



MAC ACL の設定

この章では、Cisco NX-OS デバイスの MAC アクセス コントロール リスト (ACL) を設定する手順について説明します。

この章は、次の項で構成されています。

- [MAC ACL について, on page 1](#)
- [MAC ACL の注意事項と制約事項 \(2 ページ\)](#)
- [MAC ACL のデフォルト設定, on page 3](#)
- [MAC ACL の設定, on page 3](#)
- [MAC ACL の設定の確認, on page 9](#)
- [MAC ACL の統計情報のモニタリングとクリア, on page 10](#)
- [MAC ACL の設定例, on page 10](#)
- [MAC ACL に関する追加情報, on page 10](#)

MAC ACL について

MAC ACL は、パケットのレイヤ 2 ヘッダーを使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。

MAC パケット分類

MAC パケット分類により、レイヤ 2 インターフェイス上の MAC ACL を、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用するか、非 IP トラフィックだけに適用するかを制御できます。

MAC パケット分類の状態	インターフェイスでの効果
イネーブル	• インターフェイス上の MAC ACL は、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用されます。 • IP ポート ACL をインターフェイスで適用できません。

MAC パケット分類の状態	インターフェイスでの効果
ディセーブル	• インターフェイス上の MAC ACL は、インターフェイスに入る非 IP トラフィックだけに適用されます。 • IP ポート ACL をインターフェイスで適用できます。

MAC ACL の注意事項と制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- MAC ACL は入トラフィックだけに適用されます。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- MAC ACL が VACL の一部として適用される場合、MAC パケット分類はサポートされません。
- MAC ACL が Cisco Nexus 9300 シリーズ スイッチ 40G アップリンク ポートの QoS ポリシーの一致基準として使用されている場合、MAC パケット分類はサポートされません。
- EX/FX 以外の Cisco Nexus 9000 シリーズ スイッチで MAC ACL を定義する場合は、トラフィックが適切に照合されるように **ethertype** を定義する必要があります。
- Cisco Nexus 9300-EX プラットフォーム スイッチでは、Mac パケット分類が部分的にサポートされています。パケットを L2 パケットとしてマーキングするための直接のフィールドがない場合、スイッチは、キーフィールド内に特定のフィールド (**src_mac**、**dst_mac**、**vlan** など) があるすべてのパケットのマッチングを行います。ただし、**eth_type** フィールドではマッチングを行いません。したがって、MAC プロトコル番号フィールドを除いて同一のフィールドを持つ 2 つのルールをインストールすると、マッチング条件はハードウェアで同一のままになります。したがって、ルールシーケンスの最初のエントリは、すべてのプロトコル番号のすべてのパケットに対してヒットしますが、**mac-packet** 分類が設定されている場合の MAC プロトコル番号は **no-op** になります。
- インターフェイスに適用される MAC アクセス リストは、スパニングツリー プロトコル BPDU などのブリッジ プロトコル データ ユニット (BPDU) トラフィックをブロックしません。

MAC ACL のデフォルト設定

次の表に、MAC ACL パラメータのデフォルト設定を示します。

Table 1: MAC ACL のデフォルト パラメータ

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	mac access-list name Example: switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	MAC ACL を作成して、ACL 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	{permit deny} source destination-protocol Example: switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	MAC ACL 内にルールを作成します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) statistics per-entry Example: switch(config-mac-acl)# statistics per-entry	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。

	Command or Action	Purpose
ステップ 5	(Optional) show mac access-lists <i>name</i> Example: <pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	MAC ACL の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-mac-acl)# copy running-config startup-config</pre>	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コピーします。

MAC ACL の変更

MAC ACL をデバイスから削除できます。

Before you begin

MAC ACL が設定されているインターフェイスを探すには、**show mac access-lists** コマンドを、**summary** キーワードを指定して実行します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	mac access-list <i>name</i> Example: <pre>switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#</pre>	名前で指定した ACL の ACL 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	(Optional) [<i>sequence-number</i>] { permit deny } <i>source destination-protocol</i> Example: <pre>switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806</pre>	MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。

	Command or Action	Purpose
ステップ 4	(Optional) no {sequence-number { permit deny } source destination-protocol} Example: <pre>switch(config-mac-acl)# no 80</pre>	指定したルールを MAC ACL から削除します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	(Optional) [no] statistics per-entry Example: <pre>switch(config-mac-acl)# statistics per-entry</pre>	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 no オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	(Optional) show mac access-lists name Example: <pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	MAC ACL の設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-mac-acl)# copy running-config startup-config</pre>	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コピーします。

MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 2	resequence mac access-list name starting-sequence-number increment Example: <pre>switch(config)# resequence mac access-list acl-mac-01 100 10</pre>	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい

	Command or Action	Purpose
		番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	(Optional) show mac access-lists name Example: <pre>switch(config)# show mac access-lists acl-mac-01</pre>	MAC ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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コピーします。

MAC ACL の削除

MAC ACL をデバイスから削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	no mac access-list name Example: <pre>switch(config)# no mac access-list acl-mac-01 switch(config)#</pre>	名前で指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	(Optional) show mac access-lists name summary Example: <pre>switch(config)# show mac access-lists acl-mac-01 summary</pre>	MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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コピーします。

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャンネル インターフェイス

Before you begin

適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: switch(config)# interface ethernet 2/1 switch(config-if)# Example: switch(config)# interface port-channel 5 switch(config-if)#	• レイヤ 2 またはレイヤ 3 のインターフェイス コンフィギュレーションモードを開始します。 • レイヤ 2 またはレイヤ 3 のポート チャンネル インターフェイスのインターフェイス コンフィギュレーションモードを開始します。
ステップ 3	mac port access-group access-list Example: switch(config-if)# mac port access-group acl-01	MAC ACL をインターフェイスに適用します。
ステップ 4	(Optional) show running-config aclmgr Example: switch(config-if)# show running-config aclmgr	ACL の設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	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コピーします。

MAC ACL の VACL としての適用

MAC ACL を VACL として適用できます。

MAC パケット分類のイネーブル化または無効化

レイヤ 2 インターフェイスに対して MAC パケット分類を有効または無効に設定できます。

始める前に

インターフェイスを、レイヤ 2 インターフェイスとして設定する必要があります。



(注) インターフェイスが **ip port access-group** コマンドまたは **ipv6 port traffic-filter** コマンドを使用して設定されている場合は、インターフェイス コンフィギュレーションから **ip port access-group** コマンドおよび **ipv6 port traffic-filter** コマンドを削除しない限り、MAC パケット分類を有効にできません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 interface ethernet slot/port interface port-channel channel-number 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例 :	- イーサネット インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 - ポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	<pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	
ステップ 3	[no] mac packet-classify 例 : <pre>switch(config-if)# mac packet-classify</pre>	インターフェイスの MAC パケット分類を有効にします。 no オプションを使用すると、インターフェイスの MAC パケット分類が無効になります。
ステップ 4	(任意) 次のいずれかのコマンドを入力します。 • show running-config interface ethernet slot/port • show running-config interface port-channel channel-number 例 : <pre>switch(config-if)# show running-config interface ethernet 2/1</pre> 例 : <pre>switch(config-if)# show running-config interface port-channel 5</pre>	• イーサネット インターフェイスの実行コンフィギュレーションを表示します。 • ポート チャネル インターフェイスの実行コンフィギュレーションを表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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コピーします。

MAC ACL の設定の確認

MAC ACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr [all]	MAC ACL および MAC ACL が適用されるインターフェイスを含めて、ACL の設定を表示します。 Note このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、実行コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。

コマンド	目的
show startup-config aclmgr [all]	ACL のスタートアップ コンフィギュレーションを表示します。 Note このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。

MAC ACL の統計情報のモニタリングとクリア

MAC ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に statistics per-entry コマンドが含まれている場合は、 show mac access-lists コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear mac access-list counters	MAC ACL の統計情報をクリアします。

MAC ACL の設定例

次に、acl-mac-01 という名前の MAC ACL を作成し、これをイーサネット インターフェイス 2/1 (レイヤ 2 インターフェイス) に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any 0x0806
interface ethernet 2/1
  mac port access-group acl-mac-01
```

MAC ACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
TAP アグリゲーション	『Configuring TAP Aggregation and MPLS Stripping』

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。