プライベート ホスト

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

プライベート ホストの前提条件

なし。

プライベート ホストの制約事項

- 「プライベート ホストのマルチキャスト動作」（P.27-4）

一般的なプライベート ホストの制約事項

- プライベート ホストおよびプライベート VLAN の両方は同じポート（インターフェイス）に設定できません。両方の機能はスイッチ上で共存できますが、それぞれの機能は異なるポートに設定する必要があります。
- プライベート ホストはエンドツーエンド機能です。この機能は DSLAM とアップストリーム デバイス（BRAS またはマルチキャスト サーバなど）の間のすべてのスイッチ上でイネーブルにする必要があります。
- 独立ポートとして設定できるのは信頼できるポートだけです。
- プライベート ホスト機能は、トランキング スイッチ ポートとして設定されているレイヤ 2 インターフェイス上でサポートされています。
- プライベート ホスト機能は、ポートチャネル インターフェイス上（EtherChannel、ファスト EtherChannel、ギガビット EtherChannel）でサポートされています。プライベート ホストは、ポートチャネル インターフェイス上でイネーブルにします。この機能をメンバ ポート上でイネーブルにできません。
- DAI および DHCP スヌーピングは、ポート上のすべての VLAN がスヌーピング対応に設定されている場合を除き、プライベート ホスト上でイネーブル化できません。

プライベート ホスト ACL の制約事項

- このリリースのプライベート ホスト機能は、プロトコル独立型 MAC ACL を使用します。

  プライベート ホスト用に設定されたポートには、IP ベース ACL を適用しないでください。適用すると、プライベート ホスト機能が無効になります（スイッチがポートにプライベート ホスト MAC ACL を適用できないため）。
- 次のインターフェイス タイプをプロトコル独立型 MAC ACL フィルタリングに設定できます。
  - IP アドレスのない VLAN インターフェイス
  - EoMPLS をサポートする物理 LAN ポート
  - EoMPLS をサポートする論理 LAN サブインターフェイス
- プロトコル独立型 MAC ACL フィルタリングでは、すべての入力トラフィック タイプ（MAC レイヤ トラフィック、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に MAC ACL が適用されます。
- プロトコル独立型 MAC ACL によって許可または拒否された入力トラフィックは、出力インターフェイスによって MAC レイヤ トラフィックとして処理されます。プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否されたトラフィックに、出力 IP ACL を適用できません。
- IP アドレスが設定されている VLAN インターフェイス上で、プロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックが PFC または DFC によってハードウェアでブリッジングされる、またはレイヤ 3 スイッチングされた場合、microflow ポリシングにプロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックがソフトウェアでルーティングされる場合、プロトコル独立型 MAC ACL フィルタリングはマイクロフロー ポリシングをサポートします。

- 既存の VLAN ACL（VACL）およびルーティング ACL（RACL）とトランク ポートの PACL との干渉を避けるには、トランク ポート インターフェイス上のアクセス グループ モードをポート モード優先に設定します。プライベート ホスト用に設定されているポートに VACL または RACL を設定しないでください。

トランク ポート上のプライベート ホスト VLAN の制約事項

- プライベート ホスト用に設定されたトランクポートを使用して VLAN 上で IGMP スヌーピングをイネーブル化できます。
- プライベート ホスト用に設定されたトランクポートを使用して VLAN 上で IP マルチキャストをイネーブル化できません。
- PACL はトランク ポート上で、上書きモードで動作するため、VLAN ベースの機能をスイッチポートに適用できません。
- マルチキャスト VLAN レジストレーション（MVR）機能は、マルチキャスト送信元が無差別ポートにある場合は、プライベート ホストと共存できます。

プライベート ホストとその他の機能の相互作用

- プライベート ホストはレイヤ 2 ベースのサービス（MAC 制限、ユニキャスト フラッディング プロテクション（UFP）、不明なユニキャストフラッディングのブロック（UUFB））には影響しません。
- プライベート ホスト機能は、IGMP スヌーピングには影響しません。ただし、IGMP スヌーピングがグローバルにディセーブル化されている場合は、IGMP 制御パケットが ACL チェックの対象になります。IGMP 制御パケットを許可するには、プライベート ホスト ソフトウェアでマルチキャスト permit ステートメントを独立ホスト用の PACL に追加します。この操作は自動で行われ、ユーザの介入を必要としません。
- 独立ポートでポート セキュリティをイネーブルにして、これらのポートにセキュリティを追加できます。
- 無差別ポート、または混合ポートでイネーブル化された場合は、ポート セキュリティ機能がアップストリーム デバイス用（BRAS またはマルチキャスト サーバなど）の送信元ポート内の変更を制限する場合があります。
- アクセス ポートでイネーブル化された場合は、802.1X はプライベート ホスト機能の影響を受けません。

プライベート ホストのスプーフィングからの保護

プライベート ホスト機能は MAC アドレス スプーフィングを防ぎますが、カスタマー MAC または IP アドレスを有効化しません。MAC アドレス スプーフィングを防ぐため、プライベート ホスト機能は次の処理を行います。

- BRAS またはマルチキャスト サーバにスタティック MAC アドレスを使用します。
- レイヤ 2 転送テーブル上での学習をディセーブル化します。
- BRAS またはマルチキャスト サーバがソース ポートから別のポートに移動した場合に、スイッチ ソフトウェアに通知します。ソフトウェアは移動を確認し、レイヤ 2 転送テーブルを更新します。

プライベート ホストのマルチキャスト動作

アップストリーム デバイス（BRAS やマルチキャスト サーバなど）から発信されるマルチキャスト トラフィックは常に許可されます。また、プライベート ホスト PACL はマルチキャスト制御パケット（IGMP クエリーや Join 要求など）には適用されません。この動作により独立ホストは、マルチキャスト グループに参加したり、IGMP クエリーに応答したり、関連するすべてのグループからのトラフィックを受信できるようになります。

ホストから発信されたマルチキャスト トラフィックは、プライベート ホスト PACL によりドロップされます。ただし、他のホストが、あるホストから発信されたマルチキャスト トラックを受信する必要がある場合、プライベート ホスト機能は PACL に *multicast permit* エントリを追加します。

プライベート ホストについて

プライベート ホストの概要

一般的に、サービス プロバイダーはトリプルプレイ サービス（音声、ビデオ、データ）を提供する際、各ユーザ向けの 1 つの物理インターフェイス上で 3 つの VLAN を使用します。サービス プロバイダーが複数のエンド ユーザ向けに VLAN を 1 セット導入できれば、サービス インフラストラクチャは、よりシンプルになり拡張性も向上しますが、サービス プロバイダーはレイヤ 2 のユーザ（ホスト）間のトラフィックを分離できなければなりません。プライベート ホスト機能を使用すれば、この分離が可能になり複数のエンド ユーザ間で VLAN 共有ができます。

プライベート ホスト機能の主な利点は次のとおりです。

- 同じ VLAN ID を共有しているホスト（加入者）間のトラフィックを分離
- 異なる加入者間で VLAN ID を再利用することで、4096 の VLAN の使用率を高め、VLAN の拡張性を向上
- サービス拒絶（DoS）攻撃からの保護を目的としたメディア アクセス コントロール（MAC）アドレス スプーフィングの防止

プライベート ホスト機能はプロトコル独立型のポートベース アクセス コントロール リスト（PACL）を使用して、完全レイヤ 2 上における信頼できるポート上のホスト間のレイヤ 2 分離を可能にします。PACL では、スイッチ ポートにレイヤ 2 フォワーディング制約を課すことによって、ホストが分離されます。

VLAN でのホストの分離

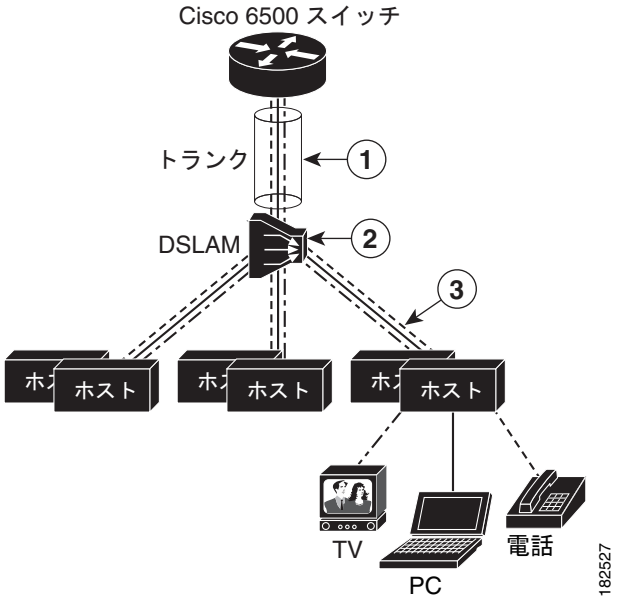
ホストを分離すると、サービス プロバイダーは同じセットのブロードバンド、またはメトロ イーサネット サービスを複数のエンド ユーザに配信する場合、1 セットの VLAN を使用できます。また、その VLAN 内でホスト同士が直接接続することもなくなります。たとえば、VLAN 10 を音声トラフィック、VLAN 20 をビデオ トラフィック、VLAN 30 をデータ トラフィックに使用できます。

スイッチが、デジタル加入者線アクセス マルチプレクサ（DSLAM）ギガビット イーサネット アグリゲータとして使われている場合、DSLAM は、複数の VLAN にデータを伝送できるトランク ポートを介してスイッチに接続されます。サービス プロバイダーは、1 つの物理ポートと 1 セットの VLAN を使って、サービスの同じセットを異なるエンド ユーザ（独立ホスト）に配信できます。それぞれの VLAN は個別のサービス（音声、ビデオ、データ）に使用できます。

図 27-1 に、スイッチから DSLAM に接続している複数のエンド ユーザにトリプルプレイ サービスを配信する例を示します。図における次の点に注意してください。

- スイッチと DSLAM 間の単一のトランク リンクによって、3 つの VLAN すべてのトラフィックが伝送されます。
- 仮想回線（VC）は、DSLAM から個別のエンド ユーザへ VLAN トラフィックを伝送します。

図 27-1　　VC から VLAN へのマッピング



1	トランク リンクは次の VLAN を伝送します。 • 音声 VLAN × 1 • ビデオ VLAN × 1 • データ VLAN × 1	2	DSLAM は、音声、ビデオ、およびデータ トラフィックを VLAN と VC の間にマッピングします。
		3	各 VC は、DSLAM と各ホスト間で音声、ビデオ、およびデータ トラフィックを伝送します。

トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）

プライベート ホスト機能は PACL を使い、プライベート ホスト用に設定された各ポートを通過するトラフィックのタイプを制限できます。ポートのモード（ポートでプライベート ホストをイネーブルにするときに指定）によって、ポートに適用される PACL のタイプが決まります。各タイプの PACL は、それぞれ異なるタイプのトラフィックのトラフィック フローを制限します（たとえば、コンテンツ サーバから独立ホスト、独立ホストからサーバ、独立ホスト間のトラフィックなど）。

次のリストで、プライベート ホスト機能で使用されるポート モードを説明します（図 27-2 を参照）。

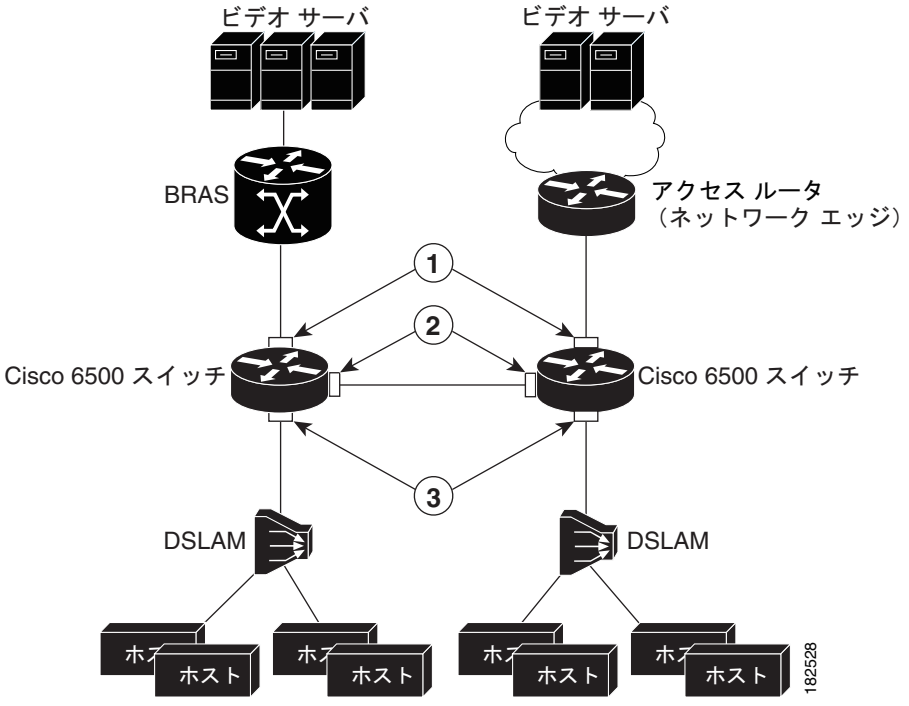
- 独立：エンド ユーザ（独立ホスト）が接続される DSLAM に接続されるポート。この場合ポートにおける VLAN 上のホストは、それぞれが独立している必要があります。このタイプのポートに接続されているホストは、アップストリーム デバイスだけにユニキャスト トラフィックを通過させることができます。
- 無差別：コア ネットワーク側か、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）デバイス側にあるポート、およびブロードバンド サービスを提供するマルチキャスト サーバ。
- 混合：スイッチを相互接続するポート。このタイプのポートは、スパニングツリー プロトコル（STP）の変更により、独立ポートとしても、無差別ポートとしても機能します。これらのポートは、アップストリーム デバイス（BRAS またはマルチキャスト サーバなど）へのユニキャスト トラフィックだけが可能です。

プライベート ホスト機能は、次の方法でトラフィックのフローを制限します。

- サービス プロバイダー ネットワークに入るブロードキャスト トラフィックは、BRAS およびマルチキャスト サーバ（ビデオ サーバなど）にリダイレクトされます。
- アクセス スイッチ（相互に接続されているスイッチ）間のユニキャスト トラフィックは、すべてブロックされます（BRAS またはマルチキャスト サーバに誘導されるものを除く）。
- Unknown Unicast Flood Blocking（UUFB; 不明なユニキャストフラッディングのブロック）機能は、DSLAM 側のポート上の不明なユニキャストのブロックに使用されます。

図 27-2 でプライベート ホストの設定で使用する各タイプのポート モード（独立、無差別、混合）を説明します。

図 27-2　プライベート ホストのポート タイプ（モード）



1	無差別ポート	BRAS からホストへのすべてのトラフィックを許可。
2	混合ポート	BRAS からのブロードキャスト トラフィックを許可。 ホストから無差別モード、および混合モードのポートへのブロードキャスト トラフィックをリダイレクト。 BRAS からホスト、およびホストから BRAS へのトラフィックを許可。 ホスト トラフィックへの他すべてのホストを拒否。
3	独立ポート	ホストから BRAS へのユニキャスト トラフィックだけを許可。ポート間のユニキャスト トラフィックをブロック。 ホストから BRAS へのすべてのブロードキャストをリダイレクト。 BRAS からのトラフィックを拒否（スプーフィング防止のため）。 マルチキャスト トラフィックを許可（IPv4 および IPv6）。

（注） このポート タイプの説明において、BRAS という用語は BRAS、マルチキャスト サーバ（ビデオ サーバなど）などのアップストリーム デバイス、またはこれらのデバイスへのアクセスを提供するコア ネットワーク デバイスを意味します。

ポート ACL

プライベート ホスト機能は、レイヤ 2 フォワーディングの制限をスイッチ ポートに課すために、ポート ACL（PACL）を数タイプ作成します。このソフトウェアは、ブロードバンド サービスと、これらのサービスを配信する独立ホストの VLAN ID を提供しているコンテンツ サーバの MAC アドレスに基づき、異なるタイプのプライベート ホスト ポート用に PACL を作成します。各プライベート ホスト ポートが動作するモードを指定すると、ポートのモード（独立、無差別、または混合）に基づいて、ソフトウェアによって適切な PACL がポートに適用されます。

次に、プライベート ホスト機能に使用される各タイプの PACL を示します。

独立ホスト PACL

独立ポート用 PACL の例：

```
deny host BRAS_MAC any
permit any host BRAS_MAC
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit any 0100.5E00.0000/0000.007F.FFFF
permit any 3333.0000.0000/000.FFFF.FFFF
deny any any
```

無差別ポート PACL

無差別ポート用 PACL の例：

```
permit host BRAS_MAC any
deny any any
```

混合ポート PACL

混合ポート用 PACL の例：

```
permit host BRAS_MAC ffff.ffff.ffff
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit host BRAS_MAC any
permit any host BRAS_MAC
deny any any
```

プライベート ホストのデフォルト設定

なし。

プライベート ホストの設定方法

設定の概要

1. Private Hosts 機能で使用するスイッチ ポート（インターフェイス）を決定します。トランキング スイッチ ポートまたはポートチャネル インターフェイスの機能を設定できます。プライベート ホストは、ポートチャネル インターフェイス上でイネーブルにする必要があります。この機能をメンバ ポート上でイネーブルにすることはできません。
2. 各ポート（インターフェイス）を標準、非プライベート ホスト サービス用に設定します。ポートのアクセス グループ モードをポート モード優先に設定します。この手順の VLAN 設定は、後で設定できます。
3. エンド ユーザにブロードバンド サービスを配信する VLAN または VLAN のセットを決定します。プライベート ホスト機能により、これらの VLAN におけるホスト間のレイヤ 2 分離が可能になります。
4. エンド ユーザ（独立ホスト）にブロードバンド サービスを提供するために使用するすべての BRAS とマルチキャスト サーバの MAC アドレスを識別します。

（注）　サーバがスイッチに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。

5. （任意）異なるセットの独立ホストに、異なるタイプのブロードバンド サービスを提供する場合は、複数の MAC および VLAN リストを作成します。
   - 各 MAC アドレス リストでは、特定のタイプのサービスを提供するサーバまたはサーバ セットを指定します。
   - 各 VLAN リストが、そのサービスを配信する独立ホストを識別します。

6. 無差別ポートを設定し、特定のサービス タイプ用のサーバと受信ホストを識別する MAC リストと VLAN リストを指定します。

（注）　異なるセットのホストに、異なるタイプのサービスを配信できるようにするには、複数の MAC と VLAN の組み合わせを指定できます。たとえば、xxxx.xxxx.xxxx の BRAS を使用して VLAN 20、25、および 30 で基本的なサービス セットを提供し、yyyy.yyyy.yyyy の BRAS を使用して VLAN 5、10、および 15 で高品質のサービス セットを提供できます。

7. プライベート ホストをグローバルにイネーブル化します。

8. 個々のポート（インターフェイス）でプライベート ホストをイネーブル化し、ポートの動作モードを指定します。ポート モードを決定するには、ポートがアップストリーム側（コンテンツ サーバ方向、またはコアネットワーク方向）か、またはダウンストリーム側（DSLAM および独立ホスト方向）か、または他のスイッチに接続されているか（通常、リング トポロジの場合）を判断する必要があります。「トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）」（P.27-5）を参照してください。

個別のポートで Private Hosts 機能をイネーブルにすると、スイッチでこの機能を実行する準備が整います。プライベート ホスト ソフトウェアは、ユーザが定義した MAC および VLAN リストを使用して、設定用の独立、無差別および混合モード PACL を作成します。次に、ソフトウェアが各プライベート ホストに適切な PACL を、ポート モードに基づいて適用します。

詳細設定手順

プライベート ホスト機能を設定するには、次の手順を実行します。次の手順は、プライベート ホストに使用するレイヤ 2 インターフェイスの設定がすでに済んでいることを前提としています。

（注）　トランキング スイッチ ポートまたは EtherChannel ポート上でだけ、プライベート ホストを設定できます。また、DSLAM とアップストリーム デバイスの間にあるすべてのスイッチで Private Hosts をイネーブルにする必要があります。

	コマンドまたはアクション	目的
ステップ 1	`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 2	`Router(config)# private-hosts mac-list mac_list_name mac_address [remark device-name | comment]`	ブロードバンド サービスの提供に使用する BRAS とマルチキャスト サーバを識別する MAC アドレス リストを作成します。 • *mac_list_name* は、このコンテンツ サーバのこのリストに割り当てる名前を指定します。 • *mac_address* は、特定のブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定します。 • **remark** を使用すると、この MAC リストに割り当てるデバイス名またはコメントをオプションで指定できます。 サービスを提供するために使用されるすべてのコンテンツ サーバの MAC アドレスを指定します。異なるタイプのサービスを異なるホストのセットに提供する場合は、特定のサービスを提供するサーバまたはサーバ セットごとに別々の MAC リストを作成します。 **（注）** サーバがスイッチに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。
ステップ 3	`Router(config)# private-hosts vlan-list vlan-IDs`	分離する必要があるホストの VLAN（*vlan-IDs*）リストを作成し、そのホストがブロードバンド サービスを受信できるようにします。 特定のサービスを異なるホストのセットに提供する場合は、別々の VLAN リストを作成します。それ以外の場合は、すべてのブロードバンド サービスがすべての独立ホストに提供されます。
ステップ 4	`Router(config)# private-hosts promiscuous mac-list-name [vlan-list vlan-IDs]`	ブロードバンドで使用するコンテンツ サーバ、およびサービスを配信するエンド ユーザ（独立ホスト）を識別します。 • *mac-list-name* は、特定のタイプのブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定する MAC アドレス リストの名前を指定します。 • *vlan-IDs* は、ホストが上記のサーバからサービスを受信する VLAN または VLAN のセットを指定します。VLAN リストを指定しない場合、ソフトウェアによりグローバル VLAN リスト（ステップ 3 で設定）が使用されます。 **（注）** 複数の MAC と VLAN の組み合わせを設定し、それぞれを特定のタイプのサービス用のサーバ、および受信ホストとして定義するために、このコマンドを複数回入力できます。
ステップ 5	`Router(config)# private-hosts`	スイッチ上でプライベート ホストをグローバルにイネーブル化します。

	コマンドまたはアクション	目的
ステップ 6	`Router(config)# interface interface`	Private Hosts に対してイネーブルにするトランキング スイッチ ポートまたは EtherChannel を選択します。
ステップ 7	`Router(config-if)# access-group mode prefer port`	トランク ポート上に既存の VACL または RACL があれば、無視するように指定します。
ステップ 8	`Router(config-if)# private-hosts mode {promiscuous | isolated | mixed}`	ポート上でプライベート ホストをイネーブル化します。次のキーワードのいずれかを使用して、ポートが動作するモードを定義します。 • **promiscuous**：無差別。ブロードバンド サーバ（BRAS、マルチキャスト、またはビデオ）か、サーバにアクセスを提供するコア ネットワーク デバイスに接続しているアップストリーム側のポート。 • **isolated**：独立。DSLAM に接続されているポート。 • **mixed**：他のスイッチに接続するポート（通常は、リング トポロジを使用）。 **（注）** プライベート ホストに使用される各ポートに対してこの手順を実行する必要があります。
ステップ 9	`Router(config-if)# end`	インターフェイスおよびグローバル 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。Private Hosts 設定が完了します。

設定例

次に、MAC アドレス リストおよび VLAN リストを作成し、VLAN 10、12、15、および 200 ～ 300 でホストを独立させる場合の例を示します。この例では、BRAS 側のポートは無差別に、ホストに接続している 2 つのポートは独立にしています。

```
Router# configure terminal
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose
Router(config)# private-hosts vlan-list 10,12,15,200-300
Router(config)# private-hosts promiscuous BRAS_list vlan-list 10,12,15,200-300
Router(config)# private-hosts
Router(config)# interface gig 4/2
Router(config-if)# private-hosts mode promiscuous
Router(config-if)# exit
Router(config)# interface gig 5/2
Router(config-if)# private-hosts mode isolated
Router(config-if)# exit
Router(config)# interface gig 5/3
Router(config-if)# private-hosts mode isolated
Router(config-if)# end
Router#
```

次に、プライベート ホストの独立ポートにおけるインターフェイスの設定例を示します。

```
Router# show run interface gig 5/2
Building configuration...

Current configuration : 200 bytes
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 access-group mode prefer port
 private-hosts mode isolated
end
```

次に、プライベート ホストの無差別ポートにおけるインターフェイスの設定例を示します。

```
Router# show run interface gig 4/2
Building configuration...

Current configuration : 189 bytes
!
interface GigabitEthernet4/2
 switchport
 switchport access vlan 200
 switchport mode access
 private-hosts mode promiscuous
end

private-hosts
private-hosts vlan-list 200
private-hosts promiscuous bras-list
private-hosts mac-list bras-list 0000.1111.1111 remark BRAS-SERVER
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する