



レイヤ2アクセスコントロールリスト

イーサネットサービスアクセスコントロールリスト (ACL) は、レイヤ2ネットワークトラフィックプロファイルを集散的に定義する1つ以上のアクセスコントロールエントリ (ACE) で構成されます。このプロファイルは、Cisco IOS XR ソフトウェア機能で参照できます。各イーサネットサービス ACL には、送信元および宛先アドレス、サービスクラス (CoS)、ether-type、または 802.1ad DEI などの基準に基づいたアクション要素 (許可または拒否) が含まれます。

レイヤ2ACLは入力トラフィックのみでサポートされています。出力トラフィックでは、レイヤ2 ACL はサポートされていません。

また、レイヤ2アクセスコントロールリストはイーサネットサービスコントロールアクセスリストとも呼ばれています。

- [レイヤ2アクセスコントロールリスト設定の前提条件 \(1 ページ\)](#)
- [レイヤ2アクセスコントロールリスト機能の特長 \(2 ページ\)](#)
- [レイヤ2アクセスコントロールリストの目的 \(2 ページ\)](#)
- [レイヤ2アクセスコントロールリストの仕組み \(2 ページ\)](#)
- [レイヤ2アクセスコントロールリストのプロセスとルール \(2 ページ\)](#)
- [レイヤ2アクセスコントロールリストの作成 \(3 ページ\)](#)
- [レイヤ2アクセスコントロールリスト設定の制約事項 \(4 ページ\)](#)
- [設定 \(4 ページ\)](#)

レイヤ2アクセスコントロールリスト設定の前提条件

この前提条件は、アクセスコントロールリストおよびプレフィックスリストの設定に適用されます。

適切なタスク ID を含むタスクグループに関連付けられているユーザグループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれません。

ユーザグループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

レイヤ2アクセスコントロールリスト機能の特長

レイヤ2アクセスコントロールリストには次の機能上の特長があります。

- 特定のシーケンス番号を使用してアクセスリストのカウンタをクリアする機能。
- 別のアクセスリストに既存のアクセスリストの内容をコピーする機能。
- ユーザがシーケンス番号を `permit` ステートメントまたは `deny` ステートメントに適用できること。
- レイヤ2ACLはインターフェイス、VLANサブインターフェイス、バンドルイーサネットインターフェイス、L2ポートのあるバンドルサブインターフェイス上に適用できること。レイヤ2ACLのアトミックな置換は、これらの物理インターフェイスとバンドルインターフェイス上でサポートされています。

レイヤ2アクセスコントロールリストの目的

レイヤ2アクセスコントロールリストは、パケットフィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。そのような制御は、着信および発信ネットワークトラフィックを制限し、ポートレベルでネットワークにユーザおよびデバイスのアクセスを制限するために役立ちます。

レイヤ2アクセスコントロールリストの仕組み

レイヤ2アクセスコントロールリストは、レイヤ2設定に適用される `permit` および `deny` ステートメントで構成された順序付きリストです。アクセスリストには、参照に使用される名前があります。

アクセスリストを設定して名前を付けることは可能ですが、アクセスリストを受け取るコマンドによってアクセスリストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセスリストを参照できます。アクセスリストはルータに着信するレイヤ2トラフィックを制御できますが、ルータを起点とするトラフィックやルータを離れるトラフィックは制御できません。

レイヤ2アクセスコントロールリストのプロセスとルール

レイヤ2アクセスコントロールリストを設定する際に、次のプロセスとルールを使用します。

- ソフトウェアは、アクセスリストの条件に対してフィルタされる各パケットの送信元アドレスや宛先アドレスをテストします。一度に1つの条件（**permit** または **deny** ステートメント）がテストされます。
- パケットがアクセスリストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセスリストのステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセスリストがアドレスまたはプロトコルを拒否する場合は、ソフトウェアはパケットを廃棄します。
- 各アクセスリストの最後には暗黙の **deny** ステートメントがあるため、一致する条件がない場合は、パケットはドロップされます。つまり、各ステートメントに対してテストするときまでにパケットを許可または拒否しないと、パケットは拒否されます。
- アクセスリストには **permit** ステートメントを1つ以上含める必要があります。そうしないと、パケットはすべて拒否されます。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- インバウンドアクセスリストは、ルータに到達するパケットを処理します。インバウンドアクセスリストが効率的なのは、フィルタリングテストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンドリストの場合、**permit** とは、インバウンドインターフェイスで受信したパケットを引き続き処理することを意味します。**deny** とは、パケットを破棄することです。
- アクセスリストは、使用中のアクセスグループによって適用されている場合には削除できません。アクセスリストを削除するには、まずアクセスリストを参照しているアクセスグループを削除してから、アクセスリストを削除します。
- アクセスリストは、**ethernet-services access-group** コマンドを使用する前に存在している必要があります。

レイヤ2アクセスコントロールリストの作成

レイヤ2アクセスコントロールリストを作成するときは以下を考慮します。

- アクセスリストは、インターフェイスに適用する前に作成します。
- より具体的な参照が、より全般的な参照よりも前に出現するように、アクセスリストを構成します。

レイヤ2アクセスコントロールリスト設定の制約事項

次の制約事項は、レイヤ2アクセスコントロールリストの設定に適用されます。

- レイヤ2アクセスコントロールリストは、管理インターフェイスではサポートされていません。
- NetIO（ソフトウェア低速パス）は、レイヤ2アクセスコントロールリストではサポートされていません。
- レイヤ2アクセスコントロールリストは、インターフェイスの入力方向にのみ付加できます。
- レイヤ2アクセスコントロールリストではCOS（サービスクラス）とDEI（Discard Eligibility Indication）のみがサポートされています。

設定

この項では、レイヤ2アクセスコントロールリストを設定する方法について説明します。

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if-l2)# commit
Router(config-if-l2)# exit
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

実行コンフィギュレーション

```
!
Configure
ethernet-services access-list es_acl_1
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
!
```

確認

レイヤ2アクセスコントロールリストが設定されていることを確認します。

```
/* Verify the Layer 2 access control lists configuration */
```

```
Router# show access-lists ethernet-services es_acl_1 hardware ingress location 0/0/CPU0

Fri Oct 21 09:39:52.904 UTC
ethernet-services access-list es_acl_1
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff (2051 matches)
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei (2050 matches)
```

