MAC ACL の設定

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

この章の内容は、次のとおりです。

- MAC ACL の概要，1 ページ
- MAC ACL のライセンス要件，2 ページ
- MAC ACL の前提条件，3 ページ
- MAC ACL の注意事項と制約事項，3 ページ
- MAC ACL のデフォルト設定，3 ページ
- MAC ACL の設定，4 ページ
- MAC ACL の設定の確認，12 ページ
- MAC ACL の統計情報のモニタリングとクリア，13 ページ
- MAC ACL の設定例，13 ページ
- MAC ACL に関する追加情報，14 ページ
- MAC ACL の機能の履歴，14 ページ

MAC ACL の概要

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。

関連トピック

ACL について

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。
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。

関連トピック

MAC パケット分類のイネーブル化またはディセーブル化, （10 ページ）

MAC ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	MAC ACL にはライセンスは必要ありません。ただし、XL ラインカードを使用して最大 128K の ACL エントリをサポートするには、スケーラブルなサービスライセンスをインストールする必要があります。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

MAC ACL の前提条件

MAC ACL を設定するための前提条件はありません。

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。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。
- サポートされる MAC ACL エントリの最大数は、XL ラインカードを使用しないデバイスで 64K、XL ラインカードを使用するデバイスで 128K です。
- XL 以外のラインカードに適用する ACL エントリが多すぎると、設定が拒否されます。
- F1 シリーズ モジュールの各転送エンジンは 1000 の入力 ACL エントリをサポートします。 また、984 のエントリがユーザ設定に使用できます。 F1 シリーズ モジュールでの MAC ACL エントリの総数は、ポリシーがどの転送エンジンで適用されるかに応じて 1000 ～ 16,000 です。
- F1 シリーズ モジュールの 16 の転送エンジンごとに、複数の ACL で最大 250 の IPv6 アドレスをサポートします。
- F1 シリーズ モジュールには、ACL ロギングをサポートしていません。
- F1 シリーズ モジュールはバンク チェーニングをサポートしていません。
- M シリーズ モジュールでは、**mac packet-classify** コマンドによってポートおよび VLAN ポリシーの MAC ACL がイネーブルになります F2 シリーズ モジュールの場合、**mac packet-classify** コマンドにより、VLAN ポリシーの IPv4 ACL または IPv6 ACL ではなく、ポート ポリシーの MAC ACL をイネーブルにします。
- F2 シリーズ モジュールの 12 の転送エンジンごとに、総数 16,000 の TCAM エントリが 2 つのバンクに対して均等に分割されます。 デフォルトの 168 エントリが予約されます。 各転送エンジンは、512 の IPv6 圧縮 TCAM エントリを持ちます。

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。

表 *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。

パラメータ	デフォルト
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。

手順の概要

1. **configure terminal**
2. **mac access-list** *name*
3. {**permit** | **deny**} *source destination protocol*
4. （任意） **statistics per-entry**
5. （任意） **show mac access-lists** *name*
6. （任意） **copy running-config startup-config**

手順の詳細

	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	**mac access-list** *name*
	
	例：
	`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* 例： `switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	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。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 4	**statistics per-entry** 例： `switch(config-mac-acl)# statistics per-entry`	（任意） 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	**show mac access-lists** *name* 例： `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-mac-acl)# copy running-config startup-config`	（任意） 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。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **mac access-list** *name*
3. （任意） [*sequence-number*] {**permit** | **deny**} *source destination protocol*
4. （任意） **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}
5. （任意） [**no**] **statistics per-entry**
6. （任意） **show mac access-lists** *name*
7. （任意） **copy running-config startup-config**

手順の詳細

	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	**mac access-list** *name*
	
	例：
	`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	[*sequence-number*] {**permit** | **deny**} *source destination protocol* 例： `switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	（任意） 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。 詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} 例： `switch(config-mac-acl)# no 80`	（任意） 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。 詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** 例： `switch(config-mac-acl)# statistics per-entry`	（任意） 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	**show mac access-lists** *name* 例： `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config-mac-acl)# copy running-config startup-config`	（任意） 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。

手順の概要

1. **configure terminal**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. （任意） **show mac access-lists** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	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	**resequence mac access-list** *name starting-sequence-number increment* 例： `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	**show mac access-lists** *name* 例： `switch(config)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

手順の概要

1. **configure terminal**
2. **no mac access-list** *name*
3. （任意） **show mac access-lists** *name* **summary**
4. （任意） **copy running-config startup-config**

手順の詳細

	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	**no mac access-list** *name*
	
	例：
	`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	**show mac access-lists** *name* **summary** 例： `switch(config)# show mac access-lists acl-mac-01 summary`	（任意） 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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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 のポート ACL としての適用

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 またはレイヤ 3 のイーサネット インターフェイス
- 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

はじめる前に

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。

手順の概要

1. **configure terminal**
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*
3. **mac port access-group** *access-list*
4. （任意） **show running-config aclmgr**
5. （任意） **copy running-config startup-config**

手順の詳細

	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)#`
		• 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

	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`	

ステップ 3	**mac port access-group** *access-list* 例： `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	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 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。

関連トピック

VACL の設定

MAC パケット分類のイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対して MAC パケット分類をイネーブルまたはディセーブルに設定できます。

はじめる前に

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 パケット分類をイネーブルにできません。

手順の概要

1. **configure terminal**
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*
3. [**no**] **mac packet-classify**
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*
5. （任意） **copy running-config startup-config**

手順の詳細

	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。
		• 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 パケット分類をイネーブルにします。 **no** オプションを使用すると、インターフェイスの MAC パケット分類がディセーブルになります。
ステップ 4	次のいずれかのコマンドを入力します。 • **show running-config interface ethernet** *slot*/*port*	（任意） • 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。

	コマンドまたはアクション	目的

	• **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`
		• 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	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 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。

関連トピック

MAC パケット分類, （2 ページ）

MAC ACL の設定の確認

MAC ACL の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。 これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

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。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、実行コンフィギュレーションのユーザ定義 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。 （注） Cisco NX-OS Release 5.2 以降では、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定義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 に関する統計情報（各ルールに一致したパケットの数など）をモニタするには、**show mac access-lists** コマンドを使用します。

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。 これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

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	すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。

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
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
MAC ACL コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。	—

MAC ACL の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2*：*MAC ACL* の機能の履歴

機能名	リリース	機能情報
MAC ACL	6.1(1)	M2 シリーズモジュールが更新されました。
MAC ACL	6.0(1)	F2 シリーズ モジュールが更新されました。

機能名	リリース	機能情報
MAC ACL	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
MAC ACL	5.0(2)	スケーラブルなサービスライセンスがインストールされており、XL ラインカードを使用している場合、最大 128,000 の ACL エントリがサポートされるようになりました。
MAC ACL	4.2(1)	MAC パケット分類がサポートされるようになりました。