

# Configurazione dell'autenticazione Layer 2 Tunnel Protocol con RADIUS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione server RADIUS](#)

[Esempio di rete](#)

[Configurazione LAC RADIUS - Cisco Secure ACS per UNIX](#)

[Configurazione LNS RADIUS - Cisco Secure ACS per UNIX](#)

[Configurazione LAC RADIUS - Cisco Secure ACS per Windows](#)

[Configurazione LNS RADIUS - Cisco Secure ACS per Windows](#)

[Configurazione RADIUS LAC - Merit RADIUS](#)

[Configurazione LNS RADIUS - Merit RADIUS](#)

[Configurazioni router](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Output di debug](#)

[Debug corretto dal router LAC](#)

[Debug corretto dal router LNS](#)

[Problemi che possono verificarsi - Debug non corretto da LAC](#)

[Problemi che possono verificarsi - Debug non corretto da LNS](#)

[Record contabili LNS](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene descritto come configurare uno scenario VPDN (Virtual Private Dialup Network) L2TP (Layer 2 Tunnel Protocol) utilizzando gli attributi del tunnel scaricati da un server RADIUS. In questo esempio, L2TP Access Concentrator (LAC) riceve la connessione in ingresso e contatta il server RADIUS LAC. Il server RADIUS cerca gli attributi del tunnel per il dominio dell'utente (ad esempio, cisco.com) e passa gli attributi del tunnel al LAC. In base a questi attributi, il LAC avvia un tunnel verso il server di rete L2TP (LNS). Una volta stabilito il tunnel, il sistema LNS autentica l'utente finale utilizzando il proprio server RADIUS.

**Nota:** In questo documento si presume che il server NAS (LAC) sia stato configurato per l'accesso dial-up generico. Per ulteriori informazioni su come configurare la composizione, consultare il

documento sulla [configurazione della base AAA RADIUS per i client di chiamata in ingresso](#).

Per ulteriori informazioni su L2TP e VPDN, fare riferimento a questi documenti:

- [Informazioni sulla VPDN](#)
- [Configurazione delle reti private virtuali](#)
- [Protocollo tunnel di livello 2](#)

## [Prerequisiti](#)

### [Requisiti](#)

Nessun requisito specifico previsto per questo documento.

### [Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Due router Cisco 2511
- Software Cisco IOS® versione 12.0(2).T
- Cisco Secure ACS per UNIX, Cisco Secure ACS per Windows o Merit RADIUS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### [Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

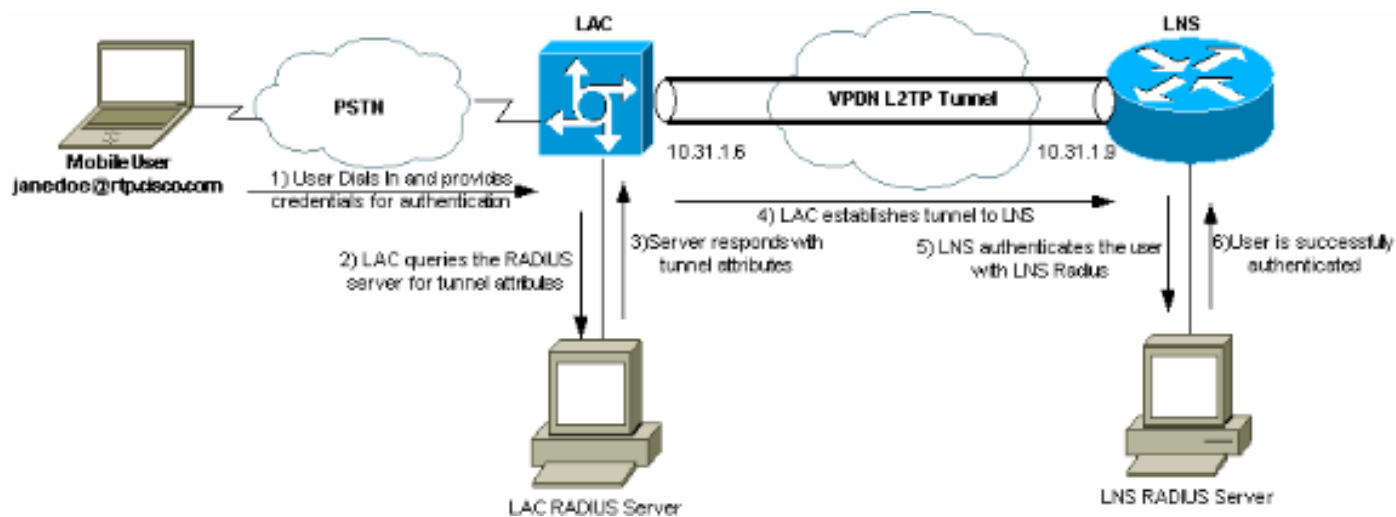
## [Configurazione server RADIUS](#)

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

### [Esempio di rete](#)

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



## [Configurazione LAC RADIUS - Cisco Secure ACS per UNIX](#)

La configurazione LAC RADIUS include l'utente "rtp.cisco.com" (che è il dominio utilizzato dal client). La password di questo utente deve essere **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"
}
}
}
```

Per ulteriori informazioni sulla configurazione di RADIUS sul LAC, consultare la sezione [RADIUS Profile for Use by the LAC](#) in the [Layer 2 Tunnel Protocol](#).

## [Configurazione LNS RADIUS - Cisco Secure ACS per 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
}
}
}
```

## [Configurazione LAC RADIUS - Cisco Secure ACS per Windows](#)

Attenersi alla seguente procedura:

1. Nell'area Configurazione rete configurare l'autenticazione LAC Network Access Server (NAS) per l'utilizzo di **RADIUS (Cisco IOS/PIX)**.
2. Configurare l'utente 'rtp.cisco.com' con la password **cisco** sia per plain che per CHAP. Nome utente utilizzato per gli attributi del tunnel.
3. Fare clic sul pulsante **Impostazioni gruppo** nella barra di navigazione a sinistra. Selezionare il gruppo a cui appartiene l'utente e fare clic su **Modifica impostazioni**. Scorrere fino alla sezione **IETF RADIUS** e selezionare Attribute 6 **Service-Type** come **Outbound**. *.Se non vengono visualizzate tutte le opzioni selezionabili, accedere a **Configurazione interfaccia** e selezionare le varie caselle per visualizzarle nell'area gruppo.*
4. Nella sezione inferiore degli attributi Cisco IOS/PIX RADIUS, selezionare la casella **009\001 cisco-av-pair** e digitare quanto segue nella casella:

```
vpdn:tunnel-id=DEFGH
```

```
vpdn:tunnel-type=l2tp
```

```
vpdn:ip-addresses=10.31.1.9
```

```
vpdn:l2tp-tunnel-password=ABCDE
```

Per ulteriori informazioni sulla configurazione di RADIUS sul LAC, consultare la sezione [RADIUS Profile for Use by the LAC](#) within [Layer 2 Tunnel Protocol](#).



## 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

### [Configurazione LNS RADIUS - Cisco Secure ACS per Windows](#)

Attendersi alla seguente procedura:

1. Configurare l'ID utente `janedoe@rtp.cisco.com` e immettere una password per la protezione CHAP e semplice.
2. Fare clic sul pulsante **Imposta gruppo** nella barra sinistra. Selezionare il gruppo a cui appartiene l'utente e fare clic su **Modifica impostazioni**.
3. Nella sezione Attributi RADIUS IETF (Internet Engineering Task Force) selezionare **Service-type (attributo 6) = Framed** and **Framed-Protocol (attributo 7)=PPP** dal menu a discesa. **Nota:** è necessario anche fare clic sulla casella di controllo accanto agli attributi **Service-Type** e **Framed-Protocol** selezionati.

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

**Nota:** i server Livingston e Merit devono essere modificati di frequente per supportare coppie av specifiche del fornitore.

```
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"
```

Per ulteriori informazioni sulla configurazione di RADIUS sul LAC, consultare la sezione [RADIUS Profile for Use by the LAC](#) within [Layer 2 Tunnel Protocol](#).

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

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

## [Configurazioni router](#)

Nel documento vengono usate queste configurazioni.

- [Configurazione router LAC](#)
- [Configurazione router LNS](#)

### Configurazione router 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 ! jnj00=tfdfdr 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

```

## Configurazione router 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 $l$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

```

## Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show vpdn tunnel**: visualizza le informazioni su tutti i tunnel Layer 2 Forwarding e L2TP attivi in formato di riepilogo.
- **show caller ip**: visualizza un riepilogo delle informazioni sul chiamante per l'indirizzo IP fornito.



## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Comandi per la risoluzione dei problemi

**Nota:** prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug aaa authentication:** visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug aaa authorization:** visualizza le informazioni sull'autorizzazione AAA/TACACS+.
- **debug aaa accounting:** visualizza le informazioni sugli eventi responsabili non appena si verificano. Le informazioni visualizzate da questo comando sono indipendenti dal protocollo di accounting utilizzato per trasferire le informazioni di accounting a un server.
- **debug radius:** visualizza informazioni di debug dettagliate associate a RADIUS.
- **debug vtemplate:** visualizza le informazioni di duplicazione per un'interfaccia di accesso virtuale dal momento in cui viene duplicata da un modello virtuale al momento in cui l'interfaccia di accesso virtuale diventa inattiva al termine della chiamata.
- **debug vpdn error:** visualizza gli errori che impediscono di stabilire un tunnel PPP o gli errori che causano la chiusura di un tunnel stabilito.
- **debug vpdn events:** visualizza i messaggi relativi agli eventi che fanno parte della normale creazione o chiusura del tunnel PPP.
- **debug vpdn l2x-errors:** visualizza gli errori del protocollo di layer 2 che impediscono la definizione del layer 2 o il normale funzionamento dello stesso.
- **debug vpdn l2x-events:** visualizza i messaggi relativi agli eventi che fanno parte della normale definizione del tunnel PPP o del processo di arresto per il layer 2.
- **debug vpdn l2tp-sequencing:** visualizza i messaggi relativi a L2TP.

## Output di debug

Per una descrizione dettagliata dei debug L2TP, consultare il documento sulla [configurazione e rimozione del tunnel L2TP](#).

### Debug corretto dal router 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 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/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
Async1, changed state to up
LAC#

```

## [Debug corretto dal router 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 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#
```

## Problemi che possono verificarsi - Debug non corretto da 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
```

L'utente viene visualizzato come janedoe@sj.cisco.com (anziché janedoe@rtp.cisco.com), ma il server RADIUS LAC non riconosce questo dominio.

```
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
```

Questi debug mostrano una situazione in cui le informazioni del tunnel vengono ricevute, ma con un indirizzo IP non valido per l'altra estremità del tunnel. L'utente tenta di stabilire una sessione, ma non riesce a connettersi.

```
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
```

Questi debug mostrano una situazione in cui le password del tunnel non corrispondono. Sull'LNS, "username the\_LNS password ABCDE" viene cambiato in "username the\_LNS password garbage" in modo che l'autenticazione tunnel non riesca quando viene tentata.

```
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
```

## Problemi che possono verificarsi - Debug non corretto da 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#
```

Nell'esempio, "accept dialing l2tp virtual-template 1 remote DEFGH" viene modificato in "accept dial in l2tp virtual-template 1 remote junk". L'LNS non riesce più a trovare il tunnel DEFGH (è invece "spazzatura").

```
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
```

## Record contabili 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
```

## Informazioni correlate

- [Accesso a VPDN Dial-in tramite L2TP](#)
- [Protocollo tunnel di livello 2](#)
- [Pagina di supporto RADIUS](#)
- [Pagina di supporto di Cisco Secure ACS per Windows](#)
- [Pagina di supporto di Cisco Secure ACS per UNIX](#)
- [RFC \(Requests for Comments\)](#)
- [Supporto tecnico – Cisco Systems](#)