

ドメインまたは DNIS 情報のないユーザごと VPDNs の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[RADIUS サーバの設定](#)

[確認](#)

[show コマンドの出力例](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[デバッグの出力例](#)

[関連情報](#)

概要

このドキュメントでは、ドメインまたは DNIS の情報なしで、ユーザごとの VPDN を設定する設定例について説明します。

前提条件

要件

このドキュメントに特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いています。

- Cisco IOS(R) ソフトウェア リリース 12.1(4) 以降
- Cisco IOS ソフトウェア リリース 12.1(4)T 以降

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。

。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「[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。

背景説明

Virtual Private Dial-up Network (VPDN; バーチャル プライベート ダイアルアップ ネットワーク) を使用する場合は、Network Access Server (NAS; ネットワーク アクセス サーバ) (L2TP アクセス コンセントレータ、つまり LAC) が、ユーザ独自の情報に基づいてホーム ゲートウェイ (LNS) への VPDN トンネルを確立します。この VPDN トンネルには、Level 2 Forwarding (L2F; レベル 2 転送) または Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) を使用できます。VPDN トンネルを使用する必要があるかどうかを判断するには、次のことを調べます。

- ユーザ名の一部にドメイン名が含まれているかどうか。たとえば、tunnelme@cisco.com というユーザ名を使用すると、cisco.com 用のトンネルに NAS がこのユーザを転送します。
- Dialed Number Information Service (DNIS; 着信番号情報サービス)。この機能は、着信番号に基づいたコール転送機能です。つまり、特定の着信番号が設定されたすべてのコールを適切なトンネルに NAS が転送できます。たとえば、着信コールの着信番号が 5551111 の場合には、VPDN トンネルにコールを転送し、5552222 へのコールの場合には、転送しないようにできます。この機能を使用するには、電話会社のネットワークから着信番号情報が配信される必要があります。

VPDN の設定の詳細については、『[VPDN について](#)』を参照してください。

一部の状況では、ドメイン名が必要かどうかに関係なく、VPDN トンネルをユーザ名ごとに起動する必要がある場合があります。たとえば、ciscouser というユーザは cisco.com にトンネリングされ、他のユーザは NAS でローカルに終端されるような場合があります。

注：このユーザ名には、前の例のようなドメイン情報は含まれません。

VPDN のユーザごとの設定機能では、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) サーバにルータが初めて接続されるときに、構造化されたユーザ名全体が AAA サーバに転送されます。この処理により、共通ドメイン名や DNIS を使用する個々のユーザのトンネル属性を Cisco IOS ソフトウェアがカスタマイズできるようになります。

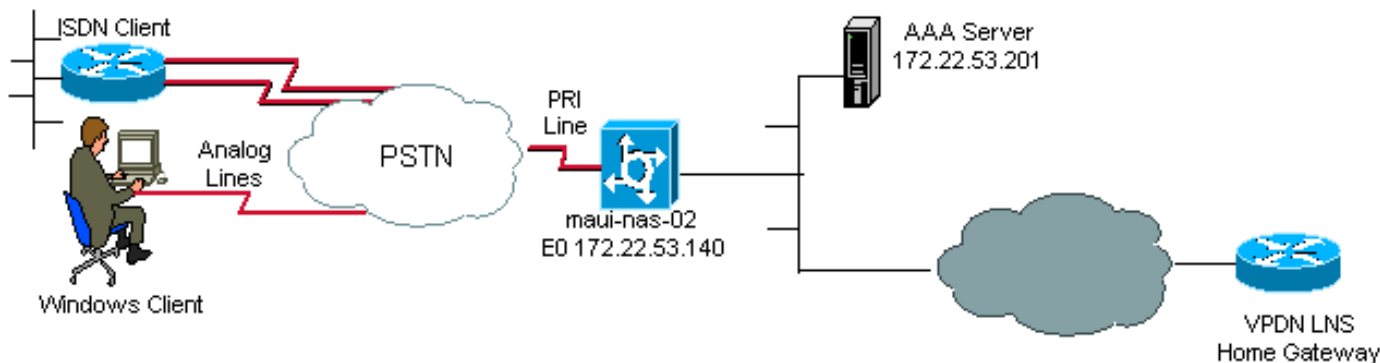
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください (登録ユーザのみ)。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

ユーザごとの VPDN をサポートするために NAS (LAC) に必要な VPDN コマンドは、`vpdn enable` と `vpdn authen-before-forward` というグローバル設定コマンドだけです。 `vpdn authen-before-forward` コマンドは、転送を決定する前に、完全なユーザ名を認証するように NAS (LAC) に指示します。次に、この個々のユーザの AAA サーバから返された情報に基づいて、VPDN トンネルが確立されます。AAA サーバから VPDN 情報が返されない場合、ユーザはローカルで終了します。このセクションの設定には、ユーザ名にドメイン情報が含まれていないときにトンネルをサポートするために必要なコマンドが示されています。

注：この設定は包括的ではありません。関連する VPDN、インターフェイス、および AAA のコマンドだけです。

注：可能なすべてのトンネルプロトコルと AAA プロトコルについて説明することは、このドキュメントの範囲外です。そのため、この設定では、AAA RADIUS サーバを使用した L2TP トンネルが実装されています。他のトンネルタイプや AAA プロトコルを設定する場合は、ここで説明されている原則や設定を適用して設定してください。

このドキュメントでは、次の設定を使用しています。

• VPDN NAS (LAC)

VPDN NAS (LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
```

```
NAS(LAC) with the VPDN attributes for the user. radius-  
server key cisco !--- The RADIUS server key.
```

RADIUS サーバの設定

Cisco Secure for Unix (CSU) RADIUS サーバのユーザ設定の一部を次に示します。

1. NAS でローカルに終端されるユーザ。

```
user1 Password = "cisco"  
Service-Type = Framed-User
```

2. VPDN セッションを確立する必要があるユーザ。

```
user2 Password = "cisco"  
Service-Type = Framed-User,  
Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",  
Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",  
Cisco-AVPair = "vpdn:tunnel-type=l2tp"
```

NAS (LAC) は、Cisco-AVPair VPDN で指定された属性を使用して、ホーム ゲートウェイへの VPDN トンネルを開始します。NAS からの VPDN トンネルを受け入れるようにホーム ゲートウェイが設定されていることを確認してください。

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドは[アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用 \)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show caller user** : 使用する TTY 回線、非同期インターフェイス (シェルフ、スロット、またはポート)、DS0 チャネル番号、モデム番号、割り当てられた IP アドレス、PPP および PPP バンドルパラメータなど、特定のユーザのパラメータを表示します。ご使用の Cisco IOS ソフトウェアバージョンでこのコマンドがサポートされていない場合は、**show user** コマンドを使用してください。
- **show vpdn** : アクティブな L2F および L2TP プロトコルトンネルに関する情報と、VPDN 内のメッセージ識別子を表示します。

show コマンドの出力例

コールが接続されたら、show caller user username コマンドおよび show vpdn コマンドを使用して、コールが正常に接続されていることを確認します。次に出力例を示します。

```
maui-nas-02#show caller user vpdn_authen
```

```
User: vpdn_authen, line tty 12, service Async  
Active time 00:09:01, Idle time 00:00:05  
Timeouts: Absolute Idle Idle  
           Session Exec  
Limits:   - - 00:10:00  
Disconnect in: - - -  
TTY: Line 12, running PPP on As12  
DS0: (slot/unit/channel)=0/0/5  
Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
```

```
Status: Ready, Active, No Exit Banner, Async Interface Active
      HW PPP Support Active
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
      Modem Callout, Modem RI is CD,
      Line is permanent async interface, Integrated Modem
Modem State: Ready
```

```
User: vpdn_authen, line As12, service PPP
```

```
Active time 00:08:58, Idle time 00:00:05
```

```
Timeouts: Absolute Idle
```

```
Limits: - -
```

```
Disconnect in: - -
```

```
PPP: LCP Open, CHAP (<- AAA)
```

```
IP: Local 172.22.53.140
```

```
VPDN: NAS , MID 4, MID Unknown
```

```
      HGW , NAS CLID 0, HGW CLID 0, tunnel open
```

```
!--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no buffer 0 input
errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0 output errors, 0
collisions, 0 interface resets maui-nas-02#show vpdn
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
```

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions
6318	3	HGW	est	172.22.53.141	1701	1

LocID	RemID	TunID	Intf	Username	State	Last Chg	Fastswitch
4	3	6318	As12	vpdn_authen	est	00:09:33	enabled

```
!--- The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active
PPTP tunnels %No active PPPoE tunnel
```

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使用できる情報を示します。

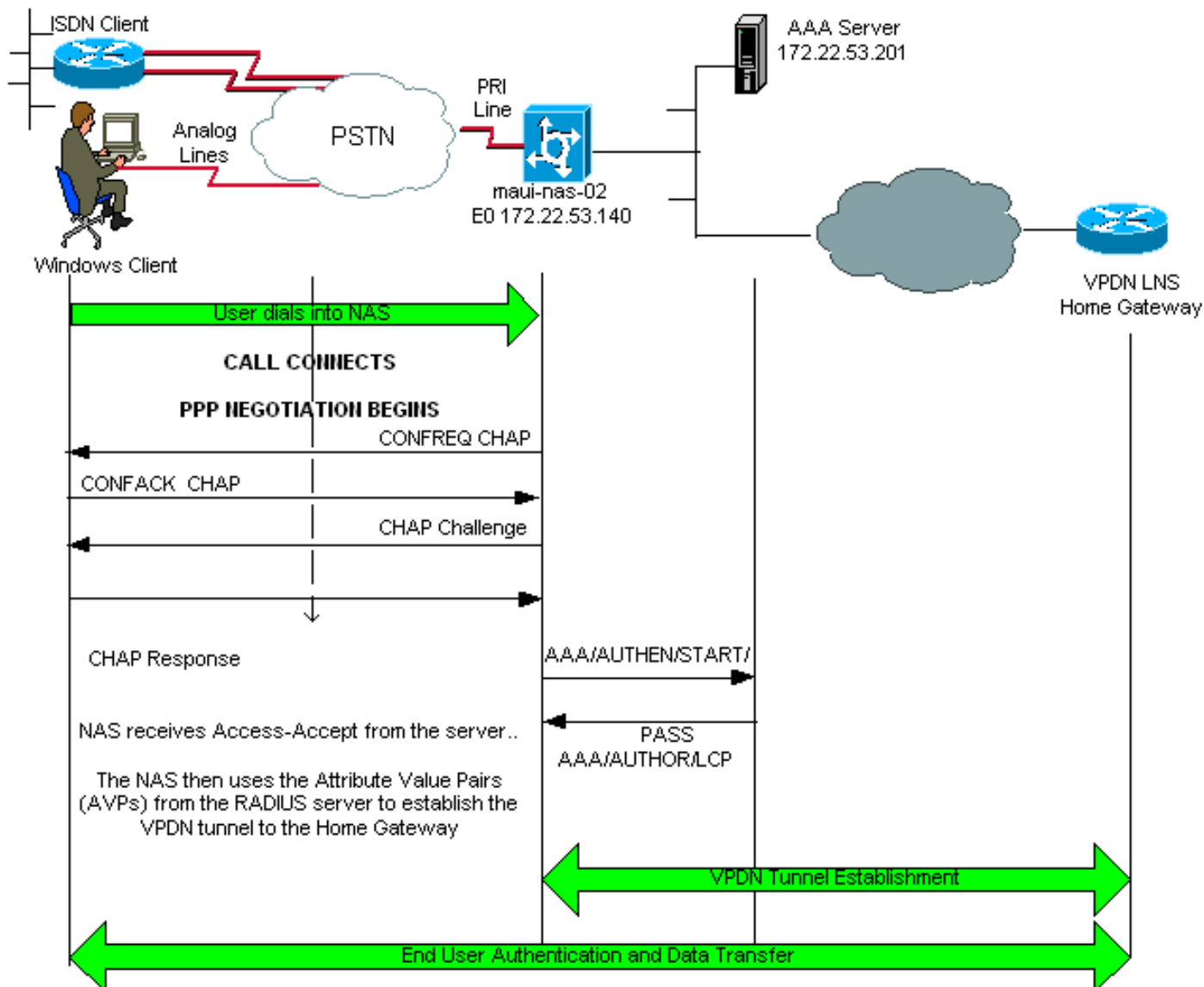
トラブルシューティングのためのコマンド

注 : debugコマンドを発行する前に、『[debugコマンドの重要な情報](#)』を参照してください。

- **debug ppp authentication:**PPP認証プロトコルメッセージを表示し、Challenge Handshake Authentication Protocol(CHAP)/パケット交換やPassword Authentication Protocol(PAP)交換を含みます。
- **debug aaa authentication:**AAA/RADIUS認証に関する情報を表示します。
- **debug aaa authorization:**AAA/RADIUS認可に関する情報を表示します。
- **debug radius -** RADIUSに関連するデバッグの詳細情報を表示します。debug radius のメッセージをデコードするには、[アウトプットインタープリタ](#) (登録ユーザ専用) を使用します。たとえば、「debug の出力例」のセクションを参照してください。どの属性がネゴシエートされているかを判断するには、debug radius の出力情報を使用します。
- **debug tacacs:**TACACS+に関連する詳細なデバッグ情報を表示します。
- **debug vpdn event:**VPDNの通常のトンネル確立またはシャットダウンの一部であるL2xエラーとイベントを表示します。
- **debug vpdn error:**VPDNプロトコルエラーを表示します。
- **debug vpdn l2x-event:**VPDNの通常のトンネル確立またはシャットダウンの一部である詳細なL2xエラーおよびイベントを表示します。
- **debug vpdn l2x-error:**VPDN L2xプロトコルエラーを表示します。

デバッグの出力例

次に、正常なコールの debug 出力を示します。この例では、VPDN トンネルの属性を Radius サーバから NAS が取得していることに注意してください。



```
maui-nas-02#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
PPP:
```

```
PPP authentication 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 onRadius protocol debugging is on
```

```
maui-nas-02#
```

```
*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial0:5 is now connected
```

```
to N/A N/A
```

```
!--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up
```

```
*Jan 21 19:07:55.352: As12 PPP: Treating connection as a dedicated line *Jan 21 19:07:55.352:
```

```
As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id
```

```
1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from
```

```
"vpdn_authen"
```

```

!--- Incoming CHAP response from user vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12
idb type=10 tty=12 *Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=12 channel=0 *Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1
*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0
channel=5 *Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, dsl=0, t3=0, slot=0, ds0=5 *Jan 21
19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12'
rem_addr='async/81560' authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): port='Async12' list='' action=LOGIN service=PPP *Jan 21
19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct
sharecount=1 *Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736: Attribute 4 6 AC16358C
*Jan 21 19:07:55.736: Attribute 5 6 0000000C
*Jan 21 19:07:55.736: Attribute 61 6 00000000
*Jan 21 19:07:55.736: Attribute 1 13 7670646E
*Jan 21 19:07:55.736: Attribute 30 7 38313536
*Jan 21 19:07:55.736: Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736: Attribute 6 6 00000002
*Jan 21 19:07:55.736: Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740: Attribute 6 6 00000002
*Jan 21 19:07:55.740: Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740: Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740: Attribute 26 30 0000000901187670

```

VPDN トンネルに必要な Attribute Value Pair (AVP; 属性値ペア) は、RADIUS サーバからプッシュされます。ただし、debug radius では、AVP とその値がコード化されて出力されます。前述の出力の太字部分を[アウトプットインタープリタ](#) ([登録ユーザ専用](#)) に貼り付けることができます。次に太字で示すデコードされた情報がアウトプットインタープリタから出力されます。

```

Access-Request 172.22.53.201:1645 id 6
Attribute Type 4: NAS-IP-Address is 172.22.53.140
Attribute Type 5: NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1: User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3: CHAP-Password is (encoded)
Attribute Type 6: Service-Type is Framed
Attribute Type 7: Framed-Protocol is PPP
    Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6: Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
...
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
!--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be

```

authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !--- the VPDN tunnel establishment debug output is omitted.

関連情報

- [VPDN について](#)
- [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設定](#)
- [RADIUS でのレイヤ2トンネルプロトコル認証の設定](#)
- [TACACS+ によるレイヤ2トンネリングプロトコル \(L2TP\) の認証の設定方法](#)
- [アクセステクノロジーに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)