CHAPTER 27

IP ソース ガードの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。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。

プラットフォームのサポートおよびシスコ 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。

IP ソース ガードの前提条件

- スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がレイヤ 2 アクセス ポート上で使用される場合にも適用されます。

IP ソース ガードの制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- IP ソース ガード（IPSG）は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。
- スタティック ホストの IPSG は、アップリンク ポートまたはトランク ポートでは使用しないでください。

IP ソース ガードの概要

IP ソース ガード

IPSG は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド レイヤ 2 インターフェイスでの IP トラフィックを制限するセキュリティ機能です。IPSG を使用して、ホストが、そのネイバーの IP アドレスの使用を試みた場合のトラフィック攻撃を防ぐことができます。

信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合は、IPSG をイネーブルにできます。インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。ポート アクセス コントロール リスト（ACL）は、このインターフェイスに適用されます。ポート ACL は、IP ソース バインディング テーブルに送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他のトラフィックはすべて拒否します。

（注）　ポート ACL は、同じインターフェイスに影響を与えるその他のルータ ACL や VLAN マップよりも優先されます。

IP ソース バインディング テーブル バインディングは、DHCP スヌーピングにより学習されるか、または手動で設定されます（スタティック IP ソース バインディング）。このテーブルのエントリはすべて、MAC アドレスと VLAN 番号が関連付けられた IP アドレスを持ちます。スイッチは、IPSG がイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

送信元 IP アドレスのフィルタリング

IPSG でこのオプションがイネーブルにされている場合、IP トラフィックは、送信元 IP アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP が DHCP スヌーピング バインディング データベースのエントリ、または IP ソース バインディング テーブルのバインディングと一致する場合に、IP トラフィックを転送します。

インターフェイス上で、DHCP スヌーピング バインディング、またはスタティック IP ソース バインディングが追加、変更、または削除された場合、スイッチは IP ソース バインディングの変更を使用して、ポート ACL を変更し、このポート ACL をインターフェイスに再度適用します。

IP ソース バインディング（DHCP スヌーピングにより動的に学習された、または手動で設定されたもの）が設定されていないインターフェイス上で IPSG をイネーブルにした場合、スイッチはこのインターフェイス上で IP トラフィックすべてを拒否するポート ACL を作成し、適用します。IPSG をディセーブルにした場合、スイッチはインターフェイスからポート ACL を削除します。

送信元 IP および MAC アドレス フィルタリング

IP トラフィックは、送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスと MAC アドレスが IP ソース バインディング テーブルのエントリと一致する場合だけ、トラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP トラフィックと非 IP トラフィックをフィルタリングします。IP パケット、または非 IP パケットの送信元 MAC アドレスが有効な IP ソース バインディングと一致する場合、スイッチはこのパケットを転送します。DHCP パケットを除き、その他の種類のパケットはすべて、スイッチによりドロップされます。

スイッチは、送信元 MAC アドレスのフィルタリングにポート セキュリティを使用します。ポート セキュリティ違反が発生した場合、インターフェイスはシャットダウンします。

スタティック ホスト用 IP ソース ガード

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存していまます。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルで使用できる DHCP によって割り当てられた IP アドレスを受信すると、同じエントリが IP デバイス トラッキング テーブルで学習されます。**show ip device tracking all** EXEC コマンドを入力する場合、IP デバイス トラッキング テーブルでエントリが ACTIVE として表示されます。

(注) 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソース アドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガード設定時の注意事項

- IP ソース ガードは、デフォルトではディセーブルに設定されています。
- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-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、次のエラー メッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

（注）　IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスの DHCP スヌーピングとポート セキュリティをイネーブルにする必要があります。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力して、DHCP サーバに確実に Option 82 をサポートさせる必要もあります。MAC アドレス フィルタリングとともに IP ソース ガードをイネーブルにした場合、DHCP ホストによりリースが認可されるまで、このホストの MAC アドレスは学習されません。サーバからホストにパケットを転送する場合、DHCP スヌーピングは Option 82 データを使用して、ホスト ポートを識別します。
- プライベート VLAN が設定されているインターフェイスに IP ソース ガードを設定した場合、ポート セキュリティはサポートされません。
- EtherChannels では、IP ソース ガードはサポートされません。
- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- Ternary Content Addressable Memory（TCAM）エントリの数が最大値を超えた場合、CPU の使用率は増加します。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

	コマンド	目的
ステップ 1	**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	**interface** *interface-id*	設定するインターフェイスを指定して、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。

	コマンド	目的
ステップ 3	**ip verify source** または **ip verify source port-security**	送信元 IP アドレスのフィルタリングによる IPSG をイネーブルにします。 送信元 IP アドレスと MAC アドレスのフィルタリングによる IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して IPSG とポート セキュリティの両方をイネーブルにする場合は、次の 2 つの警告があります。 • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 • DHCP パケットの MAC アドレスが、セキュア アドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュア アドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 4	**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。
ステップ 5	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **inteface** *interface-id*	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

	コマンド	目的
ステップ 1	**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	**ip device tracking**	IP ホスト テーブルを開き、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	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	**switchport mode access**	アクセスとしてポートを設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートに VLAN を設定します。

	コマンド	目的
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングとともにスタティック ホスト用 IPSG をイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して、IPSG とポート セキュリティの両方をイネーブルにする場合、 • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 • DHCP パケットの MAC アドレスが、セキュア アドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュア アドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 7	**ip device tracking maximum** *number*	そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートに対する MAC アドレスの最大値を設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip verify source interface** *interface-id*	設定を確認し、スタティック ホストの IPSG の許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイス上の指定ホストの IP/MAC バインディングを表示して、設定を確認します。 • **all active**：アクティブな IP または MAC バインディング エントリだけを表示します。 • **all inactive**：非アクティブな IP または MAC バインディング エントリだけを表示します。 • **all**：アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します。

プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定

	コマンド	目的
ステップ 1	**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	目的
ステップ 2	**vlan** *vlan-id1*	VLAN 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	**private-vlan primary**	プライマリ VLAN をプライベート VLAN ポート上に設定します。
ステップ 4	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 5	**vlan** *vlan-id2*	別の VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 6	**private-vlan isolated**	独立 VLAN をプライベート VLAN ポート上に設定します。
ステップ 7	**exit**	VLAN 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	**vlan** *vlan-id1*	コンフィギュレーション VLAN モードを開始します。
ステップ 9	**private-vlan association 201**	VLAN を独立プライベート VLAN ポートに関連付けます。
ステップ 10	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 11	**interface fastEthernet** *interface-id*	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	**switchport mode private-vlan host**	（任意）ポートをプライベート VLAN ホストとして設定します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）このポートに、対応するプライベート VLAN を関連付けます。
ステップ 14	**ip device tracking maximum** *number*	このポートに対して IP デバイス トラッキング テーブルに保持できるスタティック IP の数の最大値を設定します。 最大値は 10 です。 **（注）** スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポート上のスタティック ホストの IPSG と MAC アドレス フィルタリングをアクティブにします。
ステップ 16	**end**	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 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IPSG の設定を確認し、スタティック ホストの IPSG の許可 ACL を表示します。

IP ソース ガードのモニタリングおよびメンテナンス

コマンド	目的
show ip device tracking	すべてのインターフェイスに対してアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチ上の IP ソース バインディングを表示します。
show ip verify source	スイッチ上の IP ソース ガード設定を表示します。
copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

IP ソース ガードの設定例

送信元 IP アドレスと MAC アドレスのフィルタリングによる IPSG のイネーブル化：例

次に、送信元 IP および MAC フィルタリングにより VLAN 10 および 11 で IPSG をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/1
Switch(config)# end
```

スタティック ホストによる IPSG のディセーブル化：例

次に、インターフェイス上でスタティック ホストを使って IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

スタティック ホストの IPSG のイネーブル化：例

次に、ポート上でスタティック ホストを使って IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポートで IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP-MAC バインディングを確認してから、このインターフェイス上で上限に達したバインディングの数を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

IP または MAC バインディング エントリの表示：例

この例は、すべてのインターフェイスに対する IP または MAC バインディング エントリをすべて表示します。CLI はアクティブ エントリと非アクティブ エントリの両方を表示します。インターフェイスでホストが学習されると、この新しいエントリは、アクティブとマークされます。このホストをこのインターフェイスから切断し、別のインターフェイスに接続すると、ホストを検出すると同時に、新しい IP または MAC バインディング エントリがアクティブとして表示されます。以前のインターフェイスでは、このホストに対する古いエントリが非アクティブとマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

```
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

この例は、すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリをすべて表示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
```

この例は、すべてのインターフェイスに対する非アクティブな IP または MAC バインディング エントリをすべて表示します。このホストはまず、GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 で移動されます。GigabitEthernet 0/1 で学習された IP または MAC バインディング エントリは非アクティブとマークされます。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

この例は、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの総数を表示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
---------------------------------------------------------------------
  Interface          Maximum Limit          Number of Entries
---------------------------------------------------------------------
Gi0/3                 5
```

スタティック ホストの IPSG のイネーブル化：例

次に、プライベート VLAN ホスト ポート上でスタティック ホストの IPSG と IP フィルタをイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet0/3        ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3        ACTIVE
```

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合は、バインディングにはプライマリ VLAN ID が関連付けられます。この例では、プライマリ VLAN ID である 200 が表に表示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3   ip trk       active       40.1.1.22                           201
```

この出力からは、5 つの有効な IP-MAC バインディングはプライマリとセカンダリの両方の VLAN 上にあることがわかります。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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。	—