CHAPTER 12

VLAN ACL の設定

この章では、VLAN ACL（アクセス 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。

VLAN ACL の概要

VLAN ACL（VACL）は、Media Access Control（MAC; メディア アクセス制御）ACL または IP ACL のアプリケーションの 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトのみを目的としたものです。VACL は方向（入力または出力）では定義されません。

ACL のタイプおよびアプリケーションについての詳細は、「ACL の概要」（p.10-2）を参照してください。

ここでは、次の内容について説明します。

VACL とアクセス マップ

VACL は、アクセス マップを使用して、IP ACL または MAC ACL を処理とリンクします。デバイスは、VACL で許可されているパケットに対し、設定済みの処理を実行します。

VACL と処理

アクセス マップ コンフィギュレーション モードで **action** コマンドを使用し、次のいずれかの処理を指定します。

- Forward — スイッチの通常の動作で決定された宛先にトラフィックを送信します。
- Redirect — 1 つまたは複数の指定インターフェイスにトラフィックをリダイレクトします。
- Drop — トラフィックをドロップします。

処理を指定する際には、次の 2 つのオプションも指定できます。

- Log パケットをログに記録します（「drop」処理を指定した場合にのみ使用可能）。
- Send　キャプチャ機能がイネーブルになっているインターフェイスに許可トラフィックを送信します。

統計情報

VACL の各ルールのグローバル統計が維持されます。1 つの VACL が複数の VLAN に適用される場合、維持されるルール統計は、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計です。

（注）　インターフェイス レベルの VACL 統計はサポートされていません。

設定する VLAN アクセス マップごとに、その VACL の統計情報を維持するかどうかを指定できます。この機能を使用すると、VACL によってフィルタリングされたトラフィックの監視が必要かどうかに応じて、あるいは VLAN アクセスマップの設定のトラブルシューティングが必要かどうかに応じて、VACL 統計をオンまたはオフにできます。

VACL 統計の表示については、「VACL の統計情報の表示とクリア」（p.12-8）を参照してください。

Session Manager のサポート

Session Manager は VACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、設定の実行をコミットする前にその設定に必要とされるリソースが利用可能であるかどうかを確認できます。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。

バーチャライゼーション サポート

Virtual Device Context（VDC; バーチャル デバイス コンテキスト）で使用される VACL には次の事項が適用されます。

- ACL は各 VDC に固有です。ある VDC に作成した ACL を別の VDC に使用することはできません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- デバイスは、ACL やルールを VDC 単位では制限しません。

VACL のライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
NX-OS	VACL にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は、Cisco NX-OS システム イメージにバンドルされており、追加料金なしで利用できます。NX-OS のライセンス スキームに関する詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

VACL の前提条件

VACL の前提条件は次のとおりです。

- VACL を設定するには、VLAN に関する知識が必要です。
- 「ACL の概要」（p.10-2）に記載されている内容を理解している必要があります。

注意事項および制約事項

VACL の設定に関する注意事項と制約事項は次のとおりです。

- ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、設定の実行をコミットする前にその設定に必要とされるリソースが利用可能であるかどうかを確認できます。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。
- ACL に関する詳細は、「ACL の概要」（p.10-2）を参照してください。

VACL の設定

ここでは、次の内容について説明します。

VACL の作成または変更

VACL の作成または変更を行うことができます。VACL の作成には、IP または MAC ACL を一致トラフィックに適用される処理と関連付けるアクセス マップの作成が含まれます。

作業を開始する前に

VACL に使用する IP ACL または MAC ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。IP ACL の設定に関する詳細は、「IP ACL の設定」（p.10-1）を参照してください。MAC ACL の設定に関する詳細は、「MAC ACL の設定」（p.11-1）を参照してください。

手順の概要

1. **config t**
2. **vlan access-map** *map-name*
3. **match** ***ip*** **address** *ip-access-list*

   match mac address *mac-access-list*
4. **action** {***drop*** | ***forward*** | ***redirect***}
5. **[no] statistics**
6. **show running-config aclmgr**
7. **copy running-config startup-config**

詳細な手順

	コマンド	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 access-map` *map-name*
	
	例：
	`switch(config)# vlan access-map acl-mac-map`
	`switch(config-access-map)#`
		指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**match** ***ip*** **address** *ip-access-list* **例：** `switch(config-access-map)# match mac address acl-ip-lab`	マップの IPv4 ACL を指定します。
	match mac address *mac-access-list* **例：** `switch(config-access-map)# match mac address acl-mac-01`	マップの MAC ACL を指定します。
ステップ 4	**action** {***drop*** | ***forward*** | ***redirect***} **例：** `switch(config-access-map)# action forward`	ACL に一致したトラフィックにデバイスが適用する処理を指定します。 **action** コマンドはさまざまなオプションをサポートしています。詳細については、『*Cisco NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics** **例：** `switch(config-access-map)# statistics`	（任意）その VACL 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 VACL のグローバル統計の維持を停止します。
ステップ 6	**show running-config aclmgr** **例：** `switch(config-access-map)# show running-config aclmgr`	（任意）ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** **例：** `switch(config-access-map)# 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。

VACL の削除

VACL を削除できます。これにより、VLAN アクセス マップが削除されます。

作業を開始する前に

その VACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在 適用されている VACL です。VACL を削除しても、その VACL が適用されている VLAN の設定には影響しません。デバイスは削除された VACL を空であるとみなします。

手順の概要

1. **config t**
2. **no vlan access-map** *map-name*
3. **show running-config aclmgr**
4. **copy running-config startup-config**

詳細な手順

	コマンド	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	**no vlan access-map** *map-name* **例：** switch(config)# no vlan access-map acl-mac-map	指定したアクセス マップの VLAN アクセス マップの設定を削除します。
ステップ 3	**show running-config aclmgr** **例：** switch(config)# show running-config aclmgr	（任意）ACL の設定を表示します。
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。

VLAN への VACL の適用

VACL を VLAN に適用できます。

作業を開始する前に

VACL を適用する際には、その VACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。VACL の作成についての詳細は、「VACL の作成または変更」（p.12-5）を参照してください。

VACL の適用を解除する際には、必ず正しい VACL の適用を解除するとともに、その VACL が現在どのように適用されているのかを十分に理解している必要があります。VACL の設定確認についての詳細は、「VACL の設定の確認」（p.12-8）を参照してください。

手順の概要

1. **config t**
2. **[no] vlan filter** *map-name* **vlan-list** *list*
3. **show running-config aclmgr**
4. **copy running-config startup-config**

詳細な手順

	コマンド	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	[**no**] **vlan filter** *map-name* **vlan-list** *list* **例：** switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30 switch(config)#	指定したリストによって、VACL を VLAN に適用します。**no** オプションを使用すると、その VACL の適用が解除されます。
ステップ 3	**show running-config aclmgr** **例：** switch(config)# show running-config aclmgr	（任意）ACL の設定を表示します。
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。

VACL の設定の確認

VACL 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 running-config aclmgr	VACL 関連の設定を含めて、ACL の設定を表示します。
show vlan filter	VLAN に適用される VACL の情報を表示します。
show vlan access-map	VLAN アクセス マップについての情報を表示します。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

VACL の統計情報の表示とクリア

VACL の統計情報の表示またはクリアを行うには、次のいずれかの作業を行います。

コマンド	目的
show vlan access-list	VACL の設定を表示します。VLAN アクセス マップに **statistics** コマンドが含まれている場合は、**show ip 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 vlan access-list counters	すべての VACL または特定の VACL の統計情報をクリアします。

これらのコマンドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

VACL の設定例

次の例では、acl-mac-01 という名前の MAC ACL で許可されたトラフィックを転送する VACL を設定し、その VACL を VLAN 50 ～ 82 に適用します。

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

デフォルト設定

表 12-1 に VACL パラメータのデフォルトの設定値を示します。

表 12-1　VACL パラメータのデフォルト値

パラメータ	デフォルト
VACL	デフォルトでは IP 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.10-6] を参照）。

その他の参考資料

IP 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.12-9）
- 規格（p.12-9）

関連資料

関連事項	タイトル
ACL の概念	ACL の概要（p.10-2）
VACL のコマンド：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 NX-OS Security Command Reference*』

規格

規格	タイトル
この機能のサポート対象の規格には、新規規格も変更された規格もありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—