# MAC ACL の設定

この章の内容は、次のとおりです。



## 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 を設定するためには、MAC アドレッシングおよびプロトコルに関する知識が必要です。
- このマニュアルで示す ACL の概念を理解している必要があります。

# MAC ACL の注意事項と制約事項

- 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。

# MAC ACL のデフォルト設定

| 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、次の作業を実行したことを確認してください。

- CLI に EXEC モードで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。
- ACL をポート プロファイルに追加する場合は、そのポート プロファイルが作成されていること。

また、ポート プロファイルに ACL を追加する場合は、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、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）とポート プロファイルに付与する名前。
- アクセス リストのパケット フローの方向。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **mac access-list** *name* | 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 | switch(config-mac-acl)# {**permit** \| **deny**} *source destination protocol* | MAC ACL 内にルールを作成します。<br>permit キーワードと deny キーワードには、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 | switch(config-mac-acl)# **statistics per-entry** | （任意）<br>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 | switch(config-mac-acl)# **show mac access-lists** *name* | （任意）<br>確認のためにMAC ACLの設定を表示します。 |
| ステップ 6 | switch(config-mac-acl)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

# 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。

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。

## はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- 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 内で、ルールの追加または削除を実行できます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **mac access-list** *name* | 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 | switch(config-mac-acl)# [*sequence-number*] {**permit** \| **deny**} *source destination protocol* | （任意）<br>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。<br>permit キーワードと deny キーワードには、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 | switch(config-mac-acl)# **no** {*sequence-number* \| {**permit** \| **deny**} *source destination protocol*} | （任意）<br>指定したルールを MAC ACL から削除します。<br>permit キーワードと deny キーワードには、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 | switch(config-mac-acl)# [**no**] **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。<br>**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 | switch(config-mac-acl)# **show mac access-lists** *name* | （任意）<br>確認のために MAC ACL の設定を表示します。 |
| ステップ 7 | switch(config-mac-acl)# **copy running-config startup-config** | 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。 |

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# no 80
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

# MAC ACL の削除

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。

### はじめる前に

この手順を開始する前に、次のことを確認してください。

- EXEC モードで CLI にログインしていること。
- ACL がインターフェイスに適用されているかどうかがわかっていること。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **no mac access-list** *name* | 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 | switch(config)# **show mac access-lists** *name* **summary** | （任意）<br>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 | switch(config)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# no mac access-list acl-mac-01
switch(config)# show mac access-lists acl-mac-01 summary
switch(config)# copy running-config startup-config
```

# 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。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | 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** | switch(config)# **resequence mac access-list** *name starting-sequence-number increment* | 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** | switch(config-mac-acl)# **show mac access-lists** *name* | （任意）<br>確認のために MAC ACL の設定を表示します。 |
| **ステップ 4** | switch(config)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# resequence mac access-list acl-mac-01 100 10
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

# 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。

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。

### はじめる前に

この手順を開始する前に、次のことを確認してください。

- 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。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **interface vethernet** *port* | 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 | switch(config-if)# **mac port access-group** *access-list* [**in** \| **out**] | MAC ACL をインターフェイスに適用します。 |
| ステップ 4 | switch(config-if)# **show running-config aclmgr** | （任意）<br>ACL の設定を表示します。 |
| ステップ 5 | switch(config-if)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# interface vethernet 35
switch(config-if)# mac port access-group acl-01 in
switch(config-if)# show running-config aclmgr
switch(config-if)# copy running-config startup-config
```

# MAC ACL のポート プロファイルへの追加

## はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- このポート プロファイルに追加する MAC ACL が作成され、名前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、その名前がわかっていること。
- 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 フローの方向がわかっていること。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **port-profile** [**type** {**ethernet** \| **vethernet**}] *name* | 指定されたポート 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 | switch(config-port-prof)# **mac port access-group** *name* {**in** \| **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 | switch(config-port-prof)# **show port-profile name** *profile-name* | （任意）<br>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 | switch(config-port-prof)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure termnal
switch(config)# port-profile AccessProf
switch(config-port-prof)# show port-profile name AccessProf
switch(config-port-prof)# copy running-config startup-config
```

# MAC ACL の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

| 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、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。 |
| **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。 |

# 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

## 任意のプロトコル用に MAC ACL を作成する設定例

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 ACL として適用する例を示します。

```
switch(config)# configure terminal
switch(config)# mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# interface vethernet 35
switch(config-if)# mac port access-group acl-mac-01 out
```

## ポート プロファイルに MAC ACL を追加する設定例

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。

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# mac port access-group allaccess4 out
switch(config-port-prof)# 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:
```

# MAC ACL の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

| 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。 |