CHAPTER 38

Private Hosts（PACL の使用）

この章では、Private Hosts 機能について説明します。この機能は、Cisco 7600 シリーズ ルータ用に Cisco IOS Release 12.2SRB で導入されています。この章の内容は、次のとおりです。

概要

Private Hosts 機能を使用すると、VLAN のホスト間での Layer 2（L2; レイヤ 2）の分離を行うことができます。Private Hosts は、現在は Cisco 7600 ルータで使用できないプライベート VLAN 独立トランク機能に代わるものとして使用できます。

世界各国のサービス プロバイダー（SP）は、単一の物理インターフェイス（銅製またはファイバ）でトリプル プレイ サービス（音声、ビデオ、およびデータ）を顧客に提供するよう求められています。通常、トリプル プレイ サービスは、3 つの異なる VLAN で各ユーザに配信されます。ただし、ビデオ トラフィック用の VLAN については、複数のエンド ユーザによって共有される場合もあります。

Private Hosts 機能の主な利点として、次の機能があります。

- 同じ VLAN ID を共有するホスト（加入者）間でのトラフィックの分離
- 異なる加入者間での VLAN ID の再利用（使用可能な 4096 VLAN の効率的な使用による VLAN スケーラビリティの向上）
- MAC スプーフィングの防止による Denial of Service（DoS; サービス拒絶）攻撃の防止

プライベート ホスト機能は、Port-based Access Control List（PACL; ポートベース アクセス コントロール リスト）を使用して、純粋なレイヤ 2 ドメイン内部の信頼できるポート上でのホスト間のレイヤ 2 分離を可能にします。PACL では、ルータ 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。

（注） Release 12.2SRB では、PACL は Private Hosts の一部としてだけサポートされます。独自の PACL は設定できません。代わりに、Private Hosts 設定に基づき、ルータにより PACL が作成されて適用されます。

以降のセクションでは、次の Private Hosts の概念について詳細に説明します。

VLAN でのホストの分離

通常、トリプル プレイ サービス（音声、ビデオ、およびデータ）は、3 つの異なる VLAN で各ユーザに配信されます。ただし、同じサービス セットの VLAN が複数のエンド ユーザ間で共有される場合もあります。たとえば、10 人のエンド ユーザすべてが同じサービス セットを受信する場合、Private Hosts を使用して、単一の VLAN セットで 10 人のエンド ユーザすべてにサービスを配信できます。ただし、VLAN を共有するには、サービス プロバイダーはレイヤ 2 で、ユーザ（ホスト）間でトラフィックを分離できる必要があります。

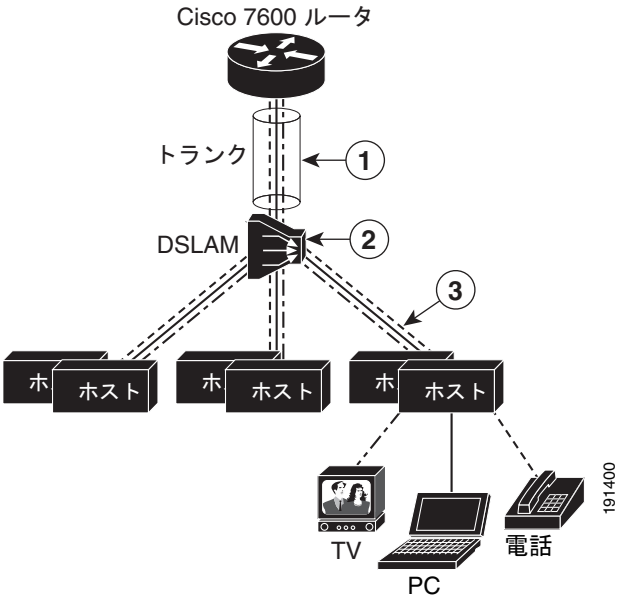
Private Hosts 機能を使用すると、VLAN のホスト（エンド ユーザ）間でのレイヤ 2 の分離を行うことができます。ホストを分離すると、サービス プロバイダーは同じセットのブロードバンド、またはメトロ イーサネット サービスを複数のエンド ユーザに配信する場合、1 セットの VLAN を使用できます。また、その VLAN 内でホスト同士が直接接続することもなくなります。たとえば、VLAN 10 を音声トラフィック、VLAN 20 をビデオ トラフィック、VLAN 30 をデータ トラフィックに使用できます。

Cisco 7600 ルータを DSLAM Gigabit Ethernet（GE; ギガビット イーサネット）集約器として使用する場合、DSLAM は複数の VLAN 向けにデータ伝送可能なトランク ポートを介してルータに接続されます。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 38-1 に、Cisco 7600 ルータから 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。この図では、次の点に注意してください。

- 単一のトランク リンク（ルータと DSLAM 間）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。
- 仮想回線によって、DSLAM から個々のエンド ユーザへ VLAN トラフィックが配信されます。

図 38-1　　VC から VLAN へのマッピング



A	トランク リンクによる伝送： • 音声 VLAN × 1 • ビデオ VLAN × 1 • データ VLAN × 1	B	DSLAM により、音声、ビデオ、およびデータ トラフィックは VLAN と VC 間でマッピングされます。
		C	個別の VC により、音声、ビデオ、およびデータ トラフィックは DSLAM と各ホスト間で伝送されます。

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）

Private Hosts 機能では、PACL を使用して、Private Hosts 用に設定された各ポートを通過できるトラフィックのタイプを制限します。ポートのモード（ポートで Private Hosts 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）。

次に、Private Hosts 機能で使用されるポート モードについて説明します（図 38-2 を参照）。

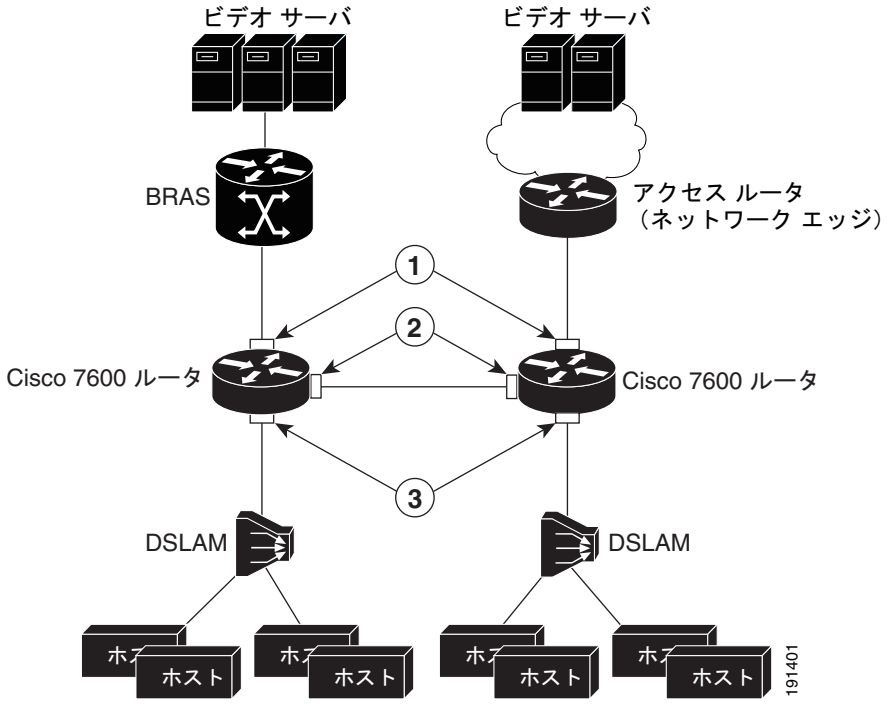
- 独立：エンド ユーザ（独立ホスト）が接続される DSLAM に接続されるポート。この場合ポートにおける VLAN 上のホストは、それぞれが独立している必要があります。このタイプのポートに接続されているホストは、アップストリーム デバイスだけにユニキャスト トラフィックを通過させることができます。
- 無差別：コア ネットワーク側か、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）デバイス側にあるポート、およびブロードバンド サービスを提供するマルチキャスト サーバ。
- 混合：Cisco 7600 ルータを相互接続するポート。これらのポートは、スパニングツリー プロトコル（STP）トポロジの変更に応じて、独立ポートまたは無差別ポートとして機能します。これらのポートでは、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）へのユニキャスト トラフィックだけが許可されます。

次に、Private Hosts によるトラフィック フローの制限方法の概要を示します。

- 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 ルータ（相互に接続された Cisco 7600 ルータ）間のすべてのユニキャスト トラフィックは、BRAS およびマルチキャスト サーバへのトラフィックを除き、ブロックされます。
- 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 38-2 に、Private Hosts 設定で使用されるさまざまなタイプのポート モード（独立、無差別、および混合）を示します。

図 38-2　プライベート ホストのポート タイプ（モード）



A	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します。
B	混合モード ポート	BRAS からのブロードキャスト トラフィックを許可します。 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します。 ホスト トラフィックへの他すべてのホストを拒否。
C	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します。ポート間のユニキャスト トラフィックをブロックします。 ホストから BRAS へのすべてのブロードキャスト トラフィックをリダイレクトします。 BRAS からのトラフィックを拒否します（スプーフィングを防止するため）。 マルチキャスト トラフィックを許可（IPv4 および IPv6）。

（注） 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）、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 デバイスなどのアップストリーム デバイスを表します。

ポート ACL

ルータ ポートにレイヤ 2 フォワーディング制約を課すために、Private Hosts ソフトウェアによって複数のタイプのポート ACL（PACL）が作成されます。それぞれのタイプの PACL により、特定のタイプのトラフィック（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）のトラフィック フローが制限されます。

このソフトウェアでは、ブロードバンド サービスを提供するコンテンツ サーバの MAC アドレスと、それらのサービスの提供先となる独立ホストの VLAN ID に基づいて、さまざまなタイプの Private Hosts ポート用の PACL が作成されます。各 Private Hosts 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、Private Hosts 機能で使用されるさまざまなタイプの PACL の例を示します。

独立ホスト PACL

次に、独立ポートの PACL の例を示します。

```
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

次に、無差別ポートの PACL の例を示します。

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

混合モード ポート PACL

次に、混合モード ポートの PACL の例を示します。

```
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
```

設定時の注意事項および制限事項

Cisco 7600 ルータで Private Hosts 機能を設定する際は、次の注意事項と制約事項に従ってください。

- ソフトウェアおよびハードウェアの要件
  - Cisco IOS Release 12.2SRB 以降
  - RSP720（PFC3C または PFC3CXL 搭載）、Sup720（PFC3B または PFC3BXL 搭載）、または Sup32
  - スイッチ ポートとして設定可能なファスト イーサネットまたはギガビット イーサネット（GE）インターフェイスを備えたラインカード（SIP-600、ESM-20、67xx LAN カードなど）でのサポート
    （SIP-400 および拡張 FlexWAN では Private Hosts はサポートされないことに注意してください）

- Private Hosts およびプライベート VLAN は、同一ポート（インターフェイス）上には設定できません。両方の機能をルータ上に共存させることはできますが、各機能を異なるポート上に設定する必要があります。
- Private Hosts はエンドツーエンド機能です。DSLAM とアップストリーム デバイス（BRAS やマルチキャスト サーバなど）の間にあるすべてのルータでイネーブルにする必要があります。
- 現在は、信頼できるポートだけを独立ポートとして設定できます。
- スイッチ ポート（802.1q または ISL トランク ポート）として設定されるレイヤ 2 インターフェイスでのサポート。
- ポートチャネル インターフェイス（Etherchannel、FastEtherchannel、および GigabitEtherchannel）でのサポート。Private Hosts 機能はポートチャネル インターフェイスでイネーブルにする必要があります。メンバー ポートでイネーブルにすることはできません。
- LAN ベース機能（DAI や DHCP スヌーピングなど）は Private Hosts のポートで機能的に共存しません。これは、Private Hosts 機能によって MAC ベースのルックアップがスイッチポートで適用されますが、VLAN ベースではないためです。つまり、Private Hosts の vlan-list と、DAI または DHCP スヌーピングの VLAN リストは、相互に排他的でなければならず、Private Hosts のスイッチポートで重複していてはなりません。

次のプロトコル独立型 MAC ACL 制約事項も適用されます。

- プロトコル独立型 MAC ACL フィルタリング用に次のインターフェイス タイプを設定できます。
  - 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。
- 許可されたトラフィックがブリッジされる場合、またはレイヤ 3 がハードウェアで PFC3 によってスイッチングされる場合は、マイクロフロー 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 MSFC によって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。

設定された VLAN のサブセットのみを備えたポートにプライベート ホストを適用する場合は、次の制約事項が適用されます。

表 38-1　PACL シナリオと制約事項

シナリオ	制限事項
Private-Host VLAN-list に関連付けられた Private-Host 対応ポート内の VLAN の場合	• IP トラフィックと非 IP トラフィックは mac-list 内に設定された MAC アドレスに基づく PACL に従うため、IP トラフィックと非 IP トラフィックの両方が許可または拒否されます。 • 12.2(SRD4) 以降は、Private Host VLAN-list に、相互接続（xconnect）が設定された VLAN を 1 つしか関連付けることができません。独立ポートから届いたトラフィックは PACL に従います。VLAN-list 内の別の VLAN に相互接続を設定しようとすると、拒否されます。同様に、相互接続が設定された VLAN がすでに VLAN-list に掲載されている場合は、相互接続が設定された VLAN を Private Host VLAN-list に追加しようとすると、拒否されます。 • 上記ケースでは、PACL によって許可されたトラフィックが相互接続経由でスイッチングされます。
Private-Host VLAN-list に関連付けられていない Private-Host 対応ポート内の VLAN の場合	• すべての非 IP トラフィックが PACL に従います。トラフィックは、Private Host mac-list 内に設定された MAC アドレスに基づいて許可または拒否されます。 • このような VLAN 上での IP トラフィックは PACL に従いません。 • このような VLAN に相互接続が設定されている場合は、IP トラフィックが PACL に従わずに相互接続にスイッチングされます。 • VLAN がレイヤ 3 ルーテッド（SVI）で、IP トラフィックがレイヤ 3 ルーテッドの場合は、ポート上のデフォルト ACL を通してすべてのパケットが拒否されます。ただし、L3 パケットは、CPU（MSFC）に転送され、そこでレート制限されます。 • VLAN が相互接続に関連付けられている場合は、PACL によってトラフィックが許可される場合にのみ、非 IP トラフィックが相互接続上でスイッチングされます。 • VLAN が **mac packet-classify** を使用して設定されている場合は、VLAN 上の IP トラフィックと非 IP トラフィックの両方が PACL に従います。

- 12.2(33) SRD4 以降は、次のプロトコルに依存しない MAC ACL 制約事項も適用されます。
  - Private Host 機能は、Private Host が設定された VLAN 上のすべてのトラフィックが、VLAN を共有する 2 人の加入者間で直接やり取りされないようにします。

- 1 つの VLAN が Private Host および相互接続と連動するようにシステムを設定することができます。
- 1 つの VLAN が相互接続と Private Host 用に設定されている場合は、その VLAN の相互接続が無差別モードになります。ただし、トラフィックがコア側からリレーされる場合は、設定された相互接続に対して ACL を適用することができません。
- MAC ACL 制約事項を適用しても、スケールやパフォーマンスは変化しません。
- Private Host では、VPLS サポートが 1 つの VLAN に限定されます。Private Host VLAN-list に VPLS VLAN（相互接続が設定された VLAN）が掲載されている場合は、別の VPLS VLAN を追加しようとすると、ブロックされます。同様に、VLAN-list 内のいずれかの VLAN に相互接続が設定されている場合は、そのリスト内の別の VLAN に相互接続を設定しようとすると、ブロックされます。

（注）　Release 12.2SRB では、PACL は Private Hosts の一部としてだけサポートされます。独自の PACL は設定できません。代わりに、Private Hosts 設定に基づき、ルータにより PACL が作成されて適用されます。

ACL の注意事項

アクセス コントロール リスト（ACL）には、次の設定時の注意事項および制約事項が適用されます。

- Private Hosts 機能の 12.2 (33) SRD4 リリースでは、プロトコルに依存しない MAC ACL が使用されます。
  Private Hosts 用に設定されたポートに IP ベースの ACL を適用しないでください。適用した場合、Private Hosts 機能は中断されます（ルータが Private Hosts MAC ACL をポートに適用できないため）。
- VLAN ACL（VACL）およびポート ACL は、同じインターフェイスには適用できません。
- Routing ACL（RACL; ルーティング ACL）および PACL は、同じインターフェイスには適用できません。ただし、別々のインターフェイスには適用することができます。

トランク ポート上の VLAN

VLAN には、次の注意事項および制約事項が適用されます。

- Private Hosts 用に設定されたトランク ポートを使用する VLAN で IGMP スヌーピングをイネーブルにすることができます。
- Private Hosts 用に設定されたトランク ポートを使用する VLAN で IP マルチキャストをイネーブルにすることはできません。
- 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することはできません。
- マルチキャスト ソースが無差別ポート上に存在している場合、マルチキャスト VLAN レジストレーション（MVR）機能は Private Hosts と共存できます。

他の機能との相互作用

Private Hosts 機能とルータで設定される他の機能との相互作用を次に示します。

- Private Hosts 機能は、MAC 制限、Unicast Flood Protection（UFP）、Unknown Unicast Flood Blocking（UUFB）などのレイヤ 2 ベースのサービスに影響しません。

- Private Hosts 機能は IGMP スヌーピングに影響しません。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ために、Private Hosts ソフトウェアによって multicast permit ステートメントが独立ホストの PACL に追加されます。この動作は自動的に行われるため、ユーザの操作は必要ありません。
- 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モード ポートでポート セキュリティ機能をイネーブルにすると、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）のソース ポートでの変更が制限される場合があります。
- アクセス ポート上でイネーブルにした場合は、802.1*x* が Private Hosts の影響を受けません。

スプーフィングからの保護

Private Hosts 機能では、MAC アドレス スプーフィングは防止されますが、カスタマー MAC または IP アドレスは確認されません。MAC アドレス スプーフィングを回避するために、Private Hosts 機能が行う処理は次のとおりです。

- BRAS およびマルチキャスト サーバのスタティック MAC アドレスを使用します。
- レイヤ 2（L2）転送テーブルでのラーニングをディセーブルにします。
- 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、ルータ ソフトウェアに通知します。ソフトウェアによって移動が確認され、L2 転送テーブルが更新されます。

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）からのマルチキャスト トラフィックは常に許可されます。また、Private Hosts 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、IGMP クエリーに応答し、目的のグループからトラフィックを受信できます。

ホストからのマルチキャスト トラフィックは、Private Hosts PACL によって廃棄されます。ただし、あるホストから発信されたマルチキャスト トラックを別のホストで受信する必要がある場合は、Private Hosts が PACL に *multicast permit* エントリを追加します。

Private Hosts の設定

ここでは、Cisco 7600 シリーズ ルータ上での Private Hosts 機能の設定およびこの機能の設定手順について説明します。

設定の概要

ここでは、Cisco 7600 ルータ上で Private Hosts 機能を設定するために実行する手順の概要について説明します。次のセクションで、詳細な設定手順を説明します。

1. Private Hosts 機能で使用するルータ ポート（インターフェイス）を決定します。この機能は、スイッチポート（802.1q または ISL トランク ポート）またはポートチャネル インターフェイス（Etherchannel、FastEtherchannel、および GigabitEtherchannel）で設定できます。Private Hosts 機能はポートチャネル インターフェイスでイネーブルにする必要があります。メンバー ポートでイネーブルにすることはできません。
2. Private Hosts 以外の通常のサービス用の各ポート（インターフェイス）を設定します。これ以降は、VLAN を設定できることに注意してください。
3. ブロードバンド サービスをエンド ユーザに提供するために使用する VLAN または VLAN セットを決定します。Private Hosts 機能を使用すると、これらの VLAN のホスト間でのレイヤ 2 の分離を行うことができます。
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されているすべての BRAS とマルチキャスト サーバの MAC アドレスを指定します。

（注）　サーバがルータ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）異なるタイプのブロードバンド サービスを異なる独立ホストのセットに提供する場合は、複数の MAC リストおよび 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 リストでは、そのサービスが提供される独立ホストを指定します。
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）　異なるタイプのサービスを異なるホストのセットに提供できるように、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. Private Hosts をグローバルにイネーブルにします。
8. Private Hosts を個別のポート（インターフェイス）でイネーブルにし、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 サーバまたはコア ネットワーク方向）か、ダウンストリーム側（DSLAM ホストと独立ホスト方向）か、別の Cisco 7600 ルータに接続されている（通常は、リング トポロジを使用）かを把握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.38-3）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、ルータでこの機能を実行する準備が整います。Private Hosts ソフトウェアによって、この設定の独立、無差別、および混合モード PACL を作成するために定義した MAC および VLAN リストが使用されます。次に、ポートのモードに応じて、適切な PACL が各 Private Hosts ポートに適用されます。

詳細設定手順

次の手順を実行して、Private Hosts 機能を設定します。これらの手順は、Private Hosts 用のレイヤ 2 インターフェイスをすでに設定していることを前提としています。次の表内のコマンドについては、「コマンド リファレンス」（P.38-13）を参照してください。

（注） Private Hosts は、スイッチポート（802.1q または ISL トランク ポート）または Etherchannel ポートだけで設定できます。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ルータで 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(config)# 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*`]`
	
	例：
	`Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose`
		ブロードバンド サービスを提供する BRAS およびマルチキャスト サーバを識別する MAC アドレスのリストを作成します。各項目の意味は次のとおりです。
		• *mac-list-name* は、このコンテンツ サーバ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） サーバがルータ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* **例：** `Router(config)# private-hosts vlan-list 10,12,15,200-300`	ホストがブロードバンド サービスを受信できるようにホストを分離する必要がある VLAN（*vlan-ids*）のリストを作成します。 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。

	コマンドまたはアクション	目的

ステップ 4	`Router(config)# private-hosts promiscuous mac-list-name [vlan-list vlan-ids]`
	
	例：
	`Router(config)# private-hosts promiscuous BRAS_list vlan-list 1,2,3`
		ブロードバンド サービスのコンテンツ サーバおよびサービスの提供先のエンド ユーザ（独立ホスト）を指定します。各項目の意味は次のとおりです。
		• *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 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）　このコマンドを複数回発行して、MAC と VLAN の組み合わせを複数設定できます。それぞれの組み合わせによって、特定のタイプのサービスのサーバおよび受信ホストが定義されます。

ステップ 5	`Router(config)# private-hosts`	Private Hosts をルータでグローバルにイネーブルにします。
ステップ 6	`Router(config)# interface interface`	Private Hosts に対してイネーブルにするスイッチポート（802.1Q または ISL トランク ポート）または Etherchannel ポートを選択します。

ステップ 7	`Router(config-if)# private-hosts mode {promiscuous | isolated | mixed}`
	
	例：
	`Router(config-if)# private-hosts mode isolated`
		Private Hosts をポートでイネーブルにします。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**：ブロードバンド サーバ（BRAS、マルチキャスト、またはビデオ）またはこれらのサーバへのアクセスを提供するコア ネットワーク デバイスに接続する、アップストリームに面したポート。
		• **isolated**：DSLAM に接続するポート。
		• **mixed**：他の Cisco 7600 ルータに接続するポート（通常は、リング トポロジを使用）。
		（注）　Private Hosts に使用される各ポートで、この手順を実行する必要があります。

ステップ 8	`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、Private Hosts 独立ポートのインターフェイス設定例を示します。

```
Router# show run int gi 5/2
Building configuration...

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

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 private-hosts mode isolated
end
```

次に、Private Hosts 無差別ポートのインターフェイス設定例を示します。

```
Router# show run int gi 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
```

コマンド リファレンス

ここでは、リリース 12.2(33) SRD4 で導入された Private Hosts 機能に関連するコマンドについて説明します。

- **private-hosts**
- **private-hosts mac-list**
- **private-hosts mode**
- **private-hosts promiscuous**
- **private-hosts vlan-list**
- **show fm private-hosts**
- **show private-hosts access-lists**
- **show private-hosts configuration**
- **show private-hosts interface configuration**
- **show private-hosts mac-list**
- **debug fm private-hosts**
- **debug private-hosts**

private-hosts

Private Hosts 機能をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで **private-hosts** コマンドを使用します。機能をディセーブルにするには、コマンドの **no** 形式を入力します。

private-hosts

no private-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、ルータ上の Private Hosts をイネーブルにします。次に、**private-hosts mode** コマンドを使用して、個別のインターフェイス（ポート）で Private Hosts をイネーブルにします。

例

次のコマンド例は、Private Hosts 機能をルータでグローバルにイネーブルにします。

```
Router(config)# private-hosts
```

関連コマンド

コマンド	説明
private-hosts mac list	ブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレス リストを作成します。
private-hosts mode	Private Hosts ポートの動作モードを指定します。
private-hosts promiscuous	ブロードバンド サービスのコンテンツ サーバおよび受信ホストを指定します。
private-hosts vlan-list	ホストを分離する必要がある VLAN を指定します。
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show **private-hosts interface configuration**	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts mac-list

独立ホストにブロードバンド サービスを提供し、MAC アドレス リストを作成するコンテンツ サーバを指定して、グローバル コンフィギュレーション モードで **private-hosts mac-list** コマンドを使用します。MAC アドレス リストからアドレスを削除して、そのデバイスを Private Hosts 機能のサービスを提供するコンテンツ サーバのリストから削除するには、コマンドの **no** 形式を入力します。

private-hosts mac-list *mac-list-name mac-address* **[remark** *device-name* **|** *comment***]**

no private-hosts mac-list *mac-list-name mac-address*

構文の説明

mac-list-name	アドレス リストに割り当てる名前（最大 80 文字）。
mac-address	Private Hosts 機能のブロードバンド サービスを提供する Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）、マルチキャスト サーバ、またはビデオ サーバの MAC アドレス。 **（注）** サーバがルータ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。
remark *device-name* | *comment*	（任意）この MAC アドレス 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します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Private Hosts 設定でブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレスのリストを作成します。

このコマンドを使用して、Private Hosts 機能のブロードバンド サービスを提供す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。*コンテンツ サーバ*は、ネットワーク内の独立ホストに Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）、マルチキャスト サーバ、またはビデオ サーバです。

すべてのコンテンツ サーバを 1 つの MAC アドレス リストに割り当てることができます。または、複数の MAC アドレス リストを作成して、それぞれで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 セットを提供するコンテンツ サーバを指定することもできます。Private Hosts 用の無差別ポートを設定する場合は、ブロードバンド サービスのサーバと受信ホストを指定する MAC アドレス リストおよび VLAN リストを指定します。

（注） MAC アドレス リストの最後のアドレスが削除されると、そのリストが自動的に削除されます。

例

この例では、アップストリーム BRAS の MAC アドレスを指定する BRAS_list という名前の MAC アドレス リストが作成されます。オプションの remark は、BRAS が San Jose にあることを示しています。

```
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_San-Jose
```

関連コマンド

コマンド	説明
show private-hosts mac-list	MAC アドレスのリストを表示します。このアドレスは、Private Hosts に対して定義されたブロードバンドを提供しているコンテンツ サーバを識別します。

private-hosts mode

Private Hosts をインターフェイス（ポート）でイネーブルにし、ポートの動作モードを指定するには、インターフェイス コンフィギュレーション モードで **private-hosts mode** コマンドを使用します。ポートで Private Hosts をディセーブルにするには、コマンドの **no** 形式を入力します。

private-hosts mode {**promiscuous** | **isolated** | **mixed**}

no private-hosts

構文の説明

promiscuous	ポートを無差別モードに設定します。このモードは、アップストリーム側のポートに使用します。これらは、ブロードバンド サービス（BRAS、マルチキャスト、またはビデオ）を提供するサーバ、または、これらのサーバへのアクセスを提供するコア ネットワーク デバイスにルータを接続するポートです。
isolated	ポートを独立モードに設定します。このモードは、独立ホストが接続される DSLAM 側のポートに使用します。
mixed	ポートを混合モードに設定します。このモードは、他の Cisco 7600 ルータに接続するポート（通常は、リング トポロジを使用）に使用します。このポートの動作は、スパニングツリー プロトコル（STP）トポロジに応じて変更されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。
mode のデフォルトは promiscuous です。

コマンド モード

インターフェイス コンフィギュレーション（スイッチポートまたはポートチャネル）

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**private-hosts** コマンドを発行して、ルータ上の Private Hosts 機能をグローバルにイネーブルにする必要があります。

このコマンドを使用して、Private Hosts 機能を個別のポートでイネーブルにし、ポートの動作モードを定義します。ポートのモードによって、ポートの通過が許可されるトラフィックのタイプを制限するためにポートに割り当てられる PACL のタイプが決定されます。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）。Private Hosts ポートに割り当てられているモードを表示するには、**show private-hosts interface configuration** コマンドを使用します。

例

次のコマンド例は、Private Hosts 機能をインターフェイス（ポート）でグローバルにイネーブルにし、ポートを独立モードに設定します。

```
Router(config-if)# private-hosts mode isolated
```

関連コマンド

コマンド	説明
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts promiscuous

ブロードバンド サービスを提供するコンテンツ サーバと受信ホストを指定するには、グローバル コンフィギュレーション モードで **private-hosts promiscuous** コマンドを使用します。無差別ポート設定を削除するには、コマンドの **no** 形式を入力します。

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]

no private-hosts promiscuous *mac-list-name*

構文の説明

mac-list-name	Private Hosts のブロードバンド サービスを提供するコンテンツ サーバ（BRAS、マルチキャスト、またはビデオ）を指定する MAC アドレス リストの名前。
vlan *vlan-ids*	（任意）MAC アドレス リストで指定されたコンテンツ サーバからホストがサービスを受信できる VLAN または VLAN セット。個別の VLAN をカンマで区切るか、VLAN の範囲を指定します（1,3,5,20-25 など）。 **（注）** VLAN リストを指定しない場合、グローバル VLAN リストが使用されます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

MAC アドレス リストと VLAN リストでは、ブロードバンド サービスを提供するコンテンツ サーバと受信ホストが定義されます。VLAN リストを指定しない場合、**private-hosts vlan-list** コマンドで作成されたグローバル VLAN リストが使用されます。

このコマンドを複数回発行して、MAC リストと VLAN リストの組み合わせを複数指定できます。それぞれの組み合わせによって、特定のタイプのサービスのサーバおよび受信ホストが定義されます。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。

例

次のコマンド例は、BRAS_list アドレス リストで定義されたコンテンツ サーバによって提供されるブロードバンド サービスが、VLAN 10、12、15、および 200 ～ 300 内の独立ホストに配信されるように設定します。

```
Router(config)# private-hosts promiscuous BRAS_list vlan 10,12,15,200-300
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts vlan-list

相互にホストを分離する必要のある VLAN を特定して（VLAN を使用してブロードバンド サービスを提供するため）、グローバル コンフィギュレーション モードで **private-hosts vlan-list** コマンドを使用します。ホストの分離が必要な VLAN のリストから VLAN を削除するには、コマンドの **no** 形式を入力します。

private-hosts vlan-list *vlan-ids*

no private-hosts vlan-list *vlan-ids*

構文の説明

vlan-ids	ホストを相互に分離する必要がある VLAN のリスト。個別の VLAN をカンマで区切るか、VLAN の範囲を指定します（1,3,5,20-25 など）。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Private Hosts 機能によってホストを分離する必要がある VLAN のリストを作成します。VLAN リストには、複数のエンド 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のすべての VLAN が含まれている必要があります。

異なるタイプのブロードバンド サービスを異なるホストのセットに提供する場合は、複数の VLAN リストと複数の MAC アドレス リストを作成できます。無差別ポートを設定する場合は、MAC リストと VLAN リストのさまざまな組み合わせを指定して、サービスのタイプごとにコンテンツ サーバと受信ホストを指定できます。

無差別ポートを設定するときに VLAN リストを指定しない場合、このコマンドで作成されたグローバル VLAN リストが使用されます。

（注） Private Hosts 機能によって、VLAN リストに含まれているすべての VLAN 内のホストが分離されます。したがって、ブロードバンド サービスを提供するために使用されている VLAN だけを VLAN リストに含める必要があります。

例

このコマンドは、Private Hosts 機能を設定して VLAN 10、12、15、および 200 ～ 300 のホストを分離します。

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。

show fm private-hosts

Private Hosts 機能マネージャに関する情報を表示するには、特権 EXEC モードで **show fm private-hosts** コマンドを実行します。

show fm private-hosts {**all** | **interface** *intf*}

構文の説明

all	Private Hosts 用に設定されているすべてのインターフェイスの機能マネージャ情報を表示します。
interface *intf*	機能マネージャ情報を表示するインターフェイスを指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show fm private-hosts interface GigabitEthernet 1/2
--------------------------------------------------------------------------------
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
================================================================================

---------------------------------------------------------------
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
---------------------------------------------------------------
Indx - VMR index      T     - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo  - Ethernet Code
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

---------------------------------------------------------------
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
---------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.1111.4001 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
```

```
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V ffff.ffff.ffff 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0100.5e00.0000 0000.0000.0000    0 0
      M ffff.ff80.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 3333.0000.0000 0000.0000.0000    0 0
      M ffff.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 3    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT


Interfaces using this pvt host feature in ingress dir.:
-------------------------------------------------
  Interfaces (I/E = Ingress/Egress)

Router#
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show **private-hosts interface configuration**	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts access-lists

Private Hosts 設定に関するアクセス リストを表示するには、特権 EXEC モードで **show private-hosts access-lists** コマンドを実行します。

show private-hosts access-lists

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、カスタマイズされた設定に関する Private Hosts アクセス リストを表示する例を示します。

```
Router# show private-hosts access-lists

Promiscuous ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny     Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Isolated ACLs
Action Deny     Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Mixed ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Router#
```

関連コマンド

コマンド	説明
show fm private-hosts	Private Hosts 機能マネージャに関する情報を表示します。
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts configuration

ルータの Private Hosts 設定に関する情報を表示するには、特権 EXEC モードで **show private-hosts configuration** コマンドを実行します。

show private-hosts configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show private-hosts configuration

    Private hosts enabled. BR INDEX 6 State 0000000F
    Privated hosts vlans lists:
    200
    Privated promiscuous MAC configuration:
    A '*' mark behind the mac list indicates non-existant mac-list
    -------------------------------------------------------------------------------
    MAC-list                       VLAN list
    -------------------------------------------------------------------------------
    bras-list                     *** Uses the isolated vlans (if any) ***
```

関連コマンド

コマンド	説明
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts interface configuration

個別のインターフェイス（ポート）の Private Hosts 設定に関する情報を表示するには、特権 EXEC モードで **show private-hosts interface configuration** コマンドを実行します。

show private-hosts interface configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show private-hosts interface configuration

    Private hosts enabled
    Debug Events: 0 Acl: 0 API: 0
    Promiscuous interface list
    --------------------------
    GigabitEthernet4/2
    Isolated interface list
    -------------------------
    GigabitEthernet5/2
    Mixed mode interface list
    -------------------------
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。

show private-hosts mac-list

Private Hosts に対して定義された MAC アドレス リストの内容を表示するには、特権 EXEC モードで **show private-hosts mac-list** コマンドを実行します。

show private-hosts mac-list [*list-name*]

構文の説明

list-name	（任意）内容を表示する MAC アドレス リストの名前。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show private-hosts mac-list

   MAC-List: bras-list
   ----------------------------------------------------------------------
   MAC address    Description
   ----------------------------------------------------------------------
   0000.1111.1111 BRAS-SERVER
```

関連コマンド

コマンド	説明
private-hosts mac-list	ブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレス リストを作成します。

debug fm private-hosts

Private Hosts 機能マネージャに関するデバッグ メッセージをイネーブルにするには、特権 EXEC モードで **debug fm private-hosts** コマンドを実行します。

debug fm private-hosts {**all** | **vmr** | **unusual** | **events**}

構文の説明

all	すべての Private Hosts エラーおよびイベントに関するデバッグ メッセージをイネーブルにします。
vmr	マルチキャスト VLAN レジストレーション（MVR）機能に関するデバッグ メッセージをイネーブルにします。
unusual	予期せぬ Private Hosts 動作に関するデバッグ メッセージをイネーブルにします。
events	Private Hosts イベントに関するデバッグ メッセージをイネーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# debug fm private-hosts all
fm private-hosts vmr debugging is on
fm private-hosts unusual debugging is on
fm private-hosts events debugging is on
Router#
```

関連コマンド

コマンド	説明
debug private-hosts	Private Hosts に関するデバッグ メッセージをイネーブルにします。

debug private-hosts

Private Hosts 機能に関するデバッグ メッセージをイネーブルにするには、特権 EXEC モードで **debug private-hosts** コマンドを実行します。

debug private-hosts {**all** | **events** | **acl** | **api**}

構文の説明

all	すべての Private Hosts エラーおよびイベントに関するデバッグ メッセージをイネーブルにします。
events	Private Hosts イベントに伴う問題に関するデバッグ メッセージをイネーブルにします。
acl	ACL に伴う問題およびイベントに関するデバッグ メッセージをイネーブルにします。
api	アプリケーション プログラミング インターフェイスに伴う問題に関するデバッグ メッセージをイネーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# debug private-hosts all
private-hosts events debugging is on
private-hosts api debugging is on
private-hosts acl debugging is on
Router#
```

関連コマンド

コマンド	説明
debug fm private-hosts	Private Hosts 機能マネージャに関するデバッグ メッセージをイネーブルにします。