CHAPTER 10

MAC ACL の設定

この章では、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次の内容で説明します。

MAC ACL の概要

MAC ACL は、各パケットのレイヤ 2 ヘッダー内の情報を使用してトラフィックをフィルタリングする ACL です。

MAC ACL の前提条件

MAC ACL の前提条件は次のとおりです。

- MAC ACL を設定するために、MAC アドレッシングおよびプロトコルに関する知識があること。
- 「ACL の概要」（P.9-1）に記載されている内容を理解していること。

注意事項および制約事項

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。

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。この場合、速度は遅くなります。
- ACL は、ポート チャネルではサポートされていません。

デフォルト設定

表 10-1 に、MAC ACL のデフォルトを示します。

表 10-1　MAC ACL パラメータのデフォルト値

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 に暗黙ルールが適用されます（「暗黙ルール」（P.9-3）を参照）。

MAC ACL の設定

ここでは、次の内容について説明します。

MAC ACL の作成

MAC ACL を作成し、これにルールを追加するには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。

手順の概要

1. **config t**
2. **mac access-list** *name*
3. {**permit** | **deny**} *source destination protocol*
4. **statistics per-entry**

5. **show mac access-lists** *name*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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：
	`n1000v(config)# mac access-list acl-mac-01`
	`n1000v(config-mac-acl)#`
		MAC ACL を作成し、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： `n1000v(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	MAC ACL のルールを作成します。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。
ステップ 4	**statistics per-entry** 例： `n1000v(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： `n1000v(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： `n1000v(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

既存の MAC ACL にルールの追加や削除などの変更を行うには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 既存の MAC ACL では、既存のルールを変更できません。
- 既存の MAC ACL に対しては、ルールの追加と削除を行うことができます。
- 既存のシーケンス番号の間にルールを追加する場合などに、シーケンス番号を再割り当てするには、**resequence** コマンドを使用します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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： n1000v(config)# mac access-list acl-mac-01 n1000v(config-mac-acl)#	名前を指定する 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： n1000v(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any	（任意）MAC ACL のルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、最後のルールの後ろに追加されます。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} 例： n1000v(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** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** 例： n1000v(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。

	コマンド	目的
ステップ 6	**show mac access-lists** *name* 例： n1000v(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 7	**copy running-config startup-config** 例： n1000v(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 の削除

MAC ACL を削除するには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- その ACL がインターフェイスに適用されているかどうかを確認します。
- 現在適用されている ACL を削除できます。ACL を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。削除された ACL は空であると見なされます。
- MAC ACL が設定されているインターフェイスを見つけるには、**show mac access-lists** コマンドを **summary** キーワードとともに使用します。

手順の概要

1. **config t**
2. **no mac access-list** *name*
3. **show mac access-lists** *name* **summary**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** n1000v# config t n1000v(config)#	CLI 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：** n1000v(config)# no mac access-list acl-mac-01 n1000v(config)#	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：** n1000v(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：** n1000v(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 のシーケンス番号の変更

MAC ACL のルールに割り当てられているシーケンス番号を変更するには、次の手順を実行します。シーケンス番号の変更は、ACL にルールを挿入する必要があり、使用できるシーケンス番号が十分にない場合に役立ちます。詳細については、「MAC ACL のシーケンス番号の変更」（P.10-6）を参照してください。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。

手順の概要

1. **config t**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. **show mac access-lists** *name*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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：** `n1000v(config)# resequence mac access-list acl-mac-01 100 10`	ACL 内のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。それ以降の各ルールには、前のルールよりも一定数だけ大きい番号が割り当てられます。番号の差異は、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：** `n1000v(config)# show mac access-lists acl-mac-01`	（任意）MAC ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(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。

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として適用するには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 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。MAC ACL の設定の詳細については、「MAC ACL の設定」（P.10-2）を参照してください。
- MAC ACL は、ポート プロファイルを使用してポートに適用することもできる。詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*』を参照してください。

手順の概要

1. **config t**
2. **interface vethernet** *port*
3. **mac port access-group** *access-list* [**in** | **out**]
4. **show running-config aclmgr**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 vethernet** *port*
	
	例：
	`n1000v(config)# interface vethernet 35`
	`n1000v(config-if)#`
		指定した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* [**in** | **out**] **例：** `n1000v(config-if)# mac port access-group acl-01 in`	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：** `n1000v(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：** `n1000v(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、次のいずれかのコマンドを使用します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr	MAC ACL およびこの ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show running-config interface	ACL を適用したインターフェイスの設定を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Security Command Reference*』を参照してください。

MAC ACL の統計情報の表示とクリア

各ルールと一致したパケット数を含めて、MAC ACL についての統計情報を表示またはクリアするには、次のコマンドを使用します。

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	すべての MAC ACL または特定の MAC ACL の統計情報をクリアします。

これらのコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

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 vethernet 35
mac port access-group acl-mac-01 in
```

その他の関連資料

MAC ACL の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.10-9）
- 「標準規格」（P.10-9）

関連資料

関連項目	マニュアル タイトル
ACL の概念	*「ACL の概要」（P.9-1）*

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MAC ACL 機能の履歴

ここでは、MAC ACL のリリース履歴を示します。

機能名	リリース	機能情報
MAC ACL	4.0	この機能が追加されました。