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

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。

（注） MAC パケット分類は、Cisco NX-OS リリース 9.3(3) ではサポートされていません。

MAC パケット分類の状態	インターフェイスでの効果
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。
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 パケット分類がは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。
- **mac address-table limit <16-256> user-defined** コマンドを使用してユーザ定義の MAC 制限を設定すると、FHRP グループ制限が自動的に調整され、ユーザ定義の MAC 制限と FHRP 制限の合計は 490 になります。たとえば、ユーザ定義の MAC 制限を 100に 設定すると、FHRP 制限は 390 に減少します。
- Cisco NX-OS リリース 9.3(2) 以降では、ユーザ定義の MAC アドレス制限を 16 ー 256 の範囲で設定できます。

- Cisco Nexus 93600CD-GX スイッチは、ポート 1/1-24 でのブレークアウトをサポートしていません。

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 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	**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。

	Command or Action	Purpose
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。
ステップ 5	(Optional) **show mac access-lists** *name* **Example:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	MAC ACL の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

UDF ベースの MAC ACL の設定

Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチの UDF ベースの MAC アクセス リスト（ACL）を設定できます。この機能により、デバイスはユーザ定義フィールド（UDF）で照合し、一致するパケットを MAC ACL に適用できます。

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチで UDF ベース MAC アクセス リスト（ACL）を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	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	**udf** *udf-name offset-base offset length* 例： `switch(config)# udf pktoff10 packet-start 10 2`	次のように UDF を定義します。 • *udf-name*：UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • *offset-base*：UDF オフセット ベースを {**packet-start**} のように指定します。 • オフセット：オフセットベースからバイトオフセットの数を指定します。

	コマンドまたはアクション	目的
		• 長さ：オフセットからバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。 複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	**hardware access-list tcam region ing-ifacl qualify** {**udf** *udf-name* } 例： `switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10`	IPv4 または IPv6 ポート ACLに適用する ing-ifacl TCAM リージョンに UDF をアタッチします。 最大 18 個の UDF がサポートされます。 （注） UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがあることを確認してください。それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「ACL TCAM リージョン サイズの設定」を参照してください。 （注） このコマンドの **no** 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。
ステップ 4	必須: **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に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て、変更を継続的に保存します。
ステップ 5	必須: **reload** 例：	デバイスがリロードされます。

	コマンドまたはアクション	目的
	`switch(config)# reload`	（注） UDF 設定は **copy running-config startup-config** + **reload** を入力した後のみ有効になります。

ステップ 6	**mac access-list** *udf-acl*
	例：
	`switch(config)# mac access-list udfacl`
	`switch(config-acl)#`
		MAC アクセス コントロール リスト（ACL）を作成して、MAC 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 7	**permit mac** *source destination* **udf** *udf-name value mask* 例： `switch(config-acl)# permit mac any any udf pktoff10 0x1234 0xffff`	MAC ACL を 設定して、外部パケット フィールドについて現在のアクセス コントロールエントリ（ACE）と併せて UDF で一致させるように設定します（例 2）。値とマスクの引数の範囲は 0x0～0xFFFF です。 シングル ACL は、UDF がある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。

ステップ 8	**interface port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		レイヤ 2 のポート 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。

ステップ 9	**mac port access-group** *udf-access-list* 例： `switch(config-if)# mac port access-group udf-acl-01`	UDF ベース MAC ACL をインターフェイスに適用します。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

インターフェイス MAC アドレスの設定と制限

SVI、レイヤ 3インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネル インターフェイスにスタティック MAC アドレスを設定できます。ポートおよびポー

トチャネルの範囲でスタティック MAC アドレスを設定することもできます。ただし、すべてのポートがレイヤ 3 にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラー メッセージが表示されます。

デフォルトでは、スイッチに設定できる MAC アドレスの最大数は 16 です。ただし、この制限を変更して、MAC アドレス数の範囲を 16 ー 256 に設定することができます。

vPC 対応スイッチでの設定制限には、ローカルに設定されたユーザ定義の MAC アドレスと、vPC ピアから同期されたユーザ定義の MAC アドレスの両方が含まれます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	[**no**] **mac-address** *static router MAC address* **例：** `switch(config-if)# mac-address 0019.D2D0.00AE`	インターフェイスに MAC アドレスを設定します。設定を削除するには、このコマンドの no 形式を使用します。MAC アドレスは、サポートされている次の4つの形式のいずれかで入力できます。 • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE （注） 次の無効な MAC アドレスは入力しないでください。 • ヌル MAC アドレス：0000.0000.0000 • ブロードキャスト MAC アドレス：FFFF.FFFF.FFFF • マルチキャスト MAC アドレス：0100.DAAA.ADDD

	コマンドまたはアクション	目的

ステップ 4	（任意） **show interface ethernet** *slot/port*
	例：
	`switch(config-if)# show interface ethernet 2/1`
	`switch(config)#`
		インターフェイスのすべての情報を表示します。

ステップ 5	**mac address-table limit** *16-256* **user-defined**
	例：
	`switch(config)# mac address-table limit 200 user-defined`
	`switch(config)#`
		スイッチに設定できるMACアドレスの最大数を設定します。

ステップ 6	（任意） **show mac address-table limit user-defined** 例： `switch(config)# show mac address-table limit user-defined`	スイッチに設定できるMACアドレスの最大数を表示します。

例

次に、インターフェイス MAC アドレスを設定する方法の例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
switch(config)# mac address-table limit 100 user-defined
Warning: Configure the same User-Defined Mac Limit on the peer.
Warning: New Fhrp max group limit is 390
switch# show  mac address-table limit user-defined
User Defined Mac Limit: 100
FHRP Mac Limit: 390
==============
```

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:
	`switch# configure terminal`
	`switch(config)#`
		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	**mac access-list** *name*
	Example:
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		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) [*sequence-number*] {**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。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。
ステップ 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *source destination-protocol*} **Example:** `switch(config-mac-acl)# no 80`	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:** `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。 **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:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	MAC ACL の設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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:
	`switch# configure terminal`
	`switch(config)#`
		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:** `switch(config)# resequence mac access-list acl-mac-01 100 10`	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:** `switch(config)# show mac access-lists acl-mac-01`	MAC ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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:
	`switch# configure terminal`
	`switch(config)#`
		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。

	Command or Action	Purpose

ステップ 2	**no mac access-list** *name*
	Example:
	`switch(config)# no mac access-list acl-mac-01`
	`switch(config)#`
		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:** `switch(config)# show mac access-lists acl-mac-01 summary`	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:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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 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	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:**	• 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 チャネル インターフェイスのイン

	Command or Action	Purpose

	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		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。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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：
	`switch# configure terminal`
	`switch(config)#`
		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	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：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• 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。

ステップ 3	[**no**] **mac packet-classify** 例： `switch(config-if)# mac packet-classify`	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：
	`switch(config-if)# show running-config interface ethernet 2/1`
	例：
	`switch(config-if)# show running-config interface port-channel 5`
		• 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： `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。
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』