EVC 上のレイヤ 2 アクセス コントロール リスト

モジュラ式でスケーラブルな方法でパケットをフィルタリングする機能は、ネットワーク セキュリティとネットワーク管理の両方の点で重要です。Access Control List（ACL; アクセス コントロール リスト）を使用すると、きめ細かくパケットをフィルタリングできます。メトロ イーサネット ネットワークでは、ACL は Ethernet Virtual Circuit（EVC; イーサネット仮想回線）に直接適用されます。

EVC 上のレイヤ 2 アクセス コントロール リストは、MAC アドレスに基づくパケットのフィルタリングが可能なセキュリティ機能です。このモジュールでは、ACLs on EVCs を実装する方法について説明します。

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、「EVC 上のレイヤ 2 アクセス コントロール リストに関する機能情報」（P.12）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、Cisco IOS ソフトウェア イメージ、Cisco Catalyst OS ソフトウェア イメージ、および Cisco IOS XE ソフトウェア イメージの各サポート情報を検索できます。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。

目次

EVC 上のレイヤ 2 アクセス コントロール リストに関する前提条件

- サービス インスタンスをどのように設定すべきかに関する知識があること。
- 拡張 MAC ACL と、それをどのように設定すべきかに関する知識があること。

EVC 上のレイヤ 2 アクセス コントロール リストに関する制約事項

- 1 つの ACL に対して最大 16 の Access Control Entry（ACE）を設定できます。
- ラインカードでは、256 以下の異なる（固有の）レイヤ 2 ACL を設定できます（ルータには 256 を超える ACL を設定できます）。
- レイヤ 2 ACL は着信のみに対して機能します。
- 現在のレイヤ 2 ACL は、許可ルールと拒否ルールで、レイヤ 3 フィルタリング オプションを提供しています。サービス インスタンスに関係のないオプションは、無視されます。

EVC 上のレイヤ 2 アクセス コントロール リストについて

Layer 2 ACLs on EVCs を実装するには、次の概念を理解しておく必要があります。

- 「EVC」
- 「ACL とイーサネット インフラストラクチャの関係」

EVC

Metro Ethernet Forum によって定義されているように、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、あるルータ上のあるポート上で EVC をインスタンス化したものです。

Ethernet Virtual Connection Services（EVCS）は、EVC とサービス インスタンスを使用して、レイヤ 2 スイッチド イーサネット サービスを提供します。Customer Edge（CE; カスタマー エッジ）デバイスは EVC ステータスを使用して、サービス プロバイダー ネットワークへの代替パスを検索したり、場合によっては、イーサネット経由または別の代替サービス経由（フレーム リレーや ATM など）でバックアップ パスに戻ります。

Metro Ethernet Forum 規格の詳細については、「規格」（P.10）を参照してください。

ACL とイーサネット インフラストラクチャの関係

ACL と Ethernet Infrastructure（EI; イーサネット インフラストラクチャ）との関係をまとめると、次のようになります。

- ACL は、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、EVC に直接適用できます。ACL は、特定のポートで、EVC をインスタンス化したサービス インスタンスに適用されます。
- 1 つの ACL を、複数のサービス インスタンスに適用できます。
- 1 つのサービス インスタンスに適用できる ACL の最大数は 1 です。すでにレイヤ 2 ACL があるサービス インスタンスにレイヤ 2 ACL を適用した場合、新しい ACL が古い ACL と置換されます。
- サービス インスタンスには、名前付き ACL だけを適用できます。コマンド構文 ACL は変更されていません。ACL の作成には **mac access-list extended** コマンドを使用します。
- **show ethernet service instance** コマンドを使用すると、サービス インスタンスの ACL に関する詳細情報を表示できます。

EVC 上のレイヤ 2 アクセス コントロール リストの設定方法

ここでは、次の手順について説明します。

- 「レイヤ 2 ACL の作成」
- 「サービス インスタンスへのレイヤ 2 ACL の適用」
- 「サービス インスタンス上での ACE のあるレイヤ 2 ACL の設定」
- 「サービス インスタンス上のレイヤ 2 ACL の存在確認」

レイヤ 2 ACL の作成

ACE が 1 つのレイヤ 2 ACL を作成するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mac access-list extended** *name*
4. **permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**} [*protocol* [**vlan** *vlan*] [**cos** *value*]]}

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	**mac access-list extended** *name* **例：** `Router(config)# mac access-list extended test-12-acl`	拡張 MAC ACL を定義し、CLI を MAC アクセス リスト コントロール コンフィギュレーション モードにします。
ステップ 4	**permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**} [*protocol* [**vlan** *vlan*] [cos *value*]]} **例：** `Router(config-ext-macl)# permit 00aa.00bb.00cc 0.0.0 any`	条件と一致した場合に、レイヤ 2 トラフィックの転送を許可します。ACL に対して ACE を作成します。

サービス インスタンスへのレイヤ 2 ACL の適用

サービス インスタンスにレイヤ 2 ACL を適用するには、次のタスクを実行します。

（注） パケット フィルタリングは、ACL を作成し、サービス インスタンスに適用した後にだけ実行されることに注意してください。

前提条件

サービス インスタンスに ACL を適用する前に、**mac access-list extended** コマンドを使用して ACL を作成しておく必要があります。「レイヤ 2 ACL の作成」（P.3）を参照してください。

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. **mac access-group** *access-list-name* **in**

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 1/0/0`	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イーサネット サービス インスタンスを設定し、CLI をイーサネット サービス 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	**mac access-group** *access-list-name* **in** **例：** `Router(config-if-srv)# mac access-group test-12-acl in`	MAC ACL を適用して、インターフェイス上で着信トラフィックを制御します。

サービス インスタンス上での ACE のあるレイヤ 2 ACL の設定

同じ ACL に 3 つの ACE を設定し、サービス インスタンスでその他すべてのトラフィックを遮断するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mac access-list extended** *name*
4. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
5. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
6. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
7. **deny any any**
8. **exit**

9. **interface** *type number*
10. **service instance** *id* **ethernet**
11. **encapsulation dot1q** *vlan-id*
12. **mac access-group** *access-list-name* **in**

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	**mac access-list extended** *name* **例：** `Router(config)# mac access list extended test-12-acl`	拡張 MAC ACL を定義し、MAC アクセス コントロール リスト 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	**permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**} **例：** `Router(config-ext-macl)# permit 00aa.bbcc.ddea 0.0.0 any`	条件と一致した場合に、レイヤ 2 トラフィックの転送を許可します。ACL に対して ACE が作成されます。
ステップ 5	**permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**} **例：** `Router(config-ext-macl)# permit 00aa.bbcc.ddeb 0.0.0 any`	条件と一致した場合に、レイヤ 2 トラフィックの転送を許可します。ACL に対して ACE が作成されます。
ステップ 6	**permit** {*src-mac mask* | **any**} {*dest-mac mask*} | **any**} **例：** `Router(config-ext-macl)# permit 00aa.bbcc.ddec 0.0.0 any`	条件と一致した場合に、レイヤ 2 トラフィックの転送を許可します。ACL に対して ACE が作成されます。
ステップ 7	**deny any any** **例：** `Router(config-ext-macl)# deny any any`	ACE で許可されたものを除き、レイヤ 2 トラフィックの転送を禁止します。
ステップ 8	**exit** **例：** `Router(config-ext-macl)# exit`	現在のコマンド モードを終了し、CLI をグローバル コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 9	**interface** *type number* **例：** `Router(config)# interface gigabitethernet 1/0/0`	インターフェイスを指定します。
ステップ 10	**service instance** *id* **ethernet** **例：** `Router(config-if)# service instance 200 ethernet`	インターフェイス上にイーサネット サービス インスタンスを設定し、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。
ステップ 11	**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 12	**mac access-group** *access-list-name* **in** **例：** `Router(config-if-srv)# mac access-group test-12-acl in`	MAC ACL を適用して、インターフェイス上で着信トラフィックを制御します。

サービス インスタンス上のレイヤ 2 ACL の存在確認

EVC 上にレイヤ 2 ACL が存在することを確認するには、次のタスクを実行します。この確認タスクは、ACL の設定後に ACL の存在を確認するために実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **show ethernet service instance id** *id* **interface** *type number* **detail**

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# show ethernet service instance id 100 interface gigabitethernet 3/0/1 detail`	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	**show ethernet service instance id** *id* **interface** *type number* **detail** **例：** `Router# show ethernet service instance id 100 interface gigabitethernet 3/0/1 detail`	イーサネット カスタマー サービス インスタンスに関する詳細情報を表示します。

EVC 上のレイヤ 2 アクセス コントロール リストの設定例

ここでは、次の設定例について説明します。

- 「ACE のあるレイヤ 2 ACL の作成：例」
- 「サービス インスタンスへのレイヤ 2 ACL の適用：例」
- 「同じインターフェイス上の 3 つのサービス インスタンスに対するレイヤ 2 ACL の適用：例」
- 「サービス インスタンス上のレイヤ 2 ACL に関する詳細情報の表示：例」

ACE のあるレイヤ 2 ACL の作成：例

次に、2 つの許可 ACE のある、mac-11-acl というレイヤ 2 ACL を作成する方法の例を示します。

```
enable
configure terminal
mac access-list extended mac-11-acl
permit 00aa.00bb.00cc 1a11.0101.11c1 any
permit 00aa.00bb.00cc 1a11.0101.11c2 any
```

サービス インスタンスへのレイヤ 2 ACL の適用：例

次に、サービス インスタンスに mac-20-acl というレイヤ 2 ACL を適用する方法の例を示します。この ACL には 5 つの許可 ACE が割り当てられ、その他のトラフィックはすべて許可されません。

```
enable
configure terminal
```

```
 mac access-list extended mac-20-acl
 permit 00aa.bbcc.adec 0.0.0 any
 permit 00aa.bbcc.bdec 0.0.0 any
 permit 00aa.bbcc.cdec 0.0.0 any
 permit 00aa.bbcc.edec 0.0.0 any
 permit 00aa.bbcc.fdec 0.0.0 any
 deny any any
 exit
interface gigabitethernet 10/0/0
 service instance 100 ethernet
 encapsulation dot1q 100
 mac access-group mac-20-acl in
```

同じインターフェイス上の 3 つのサービス インスタンスに対するレイヤ 2 ACL の適用：例

次に、同じインターフェイス上の 3 つのサービス インスタンスに、mac-07-acl というレイヤ 2 ACL を適用する方法の例を示します。

```
enable
configure terminal
mac access-list extended mac-07-acl
permit 00aa.bbcc.adec 0.0.0 any
permit 00aa.bbcc.bdec 0.0.0 any
permit 00aa.bbcc.cdec 0.0.0 any
deny any any
exit
interface gigabitethernet 10/0/0
service instance 100 ethernet
encapsulation dot1q 100
mac access-group mac-07-acl in
service instance 101 ethernet
encapsulation dot1q 101
mac access-group mac-07-acl in
service instance 102 ethernet
encapsulation dot1q 102
mac access-group mac-07-acl in
```

サービス インスタンス上のレイヤ 2 ACL に関する詳細情報の表示：例

次に、サービス インスタンス上の test-acl というレイヤ 2 ACL の詳細情報の出力例を示します。

```
Router# show ethernet service instance id 100 int e0/0 detail

Service Instance ID: 100
L2 ACL (inbound): test-acl
Associated Interface: Ethernet0/0
Associated EVC: test
L2protocol drop
CEVlans:
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
L2 ACL permit count: 10255
L2 ACL deny count: 53
```

表 1 に、出力内にある重要なフィールドを示します。

表 1　show ethernet service instance のフィールドの説明

フィールド	説明
Service Instance ID	サービス インスタンス ID を表示します。
L2 ACL (inbound):	ACL 名を表示します。
Associated Interface:	サービス インスタンスのインターフェイスに関する詳細情報を表示します。
Associated EVC:	サービス インスタンスが関連付けられている EVC を表示します。
CEVlans:	関連付けられている VLAN ID の詳細情報を表示します。
State:	サービス インスタンスがアップ状態またはダウン状態のいずれにあるかを表示します。
L2 ACL permit count:	ACL によってサービス インスタンスに渡すことを許可されたパケット フレームの数を表示します。
L2 ACL deny count	ACL によってサービス インスタンスに渡すことが許可されなかったパケット フレームの数を表示します。

その他の参考資料

ここでは、EVC 上のレイヤ 2 アクセス コントロール リスト機能に関連する参考資料を示します。

関連資料

関連項目	参照先
キャリア イーサネットのコマンド	『*Cisco IOS Carrier Ethernet Command Reference*』

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
• なし	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
このリリースによってサポートされる新しい RFC や変更された RFC 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドの詳細については、『*Cisco IOS Carrier Ethernet Command Reference*』（http://www.cisco.com/en/US/docs/ios/carrier_ethernet/command/reference/ce_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html にある『*Cisco IOS Master Command List, All Releases*』を参照してください。

- **interface**
- **mac access-group in**
- **mac access-list extended**
- **show ethernet service instance**

EVC 上のレイヤ 2 アクセス コントロール リストに関する機能情報

表 2 に、この機能のリリース履歴を示します。

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、Catalyst OS、Cisco IOS XE 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。

（注） 表 2 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 2　EVC 上のレイヤ 2 アクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
EVC 上のレイヤ 2 アクセス コントロール リスト	12.2(33)SRD 15.0(1)S	EVC 上のレイヤ 2 アクセス コントロール リスト機能によって、EVC に ACL が導入されます。 次のコマンドが、新たに導入または変更されました。**interface**、**mac access-group in**、**mac access-list extended**、**show ethernet service instance**