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。

- MAC ACL の概要, on page 1
- MAC ACL のデフォルト設定, on page 2
- MAC ACL の注意事項と制約事項 （2 ページ）
- MAC ACL の設定 （2 ページ）
- MAC ACL の設定の確認, on page 11
- MAC ACL 統計情報のクリア, on page 12

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。

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 パケット分類は、HSRP、VRRP、OSPF などのレイヤ 3 コントロール プレーン プロトコルでは機能しません。VLAN で MAC パケット分類を有効にすると、これらのプロトコルで基本的な機能が壊れます。

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すが、トラフィックのフィルタリングは行われません。
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。 • インターフェイスで IP ポート ACL を適用することができます。これにより、トラフィックがフィルタリングされます。

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。

***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。
- ハードウェアの制限により、MAC ACL は Cisco Nexus 3500 プラットフォーム スイッチの ARP パケットをフィルタ処理しません。

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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。 **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) 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) switch(config-mac-acl)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 6	(Optional) 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。

Example

次に、MAC ACL を作成する例を示します。

```
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

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config
```

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、**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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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*	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) switch(config-mac-acl)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*	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) switch(config-mac-acl)# **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}	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。

	Command or Action	Purpose
ステップ 5	(Optional) 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。 **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) switch(config-mac-acl)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 7	(Optional) 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。

Example

次に、MAC ACL を変更する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# 80 permit 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

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
        100 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config
```

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	(Optional) switch(config)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 4	(Optional) switch(config)# **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。

Example

次に、MAC ACL のシーケンスを変更する例を示します。

```
switch# configure terminal
switch(config)# resequence mac access-list acl-mac-01 100 15
switch(config)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config)# copy running-config startup-config
```

MAC ACL の削除

MAC ACL をデバイスから削除できます。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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*	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) switch(config)# **show mac access-lists** *name* **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) switch(config)# **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。

Example

次に、MAC ACL を削除する例を示します。

```
switch# configure terminal
switch(config)# show mac access-lists

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-02
        statistics per-entry
        10 permit 00a0.3f00.0000 0000.00dd.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# no mac access-list acl-mac-02
switch(config)# show mac access-lists acl-mac-02 summary
switch(config)# show mac access-lists

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# copy running-config startup-config
```

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 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

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - switch(config)# **interface ethernet** *slot*/*port*
   - switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **mac port access-group** *access-list*
4. (Optional) switch(config-if)# **show running-config aclmgr**
5. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	次のいずれかのコマンドを入力します。 • switch(config)# **interface ethernet** *slot*/*port* • switch(config)# **interface port-channel** *channel-number*	• 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。
ステップ 3	switch(config-if)# **mac port access-group** *access-list*	MAC ACL をインターフェイスに適用します。
ステップ 4	(Optional) switch(config-if)# **show running-config aclmgr**	ACL の設定を表示します。
ステップ 5	(Optional) switch(config-if)# **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。

Example

次の例は、イーサネット インターフェイスに MAC ACL をポート ACL として適用する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:36:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any

...

interface Ethernet1/3
  mac port access-group acl-mac-01

switch(config-if)# copy running-config startup-config
```

次の例は、ポートチャネル インターフェイスに MAC ACL をポート ACL として適用する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:37:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
```

```
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any


...

interface port-channel5
  mac port access-group acl-mac-01

switch(config-if)# copy running-config startup-config
```

MAC パケット分類のイネーブル化または無効化

MAC パケット分類は、VLAN 単位でイネーブルまたはディセーブルにすることができます。

手順の概要

1. **config t**
2. **vlan** *vlan-number*
3. [**no**] **mac packet-classify**
4. **exit**
5. （任意） **show running-config vlan** *vlan-number*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**config t**
	例：
	`switch# config t`
	`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	**vlan** *vlan-number*
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLANインターフェイスを作成します。numberの範囲は 1 ～ 4094 です。

ステップ 3	[**no**] **mac packet-classify**
	例：
	`switch(config-vlan)# mac packet-classify`
	`switch(config-vlan)#`
		vlan 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、vlan の MAC パケット分類がディセーブルになります。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		vlan 構成を終了します。

ステップ 5	（任意） **show running-config vlan** *vlan-number*	実行設定を表示します。

例

次に、VLAN 単位で MAC パケット分類をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan 50
switch(config-vlan)# mac packet-classify
switch(config-vlan)# exit
switch(config)# show running-config vlan 50

!Command: show running-config interface Vlan50
!Time: Wed Aug  6 20:39:03 2014

version 6.0(2)A4(1)

interface Vlan50
  mac packet-classify

switch(config-if)# copy running-config startup-config
```

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。

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** **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。 **Note** **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 統計情報のクリア

clear mac access-list counters コマンドを使用して、MAC ACL 統計情報を消去できます。

コマンド	目的
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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。