サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限の設定

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限機能では、サービス インスタンス単位のきめ細かさで、MAC アドレス ラーニング動作を制御およびフィルタリングできるようにすることで、サービス インスタンスによるポート セキュリティに対応します。違反によってシャットダウンが必要になった場合、ポートを使用しているすべてのカスタマーではなく、対象のサービス インスタンスに対して割り当てられたカスタマーだけが影響を受けます。EVC ポート チャネルでの MAC アドレス セキュリティ機能は、Multipoint Bridging over Ethernet（MPBE）をサポートします。MAC アドレス制限は MAC セキュリティのタイプの 1 つであり、MAC セキュリティ コンポーネントまたは要素とも呼ばれます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限に関する機能情報」（P.43）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限に関する前提条件

- サービス インスタンスとブリッジ ドメインを理解していること。
- MAC アドレス制限の概念と、MAC セキュリティのための使用方法を理解していること。
- ネットワークでのポート チャネルと EtherChannels の動作を理解していること。

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限に関する制約事項

サービス インスタンスとブリッジ ドメインに関する MAC アドレスの制限は、サービス インスタンスに設定され、サービス インスタンスをブリッジ ドメインで設定した後でのみ許可されます。サービス インスタンスがブリッジ ドメインから削除されると、その下のすべての MAC アドレス制限コマンドも削除されます。ブリッジ ドメインがサービス インスタンスから削除されると、すべての MAC アドレス制限コマンドも削除されます。

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限について

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス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。

イーサネット仮想回線、サービス インスタンス、およびブリッジ ドメイン

Metro Ethernet Forum によって定義されている Ethernet Virtual Circuit（EVC; イーサネット仮想回線）は、ポート レベルのポイントツーポイントまたはマルチポイントツーマルチポイントのレイヤ 2 回線です。これは、プロバイダーからカスタマーに提供されているレイヤ 2 サービスの単一インスタンスのエンドツーエンド表現です。EVC は、サービスを提供するためのさまざまなパラメータを実現したものです。サービス インスタンスは、あるポート上で EVC をインスタンス化したものです。

イーサネット ブリッジングのサポートは、EVC の一部としてルータに提供される重要なレベル 2 サービスです。イーサネット ブリッジングにより、ブリッジ ドメインとサービス インスタンスを関連付けることが可能になります。

サービス インスタンスは、ポート チャネルに設定されます。サービス インスタンスの伝送するトラフィックは、メンバ リンク全体でロード バランシングされます。ポート チャネルのサービス インスタンスはグループ化され、各グループが 1 つのメンバ リンクに関連付けられます。1 つのサービス インスタンスに対する入力トラフィックが、バンドルのすべてのメンバに届く可能性があります。サービス インスタンスのすべての出トラフィックは、メンバ リンクの 1 つだけを使用します。ロード バランシングは、サービス インスタンスをグループ化し、それをメンバ リンクに割り当てることで実現されます。

Metro Ethernet Forum 規格の詳細については、「規格」（P.41）を参照してください。

ポート チャネル上の EVC

EtherChannel は、個々のイーサネット リンクを 1 つの論理リンクにバンドルすることにより、最大 8 つの物理リンクの集約帯域幅を提供します。Ethernet Virtual Connection Services（EVCS; イーサネット仮想接続サービス）EtherChannel 機能は、サービス インスタンス上の EtherChannels をサポートします。

（注） EVC ポート チャネルでの MAC アドレス セキュリティ サービスは、イーサネット経由のブリッジ ドメイン上でのみサポートされ、ローカル接続または xconnect サービス上ではサポートされません。

EVCS は、EVC およびサービス インスタンスの概念を使用します。

ロード バランシングは、いくつかの Ethernet Flow Point（EFP）がメンバ リンクを通じて排他的にトラフィックを通過させる EFP に基づいて行われます。

MAC セキュリティと MAC アドレッシング

MAC セキュリティは、**mac security** コマンドを設定することにより、サービス インスタンスに対してイネーブルにされます。各種の MAC セキュリティ要素は、現在 **mac security** コマンドが設定されているかどうかに関係なく設定できますが、これらの設定は **mac security** コマンドが適用された場合にのみ動作するようになります。

本書において「セキュアなサービス インスタンス」という用語は、MAC セキュリティが設定されたサービス インスタンスを表すために使用されます。MAC セキュリティが設定されたサービス インスタンスの MAC アドレスは、「セキュアな MAC アドレス」と呼ばれます。セキュアな MAC アドレスは、静的に（許可リストとして）設定することも、また動的に学習することもできます。

MAC アドレス許可リスト

許可リストは、サービス インスタンス上で許可される MAC アドレスのセットです。許可されたアドレスは、サービス インスタンスの MAC アドレス テーブルに永続的に設定されます。

オペレータは、ブリッジ ドメインのメンバであるサービス インスタンス上で、1 つまたは複数の許可された MAC アドレスを設定できます。許可された各アドレスに対して適格性テストが実行され、アドレスがこれらのテストに合格した場合、次のように処理されます。

- サービス インスタンスで MAC セキュリティがイネーブルにされている場合には、ブリッジ ドメインの MAC アドレス テーブルにプログラムされます。
- サービス インスタンスで MAC セキュリティがイネーブルにされていない場合には、「MAC テーブル キャッシュ」と呼ばれるメモリ領域に格納されます。MAC セキュリティがイネーブルの場合には、MAC テーブル キャッシュからのアドレスが、セキュアなアドレスとして MAC アドレス テーブルに追加されます。

ユーザがサービス インスタンス上の許可リストに MAC アドレスを追加する場合、次のように適格性テストが行われます。

1. そのアドレスがサービス インスタンス上ですでに拒否されたアドレスの場合、設定が拒否され、該当するエラー メッセージが出力されます。
2. このアドレスを受け入れることにより、サービス インスタンス上のセキュアなアドレス数が、許可される最大数を超えて増加する場合には、MAC アドレス テーブルから既存のアドレスを削除することで空きを作ろうとします。削除の候補となるのは、サービス インスタンス上で動的に学習されたアドレスに限られます。十分な空きを作成できない場合には、設定が拒否されます。このアドレスを受け入れることにより、ブリッジ ドメイン上のセキュアなアドレス数が、許可される最大数を超えて増加する場合には、MAC アドレス テーブルから既存のアドレスを削除することで空きを作ろうとします。削除の候補となるのは、サービス インスタンス上で動的に学習されたアドレスに限られます。空きを作成できない場合には、設定が拒否されます。
3. 同じブリッジ ドメイン内の別のサービス インスタンス上でそのアドレスがすでに許可されている場合には、次のアクションのいずれかが実行されます。
   a. 競合するサービス インスタンスに MAC セキュリティが設定されている場合、設定は拒否され、該当するエラー メッセージが表示されます。
   b. 競合するサービス インスタンスに MAC セキュリティが設定されていない場合、設定が受け入れられ、メッセージは出力されません（オペレータが競合するサービス インスタンス上で MAC セキュリティをイネーブルにしようとすると、その試みは失敗します）。

MAC アドレス拒否リスト

拒否リストは、サービス インスタンス上で許可されない MAC アドレスのセットです。拒否された MAC アドレスを学習する試みは失敗します。オペレータは、ブリッジ ドメインのメンバであるサービス インスタンス上で、1 つまたは複数の拒否された MAC アドレスを設定できます。拒否リストに含まれるソース MAC アドレスを持つフレームが到着すると、違反応答がトリガーされます。

拒否するアドレスを設定する前に、次のテストが実行されます。

1. そのアドレスが特定のサービス インスタンス上で許可されたアドレスとして設定されている場合、またはそのアドレスが学習され、サービス インスタンス上でスティッキ アドレスとして保存されている場合には、設定が拒否され、該当するエラー メッセージが出力されます。

その他のすべての場合には、拒否されたアドレスの設定が受け入れられます。一般的なものとしては、次の場合があります。

- そのアドレスが同じブリッジ ドメイン内の別のサービス インスタンス上で許可されたアドレスとして設定されているか、またはそのアドレスは学習されたものであり、別のサービス インスタンス上にスティッキ アドレスとして保存されている。
- そのアドレスは特定のサービス インスタンス上で動的に学習されたアドレスとしてブリッジ ドメインの MAC テーブル内に存在し、設定が受け入れられる前に MAC テーブルから削除された。

MAC アドレスの制限と学習

ブリッジ ドメイン サービス インスタンス上で許可される、セキュアな MAC アドレス数の上限を設定できます。この制限には、許可リストの一部として追加されたアドレスと動的に学習された MAC アドレスが含まれます。

未知の MAC アドレスを学習する前に、設定され運用されている一連の制約と比較チェックされます。これらのチェックのいずれかが失敗すると、そのアドレスは学習されず、また設定された違反応答がトリガーされます。

スタティックおよびダイナミック MAC アドレス

スタティック MAC アドレスは、**mac security permit** コマンドによって、サービス インスタンス上で許可されたものとして指定されます。ダイナミック MAC アドレスは、MAC テーブル内には存在しないものの、MAC アドレス テーブルへの挿入と学習を許可されたものとしてサービス インスタンスが検出するソース MAC アドレスです。

ダイナミック MAC アドレスの学習

ブリッジング データ パスで、セキュアな入力サービス インスタンスの MAC アドレス テーブルにソース アドレスが存在しない入力フレームが検出された場合に、ダイナミック MAC アドレスの学習が行われます。

MAC セキュリティ コンポーネントが、MAC テーブルへの新しいソース アドレスの追加に関する許可と拒否を管理します。次の制約が適用されます。

1. この MAC アドレスを学習するかどうかを検討する際に、セキュアな MAC アドレス数が、個々のサービス インスタンス上およびブリッジ ドメイン全体で学習を許可された最大数を超えないか、確認するためのチェックが行われます。
2. 別のサービス インスタンス上の MAC アドレスが、同じブリッジ ドメイン内のセキュアなサービス インスタンス上で以前学習されたものかどうかを判断するためのチェックが行われます。
3. 新しいダイナミック MAC アドレスが拒否リストにないか確認するチェックが実行されます。

サービス インスタンス上での MAC アドレスの制限

ユーザは、サービス インスタンスに関連付けられた MAC テーブル内に存在する MAC アドレスの最大数を設定できます。この数には、静的に設定されたアドレスと、動的に学習された（スティッキを含む）アドレスが含まれます。

MAC セキュリティがイネーブルにされ、かつ MAC アドレスの最大数が設定されていないサービス インスタンス上では、許可されるアドレス数は 1 となります。これは、サービス インスタンスに関連付けられた許可リストが存在する場合、その許可リストは 1 つのアドレスだけを持つことができ、アドレスは動的に学習されないことを意味しています。サービス インスタンスに関連付けられた許可リストが存在しない場合には、1 つの MAC アドレスを動的に学習できます。

ブリッジ ドメインの MAC アドレスの制限

ブリッジ ドメインの MAC アドレス テーブル内に格納可能な MAC アドレス数に上限を設定できます。これは、サービス インスタンス上のセキュアな MAC アドレスの上限とは独立して設定できます。このブリッジ ドメイン MAC アドレス制限に違反すると、MAC アドレス学習の試みが失敗し、フレームが廃棄されます。

ブリッジ ドメイン MAC アドレス制限が設定されていない場合、デフォルトでは、ブリッジ ドメインで許される MAC アドレスの最大数は、そのプラットフォームでサポート可能な最大数となります。

ブリッジ ドメインとサービス インスタンスとの間の MAC アドレス制限の関係

MAC セキュリティ コマンドでは、ブリッジ ドメインとサービス インスタンスの MAC テーブル エントリの最大数を同時に指定できます。しかし、サービス インスタンスに対して設定できる数には制約がありません。

表 1 に初期設定の例を示します。ブリッジ ドメインで 3 つのサービス インスタンスが設定されています。

表 1　　ブリッジ ドメインとサービス インスタンスの MAC アドレス制限

ブリッジ ドメイン/サービス インスタンス番号	MAC アドレス制限
ブリッジ ドメイン 1000	20
サービス インスタンス 1001	5
サービス インスタンス 1002	10
サービス インスタンス 1003	未設定

サービス インスタンス 1003 に対して MAC セキュリティを設定する場合、最大数に任意の値を設定できます。次に例を示します。

```
service instance 1003 ethernet
 bridge-domain 1
 mac security
 mac security maximum addresses 35
```

3 つのサービス インスタンスの総 MAC アドレス制限（5 + 10 + 35）がブリッジ ドメインに対して設定された数（20）を上回る場合であっても、MAC アドレス制限として 35 が許可されます。実際の動作中は、ブリッジ ドメイン制限として 20 が有効であることに注意してください。動的なセキュア アドレス数は、適用可能な最小数を超えることはできません。したがって、サービス インスタンス 1003 が 35 個のアドレスを学習することはできません。

MAC の移動と MAC のロック

ある MAC アドレスが、MAC セキュリティが設定されているサービス インスタンス（たとえば、サービス インスタンス 1）のアドレス テーブルに存在する場合、同じブリッジ ドメイン内の別のサービス インスタンス（たとえば、サービス インスタンス 2）上で同じ MAC アドレスを学習することはできません。

サービス インスタンス 2 が同じ MAC アドレスを学習しようとすると、サービス インスタンス 2 に対して設定された違反応答がトリガーされます。サービス インスタンス 2 に対して MAC セキュリティが設定されていない場合で、違反応答が設定されていない場合には、サービス インスタンス 2 に対して「シャットダウン」応答シーケンスがトリガーされます。

サービス インスタンス 1 で MAC セキュリティがイネーブルにされていない場合には、違反はトリガーされません。サービス インスタンス 2 は MAC アドレスを学習し、それをサービス インスタンス 1 から移動します。

Cisco 7600 シリーズ ルータなど一部のプラットフォームでは、MAC アドレスの移動は可能ですが、セキュアなサービス インスタンスと非セキュアなサービス インスタンスとの間の移動は検出できません。

たとえば、Cisco 7600 シリーズ ルータのハードウェア制限のため、サービス インスタンス 2 に MAC セキュリティを設定しない場合、セキュアなサービス インスタンス 1 からサービス インスタンス 2 への MAC の移動が受け入れられます。したがって、同じブリッジ ドメイン内のすべてのサービス インスタンスを、セキュアなサービス インスタンスとして設定することを推奨します。

違反応答の設定

違反応答は、MAC セキュリティ違反に対する応答、またはアドレス違反により MAC アドレスの動的な学習が失敗したことへの応答です。MAC セキュリティ違反には、2 つのタイプがあります。

タイプ 1 違反：拒否リストのため、またはセキュアなアドレスの最大数を超える可能性があるため、入力フレームのアドレスを動的に学習できません（「MAC アドレスの制限と学習」（P.5）を参照）。

タイプ 2 違反：別のセキュアなサービス インスタンスにすでに「存在する」ため、入力フレームのアドレスを動的に学習できません（「MAC の移動と MAC のロック」（P.7）を参照）。

違反に対する応答としては、3 つのアクションのセットがあります。

1. **シャットダウン**
   - 入力フレームがドロップされます。
   - 問題のあるフレームが到着したサービス インスタンスがシャットダウンされます。
   - 違反数が増分され、違反したアドレスが記録されて、あとから CLI で表示できます。
   - イベントと応答が SYSLOG に記録されます。
2. **制約**
   - 入力フレームがドロップされます。
   - 違反数が増分され、違反したアドレスが記録されて、表示できます。
   - イベントと応答が SYSLOG に記録されます。
3. **保護**
   - 入力フレームがドロップされます。

違反応答が設定されていない場合のデフォルトの応答モードは、シャットダウンです。違反応答は、保護モードまたは制約モードに設定できます。違反応答の形式が「ない」場合、違反応答はデフォルト モードのシャットダウンに設定されます。

サービス インスタンス上のタイプ 1 とタイプ 2 の違反に対して、適切な応答を設定できます。ブリッジ ドメイン上のタイプ 1 違反（学習の試行がサービス インスタンス上で設定されたポリシーに適合しているものの、ブリッジ ドメイン上で設定されたポリシーに違反している）については、応答は常に「保護」になります。これは、設定できません。

シャットダウン モードでは、サービス インスタンスはただちにエラー ディセーブル状態にされ、SNMP トラップ通知が送信されて、さらに次のようにコンソールおよび SYSLOG にメッセージが送信されます。

```
%ETHER_SERVICE-6-ERR_DISABLED:
Mac security violation - shutdown service instance 100 on interface gig 0/0/0
```

サービス インスタンスのエラー ディセーブル状態を解除するには、**errdisable recovery cause mac-security** コマンドを使用して自動回復タイマーを設定するか、または EXEC コマンド **clear ethernet service instance id** *id* **interface** *type number* **errdisable** を使用して再度イネーブルにします。

制約モードでは、違反レポートが LOG_WARNING レベルで SYSLOG に送信されます。

各タイプの違反応答のサポートは、プラットフォームの機能によって異なります。サービス インスタンスに対して、所定の違反応答を設定できます。設定された違反応答は、**mac security** コマンドを使用して MAC セキュリティがイネーブルにされるまで、有効になりません。

MAC アドレス エージングの設定

サービス インスタンスとブリッジ ドメインの両方で動的に学習または静的に設定されたセキュアな MAC アドレスを期限切れにするように、特定のタイム スケジューラを設定できます。これにより、MAC アドレス テーブルから未使用のアドレスが解放され、他のアクティブなサブスクライバが使用できるようになります。

セキュアな MAC アドレスを期限切れにするために適用されるルールのセットは、セキュア エージングと呼ばれます。デフォルトでは、セキュアなサービス インスタンスの MAC アドレス テーブル内のエントリが期限切れになることはありません。これには、許可されたアドレスと動的に学習されたアドレスが含まれます。

mac security aging time *aging-time* コマンドは、MAC アドレス テーブル内のアドレスのエージング タイムを <*n*> 分に設定します。デフォルトでは、このコマンドは、動的に学習されたアドレス（スティッキは含まない）だけに作用します。許可されたアドレスおよびスティッキ アドレスは、このコマンドを適用しても影響を受けません。

デフォルトでは、**mac security aging time** *aging-time* コマンドを通じて設定されたエージング タイム <n> は、絶対時間です。つまり、MAC アドレスの経過時間は、サービス インスタンスで最初に検出された時点から測定されます。この解釈は、**mac security aging time** *aging-time* **inactivity** コマンドを使用して変更できます。この場合、経過時間 <n> は、サービス インスタンスでこの MAC アドレスが最後に検出された時点から測定されます。

mac security aging static コマンドと **mac security aging sticky** コマンドは、**mac security aging time** *aging-time* コマンドが、許可された MAC アドレスとスティッキ MAC アドレスにそれぞれ適用される必要があることを指定します。許可された MAC アドレスの場合、絶対エージング タイムは、そのアドレスが MAC アドレス テーブルに格納されたとき（たとえば、設定されたときと、**mac security** コマンドが入力されたときの遅い方）から測定します。

mac security aging time *aging-time* コマンドが設定されていない場合、**mac security aging static** コマンドは影響を与えません。

スティッキ MAC アドレスの設定

インターフェイスの移行またはデバイスのリロードの後であっても、セキュアなサービス インスタンスで動的に学習した MAC アドレスを固定する機能をセットアップおよび設定できます。動的に学習された MAC アドレスのうち、セキュアなサービス インスタンス上で固定されたものを「スティッキ MAC アドレス」と呼びます。**mac security sticky** コマンドは、サービス インスタンス上でスティッキ MAC アドレッシング機能をイネーブルにするのに使用されます。

サービス インスタンス上でイネーブルにされた「スティッキ」機能を使用すると、サービス インスタンス上で動的に学習された MAC アドレスが、サービス インスタンス ラインの移行やデバイスのリロードが行われても永続的に維持されます。

スティッキ機能は、静的に設定された MAC アドレスには影響を与えません。スティッキ アドレスは、実行コンフィギュレーションに保存されます。デバイスをリロードする前に、ユーザが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必要があります。これを実行することにより、デバイスがオンになると、以前動的に学習されたすべての MAC アドレスがすぐに MAC アドレス テーブルに格納されます。

mac security sticky address *mac-address* コマンドを使用して、特定の MAC アドレスをスティッキ MAC アドレスとして設定できます。MAC アドレスをスタティック アドレスとして設定するのと同じことなので、ユーザがこのコマンドを使用するのは推奨できません。スティッキ MAC アドレッシングが **mac security sticky** コマンドでイネーブルにされている場合、動的に学習したアドレスはスティッキとしてマークされ、**mac security sticky address** *mac-address* コマンドが自動的に生成されて、サービス インスタンス上の学習された各 MAC アドレスに対する実行コンフィギュレーションに保存されます。

スティッキ アドレスのエージング

スティッキ動作がイネーブルにされているサービス インスタンス上で学習された MAC アドレスは、**mac security aging time** コマンドと **mac security aging sticky** コマンドによって設定されたエージングの対象になります。言い換えると、エージング機能の目的では、スティッキ アドレスは、動的に学習されたアドレスと同様に取り扱われます。

移行

ここでは、たとえば設定の変更やリンクの状態遷移など、各種トリガーが発生した場合の各 MAC セキュリティ要素の予期される動作について説明します。

サービス インスタンスでイネーブルにされた MAC セキュリティ

サービス インスタンスで MAC セキュリティがイネーブルにされると、そのサービス インスタンスに関するすべての既存 MAC テーブル エントリが消去されます。次に、ブリッジ ドメインで有効な MAC アドレス制限の制約に従って、許可された MAC アドレス エントリおよびスティッキ アドレスが MAC テーブルに追加されます。

MAC アドレス制限を超えた場合、追加に失敗したすべての MAC アドレスがコンソールへのエラー メッセージで報告され、サービス インスタンスで MAC セキュリティをイネーブルにする試みが失敗し、さらにすでに追加されている許可されたエントリが取り消しまたは削除されます。

すべてのエントリのエージング タイマーが、セキュア エージング ルールに従って更新されます。

サービス インスタンスでディセーブルにされた MAC セキュリティ

このサービス インスタンスの既存の MAC アドレス テーブル エントリが消去されます。

新しいブリッジ ドメインに移動されるサービス インスタンス

この移行は、MAC セキュリティが設定されているかどうかに関係なく、すべてのサービス インスタンスに適用されます。古いブリッジ ドメインの MAC アドレス テーブル内にある、このサービス インスタンス上のすべての MAC アドレスが削除されます。古いブリッジ ドメイン内の動的に学習されたアドレス数が減算されます。次に、すべての MAC セキュリティ コマンドが、サービス インスタンスから永続的に除去されます。

ブリッジ ドメインから削除されるサービス インスタンス

このサービス インスタンスに起因する MAC アドレス テーブル内のすべての MAC アドレスが削除され、ブリッジ ドメイン内で動的に学習されたアドレス数が減算されます。MAC セキュリティは、ブリッジ ドメインのメンバであるサービス インスタンスに対してのみ適用されるため、ブリッジ ドメインからサービス インスタンスを削除すると、すべての MAC セキュリティ コマンドが永続的に除去されます。

違反によるサービス インスタンスのシャットダウン

MAC アドレス テーブル内の動的に学習されたすべての MAC アドレスが削除されますが、その他のすべての MAC セキュリティ状態値は変化せずに残ります。唯一の変化はトラフィックが転送されなかったことであり、したがって学習は実行できません。

インターフェイス/サービス インスタンスのダウン/ラインカード OIR の削除

影響を受けるブリッジ ドメインのすべての MAC テーブルから、ダウンしたサービス インスタンスに起因するすべてのエントリがクリアされます。

インターフェイス/サービス インスタンスの再アクティブ化/ラインカード OIR の挿入

影響を受けるブリッジ ドメインの MAC テーブル内のスタティック アドレスおよびスティッキ アドレスのエントリが、アクティブ化されるサービス インスタンスに対して再作成されます。

MAC アドレス制限の削減

サービス インスタンスに対する MAC アドレス制限の値が初期的に変更された場合、新しい値 <n> が許可されたエントリ数以上であることを確認するための正常性チェックが行われます。それ以外の場合には、コマンドが拒否されます。MAC テーブルでこのサービス インスタンスに起因するアドレスがスキャンされ、新しい MAC アドレス制限が古い MAC アドレス制限より小さい場合には、動的に学習された MAC アドレスが削除されます。

ブリッジ ドメインに対する値 <n> が初期的に変更される場合、新しい値 <n> がブリッジ ドメイン上のセキュアなすべてのサービス インスタンスの許可されたエントリ数の合計以上であることを確認するために、正常性チェックが行われます。正常性テストが失敗すると、コマンドが拒否されます。ブリッジ ドメイン MAC アドレス テーブルで（サービス インスタンスに関係なく）、動的に学習された（または、スティッキ）アドレスがスキャンされます。新しい MAC アドレス制限が古い MAC アドレス制限よりも少ない場合、動的に学習されたすべてのアドレスが削除されます。

サービス インスタンスに追加または除去されるスティッキ アドレス

動的に学習された既存の MAC アドレスは変化しません。学習されたすべての新しいアドレスは、「スティッキ」アドレスとなります。

スティッキ アドレスをディセーブルにすると、サービス インスタンス上のすべてのセキュアなスティッキ MAC アドレスが、MAC アドレス テーブルから除去されます。学習されたすべての新しいアドレスは、サービス インスタンス上のダイナミック アドレスとなり、エージング対象になります。

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限の設定方法

ここでは、次の設定手順について説明します。

サービス インスタンス上での MAC セキュリティのイネーブル化

サービス インスタンス上で MAC アドレス セキュリティをイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/subslot/port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security**
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。 • プロンプトが表示されたら、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** *slot/subslot/port* **例：** `Router(config)# interface gigabitethernet 1/0/0`	設定するインターフェイスのタイプと位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンスを作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。

	コマンドまたはアクション	目的
ステップ 7	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 8	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

EVC ポートチャネル上での MAC セキュリティのイネーブル化

EVC ポート チャネルで MAC セキュリティをイネーブルにするには、次のタスクを実行します。

制約事項

- ポート チャネルのすべてのメンバ リンクは、Cisco 7600-ES+ ラインカード上にあります。
- ブリッジ ドメイン、xconnect、EVC 接続、スイッチポート、および IP サブインターフェイスは、ポート チャネル インターフェイスおよびメイン インターフェイスを通じて許可されます。
- チャネル グループの一部として物理ポートを設定する場合には、その物理ポートで EVC を設定できます。
- EVC ポート チャネルに含まれる物理ポートには、スイッチポートを設定できません。
- Link Aggregation Control Protocol（LACP; リンク集約コントロール プロトコル）でのポート チャネル メンバシップの設定はサポートされていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-group*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security**
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。 • プロンプトが表示されたら、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 port-channel** *channel-group* **例：** `Router(config)# interface port-channel 2`	ポート チャネル グループ番号を指定し、CLI をインターフェイス コンフィギュレーション モードにします。 • 可能な値は、1 ～ 64 の整数です。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンスを作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 8	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

MAC アドレス許可リストの設定

ブリッジ ドメインのメンバとなっているサービス インスタンスに、許可される MAC アドレスを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot*/*subslot*/*port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security address permit** *mac-address*
8. **mac security address permit** *mac-address*
9. **mac security address permit** *mac-address*
10. **mac security address permit** *mac-address*
11. **mac security address permit** *mac-address*
12. **mac security**
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。 • プロンプトが表示されたら、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** *slot*/*subslot*/*port* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security address permit** *mac-address* **例：** `Router(config-if-srv)# mac security address permit a2aa.aaaa.aaaa`	指定された MAC アドレスを、サービス インスタンスの許可 MAC アドレスとして追加します。
ステップ 8	**mac security address permit** *mac-address* **例：** `Router(config-if-srv)# mac security address permit a2aa.aaaa.aaab`	指定された MAC アドレスを、サービス インスタンスの許可される MAC アドレスとして追加します。
ステップ 9	**mac security address permit** *mac-address* **例：** `Router(config-if-srv)# mac security address permit a2aa.aaaa.aaac`	指定された MAC アドレスを、サービス インスタンスの許可される MAC アドレスとして追加します。
ステップ 10	**mac security address permit** *mac-address* **例：** `Router(config-if-srv)# mac security address permit a2aa.aaaa.aaad`	指定された MAC アドレスを、サービス インスタンスの許可される MAC アドレスとして追加します。
ステップ 11	**mac security address permit** *mac-address* **例：** `Router(config-if-srv)# mac security address permit a2aa.aaaa.aaae`	指定された MAC アドレスを、サービス インスタンスの許可される MAC アドレスとして追加します。
ステップ 12	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 13	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

MAC アドレス拒否リストの設定

ブリッジ ドメインのメンバとなっているサービス インスタンスで、許可されない MAC アドレスのリストを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot*/*subslot*/*port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security address deny** *mac-address*
8. **mac security address deny** *mac-address*
9. **mac security address deny** *mac-address*
10. **mac security address deny** *mac-address*
11. **mac security address deny** *mac-address*
12. **mac security**
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。 • プロンプトが表示されたら、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** *slot/subslot/port* **例：** `Router(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security address deny** *mac-address* **例：** `Router(config-if-srv)# mac security address deny a2aa.aaaa.aaaa`	指定された MAC アドレスを、サービス インスタンスの拒否される MAC アドレスとして追加します。
ステップ 8	**mac security address deny** *mac-address* **例：** `Router(config-if-srv)# mac security address deny a2aa.aaaa.aaab`	指定された MAC アドレスを、サービス インスタンスの拒否される MAC アドレスとして追加します。
ステップ 9	**mac security address deny** *mac-address* **例：** `Router(config-if-srv)# mac security address deny a2aa.aaaa.aaac`	指定された MAC アドレスを、サービス インスタンスの拒否される MAC アドレスとして追加します。
ステップ 10	**mac security address deny** *mac-address* **例：** `Router(config-if-srv)# mac security address deny a2aa.aaaa.aaad`	指定された MAC アドレスを、サービス インスタンスの拒否される MAC アドレスとして追加します。

	コマンドまたはアクション	目的
ステップ 11	**mac security permit** | **deny** *mac-address* **例：** `Router(config-if-srv)# mac security address deny a2aa.aaaa.aaae`	指定された MAC アドレスを、サービス インスタンスの拒否される MAC アドレスとして追加します。
ステップ 12	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 13	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

ブリッジ ドメイン上での MAC アドレス制限の設定

ブリッジ ドメイン内に存在するセキュアな MAC アドレス数の上限を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **mac limit maximum addresses** *maximum-addresses*
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。 • プロンプトが表示されたら、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	**bridge-domain** *bridge-id* **例：** `Router(config)# bridge-domain 100`	ブリッジ ドメイン上でコンポーネントを設定し、CLI をサービス インスタンス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 4	**mac limit maximum addresses** *maximum-addresses* **例：** `Router(config-bdomain)# mac limit maximum addresses 200`	MAC 制限の最大アドレス数を設定します。
ステップ 5	**end** **例：** `Router(config-bdomain)# end`	ブリッジ ドメインのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

サービス インスタンス上での MAC アドレス制限の設定

サービス インスタンス上で許可されるセキュアな MAC アドレス数の上限を設定するには、次のタスクを実行します。この数には、許可リストの一部として追加されたアドレスと動的に学習された MAC アドレスが含まれます。上限を減らすと、学習されたすべての MAC エントリが削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security maximum addresses** *maximum-addresses*
8. **mac security**
9. **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。 • プロンプトが表示されたら、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 number* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。

	コマンドまたはアクション	目的
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security maximum addresses** *maximum-addresses* **例：** `Router(config-if-srv)# mac security maximum addresses 500`	サービス インスタンス上で許可されるセキュアなアドレスの最大数を設定します。
ステップ 8	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 9	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

MAC アドレス違反の設定

サービス インスタンス上に設定された MAC セキュリティ ポリシーに違反したため、動的に MAC アドレスを学習する試みが失敗した場合に、デバイスの予期される動作を指定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot*/subslot/*port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security violation restrict**

または

mac security violation protect

8. **mac security**
9. **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。 • プロンプトが表示されたら、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** *slot/subslot/port* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 100`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。

ステップ 7	**mac security violation restrict**
	または
	mac security violation protect
	
	例：
	`Router(config-if-srv)# mac security violation restrict`
	
	例：
	`Router(config-if-srv)# mac security violation protect`
		違反モード（タイプ 1 と 2 の違反）を restrict に設定します。
		または
		違反モード（タイプ 1 と 2 の違反）を protect に設定します。
		• MAC セキュリティ違反応答が指定されなかった場合、デフォルトの違反モードは shutdown になります。

	コマンドまたはアクション	目的
ステップ 8	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 9	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

MAC アドレス エージングの設定

MAC セキュリティ下で、セキュアな MAC アドレスのエージングを設定するには、次のタスクを実行します。セキュアな MAC アドレスは、通常の MAC テーブル エントリのエージング対象になりません。エージングを設定しなかった場合、セキュアな MAC アドレスは期限切れになりません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot*/*subslot*/*port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security aging time** *aging-time* [**inactivity**]
8. **mac security**
9. **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。 • プロンプトが表示されたら、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** *slot*/*subslot*/*port* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。

	コマンドまたはアクション	目的
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security aging time** *aging-time* [**inactivity**] **例：** `Router(config-if-srv)# mac security aging time 200 inactivity`	セキュアなアドレスのエージング タイムを、分単位で設定します。オプションの **inactivity** キーワードを指定すると、送信側ホストの非アクティブ状態に基づいて、アドレスのエージング アウトが行われます(絶対エージングとは異なります)。
ステップ 8	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 9	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

スティッキ MAC アドレスの設定

セキュアなサービス インスタンス上でスティッキ MAC アドレスが設定されている場合、そのサービス インスタンスで動的に学習された MAC アドレスは、リンクダウン状態でも維持されます。サービス インスタンス上でスティッキ MAC アドレスを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot*/*subslot*/*port*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security sticky**
8. **mac security**
9. **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。 • プロンプトが表示されたら、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** *slot/subslot/port* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security sticky** **例：** `Router(config-if-srv)# mac security sticky`	サービス インスタンス上で、スティッキ動作をイネーブルにします。
ステップ 8	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 9	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

特定のサービス インスタンスの MAC セキュリティ ステータスの表示

サービス インスタンスの MAC セキュリティ ステータスを表示するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show ethernet service instance id** *id* **interface** *type number* **mac security**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ethernet service instance id** *id* **interface** *type number* **mac security** **例：** `Router# show ethernet service instance id 100 interface GigabitEthernet 1/1 mac security`	特定のサービス インスタンスの MAC セキュリティ ステータスを表示します。

MAC セキュリティがイネーブルにされたサービス インスタンスの表示

MAC セキュリティがイネーブルにされたすべてのサービス インスタンスを表示するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show ethernet service instance mac security**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ethernet service instance mac security** **例：** `Router# show ethernet service instance mac security`	MAC セキュリティがイネーブルにされたすべてのサービス インスタンスを表示します。

特定のブリッジ ドメイン上で MAC セキュリティがイネーブルにされたサービス インスタンスの表示

特定のブリッジ ドメイン上で MAC セキュリティがイネーブルにされたサービス インスタンスを表示するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show bridge-domain** *id* **mac security**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show bridge-domain** *id* **mac security** **例：** `Router# show bridge-domain 100 mac security`	特定のブリッジ ドメイン上で MAC セキュリティがイネーブルにされたサービス インスタンスを表示します。

すべてのセキュアなサービス インスタンスの MAC アドレスの表示

すべてのセキュアなサービス インスタンス上のすべての MAC アドレスを表示するには、次のタスクを実行します。

制約事項

Cisco 7600 シリーズ ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show ethernet service instance mac security address** コマンドを使用します。

手順の概要

1. **enable**
2. **show ethernet service instance mac security address**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ethernet service instance mac security address** **例：** `Router# show ethernet service instance mac security address`	すべてのサービス インスタンス上のセキュアなアドレスを表示します。

特定のサービス インスタンスの MAC アドレスの表示

特定のサービス インスタンスのすべての MAC アドレスを表示するには、次のタスクを実行します。

制約事項

Cisco 7600 ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show ethernet service instance id** *id* **interface** *type number* **mac security address** コマンドを使用します。

手順の概要

1. **enable**
2. **show ethernet service instance id** *id* **interface** *type number* **mac security address**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ethernet service instance id** *id* **interface** *type number* **mac security address** **例：** `Router# show ethernet service instance id 200 interface GigabitEthernet 1/0 mac security address`	特定のサービス インスタンスのアドレスを表示します。

特定のブリッジ ドメイン上のすべてのサービス インスタンスの MAC アドレスの表示

特定のブリッジ ドメイン上のすべてのサービス インスタンスの MAC アドレスを表示するには、次のタスクを実行します。

制約事項

Cisco 7600 シリーズ ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show bridge-domain** *id* **mac security address** コマンドを使用します。

手順の概要

1. **enable**
2. **show bridge-domain** *id* **mac security address**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show bridge-domain** *id* **mac security address** **例：** `Router# show bridge-domain 100 mac security address`	特定のブリッジ ドメイン上のすべてのサービス インスタンスのセキュアなアドレスを表示します。

特定のサービス インスタンスの MAC セキュリティ統計情報の表示

ここでは、特定のサービス インスタンスの MAC セキュリティ統計情報を表示する方法について説明します。

手順の概要

1. **enable**
2. **show ethernet service instance id** *id* **interface** *type number* **mac security statistics**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ethernet service instance id** *id* **interface** *type number* **mac security statistics** **例：** `Router# show ethernet service instance id 100 interface GigabitEthernet 1/1 mac security statistics`	特定のサービス インスタンスの MAC セキュリティ統計情報を表示します。

特定のブリッジ ドメイン上のすべてのサービス インスタンスの MAC セキュリティ統計情報の表示

特定のブリッジ ドメイン上のすべてのサービス インスタンスの MAC セキュリティ統計情報を表示するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show bridge-domain** *bridge-id* **mac security statistics**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show bridge-domain** *bridge-id* **mac security statistics** **例：** `Router# show bridge-domain 100 mac security statistics`	特定のブリッジ ドメインに属するすべてのサービス インスタンスの MAC セキュリティ統計情報を表示します。

特定ブリッジ ドメイン上の各サービス インスタンスの最後の違反レコードの表示

特定ブリッジ ドメイン上の各サービス インスタンスで最後に記録された違反を表示するには、次のタスクを実行します。違反がないサービス インスタンスは、出力から除外されます。

手順の概要

1. **enable**
2. **show bridge-domain** *bridge-id* **mac security last violation**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show bridge-domain** *bridge-id* **mac security last violation** **例：** `Router# show bridge-domain 100 mac security last violation`	ブリッジ ドメインに属する各サービス インスタンスに記録された最後の違反に関する情報を表示します。

サービス インスタンス上で動的に学習されたすべての MAC アドレスのクリア

サービス インスタンス上で動的に学習されたすべての MAC アドレスをクリアするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **clear ethernet service instance id** *id* **interface** *type number* **mac table**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ethernet service instance id** *id* **interface** *type number* **mac table** **例：** `Router# clear ethernet service instance id 100 interface GigaBitEthernet 1/1 mac table`	指定されたサービス インスタンス上で動的に学習されたすべての MAC アドレスをクリアします。

ブリッジ ドメイン上で動的に学習されたすべての MAC アドレスのクリア

ブリッジ ドメイン上で動的に学習されたすべての MAC アドレスをクリアするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **clear bridge-domain** *bridge-id* **mac table**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear bridge-domain** *bridge-id* **mac table** **例：** `Router# clear bridge-domain 100 mac table`	指定されたブリッジ ドメイン上で動的に学習されたすべての MAC アドレスをクリアします。

特定のサービス インスタンスのエラー ディセーブル状態の解除

特定のサービス インスタンスのエラー ディセーブル状態を解除するには、次のタスクを実行します。

（注） **clear ethernet service instance id** *id* **interface** *type number* **errdisable** コマンドを使用して、サービス インスタンスのエラー ディセーブル状態を解除することもできます。「特定のサービス インスタンスのエラー ディセーブル状態の解除」（P.34）を参照してください。

手順の概要

1. **enable**
2. **config terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security**
8. **errdisable recovery cause mac-security** *interval*
9. **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。 • プロンプトが表示されたら、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 number* **例：** `Router(config)# interface gigabitethernet 2/0/1`	設定するインターフェイスのタイプと位置を、次のように指定します。 • *type*：インターフェイスのタイプを指定します。 • *number*：インターフェイスの位置を指定します。
ステップ 4	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 100 ethernet`	インターフェイス上でサービス インスタンス（EVC のインスタンス）を作成し、CLI をサービス インスタンス コンフィギュレーション モードにします。
ステップ 5	**encapsulation dot1q** *vlan-id* **例：** `Router(config-if-srv)# encapsulation dot1q 100`	インターフェイス上の入力 dot1q フレームを、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。

	コマンドまたはアクション	目的
ステップ 6	**bridge-domain** *bridge-id* **例：** `Router(config-if-srv)# bridge-domain 200`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。ここで、*bridge-id* は、ブリッジ ドメイン インスタンスの ID です。
ステップ 7	**mac security** **例：** `Router(config-if-srv)# mac security`	サービス インスタンス上で MAC セキュリティをイネーブルにします。
ステップ 8	**errdisable recovery cause mac-security** *interval* **例：** `Router(config-if-srv)# errdisable recovery cause mac-security 50`	特定のサービス インスタンスのエラー ディセーブル状態を解除し、回復間隔を指定します。
ステップ 9	**end** **例：** `Router(config-if-srv)# end`	サービス インスタンスのコンフィギュレーション モードを終了し、CLI を特権 EXEC モードにします。

特定のサービス インスタンスのエラー ディセーブル状態の解除

特定のサービス インスタンスのエラー ディセーブル状態を解除するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **clear ethernet service instance id** *id* **interface** *type number* **errdisable**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ethernet service instance id** *id* **interface** *type number* **errdisable** **例：** `Router# clear ethernet service instance id 100 interface FastEthernet 1/1 errdisable`	特定のサービス インスタンスのエラー ディセーブル状態を解除（シャットダウン）します。

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限の設定例

ここでは、次の設定例を示します。

サービス インスタンス上での MAC セキュリティのイネーブル化：例

次に、サービス インスタンス上で MAC セキュリティをイネーブルにする方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

EVC ポート チャネル上での MAC セキュリティのイネーブル化：例

次に、EVC ポート チャネル上で MAC セキュリティを表示する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 2
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

MAC アドレス許可リストの設定：例

次に、MAC アドレス許可リストを設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaab
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaac
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaad
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaae
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

MAC アドレス拒否リストの設定：例

次に、MAC アドレス拒否リストを設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security address deny a2aa.aaaa.aaaa
Router(config-if-srv)# mac security address deny a2aa.aaaa.aaab
Router(config-if-srv)# mac security address deny a2aa.aaaa.aaac
Router(config-if-srv)# mac security address deny a2aa.aaaa.aaad
Router(config-if-srv)# mac security address deny a2aa.aaaa.aaae
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

ブリッジ ドメイン上での MAC アドレス制限の設定：例

次に、ブリッジ ドメイン上で MAC アドレス制限を設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# bridge-domain 100
Router(config-bdomain)# mac limit maximum addresses 1000
Router(config-bdomain)# end
```

サービス インスタンス上での MAC アドレス制限の設定：例

次に、サービス インスタンス上で MAC アドレス制限を設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security maximum addresses 10
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

MAC アドレス違反応答の設定：例

次に、MAC アドレス違反応答を設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
Router(config-if-srv)# mac security violation protect
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

MAC アドレス エージングの設定：例

次に、MAC アドレス エージングを設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 4/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security aging time 10
Router(config-if-srv)# mac security
Router(config-if-srv)# end
```

スティッキ MAC アドレスの設定：例

次に、スティッキ MAC アドレスを設定する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1Q 100
Router(config-if-srv)# bridge-domain 100
Router(config-if-srv)# mac security sticky
Router(config-if-srv)# mac security
```

特定のセキュアなサービス インスタンス上の MAC アドレスの表示：例

次に、特定のセキュアなサービス インスタンス上の MAC アドレスを表示する方法の例を示します。

```
Router# show ethernet service instance id 1879665131 interface gigabitethernet 0/2 mac
security address

MAC Address       Type      Rem. Age(min)
0001.0001.0001    static    100
0001.0001.0002    static    100
0001.0001.aaaa    dynamic   100
0001.0001.aaab    dynamic   100
```

表 2 に、出力内にある重要なフィールドを示します。

表 2　特定のサービス インスタンス上の MAC アドレス：フィールドの説明

フィールド	説明
MAC Address	サービス インスタンスの MAC アドレスが表示されます。
Type	静的に設定されたか（static）、動的に学習されたか（dynamic）を宣言することにより、MAC アドレスのタイプを示します。
Rem.Age(min)	そのアドレスの残りの経過時間が分単位で表示されます。 ハイフン（-）は、エージングがイネーブルでないことを意味します。

（注）　Cisco 7600 シリーズ ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show ethernet service instance id** *id* **interface** *type number* **mac security address** コマンドを使用します。

特定のサービス インスタンス上の最後の違反の表示：例

次に、特定のサービス インスタンス上の最後の違反を表示する方法の例を示します。

```
Router# show ethernet service instance id 1879665131 interface gigabitethernet 0/2 mac
security last violation

At: Apr 4 06:57:25.971
Source address: ae4e.b7b5.79ae
Reason: Denied address
```

特定のサービス インスタンスの MAC セキュリティ ステータスの表示：例

次に、特定のサービス インスタンスの MAC セキュリティ ステータスを表示する方法の例を示します。

```
Router# show ethernet service instance id 1879665131 interface Ethernet0/2 mac security

MAC Security: enabled
```

すべてのセキュアなサービス インスタンスの MAC アドレスの表示：例

次に、すべてのセキュアなサービス インスタンスの MAC アドレスを表示する方法の例を示します。

```
Router# show ethernet service instance mac security address

Port                  Bridge-domain    MAC Address       Type      Rem. Age(min)
Gi1/0/0 ServInst 1    10               0001.0001.0001    static    82
Gi1/0/0 ServInst 1    10               0001.0001.0002    static    82
Gi1/0/0 ServInst 1    10               0001.0001.aaaa    dynamic   82
Gi1/0/0 ServInst 1    10               0001.0001.aaab    dynamic   82
Gi1/0/0 ServInst 2    10               0002.0002.0002    static    -
Gi1/0/0 ServInst 2    10               0002.0002.0003    static    -
Gi1/0/0 ServInst 2    10               0002.0002.0004    static    -
Gi1/0/0 ServInst 2    10               0002.0002.aaaa    dynamic   -
Gi1/0/0 ServInst 2    10               0002.0002.bbbb    dynamic   -
Gi1/0/0 ServInst 2    10               0002.0002.cccc    dynamic   -
Gi3/0/5 ServInst 10   30               0003.0003.0001    static    200
Gi3/0/5 ServInst 10   30               0003.0003.0002    static    200
```

表 3 に、出力内にある重要なフィールドを示します。

表 3　すべてのサービス インスタンスの MAC アドレス：フィールドの説明

フィールド	説明
Port	サービス インスタンス ID 番号、およびそのインターフェイス タイプと番号が表示されます。
Bridge- Domain	リストされた各サービス インスタンスのブリッジ ドメイン ID 番号が表示されます。
MAC Address	サービス インスタンスの MAC アドレスが表示されます。
Type	静的に設定されたか（static）、動的に学習されたか（dynamic）を宣言することにより、MAC アドレスのタイプを示します。
Rem.Age(min)	そのアドレスの残りの経過時間が分単位で表示されます。 ハイフン（-）は、エージングがイネーブルでないことを意味します。

（注） Cisco 7600 シリーズ ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show ethernet service instance mac security address** コマンドを使用します。

すべてのサービス インスタンスの MAC セキュリティ統計情報の表示：例

次に、すべてのサービス インスタンスの MAC セキュリティ統計情報を表示する方法の例を示します。サービス インスタンスで記録されたセキュアなアドレスの、許可された数と実際の数が表示されます。

```
Router# show ethernet service instance mac security statistics

Ethernet0/0 service instance 890597333 (bridge-domain 730)
Secure addresses: 3
Address limit: 7
```

```
Ethernet0/0 service instance 1559665780 (bridge-domain 1249)
Secure addresses: 8
Address limit: 8

Ethernet0/0 service instance 1877043343 (bridge-domain 1155)
Secure addresses: 0
Address limit: 8

Ethernet0/1 service instance 127771402 (bridge-domain 730)
Secure addresses: 12
Address limit: 12

Ethernet0/1 service instance 183598286 (bridge-domain 730)
Secure addresses: 1
Address limit: 1

Ethernet0/1 service instance 433365207 (bridge-domain 1249)
Secure addresses: 0
Address limit: 1
Ethernet0/1 service instance 858688453 (bridge-domain 1328)
Secure addresses: 0
Address limit: 2
```

ブリッジ ドメインのすべてのサービス インスタンス上の MAC アドレスの表示：例

次に、特定のブリッジ ドメインのすべてのサービス インスタンス上の MAC アドレスを表示する方法の例を示します。

```
Router# show bridge-domain 730 mac security address

Port                  MAC Address       Type      Rem. Age(min)
Gi1/0/0 ServInst 1    0001.0001.0001    static    74
Gi1/0/0 ServInst 1    0001.0001.0002    static    74
Gi1/0/0 ServInst 1    0001.0001.aaaa    dynamic   74
Gi1/0/0 ServInst 1    0001.0001.aaab    dynamic   74
Gi1/0/0 ServInst 2    0002.0002.0002    static    -
Gi1/0/0 ServInst 2    0002.0002.0003    static    -
Gi1/0/0 ServInst 2    0002.0002.0004    static    -
Gi1/0/0 ServInst 2    0002.0002.aaaa    dynamic   -
Gi1/0/0 ServInst 2    0002.0002.bbbb    dynamic   -
Gi1/0/0 ServInst 2    0002.0002.cccc    dynamic   -
```

（注） Cisco 7600 ルータなど一部のプラットフォームでは、MAC アドレスの残りのエージング タイム情報は、スイッチ コンソールにのみ表示できます。MAC アドレスの残りのエージング タイム情報を表示するには、**remote command switch** コマンドと **show bridge-domain** *id* **mac security address** コマンドを使用します。

特定のブリッジ ドメインのセキュアなサービス インスタンスの表示：例

次に、特定のブリッジ ドメインのセキュアなサービス インスタンスを表示する方法の例を示します。

```
Router# show bridge-domain 730 mac security

Gi1/0/0 ServInst 1
MAC Security enabled: yes
Gi1/0/0 ServInst 2
MAC Security enabled: yes
```

その他の参考資料

ここでは、サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限機能に関連する参考資料について説明します。

関連資料

関連項目	参照先
キャリア イーサネットのコンフィギュレーション ガイド	『*Cisco IOS Carrier Ethernet Configuration Guide*, Release 12.2SR』
キャリア イーサネットのコマンド	『*Cisco IOS Carrier Ethernet Command Reference*』
Cisco IOS マスター コマンド リスト	『*Cisco IOS Master Command List, All Releases*』

規格

規格	タイトル
MEF 6.1	『Metro Ethernet Services Definitions Phase 2 (PDF 6/08)』
MEF 10.1	『Ethernet Services Attributes Phase 2 (PDF 10/06)』

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対する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 リリース、および機能セットの 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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対する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

サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限に関する機能情報

表 4 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(33)SRD または Cisco IOS Release 12.2(33)SRE 以降のリリースで導入または変更された機能だけが示されています。

ここに記載されていないこのテクノロジーの機能情報については、『Carrier Ethernet Features Roadmap』を参照してください。ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 4　サービス インスタンス、ブリッジ ドメイン、および EVC ポート チャネルでの MAC アドレス制限に関する機能情報

機能名	リリース	機能情報
MAC Address Limiting on Service Instances and Bridge Domains	12.2(33)SRD	MAC Address Limiting on Service Instances and Bridge Domains 機能では、サービス インスタンス単位のきめ細かさで、MAC アドレス ラーニング動作を制御およびフィルタリングできるようにすることで、サービス インスタンスによるポート セキュリティに対応します。違反によってシャットダウンが必要になった場合、対象のサービス インスタンスに対して割り当てられたカスタマーだけが影響を受けます。MAC アドレス制限は MAC セキュリティのタイプの 1 つであり、MAC セキュリティ コンポーネントまたは要素とも呼ばれます。 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。 • 「イーサネット仮想回線、サービス インスタンス、およびブリッジ ドメイン」（P.3） • 「MAC セキュリティと MAC アドレッシング」（P.4） • 「サービス インスタンス上での MAC セキュリティのイネーブル化」（P.12） 次のコマンドが、新たに導入または変更されました。**bridge-domain（config）、bridge-domain（サービス インスタンス）、clear bridge-domain mac table、clear ethernet service instance、errdisable recovery cause mac-security、interface、mac limit maximum addresses、mac security、show bridge-domain、show ethernet service instance**
EVC ポート チャネルでの MAC アドレス セキュリティ	12.2(33)SRE	EVC ポート チャネルでの MAC アドレス セキュリティ機能は、MPBE、ローカル接続、および xconnect サービス タイプをサポートします。 ロード バランシングは、いくつかの EFP がメンバ リンクを通じて排他的にトラフィックを通過させる EFP に基づいて行われます。 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。 • 「ポート チャネル上の EVC」（P.3） • 「EVC ポートチャネル上での MAC セキュリティのイネーブル化」（P.13） 次のコマンドが、新たに導入または変更されました。**interface**