



マルチホップの設定

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) 環境では、リモート ホストから生成されたセッションは既存トンネルまたは特定のドメインをルーティングするために構築されたトンネルを介してルーティングされます。通常、セッションは複数の Layer 2 Tunnel Protocol (L2TP; レイヤ 2 トンネル プロトコル) トンネルを経由して、Internet Service Provider (ISP; インターネット サービス プロバイダー) または企業ネットワークに到達することはできません。ただし、マルチホップ機能を使用すると、L2TP Access Concentrator (LAC; L2TP アクセス コンセントレータ) から L2TP トンネルに着信したセッションを終端し、リモートトラフィックを新規 L2TP トンネルを介して ISP または企業ネットワーク内の L2TP Network Server (LNS; L2TP ネットワーク サーバ) 装置にルーティングするように、Cisco 10000 シリーズ ルータを設定できます。

マルチホップ機能を使用すると、Cisco 10000 シリーズ ルータは LAC から L2TP に着信したセッションを終端し、新規 L2TP トンネルを介してルータのピア LNS にセッションを転送できます。パケットは L2TP カプセル化状態でルータに着信し、そこから別の L2TP カプセル化状態で転送されます。Cisco 10000 ルータはセッションのドメインまたはセッションが着信するトンネルに基づいて、セッションを新規トンネルにマッピングします。

また、Cisco 10000 ルータは、トンネル化された IP パケットの IP Type of Service (ToS; タイプ オブ サービス) フィールドを保護することもできます。L2TP データ パケットおよび IP パケットには、それぞれ ToS フィールドがあります。ルータは L2TP データ パケットを作成するときに、トンネル化対象のカプセル化 IP パケットの ToS フィールドを無視して、ToS フィールドを 0 (標準サービス) に設定します。トンネル化パケットの QoS (Quality Of Service) を保護するために、Cisco 10000 ルータでは、`l2tp ip tos reflect` コマンドを使用してダイヤルイン受け入れおよびダイヤルアウト要求の VPDN グループを設定できます。Virtual-Access Interface (VAI; バーチャル アクセス インターフェイス) で L2TP データ パケットを作成する場合、ルータは IP パケットの ToS フィールドを無視しないで、L2TP データ パケットにこのフィールドをコピーします。

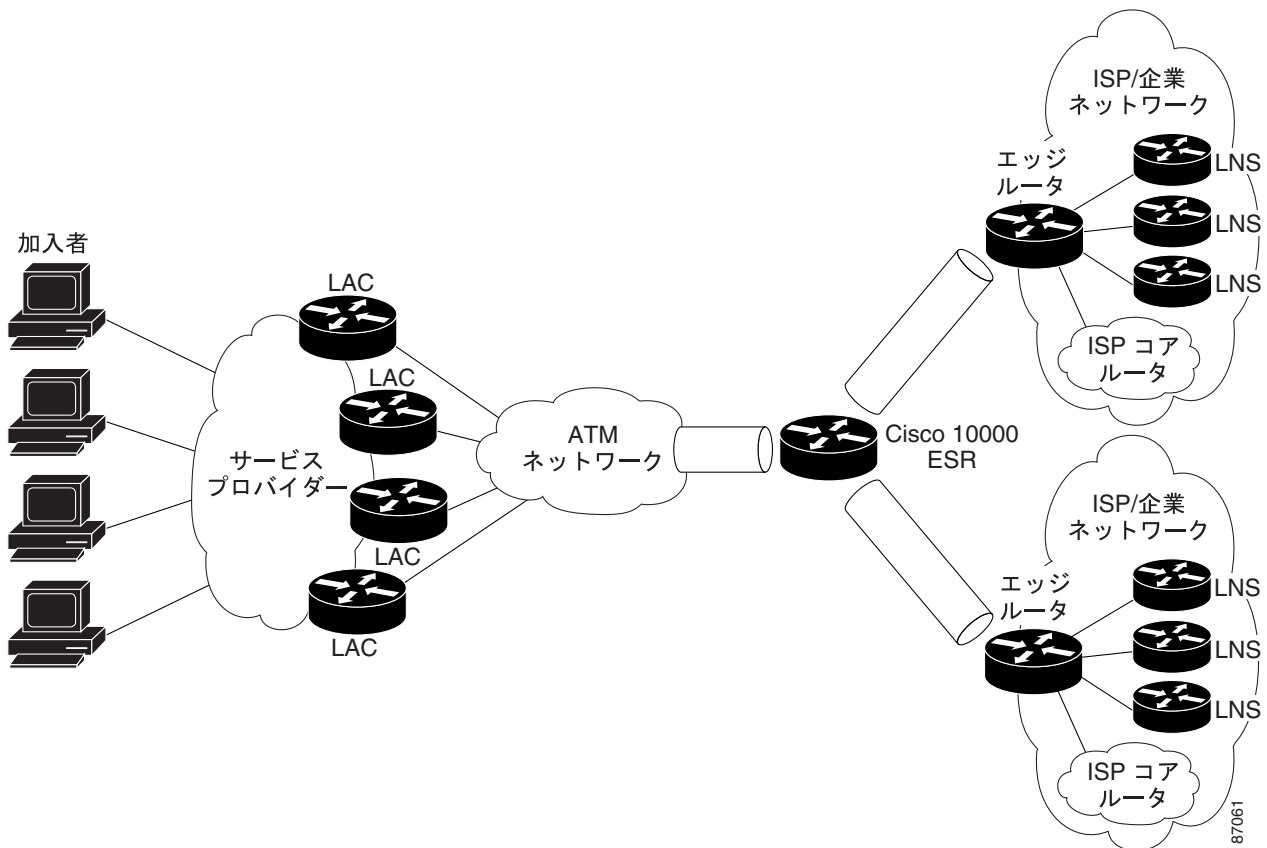


(注)

通常、Cisco IOS ソフトウェアは、内部パケット ヘッダーから外部パケット ヘッダーに ToS フィールドを反映させます。ただし、Cisco 10000 ルータは、入力ヘッダーから出力ヘッダーに ToS フィールドを伝播します。

図 9-1 に、マルチホップ トポロジの例を示します。アクセス ネットワーク側では、Cisco 10000 ルータはアクセス プロバイダーの LAC に接続しています。プロバイダー ネットワーク側では、他の ISP または企業プロバイダー ネットワークの LNS 装置に接続しています。複数の L2TP トンネルが、複数のインターフェイスまたは単一インターフェイスを介して伝送されます。通常、ルータと LAC 間またはルータと LNS 間は Asynchronous Transfer Mode (ATM; 非同期転送モード) で接続します。ただし、これは必須ではありません。L2TP トンネル化トラフィックを伝送できる任意のインターフェイスを接続に使用できます。

図 9-1 マルチホップ トポロジの例



この章では、次のマルチホップ機能について説明します。

- [マルチホップ機能の履歴 \(p.9-3\)](#)
- [マルチホップの制約事項 \(p.9-3\)](#)
- [マルチホップの必須の設定作業 \(p.9-4\)](#)
- [マルチホップの任意の設定作業 \(p.9-6\)](#)
- [マルチホップの設定例 \(p.9-8\)](#)
- [マルチホップ設定のモニタリングおよびメンテナンス \(p.9-10\)](#)

マルチホップ機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(15)BX	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2
12.3(7)XI1	この機能が Cisco IOS Release 12.3(7)XI1 に統合されました。	PRE2
12.2(28)SB	この機能が Cisco IOS Release 12.2(28)SB に統合されました。	PRE2

マルチホップの制約事項

マルチホップ機能には次の制約事項があります。

- Performance Routing Engine (PRE) (部品番号 ESR-PRE1) は、マルチホップ機能をサポートしていません。
- セッションのドメインまたはセッションが着信するトンネルに基づいて、トンネル スイッチングを行います。Cisco 10000 ルータは、Command-Line Interface (CLI; コマンドライン インターフェイス) によるセッションごとのスイッチングをサポートしていません。
- Cisco 10000 ルータは、マルチシャーシ Multilink PPP (MLP; マルチリンク PPP) をサポートしていません。
- Cisco 10000 ルータは、L2TP のマルチホップ機能をサポートしていますが、L2F プロトコルをサポートしていません。
- スイッチングされたセッションには、セッション単位の機能を適用できません。たとえば、セッションに ACL またはサービス ポリシーを適用することはできません。

トンネル化 IP パケットの IP ToS フィールドを保護する場合は、次の制約事項が適用されます。

- Cisco 10000 ルータは L2TP トンネリング プロトコルのみをサポートします。
- トンネル化されたリンクは、ToS フィールドを保護するために IP を伝送する必要があります。
- Cisco 10000 ルータはプロキシ PPP ダイアルインをサポートしていません。

マルチホップの必須の設定作業

Cisco 10000 ルータにマルチホップ機能を設定するには、次の設定作業を実行します。

- VPDN およびマルチホップ機能のイネーブル化 (p.9-4)
- LAC からのトンネルの終端 (p.9-4)
- 入力トンネル名と LNS のマッピング (p.9-5)

VPDN およびマルチホップ機能のイネーブル化

VPDN およびマルチホップ機能をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

	コマンド	目的
ステップ 1	Router(config)# vpdn enable	VPDN 機能をイネーブルにします。
ステップ 2	Router(config)# vpdn multihop	VPDN マルチホップ機能をイネーブルにします。

LAC からのトンネルの終端

LAC からのトンネルを終端するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	Router(config)# username remote-hostname password secret	リモート LAC のシークレット (パスワード) を設定します。 <i>secret</i> は、LAC に設定された <i>secret</i> と一致する必要があります。最大 11 文字の任意の ASCII 文字列で構成できます。
ステップ 2	Router(config)# username local-name password secret	ローカル装置のシークレット (パスワード) を設定します。 <i>secret</i> は、ステップ 1 で設定した <i>secret</i> と一致する必要があります。
ステップ 3	Router(config)# vpdn-group number	VPDN グループを選択します。
ステップ 4	Router(config-vpdn)# accept-dialin	LAC からのトンネル化 PPP 接続を受け入れて、ダイヤルイン受け入れ VPDN サブグループを作成します。
ステップ 5	Router(config-vpdn-acc-in)# protocol l2tp	VPDN サブグループが使用する L2TP を指定します。
ステップ 6	Router(config-vpdn-acc-in)# virtual-template number	新規 VAI をコピーするために使用されるバーチャル テンプレート インターフェイスを指定します。
ステップ 7	Router(config-vpdn-acc-in)# exit	VPDN グループ モードに戻ります。
ステップ 8	Router(config-vpdn)# terminate-from hostname remote-hostname	VPDN トンネルを受け入れる場合に必要なりモート LAC のホスト名を指定します。 <i>remote-hostname</i> は、ステップ 1 で設定した <i>remote-hostname</i> と一致する必要があります。
ステップ 9	Router(config-vpdn)# local name local-name	トンネルが自身を識別するために使用するローカル ホスト名を指定します。 <i>local-name</i> は、ステップ 2 で設定した <i>local-name</i> と一致する必要があります。

入力トンネル名と LNS のマッピング

入力トンネル名を LNS にマッピングするには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	Router(config)# username <i>username</i> password <i>secret</i>	LNS のシークレット (パスワード) を設定します。 <i>username</i> は LNS のホスト名またはトンネル ID と一致する必要があります。 <i>secret</i> は、LNS に設定された <i>secret</i> と一致する必要があります。
ステップ 2	Router(config)# username <i>egress-tunnel-name</i> password <i>secret</i>	トンネルのシークレット (パスワード) を設定します。 <i>egress-tunnel-name</i> は、トンネルのリモート (LNS) ホスト名を指定します。 <i>secret</i> は、ステップ 1 で設定した <i>secret</i> と一致する必要があります。
ステップ 3	Router(config)# vpdn-group <i>number</i>	VPDN グループを選択し、VPDN 設定モードを開始します。
ステップ 4	Router(config-vpdn)# request-dialin	Cisco 10000 ルータから LNS への L2TP トンネル要求をイネーブルにして、VPDN ダイアルイン要求サブグループモードを開始します。
ステップ 5	Router(config-vpdn-req-in)# protocol <i>l2tp</i>	VPDN サブグループが使用する L2TP を指定します。
ステップ 6	Router(config-vpdn-req-in)# multihop hostname <i>ingress-tunnel-name</i>	LAC のホスト名または入力トンネル ID に基づいて、トンネルを開始します
ステップ 7	Router(config-vpdn-req-in)# exit	VPDN グループ モードに戻ります。
ステップ 8	Router(config-vpdn)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	トンネリング先の LNS の IP アドレスを指定します。 任意で、IP アドレスに設定できる最大接続数や、IP アドレスのプライオリティ (1 が最大) を設定することもできます。
ステップ 9	Router(config-vpdn)# local name <i>egress-tunnel-name</i>	トンネルが自身を識別するために使用するローカルホスト名を指定します。 <i>egress-tunnel-name</i> は、ステップ 2 で設定した <i>egress-tunnel-name</i> と一致する必要があります。

マルチホップの任意の設定作業

Cisco 10000 ルータにマルチホップ機能を設定するには、次の任意の設定作業のいずれかを実行します。

- [入力トンネル名による VPDN トンネル許可検索の指定 \(p.9-6\)](#)
- [カプセル化 IP パケットの ToS フィールドの保護 \(p.9-6\)](#)

入力トンネル名による VPDN トンネル許可検索の指定

プロバイダーのネットワーク アクセス サーバが入力トンネル名を使用して VPDN トンネル許可検索を実行するように指定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
Router (config)# vpdn search-order multihop-hostname [domain]	設定された入力トンネル名による検索を指定します。 オプションで、ドメイン名のみによる検索を指定することもできます。


カプセル化 IP パケットの ToS フィールドの保護

カプセル化 IP パケットの ToS フィールドを保護するには、次の設定作業を行います。

- [IP ToS を保護するためのダイヤルイン受け入れ VPDN グループの設定 \(p.9-6\)](#)
- [IP ToS を保護するためのダイヤルアウト要求 VPDN グループの設定 \(p.9-7\)](#)

IP ToS を保護するためのダイヤルイン受け入れ VPDN グループの設定

IP ToS を保護するようにダイヤルイン受け入れ VPDN グループを設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	Router(config)# vpdn-group number	VPDN グループを選択し、VPDN 設定モードを開始します。
ステップ 2	Router(config-vpdn)# accept-dialin	LAC からのトンネル化 PPP 接続を受け入れて、ダイヤルイン受け入れ VPDN サブグループを作成します。
ステップ 3	Router(config-acc-in)# protocol l2tp	VPDN サブグループが使用する L2TP を指定します。  (注) L2TP は、ダイヤルアウトおよび IP ToS 保護をサポートする唯一のプロトコルです。
ステップ 4	Router(config-vpdn-acc-in)# virtual-template number	新規 VAI をコピーするために使用されるバーチャル テンプレート インターフェイスを指定します。
ステップ 5	Router(config-vpdn-acc-in)# exit	VPDN グループ モードに戻ります。
ステップ 6	Router(config-vpdn)# terminate-from hostname remote-hostname	VPDN トンネルを受け入れる場合に必要なりモート LAC のホスト名を指定します。
ステップ 7	Router(config-vpdn)# local name local-name	トンネルが自身を識別するために使用するローカル ホスト名を指定します。
ステップ 8	Router(config-vpdn)# ip tos reflect	L2TP トンネル化 IP パケットの ToS フィールドを保護するように、VPDN グループを設定します。



例 9-1 では、リモート LAC (*myhost*) からのトンネル化 PPP 接続を受け入れて、L2TP トンネル化 IP パケットの ToS フィールドを保護するように、*vpdn-group 1* を設定します。

例 9-1 IP ToS を保護するためのダイヤルイン受け入れ VPDN グループの設定

```
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname myhost
  local name local-host1
  ip tos reflect
```

IP ToS を保護するためのダイヤルアウト要求 VPDN グループの設定

IP ToS を保護するようにダイヤルアウト要求 VPDN グループを設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	Router(config)# vpdn-group <i>number</i>	VPDN グループを選択し、VPDN 設定モードを開始します。
ステップ 2	Router(config-vpdn)# request-dialout	LNS から L2TP トンネルへのダイヤルアウト コール要求をイネーブルにします。
ステップ 3	Router(config-vpdn-req-out)# protocol l2tp	VPDN サブグループが使用する L2TP を指定します。
		 (注) L2TP は、ダイヤルアウトおよび IP ToS 保護をサポートする唯一のプロトコルです。
ステップ 4	Router(config-vpdn-req-out)# pool-member <i>pool-number</i> OR Router(config-vpdn-req-out)# rotary-group <i>group-number</i>	ダイヤルアウトに使用するダイヤラ プロファイル プールまたはダイヤラ ロータリー グループを指定します。
		 (注) 設定できるのは、1 つのダイヤラ プロファイル プールまたは 1 つのダイヤラ ロータリー グループのみです。別のダイヤラ リソースを設定すると、最初のリソースが設定から削除されます。
ステップ 5	Router(config-vpdn-req-out)# exit	VPDN グループ モードに戻ります。
ステップ 6	Router(config-vpdn)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	ダイヤルアウトする LNS の IP アドレスを指定します。 任意で、IP アドレスに設定できる最大接続数や、IP アドレスのプライオリティ (1 が最大) を設定することもできます。
ステップ 7	Router(config-vpdn)# local name <i>local-name</i>	トンネルが自身を識別するために使用するローカル ホスト名を指定します。
ステップ 8	Router(config-vpdn)# ip tos reflect	L2TP トンネル化 IP パケットの ToS フィールドを保護するように、VPDN グループを設定します。

例 9-2 では、L2TP ダイアルアウト トンネルにおいて IP ToS を保護するように *vpdn-group 1* を設定します。

例 9-2 IP ToS を保護するためのダイアルアウト要求 VPDN グループの設定

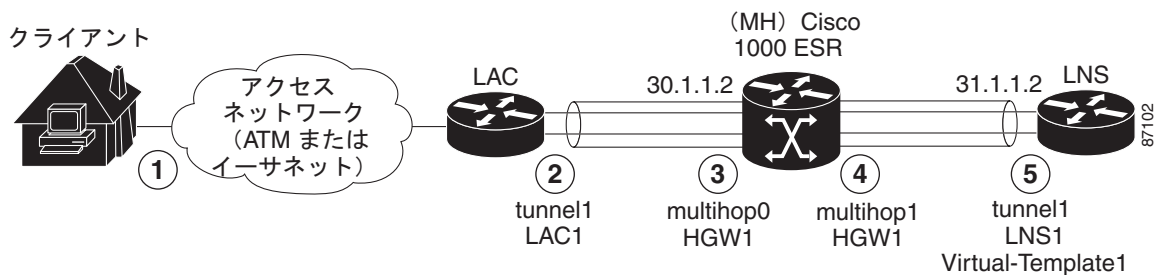
```
vpdn-group 1
  request-dialout
  protocol l2tp
  pool-member 1
  initiate-to ip 10.16.49.94
  ip tos reflect
```

マルチホップの設定例

ここでは、Cisco 10000 ルータを Multihop System (MH) として設定するマルチホップ設定の例を示します。この例には、設定を完了するための LAC および LNS の設定も含まれます。この設定例では、LAC 装置と宛先 LNS 装置間で最大 2 ホップをサポートしています。

図 9-2 にマルチホップ設定の例を示します。詳細についてはその後の説明を参照してください。

図 9-2 マルチホップ設定の例



1. リモートクライアントが LAC にダイヤルインします。LAC は Link Control Protocol (LCP; リンクコントロールプロトコル) をネゴシエーションして、ユーザを事前認証します。
2. LAC の設定により、VPDN グループ *tunnel1* が設定されます。この VPDN グループは IP アドレス 30.1.1.2 へのトンネルを開始して、*cisco.com* ドメインに関連付けられたすべてのパケットのダイヤルイン接続を要求します。tunnel1 のローカル名は *LAC1* です。この名前、tunnel1 が L2TP トンネルの受信側に対して自身を識別するために使用されます。
3. Cisco 10000 ルータは MH として機能します。LAC 側で MH 設定を使用するには、ユーザがシステムにログインする必要があります。MH 設定により、LAC から終端する L2TP トンネルを識別する VPDN グループ *multihop0* が作成されます。multihop0 トンネルは、LAC からのダイヤルイン接続のみを受け入れ、ローカル名 *Home Gateway 1 (HGW1)* を使用して自身を識別します。
4. LNS 側で、MH 接続は VPDN グループ *multihop1* を作成し、IP アドレス 31.1.1.2 の LNS への L2TP トンネルを開始します。VPDN グループ *multihop1* は、LAC のホスト名に基づいて LNS にダイヤルイン接続を要求します。multihop hostname *LAC1* コマンドを使用すると、LAC と LNS 装置が関連付けられます。multihop0 と同様に、multihop1 は同じローカル名 *HGW1* を共有します。
5. LNS の設定により、MH システムからのダイヤルイン接続を受け入れる VPDN グループ *tunnel1* が設定されます。VPDN グループ *tunnel1* は MH システム (ローカル名 *HGW1* で識別) からの L2TP トンネルを終端し、ローカル名 *LNS1* を使用して自身を識別します。LNS 設定により、バーチャル テンプレート インターフェイス *Virtual-Template1* が作成され、tunnel1 に関連付けられます。Virtual-Template1 は PAP 認証を使用し、ローカル IP アドレス プール *pool-1* を使用して IP アドレスを割り当てます。

LAC の設定

```
!  
vpdn enable  
!  
vpdn-group tunnel1  
  request-dialin  
  protocol l2tp  
  domain cisco.com  
  initiate-to ip 30.1.1.2 priority 1  
  local name LAC1  
  l2tp tunnel password 7 060A0E23  
  l2tp tunnel receive-window 100  
  l2tp tunnel retransmit timeout min 2  
!
```

マルチホップの設定


```
username user@cisco.com password 0 lab  
!  
vpdn enable  
vpdn multihop  
vpdn search-order multihop-hostname domain dnis  
!  
vpdn-group multihop0  
  accept-dialin  
  protocol l2tp  
  terminate-from hostname LAC1  
  local name HGW1  
  l2tp tunnel password 7 09404F0B  
!  
vpdn-group multihop1  
  request-dialin  
  protocol l2tp  
  multihop hostname LAC1  
  initiate-to ip 31.1.1.2 priority 1  
  local name HGW1  
  l2tp tunnel password 7 0507070D  
!
```

LNS の設定

```
vpdn enable  
!  
vpdn-group tunnel1  
  accept-dialin  
  protocol l2tp  
  virtual-template 1  
  terminate-from hostname HGW1  
  local name LNS1  
  l2tp tunnel password 7 04570A04  
  l2tp tunnel receive-window 100  
  l2tp tunnel retransmit timeout min 2  
!  
interface Virtual-Template1  
  ip unnumbered GigabitEthernet2/0/0  
  no keepalive  
  peer default ip address pool pool-1  
  ppp mtu adaptive  
  ppp authentication pap callin  
!  
ip local pool pool-1 4.2.0.0 4.2.255.255
```

マルチホップ設定のモニタリングおよびメンテナンス

マルチホップ設定および VPDN グループの監視およびメンテナンスを行うには、特権 EXEC モードで次のコマンドを入力します。

コマンド	目的
Router# show running-config	現在のルータの設定を表示します。このコマンドの出力を使用して、設定に関して次の点を確認します。 <ul style="list-style-type: none"> • VPDN およびマルチホップ機能がイネーブルである。 • LAC からのトンネルが終端されている。 • 入力トンネル名が LNS にマッピングされている。 • 入力トンネル名による VPDN トンネル許可検索が実行されている。 • (任意) L2TP トンネル化 IP パケットの ToS フィールドを保護するように、ダイヤルイン受け入れおよびダイヤルアウト要求 VPDN グループが設定されている。
Router# show vpdn	アクティブな L2TP トンネルおよびセッションの情報を表示します。
Router# show vpdn session [all [interface tunnel username] packets sequence state timers window]	インターフェイス、トンネル、ユーザ名、パケット、ステータス、ウィンドウ統計情報など、VPDN セッション情報を表示します。
Router# show vpdn tunnel [all [id local-name remote-name] packets state summary transport]	トンネルプロトコル、ID、ローカルおよびリモートトンネル名、送受信されるパケット、トンネル、トランスポートステータスなどの VPDN トンネル情報を表示します。
Router# show interface virtual-access number	VAI、LCP、プロトコル状態、およびインターフェイス統計に関する情報を表示します。次の情報は、VAI が通常の動作状態であることを示します (# は VAI の番号を示します)。 <p style="text-align: center;">Virtual-Access# is up, line protocol is up</p>
Router# clear vpdn tunnel [l2tp [remote-name local-name]]	特定のトンネルおよびそのトンネル内のすべてのセッションをシャットダウンします。
Router# debug vpdn event [protocol flow-control]	L2TP プロトコル内の VPDN エラーおよび基本イベントを表示します。フロー制御に関連するエラーも表示します。 <p> (注) フロー制御は、L2TP を使用している場合、およびリモートピア受信ウィンドウに 0 を超える値が設定されている場合のみ、使用可能です。</p>
Router# debug vpdn error	トンネルの確立を妨げるエラー、または確立されたトンネルがクローズする原因となるエラーを表示します。
Router# debug vpdn packet [control data] [detail]	シーケンス番号、フラグ、長さなど、プロトコル固有のパケットヘッダー情報を表示します。
Router# debug vpdn l2x-events	トンネルの確立時またはシャットダウン時に発生する L2TP イベントを表示します。
Router# debug vpdn l2x-errors	トンネルの確立または通常の動作を妨げる L2TP プロトコルエラーを表示します。

コマンド	目的
Router# <code>debug vpdn 12x-packets</code>	LAC と LNS 間のトンネルまたはセッション作成用ダイアログを表示します。
Router# <code>debug vpdn 12x-data</code>	L2TP データ転送をチェックします。

**注意**

デバッグ出力は CPU プロセスで高優先順位に割り当てられているので、システムを使用不能な状態にする可能性があります。そのため、特定の問題をトラブルシューティングする場合、またはシスコシステムズのテクニカル サポート担当者とのトラブルシューティング セッション時以外はデバッグ コマンドを使用しないようにしてください。また、ネットワーク トラフィックが低く、ユーザが少ないときにデバッグ コマンドを使用するのが最適です。このような時間にデバッグを行えば、デバッグ コマンドの増加したオーバーヘッド処理によってシステム利用に影響が及ぶ可能性が軽減されます。

例 9-3 に、`show vpdn` コマンドを使用した場合に表示される情報を示します。キーワードまたは引数を指定しないで `show vpdn` コマンドを使用した場合は、すべてのアクティブなセッションおよびトンネルに関する情報が表示されます。

例 9-3 show vpdn コマンド

```
Router# show vpdn
L2TP Tunnel and Session Information Total tunnels 2 sessions 22
LocID RemID Remote Name State Remote Address Port Sessions VPDN Group
12060 19602 tunnel5 est 45.1.5.5 1701 11 tunnel5

LocID RemID TunID Intf Username State Last Chg
3 3 12060 SSS Circuit u@n5 est 2d19h
2 2 12060 SSS Circuit u@n5 est 2d19h
4 4 12060 SSS Circuit u@n5 est 2d19h
5 5 12060 SSS Circuit u@n5 est 2d19h
6 6 12060 SSS Circuit u@n5 est 2d19h
7 7 12060 SSS Circuit u@n5 est 2d19h
8 8 12060 SSS Circuit u@n5 est 2d19h
9 9 12060 SSS Circuit u@n5 est 2d19h
10 10 12060 SSS Circuit u@n5 est 2d19h
11 11 12060 SSS Circuit u@n5 est 2d19h
12 12 12060 SSS Circuit u@n5 est 2d19h

LocID RemID Remote Name State Remote Address Port Sessions VPDN Group
10335 2883 tunnel6 est 45.1.6.5 1701 11 tunnel6

LocID RemID TunID Intf Username State Last Chg
14 14 10335 SSS Circuit u@n6 est 2d19h
15 15 10335 SSS Circuit u@n6 est 2d19h
16 16 10335 SSS Circuit u@n6 est 2d19h
17 17 10335 SSS Circuit u@n6 est 2d19h
18 18 10335 SSS Circuit u@n6 est 2d19h
19 19 10335 SSS Circuit u@n6 est 2d19h
20 20 10335 SSS Circuit u@n6 est 2d19h
21 21 10335 SSS Circuit u@n6 est 2d19h
22 22 10335 SSS Circuit u@n6 est 2d19h
23 23 10335 SSS Circuit u@n6 est 2d19h
13 13 10335 SSS Circuit u@n6 est 2d19h

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

例 9-4 では、**show interface virtual-access** コマンドを使用して、VAI 3 (virtual-access3) に関する情報を表示します。この例における次の情報は、通常の動作状態であることを示します。

```
Virtual-Access3 is up, line protocol is up
```

例 9-4 show interface virtual-access コマンド

```
Router# show interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 128 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open, multilink Open
  Open: IPCP
  Last input 00:02:30, output never, output hang never
  Last clearing of "show interface" counters 1d19h
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 21/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    55930 packets input, 3347967 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    105261 packets output, 9607052 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```