レイヤ 2 アクセス コントロール リストの設定

この章では、レイヤ 2 アクセス コントロール リストについて紹介し、レイヤ 2 アクセス コントロール リストの設定方法について説明します。

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 プロファイルを集合的に定義する 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 2 ACL 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

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 が含まれます。

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2 ACL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2 ACL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)
```

確認