

Configurando a autenticação do protocolo do túnel da camada 2 com RADIUS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configuração de servidor RADIUS](#)

[Diagrama de Rede](#)

[Configuração RADIUS LAC - Cisco Secure ACS para UNIX](#)

[Configuração RADIUS LNS - Cisco Secure ACS para UNIX](#)

[Configuração RADIUS LAC - Cisco Secure ACS for Windows](#)

[Configuração RADIUS LNS - Cisco Secure ACS for Windows](#)

[Configuração RADIUS LAC – RADIUS da Merit](#)

[Configuração RADIUS LNS – RADIUS da Merit](#)

[Configurações do Roteador](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Saída de depurações](#)

[Boa depuração a partir do roteador LAC](#)

[Boa depuração a partir do roteador LNS](#)

[O que pode dar errado - debug ruim a partir do LAC](#)

[O que pode dar errado – Depuração inadequada a partir do LNS](#)

[Registros de relatório de LNS](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento mostra como configurar uma situação com Virtual Private Dialup Network (VPDN) do Layer 2 Tunnel Protocol (L2TP) usando atributos de túnel baixados de um servidor RADIUS. Neste exemplo, o L2TP Access Concentrator (LAC) recebe a conexão de entrada e faz contato com o servidor RADIUS LAC. O servidor RADIUS procura os atributos de túnel do domínio do usuário (por exemplo: cisco.com) e passa os atributos de túnel ao LAC. Baseado nestes atributos, o LAC inicia um túnel para o servidor de rede L2TP (LNS). Uma vez estabelecido o túnel, o LNS autentica o usuário final que usa seu próprio servidor RADIUS.

Nota: Este documento supõe que o NAS (LAC) esteve configurado para o acesso geral do seletor. Para obter mais informações sobre de como configurar o seletor, refira [configurar](#)

[RADIUS AAA básicos para clientes de discagem de entrada.](#)

Para obter mais informações sobre do L2TP e dos VPDN, refira estes documentos:

- [Entendendo o VPDN](#)
- [Configurando redes privadas virtuais](#)
- [Protocolo de túnel camada 2](#)

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Dois Cisco 2511 Router
- Software Cisco IOS® versão 12.0(2).T
- Cisco Secure ACS para UNIX, Cisco Secure ACS para Windows ou Merit RADIUS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

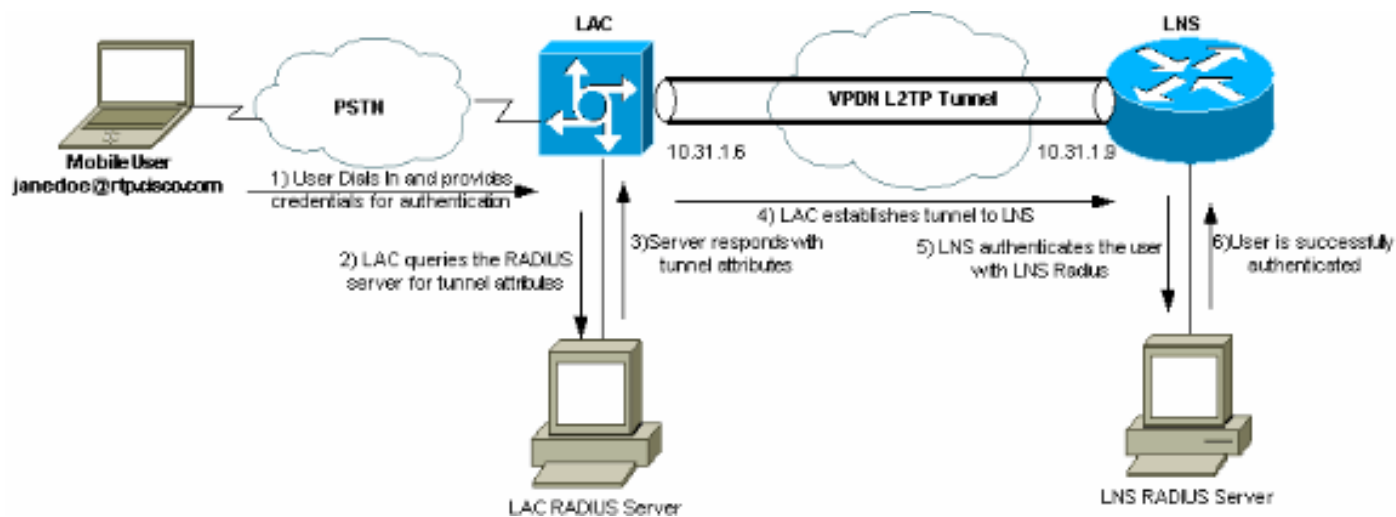
[Configuração de servidor RADIUS](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

[Diagrama de Rede](#)

Este documento utiliza a configuração de rede mostrada neste diagrama.



[Configuração RADIUS LAC - Cisco Secure ACS para UNIX](#)

A configuração RADIUS LAC inclui o usuário "rtp.cisco.com" (que é o domínio usado pelo cliente). A senha para este usuário deve ser 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"
}
}
}
```

Para obter mais informações sobre da configuração RADIUS no LAC, refira o [perfil de RADIUS para o uso da](#) seção [LAC](#) dentro do [protocolo de túnel da camada 2](#).

[Configuração RADIUS LNS - Cisco Secure ACS para 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
}
}
}
```

[Configuração RADIUS LAC - Cisco Secure ACS for Windows](#)

Conclua estes passos:

1. Na área da configuração de rede, estabelecer a autenticação do LAC Network Access Server (NAS) para usar o **RAIO (Cisco IOS/PIX)**.
2. Configurar o usuário "rtp.cisco.com" com senha Cisco para o bothplain e RACHE-O. Este é o username que é usado para os atributos de túnel.
3. Clique sobre o botão da **configuração de grupo** na barra de navegação esquerda. Selecione o grupo que o usuário pertence a e o clique **edita ajustes**. Enrole para baixo a seção do **RADIUS IETF** e selecione o **tipo de serviço** do atributo 6 como **de partida**. *Se todas as opções assinaláveis não aparecem, entre na **configuração da interface** e verifique as várias caixas para fazê-las aparecer na área do grupo.*
4. Na seção dos atributos RADIUS de Cisco IOS/PIX na parte inferior, verifique a caixa para ver se há o **Cisco-av-pair 009\001**, e datilografe isto na caixa:

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

 Para obter mais informações sobre da configuração RADIUS no LAC, refira o [perfil de RADIUS para o uso da](#) seção [LAC](#) dentro do [protocolo de túnel da camada](#)

CISCO SYSTEMS

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-Protocol

Configuração RADIUS LNS - Cisco Secure ACS for Windows

Conclua estes passos:

1. Configurar o usuário - identificação `janedoe@rtp.cisco.com` e entre toda a senha para a planície e a RACHADURA.
2. Clique sobre o **botão Group Setup Button** na barra esquerda. Selecione o grupo que o usuário pertence a e o clique **edita ajustes**.
3. Na seção para atributos RADIUS do Internet Engineering Task Force (IETF), o **tipo de serviço** seletor (**atributo 6**) = **Framed** e o **Framed-Protocol (atributo 7)=PPP** do menu suspenso.**Nota:** Você deve igualmente clicar a caixa de seleção situada ao lado dos atributos selecionados **tipo de serviço** e **Framed-Protocol**.

Configuração RADIUS LAC – RADIUS da Merit

Nota: Os server de Livingston e de Merit devem frequentemente ser alterados para apoiar AV-pares específicos de fornecedor.

```
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"
```

Para obter mais informações sobre da configuração RADIUS no LAC, refira o [perfil de RADIUS para o uso da](#) seção [LAC](#) dentro do [protocolo de túnel da camada 2](#).

Configuração RADIUS LNS – RADIUS da Merit

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

Configurações do Roteador

Este documento utiliza estas configurações.

- [Configuração do roteador de LAC](#)
- [Configuração do roteador de LNS](#)

Configuração do roteador de LAC

```
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 !
```

```

jn100=tfdfvr 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

```

Configuração do roteador de LNS

```

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 $1$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: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-
Templatel 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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre o túnel do vpdn** — A informação dos indicadores sobre toda a transmissão da camada ativa 2 e L2TP escava um túnel no formato em estilo sumário.
- **show caller ip** Exibe um resumo de informações de chamadores para o endereço IP fornecido.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Antes de emitir comandos debug, consulte [Informações importantes sobre comandos debug](#).

- **debug aaa authentication** — Exibe informações sobre autenticação AAA/TACACS+.
- **debug aaa authorization** — Exibe informações sobre autorização AAA/TACACS+.
- **debug aaa accounting** — Exibe informações sobre eventos explicáveis à medida que ocorrem. As informações exibidas por esse comando são independentes do protocolo de relatório usado para transferência das informações de relatório para um servidor.
- **debug radius** — Exibe informações de debug detalhadas associadas ao RADIUS.
- **debug vtemplate** — Exibe informações sobre clonagem de uma interface de acesso virtual do momento do clone a partir de um modelo virtual até o momento em que a interface de acesso virtual é desativada quando a chamada termina.
- **debug vpdn error** — Exibe erros que evitam que um túnel de PPP seja estabelecido ou erros que fazem com que um túnel estabelecido seja fechado.
- **debug vpdn events** — Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal de túneis PPP.
- **debug vpdn l2x-errors** — Indica os erros de protocolo da camada 2 que impedem o estabelecimento da camada 2 ou impedem sua operação normal.
- **debug vpdn l2x-events** — Indica mensagens sobre os eventos que são parte de

- estabelecimento de túnel normal ou parada programada PPP para a camada 2.
- **debug vpdn l2tp-sequencing** — Indica mensagens sobre o L2TP.

Saída de depurações

Para a descrição detalhada do L2TP debuga, referem a [configuração do túnel e o Teardown L2TP](#).

Boa depuração a partir do roteador LAC

```
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
Asyncl, 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=Asyncl idb type=10 tty=1 Feb 7 12:22:17: AAA: name=Asyncl 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='Asyncl' rem_addr='' authen_type=NONE
service=LOGIN priv=0 Feb 7 12:22:17: AAA/AUTHOR/VPDN (6239469): Port='Asyncl' 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
Asyncl 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='Asyncl' 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=Asyncl idb type=10 tty=1 Feb 7 12:22:17:
AAA: name=Asyncl 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='Asyncl'
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#

[Boa depuração a partir do roteador LNS](#)

```
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-Templatel 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: Vil AAA/AUTHOR/LCP: Authorize LCP Feb 7 12:22:19:
AAA/AUTHOR/LCP Vil (1756915964): Port='Virtual-Access1' list='' service=NET Feb 7 12:22:19:
AAA/AUTHOR/LCP: Vil (1756915964) user='janedoe@rtp.cisco.com' Feb 7 12:22:19: AAA/AUTHOR/LCP:
Vil (1756915964) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/LCP: Vil (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: Vil (1756915964) Method=RADIUS Feb 7 12:22:19: AAA/AUTHOR (1756915964): Post
authorization status = PASS_REPL Feb 7 12:22:19: Vil 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: Vil AAA/AUTHOR/FSM: (0): Can we
start IPCP? Feb 7 12:22:19: AAA/AUTHOR/FSM Vil (1311872588): Port='Virtual-Access1' list=''
service=NET Feb 7 12:22:19: AAA/AUTHOR/FSM: Vil (1311872588) user='janedoe@rtp.cisco.com' Feb 7
12:22:19: AAA/AUTHOR/FSM: Vil (1311872588) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/FSM:
Vil (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: Vil (1311872588) Method=RADIUS Feb 7 12:22:19:
AAA/AUTHOR (1311872588): Post authorization status = PASS_REPL Feb 7 12:22:19: Vil
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#
```

O que pode dar errado - debug ruim a partir do LAC

```
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
```

O usuário entra como `janedoe@sj.cisco.com` (em vez de `janedoe@rtp.cisco.com`), mas o servidor Radius LAC não reconhece este domínio.

```
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
```

Estes debugam a mostra uma situação onde a informação de túnel seja recebida, mas com um endereço IP inválido para a outra extremidade do túnel. O usuário tenta estabelecer uma sessão, mas não pode conectar.

```
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
```

Estes debugam a mostra uma situação quando há uma má combinação da senha do túnel. No LNS, “a senha ABCDE do the_LNS username” é mudada “ao lixo de senha do the_LNS username” de modo que a autenticação de túnel falhe quando tentada.

```
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
```

O que pode dar errado – Depuração inadequada a partir do LNS

```
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# Neste exemplo, o “accept dialing l2tp virtual-template 1 remote defgh” é mudado ao “accept dialin l2tp virtual-template 1 remote junk”. O LNS pode já não encontrar o túnel DEFGH (é “sucata” pelo contrário).

```
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
```

Registros de relatório de LNS

```
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
```

Informações Relacionadas

- [Alcance o discado VPDN usando o L2TP](#)
- [Protocolo de túnel camada 2](#)
- [Página de suporte RADIUS](#)
- [Cisco Secure ACS para página de suporte do Windows](#)
- [Cisco Secure ACS para página de suporte do UNIX](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico - Cisco Systems](#)