Cisco IOS XE ブロードバンド アクセス集約および DSL コンフィギュレーション ガイド

Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide

Cisco IOS XE Release 3S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco IOS XE ソフトウェア マニュアルについて

このマニュアルでは、Cisco IOS XE ソフトウェアのマニュアルで使用される目標、対象読者、表記法、およびマニュアルの構成について説明します。技術サポート、追加のマニュアル、およびその他の情報をシスコから取得するためのリソースも記載されています。このマニュアルは、次のセクションから構成されています。

- 「マニュアルの目標」（P.i）
- 「対象読者」（P.i）
- 「マニュアルの表記法」（P.i）
- 「マニュアルの構成」（P.iii）
- 「追加のリソースとマニュアルのフィードバック」（P.xi）

マニュアルの目標

Cisco IOS XE マニュアルでは、シスコのネットワーク デバイスを設定して保守するために実行可能な作業とコマンドについて説明します。

対象読者

Cisco IOS XE マニュアル セットは、シスコのネットワーク デバイス（ルータやスイッチなど）の設定と保守を行うが、設定作業と保守作業、作業間の関係、または特定の作業を実行するために必要な Cisco IOS コマンドに関する知識がないユーザを対象としています。Cisco IOS XE マニュアル セットは、Cisco IOS XE ソフトウェアの使用経験があり、Cisco IOS XE の現行リリースの新機能、新しい設定オプション、および新しいソフトウェア特性を理解する必要があるユーザも対象としています。

マニュアルの表記法

Cisco IOS XE マニュアルでは、*ルータ*という用語は、さまざまなシスコ製品（たとえば、ルータ、アクセス サーバ、およびスイッチ）を指すために使用されることがあります。Cisco IOS XE ソフトウェアをサポートするこれらの製品とその他のネットワーク デバイスは、例で同じように示され、図示のためだけに使用されます。ある製品を示す例は、他の製品がサポートされないことを必ずしも意味しているわけではありません。

このセクションには次のトピックがあります。

- 「印刷時の表記法」（P.ii）
- 「コマンド構文の表記法」（P.ii）
- 「ソフトウェアの表記法」（P.iii）
- 「読者への警告の表記法」（P.iii）

印刷時の表記法

Cisco IOS XE マニュアルでは、印刷時に次の表記法が使用されます。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（キーは大文字で表記しますが、小文字で入力してもかまいません）。
ストリング	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コミュニティ ストリングを *public* に設定する場合は、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。

コマンド構文の表記法

Cisco IOS XE マニュアルでは、コマンド構文に関して次の表記法が使用されます。

表記法	説明
太字	記載されているとおりに入力するコマンドおよびキーワードは、太字で示します。
イタリック体	ユーザが値を指定する引数は、イタリック体で示します。
[x]	省略可能なキーワードまたは引数は角カッコで囲みます。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、キーワード セットまたは引数セットのうちの選択肢を示します。
[x | y]	パイプで区切られたキーワードまたは引数を囲む角カッコは、省略可能な選択肢を示します。
{x | y}	パイプで区切られたキーワードまたは引数を囲む波カッコは、必須の選択肢を示します。
[x {y | z}]	角カッコ内の波カッコおよびパイプは、省略可能な要素の中で、必ずいずれかか 1 つを選択しなければならないことを示します。

ソフトウェアの表記法

Cisco IOS XE ソフトウェアでは、次の表記法が使用されます。

表記法	説明
courier フォント	courier フォントは PC または端末画面に表示される情報に使用されます。
太字の courier フォント	太字の courier フォントは、ユーザが入力しなければならないテキストを示します。
< >	山カッコで囲まれたテキストは、パスワードなど、表示されないテキストを表します。山カッコは、ASCII テキストなど、イタリック体スタイルがサポートされないコンテキストでも使用されます。
!	行の先頭にある感嘆符は、コードの行ではなくコメントの後に続くテキストです。感嘆符は、Cisco IOS XE ソフトウェアの特定のプロセスでも表示されます。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

読者への警告の表記法

Cisco IOS XE マニュアルでは、読者への警告について次の表記法が使用されます。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイス 「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

マニュアルの構成

ここでは、Cisco IOS XE マニュアル セット、その構成方法、および Cisco.com でのアクセス方法について説明します。コンフィギュレーション ガイド、コマンド リファレンス、およびマニュアル セットを構成する補足の参照とリソースがリストされています。

- 「Cisco IOS XE マニュアル セット」（P.iv）
- 「Cisco.com の Cisco IOS XE マニュアル」（P.iv）
- 「コンフィギュレーション ガイド、コマンド リファレンス、および補足リソース」（P.v）

Cisco IOS XE マニュアル セット

Cisco IOS XE マニュアル セットは次のように構成されます。

- リリース ノートおよび警告には、リリースのプラットフォーム、テクノロジー、および機能サポートに関する情報と、リリースされた Cisco IOS XE ソフトウェアでの重大度 1（最悪）、重大度 2（重大）、および重大度 3（中程度）の障害に関する説明が記載されています。他のマニュアルの前にリリース ノートを確認して、機能に更新が行われたかどうかを調べてください。
- テクノロジー別に編成され、標準の Cisco IOS XE リリースごとに発行される一連のコンフィギュレーション ガイドとコマンド リファレンス。
  - コンフィギュレーション ガイド：Cisco IOS XE 機能の概念的な説明とタスク指向の説明が記載されているマニュアルの組み合わせ。
  - コマンド リファレンス：関連するコンフィギュレーション ガイドを構成する、Cisco IOS XE 機能とプロセスで使用されるコマンドに関する詳細が記載された、アルファベット順のコマンド ページの組み合わせ。テクノロジーごとに、すべての Cisco IOS XE リリースを対象とし、標準のリリースのたびに更新される単一のコマンド リファレンスがあります。
- **debug** コマンドのコマンド リファレンス マニュアル。
- 特定のリリースにおける全コマンドと、リリースでの新規、変更済み、削除済み、または置き換え済みの全コマンドのリスト。
- すべての Cisco IOS XE リリースのシステム メッセージのリファレンス マニュアル。

Cisco.com の Cisco IOS XE マニュアル

次のセクションでは、マニュアルの構成と、さまざまなタイプのマニュアルへのアクセス方法について説明します。

Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

コンフィギュレーション ガイド

コンフィギュレーション ガイドは、テクノロジーとリリース別に提供され、リリースとテクノロジーに関連する個々の機能ガイド セットで構成されます。

コマンド リファレンス

コマンド リファレンス マニュアルでは、多数の異なるソフトウェア リリースとプラットフォームでサポートされる Cisco IOS XE コマンドについて説明しています。マニュアルはテクノロジー別に構成されています。すべての Cisco IOS XE コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html にある『*Cisco IOS Master Command List, All Releases*』を参照してください。

Cisco IOS XE 補足マニュアルとリソース

補足マニュアルとリソースは、表 2（P.xi）にリストされています。

コンフィギュレーション ガイド、コマンド リファレンス、および補足リソース

表 1 には、マニュアルの内容の簡単な説明を含め、Cisco IOS XE ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスがアルファベット順にリストされています。コマンド リファレンスには、すべてのリリースの Cisco IOS ソフトウェアと Cisco IOS XE ソフトウェアのコマンドが記載されています。コマンド リファレンスでは、多数の異なるソフトウェア リリースとプラットフォームがサポートされます。お使いの Cisco IOS XE ソフトウェア リリースまたはプラットフォームでは、一部のテクノロジーがサポートされないことがあります。

表 2 には、Cisco IOS XE ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスを補足するマニュアルとリソースがリストされています。これらの補足リソースには、リリース ノートおよび警告、マスター コマンド リスト、新規、変更済み、削除済み、および置き換え済みのコマンドのリスト、システム メッセージ、およびデバッグ コマンド リファレンスがあります。

特定のネットワーク デバイスの設定と操作に関する追加情報を取得して、Cisco IOS マニュアルにアクセスするには、次の URL にある Cisco.com の Product/Technologies Support エリアにアクセスしてください。

http://www.cisco.com/go/techdocs

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide*』	Cisco ASR 1000 シリーズ ルータでサポートされている SPA Interface Processor（SIP; SPA インターフェイス プロセッサ）と Shared Port Adapter（SPA; 共有ポート アダプタ）の設定とトラブルシューティング。
• 『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』	Cisco ASR 1000 シリーズの集約サービス ルータ固有のソフトウェア機能の概要。
• 『*Cisco IOS XE Access Node Control Protocol Configuration Guide*』 • 『*Cisco IOS Access Node Control Protocol Command Reference*』	Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）と Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）の間の通信プロトコル。
• 『*Cisco IOS XE Asynchronous Transfer Mode Configuration Guide*』 • 『*Cisco IOS Asynchronous Transfer Mode Command Reference*』	LAN ATM、Multiprotocol over ATM（MPoA）、および WAN ATM。
• 『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』 • 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』	PPP over Ethernet（PPPoE）。

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス（続き）

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco IOS XE Carrier Ethernet Configuration Guide*』 • 『*Cisco IOS Carrier Ethernet Command Reference*』	IEEE 802.3ad リンク バンドル。イーサネット、ギガビット イーサネット リンク、および EtherChannel バンドルの Link Aggregation Control Protocol（LACP）サポート。ギガビット EtherChannel バンドル上での Stateful Switchover（SSO; ステートフル スイッチオーバー）、In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）、Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）および Nonstop Routing（NSR; ノンストップ ルーティング）の LACP サポート。IEEE 802.3ad リンク アグリゲーション MIB。
• 『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』 • 『*Cisco IOS Configuration Fundamentals Command Reference*』	自動インストール、設定、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）、Cisco IOS File System（IFS）、Cisco IOS Web ブラウザ User Interface（UI）、基本的なファイル転送サービス、およびファイル管理。
• 『*Cisco IOS XE DECnet Configuration Guide*』 • 『*Cisco IOS DECnet Command Reference*』	DECnet プロトコル。
• 『*Cisco IOS XE Dial Technologies Configuration Guide*』 • 『*Cisco IOS Dial Technologies Command Reference*』	非同期通信、ダイヤル バックアップ、ダイヤラ テクノロジー、Multilink PPP（MLP; マルチリンク PPP）、PPP、および Virtual Private Dial-up 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）。
• 『*Cisco IOS XE High Availability Configuration Guide*』 • 『*Cisco IOS High Availability Command Reference*』	High Availability（HA; ハイ アベイラビリティ）を備えたエンドツーエンド ネットワークの作成を容易にするためのさまざまなネットワーク セグメント（企業アクセスからサービス プロバイダー コアに至る）で使用可能なさまざまなハイ アベイラビリティ機能とテクノロジー。Cisco IOS HA 機能とテクノロジーは、システムレベルの復元力、ネットワークレベルの復元力、および復元力のために埋め込まれた管理の 3 つの主な領域にカテゴリ化できます。
• 『*Cisco IOS XE Intelligent Services Gateway Configuration Guide*』 • 『*Cisco IOS Intelligent Services Gateway Command Reference*』	加入者 ID、サービスとポリシーの判別、セッション作成、セッション ポリシー適用、セッション ライフサイクル管理、アクセスおよびサービス使用のアカウンティング、およびセッション状態モニタリング。
• 『*Cisco IOS XE Interface and Hardware Component Configuration Guide*』 • 『*Cisco IOS Interface and Hardware Component Command Reference*』	LAN インターフェイス、論理インターフェイス、シリアル インターフェイス、仮想インターフェイス、およびインターフェイス コンフィギュレーション。
• 『*Cisco IOS XE IP Addressing Services Configuration Guide*』 • 『*Cisco IOS IP Addressing Services Command Reference*』	IP アドレス指定、Address Resolution Protocol（ARP; アドレス解決プロトコル）、Network Address Translation（NAT; ネットワーク アドレス変換）、Domain Name System（DNS; ドメイン ネーム システム）、Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）、および Next Hop Address Resolution Protocol（NHRP）。

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス（続き）

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco IOS XE IP Application Services Configuration Guide*』 • 『*Cisco IOS IP Application Services Command Reference*』	Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）、IP サービス、Transmission Control Protocol（TCP; 伝送制御プロトコル）、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）。
• 『*Cisco IOS XE IP Multicast Configuration Guide*』 • 『*Cisco IOS IP Multicast Command Reference*』	Protocol Independent Multicast（PIM）sparse mode 希薄モード（PIM-SM; PIM 希薄モード）、bidirectional PIM（bidir-PIM; 双方向 PIM）、Source Specific Multicast（SSM）、Multicast Source Discovery Protocol（MSDP）、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、および Multicast VPN（MVPN; マルチキャスト VPN）。
• 『*Cisco IOS XE IP Routing: BFD Configuration Guide*』	Bidirectional Forwarding Detection（BFD）。
• 『*Cisco IOS XE IP Routing: BGP Configuration Guide*』 • 『*Cisco IOS IP Routing: BGP Command Reference*』	Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、マルチプロトコル BGP、IP マルチキャスト用マルチプロトコル BGP 拡張。
• 『*Cisco IOS XE IP Routing: EIGRP Configuration Guide*』 • 『*Cisco IOS IP Routing: EIGRP Command Reference*』	Enhanced Interior Gateway Routing Protocol（EIGRP）。
• 『*Cisco IOS XE IP Routing: ISIS Configuration Guide*』 • 『*Cisco IOS IP Routing: ISIS Command Reference*』	Intermediate System-to-Intermediate System（IS-IS）。
• 『*Cisco IOS XE IP Routing: ODR Configuration Guide*』 • 『*Cisco IOS IP Routing: ODR Command Reference*』	On-Demand Routing（ODR; オンデマンド ルーティング）。
• 『*Cisco IOS XE IP Routing: OSPF Configuration Guide*』 • 『*Cisco IOS IP Routing: OSPF Command Reference*』	Open Shortest Path First（OSPF）。
• 『*Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide*』 • 『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』	IP ルーティング プロトコル独立機能およびコマンド。一般的な Policy-Based Routing（PBR; ポリシーベース ルーティング）機能およびコマンドが含まれます。
• 『*Cisco IOS XE IP Routing: RIP Configuration Guide*』 • 『*Cisco IOS IP Routing: RIP Command Reference*』	Routing Information Protocol（RIP）。
• 『*Cisco IOS XE IP SLAs Configuration Guide*』 • 『*Cisco IOS IP SLAs Command Reference*』	Cisco IOS IP Service Level Agreement（IP SLA; IP サービス レベル契約）。
• 『*Cisco IOS XE IP Switching Configuration Guide*』 • 『*Cisco IOS IP Switching Command Reference*』	シスコ エクスプレス フォワーディング。

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス（続き）

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco IOS XE IPv6 Configuration Guide*』 • 『*Cisco IOS IPv6 Command Reference*』	IPv6 機能、プロトコル、およびテクノロジーの一覧については、次の URL にある IPv6 のマニュアル『Start Here』にアクセスしてください。 http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.html
• 『*Cisco IOS XE ISO CLNS Configuration Guide*』 • 『*Cisco IOS ISO CLNS Command Reference*』	ISO Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）。
• 『*Cisco IOS XE LAN Switching Configuration Guide*』 • 『*Cisco IOS LAN Switching Command Reference*』	VLAN および Multilayer Switching（MLS; マルチレイヤ スイッチング）。
• 『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』 • 『*Cisco IOS Multiprotocol Label Switching Command Reference*』	MPLS Label Distribution Protocol（LDP; ラベル配布プロトコル）、MPLS レイヤ 2 VPN、MPLS レイヤ 3 VPN、MPLS Traffic Engineering（TE; トラフィック エンジニアリング）、および MPLS Embedded Management（EM）と MIB。
• 『*Cisco IOS XE NetFlow Configuration Guide*』 • 『*Cisco IOS NetFlow Command Reference*』	ネットワーク トラフィック データの分析、集約キャッシュ、およびエクスポート機能。
• 『*Cisco IOS XE Network Management Configuration Guide*』 • 『*Cisco IOS Network Management Command Reference*』	基本的なシステム管理、システム モニタリングとロギング、Cisco IOS Scripting with Tool Control Language（TCL）、Cisco Networking Service（CNS）、Embedded Event Manager（EEM; 組み込み型イベントマネージャ）、Embedded Syslog Manager（ESM）、HTTP、Remote Monitoring（RMON; リモート モニタリング）、および SNMP。
• 『*Cisco IOS XE Novell IPX Configuration Guide*』 • 『*Cisco IOS Novell IPX Command Reference*』	Novell Internetwork Packet Exchange（IPX）プロトコル。
• 『*Cisco IOS XE Optimized Edge Routing Configuration Guide*』 • 『*Cisco IOS Optimized Edge Routing Command Reference*』	Optimized Edge Routing（OER）モニタリング、およびネットワーク間の複数接続の場合の自動ルート最適化と負荷分散。
• 『*Cisco IOS XE Performance Routing Configuration Guide*』 • 『*Cisco IOS Performance Routing Command Reference*』	Performance Routing（PfR）は標準的なルーティング技術の機能を高める技術であり、アプリケーション トラフィック用に最適な出力パスまたは入力パスを判断するため、WAN インフラストラクチャ上の 2 つのデバイス間のパスのパフォーマンスの追跡または品質の確認が行えます。
• 『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』 • 『*Cisco IOS Quality of Service Solutions Command Reference*』	Class-based Weighted Fair Queueing（CBWFQ）、Low Latency Queueing（LLQ; 低遅延キューイング）、Modular Quality of Service（QoS）Command-Line Interface（CLI; コマンドライン インターフェイス）（MQC; モジュラ QoS コマンドライン インターフェイス）、Network-Based Application Recognition（NBAR）、プライオリティ キューイング、QoS のマルチリンク PPP（MLP）、ヘッダー圧縮、Resource Reservation Protocol（RSVP; リソース予約プロトコル）、Weighted Fair Queueing（WFQ; 均等化キューイング）、および Weighted Random Early Detection（WRED; 重み付けランダム早期検出）。

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス（続き）

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco IOS Security Command Reference*』	Access Control List（ACL; アクセス コントロール リスト）、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、ファイアウォール、IP セキュリティと暗号化、ネイバー ルータ認証、ネットワーク アクセス セキュリティ、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）、RADIUS、および TACACS+。
• 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』	IPsec VPN の Internet Key Exchange（IKE; インターネット キー エクスチェンジ）、IPsec を使用した VPN のセキュリティ、VPN アベイラビリティ機能（逆ルート注入、IPsec 優先ピア、および IPsec トンネル ピアの Real-Time Resolution）、IPsec データ プレーン機能、IPsec 管理プレーン機能、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）、Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、Easy VPN、および Cisco Group Encrypted Transport VPN（GET VPN）。
• 『*Cisco IOS XE Security Configuration Guide: Securing the Control Plane*』	Control Plane Policing、ネイバーフッド ルータ認証。
• 『*Cisco IOS XE Security Configuration Guide: Securing the Data Plane*』	アクセス コントロール リスト（ACL）、ファイアウォール、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）およびゾーンベース ファイアウォール、Cisco IOS Intrusion Prevention System（IPS; 侵入防御システム）、Flexible Packet Matching、Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）、Threat Information Distribution Protocol（TIDP）および TMS。
• 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』	AAA（Network Admission Control（NAC; ネットワーク アドミッションコントロール）を含む）、セキュリティ サーバ プロトコル（RADIUS と TACACS+）、Secure Shell（SSH; セキュア シェル）、ネットワーキング デバイスのセキュア アクセス（Autosecure とロールベース CLI アクセスを含む）、合法的傍受。
• 『*Cisco IOS XE Service Advertisement Framework Configuration Guide*』 • 『*Cisco IOS Service Advertisement Framework Command Reference*』	Cisco Service Advertisement Framework。
• 『*Cisco IOS XE VPDN Configuration Guide*』 • 『*Cisco IOS VPDN Command Reference*』	Dialed Number Identification Service（DNIS; 着信番号識別サービス）によるマルチホップ、L2TP および Layer 2 Forwarding（L2F）の場合のタイマーと再試行の改良、RADIUS アトリビュート 82（トンネル割り当て ID）、VPDN ユーザのシェルベース認証、トンネル ターミネータでの RADIUS によるトンネル認証。
• 『*Cisco IOS XE Wide-Area Networking Configuration Guide*』 • 『*Cisco IOS Wide-Area Networking Command Reference*』	フレーム リレー、L2VPN 擬似回線冗長性、Media-Independent PPP、およびマルチリンク PPP。

表 1　Cisco IOS XE コンフィギュレーション ガイドとコマンド リファレンス（続き）

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能 / プロトコル / テクノロジー
• 『*Cisco Unified Border Element (Enterprise) Configuration Guide*』 • 『*Cisco IOS Voice Command Reference*』	Cisco ASR 1000 上の Cisco Unified Border Element（Enterprise）は、エンタープライズ ユーザ向けのスケーラブルなオプションを提供します。Cisco Unified Border Element（Enterprise）は、Cisco ASR 1000 上のプロセスとして動作し、高速 RTP パケット処理パスを使用します。これは、SIP および H.323 の音声およびビデオ ネットワークを相互接続するために、エンタープライズおよび商業用の顧客によって、IP-to-IP ゲートウェイとして使用されます。Cisco UBE（Enterprise）は、シグナリング インターワーキング、メディア インターワーキング、アドレスおよびポート変換、課金、セキュリティ、Quality Of Service（QoS）、帯域幅管理のための、ネットワーク間の境界インターフェイスを提供します。
• 『*Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model*』 • 『*Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model*』	Cisco Unified Border Element（SP Edition）は、VoIP 対応でネットワーク エッジに配置される Session Border Controller（SBC; セッション ボーダー コントローラ）です。Cisco IOS XE Release 2.3 およびそれよりも前のリリースでは、Cisco Unified Border Element（SP Edition）は、分散モードだけでサポートされています。分散モードで運用される SBC は、シグナリング インターワーキング、ネットワーク隠蔽、セキュリティ、および Quality of Service など、VoIP サービスを展開および管理するために使用できる機能のツールキットです。
• 『*Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model*』 • 『*Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*』	Cisco Unified Border Element（SP Edition）は、スケーラビリティが高くキャリアグレードの Session Border Controller（SBC; セッション ボーダー コントローラ）です。これは、サービス プロバイダー向けに設計されており、一般にエンタープライズまたは SP の境界に配置され、VoIP サービスを簡単に展開および管理できるようになっています。Cisco Unified Border Element（SP Edition）は、シスコのルーティング プラットフォームに統合されており、多数のルータ機能を使用して、非常に豊富な機能とインテリジェントな SBC アプリケーションを提供します。Cisco Unified Border Element（SP Edition）は、以前は Integrated Session Border Controller と呼ばれており、シグナリング インターワーキング、メディア インターワーキング、アドレスおよびポート変換、課金、セキュリティ、Quality Of Service、コール アドミッション制御、帯域幅管理のための、ネットワーク間の境界インターフェイスを提供します。 Cisco IOS XE Release 2.4 およびそれよりも前のリリースでは、Cisco Unified Border Element（SP Edition）は、統合モードと分散モードの 2 つのモードまたは展開モデルで動作します。統合モードの機能については、コンフィギュレーション ガイドを参照してください。

表 2 には、Cisco IOS XE ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスを補足するマニュアルとリソースがリストされています。

表 2　Cisco IOS XE ソフトウェアの補足マニュアルとリソース

マニュアル タイトルまたはリソース	説明
『*Cisco IOS Master Command List, All Releases*』	すべての Cisco IOS XE ソフトウェア リリースで文書化されている全コマンドのアルファベット順のリスト。
『*Cisco IOS Debug Command Reference*』	使用に関する簡単な説明、コマンド構文、使用上のガイドラインを含む、**debug** コマンドのアルファベット順のリスト。
Cisco IOS XE システム メッセージ	Cisco IOS XE システム メッセージのリストと説明。システム メッセージは、ご使用のシステムの問題を示しているか、単なる通知である場合があります。通信回線、内部ハードウェア、またはシステム ソフトウェアの問題の診断に役立つことがあります。
リリース ノートおよび監視	新機能と変更された機能およびシステム要件に関する情報、および特定のソフトウェア リリースに関するその他の役立つ情報。特定の Cisco IOS XE ソフトウェア リリースの障害に関する情報。
MIB	ネットワークのモニタリングに使用されるファイル。選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs
RFC	（適切な場合）Cisco IOS XE マニュアルで参照する、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって保守される標準のドキュメント。参照される RFC の全文は次の URL で入手できます。 http://www.rfc-editor.org/

追加のリソースとマニュアルのフィードバック

『*What's New in Cisco Product Documentation*』は毎月更新され、シスコの新規および改訂版のすべての技術マニュアルについて説明しています。『*What's New in Cisco Product Documentation*』には、次のリソースの入手/利用方法に関する情報も記載されています。

- 技術マニュアル
- シスコ製品のセキュリティの概要
- Product Alert および Field Notice
- テクニカル サポート

Cisco IOS XE ソフトウェアの技術マニュアルには、フィードバックのための専用フォームが含まれています。ユーザはこれを使用して、マニュアルの内容を評価し、改善のための提案を行うことができます。マニュアルの品質向上のため、ぜひフィードバックをお寄せください。

Cisco IOS XE ソフトウェアのコマンドライン インターフェイスの使用

このマニュアルでは、Cisco IOS XE ソフトウェアの Command-Line Interface（CLI; コマンドライン インターフェイス）および一部の CLI 機能の使用方法に関する基本的な情報について説明します。このマニュアルの構成は、次のとおりです。

- 「デバイスの初期設定」（P.i）
- 「CLI の使用」（P.ii）
- 「コンフィギュレーションに対する変更の保存」（P.xii）
- 「その他の情報」（P.xiii）

CLI の使用方法については、『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』の「Part 1: Using the Cisco IOS Command-Line Interface (CLI)」を参照してください。

ソフトウェアのマニュアル一式については、『About Cisco IOS XE Software Documentation』のマニュアルを参照してください。

デバイスの初期設定

デバイスの初期設定はプラットフォームによって異なります。初期設定の実行方法については、製品出荷時の同梱材に含まれるハードウェア設置マニュアルを参照するか、http://www.cisco.com/go/techdocs の Cisco.com の Product Support サイトを参照してください。

初期設定を実行し、ネットワークにデバイスを接続した後、コンソール ポートまたは Telnet や Secure Shell（SSH; セキュア シェル）などのリモート アクセス方式を使用して CLI にアクセスするか、または Security Device Manager など、デバイスで提供される設定方法を使用することにより、デバイスを設定できます。

コンソール ポートまたは Auxiliary（AUX; 補助）ポートのデフォルト設定の変更

コンソール ポートまたは AUX ポートに対して変更ができる設定は次の 2 点だけです。

- **config-register 0x** コマンドを使用したポート速度の変更。ポート速度を変更することは推奨されていません。既知のデフォルト速度は 9600 です。
- たとえば、パスワードの追加やタイムアウト値の変更による、ポートの動作の変更。

（注） Cisco ASR 1000 シリーズ ルータに搭載された Route Processor（RP; ルート プロセッサ）の AUX ポートは、実用的なカスタマーの目的に提供されるものではなく、カスタマー サポート担当者の助言に基づく場合にだけアクセスする必要があります。

CLI の使用

ここでは、次の内容について説明します。

- 「コマンド モードの概要」（P.ii）
- 「対話型ヘルプ機能の使用」（P.v）
- 「コマンド構文の概要」（P.vi）
- 「イネーブル パスワードおよびイネーブル シークレット パスワードの概要」（P.viii）
- 「コマンド履歴機能の使用」（P.viii）
- 「コマンドの省略」（P.ix）
- 「CLI コマンドのエイリアスの使用」（P.ix）
- 「コマンドの no 形式および default 形式の使用」（P.x）
- 「debug コマンドの使用」（P.x）
- 「出力修飾子を使用する出力のフィルタリング」（P.xi）
- 「CLI エラー メッセージの概要」（P.xi）

コマンド モードの概要

CLI コマンド モードの構造は階層型であり、各モードで一連の特定コマンドをサポートしています。ここでは、存在する多数のモードのうち最も一般的なモードについて説明します。

表 1 に、CLI プロンプトに関連する一般的なコマンド モード、アクセス方法、終了方法、および各モードの使用方法についての簡単な説明を示します。

表 1　CLI コマンド モード

コマンド モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	ログイン。	`Router>`	**logout** コマンドまたは **exit** コマンドを発行します。	• 端末設定の変更。 • 基本的なテストの実行。 • デバイスのステータスの表示。
特権 EXEC	ユーザ EXEC モードから、**enable** コマンドを発行します。	`Router#`	**disable** コマンドまたは **exit** コマンドを発行して、ユーザ EXEC モードに戻ります。	• **show** コマンドおよび **debug** コマンドの発行。 • デバイスへのイメージのコピー。 • デバイスのリロード。 • デバイスのコンフィギュレーション ファイルの管理。 • デバイスのファイル システムの管理。
グローバル コンフィギュレーション	特権 EXEC モードから、**configure terminal** コマンドを発行します。	`Router(config)#`	**exit** コマンドまたは **end** コマンドを発行して、特権 EXEC モードに戻ります。	デバイスの設定。

表 1　CLI コマンド モード（続き）

コマンド モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードから、**interface** コマンドを発行します。	`Router(config-if)#`	**exit** コマンドを発行してグローバル コンフィギュレーション モードに戻るか、または **end** コマンドを発行して特権 EXEC モードに戻ります。	個々のインターフェイスの設定。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードから、**line vty** コマンドまたは **line console** コマンドを発行します。	`Router(config-line)#`	**exit** コマンドを発行してグローバル コンフィギュレーション モードに戻るか、または **end** コマンドを発行して特権 EXEC モードに戻ります。	個々の端末回線の設定。
ROM モニタ	特権 EXEC モードから、**reload** コマンドを発行します。システムの起動時、最初の 60 秒以内に **Break** キーを押します。	`rommon # >` # 記号は行番号を示し、プロンプトごとに番号が増分されます。	**continue** コマンドを発行します。	• 有効なイメージをロードできない場合、デフォルトの動作モードとして実行されます。 • デバイスに有効なイメージがなく、デバイスを起動できない場合、フォールバック手順を利用してイメージをロードします。 • 電源投入またはリロードのイベント発生後、60 秒以内に Ctrl+Break シーケンスが発行された場合、パスワード回復を実行します。

表 1　CLI コマンド モード（続き）

コマンド モード	アクセス方法	プロンプト	終了方法	モードの用途
診断	次の状況では、ルータが起動されるか、または診断モードが開始されます。1 つ以上の Cisco IOS XE プロセスが失敗したときは、ほとんどの場合、ルータがリロードされます。 • **transport-map** コマンドを使用して、ユーザ設定のアクセス ポリシーが設定されると、ユーザは診断モードに誘導されます。 • RP 補助ポートを使用して、ルータへのアクセスが行われた場合。 • ブレーク信号（**Ctrl+C** キー、**Ctrl+Shift+6** キー、または **send break** コマンド）が入力され、このブレーク信号の受信時に診断モードを開始するようにルータが設定されていた場合。	`Router(diag)#`	Cisco IOS XE プロセスの失敗により、診断モードが開始された場合、診断モードを終了するには、その失敗を解決し、ルータを再起動する必要があります。 transport-map のコンフィギュレーションにより、ルータが診断モードになった場合、別のポートを使用してルータにアクセスするか、または設定済みの Cisco IOS XE CLI に接続する方法を使用します。 RP 補助ポートを使用してルータにアクセスした場合、アクセスには別のポートを使用します。補助ポートを使用するルータへのアクセスは、カスタマーの目的に合わせた用途には使用しません。	• Cisco IOS XE ステートを含む、ルータの各種ステートの検査。 • コンフィギュレーションの置き換えまたはロールバック。 • Cisco IOS XE ソフトウェアまたはその他のプロセスを再起動する方法の提供。 • ハードウェア（ルータ全体、RP、ESP、SIP、SPA など）またはその他のハードウェア コンポーネントの再起動。 • FTP、TFTP、および SCP などのリモート アクセス方式を使用した、ルータに対するファイル転送、またはルータからのファイル転送。

EXEC コマンドは、ソフトウェアの再起動時に保存されません。コンフィギュレーション モードで発行するコマンドをスタートアップ コンフィギュレーションに保存できます。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する場合は、これらのコマンドをソフトウェアのリブート時に実行します。グローバル コンフィギュレーション モードは、最もレベルの高いコンフィギュレーション モードです。グローバル コンフィギュレーション モードから、プロトコル固有のモードを含む、他のさまざまなコンフィギュレーション モードを開始できます。

ROM モニタ モードは、ソフトウェアが適切にロードできない場合に使用される独立したモードです。ソフトウェアの起動時、または起動時にコンフィギュレーション ファイルが破損している場合に、有効なソフトウェア イメージが見つからなければ、ソフトウェアは ROM モニタ モードを開始することがあります。デバイスが ROM モニタ モードである間に使用できるコマンドを表示するには、疑問符記号（?）を使用します。

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
```

```
.
.
.
rommon 2 >
```

次に、別のコマンド モードを示すようにコマンド プロンプトを変える例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

（注） **end** コマンドに代わるキーは、キーボードの Ctrl+Z キーです。

対話型ヘルプ機能の使用

CLI には対話型ヘルプ機能があります。表 2 に、ヘルプ機能の使用方法を示します。

表 2　CLI 対話型ヘルプ コマンド

コマンド	目的
help	任意のコマンド モードでヘルプ機能を簡単に説明します。
?	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
コマンド（一部） **?**	この文字列で始まるコマンドをリストします（コマンドと疑問符の間にスペースなし）。
コマンド（一部） <**Tab**>	一部のみ入力したコマンド名を補完します（コマンドと <Tab> の間にスペースなし）。
コマンド **?**	このコマンドに関連付けられたキーワード、引数、またはその両方をリストします（コマンドと疑問符の間にスペースあり）。
コマンド キーワード **?**	このキーワードに関連付けられた引数をリストします（キーワードと ? の間にスペースあり）。

次に、help コマンドの使用例を示します。

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

コマンド（一部）?

```
Router(config)# zo?
zone  zone-pair
```

コマンド（一部）<Tab>

```
Router(config)# we<Tab> webvpn
```

コマンド?

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

コマンド キーワード?

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

コマンド構文の概要

コマンド構文はコマンドの形式であり、CLI ではこの形式で入力する必要があります。コマンドは、コマンド、キーワード、および引数の名前で構成されます。キーワードは、文字通り使用される英数字の文字列です。引数は、ユーザが指定する必要のある値のプレースホルダーです。キーワードおよび引数は必須の場合も、任意の場合もあります。

特定の表記法を用いて、構文およびコマンドの要素に関する情報を表します。表 3 では、これらの表記法について説明します。

表 3　　CLI 構文の表記法

記号 / テキスト	機能	注意事項
<>（山形カッコ）	オプションが引数であることを示します。	山形カッコを用いずに引数を表示することもあります。
A.B.C.D.	ドット付き 10 進 IP アドレスを入力する必要があることを示します。	山形カッコ（<>）を使用していても、IP アドレスが引数であることを常に示しているとは限りません。
WORD（すべて大文字）	1 語を入力する必要があることを示します。	山形カッコ（<>）を使用していても、WORD が引数であることを常に示しているとは限りません。

表 3　CLI 構文の表記法（続き）

記号 / テキスト	機能	注意事項
LINE（すべて大文字）	2 語以上入力する必要があることを示します。	山形カッコ（<>）を使用していても、LINE が引数であることを常に示しているとは限りません。
<cr>（復帰）	使用可能なキーワードおよび引数のリストの最後を示します。また、キーワードおよび引数が任意であるときに表示されます。<cr> が唯一のオプションである場合、分岐の最後に到達しています。または、分岐のないコマンドであれば、コマンドの最後に到達しています。	—

次に、構文の表記の例を示します。

```
Router(config)# ethernet cfm domain ?
  WORD  domain name

Router(config)# ethernet cfm domain dname ?
  level

Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number

Router(config)# ethernet cfm domain dname level 7 ?
  <cr>

Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

イネーブル パスワードおよびイネーブル シークレット パスワードの概要

一部の特権 EXEC コマンドは、システムに影響を及ぼす処理に使用します。不正使用を防ぐため、これらのコマンドにはパスワードを設定することを推奨します。イネーブル（暗号化なし）とイネーブル シークレット（暗号化あり）の 2 種類のパスワードを設定できます。次のコマンドは、これらのパスワードを設定します。次のコマンドをグローバル コンフィギュレーション モードで発行します。

- **enable** *password*
- **enable secret** *password*

イネーブル シークレット パスワードは暗号化され、イネーブル パスワードよりも安全であるため、イネーブル シークレット パスワードの使用が推奨されます。イネーブル シークレット パスワードを使用する場合、テキストが config.text ファイルに書き込まれる前に暗号化（判読できないように）します。イネーブル パスワードを使用する場合、入力されたとおりに（判読できる状態で）テキストが config.text ファイルに書き込まれます。

どちらの種類のパスワードも大文字と小文字が区別され、1 ～ 25 文字の大文字と小文字の英数字を使用できます。パスワードを数字で始めることもできます。スペースもパスワードに有効な文字です。たとえば、「two words」は有効なパスワードです。先行するスペースは無視されますが、末尾のスペースは認識されます。

（注） どちらのパスワード コマンドにも、単体の整数値である数字のキーワードがあります。パスワードの最初の文字に数字を選択し、その後にスペースを続けた場合、システムはその数字を、数字のキーワードであり、パスワードには含まれないものとして読み取ります。

両方のパスワードを設定した場合、イネーブル シークレット パスワードがイネーブル パスワードよりも優先されます。

パスワードを削除するには、**no enable** *password* コマンドまたは **no enable secret** *password* コマンドの **no** 形式を使用します。

シスコ製品のパスワードの回復手順の詳細については、次を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

コマンド履歴機能の使用

コマンド履歴機能では、セッション中に入力するコマンドをコマンド履歴バッファに保存します。保存するコマンド数のデフォルトは 10 ですが、0 ～ 256 の範囲で数を設定できます。このコマンド履歴機能は、特に長いコマンドや複雑なコマンドを再呼び出しする場合に便利です。

ターミナル セッション用の履歴バッファに保存するコマンド数を変更するには、**terminal history size** コマンドを発行します。

```
Router# terminal history size num
```

コマンド履歴バッファは、同じデフォルト値および設定のオプションを用いて、ライン コンフィギュレーション モードでも使用できます。ライン コンフィギュレーション モードでターミナル セッションのコマンド履歴バッファ サイズを設定するには、**history** コマンドを発行します。

```
Router(config-line)# history [size num]
```

履歴バッファからコマンドを再呼び出しするには、次の方法を使用します。

- Ctrl+P キーまたは上矢印キーを押す：最近使用したコマンドからコマンドを再呼び出しします。このキーを連続して繰り返すと、順に古いコマンドを再呼び出しします。
- Ctrl+N キーまたは下矢印キーを押す：Ctrl+P キーまたは上矢印キーを使用してコマンドを再呼び出しした後の履歴バッファの中から、最近使用したコマンドを再呼び出しします。このキーを連続して繰り返すと、順に新しいコマンドを再呼び出しします。

  （注） 矢印キーは、VT100 などの ANSI 互換端末上でだけ機能します。

- ユーザ EXEC モードまたは特権 EXEC モードでの **show history** コマンドの発行：最近入力したコマンドをリストします。表示されるコマンド数は、**terminal history size** コマンドおよび **history** コマンドの設定によります。

  コマンド履歴機能はデフォルトでイネーブルに設定されています。ターミナル セッションでこの機能をディセーブルにするには、ユーザ EXEC モードまたは特権 EXEC モードで **terminal no history** コマンドを発行するか、ライン コンフィギュレーション モードで **no history** コマンドを発行します。

コマンドの省略

コマンドを実行するために、常に完全なコマンド名を入力する必要はありません。CLI は、省略形でも一意に識別できるだけの十分な文字が含まれていれば、省略されたコマンドを認識します。たとえば、**show version** コマンドは、**sh ver** として省略できます。**s** は **show**、**set**、または **systat** を意味する可能性があるため、**s ver** として省略することはできません。また、**show** コマンドにはキーワードとして **version** の他に **vrrp** があるため、**sh v** の省略形は有効ではありません

CLI コマンドのエイリアスの使用

時間を節約し、何度も同じコマンド入力の繰り返しを省くために、コマンドのエイリアスを使用できます。コマンドラインで実行可能であればどのコマンドでも、実行するようにエイリアスを設定できますが、エイリアスでは、モード間の移動、パスワードの入力、対話型機能の実行のいずれも行うことができません。

表 4 に、デフォルトのコマンド エイリアスを示します。

表 4　　デフォルトのコマンド エイリアス

コマンド エイリアス	元のコマンド
h	help
lo	logout
p	ping
s	show
u または **un**	undebug
w	where

コマンド エイリアスを作成するには、グローバル コンフィギュレーション モードで **alias** コマンドを発行します。コマンド構文は、**alias** *mode command-alias original-command* です。次に、いくつかの例を示します。

- Router(config)# **alias exec prt partition**：特権 EXEC モード
- Router(config)# **alias configure sb source-bridge**：グローバル コンフィギュレーション モード
- Router(config)# **alias interface rl rate-limit**：インターフェイス コンフィギュレーション モード

デフォルトおよびユーザによって作成されたエイリアスの両方を表示するには、**show alias** コマンドを発行します。

alias コマンドの詳細については、http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html を参照してください。

コマンドの no 形式および default 形式の使用

ほとんどのコンフィギュレーション コマンドは **no** 形式があり、この形式を使用して、コマンドをデフォルト値に戻したり、フィーチャや機能をディセーブルにしたりします。たとえば、**ip routing** コマンドはデフォルトでイネーブルに設定されています。このコマンドをディセーブルにするには、**no ip routing** コマンドを発行します。IP ルーティングを再びイネーブルにするには、**ip routing** コマンドを発行します。

コンフィギュレーション コマンドはまた、**default** 形式を持つ場合もあり、この形式を使用して、コマンドの設定をデフォルト値に戻します。デフォルトでディセーブルに設定されているコマンドの場合、**default** 形式を使用することで、コマンドの **no** 形式を使用する場合と同様の作用があります。デフォルトでイネーブルに設定されていて、デフォルト設定を持つコマンドの場合、**default** 形式はコマンドをイネーブルにし、設定をデフォルト値に戻します。お使いのシステム上で使用できる **default** コマンドについては、**default ?** を コマンドライン インターフェイスの適切なコマンド モードで入力します。

no 形式は、Cisco IOS コマンド リファレンスのコマンドのページに記載されています。**default** 形式は通常、**default** 形式がコマンドのプレーン形式および **no** 形式とは異なる機能を実行する場合にだけ、コマンド ページに記載されます。

コマンド ページには、多くの場合に「コマンドのデフォルト」に関する項が設けられています。コマンドのデフォルトに関する項には、コンフィギュレーション コマンドに対してコマンドが使用されないときの設定状態、または EXEC コマンドに対して任意のキーワードまたは引数が指定されていないときのコマンドの使用結果が記載されています。

debug コマンドの使用

debug コマンドは、ネットワーク上の問題に対するトラブルシューティングを助ける広範な出力を生成します。これらのコマンドは、Cisco IOS XE ソフトウェア内の多くのフィーチャおよび機能に使用できます。**debug** コマンドの一部として、**debug all**、**debug aaa accounting**、および **debug mpls packets** があります。デバイスとの Telnet セッション中に **debug** コマンドを使用する場合は、最初に **terminal monitor** コマンドを入力する必要があります。デバッグを完全にオフにするには、**undebug all** コマンドを入力する必要があります。

debug コマンドの詳細については、http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html の『*Cisco IOS Debug Command Reference*』を参照してください。

注意 デバッグは、デバイスを使用不可にする可能性のある、高プライオリティで CPU 使用率の高いプロセスです。**debug** コマンドを使用するのは、特定の問題に対するトラブルシューティングの場合だけです。デバッグの実行に最適なのは、ネットワーク トラフィックが少ない期間で、かつネットワークを使用してやりとりしているユーザが少ないときです。このような期間にデバッグすることで、**debug** コマンド処理のオーバーヘッドにより、ネットワーク パフォーマンス、ユーザ アクセス、または応答時間に影響を及ぼす可能性を低減します。

出力修飾子を使用する出力のフィルタリング

コマンドの多くは、複数の画面にわたり表示する大量の出力を生成します。出力修飾子を使用して、この出力をフィルタし、確認の必要な情報だけを表示できます。

次の 3 つの出力修飾子を使用できます。

- **begin** *regular-expression*：正規表現の一致を検出した最初の行とそれに続くすべての行を表示します。
- **include** *regular-expression*：正規表現の一致を検出したすべての行を表示します。
- **exclude** *regular-expression*：正規表現の一致を検出した行以外のすべての行を表示します。

これらの出力修飾子のうち 1 つを使用する場合は、コマンドの後に続けて、検索またはフィルタするパイプ記号（|）、修飾子、および正規表現を入力します。正規表現は大文字と小文字を区別する英数字のパターンです。1 文字、1 数字、語句、またはさらに複雑な文字列を使用できます。

次に、**show interface** コマンドの出力をフィルタして、「protocol」の表現を含む行だけを表示する例を示します。

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

CLI エラー メッセージの概要

CLI 使用時にいくつかのエラー メッセージが表示されることがあります。表 5 に、一般的な CLI エラー メッセージを示します。

表 5　一般的な CLI エラー メッセージ

エラー メッセージ	意味	ヘルプの利用方法
% Ambiguous command: "show con"	コマンドを認識するのに十分な文字列を入力していません。	コマンドの後に続けてスペースと疑問符（?）を再入力します。コマンドに対して入力可能なキーワードが表示されます。
% Incomplete command.	コマンドに必要なキーワードまたは値をすべて入力していません。	コマンドの後に続けてスペースと疑問符（?）を再入力します。コマンドに対して入力可能なキーワードが表示されます。
% Invalid input detected at "^" marker.	コマンドを誤って入力しています。キャレット（^）は、エラーの場所を示します。	疑問符（?）を入力して、このコマンドモードで使用可能なすべてのコマンドを表示します。コマンドに対して入力可能なキーワードが表示されます。

システム エラー メッセージの詳細については、『*System Messages for Cisco IOS XE*』を参照してください。

コンフィギュレーションに対する変更の保存

デバイスのコンフィギュレーションに対して行った変更を保存するには、**copy running-config startup-config** コマンドまたは **copy system:running-config nvram:startup-config** コマンドを発行する必要があります。これらのコマンドを発行すると、コンフィギュレーションに対して行った変更がスタートアップ コンフィギュレーションに保存されます。保存されるのは、ソフトウェアのリロード時、デバイスの電源がオフになったとき、または電源が遮断された場合です。次に、**copy running-config startup-config** コマンド構文を表示する例を示します。

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

Enter キーを押して startup-config のファイル名（デフォルト）を使用するか、新しいファイル名を入力して Enter キーを押し、その名前を使用します。次の出力が表示され、コンフィギュレーションが保存されたことを示します。

```
Building configuration...
[OK]
Router#
```

ほとんどのプラットフォームで、コンフィギュレーションは NVRAM に保存されます。クラス A フラッシュ ファイル システムを備えるプラットフォームの場合、コンフィギュレーションは CONFIG_FILE 環境変数によって指定された場所に保存されます。CONFIG_FILE 変数のデフォルトは NVRAM になります。

その他の情報

- 『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』の「Part 1: Using the Cisco IOS Command-Line Interface (CLI)」

  http://www.cisco.com/en/US/docs/ios/ios_xe/fundamentals/configuration/guide/2_xe/cf_xe_book.html

  または

  『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の「Using Cisco IOS XE Software」の章

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html

- シスコ製品サポート リソース

  http://www.cisco.com/go/techdocs

- Cisco.com のサポートサイト（タスクまたは製品によるマニュアル検索もできます）

  http://www.cisco.com/en/US/support/index.html

- Software Download Center（ダウンロード/ツール/ライセンス、登録、アドバイザリ、一般情報）（Cisco.com のユーザ ID およびパスワードが必要）

  http://www.cisco.com/kobayashi/sw-center/

- エラー メッセージ デコーダ。Cisco IOS XE ソフトウェアのエラー メッセージを調査し解決を支援するツールです。

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool。Cisco IOS XE コマンドの詳しい説明の検索を支援するツールです（[Select an index] で [IOS] を選択し、[Select a release] で [All IOS Commands] を選択）（Cisco.com のユーザ ID とパスワードが必要）。

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter。サポート対象の **show** コマンドのコマンド出力を分析するトラブルシューティング ツールです。

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl¥

ブロードバンド アクセス集約の概要

ブロードバンド アクセス集約の準備

ブロードバンド アクセス集約の達成に必要な作業を実行する前に、自分の判断で実行できる準備作業がいくつかあります。これらの準備作業を実行すると、集約作業をより効率的に行うことができます。

仮想テンプレート インターフェイスを使用すると、時間を節約できます。PPP パラメータはすべて、仮想テンプレート設定内で管理されるからです。仮想テンプレートで行った設定はすべて、各仮想アクセス インターフェイスに自動的に伝播されます。

ブロードバンド スケーラビリティの拡張機能では、仮想アクセス サブインターフェイスを作成して、終了した各 PPP セッションで使用されるメモリの量を減らすことができます。仮想アクセス サブインターフェイスがシステムで使用可能かどうかを確認し、これらの拡張機能を事前に設定しておくと、集約プロセスを高速化し、システムのパフォーマンスを向上させることができます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「ブロードバンド アクセス集約の準備の機能情報」（P.11）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「ブロードバンド アクセス集約の準備の制約事項」（P.2）
- 「ブロードバンド アクセス集約の準備に関する情報」（P.2）
- 「ブロードバンド アクセス集約を準備する方法」（P.4）
- 「ブロードバンド アクセス集約の準備の設定例」（P.6）
- 「その他の関連資料」（P.8）
- 「ブロードバンド アクセス集約の準備の機能情報」（P.11）

ブロードバンド アクセス集約の準備の制約事項

次の制約事項が適用されます。

- 高度なスケーリング要件により、仮想アクセス *サブインターフェイス*のみがサポートされます。仮想アクセス サブインターフェイスのディセーブル化はサポートされません。
- 仮想アクセス インターフェイスのクローンの事前作成はサポートされません。

ブロードバンド アクセス集約の準備に関する情報

ブロードバンド アクセス集約を準備するには、次の概念を理解しておく必要があります。

- 「仮想アクセス インターフェイス」（P.2）
- 「ブロードバンド スケーラビリティの設定拡張機能」（P.3）

仮想アクセス インターフェイス

仮想テンプレート インターフェイスは、ダイナミックに作成される仮想アクセス インターフェイスに設定を提供するために使用されます。仮想テンプレート インターフェイスはユーザによって作成され、NVRAM に保存されます。

仮想テンプレート インターフェイスを作成したら、シリアル インターフェイスと同様の方法で設定できます。

仮想テンプレート インターフェイスは、仮想プロファイル、Virtual Private Dial-up 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）、プロトコル変換など、さまざまなアプリケーションで作成および適用できます。

PPP パラメータはすべて、仮想テンプレート設定内で管理されます。仮想テンプレートに対する設定変更は、各仮想アクセス インターフェイスに自動的に伝播されます。1 つの仮想テンプレートから複数の仮想アクセス インターフェイスを作成することができます。

Cisco IOS XE ソフトウェアでは、最大で 4096 の仮想テンプレート設定がサポートされます。それよりも多くのカスタム設定が必要な場合は、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバを使用できます。

インターフェイスを設定する前に仮想テンプレートのパラメータを明示的に定義しなかった場合、PPP インターフェイスは仮想テンプレートのデフォルト値を使用して起動します。一部のパラメータ（IP アドレスなど）は、PPP インターフェイスが起動する前に指定された場合にのみ有効になります。したがって、このようなパラメータを有効にするために、インターフェイスを設定する前に仮想テンプ

レートを明示的に作成して設定することを推奨します。インターフェイスを設定した後にパラメータを指定する場合は、サブインターフェイスで **shutdown** コマンドの後に **no shutdown** コマンドを実行してインターフェイスを再起動します。この再起動により、新しく設定されたパラメータ（IP アドレスなど）が有効になります。

ブロードバンド スケーラビリティの設定拡張機能

ブロードバンド スケーラビリティ機能の設定拡張機能では、仮想アクセス サブインターフェイスを作成して、終了した各 PPP セッションで使用されるメモリの量を減らすことができます。仮想アクセス サブインターフェイスを使用できるかどうかは、作成元の仮想テンプレートの設定によって異なります。この機能では、仮想テンプレートに仮想アクセス サブインターフェイスとの互換性があるかどうかを確認するコマンドも導入されます。

仮想アクセス サブインターフェイス

virtual-template コマンドでは、既存の機能と設定がサポートされます。**virtual-template subinterface** コマンドは、デフォルトでイネーブルになっています。このコマンドをディセーブルにできません。

仮想テンプレート マネージャは、仮想テンプレートで設定されているすべてのオプションがサブインターフェイスでサポートされるかどうかを確認します。仮想アクセス サブインターフェイスは、サブインターフェイスをサポートするすべての仮想テンプレートに対して作成されます。ユーザがサブインターフェイスでサポートされないコマンドを入力した場合、完全な仮想アクセス インターフェイスが作成され、その仮想テンプレートを使用するすべての PPP セッションにクローンが作成されます。

個々のアプリケーションがサブインターフェイスに対応しているかどうかに関係なく、さまざまなアプリケーションで同じ仮想テンプレートを使用できます。仮想テンプレート マネージャは、アプリケーションが仮想アクセス サブインターフェイスをサポートするかどうかを通知され、適切なリソースを作成します。

仮想テンプレートのサブインターフェイスとの互換性

The **test virtual-template subinterface** 特権 EXEC コマンドは、仮想テンプレートが仮想アクセス サブインターフェイスの作成をサポートできるかどうかを確認します。仮想テンプレートにサブインターフェイスの作成を妨げるコマンドが含まれている場合、**test virtual-template subinterface** コマンドはそれらのコマンドを特定して表示します。

debug vtemplate subinterface コマンドは、ユーザがサブインターフェイスで有効でないコンフィギュレーション コマンドを仮想テンプレートで入力した場合に生成されるデバッグ メッセージを表示します。これらのメッセージは、**debug vtemplate subinterface** コマンドと **virtual-template subinterface** コマンドがイネーブルになっていて、サブインターフェイスの作成をサポートできる仮想テンプレートが設定されている場合にのみ生成されます。仮想アクセス サブインターフェイスの作成が **no virtual-template** サブインターフェイス コマンドによってディセーブルにされている場合、**debug vtemplate subinterface** コマンドは出力を生成しません。

ブロードバンド スケーラビリティ機能の利点

ブロードバンド スケーラビリティでは、仮想アクセス サブインターフェイスを作成して、終了した各 PPP セッションで使用されるメモリの量を減らすことができます。これらの仮想アクセス サブインターフェイスは、ユーザにとって透過的な機能向上と共に、クローンの作成プロセスを高速化します。

ブロードバンド アクセス集約を準備する方法

ここでは、次の手順について説明します。

- 「仮想テンプレート インターフェイスの設定」（P.4）
- 「ブロードバンド スケーラビリティの拡張機能の設定」（P.5）

仮想テンプレート インターフェイスの設定

ギガビット イーサネット インターフェイスに PPPoE を設定する前に、仮想テンプレートを設定します。仮想テンプレート インターフェイスは、必要に応じて着信 PPP セッション要求にダイナミックに適用される論理エンティティです。仮想テンプレート インターフェイスを作成して設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered loopback** *number*
5. **mtu** *bytes*
6. **ppp authentication chap**
7. **ppp ipcp ip address required**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**Interface virtual-template** *number* 例： `Router(config)# interface virtual-template 1`	仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip unnumbered loopback** *number* 例： `Router(config-if)# ip unnumbered loopback 0`	LAN 上の特定の IP アドレスを割り当てずに IP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**mtu** *bytes* **例：** `Router(config-if)# mtu 1492`	（任意）インターフェイスの最大 MTU サイズを設定します。 **（注）** 設定できる MTU サイズは 1492 または 1500 のいずれかだけです。1492 より大きい MTU サイズを設定するには、**tag ppp-max-payload** コマンドを使用する必要があります。
ステップ 6	**ppp authentication chap** **例：** `Router(config-if)# ppp authentication chap`	仮想テンプレート インターフェイスで PPP 認証をイネーブルにします。
ステップ 7	**ppp ipcp ip address required** **例：** `Router(config-if)# ppp ipcp ip address required`	有効なアドレスのネゴシエーションなしに PPP セッションが設定されるのを防止します。 このコマンドは、レガシー ダイヤルアップ ネットワークやレガシー DSL ネットワークで必要になります。

例

次に、仮想テンプレート インターフェイスの設定例を示します。

```
interface virtual-template 1
 ip unnumbered Loopback 0
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
```

ブロードバンド スケーラビリティの拡張機能の設定

ブロードバンド スケーラビリティの拡張機能を設定するには、次の作業を実行します。

- 「仮想テンプレートの仮想アクセス サブインターフェイスとの互換性の確認」（P.5）

仮想テンプレートの仮想アクセス サブインターフェイスとの互換性の確認

仮想テンプレートをテストし、仮想テンプレートが仮想アクセス サブインターフェイスの作成に対応しているかどうかを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **test virtual-template template subinterface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**test virtual-template** *template* **subinterface** **例：** `Router# test virtual-template virtual-template1 subinterface`	指定された仮想テンプレートをテストし、その仮想テンプレートが仮想アクセス サブインターフェイスの作成に対応しているかどうかを確認します。

例

test virtual-template subinterface コマンドによって生成された出力は、仮想テンプレートがサブインターフェイスの作成に対応しているかどうかを示します。

次の例の出力は、仮想テンプレートに互換性がないことを示しています。この出力には、仮想テンプレートで設定されていて、非互換性の原因になっているコマンドのリストも含まれています。

```
Router# test virtual-template virtual-template1 subinterface

Subinterfaces cannot be created using
Virtual-Template1

Interface commands:
traffic-shape rate 50000 8000 8000 1000
```

ブロードバンド アクセス集約の準備の設定例

ここでは、次の設定例について説明します。

- 「仮想アクセス サブインターフェイスの設定：例」（P.6）

仮想アクセス サブインターフェイスの設定：例

ここでは、次の設定例について説明します。

- 「仮想アクセス サブインターフェイスの設定：例」（P.6）
- 「仮想テンプレートのサブインターフェイスとの互換性のテスト：例」（P.8）

仮想アクセス サブインターフェイスの設定：例

次に、仮想アクセス サブインターフェイスと互換性がある仮想テンプレートの例を示します。

（注） **virtual-access subinterface** コマンドは、デフォルトでイネーブルになっており、実行コンフィギュレーションには表示されません。実行コンフィギュレーションに表示されるのは、**no virtual-access subinterface** コマンドだけです。

```
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pool-1
 ppp authentication chap
 ppp multilink
```

次に、仮想アクセス サブインターフェイスの作成が **no virtual-access subinterface** コマンドによってディセーブルにされている設定例を示します。このコマンドが設定されている場合、仮想アクセス インターフェイスはルータの SNMP コードに登録されません。PPP セッションの管理に SNMP を使用しないネットワーク環境では、これによってメモリと CPU 処理を節約できます。仮想アクセス インターフェイスを SNMP コードに登録するのに必要なメモリと CPU 処理を使用せずに済むからです。

```
Current configuration :6003 bytes
!

! Last configuration change at 10:59:02 EDT Thu Sep 19 2004
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname ioswan5-lns
!
enable password lab
!
username cisco password 0 cisco
clock timezone EST -5
clock summer-time EDT recurring
aaa new-model
!
!
aaa authentication ppp default local

aaa authorization network default local
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
!
!
no ip domain lookup
ip name-server 10.44.11.21
ip name-server 10.44.11.206
!
ip vrf vpn1
rd 10:1
route-target export 10:1
route-target import 10:1
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname ioswan5-lac
local name tunnel1
l2tp tunnel password 7 01100F175804
```

```
!
!
!
no virtual-template subinterface
no virtual-template snmp
virtual-template 1 pre-clone 10
!
!
!
buffers small permanent 20000
buffers middle permanent 7500
!
!
!
interface Loopback1
ip address 10.111.1.1 255.255.255.0
```

仮想テンプレートのサブインターフェイスとの互換性のテスト：例

次に、仮想テンプレートをテストし、仮想テンプレートが仮想アクセス サブインターフェイスをサポートできるかどうかを確認する例を示します。次のコマンドは、仮想テンプレート 1 の設定を表示します。

```
Router# show running interface virtual-template 1

Building configuration...
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool pool-1
ppp authentication chap
traffic-shape rate 50000 8000 8000 1000
end
```

test virtual-template subinterface コマンドは、仮想テンプレート 1 をテストし、この仮想テンプレートがサブインターフェイスをサポートできるかどうかを確認します。出力は、仮想テンプレート 1 で設定されている **traffic-shape rate** コマンドが原因で、仮想テンプレートがサブインターフェイスをサポートできなくなっていることを示しています。

```
Router# test virtual-template 1 subinterface

Subinterfaces cannot be created using Virtual-Template1
Interface commands:
traffic-shape rate 50000 8000 8000 1000
```

その他の関連資料

ここでは、ブロードバンド アクセス集約の準備に関する参考資料を紹介します。

関連マニュアル

内容	参照先
PPPoE セッションのブロードバンド アクセス集約	*『Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions』*

内容	参照先
ppp-max payload タグ値の範囲の指定	『*PPP-Max-Payload and IWF PPPoE Tag Support*』
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

ブロードバンド アクセス集約の準備の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　ブロードバンド集約の準備の機能情報

機能名	ソフトウェア リリース	機能の設定情報
仮想サブインターフェイス（ブロードバンド スケーラビリティの設定拡張機能）	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能では、仮想アクセス サブインターフェイスを作成して、終了した各 PPP セッションで使用されるメモリの量を減らすことができます。仮想アクセス サブインターフェイスを使用できるかどうかは、作成元の仮想テンプレートの設定によって異なります。この機能では、仮想テンプレートに仮想アクセス サブインターフェイスとの互換性があるかどうかを確認するコマンドも導入されます。 この機能に関する詳細については、次の各項を参照してください。 • 「ブロードバンド スケーラビリティの拡張機能の設定」（P.5） • 「仮想アクセス サブインターフェイスの設定：例」（P.6）

PPPoE

PPPoE Circuit-ID タグ処理

PPPoE Circuit-Id タグ処理機能では、Digital Subscriber Line（DSL; デジタル加入者線）からの Circuit-Id タグをファスト イーサネットまたはギガビット イーサネット インターフェイス上の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）アクセス要求の ID として抽出できます。その結果、ATM ベースのブロードバンド アクセスをシミュレートしますが、費用対効果に優れたファスト イーサネットまたはギガビット イーサネットを使用します。このタグは、ネットワークのトラブルシューティングおよび RADIUS 認証とアカウンティングのプロセスにも使用されます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PoE Circuit-Id タグ処理の機能情報」（P.10）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE Circuit-Id タグ処理機能の前提条件」（P.2）
- 「PPPoE Circuit-Id タグ処理機能に関する情報」（P.2）
- 「PPPoE Circuit-Id タグ処理機能の設定方法」（P.4）
- 「PPPoE Circuit-Id タグ処理機能の設定例」（P.8）
- 「その他の関連資料」（P.9）

PPPoE Circuit-Id タグ処理機能の前提条件

この機能を設定する前に、RFC 2516 を理解しておくことを推奨します。この規格へのポインタについては、「RFC」（P.9）を参照してください。

PPPoE Circuit-Id タグ処理機能に関する情報

PPPoE Circuit-Id タグ処理機能を設定するには、次の概念を理解しておく必要があります。

- 「ATM とファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの違い」（P.2）
- 「DSL Forum 2004-71 ソリューション」（P.2）
- 「イーサネットベースのブロードバンド アクセス ネットワークにおける Circuit-Id タグの利用」（P.3）
- 「PPPoE Circuit-Id タグ処理機能の利点」（P.4）

ATM とファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの違い

ブロードバンド Digital Subscriber Line Multiplexer（DSLAM; デジタル加入者線マルチプレクサ）と Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）のベンダーは、ファスト イーサネットまたはギガビット イーサネットベースのアクセス ネットワークに ATM-DSL ローカル ループをブリッジして BRAS へのファスト イーサネットまたはギガビット イーサネットベースの接続を許可する DSLAM を使用し、ATM アクセス ネットワークの代わりにファスト イーサネットまたはギガビット イーサネットベースのネットワークを提供するニーズがあることを把握しています。ただし、ファスト イーサネットまたはギガビット イーサネット アクセス ネットワークでは、ATM ベースのネットワークに見られるような、加入者の Line-Id とインターフェイスとの間に固有のマッピングはありません。ATM ベースのネットワークでは、ATM VC が加入者線に関連付けられます。

PPP アクセスと AAA アカウンティング要求を開始する認証フェーズ中、「NAS-Port-Id に基づく TAL」機能が設定されている場合、BRAS は RADIUS 認証パケット内に NAS-Port-Id アトリビュートを含めます。このアトリビュートで、加入者の DSL 回線を識別します。例については、「NAS-Port-Id アトリビュートを含めるための BRAS の設定：例」（P.8）を参照してください。

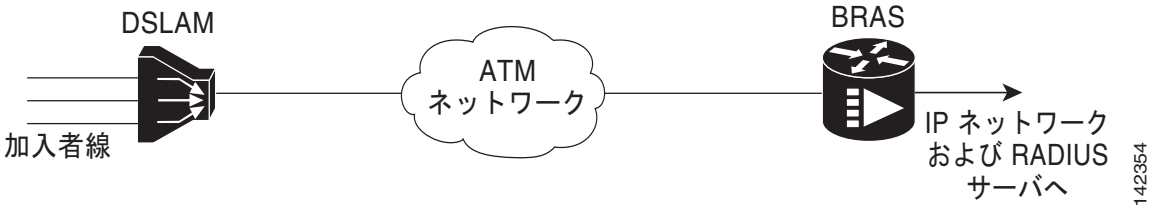
DSL Forum 2004-71 ソリューション

ATM インターフェイスで実行できる機能と同じ加入者マッピング機能をファスト イーサネットまたはギガビット イーサネット インターフェイスに適用するために、DSL Forum 2004-71 は、DSLAM が PPP over Ethernet（PPPoE）ディスカバリ フェーズで DSL Line-Id を送信するソリューションを提案します。この方法を使用すると、BRAS として機能する PPPoE サーバは Line-Id タグを抽出し、その Line-Id タグの Circuit-Id フィールドを AAA アクセスおよびアカウンティング要求の NAS-Port-Id アトリビュートとして使用できます。PPPoE Circuit-Id タグ処理機能では、提案された DSL Forum 2004-71 の方法を利用し、BRAS が PPPoE ディスカバリ フェーズ中に DSLAM で挿入された加入者 Circuit-Id タグの有無を検出できるようにします。BRAS は、このタグを PPP 認証および AAA アカウンティング要求の NAS-Port-Id アトリビュートとして送信します。このタグは、イーサネット ネットワークのトラブルシューティングおよび RADIUS 認証とアカウンティングのプロセスにも使用されます。

イーサネットベースのブロードバンド アクセス ネットワークにおける Circuit-Id タグの利用

従来の ATM ベースの DSL ブロードバンド アクセス ネットワークのトポロジを図 1 に示します。

図 1　ATM ベースの DSL ブロードバンド アクセス ネットワーク

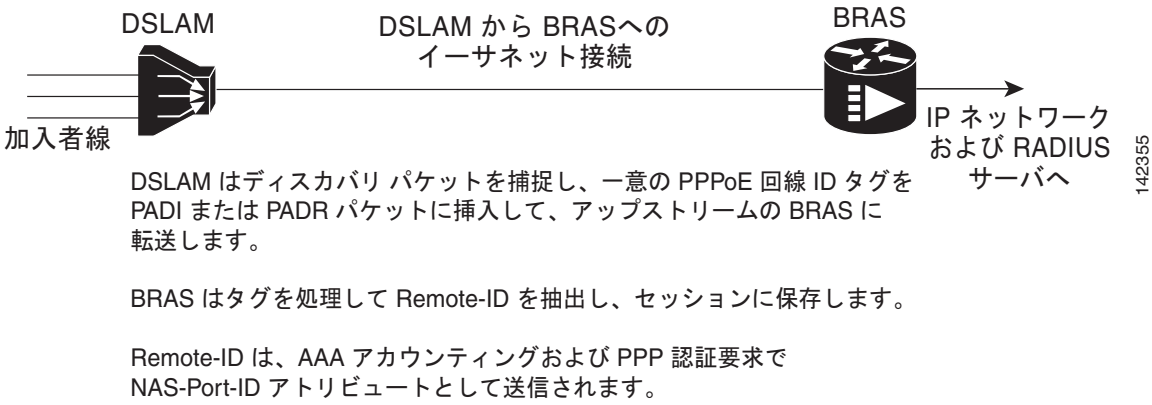


論理接続の観点では、エンド ユーザへの DSL 加入者線と、DSLAM を通じて BRAS へ PPP セッションを伝送するのに使用される ATM VC の 1 対 1 のマッピングがあります。この VC 情報は、RADIUS パケットで使用できるように NAS-Port-Id に変換されます。

エンド ユーザへの DSL ローカル ループの物理回線と VC（DSLAM から BRAS へ）の間の ATM ベースのネットワークで利用できる単純なマッピングは、ファスト イーサネットまたはギガビット イーサネットベースのネットワークでは使用できません。この問題を解決するために、PPPoE Circuit-Id タグ処理機能は、DSLAM で PPPoE 中継エージェント機能を使用して、PPPoE ディスカバリ パケットにタグを付けます。BRAS はこのタグ付きパケットを受信し、タグをデコードして、回線 ID を RADUIS サーバ宛ての RADIUS パケットに挿入します。

DSLAM は、クライアントからの PPPoE ディスカバリ フレームを捕捉し、PPoE Vendor-Specific タグ（0x0105）を使用して一意の回線 ID（circuit-id）を PPPoE Active Discovery Initiation（PADI）パケットおよび PPPoE Active Discovery Request（PADR）パケットに挿入します（図 2 を参照）。DSLAM は、挿入後にこれらのパケットを BRAS に転送します。中継エージェントが存在するアクセス ノードで、PADI または PADR パケットを受信した DSL 回線の circuit-id がタグに含まれます。

図 2　PPPoE Circuit-Id タグ処理ソリューション



Broadband Access（BBA; ブロードバンド アクセス）グループ コンフィギュレーション モードで **vendor-tag circuit-id service** コマンドを設定すると、BRAS は PADR パケットで受信した PPPoE Vendor-Specific タグを処理し、Circuit-Id フィールドを抽出します。このフィールドは、RADIUS アクセスおよびアカウンティング要求で NAS-Port-Id アトリビュート（RADIUS アトリビュート 87）としてリモート AAA サーバに送信されます。BRAS で **radius-server attribute nas-port format d** グ

ローバル コンフィギュレーション コマンドも設定すると、Acct-Session-Id アトリビュートに、ディスカバリ フレームを受信する着信アクセス インターフェイスに関する情報と確立されているセッションに関する情報が含まれます。

BRAS からの発信 PAD Offer（PADO）パケットおよび PAD Session-confirmation（PADS）パケットには、DSLAM で挿入された Circuit-Id タグが含まれます。DSLAM は、PADO および PADS パケットからタグを取り除く必要があります。DSLAM でタグを取り除くことができない場合、BRAS はパケットを送信する前にタグを削除する必要があります。タグを削除するには、**vendor-tag circuit-id strip** BBA グループ コンフィギュレーション モード コマンドを使用します。

PPPoE Circuit-Id タグ処理機能の利点

ファスト イーサネットまたはギガネット イーサネットベースの DSLAM に移行すると、次の利点があります。

- ATM ベースのネットワークではなく、ファスト イーサネットまたはギガビット イーサネットベースのバックホール ネットワークで、簡単で低コストの DSL 加入者向けプロビジョニング オプションを利用できます。
- ATM で使用できない高帯域幅接続オプションをファスト イーサネットまたはギガビット イーサネットから利用できます。
- Quality Of Service（QoS）を備えた次世代の DSLAM にアップグレードし、ADSL2 などのような、より高い帯域幅で非対称二重遅延モデムに対応できます。
- イーサネット ネットワークにビデオなどの高帯域幅コンテンツを挿入できます。

PPPoE Circuit-Id タグ処理機能の設定方法

ここでは、次の手順について説明します。

- 「PPPoE Circuit-Id タグ処理機能の設定」（P.4）（必須）
- 「PPPoE Circuit-Id タグの削除」（P.5）（必須）
- 「セッション アクティビティ ログの表示」（P.6）（任意）

PPPoE Circuit-Id タグ処理機能の設定

ここでは、Cisco BRAS でファスト イーサネットまたはギガビット イーサネットベースのアクセス ネットワークを設定する方法について説明します。抽出された Circuit-Id タグ（「PPPoE Circuit-Id タグ処理機能に関する情報」（P.2）を参照）は、DSL Forum で推奨される次の RADIUS 構文で送信されます。

「Access-Node-Identifier eth *slot*/*port*[**:***vlan-tag*]」

Access-Node-Identifier は、スペースなしで入力された一意の加入者 ID または電話番号のテキスト文字列です。DSL Forum 2004-71 に従うと、タグでサポートされる最大長は 48 バイトです。BRAS は、タグ全体を NAS-Port-Id にコピーし、AAA サーバに送信します。

手順の概要

1. **enable**
2. **configure terminal**

3. **radius-server attribute nas-port format d**
4. **bba-group pppoe** *group-name*
5. **vendor-tag circuit-id service**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute nas-port format d** **例：** `Router(config)# radius-server attribute nas-port format d`	（任意）RADIUS アクセスおよびアカウンティングに使用される PPPoE 拡張 NAS-Port 形式を選択します。 • ディスカバリ フレームが受信される着信アクセス インターフェイスに関する情報および確立されているセッションに関する情報が、**debug radius** コマンドで表示される Acct-Session-Id アトリビュートに含まれるようこのコマンドを設定します。詳細については、「セッション アクティビティ ログの表示」および「PPPoE Circuit-Id タグ処理の設定：例」を参照してください。
ステップ 4	**bba-group pppoe** *group-name* **例：** `Router(config-bba-group)# bba-group pppoe pppoe-group`	PPPoE プロファイルを定義します。
ステップ 5	**vendor-tag circuit-id service** **例：** `Router(config-bba-group)# vendor-tag circuit-id service`	PADR パケットで受信した PPPoE Vendor-Specific タグの処理をイネーブルにします。この処理によって、タグの Circuit-Id 部分が抽出され、この部分は RADIUS アクセスおよびアカウンティング要求で NAS-Port-Id アトリビュートとして AAA サーバに送信されます。

PPPoE Circuit-Id タグの削除

発信 PADO および PADS パケットには DSLAM で挿入された Vendor-Specific Line-Id タグが含まれます。また、DSLAM はパケットから Circuit-Id タグを取り除く必要があります。DSLAM でタグを取り除くことができない場合、BRAS はパケットを送信する前にタグを削除する必要があります。この作業は、BBA グループ コンフィギュレーション モードで **vendor-tag circuit-id strip** コマンドを設定して実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** *group-name* 例： `Router(config)# bba-group pppoe pppoe-group`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。
ステップ 4	**vendor-tag strip** 例： `Router(config-bba-group)# vendor-tag strip`	BRAS で発信 PADO および PADS パケットから着信 Vendor-Specific Circuit-Id タグを取り除くことができるようにします。

セッション アクティビティ ログの表示

radius-server attribute nas-port format d グローバル コンフィギュレーション コマンドが BRAS の PPPoE Circuit-Id タグ処理機能に追加されると（例については、「PPPoE Circuit-Id タグ処理の設定：例」（P.8）を参照してください）、**debug radius** 特権 EXEC コマンドからのレポートに、ディスカバリ フレームを受信する着信アクセス インターフェイスに関する情報と、確立されているセッションに関する情報が PPPoE 拡張 NAS-Port 形式（format d）で含まれます。

セッション アクティビティのレポートを表示するには、**debug radius** コマンドをイネーブルにします。ここに示す例では、次を前提とします。

- acct_session_id は、16 進形式の 79 または 4F です。
- メッセージ「Acct-session-id pre-pended with Nas Port = 0/0/0/200」で、PPPoE ディスカバリ フレームが到着したインターフェイスは FastEthernet0/0.200 です。0/0/0 は、slot/subslot/port のシスコ形式です。
- Acct-Session-Id の vendor-specific アトリビュート 44 には、入力インターフェイスとセッション ID の組み合わせを表す文字列「0/0/0/200_0000004F」が含まれます。

（注） **debug radius** 出力ログに関連する文字列は、例示を目的として太字で表示されます。

```
Router# debug radius

02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server
172.20.164.143
02:10:49: RADIUS(0000003F): Send Access-Request to 172.20.164.143:1645 id 1645/65, len 98
02:10:49: RADIUS:  authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                      [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                 [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                   [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32
02:10:49: RADIUS:  authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                   [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                      [1]
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION    Event PPP_LOCAL
02:10:49: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server
172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1 646/42,
len 117
02:10:49: RADIUS:  authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
02:10:49: RADIUS:  Acct-Session-Id     [44]  20  "0/0/0/200_0000004F"
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                      [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic      [45]  6 RADIUS                   [1]
02:10:49: RADIUS:  Acct-Status-Type    [40]  6 Start                    [1]
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                 [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                   [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time     [41]  6   0
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len
20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**debug radius** **例：** `Router# debug radius`	セッション アクティビティのレポートを表示します。

PPPoE Circuit-Id タグ処理機能の設定例

ここでは、次の例について説明します。

- 「PPPoE Circuit-Id タグ処理の設定：例」（P.8）
- 「NAS-Port-Id アトリビュートを含めるための BRAS の設定：例」（P.8）
- 「PPPoE Circuit-Id タグの削除：例」（P.9）

PPPoE Circuit-Id タグ処理の設定：例

次の例では、発信 PADO および PADS パケットで、着信 Vendor-Specific Circuit-Id タグを保持します。

```
radius-server attribute nas-port format d
!
bba-group pppoe pppoe-group
 sessions per-mac limit 50
 vendor-tag circuit-id service
!
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

NAS-Port-Id アトリビュートを含めるための BRAS の設定：例

次の例では、NAS-Port-Id に基づく TAL 機能が設定されます。この設定によって、認証フェーズ中に NAS-Port-Id アトリビュートが RADIUS 認証パケットに含まれ、PPP アクセスおよび AAA アカウンティング要求が開始されます。

```
radius-server attribute nas-port
policy-map type control test
 class type control always event session-start
 1 authorize identifier nas-port
```

PPPoE Circuit-Id タグの削除：例

次の例では、BRAS は発信 PADO および PADS パケットから着信 Vendor-Specific Circuit-Id タグを取り除きます。

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service
 vendor-tag strip

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

その他の関連資料

ここでは、PPPoE Circuit-Id タグ処理機能の関連資料に関する参考資料を紹介します。

関連マニュアル

内容	参照先
ブロードバンドと DSL の設定	『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』
RADIUS アトリビュート	『*Cisco IOS XE Security Configuration Guide*』
DSL Forum Line-Id タグ ソリューション	*Broadband Forum*

標準

標準	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	『*A Method for Transmitting PPP over Ethernet (PPPoE)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PoE Circuit-Id タグ処理の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　PPPoE Circuit-Id タグ処理の機能情報

機能名	リリース	機能情報
PPPoE Circuit-Id タグ処理	Cisco IOS XE Release 2.1	PPPoE Circuit-Id タグ処理機能では、DSL からの Circuit-Id タグをイーサネット インターフェイスの AAA アクセス要求の ID として抽出できます。その結果、ATM ベースのブロードバンド アクセスをシミュレートしますが、費用対効果に優れたイーサネットを使用します。このタグは、ネットワークのトラブルシューティングおよび RADIUS 認証とアカウンティングのプロセスにも使用されます。 この機能は、Cisco ASR 1000 シリーズの集約サービス ルータで導入されました。 この機能は、Cisco IOS XE Release 2.3.1 に統合されました。 次のコマンドが導入または変更されました。**vendor-tag circuit-id service**、**vendor-tag strip**

セッション制限のサポートの提供

PPP over Ethernet セッション制限機能を使用すると、設定用にルータ上またはギガビット イーサネット インターフェイス上に作成できる PPP over Ethernet（PPPoE）セッションの数を制限できます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「セッション制限のサポートの提供の機能情報」（P.8）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「セッション制限のサポートの提供に関する情報」（P.2）
- 「セッション制限のサポートを提供する方法」（P.2）
- 「セッション制限のサポートの提供の設定例」（P.5）
- 「その他の関連資料」（P.6）
- 「セッション制限のサポートの提供の機能情報」（P.8）

セッション制限のサポートの提供に関する情報

セッション制限のサポートを設定するには、次の概念を理解しておく必要があります。

- 「セッション制限のサポートの提供の利点」（P.2）

セッション制限のサポートの提供の利点

PPPoE セッション制限機能は、ルータに作成できる PPPoE セッションの数、またはすべてのイーサネット インターフェイスとサブインターフェイスおよび ATM インターフェイスとサブインターフェイスに作成できる PPPoE セッションの数を制限することで、ルータが仮想アクセス用に使用するメモリが多くなりすぎないようにします。

セッション制限のサポートを提供する方法

PPPoE セッション制限を設定するには、次のいずれかまたは両方の作業を行います。

- 「ルータでの PPPoE セッションの最大数の指定」（P.2）（任意）
- 「ギガビット イーサネット インターフェイスでの PPPoE セッションの最大数の指定」（P.4）（任意）

ルータでの PPPoE セッションの最大数の指定

ルータに作成できる PPPoE セッションの最大数を指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*word* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions per-vlan limit** *per-vlan-limit* [**inner**]
7. **sessions per-vc limit** [**threshold** *threshold-value*]
8. **sessions max limit** *number-of-sessions* [*threshold-value*]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** {*name* | **global**} **例：** `Router(config)# bba-group pppoe global`	BBA グループが PPPoE セッションの確立に使用されるように設定し、BBA グループ コンフィギュレーション モードを開始します。 • *name* : Broadband Aggregation（BBA; ブロードバンド集約）グループを示します。複数の BBA グループを作成できます。 • **global** : 特定の PPPoE プロファイルが割り当てられていない PPPoE ポート（ギガビット イーサネット インターフェイスまたは VLAN）のデフォルト プロファイルとして機能する PPPoE プロファイル。
ステップ 4	**virtual-template** *template-number* **例：** `Router(config-bba-group)# virtual-template 1`	この PPPoE プロファイルを使用するすべての PPPoE ポートの仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 5	**sessions per-mac limit** *per-mac-limit* **例：** `Router(config-bba-group)# sessions per-mac limit 1000`	（任意）PPPoE プロファイルの MAC セッション制限あたりの PPPoE セッションの最大数を設定します。
ステップ 6	**sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id*] **例：** `Router(config-bba-group)# session per-vlan limit 4000 inner 3500`	（任意）QinQ サブインターフェイスの内部 VLAN に対するセッション制限を設定します。 **（注）** VLAN 単位の制限は、ギガビット イーサネット サブインターフェイスだけに適用できます（802.1q VLAN）。
ステップ 7	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **例：** `Router(config-bba-group)# sessions per-vc limit 2000`	（任意）PPPoE プロファイルの VC セッション制限あたりの PPPoE セッションの最大数を設定します。 **（注）** VC 単位の制限は、ATM インターフェイスとサブインターフェイスだけに適用できます。

	コマンドまたはアクション	目的
ステップ 8	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **例：** `Router(config-bba-group)# sessions max limit 32000`	PPPoE グローバル プロファイルで、ルータで許可される PPPoE セッションの最大数と、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成される PPPoE セッション数のしきい値を設定します。 **（注）** このコマンドは、グローバル プロファイルだけに適用されます。
ステップ 9	**exit** **例：** `Router(config-bba-group)# exit`	グローバル コンフィギュレーション モードに戻ります。

ギガビット イーサネット インターフェイスでの PPPoE セッションの最大数の指定

ギガビット イーサネット インターフェイスに作成できる PPPoE セッションの最大数を指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {`GigabitEthernet` | `tenGigabitEthernet`} /*subslot*/*port*[.*subinterface*]
4. **pppoe enable** [`group` *group-name*]
5. **pppoe max-sessions** *number*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**GigabitEthernet** | **tenGigabitEthernet**} *slot*/*subslot*/*port*[.*subinterface*] **例：** `Router(config)# interface GigabitEthernet0/0/1`	ギガビット イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**pppoe enable** [**group** *group-name*] **例：** `Router(config-if)# pppoe enable group one`	ギガビット イーサネット インターフェイスまたはサブインターフェイスで PPPoE セッションをイネーブルにします。 **（注）** **group** *group-name* オプションを使用してインターフェイスに PPPoE プロファイルを割り当てない場合、そのインターフェイスではグローバル PPPoE プロファイルが使用されます。
ステップ 5	**pppoe max-sessions** *number* **例：** `Router(config-if)# pppoe max-sessions 10`	インターフェイスまたはサブインターフェイスで許可される PPPoE セッションの最大数を指定します。
ステップ 6	**end** **例：** `Router(config-if)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セッション制限のサポートの提供の設定例

ここでは、次の設定例について説明します。

- 「ルータでの PPPoE セッションの最大数の指定：例」（P.5）
- 「ギガビット イーサネット インターフェイスでの PPPoE セッションの最大数の指定：例」（P.5）

ルータでの PPPoE セッションの最大数の指定：例

次の例では、32,000 PPPoE セッションの制限をルータに設定します。

```
bba-group pppoe global
  virtual-template 1
  sessions per-mac limit 1000
  sessions per-vlan limit 4000 inner 3500
  sessions per-vc limit 2000
```

ギガビット イーサネット インターフェイスでの PPPoE セッションの最大数の指定：例

次の例では、10 PPPoE セッションの制限をギガビット イーサネット インターフェイスに設定します。

```
interface GigabitEthernet1/0/0
  pppoe enable
  pppoe max-sessions 10
```

次の例では、**encapsulation** コマンドを使用して 10 PPPoE セッションの制限をギガビット イーサネット サブインターフェイスに設定します。

```
interface GigabitEthernet0/0/0.1
```

```
encapsulation dot1q 2
pppoe enable
pppoe max-sessions 10
```

その他の関連資料

ここでは、レガシー設定でのセッション制限のサポートに関する参考資料を紹介します。

関連マニュアル

内容	参照先
PPPoE セッションのブロードバンド アクセス集約	『*Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions*』
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

セッション制限のサポートの提供の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　セッション制限のサポートの提供の機能情報

機能名	リリース	機能情報
PPP over Ethernet セッション制限	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.4	この機能は、Cisco ASR 1000 シリーズの集約サービス ルータで導入されました。 PPP over Ethernet（PPPoE）セッション制限機能を使用すると、設定用にルータ上またはギガビット イーサネット インターフェイス上に作成できる PPPoE セッションの数を制限できます。 この機能は、Cisco IOS XE Release 2.4 に統合されました。

PPPoE セッション制限ローカル オーバーライド

PPPoE セッション制限ローカル オーバーライド機能を使用すると、Subscriber Service Switch（SSS）の事前承認が有効になっているときに、RADIUS サーバからダウンロードされる NAS ポート単位のセッション制限を、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）または L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）でローカルに設定されているセッション制限によって上書きできます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPPoE セッション制限ローカル オーバーライドの機能情報」（P.7）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE セッション制限ローカル オーバーライドに関する情報」（P.2）
- 「PPPoE セッション制限ローカル オーバーライドの設定方法」（P.3）
- 「PPPoE セッション制限ローカル オーバーライドの設定例」（P.4）
- 「その他の関連資料」（P.4）
- 「PPPoE セッション制限ローカル オーバーライドの機能情報」（P.7）

PPPoE セッション制限ローカル オーバーライドに関する情報

PPPoE セッション制限ローカル オーバーライド機能を設定するには、次の概念を理解しておく必要があります。

- 「PPPoE セッション制限ローカル オーバーライド機能の動作方法」

PPPoE セッション制限ローカル オーバーライド機能の動作方法

PPP over Ethernet（PPPoE）セッション制限は、**subscriber access pppoe pre-authorize nas-port-id** コマンドを使用して LAC で SSS 事前承認がイネーブルになっていると、RADIUS サーバからダウンロードされます。事前承認をイネーブルにすると、特定の VLAN での PPPoE セッションの数が制限されます。つまり、RADIUS サーバからダウンロードされる PPPoE の NAS ポート単位のセッション制限が、VLAN 単位のセッション制限などのローカルに設定された（ポートベースの）セッション制限より優先されます。次に、RADIUS を使用してセッション制限を設定するユーザ プロファイルの例を示します。

```
Username=nas_port:10.10.10.10:4/0/0/1.100
Password = "password1"
cisco-avpair= "pppoe:session-limit=session limit per NAS-port"
```

PPPoE セッション制限ローカル オーバーライド機能を使用すると、BRAS で設定されたローカルなセッション制限で、SSS 事前承認が設定されているときに RADIUS サーバで設定される NAS ポート単位のセッション制限を上書きできます。

（注） PPPoE セッション制限ローカル オーバーライド機能は、BRAS または LAC で SSS 事前承認を設定してあるときだけ有効です。

PPPoE セッション制限ローカル オーバーライド機能をイネーブルにするには、インターフェイスに関連する Broadband Access（BBA; ブロードバンド アクセス）グループで **sessions pre-auth limit ignore** コマンドを設定します。PPPoE セッション制限ローカル オーバーライド機能をイネーブルにすると、PPP が開始される前に、つまり BRAS が PPPoE Active Discovery Offer（PADO）パケットをクライアントに送信して、使用可能なサービスのリストをアドバタイズする前に、ローカルに設定されているセッション制限が適用されます。

PPPoE セッション制限ローカル オーバーライド機能をイネーブルにしないで事前承認を設定した場合、RADIUS サーバからセッション制限がダウンロードされていない状態で、ローカルに設定されているセッション制限を超過すると、クライアントは認証失敗応答を BRAS から受け取ります。BRAS は、PPP ネゴシエーションが完了するまで、ローカルに設定されている制限の適用を待ちます。コールが最終的に拒否されると、クライアントは認証失敗応答を受信してセッションは失敗します。セッションの障害が、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）認証の失敗によるものか、または PPPoE セッション制限の超過によるものかを区別する方法はありません。PPPoE セッション制限ローカル オーバーライド機能は、NAS ポート単位での処理の障害とセッション制限の障害を区別できます。

PPPoE セッション制限ローカル オーバーライド機能をイネーブルにしても、ローカルに設定されたポート単位のセッション制限がない場合は、RADIUS サーバからダウンロードされた NAS ポート単位のセッション制限が適用されます。

PPPoE セッション制限ローカル オーバーライドの設定方法

ここでは、次の手順について説明します。

- 「PPPoE セッション制限ローカル オーバーライドのイネーブル化」（P.3）

PPPoE セッション制限ローカル オーバーライドのイネーブル化

PPPoE セッション制限ローカル オーバーライド機能をイネーブルにすると、BRAS で設定されたローカルなセッション制限で、RADIUS サーバからダウンロードされる NAS ポート単位のセッション制限を上書きできます。

制約事項

ローカルに設定されたポート単位のセッション制限がない場合は、RADIUS サーバからダウンロードされた NAS ポート単位のセッション制限が適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **sessions per-vlan limit** *per-vlan-limit*
5. **sessions pre-auth limit ignore**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** {*group-name* | **global**} **例：** `Router(config)# bba-group pppoe test`	PPPoE プロファイルを作成し、BBA グループ コンフィギュレーション モードを開始します。 • *group-name*：PPPoE プロファイルの名前。
ステップ 4	**sessions per-vlan limit** *per-vlan-limit* **例：** `Router(config-bba-group)# sessions per-vlan limit 3`	PPPoE プロファイルの VLAN あたりの PPPoE セッションの数を制限します。 • *per-vlan-limit*：イーサネット VLAN で確立できる PPPoE セッションの最大数。デフォルト値は 100 です。

	コマンドまたはアクション	目的
ステップ 5	**sessions pre-auth limit ignore** **例：** `Router(config-bba-group)# sessions pre-auth limit ignore`	PPPoE セッション制限ローカル オーバーライド機能をイネーブルにします。ローカルに設定された制限で、RADIUS サーバで設定されている NAS ポート単位でのセッション制限を上書きできます。
ステップ 6	**end** **例：** `Router(config-bba-group)# end`	BBA グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PPPoE セッション制限ローカル オーバーライドの設定例

ここでは、次の例について説明します。

- 「PPPoE セッション制限ローカル オーバーライドのイネーブル化：例」

PPPoE セッション制限ローカル オーバーライドのイネーブル化：例

次の例では、test という名前の PPPoE グループを作成し、VLAN ごとに 3 つのセッションの制限を設定し、bba-group コンフィギュレーション モードで PPPoE セッション制限ローカル オーバーライド機能をイネーブルにします。実行中のコンフィギュレーションでは、**sessions pre-auth limit ignore** コマンドを使用してこの機能がイネーブルにされたことが示されます。

```
Router(config)# bba-group pppoe test
Router(config-bba-group)# sessions per-vlan limit 3
Router(config-bba-group)# sessions pre-auth limit ignore
.
.
!
bba-group pppoe test
virtual-template 2
sessions per-vlan limit 3
sessions pre-auth limit ignore
!
```

その他の関連資料

ここでは、PPPoE セッション制限ローカル オーバーライド機能に関する参考資料を紹介します。

関連マニュアル

内容	参照先
このマニュアルで使用しているコマンドのその他の情報	• *『Cisco IOS Broadband Access Aggregation and DSL Command Reference』* • *『Cisco IOS Master Command List, All Releases』*

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PPPoE セッション制限ローカル オーバーライドの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　PPPoE セッション制限ローカル オーバーライドの機能情報

機能名	リリース	機能情報
PPPoE セッション制限ローカル オーバーライド	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能を使用すると、Subscriber Service Switch（SSS）の事前承認が有効になっているときに、RADIUS サーバからダウンロードされる NAS ポート単位のセッション制限を、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）または L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）でローカルに設定されているセッション制限によって上書きできます。 次のコマンドが導入または変更されました。**sessions pre-auth limit ignore**

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供

PPP over Ethernet（PPPoE）プロファイルには、PPPoE セッションのグループの設定情報が含まれています。1 つのデバイスに対して複数の PPPoE プロファイルを定義できるため、PPPoE セッションのブロードバンド アクセス集約をサポートするために使用されているさまざまな PPP インターフェイス、VLAN、および ATM PVC にさまざまな仮想テンプレートやその他の PPPoE 設定パラメータを割り当てることができます。

（注） ここでは、プロファイルを使用して PPPoE セッションを設定する方法について説明します。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の機能情報」（P.32）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の前提条件」（P.2）
- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の制約事項」（P.2）
- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供に関する情報」（P.3）
- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートを提供する方法」（P.6）

- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の設定例」（P.23）
- 「関連情報」（P.28）
- 「その他の関連資料」（P.29）
- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の機能情報」（P.32）

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の前提条件

- 「Understanding Broadband Access Aggregation」で説明されている概念について理解している必要があります。
- 「Preparing for Broadband Access Aggregation」に含まれている作業を実行する必要があります。

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の制約事項

PPPoE ポート（ギガビット イーサネット インターフェイス、VLAN、または PVC）、Virtual Circuit（VC; 仮想回線）クラス、または ATM PVC 範囲に PPPoE プロファイルを割り当てた場合にそのプロファイルがまだ定義されていないと、そのポート、VC クラス、または範囲では PPPoE パラメータが設定されず、グローバル グループのパラメータも使用されません。

サブインターフェイスを使用せずに PPPoE over 802.1Q VLAN のサポートを設定できるのは PPPoE サーバだけです。

ATM PVC で PPPoE over 802.1Q VLAN のサポートを設定できるのは PPPoE サーバだけです。

メイン インターフェイスで設定されている VLAN のトラフィックを個別にシャットダウンすることはできません。サブインターフェイスで設定されている VLAN を個別にシャットダウンすることはできます。

メイン インターフェイスで VLAN の範囲を設定し、同じメイン インターフェイスのサブインターフェイスでその範囲外の VLAN を同時に設定することはできますが、メイン インターフェイスとサブインターフェイスで特定の VLAN を同時に設定することはできません。

PPP セッションでサポートされている（サポートされていない）加入者機能を表 1 に示します。

表 1　PPP セッションでサポートされている（サポートされていない）加入者機能

機能名	サポートしているリリース
LNS での加入者ごとのファイアウォール	Cisco IOS XE Release 2.2.1 *http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp1045661*
PTA での加入者ごとのファイアウォール	サポートされていません
加入者ごとの NAT	サポートされていません
加入者ごとの PBR	サポートされていません
加入者ごとの NBAR	サポートされていません

表 1　PPP セッションでサポートされている（サポートされていない）加入者機能 （続き）

機能名	サポートしているリリース
加入者ごとのマルチキャスト	Cisco IOS XE Release RLS 2.2.1 以降（3,000 セッションまで） *http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp1105824*
加入者ごとの Netflow	サポートされていません
MLPPP on LNS	サポートされていません
MLPoE on PTA	サポートされていません
MLPoE LAC スイッチング	サポートされていません

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供に関する情報

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートを提供するには、次の概念を理解しておく必要があります。

- 「PPPoE 仕様の定義」（P.3）
- 「PPPoE 接続スロットリング」（P.4）
- 「サブインターフェイスを使用しない VLAN への PPPoE プロファイルの割り当て」（P.4）
- 「ATM PVC 用自動検知」（P.5）

PPPoE 仕様の定義

PPP over Ethernet（PPPoE）は、ホスト PC が一般的なブロードバンド メディア（Digital Subscriber Line（DSL; デジタル加入者線）、ワイヤレス モデム、ケーブル モデムなど）とやり取りして高速データ ネットワークにアクセスするための方法を定義する仕様です。ギガビット イーサネットと PPP という広く受け入れられている 2 つの標準に依存している PPPoE の実装では、ギガビット イーサネット上のユーザが共通の接続を共有することができます。この接続は、LAN で複数のユーザをサポートするギガビット イーサネットの原則と、シリアル接続に適用される PPP の原則の組み合わせによってサポートされます。

基本プロトコルは RFC 2516 で定義されています。

PPPoE 接続スロットリング

PPPoE セッションの開始要求が頻繁に行われると、ルータや RADIUS サーバのパフォーマンスが低下する可能性があります。PPPoE 接続スロットリング機能を使用すると、PPPoE 接続要求を制限して、意図的なサービス拒否攻撃や意図的でない PPP 認証ループを防止することができます。この機能は、PPPoE サーバにセッション スロットリングを実装して、指定した期間に 1 つの MAC アドレスまたは VC から開始できる PPPoE セッション要求の数を制限します。

サブインターフェイスを使用しない VLAN への PPPoE プロファイルの割り当て

サブインターフェイスを使用せずに PPPoE プロファイルを VLAN に割り当てると、PPP over Ethernet（PPPoE）over IEEE 802.1Q VLAN 機能が次の 2 つの点で強化されます。

- PPPoE VLAN をサブインターフェイスで個別に作成する必要がなくなるため、ルータで設定できる VLAN の数が 1 インターフェイスあたり 4000 個に増加します。
- ブリッジド RFC 1483 カプセル化を使用する PPPoE over VLAN トラフィックが ATM PVC でサポートされるようになります。

PPPoE over 802.1Q VLAN のサポートをサブインターフェイスではなくインターフェイスで設定する場合、および ATM で PPPoE over 802.1Q VLAN のサポートを設定する場合は、次の概念について理解しておく必要があります。

- 「サブインターフェイスを使用しない PPPoE over VLAN の設定」（P.4）
- 「ATM PVC での PPPoE over VLAN のサポート」（P.4）
- 「PPPoE over VLAN のスケーリングと ATM での PPPoE over VLAN のサポートの利点」（P.5）

サブインターフェイスを使用しない PPPoE over VLAN の設定

サブインターフェイスを使用せずに PPPoE プロファイルを VLAN に割り当てると、PPPoE VLAN をサブインターフェイスで個別に作成する必要がなくなります。メイン インターフェイスで複数の PPPoE VLAN を設定できるようになるため、ルータで設定できる VLAN の数が 1 インターフェイスあたり 4000 個に増加します。

インターフェイスでは、VLAN を個別に設定することも、VLAN の範囲を設定することもできます。メイン インターフェイスで VLAN の範囲を設定し、同じインターフェイスのサブインターフェイスでその範囲外の VLAN を同時に設定することができます。

ATM PVC での PPPoE over VLAN のサポート

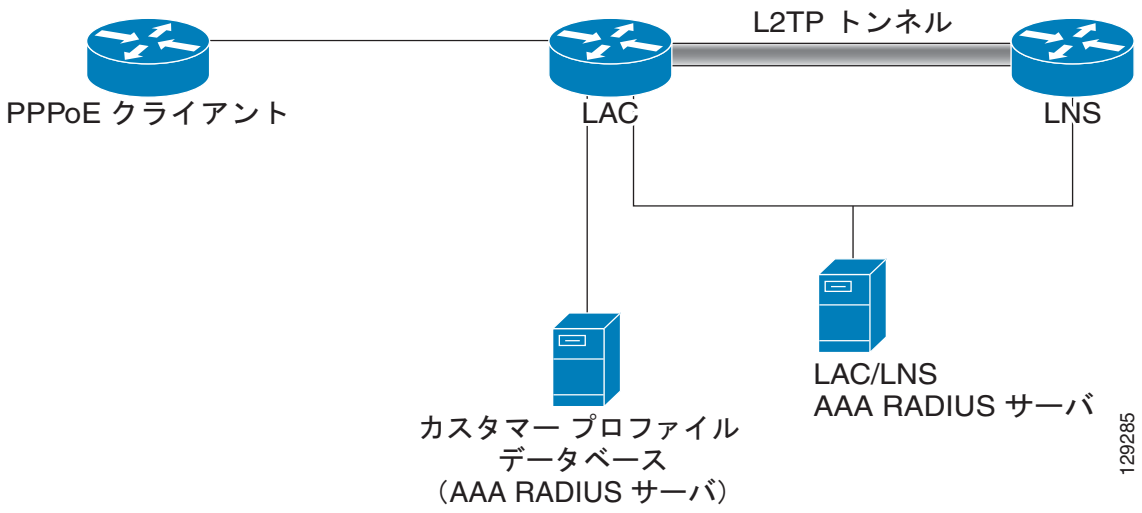
サブインターフェイスを使用せずに PPPoE プロファイルを VLAN に割り当てると、ブリッジド RFC 1483 カプセル化を使用する PPPoE over VLAN パケットを ATM PVC で処理できるようになります。これにより、異なる 802.1Q VLAN の PPPoE トラフィックを同じ ATM PVC で多重化できます。

図 1 は、ATM PVC 上の PPPoE over VLAN を実装するサンプル ネットワーク トポロジを示しています。このトポロジのサービス プロバイダーは、ホーム ユーザにギガビット イーサネット サービスを提供するためのギガビット イーサネット スイッチと、WAN アクセスとのスイッチを提供するための単一の PVC を使用しています。ホーム ユーザは、PPPoE を使用して Network Access Server（NAS; ネットワーク アクセス サーバ）上のサービスにアクセスします。スイッチの各ポートにそれぞれ異なる VLAN が割り当てられており、ブリッジとして機能する DSL モデムに接続されたギガビット イーサネット インターフェイスで VLAN がトランキングされます。

ギガビット イーサネット スイッチ トランクから送られてくる 802.1Q VLAN カプセル化トラフィックは、DSL モデムによって RFC 1483 ブリッジド カプセル化でカプセル化されて、ATM WAN 経由で NAS に送信されます。ATM PVC 上の PPPoE over VLAN をサポートするように設定されている NAS は、RFC 1483 ブリッジド カプセル化上の PPPoE over 802.1Q VLAN から PPPoE パケットを抽出して、ユーザに PPPoE サービスを提供します。

ダウンリンクでは、NAS が RFC 1483 ブリッジド カプセル化上の PPPoE over 802.1Q VLAN でパケットを送信し、DSL モデムが RFC 1483 カプセル化を取り除いて 802.1Q VLAN パケットをトランク経由でスイッチに転送します。スイッチは、802.1 VLAN ID に関連付けられているポートにギガビット イーサネット パケットを送信します。

図 1　ATM 上の PPPoE over 802.1Q VLAN のサンプル ネットワーク トポロジ



PPPoE over VLAN のスケーリングと ATM での PPPoE over VLAN のサポートの利点

PPPoE over VLAN のスケーリングと ATM での PPPoE over VLAN のサポートの利点を以下に示します。

- PPPoE VLAN をサブインターフェイスで個別に設定する必要がなくなるため、ルータで設定できる VLAN の数が 1 インターフェイスあたり 4000 個に増加します。
- RFC 1483 ブリッジド カプセル化を使用して ATM インターフェイス上の PPPoE over VLAN をサポートできます。

ATM PVC 用自動検知

ATM PVC 用の PPPoA/PPPoE 自動検知 機能を使用すると、ルータで着信 PPP over Ethernet（PPPoE）over ATM セッションを識別して、この両方のタイプの PPP のニーズに基づく仮想アクセスを作成できます。

（注）　ATM PVC 用の PPPoA/PPPoE 自動検知 機能は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）でカプセル化された ATM PVC でのみサポートされます。Multiplexer（MUX; マルチプレクサ）でカプセル化された PVC ではサポートされません。

ATM PVC 用自動検知の利点

ATM PVC 用自動検知を使用すると、リソースをオンデマンドで割り当てることができます。PPPoE 用に設定された各 PVC では、PPPoE セッションが存在するかどうかに関係なく、設定時に特定のリソース（1 つの仮想アクセス インターフェイスを含む）が割り当てられます。ATM PVC 用自動検知では、クライアントが PPPoE セッションを開始したときにのみリソースが割り当てられるため、NAS のオーバーヘッドが軽減されます。

（注）　ATM PVC 用自動検知でサポートされているのは ATM PVC だけです。Switched Virtual Circuit（SVC; 相手先選択接続）はサポートされていません。

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートを提供する方法

プロファイルを割り当てることによってブロードバンド アクセス集約に対するプロトコル サポートを提供するには、プロファイルを定義する必要があります。プロファイルの定義については、「PPPoE プロファイルを定義する」（P.6）を参照してください。そのほかに、プロファイルを特定のプロトコルタイプに割り当てる作業も必要になります。

- 「PPPoE プロファイルを定義する」（P.6）（必須）
- 「インターフェイスで PPPoE をイネーブルにする」（P.8）（必須）
- 「ATM PVC に PPPoE プロファイルを割り当てる」（P.9）（任意）
- 「ATM PVC 範囲および範囲内の PVC に PPPoE プロファイルを割り当てる」（P.10）（任意）
- 「ATM VC クラスに PPPoE プロファイルを割り当てる」（P.12）（任意）
- 「PPPoE に対して別の MAC アドレスを設定する」（P.18）（任意）
- 「VLAN サブインターフェイスに PPPoE プロファイルを割り当てる」（P.13）（任意）

サブインターフェイスを使用せずに PPPoE プロファイルを VLAN に割り当てるには、次のいずれかの作業を行います。

- 「メイン ギガビット イーサネット インターフェイスで PPPoE over IEEE 802.1Q VLAN のサポートを設定する」（P.14）（任意）
- 「ブリッジ カプセル化 PPPoE over IEEE 802.1Q VLAN トラフィックをサポートするように ATM PVC を設定する」（P.16）（任意）
- 「VC クラスで PPPoE over IEEE 802.1Q VLAN のサポートをイネーブルにする」（P.17）（任意）

システムのリロード後に PPPoE セッションが回復されるように設定するには、次の作業を実行します。

- 「PPPoE に対して別の MAC アドレスを設定する」（P.18）（任意）

PPPoE プロファイルを定義する

PPPoE プロファイルを定義するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*]
6. **sessions per-mac limit** *per-mac-limit*
7. **sessions per-vlan limit** *per-vlan-limit* [**inner** *per-inner-vlan-limit*]
8. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
9. **sessions** {**per-mac** | **per-vc**} **throttle** *session-request session-request-period blocking-period*
10. **ac name** *name*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** {*group-name* | **global**} **例：** `Router(config)# bba-group pppoe global`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。 • **global** キーワードは、特定のプロファイルが割り当てられていない PPPoE ポートのデフォルト プロファイルとして機能するプロファイルを作成します。
ステップ 4	**virtual-template** *template-number* **例：** `Router(config-bba-group)# virtual-template 1`	この PPPoE プロファイルを使用するすべての PPPoE ポートの仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 5	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **例：** `Router(config-bba-group)# sessions max limit 8000`	PPPoE グローバル プロファイルで、ルータで許可される PPPoE セッションの最大数と、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成される PPPoE セッション数のしきい値を設定します。 **（注）** このコマンドは、グローバル プロファイルだけに適用されます。
ステップ 6	**sessions per-mac limit** *per-mac-limit* **例：** `Router(config-bba-group)# sessions per-mac limit 2`	PPPoE プロファイルの MAC アドレスあたりの PPPoE セッションの最大数を設定します。
ステップ 7	**sessions per-vlan limit** *per-vlan-limit* **inner** *per-inner-vlan-limit* **例：** `Router(config-bba-group)# sessions per-vlan limit 200`	PPPoE プロファイルの VLAN あたりの PPPoE セッションの最大数を設定します。 • **inner** キーワードは、外部 VLAN あたりのセッション数を設定します。
ステップ 8	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **例：** `Router(config-bba-group)# sessions per-vc limit 8`	PPPoE プロファイルで、VC で許可される PPPoE セッションの最大数と、SNMP トラップが生成される PPPoE セッション数のしきい値を設定します。

	コマンドまたはアクション	目的
ステップ 9	**sessions** {**per-mac** | **per-vc**} **throttle** *session-requests session-request-period blocking-period* **例：** `Router(config-bba-group)# sessions per-vc throttle 100 30 3008`	（任意）PPPoE 接続スロットリング を設定します。この機能は、指定した期間に 1 つの VC または MAC アドレスから開始できる PPPoE セッション要求の数を制限します。
ステップ 10	**ac name** *name* **例：** `Router(config-bba-group)# ac name ac1`	（任意）PPPoE Active Discovery Offer（PADO）で使用するアクセス コンセントレータの名前を指定します。
ステップ 11	**end** **例：** `Router(config-bba-group)# end`	（任意）BBA グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスで PPPoE をイネーブルにする

ギガビット イーサネット インターフェイスで PPPoE をイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *number*
4. **pppoe enable** [**group** *group-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface gigabitethernet** *number* **例：** `Router(config)# interface gigabitethernet 0/0/0[.0]`	ギガビット イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**pppoe enable** [**group** *group-name*] **例：** `Router(config-subif)# pppoe enable group one`	ギガビット イーサネット インターフェイスまたはサブインターフェイスで PPPoE セッションをイネーブルにします。 **（注）** **group** *group-name* オプションを使用してインターフェイスに PPPoE プロファイルを割り当てない場合、そのインターフェイスでは global PPPoE プロファイルが使用されます。
ステップ 5	**end** **例：** `Router(config-subif)# end`	（任意）サブインターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ATM PVC に PPPoE プロファイルを割り当てる

ATM PVC に PPPoE プロファイルを割り当てるには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **pvc** *vpi*/*vci*
5. **protocol pppoe** [**group** *group-name*]

   または

   encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface atm** *number* [**point-to-point** | **multipoint**] **例：** `Router(config)# interface atm 5/0.1 multipoint`	ATM のインターフェイスまたはサブインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**pvc** *vpi*/*vci* **例：** `Router(config-if)# pvc 2/101`	ATM PVC を作成し、ATM 仮想回線コンフィギュレーション モードを開始します。

ステップ 5	**protocol pppoe** [**group** *group-name*]
	または
	encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
	
	例：
	`Router(config-if-atm-vc)# protocol pppoe group one`
	または
	`Router(config-if-atm-vc)# encapsulation aal5autoppp virtual-template 1 group one`
		ATM PVC で PPPoE セッションを確立できるようにします。
		または
		PVC で PPPoE の自動検知を設定します。
		（注） **group** *group-name* オプションを使用して PVC に PPPoE プロファイルを割り当てない場合、その PVC では global PPPoE プロファイルが使用されます。

ステップ 6	**end** **例：** `Router(config-if-atm-vc)# end`	（任意）ATM 仮想回線コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ATM PVC 範囲および範囲内の PVC に PPPoE プロファイルを割り当てる

ATM PVC 範囲および範囲内の PVC に PPPoE プロファイルを割り当てるには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*

5. **protocol pppoe** [**group** *group-name*]

   または

   encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
6. **pvc-in-range** [*pvc-name*] [[*vpi*/]*vci*]
7. **protocol pppoe** [**group** *group-name*]

   または

   encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface atm** *number* [**point-to-point** | **multipoint**] **例：** `Router(config)# interface atm 5/0.1 multipoint`	ATM のインターフェイスまたはサブインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci* **例：** `Router(config-if)# range range-one pvc 100 4/199`	PVC の範囲を定義し、ATM PVC 範囲コンフィギュレーション モードを開始します。

ステップ 5	**protocol pppoe** [**group** *group-name*]
	
	または
	
	encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
	
	例：
	`Router(config-if-atm-range)# protocol pppoe group one`
	
	または
	
	`Router(config-if-atm-range)# encapsulation aal5autoppp virtual-template 1 group one`
		ATM PVC の範囲で PPPoE セッションを確立できるようにします。
		または
		PPPoE の自動検知を設定します。
		（注） **group** *group-name* オプションを使用して PVC 範囲に PPPoE プロファイルを割り当てない場合、その範囲内の PVC では global PPPoE プロファイルが使用されます。

	コマンドまたはアクション	目的
ステップ 6	**pvc-in-range** [*pvc-name*] [[*vpi*/]*vci*] **例：** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	PVC 範囲内の PVC を定義し、ATM PVC-in-range コンフィギュレーション モードをイネーブルにします。

ステップ 7	**protocol pppoe** [**group** *group-name*]
	
	または
	
	encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
	
	例：
	`Router(cfg-if-atm-range-pvc)# protocol pppoe group two`
	
	または
	
	`Router(cfg-if-atm-range-pvc)# encapsulation aal5autoppp virtual-template 1 group two`
		範囲内の PVC で PPPoE セッションを確立できるようにします。
		
		または
		
		PPPoE の自動検知を設定します。
		
		（注） **group** *group-name* オプションを使用して PVC に PPPoE プロファイルを割り当てない場合、その PVC では global PPPoE プロファイルが使用されます。

ステップ 8	**end** **例：** `Router(cfg-if-atm-range-pvc)# end`	（任意）ATM PVC-in-range コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ATM VC クラスに PPPoE プロファイルを割り当てる

ATM VC クラスに PPPoE プロファイルを割り当てるには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **protocol pppoe** [**group** *group-name*]

   または

   encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vc-class atm** *vc-class-name* **例：** `Router(config)# vc-class atm class1`	ATM VC クラス を作成し、ATM VC クラス コンフィギュレーション モードを開始します。 • VC クラスは、ATM インターフェイス、ATM サブインターフェイス、または ATM VC に適用できます。

ステップ 4	**protocol pppoe** [**group** *group-name*]
	
	または
	
	encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
	
	例：
	`Router(config-vc-class)# protocol pppoe group two`
	
	または
	
	`Router(config-vc-class)# encapsulation aal5autoppp virtual-template 1 group two`
		PPPoE セッションを確立できるようにします。
		または
		PPPoE の自動検知を設定します。
		（注） **group** *group-name* オプションを使用して PPPoE プロファイルを割り当てない場合は、global PPPoE プロファイルを使用して PPPoE セッションが確立されます。

ステップ 5	**end** **例：** `Router(config-vc-class)# end`	（任意）ATM VC クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VLAN サブインターフェイスに PPPoE プロファイルを割り当てる

VLAN サブインターフェイスに PPPoE プロファイルを割り当てるには、この作業を実行します。

（注） この設定方法ではサブインターフェイスを使用する必要があります。1 つのサブインターフェイスで 1 つの VLAN がサポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface range** {**gigabitethernet** | **atm**} *slot/interface*.*subinterface* **-** {**gigabitethernet** | **atm**} *slot/interface*.*subinterface*

4. **encapsulation dot1q** *vlan-id*
5. **pppoe enable** [**group** *group-name*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** {**gigabitethernet** | **atm**} *slot*/*interface.subinterface* - {**gigabitethernet** | **atm**} *slot*/*interface.subinterface* 例： `Router(config)# interface range gigabitethernet 0/5/1.1 - gigabitethernet 0/5/1.4`	インターフェイスにサブインターフェイスを割り当てて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**encapsulation dotlq** *vlan-id* 例： `Router(config-if-range)# encapsulation dot1q 301`	インターフェイスで使用するカプセル化方法を設定します。
ステップ 5	**pppoe enable** [**group** *group-name*} 例： `Router(config-if-range)# pppoe enable group two`	PPPoE セッションを確立できるようにします。
ステップ 6	**end** 例： `Router(config-if-range)# end`	（任意）インターフェイス範囲コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

メイン ギガビット イーサネット インターフェイスで PPPoE over IEEE 802.1Q VLAN のサポートを設定する

メイン ギガビット イーサネット インターフェイスで PPPoE over IEEE 802.1Q VLAN のサポートをイネーブルにするには、この作業を実行します。

PPPoE over VLAN の機能強化 : 設定の制限の削除と ATM のサポートの機能により、PPPoE VLAN をサブインターフェイスで個別に作成する必要がなくなります。メイン インターフェイスで複数の PPPoE VLAN を設定できるようになるため、ルータで設定できる VLAN の数が 1 インターフェイスあたり 4000 個に増加します。

インターフェイスでは、VLAN を個別に設定することも、VLAN の範囲を設定することもできます。メイン インターフェイスで VLAN の範囲を設定し、同じインターフェイスのサブインターフェイスでその範囲外の VLAN を同時に設定することができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/subslot/port*[*.subinterface*]
4. **vlan-id dot1q** *vlan-id*

   または

   vlan-range dot1q *start-vlan-id end-vlan-id*
5. **pppoe enable** [**group** *group-name*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/subslot/port*[*.subinterface*] **例：** `Router(config)# interface gigabitethernet 0/1/0.2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**vlan-id dot1q** *vlan-id*
	
	または
	vlan-range dot1q *start-vlan-id end-vlan-id*
	
	例：
	`Router(config-if)# vlan-id dot1q 3`
	または
	`Router(config-if)# vlan-range dot1q 360`
		ギガビット イーサネット インターフェイス上の特定の VLAN で IEEE 802.1Q VLAN カプセル化をイネーブルにします。
		または
		ギガビット イーサネット インターフェイス上の VLAN の範囲で IEEE 802.1Q VLAN カプセル化をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**pppoe enable** [**group** *group-name*] **例：** `Router(config-if-vlan-range)# pppoe enable group pppoe1`	特定の VLAN または VLAN の範囲で PPPoE セッションをイネーブルにします。
ステップ 6	**end** **例：** `Router(config-if-vlan-range)# end`	（任意）インターフェイス VLAN 範囲コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ブリッジ カプセル化 PPPoE over IEEE 802.1Q VLAN トラフィックをサポートするように ATM PVC を設定する

ATM PVC で RFC 1483 ブリッジ カプセル化 PPPoE over IEEE 802.1Q VLAN トラフィックをサポートできるようにするには、次の作業を実行します。PPPoE over VLAN の機能強化：設定の制限の削除と ATM のサポートの機能により、ブリッジド RFC 1483 カプセル化を使用する PPPoE over VLAN パケットを ATM PVC で処理できるようになります。これにより、異なる 802.1Q VLAN の PPPoE トラフィックを同じ ATM PVC で多重化できます。

詳細については、「ATM PVC での PPPoE over VLAN のサポート」（P.4）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/*subslot*/*port*[.*subinterface-number*] {**multipoint** | **point-to-point**}
4. **pvc** [*name*] *vpi*/*vci*
5. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface atm** *slot*/*subslot*/*port*[.*subinterface-number*] {**multipoint** | **point-to-point**} **例：** `Router(config)# interface atm 0/2/0.1 multipoint`	ATM マルチポイント サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**pvc** [*name*] *vpi*/*vci* **例：** `Router(config-subif)# pvc 0/60`	PVC を設定し、ATM VC コンフィギュレーション モードを開始します。
ステップ 5	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **例：** `Router(config-if-atm-vc)# protocol pppovlan dot1q 3 50 group pppoe1`	ATM PVC 上の特定の IEEE 802.1Q VLAN または VLAN の範囲で PPPoE をイネーブルにします。
ステップ 6	**end** **例：** `Router(config-if-atm-vc)# end`	（任意）ATM VC コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VC クラスで PPPoE over IEEE 802.1Q VLAN のサポートをイネーブルにする

VC クラスで PPPoE over IEEE 802.1Q VLAN のサポートをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vc-class atm** *name* **例：** `Router(config)# vc-class atm class1`	ATM VC クラス を設定し、ATM VC クラス コンフィギュレーション モードを開始します。
ステップ 4	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **例：** `Router(config-vc-class)# protocol pppovlan dot1q 3 50 group pppoe1`	VC クラスで特定の IEEE 802.1Q VLAN または VLAN の範囲の PPPoE のサポートをイネーブルにします。 **（注）** VC クラスは、ATM インターフェイス、ATM サブインターフェイス、ATM PVC、または PVC の範囲に適用できます。
ステップ 5	**end** **例：** `Router(config-vc-class)# end`	（任意）ATM VC クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PPPoE に対して別の MAC アドレスを設定する

PPPoE 用の設定可能 MAC アドレス機能を使用すると、Broadband Access（BBA; ブロードバンド アクセス）グループで ATM PVC の MAC アドレスを設定して、PPP over Ethernet over ATM（PPPoEoA）に対して別の MAC アドレスを使用することができます。

PPPoE に対して別の MAC アドレスを設定して、集約ルータでギガビット イーサネットからのパケットを適切な PVC にブリッジできるようにするには、この作業を実行します。

PPPoE 用の設定可能 MAC アドレスの前提条件

BBA グループ プロファイルがすでに存在している必要があります。BBA グループ コマンドを使用して、PPPoE と Routed Bridge Encapsulation（RBE; ルーテッド ブリッジ エンカプセレーション）を使用する集約デバイスとクライアント デバイスでブロードバンド アクセスを設定します。

PPPoE に対して別の MAC アドレスを設定して、集約ルータでギガビット イーサネットからのパケットを適切な PVC にブリッジできるようにするには、この作業を実行します。

PPPoE 用を設定するには、次の概念を理解しておく必要があります。

- 「PPPoEoA 用の MAC アドレス」（P.19）
- 「PPPoE 用の設定可能 MAC アドレス機能の利点」（P.19）

PPPoEoA 用の MAC アドレス

システム変更の結果、システムで予想外の動作が発生するのを防ぐために、MAC アドレスの使用方法は、明示的に設定されない限り変更されません。

この機能では、別の MAC アドレスを使用する以外に PPPoE の動作は変更されません。この変更が適用されるのは ATM インターフェイス（PPPoEoA）だけで、ギガビット イーサネット、イーサネット VLAN、Data-over-Cable Service Interface Specifications（DOCSIS）など、PPPoE が動作するその他のインターフェイスには適用されません。それらのインターフェイスは、本質的にブロードキャスト インターフェイスであるため、PPPoE の MAC アドレスを変更するには無差別モードにする必要があります。インターフェイスを無差別モードにすると、ルータ ソフトウェアがすべてのギガビット イーサネット フレームを受信して不要なフレームをソフトウェア ドライバで廃棄しなければならなくなるため、ルータのパフォーマンスが低下します。

この機能は、デフォルトではディセーブルになっています。イネーブルにすると、BBA グループで設定されている ATM PVC インターフェイスのすべての PPPoE セッションに適用されます。

PPPoE と RBE が同じ DSL 上の 2 つの異なる PVC で設定されている場合は、Customer Premises Equipment（CPE; 顧客宅内機器）が純粋なブリッジのように機能して、ギガビット イーサネットから DSL 上の 2 つの ATM PVC にパケットをブリッジします。CPE がブリッジとして機能する場合、集約ルータでは PPPoE と RBE の両方に同じ MAC アドレスが使用されているため、CPE はパケットを正しい PVC にブリッジできません。この問題は、PPPoE 専用の別の MAC アドレスを使用することによって解決できます。その MAC アドレスは、設定することも、自動的に選択することもできます。

PPPoEoA セッションの MAC アドレスは、ATM インターフェイスで **mac-address** コマンドを使用して設定されている場合はその値になり、設定されていない場合は Burned-In MAC Address になります。この機能が有効になるのは、BBA グループで autoselect も特定の MAC アドレスも指定されていない場合だけです。

BBA グループで MAC アドレスが指定されている場合は、VC に適用されている BBA グループで指定されている MAC アドレスがすべての PPPoEoA セッションで使用されます。

MAC アドレスが自動的に選択される場合は、ATM インターフェイスの MAC アドレスに 7 が追加されます。

PPPoE 用の設定可能 MAC アドレス機能の利点

Cisco IOS XE 集約ルータは、インターフェイスの MAC アドレスをそのインターフェイス上のすべてのブロードバンド集約プロトコルの送信元 MAC アドレスとして使用するため、RBE と PPPoE の両方が同じ ATM インターフェイス上に展開されていると問題が発生する可能性があります。この機能を使用すると、その問題を解決できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*bba-group-name* | **global**}
4. **mac-address** {**autoselect** | *mac-address*}
5. **end**
6. **show pppoe session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** {*bba-group-name* | **global**} **例：** `Router(config)# bba-group pppoe bba group1`	BBA グループ コンフィギュレーション モードを開始します。
ステップ 4	**mac-address** {**autoselect** | *mac-address*} **例：** `Router(config-bba-group)# mac-address autoselect`	次のいずれかを指定して MAC アドレスを選択します。 • **autoselect**：MAC アドレスを自動的に選択します。ATM インターフェイスのアドレスに 7 を足した値が使用されます。 • *mac-address*：48 ビットの MAC アドレスを持つ標準のデータリンク層アドレス（ハードウェア アドレス、MAC 層アドレス、物理アドレスとも呼ばれます）を指定します。VC に適用されている BBA グループで指定されている MAC アドレスがすべての PPPoEoA セッションで使用されます。
ステップ 5	**end** **例：** `Router(config-bba-group)# end`	BBA グループ コンフィギュレーション モードを終了します。
ステップ 6	**show pppoe session** **例：** `Router# show pppoe session`	出力の最後の行に MAC アドレスがローカル MAC（LocMac）アドレスとして表示されます。

例

次の例では、MAC アドレスが LocMac として表示されています。

```
Router# show pppoe session

1 session in LOCALLY_TERMINATED (PTA) State
     1 session total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      3      3  000b.fdc9.0001  ATM3/0.1                 1  Vi2.1
PTA
                0008.7c55.a054  VC:  1/50                   UP
```

```
LocMAC is burned in mac-address of ATM interface(0008.7c55.a054).
```

リロード後の PPPoE セッションの回復を設定する

「半分アクティブ」な PPPoE セッション（CPE 側のみがアクティブな PPPoE セッション）で PPPoE パケットを受信した場合に CPE デバイスに PPPoE Active Discovery Terminate（PADT）パケットを送信するように集約デバイスを設定するには、この作業を実行します。

Customer Premises Equipment（CPE; 顧客宅内機器）デバイスで PPP キープアライブ メカニズムがディセーブルになっていると、集約デバイスのリロード後に PPP over Ethernet（PPPoE）セッションが無期限にハングします。リロード後の PPPoE セッションの回復機能を使用すると、集約デバイスが CPE デバイスに PPPoE セッションの失敗を通知して、リロードのために失敗した PPPoE セッションを回復しようとします。

PPPoE プロトコルは、リンクやピア デバイスの障害の検出を PPP キープアライブ メカニズムに依存しています。PPP は、障害を検出すると PPPoE セッションを終了します。CPE デバイスで PPP キープアライブ メカニズムがディセーブルになっていると、その CPE デバイスでは PPPoE 接続のリンクやピア デバイスの障害が検出されません。そのため、PPPoE セッションのエンドポイントとして機能している集約ルータがリロードしても接続障害が検出されず、集約デバイスへのトラフィックの送信が続けられます。障害が発生した PPPoE セッションのトラフィックは集約デバイスでドロップされます。

sessions auto cleanup コマンドを使用すると、リロード前に存在していた PPPoE セッションを集約デバイスが回復しようとします。集約デバイスは、半分アクティブな PPPoE セッションの PPPoE パケットを検出すると、PPPoE PADT パケットを送信して CPE に PPPoE セッションの失敗を通知します。PADT パケットを受信した CPE デバイスでは障害回復処理が開始されると想定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **sessions auto cleanup**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**bba-group pppoe** {*group-name* | **global**} **例：** `Router(config)# bba-group pppoe global`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。 • **global** キーワードは、特定のプロファイルが割り当てられていない PPPoE ポートのデフォルト プロファイルとして機能するプロファイルを作成します。
ステップ 4	**sessions auto cleanup** **例：** `Router(config-bba-group)# sessions auto cleanup`	リロードのために失敗した PPPoE セッションを回復するために CPE デバイスに PPPoE セッションの失敗を通知するように集約デバイスを設定します。
ステップ 5	**end** **例：** `Router(config-bba-group)# end`	（任意）BBA グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

PPPoE セッションのトラブルシューティングには、**show pppoe session** コマンドと **debug pppoe** コマンドを使用します。

PPPoE プロファイルのモニタおよびメンテナンスを行う

PPPoE プロファイルのモニタおよびメンテナンスを行うには、この作業を実行します。

手順の概要

1. **enable**
2. **show pppoe session** [**all** | **packets**]
3. **clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] | **rmac** *mac-addr* [**sid** *session-id*] | **all**}
4. **debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show pppoe session** [**all** | **packets**] **例：** `Router# show pppoe session all`	アクティブな PPPoE セッションに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] | **rmac** *mac-addr* [**sid** *session-id*] | **all**} **例：** `Router# clear pppoe interface atm 0/0/0.0`	PPPoE セッションを終了します。
ステップ 4	**debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}]] **例：** `Router# debug pppoe events`	PPPoE セッションのデバッグ情報を表示します。

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の設定例

ここでは、次の設定例について説明します。

- 「PPPoE プロファイルの設定：例」（P.23）
- 「PPPoEoA セッションの MAC アドレスが Burned-In MAC Address になる場合：例」（P.25）
- 「ATM インターフェイスでの MAC アドレスの設定：例」（P.27）
- 「autoselect が設定されていて MAC アドレスが設定されていない場合：例」（P.25）
- 「BBA グループでの MAC アドレスの設定：例」（P.27）
- 「ギガビット イーサネット インターフェイスでの PPPoE over 802.1Q VLAN のサポート：例」（P.26）
- 「ATM PVC での PPPoE over 802.1Q VLAN のサポート：例」（P.26）
- 「BBA グループでの MAC アドレスの設定：例」（P.27）
- 「リロード後の PPPoE セッションの回復：例」（P.28）

PPPoE プロファイルの設定：例

次の例は、vpn1、vpn2、および global の 3 つの PPPoE プロファイルの設定を示しています。プロファイル vpn1 と vpn2 は、PVC、VC クラス、VLAN、および PVC 範囲に割り当てられています。PPPoE に対して設定されているが、vpn1 も vpn も割り当てられていないギガビット イーサネット インターフェイス、VLAN、PVC、PVC 範囲、または VC クラス（VC クラス class-pppoe-global など）は、global プロファイルを使用します。

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
 sessions per-mac limit 2
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
```

```
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
 sessions per-mac limit 1 !
vc-class atm class-pppoe-global
 protocol pppoe
!
vc-class atm class-pppox-auto
 encapsulation aal5autoppp virtual-template 1 group vpn1
!
vc-class atm class-pppoe-1
 protocol pppoe group vpn1
!
vc-class atm class-pppoe-2
 protocol pppoe group vpn2
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
 !
interface ATM1/0.20 multipoint
 class-int class-pppox-auto
 pvc 0/200
  encapsulation aal5autoppp virtual-template 1
 !
 pvc 0/201
 !
 pvc 0/202
  encapsulation aal5autoppp virtual-template 1 group vpn2
 !
 pvc 0/203
  class-vc class-pppoe-global
 !
!
interface gigabitEthernet0/2/3.1
 encapsulation dot1Q 4
 pppoe enable group vpn1
!
interface gigabitEthernet0/2/3.2
 encapsulation dot1Q 2
 pppoe enable group vpn2
!
interface ATM0/6/0.101 point-to-point
 ip address 10.12.1.63 255.255.255.0
 pvc 0/101
 !
interface ATM0/6/0.102 point-to-point
 ip address 10.12.2.63 255.255.255.0
 pvc 0/102
 !
interface Virtual-Template1
 ip unnumbered loopback 1
 no logging event link-status
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
!
interface Virtual-Template2
```

```
 ip unnumbered loopback 1
no logging event link-status
 no keepalive
 peer default ip address pool pool-2
 ppp authentication chap
!
ip local pool pool-1 198.x.1.z 198.x.1.y
ip local pool pool-2 198.x.2.z 198.x.2.y
!
```

PPPoEoA セッションの MAC アドレスが Burned-In MAC Address になる場合：例

次の例では、BBA グループで autoselect も特定の MAC アドレスも設定されておらず、ATM インターフェイスでも MAC アドレスが設定されていません（デフォルトの状態）。**show pppoe session** コマンドを使用すると、PPPoEoA セッションの MAC アドレスが ATM インターフェイスの Burned-In MAC Address になっていることがわかります。

```
bba-group pppoe one
 virtual-template 1

interface ATM0/3/0.0
 no ip address
 no ip route-cache
no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one
 !

Router# show pppoe session

1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      3      3  000b.fdc9.0001  ATM0/3/0.1                 1  Vi2.1
PTA
                0008.7c55.a054  VC:  1/50                   UP


LocMAC is burned in mac-address of ATM interface(0008.7c55.a054).
```

autoselect が設定されていて MAC アドレスが設定されていない場合：例

次の例では、BBA グループで autoselect が設定されていて、ATM インターフェイスで MAC アドレスが設定されていません。**show pppoe session** コマンドを使用すると、インターフェイスの MAC アドレスに 7 を足した値が表示されます。

```
bba-group pppoe one
 virtual-template 1
 mac-address autoselect
!
```

```
interface ATM3/0
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one

Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      5      5  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0008.7c55.a05b  VC:  1/50                    UP

LocMAC = burned in mac-address of ATM interface + 7 (0008.7c55.a05b)
```

ギガビット イーサネット インターフェイスでの PPPoE over 802.1Q VLAN のサポート：例

次の例は、ギガビット イーサネット インターフェイス上の 802.1Q VLAN 範囲で PPPoE を設定する方法を示しています。この VLAN 範囲はメイン インターフェイスで設定されているため、各 VLAN が個別のサブインターフェイスを占有することはありません。

```
bba-group pppoe PPPOE
 virtual-template 1
 sessions per-mac limit 1

interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492

interface gigabitethernet 0/0/0.0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
  pppoe enable group PPPOE
  exit-vlan-config
```

ATM PVC での PPPoE over 802.1Q VLAN のサポート：例

次の例は、802.1Q VLAN 範囲で PPPoE をサポートするように ATM PVC を設定する方法を示しています。

```
bba-group pppoe PPPOEOA
 virtual-template 1
 sessions per-mac limit 1

interface virtual-template 1
```

```
 ip address 10.10.10.10 255.255.255.0
 mtu 1492

interface atm 0/4/0.10 multipoint
 pvc 10/100
  protocol pppovlan dot1q range 10 30 group PPPOEOA
```

ATM インターフェイスでの MAC アドレスの設定：例

次の例では、BBA グループでは autoselect も特定の MAC アドレスも設定されていませんが、ATM インターフェイスで MAC アドレスが設定されています。このことは、**show pppoe session** コマンドのレポートに示されています。

```
bba-group pppoe one
 virtual-template 1

interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
protocol pppoe group one
 !

Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      7      7  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0001.0001.0001  VC:  1/50                    UP


LocMAC = configured mac-address on atm interface(0001.0001.0001).
```

BBA グループでの MAC アドレスの設定：例

次の例では、BBA グループで MAC アドレスが設定されています。**show pppoe session** コマンドの出力から、この BBA グループに関連付けられている ATM インターフェイスのすべての PPPoEoA セッションで、この BBA グループで指定されているのと同じ MAC アドレスが使用されることがわかります。

```
bba-group pppoe one
 virtual-template 1
 mac-address 0002.0002.0002

interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
```

```
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one

Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      8      8  000b.fdc9.0001  ATM0/3/0.1                 1  Vi2.1
PTA
                0002.0002.0002  VC:  1/50                     UP

LocMac(Mac address of PPPoEoA session) is mac-address specified on bba-group one
(0002.0002.0002)
```

リロード後の PPPoE セッションの回復：例

次の例では、「range-pppoe-1」という ATM PVC 範囲の PVC の失敗した PPPoE セッションをルータが回復しようとします。

```
bba-group pppoe group1
 virtual-template 1
 sessions auto cleanup
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group group1
!
interface virtual-template1
 ip address negotiated
 no peer default ip address
 ppp authentication chap
```

関連情報

- Layer Two Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）アクセス コンセントレータで設定されている特定の相手先固定接続または VLAN のセッションに対して PPPoE セッションの制限を設定するには、「Establishing PPPoE Session Limits per NAS Port」を参照してください。
- service タグを使用して、コール セットアップの間に PPPoE サーバが PPPoE クライアントにサービスの選択肢を提示できるようにするには、「Offering PPPoE Clients a Selection of Services During Call Setup」を参照してください。

- L2TP アクセス コンセントレータから L2TP Network Server（LNS; L2TP ネットワーク サーバ）または L2TP トンネル スイッチに PPPoE のアクティブ ディスカバリとサービスの選択の機能を L2TP 制御チャネルでリレーできるようにするには、「Enabling PPPoE Relay Discovery and Service Selection Functionality」を参照してください。
- PPPoX セッションの転送アップストリーム速度の値を設定するには、「Configuring Upstream Connections Speed Transfer」を参照してください。
- SNMP を使用して PPPoE セッションをモニタするには、「Monitoring PPPoE Sessions with SNMP」を参照してください。
- RADIUS サーバとの RADIUS 通信の物理的な加入者線を指定するには、「Identifying a Physical Subscriber Line for RADIUS Access and Accounting」を参照してください。
- Cisco Subscriber Service Switch を設定するには、「Configuring Cisco Subscriber Service Switch Policies」を参照してください。

その他の関連資料

ここでは、PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供に関する参考資料を紹介します。

関連マニュアル

内容	参照先
Cisco IOS コマンド	*『Cisco IOS Master Commands List』、すべてのリリース*
ブロードバンドと DSL のコマンド	*『Cisco IOS Broadband Access Aggregation and DSL Command Reference』*
ブロードバンド アクセス集約の概念	*『Understanding Broadband Access Aggregation』*
ブロードバンド アクセス集約の準備作業	*『Preparing for Broadband Access Aggregation』*モジュール
Layer Two Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）アクセス コンセントレータで設定されている特定の相手先固定接続または VLAN のセッションに対して PPPoE セッションの制限を設定する	*『Establishing PPPoE Session Limits per NAS Port』*
service タグを使用して、コール セットアップの間に PPPoE サーバが PPPoE クライアントにサービスの選択肢を提示できるようにする	*『Offering PPPoE Clients a Selection of Services During Call Setup』*
L2TP アクセス コンセントレータから L2TP Network Server（LNS; L2TP ネットワーク サーバ）または L2TP トンネル スイッチに PPPoE のアクティブ ディスカバリとサービスの選択の機能を L2TP 制御チャネルでリレーできるようにする	*『Enabling PPPoE Relay Discovery and Service Selection Functionality』*
PPPoX セッションの転送アップストリーム速度の値を設定する	*『Configuring Upstream Connections Speed Transfer』*
SNMP を使用して PPPoE セッションをモニタする	*『Monitoring PPPoE Sessions with SNMP』*
RADIUS サーバとの RADIUS 通信の物理的な加入者線を指定する	*『Identifying a Physical Subscriber Line for RADIUS Access and Accounting』*
Cisco Subscriber Service Switch を設定する	*『Configuring ISG Policies for Automatic Subscriber Logon』*

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1483	『*Multiprotocol Encapsulation over ATM Adaptation Layer 5*』
RFC 2516	『*A Method for Transmitting PPP over Ethernet (PPPoE)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の機能情報

表 2 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 2　PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供の機能情報

機能名	リリース	機能情報
PPPoE 接続スロットリング	Cisco IOS XE Release 2.1	PPPoE 接続スロットリング機能を使用すると、PPPoE 接続要求を制限して、意図的なサービス拒否攻撃や意図的でない PPP 認証ループを防止することができます。この機能は、PPPoE サーバにセッション スロットリングを実装して、指定した期間に 1 つの MAC アドレスまたは仮想回線から開始できる PPPoE セッション要求の数を制限します。 この機能に関する詳細については、次の各項を参照してください。 • 「PPPoE 接続スロットリング」（P.4） • 「PPPoE プロファイルを定義する」（P.6）
PPPoE サーバの再構成と PPPoE プロファイル	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズの集約サービス ルータで導入されました。

PPPoE—QinQ サポート

サブインターフェイス レベルでインストールされた PPPoE—QinQ サポート機能は VLAN ID をそのまま維持し、他のお客様の VLAN のトラフィックと区別します。IEEE 802.1Q VLAN タグを 802.1Q 内にカプセル化すると、サービス プロバイダーは、1 つの VLAN を使用して、複数の VLAN を持つお客様をサポートできます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPPoE—QinQ サポートの機能情報」（P.15）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE—QinQ サポートの前提条件」（P.2）
- 「PPPoE—QinQ サポートに関する情報」（P.2）
- 「PPPoE—QinQ サポートの設定方法」（P.5）
- 「PPPoE—QinQ サポートの設定例」（P.10）
- 「その他の関連資料」（P.12）
- 「PPPoE—QinQ サポートの機能情報」（P.15）

PPPoE—QinQ サポートの前提条件

- Cisco Feature Navigator（http://www.cisco.com/go/cfn）で、使用しているシスコ デバイスおよび Cisco IOS XE リリースがこの機能をサポートしていることを確認しておく必要があります。
- 二重 VLAN タグのインポジションとディスポジションやスイッチングをサポートするイーサネット デバイスに接続している必要があります。

PPPoE—QinQ サポートに関する情報

PPPoE—QinQ サポート機能を設定するには、次の概念を理解しておく必要があります。

- 「サブインターフェイスでの PPPoE—QinQ サポート」（P.2）
- 「QinQ VLAN のイーサネットベースのブロードバンド DSLAM モデル」（P.4）
- 「一義的なサブインターフェイスとあいまいなサブインターフェイス」（P.5）

サブインターフェイスでの PPPoE—QinQ サポート

PPPoE—QinQ サポート機能は、IEEE 802.1Q タグ（「メトロ タグ」または「PE-VLAN」と呼ばれる）のレイヤを、ネットワークに侵入する 802.1Q タグ付きパケットにもう 1 つ追加します。タグ付きパケットにタグ付けすることで「二重タグ付き」フレームを形成し、VLAN スペースを拡張することを目的としています。拡張された VLAN スペースにより、サービス プロバイダーは、VLAN ごとに異なるサービスを提供できます。たとえば、特定のお客様に特定の VLAN 上のインターネット アクセスを提供し、他のお客様に別の VLAN 上の他のサービスを提供することができます。

通常、サービス プロバイダーのお客様は、複数のアプリケーションを処理するために VLAN の範囲を必要とします。サービス プロバイダーは、サブインターフェイスでお客様独自の VLAN ID を安全に割り当てる方法として、この機能の使用をお客様に許可することができます。これは、それらのサブインターフェイスの VLAN ID が、サービス プロバイダーが指定するそのお客様用の VLAN ID 内にカプセル化されるからです。そのため、お客様間で VLAN ID が重複することはなく、別のお客様のトラフィックが混合することもありません。二重タグ付きフレームは、拡張 **encapsulation dot1q** コマンドを使用してサブインターフェイスで「終端」または割り当てられます。このコマンドでは、サブインターフェイスで終端される 2 つの VLAN ID タグ（外部 VLAN ID と内部 VLAN ID）を指定します。図 1（P.3）を参照してください。

PPPoE—QinQ サポート機能は、通常、Cisco IOS XE の機能またはプロトコルがサブインターフェイスでサポートされているのであれば、これらに対してサポートされます。たとえば、サブインターフェイスで PPPoE を実行できる場合は、PPPoE に対して二重タグ付きフレームを設定できます。IPoQinQ は、二重タグ付け（スタックとも呼ばれます）された 802.1Q ヘッダーを持つ IP トラフィックを転送することで、QinQ VLAN タグ終端のために二重タグ付けされた IP パケットをサポートします。

特に注意が必要な箇所は、内部 VLAN ID にあいまいなサブインターフェイスと一義的なサブインターフェイスのどちらを割り当てるかについてです。「一義的なサブインターフェイスとあいまいなサブインターフェイス」（P.5）を参照してください。

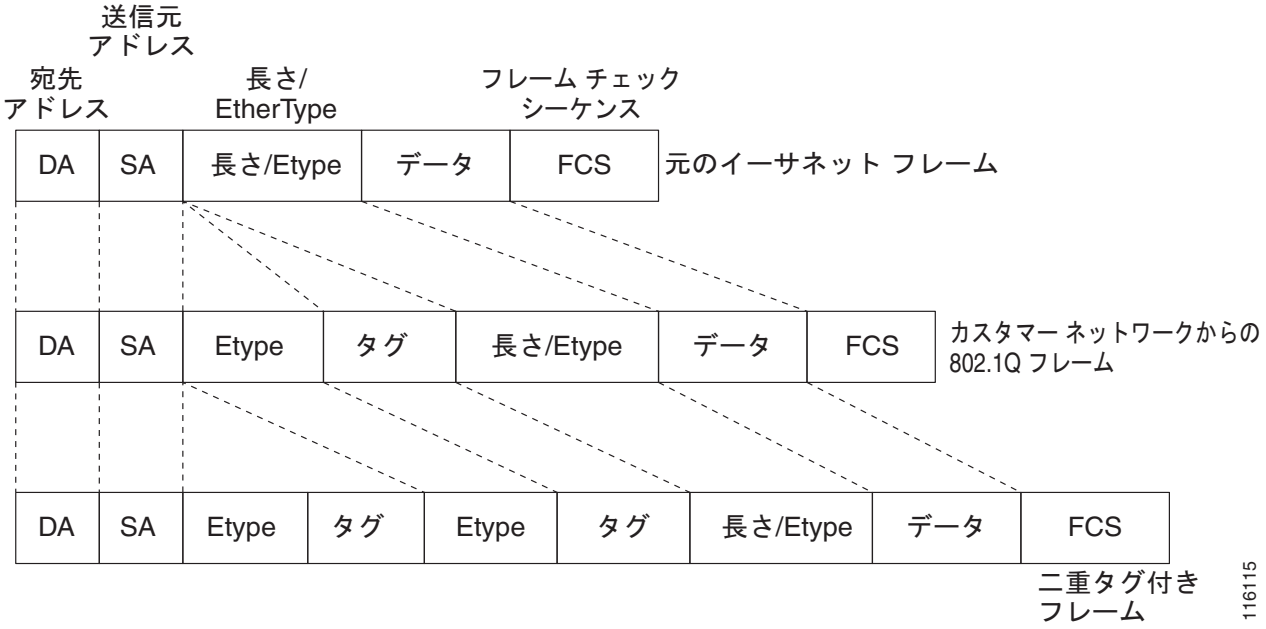
サービス プロバイダーにとっての最大の利点は、同数のお客様で比べた場合に、サポートする VLAN の数が少なくてすむことです。この機能には、次のような利点もあります。

- PPPoE のスケーラビリティ。使用可能な VLAN スペースが 4096 から約 1680 万（4096X4096）に拡張されるため、特定のインターフェイスで終端できる PPPoE セッションの数が増加します。

- ホールセール モデルでギガビット イーサネットの DSL Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）を展開する場合、内部 VLAN ID を割り当ててエンドカスタマーの Virtual Circuit（VC; 仮想回線）を表し、外部 VLAN ID を割り当ててサービス プロバイダー ID を表すことができます。

QinQ VLAN タグ終端機能は、スイッチ用に展開される IEEE 802.1Q トンネリング機能よりも簡単です。スイッチでは、インターフェイスの IEEE 802.1Q トンネルを使用して二重タグ付きトラフィックを伝送する必要がありますが、ルータでは、QinQ VLAN タグをもう 1 つのレベルの 802.1Q タグ内にカプセル化するだけで、正しい送信先にパケットを到達させることができます。

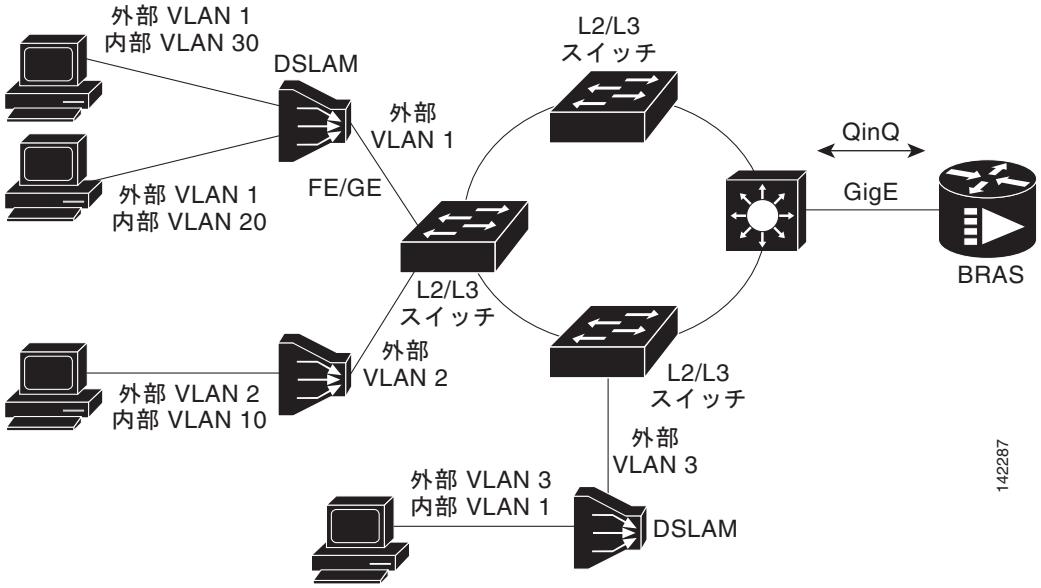
図 1　タグなし、802.1Q タグ付き、および二重タグ付きのイーサネット フレーム



QinQ VLAN のイーサネットベースのブロードバンド DSLAM モデル

イーサネットベースのブロードバンド DSLAM の新興市場向けに、Cisco ASR 1000 シリーズ ルータは QinQ カプセル化をサポートしています。お客様は通常、図 2 に示すイーサネットベースの DSLAM モデルで独自の VLAN を取得します。それらの VLAN はすべて DSLAM に集約されます。

図 2　　QinQ VLAN のイーサネットベースのブロードバンド DSLAM モデル



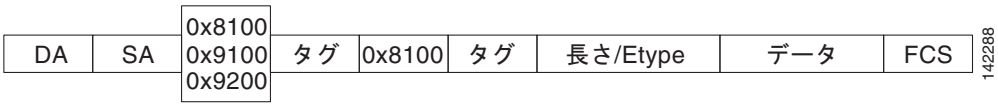
VLAN を DSLAM に集約すると、ある時点で Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）で終端する必要がある複数の集約 VLAN になります。このモデルでは DSLAM を BRAS に直接接続することができますが、より一般的なモデルでは既存のイーサネット スイッチド ネットワークが使用され、イーサネット スイッチド ネットワークに接続するときに DSLAM の各 VLAN ID に 2 番目のタグ（QinQ）が付けられます。

1 つのサブインターフェイスで PPPoE セッションと IP の両方をイネーブルにできます。PPPoEoQinQ モデルは、PPP-terminated セッションです。

PPPoEQinQ および IPoQinQ のカプセル化処理は、802.1Q カプセル化処理を拡張したものです。QinQ フレームは、802.1Q タグが 1 つではなく 2 つあることを除けば、VLAN 802.1Q フレームと同じです。図 1 を参照してください。

QinQ カプセル化は、設定可能な外部タグ Ethertype をサポートします。Ethertype フィールドに設定できる値は、0x8100（デフォルト）、0x9100、0x9200、および 0x8848 です。図 3 を参照してください。

図 3　　Ethertype フィールドに設定可能なサポートされる値



一義的なサブインターフェイスとあいまいなサブインターフェイス

（注） あいまいなサブインターフェイスでは PPPoE だけがサポートされます。標準の IP ルーティングは、あいまいなサブインターフェイスではサポートされません。

サブインターフェイスで QinQ 終端を設定するには、**encapsulation dot1q** コマンドを使用します。このコマンドに対応しているのは、1 つの外部 VLAN ID と 1 つ以上の内部 VLAN ID です。外部 VLAN ID には常に特定の値を指定しますが、内部 VLAN ID には特定の値または値の範囲のいずれかを指定できます。

内部 VLAN ID が 1 つだけ設定されたサブインターフェイスのことを *一義的な QinQ サブインターフェイス*と呼びます。次の例では、外部 VLAN ID が 101 で内部 VLAN ID が 1001 の QinQ トラフィックが、ギガビット イーサネット 1/1/0.100 サブインターフェイスにマッピングされます。

```
Router(config)# interface gigabitethernet1/1/0.100
Router(config-subif)# encapsulation dot1q 101 second-dot1q 1001
```

内部 VLAN ID が複数設定されたサブインターフェイスのことを*あいまいな QinQ サブインターフェイス*と呼びます。あいまいな QinQ サブインターフェイスでは複数の内部 VLAN ID をグループ化できるため、設定が少なくてすみ、メモリの使用が改善され、スケーラビリティも向上します。

次の例では、外部 VLAN ID が 101 で内部 VLAN ID が 2001 ～ 2100 および 3001 ～ 3100 の範囲の QinQ トラフィックが、ギガビット イーサネット 1/1/0.101 サブインターフェイスにマッピングされます。

```
Router(config)# interface gigabitethernet1/1/0.101
Router(config-subif)# encapsulation dot1q 101 second-dot1q 2001-2100,3001-3100
```

あいまいなサブインターフェイスでは、**any** キーワードを使用して内部 VLAN ID を指定することもできます。

VLAN ID をサブインターフェイスに割り当てる方法の例、およびあいまいなインターフェイスで **any** キーワードを使用する方法の詳細な例については、「PPPoE—QinQ サポートの設定例」（P.10）を参照してください。

（注） IPoQinQ に対して設定されているサブインターフェイスでは、**second-dot1q** キーワードでの **any** の使用はサポートされていません。これは、あいまいなサブインターフェイスでは IP ルーティングがサポートされないからです。したがって、IPoQinQ では、内部 VLAN ID に複数の値や範囲を指定することはサポートされません。

PPPoE—QinQ サポートの設定方法

ここでは、次の作業について説明します。

- 「PPPoE—QinQ サポートのインターフェイスの設定」（P.6）（必須）
- 「PPPoE—QinQ サポートの確認」（P.8）（任意）

PPPoE—QinQ サポートのインターフェイスの設定

QinQ 二重タギングに使用するメイン インターフェイスを設定し、サブインターフェイスを設定するには、この作業を実行します。この作業の任意の手順では、必要に応じて外部 VLAN タグの Ethertype フィールドを 0x9100 に設定する方法を示しています。サブインターフェイスを定義した後、二重タギングを使用するように 802.1Q カプセル化を設定します。

前提条件

- PPPoE または IP が事前に設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*subslot*/*port*
4. **dot1q tunneling ethertype** *ethertype*
5. **exit**
6. **interface** *type slot*/*subslot*/*port*[*.subinterface*]
7. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[**,***vlan-id*-*vlan-id*]}
8. **pppoe enable** [**group** *group-name*]
9. **ip address** *ip-address mask* [**secondary**]
10. **exit**
11. ステップ 6 を繰り返して、別のサブインターフェイスを設定します。
12. ステップ 7、ステップ 8、およびステップ 9 を必要に応じて繰り返して、サブインターフェイスで終端する VLAN タグを指定し、サブインターフェイスで PPPoE セッションまたは IP をイネーブルにします。
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/subslot/port* 例： `Router(config)# interface gigabitethernet 1/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**dot1q tunneling ethertype** *ethertype* **例：** `Router(config-if)# dot1q tunneling ethertype 0x9100`	（任意）QinQ VLAN タギングを実装するときにピア装置で使用される Ethertype フィールドのタイプを定義します。 • このコマンドを使用するのは、ピア装置の Ethertype が 0x9100 または 0x9200 である場合です。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**interface** *type slot/subslot/port*[*.subinterface*] **例：** `Router(config-if)# interface gigabitethernet 1/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[,*vlan-id*-*vlan-id*]} **例：** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	（必須）VLAN の指定されたサブインターフェイス上でトラフィックの 802.1Q カプセル化をイネーブルにします。 • **second-dot1q** キーワードと *vlan-id* 引数を使用して、サブインターフェイスで終端する VLAN タグを指定します。 • この例では、内部 VLAN ID が 1 つだけ指定されているため、一義的な QinQ サブインターフェイスが設定されます。 • 外部 VLAN ID が 100 で内部 VLAN ID が 200 の QinQ フレームが終端されます。
ステップ 8	**pppoe enable** [**group** *group-name*] **例：** `Router(config-subif)# pppoe enable group vpn1`	（任意）サブインターフェイスで PPPoE セッションをイネーブルにします。 • この例では、サブインターフェイスの PPPoE セッションで PPPoE プロファイル vpn1 を使用するように指定します。 **（注）** このステップは、PPPoEoQinQ でのみ必要になります。
ステップ 9	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-subif)# ip address 192.168.1.2 255.255.255.0`	（任意）サブインターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • この例では、IP アドレス 192.168.1.2 およびマスク 255.255.255.0 のサブインターフェイスで IP をイネーブルにします。 **（注）** このステップは、IPoQinQ でのみ必要になります。
ステップ 10	**exit** **例：** `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 11	ステップ 6 を繰り返して、他のサブインターフェイスを設定します。 **例：** `Router(config-if)# interface gigabitethernet 1/0/0.2`	（任意）サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。

ステップ 12	ステップ 7、ステップ 8、およびステップ 9 を必要に応じて繰り返して、サブインターフェイスで終端する VLAN タグを指定します。
	
	例：
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600`
	
	例：
	`Router(config-subif)# pppoe enable group vpn1`
	
	例：
	`Router(config-subif)# ip address 192.168.1.2 255.255.255.0`
		サブインターフェイスで終端する VLAN タグを指定し、サブインターフェイスで PPPoE セッションまたは IP をイネーブルにします。
		• **second-dot1q** キーワードと *vlan-id* 引数を使用して、サブインターフェイスで終端する VLAN タグを指定します。
		• この例では、内部 VLAN ID の範囲が指定されているため、あいまいな QinQ サブインターフェイスが設定されます。
		• 外部 VLAN ID が 100 で内部 VLAN ID が 100 ～ 199 または 201 ～ 600 の範囲の QinQ フレームが終端されます。
		• ステップ 7 を実行して、VLAN の指定されたサブインターフェイスでトラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
		• ステップ 8 を実行して、サブインターフェイスで PPPoE セッションをイネーブルにします。この例では、サブインターフェイスの PPPoE セッションで PPPoE プロファイル vpn1 を使用するように指定します。
		• ステップ 9 を実行して、IP アドレスとマスクで指定されたサブインターフェイスで IP をイネーブルにします。この例では、IP アドレス 192.168.1.2 およびマスク 255.255.255.0 のサブインターフェイスで IP をイネーブルにします。
		（注） 1 つのサブインターフェイスで PPPoE セッションと IP の両方をイネーブルにできます。

ステップ 13	**end** **例：** `Router(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PPPoE—QinQ サポートの確認

PPPoE—QinQ サポート機能のコンフィギュレーションを確認するには、この作業を任意で実行します。

手順の概要

1. **enable**

2. **show running-config**
3. **show vlans dot1q** [**internal** | *interface-type interface-number.subinterface-number* [**detail**] | *outer-id* [*interface-type interface-number* | **second-dot1q** [*inner-id* | **any**]] [**detail**]]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。必要に応じてパスワードを入力します。

```
Router> enable
```

ステップ 2 **show running-config**

このコマンドを使用して、デバイスで現在実行中のコンフィギュレーションを表示します。区切り文字を使用してコンフィギュレーションの関連する部分だけを表示できます。

次の出力は、現在実行中の PPPoEoQinQ および IPoQinQ のコンフィギュレーションを示しています。

```
Router# show running-config

interface GigabitEthernet0/0/0.201
 encapsulation dot1Q 201
 ip address 10.7.7.5 255.255.255.252
!
interface GigabitEthernet0/0/0.401
 encapsulation dot1Q 401
 ip address 10.7.7.13 255.255.255.252
!
interface GigabitEthernet0/0/0.201999
 encapsulation dot1Q 201 second-dot1q any
 pppoe enable
!
interface GigabitEthernet0/0/0.2012001
 encapsulation dot1Q 201 second-dot1q 2001
 ip address 10.8.8.9 255.255.255.252
!
interface GigabitEthernet0/0/0.2012002
 encapsulation dot1Q 201 second-dot1q 2002
 ip address 10.8.8.13 255.255.255.252
 pppoe enable
!
interface GigabitEthernet0/0/0.4019999
 encapsulation dot1Q 401 second-dot1q 100-900,1001-2000
 pppoe enable
!
interface GigabitEthernet1/0/0.101
 encapsulation dot1Q 101
 ip address 10.7.7.1 255.255.255.252
!
interface GigabitEthernet1/0/0.301
 encapsulation dot1Q 301
 ip address 10.7.7.9 255.255.255.252
!
interface GigabitEthernet1/0/0.301999
 encapsulation dot1Q 301 second-dot1q any
 pppoe enable
!
interface GigabitEthernet1/0/0.1011001
 encapsulation dot1Q 101 second-dot1q 1001
 ip address 10.8.8.1 255.255.255.252
!
```

```
interface GigabitEthernet1/0/0.1011002
 encapsulation dot1Q 101 second-dot1q 1002
 ip address 10.8.8.5 255.255.255.252
!
interface GigabitEthernet1/0/0.1019999
 encapsulation dot1Q 101 second-dot1q 1-1000,1003-2000
 pppoe enable
```

ステップ 3 **show vlans dot1q** [**internal** | *interface-type interface-number.subinterface-number* [**detail**] | *outer-id* [*interface-type interface-number* | **second-dot1q** [*inner-id* | **any**]] [**detail**]]

このコマンドを使用して、すべての 802.1Q VLAN ID の統計情報を表示します。次の例では、外部 VLAN ID だけが表示されます。

（注） IPoQinQ に対して設定されているサブインターフェイスでは、**any** キーワードはサポートされていません。これは、あいまいなサブインターフェイス上では IP ルーティングはサポートされていないからです。

```
Router# show vlans dot1q

Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

PPPoE—QinQ サポートの設定例

ここでは、次の例について説明します。

- 「PPPoE—QinQ サポートのサブインターフェイスでの any キーワードの設定：例」（P.10）

PPPoE—QinQ サポートのサブインターフェイスでの any キーワードの設定：例

一部のあいまいなサブインターフェイスでは、内部 VLAN ID の指定に **any** キーワードを使用できます。**any** は、他のインターフェイスで明示的に設定されていない任意の内部 VLAN ID を表します。次の例では、外部 VLAN ID と内部 VLAN ID の組み合わせがそれぞれ異なるサブインターフェイスを 7 つ設定します。

（注） **any** キーワードは、物理インターフェイスと外部 VLAN ID が指定された 1 つのサブインターフェイスに対してのみ設定できます。

（注） IPoQinQ に対して設定されているサブインターフェイスでは、**second-dot1q** キーワードでの **any** の使用はサポートされていません。これは、あいまいなサブインターフェイスでは IP ルーティングがサポートされないからです。したがって、IPoQinQ では、内部 VLAN ID に複数の値や範囲を指定することはサポートされません。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100

interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200

interface GigabitEthernet1/0/0.3
 encapsulation dot1q 100 second-dot1q 300-400,500-600

interface GigabitEthernet1/0/0.4
 encapsulation dot1q 100 second-dot1q any

interface GigabitEthernet1/0/0.5
 encapsulation dot1q 200 second-dot1q 50

interface GigabitEthernet1/0/0.6
 encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000

interface GigabitEthernet1/0/0.7
 encapsulation dot1q 200 second-dot1q any
```

表 1 に、ギガビット イーサネット（GE; ギガビット イーサネット）インターフェイス 1/0/0 に入ってくる QinQ フレームに、外部 VLAN ID と内部 VLAN ID の値に応じてどのサブインターフェイスがマッピングされるかを示します。

表 1　GE インターフェイス 1/0/0 の外部 VLAN ID および内部 VLAN ID にマッピングされるサブインターフェイス

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
100	1 ～ 99	GigabitEthernet1/0/0.4
100	100	GigabitEthernet1/0/0.1
100	101 ～ 199	GigabitEthernet1/0/0.4
100	200	GigabitEthernet1/0/0.2
100	201 ～ 299	GigabitEthernet1/0/0.4
100	300 ～ 400	GigabitEthernet1/0/0.3
100	401 ～ 499	GigabitEthernet1/0/0.4
100	500 ～ 600	GigabitEthernet1/0/0.3
100	601 ～ 4094	GigabitEthernet1/0/0.4
200	1 ～ 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 ～ 999	GigabitEthernet1/0/0.7

表 1　GE インターフェイス 1/0/0 の外部 VLAN ID および内部 VLAN ID にマッピングされるサブインターフェイス（続き）

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
200	1000 ～ 2000	GigabitEthernet1/0/0.6
200	2001 ～ 2999	GigabitEthernet1/0/0.7
200	3000 ～ 4000	GigabitEthernet1/0/0.6
200	4001 ～ 4094	GigabitEthernet1/0/0.7

ここで、次の新しいサブインターフェイスを設定します。

```
interface GigabitEthernet 1/0/0.8
 encapsulation dot1q 200 second-dot1q 200-600,900-999
```

表 2 に、前の表からの変更箇所として外部 VLAN ID が 200 のマッピングを示します。**any** キーワードを使用して設定されたサブインターフェイス 1/0/0.7 の内部 VLAN ID のマッピングが変わっていることに注意してください。

表 2　GE インターフェイス 1/0/0 の外部 VLAN ID および内部 VLAN ID へのサブインターフェイスのマッピング：GE サブインターフェイス 1/0/0.8 を設定したことによる変更点

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
200	1 ～ 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 ～ 199	GigabitEthernet1/0/0.7
200	200 ～ 600	GigabitEthernet1/0/0.8
200	601 ～ 899	GigabitEthernet1/0/0.7
200	900 ～ 999	GigabitEthernet1/0/0.8
200	1000 ～ 2000	GigabitEthernet1/0/0.6
200	2001 ～ 2999	GigabitEthernet1/0/0.7
200	3000 ～ 4000	GigabitEthernet1/0/0.6
200	4001 ～ 4094	GigabitEthernet1/0/0.7

その他の関連資料

ここでは、PPPoE—QinQ サポート機能に関する参考資料を紹介します。

関連マニュアル

内容	参照先
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
IEEE 802.1Q	*IEEE Standard for Local and Metropolitan Area Networks*

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PPPoE—QinQ サポートの機能情報

表 3 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 3　PPPoE—QinQ サポートの機能情報

機能名	リリース	機能情報
IEEE 802.1Q-in-Q VLAN タグ終端	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 IEEE 802.1Q VLAN タグを 802.1Q 内にカプセル化すると、サービス プロバイダーは、1 つの VLAN を使用して、複数の VLAN を持つお客様をサポートできます。この機能については、次の項に説明があります。 • 「サブインターフェイスでの PPPoE—QinQ サポート」（P.2）
PPPoE—QinQ サポート	Cisco IOS XE Release 2.2	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 サブインターフェイス レベルのこの機能は VLAN ID をそのまま維持し、他のお客様の VLAN のトラフィックと区別します。この機能については、次の項に説明があります。 • 「PPPoE—QinQ サポートの設定方法」（P.5） 次のコマンドが導入または変更されました。**dot1q tunneling ethertype**、**encapsulation dot1q**、**show vlans dot1q**

PPP-Max-Payload および IWF PPPoE タグ サポート

PPP-Max-Payload および IWF PPPoE タグ サポート機能では、PPPoE ディスカバリ フレーム内の PPP-Max-Payload および Interworking Functionality（IWF; インターワーキング機能）PPPoE タグを PPP over Ethernet（PPPoE）コンポーネントで処理できます。

- **tag ppp-max-payload** コマンドを使用すると、基礎になるネットワークで 1500 オクテットより大きい Maximum Transmission Unit（MTU; 最大伝送ユニット）がサポートされる場合に、PPPoE ピアが 1492 オクテットより大きい PPP Maximum Receive Unit（MRU; 最大受信ユニット）をネゴシエーションできるようになります。
- IWF PPPoE タグを使用すると、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）が IWF PPPoE と通常の PPPoE セッションを区別できるようになります。これにより、同じ MAC アドレスからの Denial-of-Service（DoS; サービス拒絶）攻撃から保護するために BRAS に課されている MAC ごとのセッション制限を克服することができます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPP-Max-Payload および IWF PPPoE タグ サポートの機能情報」（P.9）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPP-Max-Payload および IWF PPPoE タグ サポートに関する情報」（P.2）
- 「PPP-Max-Payload および IWF PPPoE タグ サポートの設定方法」（P.3）
- 「PPP-Max-Payload および IWF PPPoE タグ サポートの設定例」（P.6）
- 「その他の関連資料」（P.7）

- 「PPP-Max-Payload および IWF PPPoE タグ サポートの機能情報」（P.9）

PPP-Max-Payload および IWF PPPoE タグ サポートに関する情報

この機能を実装するには、次の概念を理解しておく必要があります。

- 「PPoE での 1492 より大きい MTU/MRU への対応」
- 「インターワーキング機能」

PPoE での 1492 より大きい MTU/MRU への対応

RFC の「Accommodating an MTU/MRU Greater than 1492 in PPPoE」によると、PPPoE ピアがネゴシエーションできるのは 1492 オクテット以下の MRU だけです。これは、PPPoE セッション データパケットに PPPoE ヘッダーと PPP プロトコル ID を挿入する必要があるからです。イーサネット ペイロードの最大値は 1500 オクテットです。

RFC 2516 では、基礎になるネットワークで 1500 バイトより大きいイーサネット ペイロードがサポートされる場合に、PPPoE ピアが 1492 より大きい PPP MRU をネゴシエーションできるようにするための新しいタグが定義されています。この新しいタグを処理できるように、Cisco IOS コマンドライン インターフェイスに **tag ppp-max-payload** というコマンドが定義されました。PPP-Max-Payload および IWF PPPoE タグ サポート機能では、**tag ppp-max-payload** コマンドで新しいタグを処理し、PPPoE クライアントからのタグで指定された MRU 値に基づいて PPP セッションの Link Control Protocol（LCP; リンク制御プロトコル）MRU ネゴシエーションを変化させることができるように、PPPoE コンポーネントが拡張されます。

インターワーキング機能

DSL Forum では、BRAS への Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）で PPP over ATM（PPPoA）セッションを PPPoE セッションに変換するプロセスを定義するために、IWF が定義されました。この機能は、DSLAM ネットワークを ATM からイーサネット メディアに移行できるようにするために定義されたものです。そのため、基本的には、PPPoA セッションは ATM 経由で DSLAM に入り、DSLAM で PPPoE セッションに変換され、その後、PPPoE セッションとして BRAS に接続されます。各 PPPoA セッションは、対応する PPPoE セッションにマッピングされます。

通常、BRAS は、DoS 攻撃から自身を保護するために、同じ MAC アドレスから始まる PPPoE セッションを制限するように設定されます。これにより、IWF PPPoE セッションに問題が生じます。PPPoE セッションはすべて、同じ MAC アドレスの DSLAM から始まるからです。この問題を克服するために、IWF PPPoE タグが DSLAM に挿入されます。この IWF PPPoE タグは、PPPoE ディスカバリ フレームの受信時に BRAS によって読み取られ、IWF PPPoE セッションと通常の PPPoE セッションを区別するために使用されます。

この問題の詳細については、DSL Forum Technical Report 101「Migration to Ethernet-Based DSL Aggregation」を参照してください。

PPP-Max-Payload および IWF PPPoE タグ サポートの設定方法

ここでは、次の作業について説明します。

- 「PPP-Max-Payload および IWF PPPoE タグ サポートのイネーブル化」
- 「PPP-Max-Payload および IWF PPPoE タグ サポートのディセーブル化」

PPP-Max-Payload および IWF PPPoE タグ サポートのイネーブル化

PPP-Max-Payload および IWF PPPoE タグ サポート機能をイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-name*
5. **tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**]
6. **sessions per-mac iwf limit** *per-mac-limit*
7. **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot*/*subslot*/*port*[.*subinterface*]
8. **pppoe enable** [**group** *group-name*]
9. **virtual-template** *template-number*
10. **ppp lcp echo mru verify** [**minimum** *value*]
11. **end**
12. **show pppoe session** [**all** | **packets**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**bba-group pppoe** {*group-name* | **global**} **例：** `Router(config)# bba-group pppoe pppoe-group`	BBA グループ コンフィギュレーション モードを開始し、PPPoE プロファイルを定義します。
ステップ 4	**virtual-template** *template-number* **例：** `Router(config-bba-group)# virtual-template 1`	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートで PPPoE プロファイルを設定します。 • *template-number* 引数は、仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートの識別番号です。
ステップ 5	**tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**] **例：** `Router(config-bba-group)# tag ppp-max-payload minimum 1200 maximum 3000`	BRAS によって受け入れられる ppp-max payload タグ値の範囲を指定します。 • デフォルトの最小値は 1492 で、最大値は 1500 です。 • クライアントから受け入れられる ppp-max-payload タグ値は、MTU の物理インターフェイス値から 8 を引いた値を超えることはできません。
ステップ 6	**sessions per-mac iwf limit** *per-mac-limit* **例：** `Router(config-bba-group)# sessions per-mac iwf limit 200`	MAC アドレスごとの IWF-specific セッションの制限を（IWF-specific でないセッションの制限とは別に）指定します。 • このコマンドを入力しない場合は、通常の MAC アドレス セッション制限が IWF セッションに適用されます。 • *per-mac-limit* 引数には、許容できる IWF セッション数を指定します。デフォルト値は 100 です。
ステップ 7	**interface fastethernet gigabitethernet tengigabitethernet** *slot*/*subslot port*[*subinterface*] **例：** `Router(config-bba-group)# interface gigabitethernet 0/0/0`	ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**pppoe enable** [**group** *group-name*] **例：** `Router(config-if)# pppoe enable group 1`	イーサネット インターフェイスまたはサブインターフェイスで PPPoE セッションをイネーブルにします。
ステップ 9	**virtual-template** *template-number* **例：** `Router(config-if)# virtual-template 1`	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートで PPPoE プロファイルを設定します。 • *template-number* 引数は、仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートの識別番号です。

	コマンドまたはアクション	目的
ステップ 10	**ppp lcp echo mru verify** [**minimum** *value*] **例：** `Router(config-if)# ppp lcp echo mru verify minimum 1304`	トラブルシューティングのために、ネゴシエーションされた MRU を検証し、PPP 仮想アクセス インターフェイス MTU を調整します。 • 任意の **minimum** キーワードを入力する場合、*value* には 64 ～ 1500 の値を指定できます。 • 最小 MTU の検証が成功した場合、PPP 接続のインターフェイス MTU はその値に設定されます。このリセットは、トラブルシューティング時に、基礎になる物理ネットワークの機能に応じてセッションを調整する必要が生じた場合に役立ちます。このコマンドを設定すると、MTU が LCP で完了するまで IP Control Protocol（IPCP; IP 制御プロトコル）が遅延されます。
ステップ 11	**end** **例：** `Router(config-if)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show pppoe session** [**all** | **packets**] **例：** `Router# show pppoe session all`	設定を確認し、セッション情報を表示します。 • **all**：セッションが IWF-specific かどうか、または PPP-Max-Payload タグがディスカバリ フレームに含まれていて受け入れられるかどうかを示す出力を表示します。 • **packets**：PPPoE セッションのパケット統計情報を表示します。

PPP-Max-Payload および IWF PPPoE タグ サポートのディセーブル化

tag ppp-max-payload コマンドは、PPPoE セッションの PPP MTU を、デフォルトの最大制限である 1492 バイトより大きい値に調整します。ただし、1492 より大きい MTU 値がサポートされるのは、基礎となるイーサネット ネットワークでこのような大きなフレームがサポートされる場合だけです。すべてのイーサネット ネットワークで大きな値がサポートされるわけではありません。デフォルトの最大値より大きい値がネットワークでサポートされない場合は、この作業を実行して、PPP-Max-Payload および IWF PPPoE タグ サポート機能をディセーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **tag ppp-max-payload deny**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** {*group-name* | **global**} **例：** `Router(config-if)# bba-group pppoe pppoe-group`	BBA グループ コンフィギュレーション モードを開始し、PPPoE プロファイルを定義します。
ステップ 4	**tag ppp-max-payload deny** **例：** `Router(config-bba-group)# tag ppp-max-payload deny`	デフォルトの 1492 バイトより大きい ppp-max-payload タグ値の処理をディセーブルにします。

PPP-Max-Payload および IWF PPPoE タグ サポートの設定例

ここでは、PPP-Max-Payload および IWF PPPoE タグ サポート機能がイネーブルになっている設定例と、この機能の効果がディセーブルになっている設定について説明します。

- 「PPP-Max-Payload および IWF PPPoE タグ サポートがイネーブル：例」（P.6）
- 「PPP-Max-Payload および IWF PPPoE タグ サポートがディセーブル：例」（P.7）

PPP-Max-Payload および IWF PPPoE タグ サポートがイネーブル：例

次に、PPP-Max-Payload および IWF PPPoE タグ サポートがイネーブルになっている設定例を示します。この例では、1492 ～ 1892 の PPP-Max-Payload タグ値を受け入れ、IWF が存在する場合には MAC アドレスごとのセッション数を 2000 に制限し、PPP セッションが 1500 バイトのパケットを双方向で受け入れることができることを確認します。

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload minimum 1492 maximum 1892
 sessions per-mac limit 1
 sessions per-mac iwf limit 2000
 ppp lcp echo mru verify
!
 interface Virtual-Template 1
!
```

PPP-Max-Payload および IWF PPPoE タグ サポートがディセーブル : 例

次に、**tag ppp-max-payload** コマンドの効果をディセーブルにする設定例を示します。

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload deny
```

その他の関連資料

ここでは、PPP-Max-Payload および IWF PPPoE タグ サポート機能に関する参考資料を紹介します。

関連マニュアル

内容	参照先
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
DSL Forum Technical Report 101	「*Migration to Ethernet-Based DSL Aggregation*」

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	『*A Method for Transmitting PPP Over Ethernet (PPPoE)*』
ドラフト RFC ドキュメント	『*Accommodating an MTU/MRU Greater than 1492 in PPPoE*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PPP-Max-Payload および IWF PPPoE タグ サポートの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　PPP-Max-Payload および IWF PPPoE タグ サポートの機能情報

機能名	リリース	機能情報
PPP-Max Payload および IWF PPPoE タグ サポート	Cisco IOS XE Release 2.3	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能では、PPPoE ディスカバリ フレーム内の PPP-Max-Payload および Interworking Functionality（IWF; インターワーキング機能）PPPoE タグを PPP over Ethernet（PPPoE）コンポーネントで処理できます。 次のコマンドが導入または変更されました。**ppp lcp echo mru verify**、**sessions per-mac iwf limit**、**show pppoe session**、**tag ppp-max-payload**

内部 QinQ VLAN での PPPoE セッション制限

内部 QinQ VLAN での PPPoE セッション制限機能を使用すると、サービス プロバイダーは、サブインターフェイスで設定されている内部 VLAN ID に基づいて PPPoE over QinQ（IEEE 802.1Q VLAN トンネル）セッションの数を制限できるようにすることで、それぞれのお客様が使用する PPP over Ethernet（PPPoE）クライアントを 1 つに制限できます。この機能により、多数のサブインターフェイスを設定する必要がなくなります。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「内部 QinQ VLAN での PPPoE セッション制限の機能情報」（P.7）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「内部 QinQ VLAN での PPPoE セッション制限の前提条件」（P.2）
- 「内部 QinQ VLAN での PPPoE セッション制限に関する制約事項」（P.2）
- 「内部 QinQ VLAN での PPPoE セッション制限について」（P.2）
- 「内部 QinQ VLAN での PPPoE セッション制限の設定方法」（P.3）
- 「内部 QinQ VLAN での PPPoE セッション制限の設定例」（P.4）
- 「その他の関連資料」（P.5）
- 「内部 QinQ VLAN での PPPoE セッション制限の機能情報」（P.7）

内部 QinQ VLAN での PPPoE セッション制限の前提条件

- PPPoE サーバの機能を設定する必要があります。
- PPPoE over IEEE 802.1Q VLAN 機能を設定する必要があります。

内部 QinQ VLAN での PPPoE セッション制限に関する制約事項

- 内部 VLAN セッション制限を外部セッション制限より大きい値に設定しないでください。

内部 QinQ VLAN での PPPoE セッション制限について

内部 QinQ VLAN での PPPoE セッション制限機能を設定するには、次の概念を理解しておく必要があります。

- 「内部 QinQ VLAN での PPPoE セッション制限の利点」（P.2）
- 「内部 QinQ VLAN での PPPoE セッション制限の機能設計」（P.2）

内部 QinQ VLAN での PPPoE セッション制限の利点

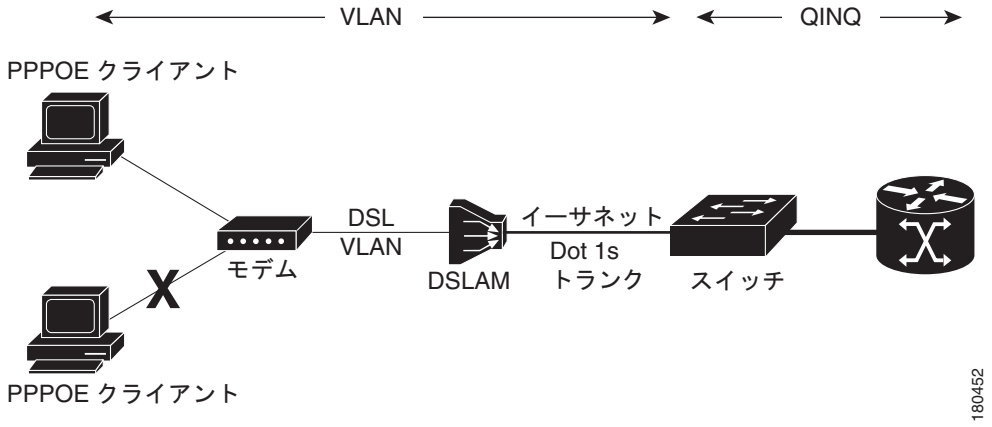
- 管理がより単純で簡単な設定を使用することで、固有の内部 VLAN を使用する何千もの PPPoE over QinQ セッションのプロビジョニングが容易になります。
- サービス プロバイダーは、QinQ 内部 VLAN ID に基づいて PPPoE セッションを制限できます。

内部 QinQ VLAN での PPPoE セッション制限の機能設計

内部 QinQ VLAN での PPPoE セッション制限機能が提供される前は、PPPoE セッションを制限するには、セッションを制限する各 QinQ 内部 VLAN に対して QinQ サブインターフェイスを設定する必要があり、設定要件は多数の QinQ VLAN ID ペアには対応しませんでした。内部 QinQ VLAN での PPPoE セッション制限 機能では、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）機能が追加され、外部 VLAN の単位ですべての固有の内部 VLAN に対して 1 つのサブインターフェイスを設定しながら、セッションを内部 VLAN ごとに 1 つに制限できます。

図 1 に、内部 QinQ VLAN での PPPoE セッション制限機能の一般的な実装を示します。

図 1　PPPoE over QinQ のセッション制限



内部 QinQ VLAN での PPPoE セッション制限の設定方法

ここでは、次の手順について説明します。

- 「内部 QinQ VLAN での PPPoE セッション制限の設定」（P.3）

内部 QinQ VLAN での PPPoE セッション制限の設定

PPPoE over QinQ セッション制限を設定し、それぞれのお客様の QinQ 内部 VLAN 接続の数を制限できるようにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **sessions per-vlan limit** *outer-per-vlan-limit* **inner** *inner-per-vlan-limit*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**bba-group pppoe** *group-name* **例：** `Router(config)# bba-group pppoe group 1`	PPPoE プロファイルを作成し、bba-group コンフィギュレーション モードを開始します。
ステップ 4	**sessions per-vlan limit** *outer-per-vlan-limit* **inner** *inner-per-vlan-limit* **例：** `Router(config-bba-group)# sessions per-vlan-limit 400 inner 1`	内部 VLAN 制限および外部 VLAN 制限を設定します。
ステップ 5	**end** **例：** `Router(config-bba-group)# end`	（任意）現在のコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

トラブルシューティングのヒント

PPPoE セッション制限のトラブルシューティングには、次のコマンドが役に立ちます。

- **debug pppoe error**
- **show pppoe session**
- **show pppoe summary**

内部 QinQ VLAN での PPPoE セッション制限の設定例

ここでは、次の設定例について説明します。

- 「内部 QinQ VLAN での PPPoE セッション制限：例」（P.4）

内部 QinQ VLAN での PPPoE セッション制限：例

次の例は、外部 VLAN ID が 10 でセッションごとに 1 つの固有の内部 VLAN ID を使用するファストイーサネット インターフェイス 1/0/0.1 で PPPoE over QinQ セッション制限をイネーブルにする方法を示しています。

```
Router(config)# bba-group pppoe group1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vlan limit 1000 inner 1
Router(config)#interface eth1/0/0.1
Router(config-subif)# encapsulation dot1q 10 second-dot1q any
Router(config-subif)# enable group group1
```

その他の関連資料

ここでは、内部 QinQ VLAN での PPPoE セッション制限 機能に関する関連資料について説明します。

関連マニュアル

内容	参照先
ブロードバンド アクセス集約の概念	『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』
ブロードバンド アクセス コマンド	『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』

標準

標準	タイトル
IEEE 標準 802.1Q	「*Virtual Bridged Local Area Networks*」

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	「*PPP over Ethernet*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

内部 QinQ VLAN での PPPoE セッション制限の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　内部 QinQ VLAN での PPPoE セッション制限の機能情報

機能名	リリース	機能情報
内部 QinQ VLAN での PPPoE セッション制限	Cisco IOS XE Release 2.1	内部 QinQ VLAN での PPPoE セッション制限機能は、サブインターフェイスで設定されている内部 VLAN ID に基づいて PPPoE over QinQ（IEEE 802.1Q VLAN トンネル）セッションの数を制限できるようにします。12.2(31)SB2 では、この機能は Cisco 10000 ルータで導入されました。 この機能により次のコマンドが変更されました。**session per-vlan limit**

PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能

PPPoE リレー機能を使用すると、L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）から L2TP Network Server（LNS; L2TP ネットワーク サーバ）またはトンネル スイッチ（マルチホップ ノード）に PPP over Ethernet（PPPoE）のアクティブ ディスカバリとサービスの選択の機能を Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）制御チャネルでリレーできます。この機能のリレー機能を使用することで、LNS またはトンネル スイッチはクライアントに提供するサービスをアドバタイズでき、それによって LNS と PPPoE クライアントの間でサービスのエンドツーエンド制御を提供できます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の機能情報」（P.14）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の前提条件」（P.2）
- 「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能に関する情報」（P.2）
- 「PPPoE リレー ディスカバリおよびサービス選択機能をイネーブルにする方法」（P.2）
- 「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の設定例」（P.7）
- 「その他の関連資料」（P.13）
- 「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の機能情報」（P.14）

PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の前提条件

- 「ブロードバンド アクセス集約の準備」で説明されている概念について理解している必要があります。
- 「PPPoE セッションのブロードバンド アクセス集約に対するプロトコル サポートの提供」の手順を使用して、PPPoE セッションを確立する必要があります。
- このマニュアルでは、Virtual Private Dial-up 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）トンネルおよびトンネル スイッチの設定方法を理解していることを前提としています。これらの機能の詳細については、「関連マニュアル」（P.13）を参照してください。

PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能に関する情報

PPPoE リレーを設定するには、次の概念を理解しておく必要があります。

- 「PPPoE の L2TP アクティブ ディスカバリ リレー」（P.2）

PPPoE の L2TP アクティブ ディスカバリ リレー

RFC 2516 で説明されている PPPoE プロトコルでは、LAC によるネットワーク内のデバイスのアクティブ ディスカバリとサービスの選択のための方法が定義されています。PPPoE クライアントはこれらの方法を使用してネットワーク内のアクセス コンセントレータを検出し、アクセス コンセントレータはこれらの方法を使用して、提供するサービスをアドバタイズします。

PPPoE リレー機能を使用することで、LAC だけでなく LNS も、アクティブ ディスカバリとサービスの選択の機能を提供できます。PPPoE リレー機能は、「*L2TP Active Discovery Relay for PPPoE*」というタイトルの Network Working Group Internet-Draft を実装します。Internet-Draft では、L2TP 制御チャネル（トンネル）経由で PPPoE Active Discovery（PAD）メッセージおよび Service Relay Request（SRRQ）メッセージをリレーする方法が記述されています。Network Working Group Internet-Draft にアクセスする方法については、「RFC」（P.13）を参照してください。

PPPoE リレー機能の重要な利点は、LNS と PPPoE クライアントの間でのサービスのエンドツーエンド制御です。

PPPoE リレー ディスカバリおよびサービス選択機能をイネーブルにする方法

ここでは、次の手順について説明します。

- 「PPPoE リレーのための LAC とトンネル スイッチの設定」（P.3）（必須）
- 「リレーされた PAD メッセージに応答するための LNS（マルチホップ ノード）の設定」（P.4）（必須）
- 「その他の関連資料」（P.13）（任意）

PPPoE リレーのための LAC とトンネル スイッチの設定

PPPoE リレー用に LAC およびトンネル スイッチを設定するには、この作業を実行します。この作業では、リレーされる PAD メッセージを L2TP トンネルに送信する加入者プロファイルを設定します。加入者プロファイルには、発信 L2TP トンネルの認証キーも含まれます。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service relay pppoe vpdn group** *vpdn-group-name*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**subscriber profile** *profile-name* **例：** `Router(config)# subscriber profile profile-1`	加入者プロファイル名を設定し、加入者プロファイル コンフィギュレーション モードを開始します。 • *profile-name* : **bba-group pppoe** グローバル コンフィギュレーション コマンドによって設定される PPPoE プロファイルから参照されます。これにより、**bba-group pppoe** コマンドによって定義される PPPoE プロファイルを使用するすべての PPPoE セッションが、定義されている加入者プロファイルに従って処理されるようになります。
ステップ 4	**service relay pppoe vpdn group** *vpdn-group-name* **例：** `Router(config-sss-profile)# service relay pppoe vpdn group Group-A`	リレーに VPDN L2TP トンネルを使用する PPPoE リレー サービスを提供します。指定されている VPDN グループ名は、発信 L2TP トンネルの情報を取得するために使用されます。 • 同等の RADIUS プロファイル エントリについては、「次の例は、AAA RADIUS サーバ プロファイルで Subscriber Service Switch 加入者サービス アトリビュートを入力する方法を示しています。」を参照してください。

ステップ 5	`exit`
	
	例：
	`Router(config-sss-profile)# exit`
		（任意）コンフィギュレーション セッションを終了し、特権 EXEC モードに戻ります。

次の作業

「リレーされた PAD メッセージに応答するための LNS（マルチホップ ノード）の設定」で説明されている作業を実行して、設定の LNS 側を設定します。

リレーされた PAD メッセージに応答するための LNS（マルチホップ ノード）の設定

リレーされた PAD メッセージに応答するルータで次の作業を実行して、PPPoE グループを設定し、L2TP のダイヤルイン コールを受け付ける VPDN グループにそれを接続します。リレーされた PAD メッセージは、VPDN L2TP トンネルおよびセッションから、PAD 応答を受け取るための PPPoE ブロードバンド グループに渡されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vpdn-group** *vpdn-group-name*
4. **accept-dialin**
5. **protocol l2tp**
6. **virtual-template** *template-number*
7. **exit**
8. **terminate-from hostname** *host-name*
9. **relay pppoe bba-group** *pppoe-bba-group-name*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group** *vpdn-group-name* 例： `Router(config)# vpdn-group Group-A`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**accept-dialin** **例：** `Router(config-vpdn)# accept-dialin`	LAC からトンネル化 PPP 接続を受け付ける LNS を設定し、accept-dialin VPDN サブグループを作成します。
ステップ 5	**protocol l2tp** **例：** `Router(config-vpdn-req-in)# protocol l2tp`	L2TP トンネリング プロトコルを指定します。
ステップ 6	**virtual-template** *template-number* **例：** `Router(config-vpdn-req-in)# virtual-template 2`	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 7	**exit** **例：** `Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 8	**terminate-from hostname** *host-name* **例：** `Router(config-vpdn)# terminate-from hostname LAC-1`	VPDN トンネルを受け付けるときに必要になる LAC ホスト名を指定します。
ステップ 9	**relay pppoe bba-group** *pppoe-bba-group-name* **例：** `Router(config-vpdn)# relay pppoe bba-group group-2`	PAD メッセージに応答する PPPoE BBA グループを指定します。 • PPPoE BBA グループ名は、**bba-group pppoe** *group-name* グローバル コンフィギュレーション コマンドで定義します。 • 同等の RADIUS プロファイル エントリについては、「LNS の RADIUS VPDN グループ ユーザ プロファイル エントリ」を参照してください。
ステップ 10	**exit** **例：** `Router(config-vpdn)# exit`	グローバル コンフィギュレーション モードに戻ります。

PPPoE リレーの監視

PPPoE リレーを監視するには、この作業を実行します。

手順の概要

1. **enable**
2. **show pppoe session**
3. **show pppoe relay context all**
4. **clear pppoe relay context**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show pppoe session** **例：** `Router# show pppoe session`	現在アクティブな PPPoE セッションに関する情報を表示します。

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

- 必要に応じてパスワードを入力します。

Router> **enable**

ステップ 2 **show pppoe session**

現在アクティブな PPPoE セッションに関する情報を表示します。

Router# **show pppoe session**

```
     1 session  in FORWARDED (FWDED) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
     26     19  0001.96da.a2c0  Et0/0.1                  5  N/A RELFWD
                000c.8670.1006  VLAN:3434
```

ステップ 3 **show pppoe relay context all**

PAD メッセージのリレー用に作成された PPPoE リレー コンテキストを表示します。

```
Router# show pppoe relay context all

Total PPPoE relay contexts 1
UID    ID     Subscriber-profile      State
25     18     cisco.com                 RELAYED
```

ステップ 4 **clear pppoe relay context**

このコマンドは PAD メッセージのリレー用に作成された PPPoE リレー コンテキストをクリアします。

```
Router(config)# clear pppoe relay context
```

トラブルシューティングのヒント

PPPoE リレー機能をトラブルシューティングするときは、特権 EXEC モードで次のコマンドを使用します。

- **debug ppp forwarding**
- **debug ppp negotiation**
- **debug pppoe events**
- **debug pppoe packets**
- **debug vpdn l2x-events**
- **debug vpdn l2x-packets**

PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の設定例

ここでは、次の設定例について説明します。

- 「LAC 設定での PPPoE リレー：例」（P.8）
- 「PPPoE リレー用の LNS の基本設定：例」（P.8）
- 「PAD メッセージに応答するためのトンネル スイッチ（またはマルチホップ ノード）の設定：例」（P.10）
- 「PAD メッセージをリレーするためのトンネル スイッチの設定：例」（P.11）
- 「LAC の RADIUS 加入者プロファイル エントリ：例」（P.12）
- 「LNS の RADIUS VPDN グループ ユーザ プロファイル エントリ：例」（P.12）

LAC 設定での PPPoE リレー：例

次に示すのは、PPPoE リレーをイネーブルにするコマンドが追加された標準的な LAC 設定の例です。

```
hostname User2
!
username User1 password 0 field
username User2 password 0 field
username user-group password 0 field
username User5 password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
username User3-lns-domain password 0 field
!
ip domain-name cisco.com
!
vpdn enable
vpdn source-ip 10.0.195.151
!
vpdn-group User2-vpdn-group-domain
 request-dialin
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.133
 local name User2-lac-domain
```

```
!
!
interface Loopback123
 ip address 10.22.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.195.151 255.255.255.0
 no keepalive
 half-duplex
 pppoe enable group group-1
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback123
 ppp authentication chap
 ppp chap hostname User2-lac-domain
!
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
subscriber profile Profile1
 service relay pppoe vpdn group User2-vpdn-group-domain
!
bba-group pppoe group-1
 virtual-template 1
 service profile Profile1
!
```

PPPoE リレー用の LNS の基本設定：例

次に、PPPoE リレー用のコマンドが追加された LNS の基本設定の例を示します。

```
hostname User5
!
!
username User5 password 0 field
username user-group password 0 field
username User1 password 0 field
username User2 password 0 field
username User3 password 0 field
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 field
username mysgbpgroup password 0 cisco
username User3-lns-domain password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
username User5-mh password 0 field
username User1@domain.net password 0 field
ip subnet-zero
!
!
ip domain-name cisco.com
!
vpdn enable
vpdn multihop
vpdn source-ip 10.0.195.133
!
vpdn-group 1
 request-dialin
```

```
  protocol l2tp
!
vpdn-group 2
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
!
vpdn-group User5-mh
 request-dialin
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.143
 local name User5-mh
!
vpdn-group User3-vpdn-group-domain
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname User2-lac-domain
 local name User3-lns-domain
 relay pppoe group group-1
!
!
interface Loopback0
 no ip address
!
!
interface Loopback123
 ip address 10.23.3.2 255.255.255.0
!
!
interface FastEthernet0/0
 ip address 10.0.195.133 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
!
!
interface Virtual-Template2
 mtu 1492
 ip unnumbered Loopback123
 ip access-group virtual-access3#234 in
 ppp mtu adaptive
 ppp authentication chap
 ppp chap hostname User3-lns-domain
!
!
ip default-gateway 10.0.195.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
bba-group pppoe group-1
 virtual-template 2
!
```

PAD メッセージに応答するためのトンネル スイッチ（またはマルチホップ ノード）の設定：例

次に示すのは、PPPoE リレー メッセージへの応答をイネーブルにするコマンドが追加された標準的なトンネル スイッチ設定の例です。

```
hostname User3
!
!
username User1 password 0 room1
username User2 password 0 room1
username User3 password 0 room1
username User1@domain.net password 0 room1
username User3-lns-dnis password 0 cisco
username User3-lns-domain password 0 room1
username User2-lac-dnis password 0 cisco
username User2-lac-domain password 0 room1
username User5 password 0 room1
username User5-mh password 0 room1
username user-group password 0 room1
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 room1
username mysgbpgroup password 0 cisco
username User1-client-domain@cisco.net password 0 room1
username User4-lns-domain password 0 room1
!
ip domain-name cisco.com
!
vpdn enable
!
vpdn-group User3-mh
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname User5-mh
 relay pppoe bba-group group-1
!
interface Loopback0
 ip address 10.4.4.2 255.255.255.0
!
interface Loopback1
 ip address 10.3.2.2 255.255.255.0
!
interface Ethernet2/0
 ip address 10.0.195.143 255.255.0.0
 half-duplex
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback0
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
 ppp chap hostname User3-lns-domain
!
ip default-gateway 10.0.195.1
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
```

```
bba-group pppoe group-1
 virtual-template 1
!
```

PAD メッセージをリレーするためのトンネル スイッチの設定：例

次の部分的な例では、トンネル スイッチが PAD メッセージをリレーできるようにする設定を示します。

```
subscriber profile profile-1
! Configure profile for PPPoE Relay
 service relay pppoe vpdn group Example1.net
.
.
.
vpdn-group Example2.net
! Configure L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from host Host1
 relay pppoe bba-group group-1
.
.
.
vpdn-group Example1.net
! Configure L2TP tunnel for PPPoE Relay
 request-dialin
  protocol l2tp
.
.
.
 initiate-to ip 10.17.1.3
.
.
.
! PPPoE-group configured for relay
bba-group pppoe group-1
.
.
.
service profile profile-1
```

LAC の RADIUS 加入者プロファイル エントリ：例

次の例は、AAA RADIUS サーバ プロファイルで Subscriber Service Switch 加入者サービス アトリビュートを入力する方法を示しています。

```
profile-1 = profile-name
.
.
.
   Cisco:Cisco-Avpair = ”sss:sss-service=relay-pppoe”
```

次に示すのは、LAC の一般的な RADIUS 加入者プロファイル エントリの例です。

```
cisco.com Password = "password"
    Cisco:Cisco-Avpair = "sss:sss-service=relay-pppoe",
```

```
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Tunnel-Assignment-Id = assignment-id
```

LNS の RADIUS VPDN グループ ユーザ プロファイル エントリ：例

次の例は、AAA RADIUS サーバ プロファイルで VPDN グループ アトリビュートを入力する方法を示しています。

```
profile-1 = profile-name
.
.
.
   Cisco:Cisco-Avpair = ”vpdn:relay-pppoe-bba-group=group-name
```

次に示すのは、LNS の一般的な RADIUS 加入者プロファイル エントリの例です。

```
cisco.com Password = "password"
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Cisco:Cisco-Avpair = "vpdn:relay-pppoe-bba-group=group-name"
    Tunnel-Assignment-Id = assignment-id
```

その他の関連資料

ここでは、PPPoE リレー機能に関する参考資料を紹介します。

関連マニュアル

内容	参照先
VPDN トンネル	『*Cisco IOS XE Dial Technologies Configuration Guide*』
VPDN トンネル コマンド	『*Cisco IOS XE Dial Technologies Configuration Guide*』
トンネル スイッチング	『*L2TP Tunnel Switching*』機能モジュール
PPPoE ブロードバンド グループ	『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』
PPPoE ブロードバンド コマンド	『*Cisco IOS XE Broadband Access Aggregation and DSL Command Reference*』
ブロードバンド アクセス集約の概念	『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』
ブロードバンド アクセス集約の準備作業	『*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*』

標準

標準	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	『*Method for Transmitting PPP Over Ethernet (PPPoE)*』
RFC 3817	• 『*L2TP Active Discovery Relay for PPPoE*』 • Network Working Group Internet-Draft『*L2TP Active Discovery Relay for PPPoE*』: これは次の URL で参照できます。http://www.ietf.org/internet-drafts/draft-dasilva-l2tp-relaysvc-06.txt

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能の機能情報

機能名	リリース	機能の設定情報
PPPoE リレー	Cisco IOS XE Release 2.1	PPPoE リレー機能を使用すると、L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）から L2TP Network Server（LNS; L2TP ネットワーク サーバ）またはトンネル スイッチ（マルチホップ ノード）に PPP over Ethernet（PPPoE）のアクティブ ディスカバリとサービスの選択の機能を Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）制御チャネルでリレーできます。 この機能に関する詳細については、次の各項を参照してください。 • 「PPPoE リレー ディスカバリのイネーブル化およびサービス選択機能に関する情報」（P.2） • 「PPPoE リレー ディスカバリおよびサービス選択機能をイネーブルにする方法」（P.2） この機能は、Cisco IOS XE Release 2.1 に統合されました。
PPPoE Service Selection	Cisco IOS XE Release 2.4	この機能は、Cisco IOS XE Release 2.4 に統合されました。

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能を使用すると、Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）のディスカバリ フェーズで、ファスト イーサネットまたはギガビット イーサネット インターフェイスに対する Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）アクセス要求 ID として DSL Remote-ID タグを送信できます。その結果、ATM ベースのブロードバンド アクセスをシミュレートしますが、費用対効果に優れたファスト イーサネットまたはギガビット イーサネットを使用します。Remote-ID タグは、トラブルシューティング、認証、およびアカウンティングにも使用されます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の機能情報」（P.12）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の前提条件」（P.2）
- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能に関する情報」（P.2）
- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定方法」（P.5）
- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定例」（P.8）
- 「その他の関連資料」（P.9）
- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の機能情報」（P.12）
- 「用語集」（P.13）

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の前提条件

この機能を設定する前に、次のマニュアルの内容を理解しておくことを推奨します。

- RFC 2516 :『*A Method for Transmitting PPP over Ethernet (PPPoE)*』
- DSL Forum 2004-71 :『*Solution for a Remote-ID in PPPoE Discovery Phase*』

詳細については、「その他の関連資料」（P.9）を参照してください。

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能に関する情報

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能を設定するには、次の概念を理解しておく必要があります。

- 「ATM とファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの違い」（P.2）
- 「DSL Forum 2004-71 :「Solution for Remote-ID in PPPoE Discovery Phase」」（P.3）
- 「ファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの Remote-ID タグ」（P.3）
- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の利点」（P.4）

ATM とファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの違い

ブロードバンド DSLAM と Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）のベンダーは、ファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークに ATM-DSL ローカル ループをブリッジして BRAS へのファスト イーサネットまたはギガビット イーサネットベースの接続を許可する DSLAM を使用し、ATM アクセス ネットワークの代わりにファスト イーサネットまたはギガビット イーサネットベースのネットワークを提供する必要があります。ATM VC が加入者線に関連付けられている ATM ベースのブロードバンド ネットワークに見られる固有のマッピングは、加入者の Line-ID タグとファスト イーサネットまたはギガビット イーサネットのブロードバンド アクセス ネットワークのインターフェイスとの間にはありません。PPP アクセスおよび AAA アカウンティング要求を開始する認証フェーズ中に、BRAS は、加入者の DSL を識別する RADIUS 認証パケット内に NAS-Port-ID アトリビュートを含めます。

DSL Forum 2004-71 :「Solution for Remote-ID in PPPoE Discovery Phase」

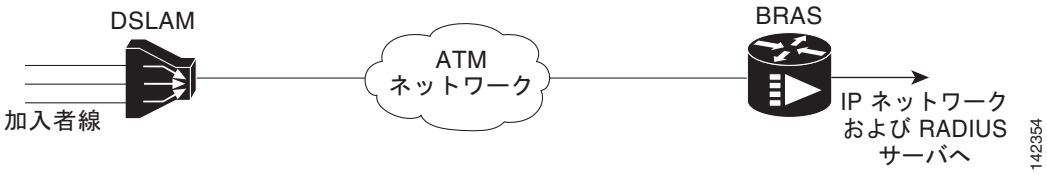
ATM インターフェイスで実行できる機能と同じ加入者マッピング機能をファスト イーサネットまたはギガビット イーサネット インターフェイスに適用するために、DSL Forum 2004-71 は、DSLAM が PPP over Ethernet（PPPoE）ディスカバリ フェーズで DSL Remote-ID タグを送信するソリューションを提案します。この方法により、BRAS として機能する PPPoE サーバに対するサポートが追加され、AAA 認証およびアカウンティング要求で新しい Vendor Specific Attribute（VSA; ベンダー固有アトリ

ビュート）（AAA_AT_REMOTE_ID）として Remote-ID タグをレポートできるようになります。BRAS で **radius-server attribute 31 remote-id** コマンドが設定されている場合、Remote-ID タグは、RADIUS サーバに Calling Station-ID タグ（アトリビュート 31）として送信されます。

ファスト イーサネットまたはギガビット イーサネットベースのブロードバンド アクセス ネットワークの Remote-ID タグ

従来の ATM ベースの DSL ブロードバンド アクセス ネットワークのトポロジを図 1 に示します。

図 1　ATM ベースの DSL ブロードバンド アクセス ネットワーク

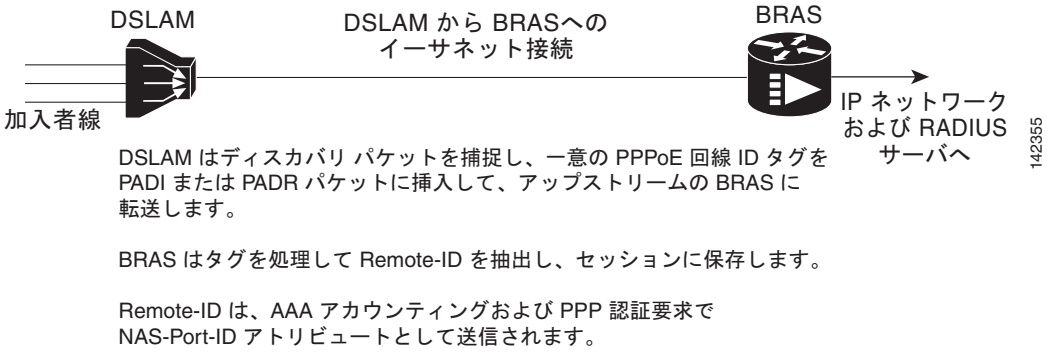


論理接続の観点では、エンド ユーザへの DSL 加入者線と、DSLAM を通じて BRAS へ PPP セッションを伝送するのに使用される ATM ATM Virtual Circuit（VC; 仮想回線）の 1 対 1 のマッピングがあります。この VC 情報は、RADIUS パケットで使用できるように NAS-Port-ID タグに変換されます。

エンド ユーザへの DSL ローカル ループの物理回線と仮想回線（DSLAM から BRAS へ）の間の ATM ベースのネットワークで利用できる単純なマッピングは、ファスト イーサネットまたはギガビット イーサネットベースのネットワークでは使用できません。この問題を解決するために、PPPoE Remote-ID タグ処理機能では、DSLAM で PPPoE 中継エージェント機能を使用して、PPPoE ディスカバリ パケットにタグを付けます。BRAS はこのタグ付きパケットを受信し、タグをデコードして、回線 ID を RADUIS サーバ宛ての RADIUS パケットに挿入します。

DSLAM は、クライアントからの PPPoE ディスカバリ フレームを捕捉するか、PPPoE Active Discovery（PAD）クライアントがレガシー PPP over ATM（PPPoA）デバイスの場合はディスカバリ フレームを開始します。DSLAM は、一意の Remote-ID タグと、PPPoE Vendor-Specific タグ（0x0105）を使用する DSL sync rate タグを、PPPoE Active Discovery Initiation（PADI）パケットおよび PPPoE Active Discovery Request（PADR）パケットに挿入します（図 2 を参照）。DSLAM は、挿入後にこれらのパケットを BRAS にアップストリームで転送します。タグには、中継エージェントがあるアクセス ノードの、PADI または PADR パケットを受信した DSL 回線の識別番号が含まれます。

図 2　PPPoE Remote-ID タグ処理ソリューション



Broadband Access（BBA; ブロードバンド アクセス）グループ コンフィギュレーション モードで **vendor-tag remote-id service** コマンドを設定すると、BRAS は PADR フレームで受信した PPPoE Vendor-Specific タグを処理し、Remote-ID タグを抽出します。このタグは、すべての AAA アクセスおよびアカウンティング要求で、VSA としてリモート AAA サーバに送信されます。BRAS で **radius-server attribute 31 remote-id** グローバル コンフィギュレーション コマンドも設定されている場合、Remote-ID の値がアトリビュート 31 に挿入されます。

BRAS からの発信 PAD Offer（PADO）および PAD Session-Confirmation（PADS）パケットには、DSLAM で挿入された Remote-ID タグが含まれます。DSLAM は、PADO および PADS フレームからこのタグを取り除く必要があります。DSLAM でタグを取り除くことができない場合、BRAS はフレームを送信する前にタグを削除する必要があります。これを行うには、**vendor-tag strip** BBA グループ コンフィギュレーション モード コマンドを使用します。このコマンドを BBA グループで設定すると、BRAS で、発信 PADO および PADS フレームから着信 Remote-ID タグ（その他のベンダータグも含む）が取り除かれます。これは、*DSL Forum Technical Report 101* に準拠した処理です。

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の利点

ファスト イーサネットまたはギガビット イーサネットベースの DSLAM に移行すると、次の利点があります。

- ATM ベースのネットワークではなく、ファスト イーサネットまたはギガビット イーサネットベースのバックホール ネットワークで、簡単で低コストの DSL 加入者向けプロビジョニング オプションを利用できます。
- ATM で使用できない高帯域幅接続オプションをファスト イーサネットまたはギガビット イーサネットから利用できます。
- Quality Of Service（QoS）を備えた次世代の DSLAM にアップグレードし、ADSL2 などのような、より高い帯域幅で非対称二重遅延モデムに対応できます。

ファスト イーサネットまたはギガビット イーサネット ネットワークに、ビデオなどの高帯域幅コンテンツを挿入できます。

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定方法

ここでは、次の手順について説明します。

- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定」（P.5）
- 「Vendor-Specific タグの削除」（P.7）

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定

ここでは、PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能を設定する方法について説明します。この機能を設定すると、BRAS で着信 PADR フレームが処理され、VSA として着信タグの Remote-ID フィールドが RADIUS サーバに送信されます。

DSL-Sync-Rate タグの場合、BBA グループで **vendor-tag dsl-sync-rate service** コマンドを入力する必要があります。このコマンドを入力すると、BRAS で着信 PADR フレームが処理され、VSA として DSL-Sync-Rate タグが RADIUS サーバに送信されます。

RADIUS サーバから Access-Accept メッセージが送信されます。RADIUS サーバからそのままエコーされる場合、Access-Request メッセージで送信された vendor-tag アトリビュートが Access-Accept メッセージに含まれます。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**
4. **bba-group pppoe** *group-name*
5. **vendor-tag remote-id service**
6. **vendor-tag dsl-sync-rate service**
7. **nas-port-id format c**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** **例：** `Router(config)# aaa new-model`	（任意）AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-server attribute 31 remote-id** **例：** `Router(config)# radius-server attribute 31 remote-id`	（任意）新しい VSA（AAA_AT_REMOTE_ID）でアトリビュート 31（Calling Station ID）として Remote-ID タグを RADIUS サーバに送信します。 • ディスカバリ フレームが受信される着信アクセス インターフェイスに関する情報および確立されているセッションに関する情報が、**debug radius** コマンドで表示される Acct-Session-Id アトリビュートに含まれるようこのコマンドを設定します。詳細については、「トラブルシューティングのヒント」（P.8）とそれに続く「Vendor-Specific タグの削除」を参照してください。
ステップ 5	**bba-group pppoe** *group-name* **例：** `Router(config)# bba-group pppoe pppoe-group`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**vendor-tag remote-id service** 例： `Router(config-bba-group)# vendor-tag remote-id service`	BRAS で着信 PADR フレームが処理され、VSA として着信タグの Remote-ID フィールドが RADIUS サーバに送信されるようにします。
ステップ 7	**vendor-tag dsl-sync-rate service** 例： `Router(config-bba-group)# vendor-tag dsl-sync-rate service`	BRAS で着信 PADR フレームが処理され、VSA として DSL-Sync-Rate タグが RADIUS サーバに送信されるようにします。
ステップ 8	**nas-port-id format c** 例： `Router(config-bba-group)# nas-port-id format c`	ブロードバンド加入者のアクセス回線識別番号のコーディングの形式を指定します。 • **format c** は、特定のコーディング形式用の特別な形式です。この形式の例を次に示します。 NAS_PORT_ID=atm 31/31/7:255.65535 example001/0/31/63/31/127 • この例の場合、BRAS の機器の加入者インターフェイス タイプは ATM インターフェイスです。BRAS のスロット番号は 31、BRAS のサブスロット番号は 31 です。BRAS のポート番号は 7 です。Virtual Path Identifier（VPI; 仮想パス識別子）は 255 で、Virtual Circuit Identifier（VCI; 仮想回線識別子）は 65535 です。 Circuit-ID/Remote-ID タグは example001/0/31/63/31/127 です。
ステップ 9	**end** 例： `Router(config-bba-group)# end`	（任意）現在のコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Vendor-Specific タグの削除

発信 PADO および PADS パケットには、DSLAM で挿入された Remote-ID タグと DSL-Sync-Rate タグが含まれます。DSLAM では、パケットからそれらのタグを取り除く必要があります。DSLAM でタグを取り除くことができない場合、BRAS はパケットを送信する前にタグを削除する必要があります。この作業は、BBA グループ コンフィギュレーション モードで **vendor-tag strip** コマンドを設定して実行します。このとき、**vendor-tag strip** コマンドによって、Circuit-ID タグも削除されることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**

5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe** *group-name* **例：** `Router(config)# bba-group pppoe pppoe-group`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。
ステップ 4	**vendor-tag strip** **例：** `Router(config-bba-group)# vendor-tag strip`	BRAS で発信 PADO および PADS フレームから着信 Vendor-Specific タグ（Remote-ID、DSL-Sync-Rate タグ、および Circuit-ID）を取り除くことができるようにします。
ステップ 5	**end** **例：** `Router(config-bba-group)# end`	（任意）現在のコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

トラブルシューティングのヒント

BRAS で PPPoE エージェントの Remote-ID タグおよび DSL 回線の特性拡張機能設定で **radius-server attribute 31 remote-id** グローバル コンフィギュレーション コマンドを入力すると、**debug radius** 特権 EXEC コマンドを使用してレポートを生成できます。

このレポートには次の情報が含まれます。

- 着信アクセス インターフェイス
- ディスカバリ フレームを受信する場所
- PPPoE 拡張 NAS-Port 形式（format d）で確立されているセッションの詳細

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定例

ここでは、次の例について説明します。

- 「PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定：例」（P.9）
- 「Vendor-Specific タグの削除：例」（P.9）

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の設定：例

次の例では、発信 PADO および PADS パケットで、着信 Vendor-Specific Circuit-Id タグを保持します。

```
Router(config)# radius-server attribute 31 remote-id
!
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag remote-id service
Router(config-bba-group)# vendor-tag dsl-sync-rate service
Router(config-bba-group)# nas-port-id format c

!
Router(config)# interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

Vendor-Specific タグの削除：例

次の例では、BRAS は発信 PADO および PADS パケットから着信 Vendor-Specific Circuit-Id タグを取り除きます。

```
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag strip

Router(config)#interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

その他の関連資料

ここでは、PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能に関する参考資料を紹介します。

関連マニュアル

内容	参照先
ブロードバンドと DSL の設定	『*Cisco IOS XE Broadband and DSL Configuration Guide*』
RADIUS アトリビュート	『*RADIUS Attributes Overview and RADIUS IETF Attributes*』モジュール
DSL Line-ID タグ ソリューション	*RFC 4679*：『*DSL Forum Vendor Specific RADIUS Attributes*』
ファスト イーサネットまたはギガビット イーサネットベースの DSL 集約への移行	*DSL Forum Technical Report 101*

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	『*A Method for Transmitting PPP over Ethernet (PPPoE)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能の機能情報

機能名	リリース	機能情報
PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能	Cisco IOS XE Release 2.1	PPPoE エージェント Remote-ID および DSL 回線の特性拡張機能を使用すると、Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）のディスカバリ フェーズで、ファスト イーサネットまたはギガビット イーサネット インターフェイスに対する Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）アクセス要求 ID として DSL Remote-ID タグを送信できます。その結果、ATM ベースのブロードバンド アクセスをシミュレートしますが、費用対効果に優れたファスト イーサネットまたはギガビット イーサネットを使用します。Remote-ID タグは、トラブルシューティング、認証、およびアカウンティングにも使用されます。 次のコマンドが導入または変更されました。**radius-server attribute**、**bba-group pppoe group-name**、**vendor-tag remote-id service**、**vendor-tag dsl-sync-rate service**、**nas-port-id format c**

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。

ATM：Asynchronous Transfer Mode（非同期転送モード）。

BBA：Broadband Access（ブロードバンド アクセス）。

BRAS：Broadband Remote Access Server（ブロードバンド リモート アクセス サーバ）。

DSLAM：Digital Subscriber Line Access Multiplexer（デジタル加入者線アクセス マルチプレクサ）。DSL トラフィックを 1 つまたは複数のネットワーク トランク ラインに多重化して、1 つのネットワークに複数のデジタル加入者線を接続するデバイスです。

PADO：PPPoE Active Discovery Offer。

PADR：PPPoE Active Discovery Request。

PADS：PPPoE Active Discovery Session-Confirmation。

PPPoE：Point-to-Point Protocol over Ethernet。

RADIUS：Remote Authentication Dial-In User Service。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

VCI：Virtual Circuit Identifier（仮想回線識別子）。

VLAN：Virtual Local-Area Network（仮想 LAN）。

VPI：Virtual Path Identifier（仮想パス識別子）。

VSA：Vendor Specific Attribute（ベンダー固有アトリビュート）。特定のベンダーによって実装されたアトリビュートです。Vendor-Specific アトリビュートが使用された結果、AV ペアがカプセル化されます。基本的には、Vendor-Specific = プロトコル :Attribute = 値となります。

ハイ アベイラビリティ

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、二重のルート プロセッサ システムに対して Point-to-Point Protocol over <各種メディア>（PPPoX）セッションのステートフル スイッチオーバーをサポートする機能を提供し、システムの制御およびルーティング プロトコルの実行をアクティブ プロセッサとスタンバイ プロセッサ間で転送するときにアプリケーションと機能で状態を維持できるようにするため、SSO—PPPoE 機能を使用します。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報」（P.17）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの前提条件」（P.2）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーに関する制約事項」（P.2）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーについて」（P.2）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定方法」（P.4）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例」（P.10）
- 「その他の関連資料」（P.15）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報」（P.17）

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの前提条件

Stateful Switchover（SSO; ステートフル スイッチオーバー）機能と Nonstop Forwarding（NSF; ノンストップ フォワーディング）機能がイネーブルになっている必要があります。SSO の詳細については、「*Stateful Switchover*」を参照してください。NSF の詳細については、「*Cisco Nonstop Forwarding*」を参照してください。

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーに関する制約事項

SSO は、High Availability（HA; ハイ アベイラビリティ）ネットワーク デバイスでのみサポートされます。

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーについて

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能を設定するには、次の概念を理解しておく必要があります。

- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能設計」（P.2）
- 「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの利点」（P.4）

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能設計

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能が実装される前は、コントロール プレーンとデータプレーンで予期せぬ障害が発生すると、PPPoX セッションでサービスの停止およびネットワークのダウンタイムが生じていました。SSO を含むシスコのハイ アベイラビリティ機能では、このような障害から迅速に回復することで、ネットワークを保護できます。ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能では、トラフィックの転送を続けながら、スタンバイ プロセッサへのステートフル スイッチオーバーを提供することで、停止の原因を排除します。SSO は、サポートされる機能のプロトコルと状態情報をスタンバイ ルート プロセッサと同期し、スイッチオーバーが行われるときにセッションや接続が中断されないようにすることで、アクティブなルート プロセッサでハードウェアまたはソフトウェアの障害が発生するのを防ぎます。

SSO 機能は、ルート プロセッサの 1 つをアクティブ プロセッサとし、もう一方のルート プロセッサをスタンバイ プロセッサに設定し、それらのプロセッサ間で重要な状態情報を同期して、ルートプロセッサの冗長性を利用します。2 つのプロセッサ間で初期（バルク）同期が行われた後、SSO はそれらのプロセッサ間でルート プロセッサの状態情報をダイナミックに維持します。アクティブなルート プロセッサに障害が発生したとき、ネットワーク デバイスから削除されたとき、または手動でメンテナンスから排除されたときに、アクティブなプロセッサからスタンバイ プロセッサへのスイッチオーバーが発生します。その後、スタンバイ ルート プロセッサが制御を引き継ぎ、アクティブなルート プロセッサになるため、サポートされる機能のセッションおよび接続は保持されます。この時点では、新しいアクティブなルート プロセッサでルート収束が行われている間もパケット転送は続行されます。

SSO とシスコ HA テクノロジーの不可欠な構成要素は、スタンバイ プロセッサ上でセッションの再作成を管理する Cluster Control Manager（CCM; クラスタ コントロール マネージャ）です。ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能では、加入者冗長性ポリシーを設定して、同期処理を調整できます。詳細については、「ブロードバンド HA ステートフル スイッチオーバーの加入者冗長性ポリシーの設定」（P.5）を参照してください。

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能は、Cisco NSF および SSO HA 機能と連携して、PPPoX セッションを維持します。NSF は、ネットワーク トラフィックとアプリケーション状態情報の転送を継続するため、スイッチオーバーの後もユーザ セッション情報は維持されます。

ハイ アベイラビリティおよびステートフル スイッチオーバーの詳細については、『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の「High Availability Overview」の章を参照してください。

サポートされているブロードバンド集約プロトコル

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーフィーチャ セットは、次のブロードバンド集約プロトコルをサポートしています。

- 「SSO L2TP」（P.3）
- 「SSO PPPoE」（P.3）
- 「SSO RA-MLPS VPN」（P.3）

SSO L2TP

L2TP HA Session SSO/ISSU on a LAC/LNS 機能は、Layer 2 Access Concentrator（LAC; レイヤ 2 アクセス コンセントレータ）および Layer 2 Network Server（LNS; レイヤ 2 ネットワーク サーバ）上の Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）のための、汎用 Stateful Switchover/In Service Software Upgrade（SSO/ISSU; ステートフル スイッチオーバー / インサービス ソフトウェア アップグレード）メカニズムを提供します。この機能では、SSO スイッチオーバーや、ISSU アップグレードまたはダウングレード中に、完全に確立された PPP および L2TP セッションが保持されます。

SSO PPPoE

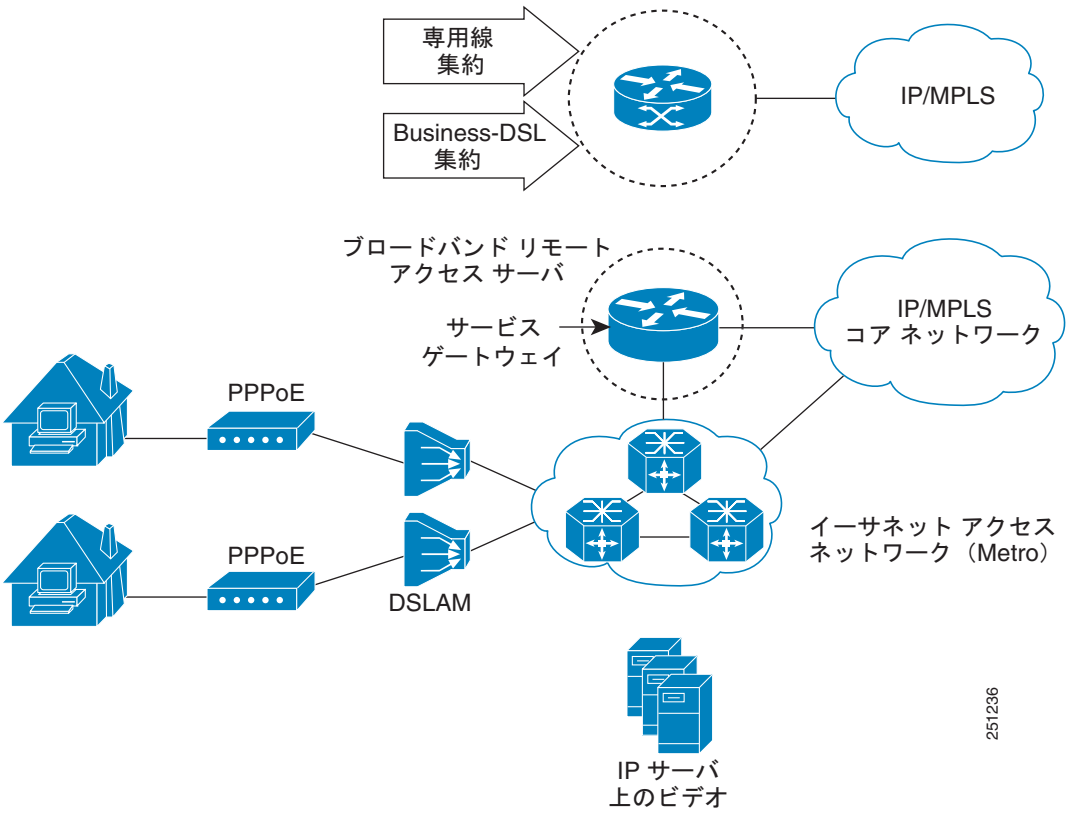
ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能は、PPPoE、PPPoEoVLAN、および PPPoEoQinQ を含む PPP over Ethernet（PPPoE）加入者アクセス セッションに対し、ステートフル スイッチオーバー機能を提供します。

SSO RA-MLPS VPN

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、プロセッサのスイッチオーバー中に Remote Access（RA; リモート アクセス）-MPLS VPN に終端する PPPoX セッションまたは MPLS VPN への PPPoX セッションに対し、ステートフル スイッチオーバー機能を提供します。

図 1 に、SSO 機能を使用した一般的なブロードバンド集約 HA 展開を示します。

図 1　ブロードバンド集約ハイ アベイラビリティ展開



ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの利点

- 停止に関連する運用コストが削減されます。
- 高いサービス レベルが加入者に提供されます。
- ネットワークのアベイラビリティが向上します。
- 特定のネットワーク サービスを提供するノードを通じて、継続的な接続、低パケット損失、および一貫したパス フローが促進されます。
- サービスの中断が軽減され、ダウンタイムのコストが削減されて、運用効率が向上します。

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定方法

ここでは、次の作業について説明します。

- 「ブロードバンド HA ステートフル スイッチオーバーの加入者冗長性ポリシーの設定」（P.5）
- 「ブロードバンド HA ステートフル スイッチオーバーの加入者冗長性ポリシーの確認とトラブルシューティング」（P.6）

ブロードバンド HA ステートフル スイッチオーバーの加入者冗長性ポリシーの設定

ブロードバンド加入者セッションで HA SSO 機能の加入者冗長性ポリシーを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber redundancy** [**bulk limit cpu** *percentage* **delay** *seconds* **allow** value] [**dynamic limit cpu** *percentage* **delay** *seconds* **allow** value] [**delay** *time*] [**rate** *sessions time*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**subscriber redundancy** [**bulk limit cpu** *percentage* **delay** *seconds* **allow** *value*][**dynamic limit cpu** *percentage* **delay** *seconds* **allow** *value*][**delay** *time*][**rate** *sessions time*] **例：** `Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`	（任意）加入者冗長性ポリシーを設定します。 • **bulk**：バルク同期冗長性ポリシーを設定します。 • **limit cpu** *percentage*：CPU のビジー状態のしきい値をパーセンテージで指定します。範囲は 0 ～ 100 で、デフォルトは 90 です。 • **delay** *seconds*：CPU のビジー状態のしきい値を超えた後で、CCM コンポーネントでセッションを同期化する前に遅延を秒単位で指定します。 • **allow** *value*：CPU のビジー状態のしきい値を超え、指定された遅延を満たすと、同期化するセッションの最小数を指定します。範囲は 1 ～ 2147483637 で、デフォルトは 25 です。 • **dynamic**：ダイナミック同期冗長性ポリシーを設定します。 • **delay** *time*：ダイナミック同期が発生する前にセッションで準備しておく必要のある最小時間を秒単位で指定します。値の範囲は 1 ～ 33550 です。 • **rate** *sessions time*：バルク同期とダイナミック同期の期間ごとのセッション数を指定します。 – *sessions*：範囲は 1 ～ 32000 で、デフォルトは 250 です。 – *time*：範囲は 1 ～ 33550 で、デフォルトは 1 です。
ステップ 4	**exit** **例：** `Router(config)# exit`	現在のコンフィギュレーション モードを終了します。

ブロードバンド HA ステートフル スイッチオーバーの加入者冗長性ポリシーの確認とトラブルシューティング

コンフィギュレーションを表示するには、**show running-config** コマンドを使用します。出力例は、「ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例」（P.10）にあります。

ステップ 1 およびステップ 2 は、CCM 同期コンポーネントをトラブルシューティングするのに役立ちます。ステップ 3 およびステップ 4 は、PPPoX セッション統計情報を確認するのに役立ちます。ステップ 5 およびステップ 6 は、L2TP トンネルまたは VPDN グループの障害を確認するのに役立ちます。ステップ 7 は、一般にシスコの技術者が、内部的なデバッグ目的で使用します。

手順の概要

1. **show ccm clients**
2. **show ccm sessions**
3. **show ppp subscriber statistics**
4. **show pppoe statistics**

5. **show vpdn redundancy**
6. **show vpdn history failure**
7. **debug pppoe redundancy**

手順の詳細

ステップ 1 **show ccm clients**

このコマンドは、冗長なプロセッサ HA システムのスタンバイ プロセッサでセッション起動を同期する機能を管理する HA コンポーネント、CCM に関する情報を示します。CCM クライアントに関する情報を表示するには、**show ccm clients** コマンドを使用します

アクティブなルート プロセッサ

```
Router# show ccm clients
CCM bundles sent since peer up:
Sent Queued for flow control
Sync Session 16000 0
Update Session 0 0
Active Bulk Sync End 1 0
Session Down 0 0
ISSU client msgs 346 0
Dynamic Session Sync 0 0
Unknown msgs 0 0
Client events sent since peer up:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

スタンバイのルート プロセッサ

```
Router# show ccm clients
CCM bundles rcvd since last boot:
Sync Session 16000
Update Session 0
Active Bulk Sync End 1
Session Down 0
ISSU client msgs 173
Dynamic Session Sync 0
Unknown msgs 0
Client events extracted since last boot:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

ステップ 2 **show ccm sessions**

このコマンドは、CCM で管理されているセッションについての情報を表示します。

アクティブなルート プロセッサ

```
Router# show ccm sessions
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFE

Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 9279
Number of sessions in state Ready: 0 0 6721
Number of sessions in state Dyn Sync: 16000 16000 0

Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 64 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 475 - -
```

スタンバイのルート プロセッサ

```
Router# show ccm sessions
Global CCM state: CCM HA Standby - Collecting
Global ISSU state: Compatible, Clients Cap 0x9EFFE

Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 8384
Number of sessions in state Ready: 16000 0 7616
Number of sessions in state Dyn Sync: 0 0 0

Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 0 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 0 - -
```

ステップ 3 **show ppp subscriber statistics**

このコマンドは、PPP 加入者のイベントおよび統計情報を表示するのに便利です。**show ppp subscriber statistics** コマンドは、PPP 加入者イベントと統計情報の累積数を表示するためと、最後に **clear ppp subscriber statistics** コマンドを発行してからの増分を表示するために使用します。

次に、**show ppp subscriber statistics** コマンドの出力例を示します。

```
Router# show ppp subscriber statistics

PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       7             7
Forwarding                     0             0
Forwarded                      0             0
```

```
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        0             0
PPPBindResp                    7             7
PPPReneg                       3             3
RestartTimeout                 5             5

PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  4             4
IDB CSTATE DOWN                8             8
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 8             8
```

ステップ 4　show pppoe statistics

このコマンドは、PPPoE セッションの統計情報とイベントを取得するのに便利です。**show pppoe statistics** コマンドは、PPPoE イベントおよび統計情報の累積数を表示するためと、最後に **clear pppoe statistics** コマンドを発行してからの増分を表示するために使用します。

次に、**show pppoe statistics** コマンドの出力例を示します。

```
Router# show pppoe statistics

PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              0             0
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM DISCONNECT                 0             0

PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        0             0
PPPoE Handles Freed            0             0
Dynamic Bind Request           0             0
Static Bind Request            0             0
```

ステップ 5　show vpdn redundancy

このコマンドは、L2TP トンネルの障害を確認するために使用します。

```
Router# show vpdn redundancy
L2TP HA support: Silent Failover

L2TP HA Status:
Checkpoint Messaging on: FALSE
```

```
Standby RP is up: TRUE
Recv'd Message Count: 0
L2TP Tunnels: 2/2/2/0 (total/HA-enabled/HA-est/resync)
L2TP Sessions: 10/10/10 (total/HA-enabled/HA-est)
L2TP Resynced Tunnels: 0/0 (success/fail)
```

ステップ 6 **show vpdn history failure**

このコマンドは、VPDN グループの障害を確認するために使用します。

```
Router# show vpdn history failure
% VPDN user failure table is empty
```

ステップ 7 **debug pppoe redundancy**

debug pppoe redundancy コマンドは、HA システム上の PPPoE セッションの CCM イベントとメッセージを表示するために使用します。このコマンドは、一般にシスコの技術者だけが、CCM プロセスの内部的なデバッグのために使用します。

```
Router# debug pppoe redundancy

Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例

ここでは、次の設定例について説明します。

- 「SSO を使用した RA-MPLS ネットワークに終端する PPPoX：例」（P.10）

SSO を使用した RA-MPLS ネットワークに終端する PPPoX：例

次の例は、RA-MPLS ネットワークでブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能を設定する方法を示しています。

```
Router# show running-config

hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
```

```
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

次の行は、加入者冗長性ポリシーの設定を示します。

```
subscriber redundancy dynamic limit cpu 90 delay 10
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
  virtual-template 2
!
bba-group pppoe grp3
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
```

```
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 10.1.1.1 255.255.255.255
!
interface Loopback100
  ip address 192.168.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
encapsulation dot1Q 2
pppoe enable group grp2
!
!
interface GigabitEthernet1/0/1
no ip address
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
encapsulation dot1Q 2
pppoe enable group grp5
!
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
```

```
!
interface GigabitEthernet7/0/3
no ip address
!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
```

```
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
  network 224.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 224.0.0.3 remote-as 1
  neighbor 224.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 224.0.0.3 activate
  neighbor 224.0.0.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.13.1.1 10.13.16.160
ip local pool pool4 10.14.1.1 10.14.16.160
ip local pool pool5 10.15.1.1 10.15.16.160
ip local pool pool6 10.16.1.1 10.16.16.160
ip local pool pool7 10.17.1.1 10.17.16.160
ip local pool pool8 10.18.1.1 10.18.16.160
ip classless !
!
no ip http server
!
!
arp 10.20.1.1 0020.0001.0001 ARPA
```

```
arp vrf vrf1 10.20.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

その他の関連資料

ここでは、ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能に関する関連資料について説明します。

関連マニュアル

内容	参照先
ハイ アベイラビリティ	『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の「High Availability Overview」の章
ISSU の実行	『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の次の章 • 「Cisco IOS XE Software Package Compatibility for ISSU」 • 「In Service Software Upgrade (ISSU)」
ブロードバンド ISSU	『*Broadband High Availability In Service Software Upgrade*』
ステートフル スイッチオーバー	『*Stateful Switchover*』
シスコ ノンストップ フォワーディング	『*Cisco Nonstop Forwarding*』
レイヤ 2 トンネル プロトコル	『*Layer 2 Tunnel Protocol Technology Brief*』
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、および フィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能の機能情報

機能名	リリース	機能情報
SSO—PPPoE	Cisco IOS XE Release 2.1、 Cisco IOS XE Release 2.5	この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 ルータに実装されました。 この機能は、二重のルート プロセッサ システムに対して PPPoX セッションのステートフル スイッチオーバーをサポートする機能を提供し、システムの制御およびルーティング プロトコルの実行をアクティブ プロセッサとスタンバイ プロセッサ間で転送するときにアプリケーションと機能で状態を維持できるようにするため、SSO—PPPoE 機能を使用します。 次のコマンドが導入または変更されました。**clear ppp subscriber statistics**、**clear pppoe statistics**、**debug pppoe redundancy**、**show ccm clients**、**show ccm sessions**、**show ppp subscriber statistics**、show **pppoe statistic**、**subscriber redundancy**

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー

ブロードバンド High Availability（HA; ハイ アベイラビリティ）インサービス ソフトウェア アップグレード機能は、ソフトウェアのアップグレード、ダウングレード、サービス拡張の間にブロードバンド アクセス プロトコルが継続して動作できるようにするため、ISSU—PPPoE 機能を使用します。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報」（P.18）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの前提条件」（P.2）
- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーに関する制約事項」（P.2）
- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーについて」（P.2）
- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー の設定方法」（P.5）
- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例」（P.10）
- 「その他の関連資料」（P.15）

- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報」（P.18）

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの前提条件

Stateful Switchover（SSO; ステートフル スイッチオーバー）機能と Nonstop Forwarding（NSF; ノンストップ フォワーディング）機能がイネーブルになっている必要があります。SSO の詳細については、「*Stateful Switchover*」を参照してください。NSF の詳細については、「*Cisco Nonstop Forwarding*」を参照してください。

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーに関する制約事項

- 主要な Cisco IOS XE リリースにまたがって ISSU を実行できます。
- ISSU は、ISSU 機能をサポートしている Cisco IOS XE リリースから実行できます。

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーについて

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能を設定するには、次の概念を理解しておく必要があります。

- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能設計」（P.2）
- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの利点」（P.4）

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能設計

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能が実装される前は、ソフトウェアをアップグレードするために、計画的な停止を行ってルータまたはネットワークをアウト オブ サービス状態することが一般に必要でした。Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能を使用すると、サービス プロバイダーは、ルータまたはネットワークをアウト オブ サービス状態にせずに Cisco IOS XE リリースをアップグレードできます。これにより、ネットワークのアベイラビリティが最大化され、計画的な停止をなくすことができます。ISSU は、シスコの High Availability（HA; ハイ アベイラビリティ）アーキテクチャに基づく手順です。これにより、Cisco IOS XE インフラストラクチャは、パケット転送を継続し、ブロードバンド セッションを維持したまま、アップグレードを実現します。シスコの HA アーキテクチャは、冗長なルート プロセッサ、NSF 機能および SSO 機能に基づいており、ポートはアクティブなままとなり、コールはドロップされず、アップグレード中にネットワークは中断されません。

ISSU 機能を使用すると、新しい機能、ハードウェア、サービス、およびメンテナンス用の修正プログラムを、エンド ユーザにとってシームレスな手順で展開できます。ISSU とシスコ HA テクノロジーの不可欠な構成要素は、スタンバイ プロセッサ上でセッションの再作成と同期を管理する Cluster Control Manager（CCM; クラスタ コントロール マネージャ）です。Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能では、加入者冗長性ポリシーを設定して、同期処理を調整できます。詳細については、「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの加入者冗長性ポリシーの設定」（P.5）を参照してください。

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、アップグレードとダウングレードを扱い、次のことをサポートします。

- Cisco IOS XE Release 2.2 から Cisco IOS XE Release 2.3 など、ソフトウェア フィーチャ リリース間のアップグレード（ただし、どちらのバージョンも ISSU 機能をサポートしている必要があります）。
- Cisco IOS XE Release 2.2.1 から Cisco IOS XE Release 2.2.2 など、ソフトウェア メンテナンス リリース間のアップグレード。

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能は、他の Cisco IOS XE HA 機能である NSF および SSO と連携して、ブロードバンド セッションを維持します。

ISSU の実行

ハイ アベイラビリティおよび ISSU の実行の詳細については、『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の次の章を参照してください。

- 「High Availability Overview」
- 「Cisco IOS XE Software Package Compatibility for ISSU」
- 「In Service Software Upgrade (ISSU)」

サポートされているブロードバンド集約プロトコル

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、次のブロードバンド集約プロトコルをサポートしています。

- 「ISSU L2TP」（P.3）
- 「ISSU PPPoE」（P.4）
- 「ISSU RA-MLPS VPN」（P.4）

ISSU L2TP

L2TP HA Session SSO/ISSU on a LAC/LNS 機能は、Layer 2 Access Concentrator（LAC; レイヤ 2 アクセス コンセントレータ）および Layer 2 Network Server（LNS; レイヤ 2 ネットワーク サーバ）上の Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）のための、汎用 Stateful Switchover/In Service Software Upgrade（SSO/ISSU; ステートフル スイッチオーバー / インサービス ソフトウェア アップグレード）メカニズムを提供します。この機能では、SSO スイッチオーバーや、ISSU アップグレードまたはダウングレード中に、完全に確立された PPP および L2TP セッションが保持されます。

ISSU PPPoE

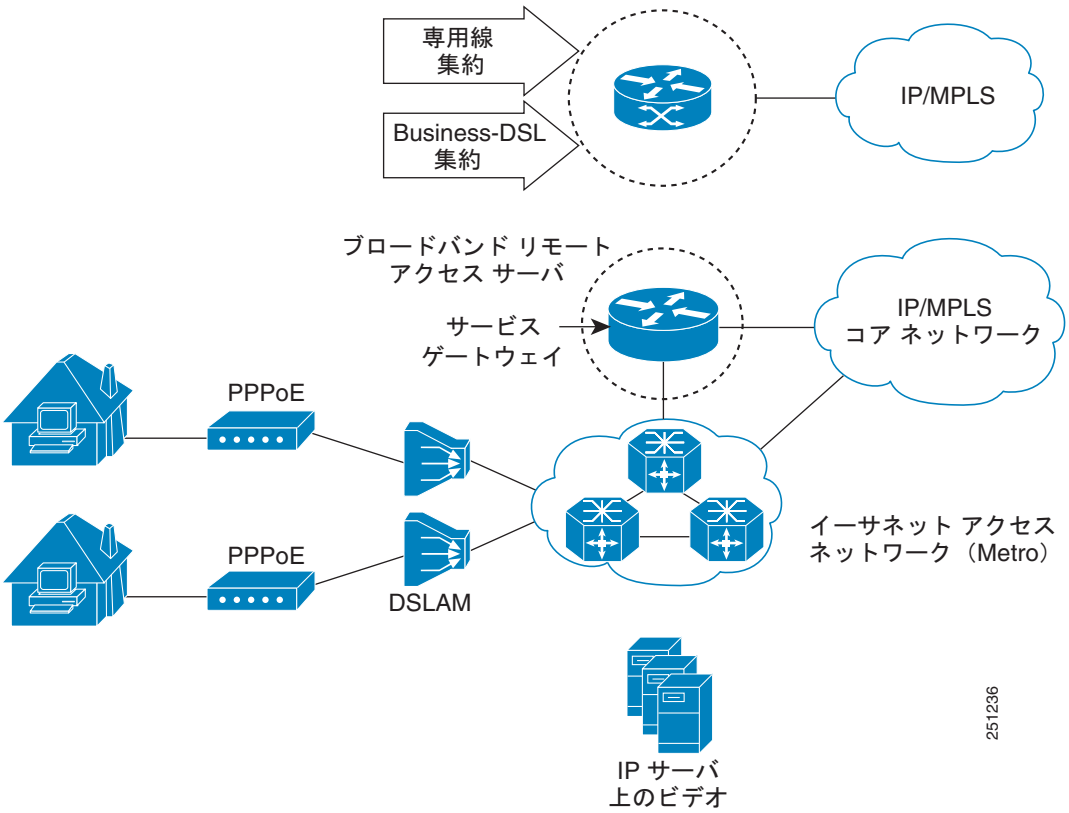
Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー 機能は、PPPoE セッション、PPPoEoVLAN セッション、および PPPoEoQinQ セッションを含む PPP over Ethernet（PPPoE）加入者アクセス セッションに対し、サポートされているソフトウェアのアップグレード、ダウングレード、機能拡張中の ISSU 機能を提供します。

ISSU RA-MLPS VPN

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、Remote Access（RA; リモート アクセス）Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に終端する PPPoA および PPPoE（PPPoX）セッションや、MPLS VPN への PPPoX に対し、サポートされているソフトウェアのアップグレード、ダウングレード、機能拡張中の ISSU 機能を提供します。

図 1 に、ISSU 機能を使用した一般的なブロードバンド集約 HA 展開を示します。

図 1　　ブロードバンド集約ハイ アベイラビリティ展開



Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの利点

- Cisco IOS XE ソフトウェアのアップグレードのためのダウンタイムがなくなります。

- 計画的な停止と深夜のメンテナンス時間に関連するリソース スケジューリングの問題がなくなります。
- 新しいサービスとアプリケーションを容易に展開でき、新しい機能、ハードウェア、修正を素早く実装できます。
- 高いサービス レベルを提供しつつ、停止に伴う運用コストが削減されます。
- メンテナンス時間を調整するための追加オプションが増えます。
- サービスに対するアップグレードの影響が最小化され、迅速なアップグレードが可能になるため、アベイラビリティが高まります。

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー の設定方法

ここでは、次の手順について説明します。

- 「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの加入者冗長性ポリシーの設定」（P.5）
- 「ブロードバンド HA ISSU の加入者冗長性ポリシーの確認とトラブルシューティング」（P.6）

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの加入者冗長性ポリシーの設定

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能は、デフォルトでイネーブルにされています。この作業では、HA ISSU 機能のための加入者冗長性ポリシーを設定します。これにより、HA のアクティブ プロセッサとスタンバイ プロセッサの間の同期を管理できます。

前提条件

ハイ アベイラビリティおよび ISSU の実行の詳細については、『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の次の章を参照してください。

- 「High Availability Overview」
- 「Cisco IOS XE Software Package Compatibility for ISSU」
- 「In Service Software Upgrade (ISSU)」

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber redundancy** [**bulk limit cpu** *percentage* **delay** *seconds* **allow** value] [**dynamic limit cpu** *percentage* **delay** *seconds* **allow** value] [**delay** *time*] [**rate** *sessions time*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**subscriber redundancy** [**bulk limit cpu** *percentage* **delay** *seconds* **allow** *value*][**dynamic limit cpu** *percentage* **delay** *seconds* **allow** *value*][**delay** *time*][**rate** *sessions time*] **例：** `Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`	（任意）加入者冗長性ポリシーを設定します。 • **bulk**：バルク同期冗長性ポリシーを設定します。 • **limit cpu** *percentage*：CPU のビジー状態のしきい値をパーセンテージで指定します。範囲は 0 ～ 100 で、デフォルトは 90 です。 • **delay** *seconds*：CPU のビジー状態のしきい値を超えた後で、CCM コンポーネントでセッションを同期化する前に遅延を秒単位で指定します。 • **allow** *value*：CPU のビジー状態のしきい値を超え、指定された遅延を満たすと、同期化するセッションの最小数を指定します。範囲は 1 ～ 2147483637 で、デフォルトは 25 です。 • **dynamic**：ダイナミック同期冗長性ポリシーを設定します。 • **delay** *time*：ダイナミック同期が発生する前にセッションで準備しておく必要のある最小時間を秒単位で指定します。値の範囲は 1 ～ 33550 です。 • **rate** *sessions time*：バルク同期とダイナミック同期の期間ごとのセッション数を指定します。 – *sessions*：範囲は 1 ～ 32000 で、デフォルトは 250 です。 – *time*：範囲は 1 ～ 33550 で、デフォルトは 1 です。
ステップ 4	**exit** **例：** `Router(config)# exit`	現在のコンフィギュレーション モードを終了します。

ブロードバンド HA ISSU の加入者冗長性ポリシーの確認とトラブルシューティング

加入者冗長性ポリシーの設定を確認するには、**show running-config** コマンドを使用します。出力例は、「Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例」（P.10）にあります。

ステップ 1 およびステップ 2 は、CCM 同期コンポーネントをトラブルシューティングするのに役立ちます。ステップ 3 およびステップ 4 は、PPPoX セッション統計情報を確認するのに役立ちます。ステップ 5 およびステップ 6 は、L2TP トンネルまたは VPDN グループの障害を確認するのに役立ちます。ステップ 7 は、一般にシスコの技術者が、内部的なデバッグ目的で使用します。

手順の概要

1. **show ccm clients**
2. **show ccm sessions**
3. **show ppp subscriber statistics**
4. **show pppoe statistics**
5. **show vpdn redundancy**
6. **show vpdn history failure**
7. **debug pppoe redundancy**

手順の詳細

ステップ 1 show ccm clients

このコマンドは、冗長なプロセッサ HA システムのスタンバイ プロセッサでセッション起動を同期する機能を管理する HA コンポーネント、CCM に関する情報を示します。CCM クライアントに関する情報を表示するには、**show ccm clients** コマンドを使用します。

アクティブなルート プロセッサ

```
Router# show ccm clients
CCM bundles sent since peer up:
Sent Queued for flow control
Sync Session 16000 0
Update Session 0 0
Active Bulk Sync End 1 0
Session Down 0 0
ISSU client msgs 346 0
Dynamic Session Sync 0 0
Unknown msgs 0 0
Client events sent since peer up:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

スタンバイのルート プロセッサ

```
Router# show ccm clients
CCM bundles rcvd since last boot:
Sync Session 16000
Update Session 0
Active Bulk Sync End 1
Session Down 0
ISSU client msgs 173
```

```
Dynamic Session Sync 0
Unknown msgs 0
Client events extracted since last boot:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

ステップ 2 **show ccm sessions**

このコマンドは、CCM で管理されているセッションについての情報を表示します。

アクティブなルート プロセッサ

```
Router# show ccm sessions
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFE

Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 9279
Number of sessions in state Ready: 0 0 6721
Number of sessions in state Dyn Sync: 16000 16000 0

Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 64 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 475 - -
```

スタンバイのルート プロセッサ

```
Router# show ccm sessions
Global CCM state: CCM HA Standby - Collecting
Global ISSU state: Compatible, Clients Cap 0x9EFFE

Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 8384
Number of sessions in state Ready: 16000 0 7616
Number of sessions in state Dyn Sync: 0 0 0

Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 0 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 0 - -
```

ステップ 3 **show ppp subscriber statistics**

このコマンドは、PPP 加入者のイベントおよび統計情報を表示するのに便利です。
show ppp subscriber statistics コマンドは、PPP 加入者イベントと統計情報の累積数を表示するためと、最後に **clear ppp subscriber statistics** コマンドを発行してからの増分を表示するために使用します。

次に、**show ppp subscriber statistics** コマンドの出力例を示します。

```
Router# show ppp subscriber statistics

PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       7             7
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        0             0
PPPBindResp                    7             7
PPPReneg                       3             3
RestartTimeout                 5             5

PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  4             4
IDB CSTATE DOWN                8             8
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 8             8
```

ステップ 4 **show pppoe statistics**

このコマンドは、PPPoE セッションの統計情報とイベントを取得するのに便利です。**show pppoe statistics** コマンドは、PPPoE イベントおよび統計情報の累積数を表示するためと、最後に **clear pppoe statistics** コマンドを発行してからの増分を表示するために使用します。

次に、**show pppoe statistics** コマンドの出力例を示します。

```
Router# show pppoe statistics

PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              0             0
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM DISCONNECT                 0             0

PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
```

```
SSS Disconnect                  0             0
PPPoE Handles Allocated         0             0
PPPoE Handles Freed             0             0
Dynamic Bind Request            0             0
Static Bind Request             0             0
```

ステップ 5 **show vpdn redundancy**

このコマンドは、L2TP トンネルの障害を確認するために使用します。

```
Router# show vpdn redundancy
L2TP HA support: Silent Failover

L2TP HA Status:
Checkpoint Messaging on: FALSE
Standby RP is up: TRUE
Recv'd Message Count: 0
L2TP Tunnels: 2/2/2/0 (total/HA-enabled/HA-est/resync)
L2TP Sessions: 10/10/10 (total/HA-enabled/HA-est)
L2TP Resynced Tunnels: 0/0 (success/fail)
```

ステップ 6 **show vpdn history failure**

このコマンドは、VPDN グループの障害を確認するために使用します。

```
Router# show vpdn history failure
% VPDN user failure table is empty
```

ステップ 7 **debug pppoe redundancy**

debug pppoe redundancy コマンドは、HA システム上の PPPoE セッションの CCM イベントとメッセージを表示するために使用します。このコマンドは、一般にシスコの技術者だけが、CCM プロセスの内部的なデバッグのために使用します。

```
Router# debug pppoe redundancy

Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの設定例

ここでは、次の設定例について説明します。

- 「ISSU を使用した RA-MPLS ネットワークに終端する PPPoX：例」（P.11）

ISSU を使用した RA-MPLS ネットワークに終端する PPPoX：例

次の例は、RA-MPLS ネットワークでCisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能の PPPoX セッション加入者冗長性ポリシーを設定する方法を示しています。

```
Router# show running-config

hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

次の行は、加入者冗長性ポリシーの設定を示します。

```
subscriber redundancy dynamic limit cpu 90 delay 10
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
buffers small permanent 15000
buffers middle permanent 12000
buffers large permanent 1000
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
  virtual-template 2
!
bba-group pppoe grp3
```

```
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 172.16.1.1 255.255.255.255
!
interface Loopback100
  ip address 172.31.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
encapsulation dot1Q 2
pppoe enable group grp2
!
!
interface GigabitEthernet1/0/1
no ip address
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
encapsulation dot1Q 2
pppoe enable group grp5
!
```

```
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
!
interface GigabitEthernet7/0/3
no ip address

!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
```

```
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
  network 10.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 10.0.0.3 remote-as 1
  neighbor 10.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
  redistribute connected
```

```
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.1.1.1 10.1.16.160
ip local pool pool4 10.1.1.1 10.1.16.160
ip local pool pool5 10.1.1.1 10.1.16.160
ip local pool pool6 10.1.1.1 10.1.16.160
ip local pool pool7 10.1.1.1 10.1.16.160
ip local pool pool8 10.1.1.1 10.1.16.160
ip classless !
!
no ip http server
!
!
arp 10.1.1.1 0020.0001.0001 ARPA
arp vrf vrf1 10.1.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

その他の関連資料

ここでは、Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー機能に関する関連資料について説明します。

関連マニュアル

内容	参照先
ハイ アベイラビリティ	『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide* 』の「High Availability Overview」の章
ISSU の実行	『 *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の次の章 • 「Cisco IOS XE Software Package Compatibility for ISSU」 • 「In Service Software Upgrade (ISSU)」
ブロードバンド SSO	『*Broadband High Availability Stateful Switchover*』
ステートフル スイッチオーバー	『*Stateful Switchover*』
シスコ ノンストップ フォワーディング	『*Cisco Nonstop Forwarding*』
レイヤ 2 トンネル プロトコル	『*Layer 2 Tunnel Protocol Technology Brief*』
このマニュアルで使用しているコマンドのその他の情報	• 『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』 • 『*Cisco IOS Master Command List, All Releases*』

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、および フィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバーの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS XE のソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　Cisco IOS ブロードバンド ハイ アベイラビリティ ステートフル スイッチオーバー の機能情報

機能名	リリース	機能情報
ISSU—PPPoE、PPPoE 用の Cisco IOS ブロードバンド ハイ アベイラビリティ インサービス ソフトウェア アップグレード	Cisco IOS XE Release 2.1、 Cisco IOS XE Release 2.5	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能は、ソフトウェアのアップグレード、ダウングレード、サービス拡張の間にブロードバンド アクセス プロトコルが継続して動作できるようにするため、ISSU—PPPoE 機能を使用します。 次のコマンドが導入または変更されました。**clear ppp subscriber statistics**、**clear pppoe statistics**、**debug pppoe redundancy**、**show ccm clients**、**show ccm sessions**、**show ppp subscriber statistics**、**show pppoe statistic**、**subscriber redundancy**