ポート セキュリティ

（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

ポート セキュリティの前提条件

なし。

ポート セキュリティの制約事項

- ポート セキュリティがデフォルト設定の場合に、errdisable ステートからすべてのセキュア ポートを回復させるには、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力します。または、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動でセキュア ポートを再びイネーブルに戻すことができます。
- ダイナミックに学習されたすべてのセキュア アドレスを消去するには、**clear port-security dynamic** グローバル コンフィギュレーション コマンドを入力します。
- 無許可の MAC アドレスは、特定のビット セットとともに学習されます。このビット セットにより、このアドレスから送信されるトラフィック、およびこのアドレス宛てに送信されるトラフィックはいずれもドロップされます。**show mac-address-table** コマンドを使用すると、無許可の MAC アドレスを表示できますが、ビット ステートは表示されません。（CSCeb76844）。
- スティッキ MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、起動またはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。
- ポート セキュリティは、Private VLAN（PVLAN; プライベート VLAN）ポートをサポートします。
- ポート セキュリティは、IEEE 802.1Q トンネル ポートをサポートします。
- ポート セキュリティは、スイッチド ポート アナライザ（SPAN）宛先ポートをサポートしません。
- ポート セキュリティは、EtherChannel ポートチャネル インターフェイスへのアクセスおよびトランキングをサポートします。
- ポート セキュリティと 802.1X ポートベース認証は同じポート上に設定できます。
- ポート セキュリティは、非交渉トランクをサポートします。
  - ポート セキュリティは、次のコマンドで設定したトランクだけをサポートします。

    switchport
    switchport trunk encapsulation
    switchport mode trunk
    switchport nonegotiate

  - セキュア アクセス ポートをトランクとして再設定すると、ポート セキュリティは、アクセス VLAN でダイナミックに学習されたこのポートのすべてのスティッキおよびスタティック セキュア アドレスを、トランクのネイティブ VLAN 上のスティッキまたはスタティック セキュア アドレスに変換します。ポート セキュリティによって、アクセス ポートの音声 VLAN 上のすべてのセキュア アドレスが削除されます。
  - セキュア トランクをアクセス ポートとして再設定すると、ポート セキュリティは、ネイティブ VLAN で学習されたすべてのスティッキおよびスタティック アドレスを、アクセス ポートのアクセス VLAN で学習されたアドレスに変換します。ポート セキュリティによって、ネイティブ VLAN 以外の VLAN で学習されたすべてのアドレスが削除されます。

（注） ポート セキュリティは、**switchport trunk native vlan** コマンドで設定した VLAN ID を使用します。

- 隣接スイッチ間で実行されている冗長リンクがある場合は、これらのスイッチに接続されているポートでポート セキュリティをイネーブルにする際に注意が必要です。これは、ポート セキュリティ違反が原因でポート セキュリティによってポートが errdisable に設定されるためです。

ポート セキュリティについて

ダイナミックに学習される MAC アドレスとスタティック MAC アドレスによるポート セキュリティ

ダイナミックに学習される MAC アドレス、およびスタティック MAC アドレスを使用したポート セキュリティでは、ポートへのトラフィック送信を許可する MAC アドレスを制限することで、ポートの入力トラフィックを制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは、定義されたアドレスのグループ外に送信元アドレスがある入力トラフィックを転送しません。セキュア MAC アドレスの数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されているデバイスはそのポートの全帯域を使用できます。

次のいずれかの場合に、セキュリティ違反が発生します。

- ポート セキュリティは、セキュア MAC アドレスがセキュア ポートで最大数に達した場合に、識別されたどのセキュア MAC アドレスとも入力トラフィックの送信元 MAC アドレスが異なると、設定された違反モードを適用します。
- あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つトラフィックが、同一 VLAN 内の別のセキュア ポートにアクセスしようとすると、設定された違反モードが適用されます。

（注） 特定のセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同一 VLAN 上の別のポートでポート セキュリティがセキュア MAC アドレスを検出したときに発生する一連のイベントは、MAC 移動の違反と呼ばれます。

違反モードの詳細については、「ポートでのポート セキュリティ違反モードの設定」（P.78-6）を参照してください。

ポートにセキュア MAC アドレスの最大数を設定すると、ポート セキュリティによって、次のいずれかの方法でアドレス テーブルにセキュア アドレスが組み込まれます。

- すべてのセキュア MAC アドレスを、**switchport port-security mac-address** *mac_address* 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スタティックに設定できます。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定するようにすることができます。
- アドレス数をいくつかスタティックに設定し、残りのアドレスがダイナミックに設定されるようにすることができます。

ポートがリンクダウン状態になると、ダイナミックに学習されたアドレスはすべて削除されます。

起動、リロード、またはリンクダウン状態のあとは、ポートが入力トラフィックを受信するまで、ポート セキュリティは、ダイナミックに学習された MAC アドレスをアドレス テーブルに読み込みません。

最大数のセキュア MAC アドレスがアドレス テーブルに追加された時点で、アドレス テーブルにはない MAC アドレスからのトラフィックをポートが受信すると、セキュリティ違反となります。

protect、restrict、または shutdown の違反モードのいずれかにポートを設定できます。「ポート セキュリティの設定方法」（P.78-5）を参照してください。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

スティッキ MAC アドレスによるポート セキュリティ

スティッキ MAC アドレスを使用するポート セキュリティには、スタティック MAC アドレスによるポート セキュリティと同様の多数の利点がありますが、さらに、スティッキ MAC アドレスはダイナミックに学習できます。スティッキ MAC アドレスを使用したポート セキュリティでは、リンクダウン状態の発生中も、ダイナミックに学習された MAC アドレスを維持します。

write memory または **copy running-config startup-config** コマンドを入力すると、スティッキ MAC アドレスによるポート セキュリティは、ダイナミックに学習された MAC アドレスを startup-config ファイルに保存します。したがって、起動後または再起動後に、ポートが入力トラフィックからアドレスを学習する必要がありません。

IP Phone でのポート セキュリティ

図 78-1　　IP Phone を介して接続した装置

装置はスイッチに直接接続されていないため、スイッチでは、装置の接続が切断されている場合に、ポート リンクが失われていることを物理的に検出できません。最近の Cisco IP Phone は、Cisco Discovery Protocol（CDP）でホストの存在を示す Type Length Value（TLV）を送信して、接続されている装置のポートのリンク ステートの変更をスイッチに通知します。スイッチはホスト存在 TLV を認識します。ポート セキュリティでは、IP Phone のデータ ポートでのリンク ダウンを知らせる、ホストの存在を示す TLV 通知を受け取るとすぐに、スタティック MAC アドレス、スティッキ MAC アドレス、およびダイナミックに学習された MAC アドレスがすべてアドレス テーブルから削除されます。削除されたアドレスは、ダイナミックに学習されるかまたは設定された場合に限り、再び追加されます。

デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ディセーブル

機能	デフォルト設定
セキュア MAC アドレスの最大数	1.
違反モード	shutdown。セキュア MAC アドレスが最大数を超過した場合、ポートはシャットダウンし、SNMP トラップ通知が送信されます。

ポート セキュリティの設定方法

ポート セキュリティのイネーブル化

トランクでのポート セキュリティのイネーブル化

ポート セキュリティは、非交渉トランクをサポートします。

注意　セキュア アドレス数はデフォルトで 1 であり、違反に対するデフォルト アクションはポートのシャットダウンであるため、トランクでポート セキュリティをイネーブルにする前に、このポートのセキュア MAC アドレスの最大数を設定します（「ポートでのセキュア MAC アドレスの最大数の設定」（P.78-7）を参照）。

トランクでポート セキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# switchport`	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	カプセル化を 802.1Q として設定します。
ステップ 4	`Router(config-if)# switchport mode trunk`	無条件にポートをトランクに設定します。
ステップ 5	`Router(config-if)# switchport nonegotiate`	DTP を使用しないようにトランクを設定します。
ステップ 6	`Router(config-if)# switchport port-security`	トランクでポート セキュリティをイネーブルにします。
ステップ 7	`Router(config-if)# do show port-security interface type slot/port | include Port Security`	設定を確認します。

次に、ギガビット イーサネット ポート 5/36 を非交渉トランクとして設定し、ポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/36 | include Port
Security
Port Security              : Enabled
```

アクセス ポートでのポート セキュリティのイネーブル化

アクセス ポートでポート セキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定するインターフェイスを選択します。 **（注）** ポートは、トンネル ポートまたは PVLAN ポートとして使用できます。
ステップ 2	Router(config-if)# **switchport**	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	Router(config-if)# **switchport mode access**	ポートをレイヤ 2 アクセス ポートとして設定します。 **（注）** デフォルト モード（dynamic desirable）のポートは、セキュア ポートとして設定できません。
ステップ 4	Router(config-if)# **switchport port-security**	ポートのポート セキュリティをイネーブルにします。
ステップ 5	Router(config-if)# **do show port-security interface** *type slot/port* **| include Port Security**	設定を確認します。

次に、ギガビット イーサネット ポート 5/12 でポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Port Security
Port Security              : Enabled
```

ポートでのポート セキュリティ違反モードの設定

ポートでポート セキュリティの違反モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定する LAN ポートを選択します。

	コマンド	目的
ステップ 2	`Router(config-if)# switchport port-security violation {protect | restrict | shutdown}`	（任意）違反モード、およびセキュリティ違反が検出されたときのアクションを設定します。
ステップ 3	`Router(config-if)# do show port-security interface type slot/port | include violation_mode`	設定を確認します。*violation_mode* の値は、**protect**、**restrict**、または **shutdown** です。

- **protect**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、PFC は送信元アドレスが不明なパケットをドロップします。
- **restrict**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、PFC は送信元アドレスが不明なパケットをドロップし、Security Violation カウンタを増分させます。
- **shutdown**：インターフェイスをただちに errordisable ステートにして、SNMP トラップ通知を送信します。

（注） errdisable ステートからセキュア ポートを回復するには、**errdisable recovery cause** *violation_mode* グローバル コンフィギュレーション コマンドを入力します。または、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動でセキュア ポートを再びイネーブルに戻すことができます。

次に、ギガビット イーサネット ポート 5/12 のセキュリティ違反モードを protect に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Protect
Violation Mode             : Protect
```

次に、ギガビット イーサネット ポート 5/12 のセキュリティ違反モードを restrict に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Restrict
Violation Mode             : Restrict
```

ポートでのセキュア MAC アドレスの最大数の設定

セキュア MAC アドレスの最大数をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# switchport port-security maximum number_of_addresses vlan {vlan_ID | vlan_range}`	ポートに対し、セキュア MAC アドレスの最大数を設定します（デフォルトは 1）。 **（注）** VLAN ごとの設定は、トランクだけでサポートされます。

- *number_of_addresses* の有効範囲は 1 ～ 4,097 です。
- ポート セキュリティは、トランクをサポートします。
  - トランクでは、トランクおよびトランク上のすべての VLAN に対して、セキュア MAC アドレスの最大数を設定できます。
  - セキュア MAC アドレスの最大数は、1 つの VLAN、または特定の VLAN 範囲に対して設定できます。
  - 特定の VLAN 範囲は、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、ギガビット イーサネット ポート 5/12 に対し、セキュア MAC アドレスの最大数を 64 に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

スティッキ MAC アドレスによるポート セキュリティのポートでのイネーブル化

スティッキ MAC アドレスによるポート セキュリティをポートでイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **switchport port-security mac-address sticky**	スティッキ MAC アドレスによるポート セキュリティをポートでイネーブルにします。

- **switchport port-security mac-address sticky** コマンドを入力すると、次のようになります。
  - ポートでダイナミックに学習されたすべてのセキュア MAC アドレスは、スティッキ セキュア MAC アドレスに変換されます。
  - スタティックなセキュア MAC アドレスは、スティッキ MAC アドレスに変換されません。
  - 音声 VLAN でダイナミックに学習されたセキュア MAC アドレスは、スティッキ MAC アドレスに変換されません。
  - ダイナミックに学習された新規のセキュア MAC アドレスは、スティッキ アドレスとなります。
- **no switchport port-security mac-address sticky** コマンドを入力すると、ポート上のすべてのスティッキ セキュア MAC アドレスは、ダイナミックなセキュア MAC アドレスに変換されます。

- スティッキ MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、起動またはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。

次に、スティッキ MAC アドレスによるポート セキュリティをギガビット イーサネット ポート 5/12 でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address sticky
```

ポートでのスタティック セキュア MAC アドレスの設定

スタティック セキュア MAC アドレスをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type slot/port | port-channel channel_number}`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security mac-address sticky mac_address [vlan vlan_ID]`	ポートに対し、スタティック MAC アドレスをセキュア アドレスとして設定します。 **（注）** VLAN ごとの設定は、トランクだけでサポートされます。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- スティッキ MAC アドレスによるポート セキュリティをイネーブルにしている場合に、スティッキ セキュア MAC アドレスを設定できます（「スティッキ MAC アドレスによるポート セキュリティのポートでのイネーブル化」（P.78-8）を参照）。
- **switchport port-security maximum** コマンドでポートに設定するセキュア MAC アドレスの最大数により、設定可能なセキュア MAC アドレスの数が定義されます。
- 最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習されます。
- トランクでは、ポート セキュリティがサポートされます。
  - トランクでは、VLAN 内でスタティック セキュア MAC アドレスを設定できます。
  - トランクでは、スタティック セキュア MAC アドレスに対応するように VLAN を設定していない場合、このアドレスは **switchport trunk native vlan** コマンドで設定した VLAN でセキュアとなります。

次に、ギガビット イーサネット ポート 5/12 で MAC アドレス 1000.2000.3000 をセキュア アドレスとして設定し、その設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------

Vlan    Mac Address       Type                Ports
```

```
----    -----------       ----                 -----
   1    1000.2000.3000    SecureConfigured     Gi5/12
```

ポートでのセキュア MAC アドレスのエージング設定

（注）
- スタティック セキュア MAC アドレスおよびスティッキ セキュア MAC アドレスは、期限切れとなりません。
- **absolute** キーワードを使用してエージング タイプを設定すると、ダイナミックに学習されるすべてのセキュア アドレスは、エージング タイムを過ぎると期限切れとなります。**inactivity** キーワードを使用してエージング タイプを設定すると、エージング タイムは、ダイナミックに学習されたすべてのセキュア アドレスが期限切れとなるまでの非アクティブ期間として定義されます。

ポートでのセキュア MAC アドレスのエージング タイプの設定

セキュア MAC アドレスのエージング タイムをポートに設定できます。セキュア MAC アドレスのエージング タイプをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging type** {**absolute** | **inactivity**}	セキュア MAC アドレスのエージング タイプをポートに設定します（デフォルトは absolute）。

次に、ギガビット イーサネット ポート 5/12 のエージング タイプを inactivity に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/12
Router(config-if)# switchport port-security aging type inactivity
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Type
Aging Type                : Inactivity
```

ポートでのセキュア MAC アドレスのエージング タイムの設定

セキュア MAC アドレスのエージング タイムをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type slot/port* | **port-channel** *channel_number*}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging time** *aging_time*	セキュア MAC アドレスのエージング タイムをポートに設定します。aging_time の有効範囲は 1 ～ 1440 分です（デフォルトは 0）。

次に、ギガビット イーサネット ポート 5/1 のセキュア MAC アドレス エージング タイムを 2 時間（120 分）に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/1
Router(config-if)# switchport port-security aging time 120
Router(config-if)# do show port-security interface gigabitethernet 5/12 | include Time
Aging Time                : 120 mins
```

ポート セキュリティの設定の確認

ポート セキュリティ設定を表示するには、次のコマンドを入力します。

コマンド	目的
Router# **show port-security** [**interface** {{**vlan** *vlan_ID*} | {*type slot/port*}}] [**address**]	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を表示します。

- ポート セキュリティでは、**vlan** キーワードはトランクだけでサポートされます。
- **address** キーワードを入力してセキュア MAC アドレスを表示すると、各アドレスのエージング情報（スイッチに対するグローバル情報、またはインターフェイスごとの情報）が表示されます。
- 次の値が表示されます。
  - 各インターフェイスで許可されるセキュア MAC アドレスの最大数
  - インターフェイスに設定されたセキュア MAC アドレスの数
  - 発生したセキュリティ違反の数
  - 違反モード

次に、インターフェイスを入力しない場合の **show port-security** コマンドの出力例を表示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------

     Gi5/1           11            11            0            Shutdown
     Gi5/5           15            5             0            Restrict
     Gi5/11          5             4             0            Protect
-------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

次に、特定のインターフェイスに対する **show port-security** コマンドの出力例を示します。

```
Router# show port-security interface gigabitethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

次に、**show port-security address** 特権 EXEC コマンドの出力例を示します。

```
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                          (mins)
----    -----------       ----                -----   -------------
   1    0001.0001.0001    SecureDynamic       Gi5/1       15 (I)
   1    0001.0001.0002    SecureDynamic       Gi5/1       15 (I)
   1    0001.0001.1111    SecureConfigured    Gi5/1       16 (I)
   1    0001.0001.1112    SecureConfigured    Gi5/1       -
   1    0001.0001.1113    SecureConfigured    Gi5/1       -
   1    0005.0005.0001    SecureConfigured    Gi5/5       23
   1    0005.0005.0002    SecureConfigured    Gi5/5       23
   1    0005.0005.0003    SecureConfigured    Gi5/5       23
   1    0011.0011.0001    SecureConfigured    Gi5/11      25 (I)
   1    0011.0011.0002    SecureConfigured    Gi5/11      25 (I)
------------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

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