件出现时显示其相关信息。使用此命令显示的信息与用于向服务器传输记帐信息的记帐协议无关。
- `debug radius` - 显示与 RADIUS 关联的详细调试信息。
- `debug vtemplate` - 显示从虚拟模板克隆虚拟访问接口时到虚拟访问接口因呼叫结束而关闭时虚拟访问接口的克隆信息。
- `debug vpdn error` - 显示防止一个 PPP 隧道被设立造成一个已建隧道被关闭的错误。
- `debug vpdn events` - 显示关于正常 PPP 隧道建立或关闭的一部分事件的消息。
- `debug vpdn l2x-errors` - 显示妨碍建立第二层或妨碍其正常操作的第二层协议错误。
- `debug vpdn l2x-events` - 显示第二层的正常 PPP 隧道建立或关闭过程中的事件相关消息。
- `debug vpdn l2tp-sequencing` - 显示有关 L2TP 的消息。

## 调试输出

有关 L2TP 调试的详细说明，请参阅[L2TP 隧道设置和终止](#)。

### LAC 路由器的正确调试

```
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: Tnl/Cl 51/1 L2TP: Session FS enabled Feb 7 12:22:17: Tnl/Cl 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 SCCRQ 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 Async1, changed state to up LAC#

```

## [LNS路由器的正常调试](#)

```

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 SCCRQ 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: Vil VTEMPLATE: Reuse Vil,
recycle queue size 0 Feb 7 12:22:17: Vil VTEMPLATE: Hardware address 00e0.1e68.942c !--- Use
Virtual-template 1 for this user. Feb 7 12:22:17: Vil VPDN: Virtual interface created for
janedoe@rtp.cisco.com Feb 7 12:22:17: Vil VPDN: Set to Async interface Feb 7 12:22:17: Vil VPDN:
Clone from Vtemplate 1 filterPPP=0 blocking Feb 7 12:22:17: Vil VTEMPLATE: Has a new cloneblk
vtemplate, now it has vtemplate Feb 7 12:22:17: Vil VTEMPLATE: ***** CLONE VACCESS1
***** Feb 7 12:22:17: Vil VTEMPLATE: Clone from Virtual-Template1 interface Virtual-
Access1 default ip address no ip address encaps 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: Vil AAA/AUTHOR/FSM: (0): LCP succeeds trivially Feb 7 12:22:19: Vil VPDN:
Bind interface direction=2 Feb 7 12:22:19: Vil VPDN: PPP LCP accepted rcv CONFACK Feb 7
12:22:19: Vil VPDN: PPP LCP accepted sent CONFACK Feb 7 12:22:19: Vil 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: 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#
```

## 可能的出错原因 – LAC 的错误调试

```
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
用户以 janedoe@sj.cisco.com ( 而不是 janedoe@rtp.cisco.com ) 身份进入 , 但 LAC RADIUS 服务
器无法识别此域。
```

```
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
```

这些调试显示一种已收到隧道信息但隧道另一端的 IP 地址无效的情况。用户尝试建立会话，但无法连接。

```
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
```

这些调试显示隧道口令不匹配时的一种情况。在 LNS 上，“username the\_LNS password ABCDE”已更改为“username the\_LNS password garbage”，因此隧道身份验证在尝试时失败。

```
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
```

## 可能的出错原因 - LNS 的错误调试

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”已更改为“accept dialin l2tp virtual-template 1 remote junk”。LNS 无法再找到隧道 DEFGH ( 它已改为“junk” )。

```
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计费记录

```
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

## 相关信息

- [使用 L2TP 访问 VPDN 拨入](#)
- [第二层隧道协议](#)
- [RADIUS 支持页](#)
- [Cisco Secure ACS for Windows 支持页](#)
- [Cisco Secure ACS for UNIX 支持页](#)
- [请求注解 \(RFC\)](#)
- [技术支持 - Cisco Systems](#)