RADIUS でのレイヤ 2 トンネルプロトコル認証の設定

目次

概要

このドキュメントでは、RADIUS サーバからダウンロードされたトンネル属性を使用して、Layer 2 Tunnel Protocol（L2TP; レイヤ 2 トンネル プロトコル）の Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）のシナリオの設定方法を示しています。 この例では、L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）が着信接続を受け付け、LAC RADIUS サーバと通信します。 RADIUS サーバは、ユーザのドメイン（cisco.com など）のトンネル属性を検索し、トンネル属性を LAC に渡します。 これらのアトリビュートに基づいて、LAC は L2TP Network Server（LNS; L2TP ネットワーク サーバ）へのトンネルを開始します。 トンネルが確立されると、LNS はそれ自体の RADIUS サーバを使用してエンド ユーザを認証します。

注: このドキュメントでは、一般のダイヤル アクセス用に NAS（LAC）が設定済みであることを前提としています。 ダイヤルの設定方法についての詳細は、『ダイヤルイン クライアントの AAA RADIUS の基本設定』を参照してください。

L2TP と VPDN の詳細は、次のドキュメントを参照してください。

- VPDN について
- バーチャル プライベート ネットワークの設定
- レイヤ 2 トンネル プロトコル

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2511 ルータ 2 台
- Cisco IOS(R) ソフトウェア リリース 12.0（2）.T
- Cisco Secure ACS for UNIX、Cisco Secure ACS for Windows、または Merit RADIUS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

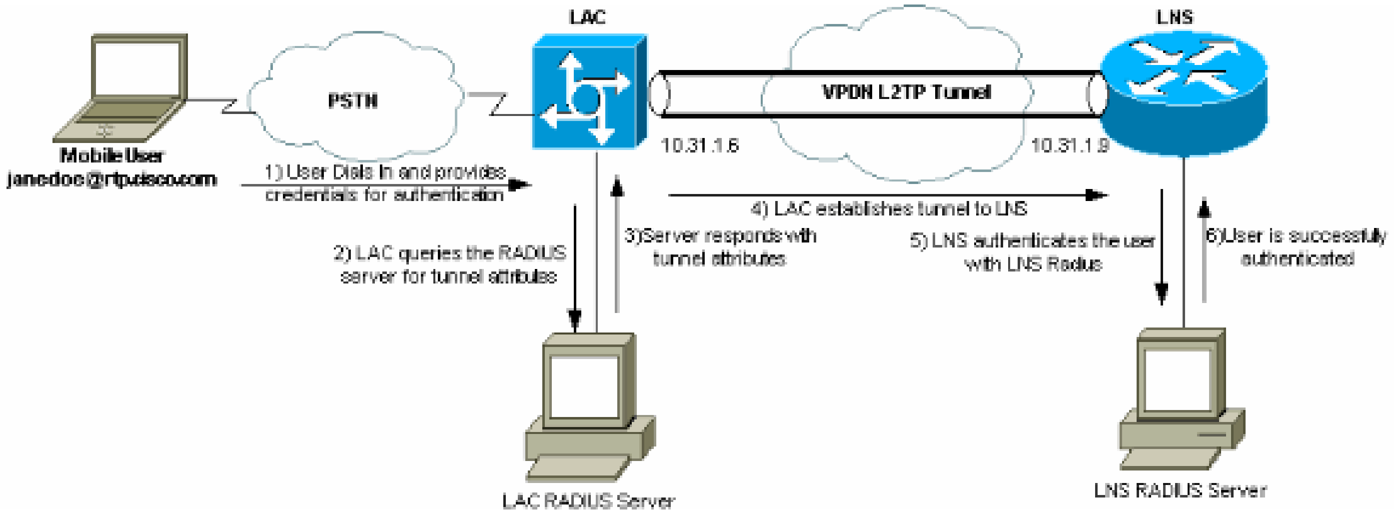
RADIUS サーバの設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。



LAC RADIUS 設定：Cisco Secure ACS for UNIX

LAC RADIUS 設定には、ユーザ「rtp.cisco.com」（クライアントが使用するドメイン）が含まれます。 このユーザのパスワードは cisco である必要があります。

```
# ./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"
}
}
}
```

LAC 上での RADIUS 設定の詳細については、『レイヤ 2 トンネル プロトコル』の「LAC による使用のための RADIUS プロファイル」セクションを参照してください。

LNS RADIUS 設定：Cisco Secure ACS for UNIX

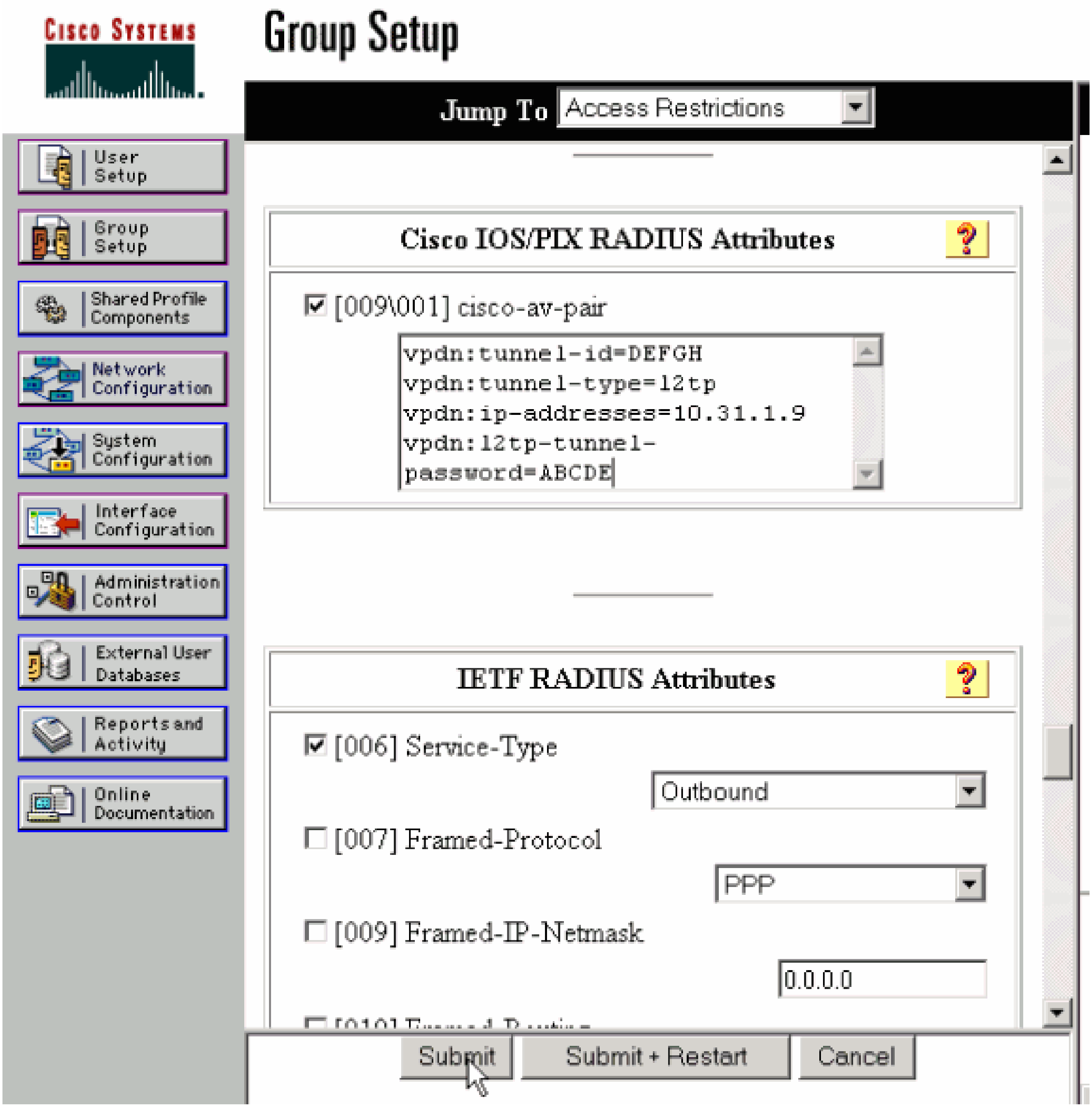
```
# ./ViewProfile -p 9900 -u janedoe@rtp.cisco.com
user = janedoe@rtp.cisco.com{
radius=Cisco {
check_items= {
2="rtp"
}
reply_attributes= {
6=2
7=1
}
}

}
```

LAC RADIUS 設定：Cisco Secure ACS for Windows

次の手順を実行します。

1. [Network Configuration] エリアで、LAC Network Access Server (NAS; ネットワーク アクセス サーバ) 認証に **[RADIUS (Cisco IOS/PIX)]** を使用するように設定します。
2. プレーンおよび CHAP の両方に、パスワードが cisco のユーザ「rtp.cisco.com」を設定します。 これは、トンネル属性に使用されるユーザ名です。
3. 左側のナビゲーション バーにある [Group Setting] ボタンをクリックします。 ユーザが属するグループを選択し、**[Edit Settings]**をクリックします。 下にスクロールして [IETF RADIUS] **セクション**に移動し、Attribute 6 の [Service-Type] に [Outbound] を選択します。 *チェック オプションがすべて表示されていない場合は、[Interface Configuration] を開き、各種ボックスにチェックを入れて、グループ エリアにこれらのボックスを表示させます。*
4. 最下部の [Cisco IOS/PIX RADIUS attributes] セクションで、**[009\001 cisco-av-pair]** のボックスにチェックマークを入れ、ボックスに次のように入力します。`vpdn:tunnel-id=DEFGH`
`vpdn:tunnel-type=l2tp`
`vpdn:ip-addresses=10.31.1.9`
`vpdn:l2tp-tunnel-password=ABCDE`LAC 上での RADIUS 設定の詳細については、『レイヤ 2 トンネル プロトコル』の「LAC による使用のための RADIUS プロファイル」セクションを参照してください。



LNS RADIUS 設定：Cisco Secure ACS for Windows

次の手順を実行します。

1. ユーザ ID **janedoe@rtp.cisco.com** を設定し、プレーンおよび CHAP 用に任意のパスワードを入力します。
2. 左側のバーにある [Group Setup] ボタンをクリックします。 ユーザが属するグループを選択し、**[Edit Settings]**をクリックします。
3. [Internet Engineering Task Force (IETF) RADIUS Attributes] のセクションのドロップダウンメニューから、[**Service-type (attribute 6) = Framed**] および [**Framed-Protocol (attribute 7)=PPP**] を選択します。**注:** 選択した属性の [Service-Type] および [Framed-Protocol] の隣にあるチェックボックスもクリックする必要があります。

LAC RADIUS 設定 - Merit RADIUS

注: Livingston サーバおよび Merit サーバは、ベンダー固有の AV ペアをサポートするために頻繁に修正する必要があります。

```
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"
```

LAC 上での RADIUS 設定の詳細については、『レイヤ 2 トンネル プロトコル』の「LAC による使用のための RADIUS プロファイル」セクションを参照してください。

LNS RADIUS 設定：Merit RADIUS

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

ルータの設定

このドキュメントでは、次の設定を使用します。

- LAC ルータの設定
- LNS ルータの設定

LAC ルータの設定
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 1Dj3K$9jkyuJR6fJV2JO./Qt01C1 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 ルータの設定

```
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
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show vpdn tunnel**：アクティブなすべてのレイヤ 2 転送および L2TP トンネルに関する情報を概要の形式で表示します。
- **show caller ip**：指定した IP アドレスの発信者情報の概要を表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『debug コマンドに関する重要な情報』を参照してください。

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。
- **debug aaa accounting**：アカウンティング可能なイベントが発生したときのそのイベントに関する情報を表示します。 このコマンドで表示される情報は、アカウンティング情報のサーバへの転送に使用されるアカウンティング プロトコルに依存しません。
- **debug radius**：RADIUS に関連するデバッグの詳細情報を表示します。
- **debug vtemplate**：仮想テンプレートからクローニングされた時点から、コールが終了して仮想アクセス インターフェイスがダウン状態になるまでの、仮想アクセス インターフェイスのクローニング情報を表示します。
- **debug vpdn error**：PPP トンネルの確立を阻止するエラー、または確立されたトンネルをクローズするエラーを表示します。
- **debug vpdn events**：通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debug vpdn l2x-errors**：レイヤ 2 の確立を阻害したり、またはその通常動作を阻害したりするレイヤ 2 プロトコルのエラーを表示します。
- **debug vpdn l2x-events**：レイヤ 2 の通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debug vpdn l2tp-sequencing**：L2TP に関するメッセージを表示します。

デバッグ出力

L2TP デバッグの詳細については、『L2TP トンネルの確立と解放』を参照してください。

LAC ルータからの正常なデバッグ

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#

LNS ルータからの正常なデバッグ

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#
```

考えられる問題：LAC からの不適切なデバッグ

```
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
```

ユーザは（janedoe@rtp.cisco.com ではなく）janedoe@sj.cisco.com として入ってきますが、LAC RADIUS サーバではこのドメインが認識されません。

```
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
```

次のデバッグは、トンネル情報が受信されるが、トンネルの相手側に対しては無効な IP アドレスとなっている状況を示します。 ユーザはセッションを確立しようとしても、接続できません。

```
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
```

次のデバッグは、トンネル パスワードの不一致がある状況を示します。 LNS では、「username the_LNS password ABCDE」が「username the_LNS password garbage」に変わるため、トンネル認証を試行しようとすると失敗します。

```
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
```

不具合の原因：LNS からの不適切なデバッグ

```
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#
```

この例では、「accept dialing l2tp virtual-template 1 remote DEFGH」が「accept dialin l2tp virtual-template 1 remote junk」に変更されます。 LNS ではもうトンネル DEFGH を見つけられ

ません（代わりに「junk」になっています）。

```
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 アカウンティング レコード

```
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
```

関連情報

- L2TP を使用した VPDN ダイヤルイン アクセス
- レイヤ 2 トンネル プロトコル
- RADIUS に関するサポート ページ
- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco Secure ACS for UNIX に関するサポート ページ
- Requests for Comments（RFC）
- テクニカルサポート - Cisco Systems