

Настройка аутентификации по протоколу L2TP с использованием RADIUS

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Конфигурация сервера RADIUS](#)

[Схема сети](#)

[Настройка LAC RADIUS – Cisco Secure ACS для UNIX](#)

[Настройка LNS RADIUS – Cisco Secure ACS для UNIX](#)

[Настройка LNS RADIUS – Cisco Secure ACS для Windows](#)

[Настройка LNS RADIUS – Cisco Secure ACS для Windows](#)

[Настройка LAC RADIUS – Merit RADIUS](#)

[Настройка LNS RADIUS – Merit RADIUS](#)

[Конфигурации маршрутизатора](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Выходные данные отладки](#)

[Нормальные отладочные данные от маршрутизатора LAC](#)

[Нормальные отладочные данные от маршрутизатора LNS](#)

[Отладочные данные от маршрутизатора LAC с иллюстрацией возможных сбоев](#)

[Отладочные данные от маршрутизатора LNS с иллюстрацией возможных сбоев](#)

[Записи учета LNS](#)

[Дополнительные сведения](#)

Введение

Этот документ показывает, как настроить сценарий Layer 2 Tunnel Protocol (L2TP) Virtual Private Dialup Network (VPDN) с использованием атрибутов туннеля, загруженных с сервера RADIUS. В этом примере концентратор доступа L2TP (LAC) получает входящее соединение и обращается к серверу RADIUS LAC. Сервер RADIUS производит поиск атрибутов туннеля для домена пользователя (например, cisco.com) и передает атрибуты туннеля маршрутизатору LAC. На основе этих атрибутов LAC инициализирует туннель к сетевому серверу L2TP (LNS). После установления туннеля LNS выполняет аутентификацию конечного пользователя, используя свой собственный сервер RADIUS.

Примечание: Этот документ предполагает, что NAS (LAC) был настроен для общего доступа

через коммутируемую телефонную сеть. [Подробнее настройка доступа через коммутируемую сеть описана в документе Настройка базового AAA RADIUS для клиентов удаленного доступа.](#)

Для более подробной информации о L2TP и VPDN обращайтесь к следующим документам:

- [Общие сведения о VPDN \(виртуальная частная коммутируемая сеть\)](#)
- [Настройка виртуальных частных сетей \(VPN\)](#)
- [Протокол туннелирования 2-го уровня](#)

[Предварительные условия](#)

[Требования](#)

Для этого документа отсутствуют особые требования.

[Используемые компоненты](#)

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Два маршрутизатора Cisco 2511
- Cisco IOS® Software Release 12.0(2).T
- Cisco Secure ACS для UNIX, Cisco Secure ACS для Windows или Merit RADIUS

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

[Условные обозначения](#)

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

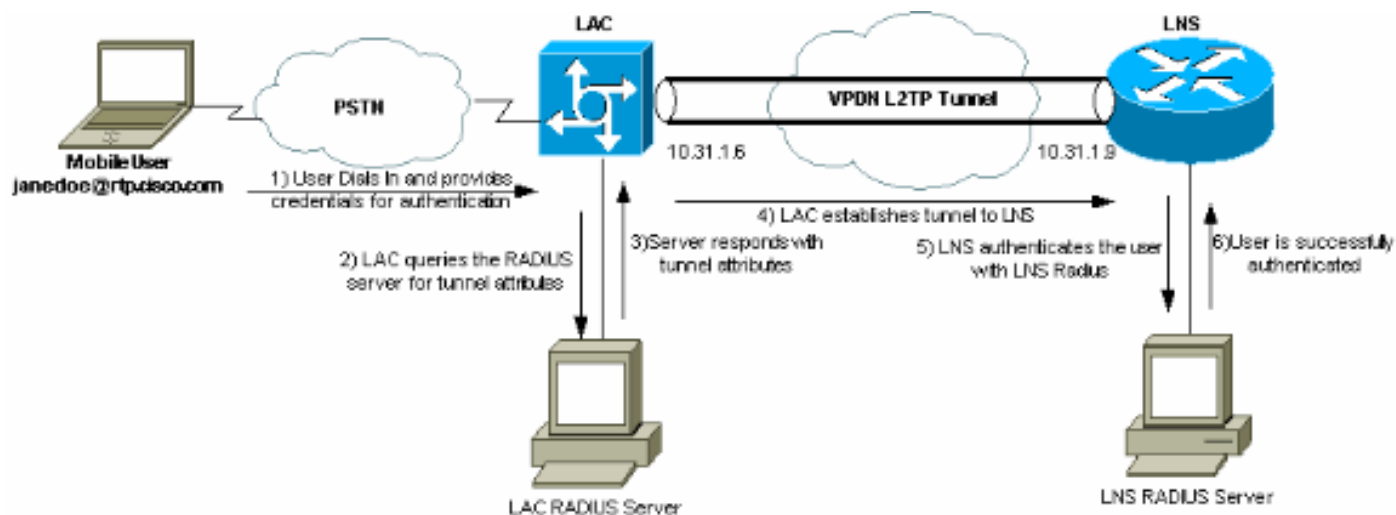
[Конфигурация сервера RADIUS](#)

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

[Схема сети](#)

В этом документе используются настройки сети, показанные на данной диаграмме.



[Настройка LAC RADIUS – Cisco Secure ACS для UNIX](#)

Конфигурация LAC RADIUS включает в себя пользователя `rtp.cisco.com` (который соответствует домену, используемому клиентом). Пароль для данного пользователя по умолчанию должен быть `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"
}
}
}
```

[Более подробно настройка RADIUS на маршрутизаторе LAC описана в разделе Профиль RADIUS для использования маршрутизатором LAC документа Протокол туннелирования 2-го уровня.](#)

[Настройка LNS RADIUS – Cisco Secure ACS для 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
}
}
}
```

[Настройка LNS RADIUS – Cisco Secure ACS для Windows](#)

Выполните следующие действия:

1. В разделе Network Configuration (Конфигурация сети) установите для сервера доступа к сети LAC NAS использование аутентификации RADIUS (Cisco IOS/PIX).
2. Настройте запись пользователя rtp.cisco.com с паролем cisco как для аутентификации открытым текстом, так и для CHAP. Это имя пользователя будет применяться для атрибутов туннеля.
3. На панели навигации нажмите кнопку Group Setting (Настройка групп). Выделите группу, к которой относится пользователь, и щелкните Edit Settings (Редактировать настройки). Пролитайте вниз до раздела IETF RADIUS и выберите для Attribute 6 значение Service-Type, равное Outbound..*Если появились не все доступные для выбора параметры, войдите в раздел Interface Configuration (Настройка интерфейсов) и отметьте флажками поля, которые должны присутствовать в области группы.*
4. В разделе атрибутов Cisco IOS/PIX RADIUS внизу отметьте 009\001 cisco-av-pair и наберите в этом поле следующее:

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

vpdn:l2tp-tunnel-password=ABCDE [Настройка RADIUS на маршрутизаторе с функцией LAC более подробно описана в разделе Профиль RADIUS для LAC документа Протокол туннелирования 2-го уровня.](#)



Group Setup

Jump To

Cisco IOS/PIX RADIUS Attributes

[009\001] cisco-av-pair

```
vpdn:tunnel-id=DEFGH
vpdn:tunnel-type=12tp
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-IP-Netmask

[Настройка LNS RADIUS – Cisco Secure ACS для Windows](#)

Выполните следующие действия:

1. Настройте идентификатор пользователя janedoe@rtp.cisco.com и введите пароль для аутентификации открытым текстом и для CHAP.
2. На панели слева нажмите кнопку Group Setup (Настройка групп). Выделите группу, к которой относится пользователь, и щелкните Edit Settings (Редактировать настройки).
3. В разделе атрибутов RADIUS IETF (Инженерной группы по развитию Интернета) в раскрывающемся меню выберите Service-type (attribute 6) = Framed (Тип службы [атрибут 6] = кадрирование) и Framed-Protocol (attribute 7)=PPP (Кадрированный протокол [атрибут 7] = PPP).Примечание: Вы должны также щелкнуть по флажку, который расположен рядом с выбранными атрибутами: Service-Type и кадрированный протокол.

Настройка LAC RADIUS – Merit RADIUS

Примечание: Ливингстон и серверы Merit должны часто модифицироваться для поддержки определяемых поставщиком ав-пар.

```
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"
```

[Настройка RADIUS на маршрутизаторе с функцией LAC более подробно описана в разделе Профиль RADIUS для LAC документа Протокол туннелирования 2-го уровня.](#)

Настройка LNS RADIUS – Merit RADIUS

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

Конфигурации маршрутизатора

Эти конфигурации используются в данном документе.

- [Конфигурация LAC-маршрутизатора](#)
- [Конфигурация маршрутизатора LNS](#)

Конфигурация LAC-маршрутизатора

```
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
```

Конфигурация маршрутизатора 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-
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
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе

конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- show vdpn tunnel– показывает сведения о всех активных туннелях пересылки 2-го уровня (L2F) и L2TP в формате сводки.
- команда show caller ip отображает сводные сведения вызывающей программы для указанного IP-адреса.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- debug aaa authentication — отображаются сведения при аутентификации AAA/TACACS+.
- debug aaa authorization — отображаются данные авторизации AAA/TACACS+.
- debug aaa accounting– выводит сведения по учетным событиям в порядке их возникновения. Информация, показанная этой командой, не зависит от протокола учета, используемого для передачи учетной информации на сервер.
- debug radius– выводит подробные данные об отладке сервера RADIUS.
- debug vtemplate– выводит информацию о клонировании интерфейса виртуального доступа с момента его клонирования из виртуального шаблона до момента отключения при завершении вызова.
- debug vpdn error– показывает ошибки, не позволяющие установить туннель или вызывающие закрытие установленного туннеля.
- debug vpdn events– выводит сообщения о событиях, свидетельствующих о нормальном ходе установления или закрытия туннеля PPP.
- debug vpdn l2x-errors– показывает ошибки протокола 2-го уровня, препятствующие установлению 2-го уровня или его нормальной работе.
- debug vpdn l2x-events– выводит сообщения о событиях, сопровождающих нормальный ход установления или закрытия туннеля PPP для 2-го уровня.
- debug vpdn l2tp-sequencing– выводит сообщения о протоколе L2TP.

Выходные данные отладки

[Подробное описание отладки L2TP см. в документе Установление и разрыв туннеля L2TP.](#)

Нормальные отладочные данные от маршрутизатора 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 Asyncl, changed state to up LAC#

Нормальные отладочные данные от маршрутизатора 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: Vil AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want
0.0.0.0 Feb 7 12:22:19: Vil AAA/AUTHOR/IPCP: Processing AV service=ppp Feb 7 12:22:19: Vil
AAA/AUTHOR/IPCP: Authorization succeeded Feb 7 12:22:19: Vil 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: Vil AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 10.6.1.1 Feb 7 12:22:19: Vil AAA/AUTHOR/IPCP: Processing AV service=ppp Feb 7 12:22:19: Vil
AAA/AUTHOR/IPCP: Authorization succeeded Feb 7 12:22:19: Vil AAA/AUTHOR/IPCP: Done. Her address
0.0.0.0, we want 10.6.1.1 Feb 7 12:22:19: Vil AAA/AUTHOR/IPCP: Start. Her address 10.6.1.1, we
want 10.6.1.1 Feb 7 12:22:19: AAA/AUTHOR/IPCP Vil (2909132255): Port='Virtual-Access1' list=''
service=NET Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vil (2909132255) user='janedoe@rtp.cisco.com' Feb 7
12:22:19: AAA/AUTHOR/IPCP: Vil (2909132255) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/IPCP:
Vil (2909132255) send AV protocol=ip Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vil (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#
```

[Отладочные данные от маршрутизатора LAC с иллюстрацией возможных сбоев](#)

```
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
Пользователь входит как janedoe@sj.cisco.com (вместо janedoe@rtp.cisco.com), но сервер
LAC RADIUS не распознает этот домен.
```

```
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
```

Эти отладочные сообщения иллюстрируют ситуацию, в которой информация о туннеле принимается, но содержит неверный IP-адрес другого конца туннеля. Пользователь пытается установить сеанс, но не может подключиться.

```
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
```

Эти отладочные сообщения иллюстрируют ситуацию, в которой не согласован пароль туннеля. На маршрутизаторе LNS запись username the_LNS password ABCDE заменяется на username the_LNS password ABCDE, вызывающую сбой при попытке аутентификации туннеля.

```
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
```

[Отладочные данные от маршрутизатора LNS с иллюстрацией возможных сбоев](#)

```
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#
```

В этом примере вместо команды accept dialing l2tp virtual-template 1 remote DEFGH вводится команда accept dialin l2tp virtual-template 1 remote junk. В результате LNS теряет возможность отыскать туннель DEFGH (он теперь именуется junk).

```
Feb 7 13:45:32: L2TP: I SCCRQ from DEFGH tnl 62 Feb 7 13:45:32: L2X: Never heard of DEFGH Feb 7
13:45:32: L2TP: Could not find info block for DEFGH
```

[Записи учета 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
```

[Дополнительные сведения](#)

- [Доступ к серверу коммутируемого доступа VPDN по протоколу L2TP](#)
- [Протокол туннелирования 2-го уровня](#)
- [Страница поддержки RADIUS](#)
- [Страница поддержки Cisco Secure ACS для Windows](#)
- [Страница поддержки Cisco Secure ACS для UNIX](#)
- [Запросы комментариев \(RFC\)](#)
- [Техническая поддержка - Cisco Systems](#)