Configuring Layer 2 Tunnel Protocol Authentication with RADIUS

Document ID: 13856

Contents

Introduction

This document depicts how to configure a Layer 2 Tunnel Protocol (L2TP) Virtual Private Dialup Network (VPDN) scenario using tunnel attributes downloaded from a RADIUS server. In this example, the L2TP Access Concentrator (LAC) receives the incoming connection and contacts the LAC RADIUS server. The RADIUS server looks up the tunnel attributes for the user's domain (for example, cisco.com) and passes the tunnel attributes to the LAC. Based on these attributes, the LAC initiates a tunnel to the L2TP Network Server (LNS). Once the tunnel is established, the LNS authenticates the end user using its own RADIUS server.

Note: This document assumes that the NAS (LAC) has been configured for general Dial access. For more information on how to configure dial, refer to Configuring Basic AAA RADIUS for Dial−in Clients.

For more information on L2TP and VPDNs, refer to these documents:

- Understanding VPDN
- Configuring Virtual Private Networks
- Layer 2 Tunnel Protocol

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Two Cisco 2511 routers
- Cisco IOS® Software Release 12.0(2).T
- Cisco Secure ACS for UNIX, Cisco Secure ACS for Windows, or Merit RADIUS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

RADIUS Server Configuration

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in this diagram.
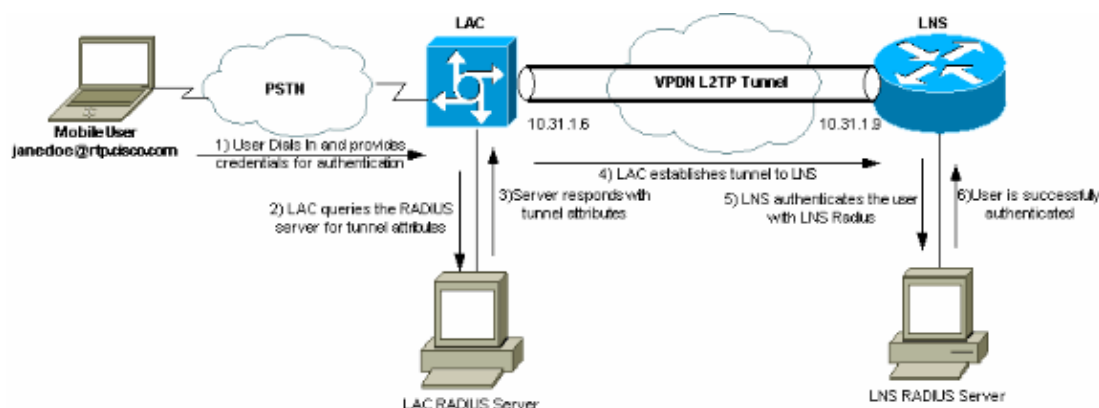
LAC RADIUS Configuration – Cisco Secure ACS for UNIX

The LAC RADIUS configuration includes the user "rtp.cisco.com" (which is the domain used by the client). The password for this user must be **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"
}
}
}
```

For more information on RADIUS configuration on the LAC, refer to the RADIUS Profile for Use by the LAC section within the Layer 2 Tunnel Protocol.

LNS RADIUS Configuration – 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 Configuration – Cisco Secure ACS for Windows

Complete these steps:

1. In the Network Configuration area, set up the LAC Network Access Server (NAS) authentication to use **RADIUS (Cisco IOS/PIX)**.
2. Configure the user 'rtp.cisco.com' with password **cisco** for both plain and CHAP. This is the username that is used for the tunnel attributes.
3. Click on the **Group Setting** button in the left navigation bar. Select the Group the user belongs to and click **Edit Settings**. Scroll down to the **IETF RADIUS** section and select Attribute 6 **Service–Type** as **Outbound.** .

   *If all checkable options do not appear, go into **Interface Configuration** and check the various boxes to make them appear in the group area.*
4. In the Cisco IOS/PIX RADIUS attributes section at the bottom, check the box for **009\001 cisco–av–pair**, and type this in the box:

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

   For more information on RADIUS configuration on the LAC, refer to the RADIUS Profile for Use by the LAC section within Layer 2 Tunnel Protocol.
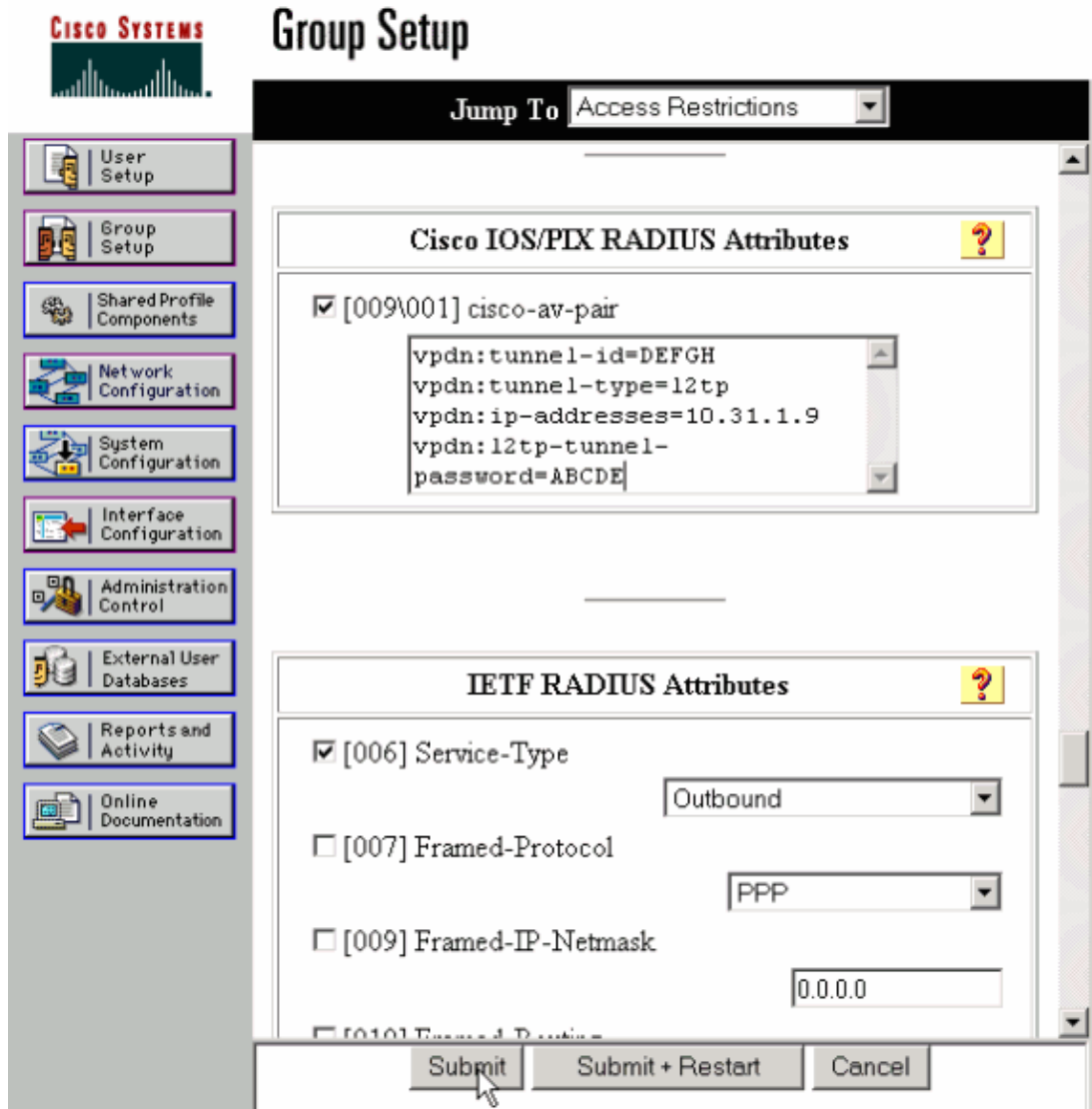
LNS RADIUS Configuration – Cisco Secure ACS for Windows

Complete these steps:

1. Configure the user id **janedoe@rtp.cisco.com** and input any password for plain and CHAP.
2. Click on the **Group Setup** button in the left bar. Select the Group the user belongs to and click **Edit Settings**.
3. In the section for Internet Engineering Task Force (IETF) RADIUS Attributes, select **Service−type (attribute 6) = Framed** and **Framed−Protocol (attribute 7)=PPP** from the drop−down menu.

   Note: You must also click the checkbox located next to the selected attributes **Service−Type** and **Framed−Protocol**.

LAC RADIUS Configuration – Merit RADIUS

Note: Livingston and Merit servers must frequently be modified to support vendor−specific av−pairs.

```
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"
```

For more information on RADIUS configuration on the LAC, refer to the RADIUS Profile for Use by the LAC section within Layer 2 Tunnel Protocol.

LNS RADIUS Configuration – Merit RADIUS

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

Router Configurations

This document uses these configurations.

- LAC Router Configuration
- LNS Router Configuration

LAC Router Configuration
```
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=tfdfr
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 Router Configuration

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

Current configuration:
!
! Last configuration change at 12:17:54 UTC Sun Feb 7 1999
!==m6knr5yui6yt6egv2wr25nfd1rsion 12.0=4rservice exec-callback
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname LNS
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default radius local
aaa authorization network default radius local
aaa accounting exec default start-stop radius
aaa accounting network default start-stop radius
enable secret 5 $1$pnYM$B.FveZjZpgA3C9ZPq/cma/
enable password ww
!
username john password 0 doe

!--- User the_LNS is used to authenticate the tunnel.
!--- The password used here must match the vpdn: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
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show vpdn tunnel** Displays information about all active Layer 2 Forwarding and L2TP tunnels in summary−style format.
- **show caller ip** Displays a summary of caller information for the IP address you provide.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug aaa authentication** Displays information on AAA/TACACS+ authentication.
- **debug aaa authorization** Displays information on AAA/TACACS+ authorization.
- **debug aaa accounting** Displays information on accountable events as they occur. The information displayed by this command is independent of the accounting protocol used to transfer the accounting information to a server.
- **debug radius** Displays detailed debugging information associated with the RADIUS.
- **debug vtemplate** Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.
- **debug vpdn error** Displays errors that prevent a PPP tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn events** Displays messages about events that are part of normal PPP tunnel establishment or shutdown.
- **debug vpdn l2x−errors** Displays Layer 2 protocol errors that prevent Layer 2 establishment or prevent its normal operation.
- **debug vpdn l2x−events** Displays messages about events that are part of normal PPP tunnel establishment or shutdown for Layer 2.
- **debug vpdn l2tp−sequencing** Displays messages about L2TP.

Debug Output

For detailed description of the L2TP debugs, refer to L2TP Tunnel Setup and Teardown.

Good Debug from LAC Router

```
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 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#
```

Good Debug from LNS Router

```
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-Template1
interface Virtual-Access1
default ip address
no ip address
encap ppp
ip unnum eth 0
no ip directed-broadcast
peer default ip address pool default
ppp authen chap
end

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

```
Feb  7 12:22:19: Vi1 L2X: Discarding packet because of
    no mid/session
Feb  7 12:22:19: AAA: parse name=Virtual-Access1 idb
    type=21 tty=-1
Feb  7 12:22:19: AAA: name=Virtual-Access1 flags=0x11
    type=5 shelf=0 slot=0 adapter=0 port=1 channel=0
Feb  7 12:22:19: AAA/AUTHEN: create_user (0x2462A0)
    user='janedoe@rtp.cisco.com' ruser='' port='Virtual-Access1'
    rem_addr='' authen_type=CHAP service=PPP priv=1
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    port='Virtual-Access1' list='' action=LOGIN
    service=PPP
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    using "default" list
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    Method=RADIUS
Feb  7 12:22:19: RADIUS: ustruct sharecount=1
Feb  7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
    id 78 171.68.120.194:1645, Access-Request, len 92
Feb  7 12:22:19:          Attribute 4 6 0A1F0109
Feb  7 12:22:19:          Attribute 5 6 00000001
Feb  7 12:22:19:          Attribute 61 6 00000005
Feb  7 12:22:19:          Attribute 1 23 6464756E
Feb  7 12:22:19:          Attribute 3 19 34A66389
Feb  7 12:22:19:          Attribute 6 6 00000002
Feb  7 12:22:19:          Attribute 7 6 00000001
Feb  7 12:22:19: RADIUS: Received from id 78
    171.68.120.194:1645, Access-Accept, len 32
Feb  7 12:22:19:          Attribute 6 6 00000002
Feb  7 12:22:19:          Attribute 7 6 00000001
Feb  7 12:22:19: AAA/AUTHEN (2229277178): status = PASS
Feb  7 12:22:19: Vi1 AAA/AUTHOR/LCP: Authorize LCP
Feb  7 12:22:19: AAA/AUTHOR/LCP Vi1 (1756915964):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    send AV protocol=lcp
Feb  7 12:22:19: AAA/AUTHOR/LCP (1756915964) found
    list "default"
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (1756915964): Post
    authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/LCP: Processing
    AV service=ppp
Feb  7 12:22:19: AAA/ACCT/NET/START User
    janedoe@rtp.cisco.com, Port Virtual-Access1, List ""
Feb  7 12:22:19: AAA/ACCT/NET: Found list "default"
Feb  7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): Can we
    start IPCP?
Feb  7 12:22:19: AAA/AUTHOR/FSM Vi1 (1311872588):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    send AV protocol=ip
Feb  7 12:22:19: AAA/AUTHOR/FSM (1311872588)
    found list "default"
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (1311872588): Post
```

```
       authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/FSM: We can start
    IPCP
Feb  7 12:22:19: RADIUS: ustruct sharecount=2
Feb  7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
    id 79 171.68.120.194:1646, Accounting-Request, len 101
Feb  7 12:22:19:          Attribute 4 6 0A1F0109
Feb  7 12:22:19:          Attribute 5 6 00000001
Feb  7 12:22:19:          Attribute 61 6 00000005
Feb  7 12:22:19:          Attribute 1 23 6464756E
Feb  7 12:22:19:          Attribute 40 6 00000001
Feb  7 12:22:19:          Attribute 45 6 00000001
Feb  7 12:22:19:          Attribute 6 6 00000002
Feb  7 12:22:19:          Attribute 44 10 30303030
Feb  7 12:22:19:          Attribute 7 6 00000001
Feb  7 12:22:19:          Attribute 41 6 00000000
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.  Her
    address 0.0.0.0, we want 0.0.0.0
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.  Her
    address 0.0.0.0, we want 0.0.0.0
Feb  7 12:22:19: RADIUS: Received from id 79
    171.68.120.194:1646, Accounting-response,
    len 20
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
    Her address 0.0.0.0, we want 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.
    Her address 0.0.0.0, we want 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
    Her address 10.6.1.1, we want 10.6.1.1
Feb  7 12:22:19: AAA/AUTHOR/IPCP Vi1 (2909132255):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV protocol=ip
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV addr*10.6.1.1
Feb  7 12:22:19: AAA/AUTHOR/IPCP (2909132255)
    found list "default"
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (2909132255): Post
    authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Reject
    10.6.1.1, using 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV addr*10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.
    Her address 10.6.1.1, we want 10.6.1.1
02:24:00: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface Virtual-Access1, changed state to up
LNS#
```

What Can Go Wrong – Bad Debug from 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
```

The user comes in as janedoe@sj.cisco.com (instead of janedoe@rtp.cisco.com), but the LAC RADIUS server does not recognize this domain.

```
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
```

These debugs show a situation where the tunnel information is received, but with an invalid IP address for the other end of the tunnel. The user attempts to establish a session, but cannot connect.

```
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
```

These debugs show a situation when there is a tunnel password mismatch. On the LNS, "username the_LNS password ABCDE" is changed to "username the_LNS password garbage" so that tunnel authentication fails when attempted.

```
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
```

What Can Go Wrong – Bad Debug from 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#
```

In this example, "accept dialing l2tp virtual–template 1 remote DEFGH" is changed to "accept dialin l2tp virtual–template 1 remote junk". The LNS can no longer find the tunnel DEFGH (it is "junk" instead).

```
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 Accounting Records

```
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
```

Related Information

- **Access VPDN Dial–in Using L2TP**
- **Layer 2 Tunnel Protocol**
- **RADIUS Support Page**
- **RADIUS in IOS Documentation**
- **Cisco Secure ACS for Windows Support Page**
- **Documentation for Cisco Secure ACS for Windows**
- **Cisco Secure ACS for UNIX Support Page**
- **Documentation for Cisco Secure ACS for UNIX**
- **Requests for Comments (RFCs)**
- **Technical Support – Cisco Systems**