ハードウェアパケットフィルター

概要・基本設定

ハードウェアパケットフィルターは、ハードウェア（ASIC）レベルで入力パケットをフィルタリング（許可・拒否）する機能です。
ハードウェアパケットフィルターには以下の特長があります。

- ハードウェアで処理するため高速
- 入力ポート単位でフィルタリングが可能

パケットのフィルタリング条件には、以下の各項目を使用できます。フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。クラシファイアの詳細については「クラシファイア」の章をご覧ください。

- Ethernet の送信元・宛先 MAC アドレス、フレームフォーマットとプロトコルタイプ（タグ付き、タグなし）
- 入力 VLAN
- 802.1p プライオリティー値
- IP ヘッダーの TOS 優先度（precedence）または DSCP（DiffServ Code Point）、プロトコル、始点・終点 IP アドレス
- TCP ヘッダーの始点・終点ポート、制御フラグのフィールド値
- UDP ヘッダーの始点・終点ポート

条件に一致したパケットに対しては、以下の処理（アクション）が可能です。

- 許可（permit）
- 破棄（deny）

基本動作

ハードウェアパケットフィルターの基本動作について説明します。

フィルターの構成

ハードウェアパケットフィルターは、複数のエントリーをリストとして保持する「アクセスコントロールリスト（ACL）」から構成されます。エントリーは、クラシファイア（汎用パケットフィルター）とアクション、および適用対象のスイッチポート（入力ポート）で構成されます。
エントリーの構成は、次のとおりです。

ACL	エントリーの ID
DESCRIPTION	エントリーの説明
ACTION	マッチした場合のアクション
CLASSIFIERLIST	エントリーに割り当てるクラシファイアの ID
PORTLIST	エントリーに割り当てるポート

表 1:

ACL の仕様は、次のとおりです。

- 最大エントリー数は 64 個
- 同一ポートに複数のエントリーを割り当てることができる（ただし、同じクラシファイアを含むエントリーを、同一ポートに割り当てることはできない）
- 同一エントリーを複数ポートに割り当てることができる
- 1 ポートに割り当てられるクラシファイアの数は、128 個まで（ポリシーベース QoS とハードウェアパケットフィルター機能合わせて）

フィルター処理の流れ

ハードウェアパケットフィルターでは、パケット受信時に次の処理が行われます。
ACL のモードは以下の 2 つがあり、モードにより処理の流れが異なります。

- レガシーモード（ファームウェアバージョン 2.3.2J 以前より動作するモード）
- エンハンスモード（ファームウェアバージョン 2.3.3J 以降で動作するモード）

デフォルトはレガシーモードです。
レガシーモードを無効にし、エンハンスモードにする場合は、DISABLE ACL LEGACYMODE コマンド（11 ページ）を実行します。

レガシーモード（アクションに許可が指定されているエントリーを優先処理）

レガシーモードでは、パケット受信時に次の処理が行われます。

1. 受信したパケットがエントリーにマッチするかどうか調べます。
2. 許可するエントリーにマッチした場合、そのパケットを出力します。
3. 許可するエントリーにマッチせず、破棄するエントリーにマッチした場合、そのパケットを破棄します。
4. エントリーにマッチしないパケットを出力します。

✎ 設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。

エンハンスモード（エントリー ID 順に処理）

エンハンスモードでは、パケット受信時にエントリー ID 順に処理が行われます。

1. 受信したパケットがエントリーにマッチするかどうか、ACL のエントリー ID の番号順に調べます。
2. 条件にマッチした場合は、残りの条件は調べずに、その条件のアクションをします。
3. エントリーにマッチしないパケットを出力します。

✎ 設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。

✎ レガシーモードですでにハードウェアパケットフィルターを設定している場合に無効にすると、ハードウェアパケットフィルターが正しく動作しないことがあります。PURGE ACL コマンド（13 ページ）で ACL の設定を工場出荷時の状態に戻してから、エンハンスモードの処理フローに適した ACL を設定しなおしてください。

設定手順

ハードウェアパケットフィルターの設定は、次の流れで行います。

1. クラシファイアの作成（CREATE CLASSIFIER コマンド（「クラシファイア」の 7 ページ））
2. ACL のエントリーの作成（CREATE ACL コマンド（9 ページ））

以下、各手順について詳しく解説します。
ここでは例として、ポート 8 に接続されているクライアントから、サーバー 192.168.10.5 宛てのパケットを遮断するよう設定します。

1. クラシファイアを作成します。詳細は「クラシファイア」の章をご覧ください。

   ```
   CREATE CLASSIFIER=1 IPDADDR=192.168.10.5/32 ↵
   ```

2. ACL にエントリーを追加します。エントリーを追加するには、クラシファイア、マッチ時のアクション（許可か破棄）、エントリーを適用する入力ポートの指定が必要です。

   ```
   CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=8 ↵
   ```

基本設定は以上です。

コマンド例

■ 送信元 MAC アドレスが、00-00-f4-33-22-11 のパケットを破棄

```
CREATE CLASSIFIER=1 MACSADDR=00-00-f4-33-22-11 ↵
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=6 ↵
```

■ 192.168.10.100 から 192.168.20.0 / 24 への IP パケットを破棄

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.100/32 IPDADDR=192.168.20.0/24 ↵
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=5 ↵
```

■ 192.168.30.100 への telnet パケットを破棄。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.30.100/32 TCPDPORT=23 ↵
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=4 ↵
```

■ ACL の一覧を表示するには、SHOW ACL コマンド（15 ページ）を使います。

```
SHOW ACL ↵
```

■ クラシファイアの一覧を表示するには、SHOW CLASSIFIER コマンド（「クラシファイア」の 14 ページ）を実行します。CLASSIFIER パラメーターに番号を指定すれば、該当するクラシファイアのみが表示されます。

```
SHOW CLASSIFIER ↵
SHOW CLASSIFIER=1-3 ↵
```

■ ACL からエントリーを削除するには、DESTROY ACL コマンド（10 ページ）を使います。

```
DESTROY ACL=1 ↵
```

✎ ACL からエントリーを削除しても、クラシファイアは削除されません。ACL とクラシファイアの関連付けが削除されるだけです。クラシファイアを削除するには、DESTROY CLASSIFIER コマンド（「クラシファイア」の 10 ページ）を使います。

エンハンスモードで可能になった設定例

■ ポート 1 で受信する通信のうち 192.168.0.0 / 16 宛ての通信のみ許可します。ただし 192.168.1.0 / 24 宛ての通信は破棄します。

1. ACL の動作モードを変更します。

   ```
   DISABLE ACL LEGACYMODE ↵
   ```

2. クラシファイアを作成します。

   ```
   CREATE CLASSIFIER=1 PROTOCOL=ARP ↵
   CREATE CLASSIFIER=2 IPDADDR=192.168.0.0/16 ↵
   CREATE CLASSIFIER=3 IPDADDR=192.168.1.0/24 ↵
   CREATE CLASSIFIER=4 ↵
   ```

3. ARP を許可します。

   ```
   CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=1 ↵
   ```

4. ACL ID の小さいエントリーに、サブネットマスクの長いクラシファイア 2（192.168.1.0 / 24）を登録します。クラシファイア 1（192.168.0.0 / 16）は、クラシファイア 2 の条件も含むため、先に登録しなければなりません。

```
CREATE ACL=2 ACTION=DENY CLASSIFIERLIST=3 PORTLIST=1 ↵
```

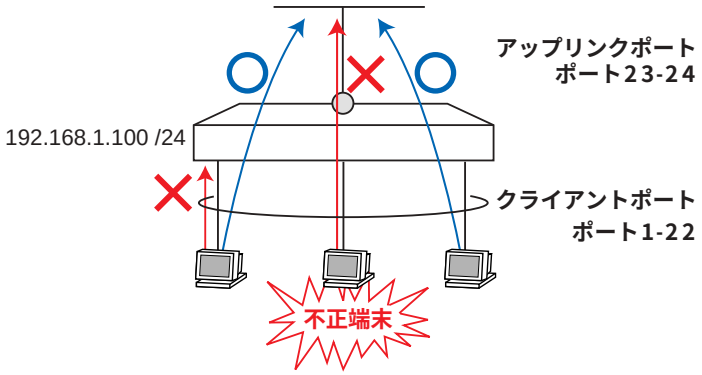
5. クラシファイア 1（192.168.0.0/16）を登録し、クラシファイア 2 の条件を除いてクラシファイア 1 にマッチする通信を許可します。

```
CREATE ACL=3 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=1 ↵
```

6. クラシファイア 1、2 のいずれにもマッチしないすべての通信を拒否するためにクラシファイア 3 を登録します。

```
CREATE ACL=4 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=1 ↵
```

■ マルチプル VLAN 構成でクライアントポートから特定端末（00:01:23:xx:xx:xx）のみ通信を許可します。ただし本製品宛て（192.168.1.100）の通信は破棄します。



1. マルチプル VLAN を設定します。

```
CREATE VLAN=mv VID=2 PORTPROTECTED ↵
ADD VLAN=mv VID=2 UNTAGGEDPORTS=1 GROUP=1 ↵
ADD VLAN=mv VID=2 UNTAGGEDPORTS=2 GROUP=2 ↵
ADD VLAN=mv VID=2 UNTAGGEDPORTS=3 GROUP=3 ↵
```

・
・
・

```
ADD VLAN=mv VID=2 UNTAGGEDPORTS=23-24 GROUP=uplink ↵
```

2. ACL の動作モードを変更します。

```
DISABLE ACL LEGACYMODE ↵
```

3. クラシファイアを作成します。

```
CREATE CLASSIFIER=1 MACSADDR=00:01:23:00:00:00
  MACSMASK=ff:ff:ff:00:00:00 ↵
CREATE CLASSIFIER=2 MACSADDR=00:01:23:00:00:00
  MACSMASK=ff:ff:ff:00:00:00 IPDADDR=192.168.1.100 ↵
CREATE CLASSIFIER=3 ↵
```

4. ACL ID の小さいエントリーに、条件の多いクラシファイア 2（特定端末＋本製品宛て）を登録します。クラシファイア 1（特定端末）は、クラシファイア 2 の条件の一部と重なるため、先に登録しなければなりません。

   ```
   CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=2 PORTLIST=1-22 ↵
   ```

5. クラシファイア 1（特定端末）を登録し、クラシファイア 2 の条件を除いてクラシファイア 1 にマッチする通信を許可します。

   ```
   CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=1-22 ↵
   ```

6. クラシファイア 1、2 のいずれにもマッチしないすべての通信を拒否するためにクラシファイア 3 を登録します。

   ```
   CREATE ACL=3 ACTION=DENY CLASSIFIERLIST=3 PORTLIST=1-22 ↵
   ```

注意事項

ここでは、設定時に注意が必要なハードウェアパケットフィルターの仕様について解説します。

本体宛てのパケット

スイッチ本体（CPU）宛てのパケットに対し、ハードウェアパケットフィルター機能は動作します。

IGMP Snooping 機能との併用

ハードウェアパケットフィルターで、IPPROTOCOL に IGMP を指定したクラシファイアを使用した場合は、IGMP Snooping 機能は有効にできません。

コマンドリファレンス編

機能別コマンド索引

一般コマンド

CREATE ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

```
CREATE ACL=0..255 [DESCRIPTION=string] [ACTION={DENY |PERMIT}]
   [CLASSIFIERLIST={rule-list|NONE}] [PORTLIST={port-list|ALL|NONE}]
```

string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

ACL にエントリーを追加する。
パケットをフィルタリングするためのパラメーター（MAC アドレス、IP アドレスなど）は、汎用のパケットフィルターであるクラシファイア（CREATE CLASSIFIER コマンドで作成）で定義する。本コマンドでは、クラシファイア番号とマッチ時のアクションを一組のエントリーとして ACL に追加する。

パラメーター

ACL　作成するエントリーの ID。
DESCRIPTION　作成するエントリーの説明。
ACTION　パケットがクラシファイアに一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。デフォルトは DENY。
CLASSIFIERLIST　ACL に対応付けるクラシファイアの ID を指定する。デフォルトは NONE。
PORTLIST　ACL を割り当てるポートを指定する。デフォルトは NONE。

例

■ACL にエントリーを追加する。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=8
```

関連コマンド

DESTROY ACL（10 ページ）
SHOW ACL（15 ページ）

DESTROY ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

DESTROY ACL=*0..255*

解説

ACL のエントリーを削除する。

パラメーター

ACL　削除するエントリーの ID。

例

■ACL のエントリーを削除する。

```
DESTROY ACL=1
```

関連コマンド

CREATE ACL（9 ページ）
SHOW ACL（15 ページ）

DISABLE ACL LEGACYMODE

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

DISABLE ACL LEGACYMODE

解説

ACL をエンハンスモード（ファームウェアバージョン 2.3.3J 以降で動作するモード）にする。デフォルトは ENABLE（レガシーモード）

例

■ACL をエンハンスモードにする。

```
DISABLE ACL LEGACYMODE
```

関連コマンド

ENABLE ACL LEGACYMODE（12 ページ）

ENABLE ACL LEGACYMODE

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

ENABLE ACL LEGACYMODE

解説

ACL をレガシーモード（ファームウェアバージョン 2.3.2J 以前より動作するモード）にする。デフォルトは ENABLE（レガシーモード）

例

■ACL をレガシーモードにする。

```
ENABLE ACL LEGACYMODE
```

関連コマンド

DISABLE ACL LEGACYMODE（11 ページ）

PURGE ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

PURGE ACL

解説

ACL の設定を工場出荷時の状態に戻す。

例

■ACL の設定を工場出荷時の状態に戻す。

```
PURGE ACL
```

関連コマンド

SHOW ACL（15 ページ）

SET ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

SET ACL=*0..255* [DESCRIPTION=*string*] [ACTION={DENY |PERMIT}]
[CLASSIFIERLIST={*rule-list*|NONE}] [PORTLIST={*port-list*|ALL|NONE}]

string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

ACL エントリーの設定を変更する。

パラメーター

ACL　変更するエントリーの ID。
DESCRIPTION　作成するエントリーの説明。
ACTION　パケットがクラシファイアに一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。デフォルトは DENY。
CLASSIFIERLIST　ACL に対応付けるクラシファイアの ID を指定する。デフォルトは NONE。
PORTLIST　ACL を割り当てるポートを指定する。デフォルトは NONE。

例

■ACL エントリーの設定を変更する。

```
SET ACL=1 CLASSIFIERLIST=2-5
```

関連コマンド

SHOW ACL（15 ページ）

SHOW ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

SHOW ACL[={*id-list*|All}]

id-list: ACL の ID（0〜255。ハイフン、カンマを使った複数指定も可能）

解説

ACL のエントリーを表示する。

パラメーター

ACL　表示するエントリーの ID。省略時および ALL を指定した場合は、すべてのフローグループ情報が表示される。

入力・出力・画面例

```
# show acl
ACL Legacy mode ............................... Enable

-----------------------------------------------
ACL ID ............... 1
Description .........
Action ............... Deny
Classifier List ..... 1
Port List ............ 6
Is Active ............ Yes
```

ACL Legacy mode	ACL の動作モード。Enable（レガシーモード）または Disable（エンハンスモード）
ACL ID	エントリーの ID
Description	エントリーの説明
Action	パケットがクラシファイアに一致したときのアクション。Permit または Deny
Classifier List	クラシファイアの ID
Port List	エントリーを割り当てるポート
Is Active	エントリーがポートに割り当てられている（Yes）、またはいない（No）

表 2:

関連コマンド

CREATE ACL（9 ページ）
DESTROY ACL（10 ページ）