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」（P.10-1）
- 「MAC ACL の前提条件」（P.10-1）
- 「注意事項および制約事項」（P.10-2）
- 「デフォルト設定」（P.10-2）
- 「MAC ACL の設定」（P.10-2）
- 「MAC ACL の設定の確認」（P.10-9）
- 「MAC ACL のモニタリング」（P.10-10）
- 「MAC ACL の設定例」（P.10-11）
- 「その他の関連資料」（P.10-11）
- 「MAC ACL 機能の履歴」（P.10-12）

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 について」（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 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 に暗黙ルールが適用されます（「暗黙のルール」（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」（P.10-2）
- 「MAC ACL の変更」（P.10-4）
- 「MAC ACL の削除」（P.10-5）
- 「MAC ACL 内のシーケンス番号の変更」（P.10-6）
- 「MAC ACL のポート ACL としての適用」（P.10-7）
- 「MAC ACL のポート プロファイルへの追加」（P.10-8）

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。また、ACL をポート プロファイルに追加する場合にも、次の手順を実行します。

はじめる前に

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 にログインしていること。
- 作成する ACL に割り当てる名前があること。
- また、ポートプロファイルに ACL も追加する場合は、次の事項がわかっていること。

- 既存のポート プロファイルを使用する場合は、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』に従ってすでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- アクセス リストのパケット フローの方向を知っています。

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：** `n1000v(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 1000V Command Reference, Release 4.2(1)SV1(5.1)*』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）確認のために MAC ACL 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 を変更して、ルールの追加または削除を行うには、次の手順を実行します。

はじめる前に

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 にログインしていること。
- 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 内で、ルールの追加または削除を実行できます。
- 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 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 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

	コマンド	目的
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} 例： n1000v(config-mac-acl)# no 80	（任意）MAC ACL から指定したルールを削除します。 **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 1000V Command Reference, Release 4.2(1)SV1(5.1)*』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。
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。

はじめる前に

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 にログインしていること。
- 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 が適用されていたインターフェイスの設定は影響を受けません。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 内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。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。詳細については、「MAC ACL 内のシーケンス番号の変更」（P.10-6）を参照してください。

はじめる前に

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 にログインしていること。

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： 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。

MAC ACL のポート ACL としての適用

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。

はじめる前に

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 にログインしていること。
- 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。ポート プロファイルについては、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』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 のポート プロファイルへの追加

MAC ACL をポート プロファイルに追加するには、次の手順を実行します。

はじめる前に

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 にログインしていること。
- 「MAC ACL の作成」（P.10-2）の手順に従ってこのポート プロファイルに追加する MAC ACL をすでに作成しており、名前を知っていること。
- 既存のポート プロファイルを使用する場合は、すでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
- アクセス リストのパケット フローの方向を知っています。

手順の概要

1. **config t**

2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **mac port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明
ステップ 1	**config t** 例： n1000v# config t n1000v(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	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* 例： n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	名前付きポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**mac port access-group** *name* {**in** | **out**} 例： n1000v(config-port-prof)# mac port access-group allaccess4 out	着信トラフィックまたは発信トラフィックのポート プロファイルに名前付き ACL を追加します。
ステップ 4	**show port-profile name** *profile-name* 例： n1000v(config-port-prof)# show port-profile name AccessProf	（任意）確認のために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： n1000v(config-port-prof)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

MAC ACL の設定の確認

次のコマンドを使用して、MAC ACL 設定を確認できます。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。 例 10-1（P.10-10）を参照してください。
show running-config aclmgr	MAC ACL、MAC ACL が適用されるインターフェイスなど、MAC ACL の設定を表示します。 例 10-2（P.10-10）を参照してください。
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。 例 10-3（P.10-10）を参照してください。

例 10-1　show mac access-list

```
n1000v# show mac access-list

MAC access list acl-mac-01
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
n1000v#
```

例 10-2　show running-config aclmgr

```
n1000v# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Mon Jan  3 15:53:50 2011

version 4.2(1)SV1(4)
mac access-list acl-mac-01
  10 permit 00c0.4f00.0000 0000.00ff.ffff any

interface Vethernet35
  mac port access-group acl-mac-01 in

n1000v#
```

例 10-3　show running-config interface

```
n1000v# show running-config interface

!Command: show running-config interface
!Time: Mon Jan  3 15:58:25 2011

version 4.2(1)SV1(4)

interface mgmt0
  ip address 172.23.180.75/24

interface Vethernet35
  mac port access-group acl-mac-01 in

interface Vethernet1998

interface control0
  ip address 10.2.10.10/24

n1000v#
```

MAC ACL のモニタリング

MAC ACL のモニタリングには、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 の統計情報を消去します。

MAC ACL の設定例

次に、MAC ACL acl-mac-01 を作成して任意のプロトコルの MAC 00c0.4f00.00.000.00ff.ffff を許可し、ACL を vEthernet インターフェイス 35 の発信トラフィックのポートとして適用する例を示します。

```
config t
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface vethernet 35
mac port access-group acl-mac-01 out
```

次に、ポート プロファイル *AccessProf* に MAC ACL *allaccess4* を追加する例を示します。

```
config t
port-profile AccessProf
mac port access-group allaccess4 out
show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    mac port access-group allaccess4 out
  evaluated config attributes:
    mac port access-group allaccess4 out
  assigned interfaces:
```

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.10-12）
- 「標準」（P.10-12）

関連資料

関連項目	参照先
ACL の概念。	*「ACL について」（P.9-1）*
インターフェイスの設定。	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』
ポート プロファイルの設定。	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』
Cisco Nexus 1000V のすべてのコマンドのコマンド構文、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、および例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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(4)SV1(1)	この機能が導入されました。