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 IP トラフィックのフィルタリングを行う機能です。
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
- ポート単位での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。

- Ethernet ヘッダーの送信元、宛先 MAC アドレスとプロトコルタイプ（タグ付き、タグなし）
- 入出力スイッチポート
- IP ヘッダーの TOS 優先度（precedence）または DSCP（DiffServ Code Point）、TTL、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（Syn、Ack、Fin）
- 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）を適用できます（複数の処理を適用することも可能）。一致しなかったパケットは通常通り処理されます。

- 破棄・許可
- 出力スイッチポートの変更
- 出力キューレベルの変更
- VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを書き換え
- IP パケットの TOS 優先度フィールド、または、DSCP フィールドを書き換え
- ミラーポートにパケットをコピー

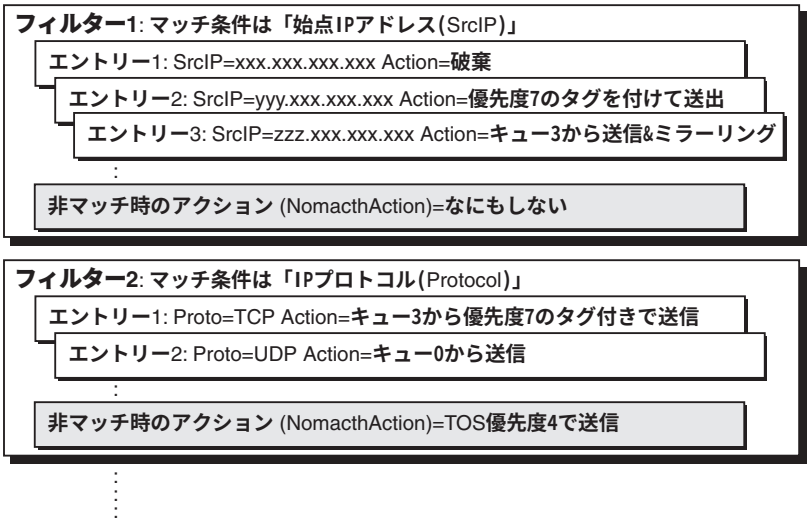
基本動作

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、マッチ条件（フィルター）とフィルターエントリーで構成されます。

- マッチ条件（フィルター）は、パケットヘッダーのどのフィールドを使ってパケットをふるいわけるかを指定するもので、ADD SWITCH L3FILTER MATCH コマンド（27 ページ）で作成します。オプションで、どのエントリーにもマッチしなかった場合の処理も指定できます（NOMATCHACTION）。
- フィルターエントリーは、マッチ条件に対して具体的な値を指定し、マッチしたパケットに対して行う処理（アクション）を指定するもので、ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）で追加します。



作成可能なフィルター数は次のとおりです。

- マッチ条件（フィルター）はシステム全体で 14 個まで（IGMP Snooping および MLD Snooping 無効時は 16 個）
- フィルターエントリーは、10/100M ポートで最大 252 個まで（IGMP Snooping および MLD Snooping 無効時は 254 個）、1000M ポートで最大 124 個まで（IGMP Snooping および MLD Snooping 無効時は 126 個）

■ IPORT オプションを指定した場合のエントリー数のイメージは、次のとおりです。

各ブロックのエントリー数	1〜8ポート	9〜16ポート	17〜24ポート	25ポート	26ポート
8316XL	254	254	126	-	-
8324XL	254	254	254	126	126

- IPORT オプションを指定した場合は、10/100M ポートの 1 ブロックあたり 254 エントリーまで、1000M ポートの 1 ブロックあたり 126 エントリーまで作成できる
- IPORT オプションを指定した場合は、該当ブロックから 1 エントリー消費される（該当ブロックがフルエントリーの場合は追加できない）
- IPORT オプションを指定しない場合は、各ブロックから 1 エントリーずつ消費される（いずれかのブロックがフルエントリーの場合は追加できない）

また、DHCP Snooping 機能を使用する場合、ハードウェアパケットフィルターのエントリーを消費します。

- DHCP Snooping 機能を有効にすると、10/100M ポートのブロックでは 10 エントリー、1000M ポートのブロックでは 3 エントリー消費される
- DHCP クライアントを 1 クライアント登録するごとに、該当ブロックから 1 エントリー消費される

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の処理は、おおむね次の手順にしたがって行われます。

✎ 以下の説明は、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。あらかじめご了承ください。

1. パケットを受信すると、FDB を参照して出力先（出力ポート）を決定します。
2. すべてのフィルター（マッチ条件）、すべてのフィルターエントリーをチェックし、受信パケットの入出力スイッチポート、IP、TCP、UDP ヘッダーフィールドと一致するものがあるかどうかを調べていきます。一致するエントリーが 1 つ以上あった場合は、一致したエントリーのアクションをすべて「アクションリスト」にリストアップしておきます。

   ✎ NOMATCHACTION が指定されているフィルターの場合、該当フィルターのどのエントリーにもマッチしなかったパケットには、NOMATCHACTION パラメーターで指定されたアクションが適用されます。NOMATCHACTION パラメーターが指定されていない場合は、アクションなしとなります。

3. この時点で「アクションリスト」が空の場合は、フィルター処理を完了し、通常どおりパケットを処理します（パケットを出力）。
4. アクションリストが完成したら、以下の順序でパケットを処理します。フィルター番号順に処理されるのではない点に注意してください。また、以下の各手順では「フィルター処理を終了」と明記していない限り、自動的に次の手順に進みます（パケットに対し、複数のアクションが適用される場合があります）。

   （a） アクションリスト内に「TOS 書き換え系のアクション」（SETTOS、SETIPDSCP、MOVEPRIOTOTOS）があるか調べます。同系のアクションが複数あるときは、フィルター番号の最も大きなアクションだけを選択して実行します。したがって、以下の 3 つのうち、どれか 1 つだけが実行されることになります。

   - SETTOS アクションの場合は、IP ヘッダーの TOS 優先度（precedence）フィールドに NEWTOS パラメーターで指定された値を書き込みます。
   - SETIPDSCP アクションの場合は、IP ヘッダーの DSCP フィールドに NEWIPDSCP パラメーターで指定された値を書き込みます。
   - MOVEPRIOTOTOS アクションの場合は、受信時の 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度（precedence）フィールドにコピーします。

     ✎ ここで書き込んだ TOS 優先度値、DSCP 値が、フィルターエントリーの検索に影響することはありません（アクションリストの検証に入った時点で、すでにエントリーの検索が完了しているため）。フィルターエントリー検索時には、パケット受信時の TOS 優先度値、DSCP 値が使われます。

     ✎ MOVEPRIOTOTOS アクションで使われる 802.1p フィールド値は、パケット受信時の値です。802.1p フィールドを書き換えるアクション（SETPRIORITY、MOVETOSTOPRIO）によって書き換えられた値ではありません。

   （b） アクションリスト内に「802.1p 書き換え系のアクション」（SETPRIORITY、MOVETOSTOPRIO）があるか調べます。同系のアクションが複数あるときは、フィルター番号の最も大きなアクションだけを選択して実行します。したがって、以下の 2 つのうち、どれか 1 つだけが実行されることになります。

   - SETPRIORITY アクションの場合は、VLAN タグフレームの 802.1p ユーザープライオリ

ティーフィールドに PRIORITY パラメーターで指定された値を書き込みます。

- MOVETOSTOPRIO アクションの場合は、受信時の IP TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーします。

✎ 実際にプライオリティー値がセットされた状態でパケットが出力されるには、出力ポートがタグ付き（TAGGED）に設定されている必要があります。出力ポートがタグなし（UNTAGGED）の場合は、VLAN タグがない状態でパケットが出力されるため、本アクションは実質的な意味を持ちません。

（c） アクションリスト内に「SENDMIRROR アクション」があるか調べます。SENDMIRROR アクションがある場合は、ミラーポートとして設定されているポートからパケットのコピーを出力します。仕様により、すべてのパケットが VLAN タグ付きでミラーポートから出力されます。

✎ SENDMIRROR アクションによってミラーされたパケットには、SETTOS、SETIPDSCP、MOVEPRIOTOTOS、SETPRIORITY、MOVETOSTOPRIO アクションによるフィールド書き換えが反映されています。

（d） アクションリスト内に「破棄・通過系のアクション」（DENY、NODROP）があるか調べます。同系のアクションが複数あるときは、フィルター番号の最も大きなアクションだけを選択して実行します。したがって、以下の 2 つのうち、どれか 1 つだけが実行されることになります。

- DENY アクションの場合は、パケットを破棄してフィルター処理を終了します。この場合、通常のポートからパケットが出力されることはありません（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されません）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力されます（SENDMIRROR アクションも有効です）。
- NODROP アクションの場合は次のステップに進みます。

（e） アクションリスト内に「出力ポート変更系のアクション」（SENDEPORT、SENDNONUNICASTTOPORT）があるか調べます。

- パケットがユニキャスト（ブロードキャスト、マルチキャスト、未学習のユニキャスト以外）で、アクションが SENDEPORT の場合は、パケットの出力先を、FDB を参照して決定された出力ポートではなく、PORT パラメーターで指定されたポートに変更します。
- パケットが非ユニキャスト（ブロードキャスト、マルチキャスト、未学習のユニキャスト）で、アクションが SENDNONUNICASTTOPORT の場合は、パケットの出力先を、同一 VLAN 内の全ポートではなく、PORT パラメーターで指定されたポートだけに変更します。

✎ SENDEPORT、SENDNONUNICASTTOPORT アクションを使う場合は、入力ポートと出力ポートが同じ VLAN になるよう設定に注意してください。

（f） アクションリスト内に「出力キューレベル変更系のアクション」（SENDCOS、MOVETOSTOPRIO）があるか調べます。同系のアクションが複数あるときは、フィルター番号の最も大きなアクションだけを選択して実行します。したがって、以下の 2 つのうち、どれか 1 つだけが実行されることになります。

- SENDCOS アクションの場合は、ここまでの手順で確定した出力先ポートの送信キューにパケットを格納し（出力し）、フィルター処理を完了します。このとき、PRIORITY パラメーターで指定されたユーザープライオリティー値に対応するレベルの送信キューを使います。
- MOVETOSTOPRIO アクションの場合は、ここまでの手順で確定した出力先ポートの送信

キューにパケットを格納し（出力し）、フィルター処理を完了します。このとき、受信時のIP TOS 優先度（precedence）フィールドの値に対応するレベルの送信キューを使います。

✎ SENDCOS アクションでは、PRIORITY パラメーターを送信キュー選択のためだけに使います。出力するパケットにプライオリティー値をセットするわけではありません（セットするにはSETPRIORITY か MOVETOSTOPRIO アクションを使います）。

（g） アクションリスト内に「出力キューレベル変更系のアクション」（SENDCOS、MOVETOSTOPRIO）がない場合は、ここまでの手順で確定した出力先ポートの送信キューにパケットを格納します。このとき、パケット受信時の 802.1p ユーザープライオリティー値をもとに、どのレベルのキューに入れるかを決定します。

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. フィルター（マッチ条件）の作成（ADD SWITCH L3FILTER MATCH コマンド（27 ページ））
2. フィルター番号の確認（SHOW SWITCH L3FILTER コマンド（44 ページ））
3. フィルターエントリーの追加（ADD SWITCH L3FILTER ENTRY コマンド（22 ページ））

以下、各手順について詳しく解説します。

フィルター（マッチ条件）の作成

最初に、ADD SWITCH L3FILTER MATCH コマンド（27 ページ）でフィルター（マッチ条件）を作成し、IP/TCP/UDP ヘッダーのどのフィールドを比較条件として使用するかを指定します。

■ MATCH パラメーターには、フィルタリング条件として使用するヘッダーフィールドを以下から指定します。複数指定する場合はカンマで区切って指定してください。TCPxxx、UDPxxx を指定する場合は、PROTOCOL も条件として指定し、さらに ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）（後述）でそれぞれ「PROTOCOL=TCP」、「PROTOCOL=UDP」を指定する必要があります。

Ethernet ヘッダー	
MACDADDR	宛先 MAC アドレスフィールド
MACSADDR	送信元 MAC アドレスフィールド
TYPE	プロトコルタイプフィールド。他のヘッダー項目との併用は不可
IP ヘッダー	
TOS	TOS オクテットの優先度値（precedence）フィールド
IPDSCP	TOS オクテットの DSCP（DiffServ Code Point）フィールド
TTL	生存時間（TTL）フィールド
PROTOCOL	プロトコルフィールド
SIPADDR	始点 IP アドレス（SCLASS も指定すること）
DIPADDR	終点 IP アドレス（DCLASS も指定すること）
TCP ヘッダー	

TCPSPORT	始点ポート（PROTOCOL も指定すること）
TCPDPORT	終点ポート（PROTOCOL も指定すること）
TCPSYN	Syn フラグ（PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと）
TCPACK	Ack フラグ（PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと）
TCPFIN	Fin フラグ（PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと）
	UDP ヘッダー
UDPSPORT	始点ポート（PROTOCOL も指定すること）
UDPDPORT	終点ポート（PROTOCOL も指定すること）

表 1: MATCH パラメーターに指定できる項目

■ MATCH パラメーターに SIPADDR か DIPADDR を指定した場合は、SCLASS、DCLASS パラメーターでそれぞれアドレスマスクも指定します。マスク値は、クラス A、B、C の標準マスク（8, 16, 24 ビット長）か単一ホストを対象とする HOST、あるいは、任意のマスク長（1〜32 ビット）で指定します。ここで指定したマスクは、IP アドレスを実際に指定する際、指定した IP アドレスに対して適用されます。

■ 特定のポートでのみフィルタリングを行うには、IMPORT（入力ポート）、EMPORT（出力ポート）パラメーターに TRUE を指定します。IMPORT、EMPORT パラメーターに TRUE を指定すると、特定のスイッチポートで送受信されるパケットだけがフィルタリングの対象になります。デフォルト（FALSE）では、すべてのポートがフィルタリングの対象になります。なお、具体的なポート番号は、後述する ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）の IPORT、EPORT パラメーターで指定します。

✎ EMPORT パラメーターに TRUE を指定した場合は、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットがフィルタリング対象にならないという制限があります。TCP 制御フラグによるフィルタリングを行う場合（マッチ条件に TCPSYN、TCPACK、TCPFIN を指定する場合）、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EMPORT に TRUE を指定しないでください。

■ NOMATCHACTION パラメーターには、オプションとして、どのエントリーともマッチしなかったパケットに適用するアクションを指定できます。指定できるアクションは ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）の ACTION パラメーターと同じです（ただし、NODROP は除く）。また、アクションパラメーターは NOMATCHDSCP、NOMATCHPORT、NOMATCHPRIORITY、NOMATCHTOS で指定します（それぞれ、ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）の NEWIPDSCP、PORT、PRIORITY、NEWTOS に相当）。

✎ 複数のマッチ条件を指定したとき、マッチ条件の型が一致するような場合には、本製品のソフトウェアでマッチ条件が一つにまとめられる場合があります。同じパケットに対する処理でも、複数のマッチ条件がまとめられた場合と、一つ一つ実行された場合で、結果が異なることがあります。

フィルター番号の確認

次に、SHOW SWITCH L3FILTER コマンド（44 ページ）を実行し、手順 1 で作成したフィルター（マッチ

条件）の番号を確認します。

✎ フィルター番号は、ADD SWITCH L3FILTER MATCH コマンド（27 ページ）実行時にシステムが自動で割り当てます。この番号は可変なので、他のフィルターの削除によって変更される可能性があります。フィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（44 ページ）で確認してから指定してください。

フィルターエントリーの追加

次に、ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）を使って、フィルター（マッチ条件）にエントリーを追加します。
フィルターエントリーを追加するには、次の 3 つの情報を入力する必要があります。以下、それぞれについて詳しく解説します。

- フィルター番号
- フィルタリング条件
- マッチ時のアクション

フィルター番号の指定

ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）の L3FILTER パラメーターには、SHOW SWITCH L3FILTER コマンド（44 ページ）で確認したフィルター番号を指定します。

✎ エントリー番号は、ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）実行時にシステムが自動で割り当てます。この番号は可変なので、他のエントリーの追加・削除によって変更される可能性があります。エントリー番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（44 ページ）に ENTRY パラメーターを付けて実行し、希望するエントリーの番号を確認してから指定してください。

フィルタリング条件の指定

フィルタリング条件は、以下の各パラメーターで指定します。マッチ条件作成時に MATCH パラメーターで指定したすべてのフィールドに対して具体的な値を指定してください。

入出力スイッチポート	
IPORT	入力スイッチポート。指定ポートから入力されたパケットだけがマッチする
EPORT	出力スイッチポート。指定ポートから出力されるパケットだけがマッチする（ただし、若干の制限あり。詳細は後述）
Ethernet ヘッダー	
MACDADDR	宛先 MAC アドレス。ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの MACDADDR パラメーターで指定したマスクが適用される
MACSADDR	送信元 MAC アドレスフィールド。ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの MACSADDR パラメーターで指定したマスクが適用される

TYPE	Ethernet フレームのレイヤー 3 プロトコルタイプフィールド値（16 進数）。ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームフォーマットにおける値を指定する。Ethernet Version 2 と 802.2 LLC（DSAP、SSAP）におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長
	IP ヘッダー
TOS	TOS 優先度値（TOS オクテットの precedence フィールド）。有効範囲は 0〜7
IPDSCP	DSCP（DiffServ Code Point）フィールド値。有効範囲は 0〜63
TTL	生存時間（TTL）フィールドの値。有効範囲は 0〜255
PROTOCOL	IP の上位プロトコル。TCP、UDP などのプロトコル名、または、IP プロトコル番号で指定する
SIPADDR	始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される
DIPADDR	終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される
	TCP ヘッダー
TCPSPORT	始点ポート番号またはサービス名
TCPDPORT	終点ポート番号またはサービス名
TCPSYN	Syn フラグのオン（TRUE）、オフ（FALSE）。EPORT パラメーターと併用しないこと
TCPACK	Ack フラグのオン（TRUE）、オフ（FALSE）。EPORT パラメーターと併用しないこと
TCPFIN	Fin フラグのオン（TRUE）、オフ（FALSE）。EPORT パラメーターと併用しないこと
	UDP ヘッダー
UDPSPORT	始点ポート番号またはサービス名
UDPDPORT	終点ポート番号またはサービス名

表 2: 条件パラメーター（受信パケットのヘッダーその他とつきあわせるパラメーター）

■ 特定のポートでのみフィルタリングを行いたい場合（ADD SWITCH L3FILTER MATCH コマンド（27 ページ）で IMPORT=TRUE または EMPORT=TRUE を指定した場合）は、IPORT（入力ポート）、EPORT（出力ポート）パラメーターでフィルタリングを行うポートの番号を指定してください。IPORT で指定したポートから入力されたパケット、EPORT で指定したポートから出力されるパケットだけが、フィルタリングの対象となります。

✎ ADD SWITCH L3FILTER MATCH コマンド（27 ページ）で IMPORT=TRUE か EMPORT=TRUE を指定していながら、IPORT、EPORT パラメーターでポートの番号を指定していないと、フィルタリングが行われません。なお、ポートは一度に 1 つしか指定できないので、複数のポートでフィルタリングを有効にしたい場合は、ポートの数だけエントリーを作成してください。

✎ フィルタリング条件として EPORT（出力スイッチポート）を指定した場合、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットにはフィルターが適用されなくなります。したがって、TCP 制御フラグによるフィルタリング（TCPSYN、TCPACK、TCPFIN パラメーター）を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないでください。

■ TCP の制御フラグはコネクション方向の判別に使用できますが、前述の制限があるため、EPORT パラメーターとは併用しないでください。

アクションの指定

パケットが条件に一致したときのアクションは、ACTION パラメーターで指定します。ACTION はカンマ区切りで複数指定が可能です。

	パケットの破棄・通過を制御するアクション（相互排他）
DENY	パケットを破棄する。マッチしたエントリーの中に DENY アクションが含まれている場合は、NODROP によって打ち消されない限り、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う
	出力ポートを変更するアクション
SENDEPORT	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストを除くパケットのこと）の出力先を PORT パラメーターで指定されたポートに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること
SENDNONUNICASTTOPORT	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストのこと）の出力先を PORT パラメーターで指定されたポートだけに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること
	出力キューを変更するアクション（相互排他）
SENDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる
MOVETOSTOPRIO	（受信時の）IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
	802.1p プライオリティーを書き換えるアクション（相互排他）
MOVETOSTOPRIO	（受信時の）IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない
	IP TOS/DSCP フィールドを書き換えるアクション（相互排他）
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
MOVEPRIOTOTOS	（受信時の）VLAN タグフレームの 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度（precedence）フィールドにコピーする

SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールドに、NEWIPDSCP パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
	その他のアクション
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。パケットが複数のエントリーにマッチした場合、DENY、NODROP、SEND〜を除く他のアクションがすべて適用された状態でパケットがミラーされる。また、DENY 対象のパケットであってもミラーされる

表 3: ACTION パラメーターに指定できるオプション

コマンド例

次に具体的なコマンド例を示します。
なお以下の例では、いずれの例でも、フィルターは 1 つしか作成していないものと仮定しています。複数のフィルターを作成する場合は、ADD SWITCH L3FILTER ENTRY コマンド（22 ページ）の L3FILTER パラメーターで適切なフィルター番号を指定してください。フィルター番号は SHOW SWITCH L3FILTER コマンド（44 ページ）で確認できます。

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

```
ADD SWITCH L3FILTER MATCH=MACSADDR ↵
ADD SWITCH L3FILTER=1 ENTRY MACSADDR=00-00-f4-33-22-11 ACTION=DENY ↵
```

■ 送信元 MAC アドレスが、00-00-f4-33-22-00〜00-00-f4-33-22-ff の IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=MACSADDR MACSADDR=ff-ff-ff-ff-ff-00 ↵
ADD SWITCH L3FILTER=1 ENTRY MACSADDR=00-00-f4-33-22-00 ACTION=DENY ↵
```

■ ポート 1〜3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY ↵
```

■ 192.168.10.100（単一ホスト）からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 ACTION=DENY ↵
```

■ ポート 2 から送信される ICMP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=PROTOCOL EMPORT=TRUE ↵
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=ICMP EPORT=2 ACTION=DENY ↵
```

■ 192.168.10.0/24 からのパケットは原則拒否だが、192.168.10.103 からのパケットだけは許可。NODROP アクションの使用例です。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 ACTION=DENY ↵
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=2 ENTRY SIPADDR=192.168.10.103 ACTION=NODROP ↵
```

■ telnet パケットをユーザープライオリティー 7 に対応した送信キューに入れる

```
ADD SWITCH L3FILTER MATCH=PROTOCOL,TCPDPORT ↵
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=TCP TCPDPORT=TELNET PRIORITY=7
  ACTION=SENDCOS ↵
```

■ 192.168.30.100 への telnet パケットを破棄

```
ADD SWITCH L3FILTER MATCH=DIPADDR,PROTOCOL,TCPDPORT DCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY DIPADDR=192.168.30.100 PROTOCOL=TCP
  TCPDPORT=TELNET ACTION=DENY ↵
```

■ 192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4
  ACTION=SETPRIORITY ↵
```

■ 受信パケットの IP TOS 優先度が 1 の場合、ユーザープライオリティーを 4 にして送信

```
ADD SWITCH L3FILTER MATCH=TOS ↵
ADD SWITCH L3FILTER=1 ENTRY TOS=1 PRIORITY=4 ACTION=SETPRIORITY ↵
```

■ 192.168.10.100 宛てのパケットをミラーポート 1 から出力。ミラーリングされたパケットには VLAN タグが付いています。

```
SET SWITCH MIRROR=1 ↵
ENABLE SWITCH MIRROR ↵
ADD SWITCH L3FILTER MATCH=DIPADDR DCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY DIPADDR=192.168.10.100 ACTION=SENDMIRROR ↵
```

■ 192.168.10.100 からの TCP コネクション確立要求を拒否（片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる）

```
ADD SWITCH L3FILTER MATCH=SIPADDR,PROTOCOL,TCPSYN,TCPACK SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
  TCPSYN=TRUE TCPACK=FALSE ACTION=DENY ↵
```

■ 192.168.10.0/24 から 192.168.20.0/24 への TCP コネクション確立要求を拒否（片方向のみ拒否。192.168.20.0/24 から 192.168.10.0/24 へはコネクションを張れる）

```
ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR,PROTOCOL,TCPSYN,TCPACK SCLASS=C
  DCLASS=C ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 DIPADDR=192.168.20.0
  PROTOCOL=TCP TCPSYN=TRUE TCPACK=FALSE ACTION=DENY ↵
```

通常、ネットワーククラス単位でフィルターを設定するとき（SCLASS、DCLASS に A, B, C または 1〜32 のマスク長を指定したとき）は、前の例のように送信元（SIPADDR）と宛先（DIPADDR）の両方を指定してください。

■ ある条件を満たしたパケットに対して複数の処理を行いたい場合は、1 つのエントリーで複数のアクションを指定してください。同一フィルター（マッチ条件）内で、同じフィルタリング条件を持つエントリーを複数作ることはできません。
たとえば、192.168.1.1 からのパケットに対して、TOS precedence の書き換えと送信キューの指定を行いたい場合、次のように設定することはできません。2 行目と 3 行目のエントリーのフィルタリング条件が同じため、3 行目を入力するときにエラーになります。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SETTOS NEWTOS=1 ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SENDCOS
  PRIORITY=7 ↵
```

このような場合は、次のようにしてください。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SETTOS,SENDCOS
  NEWTOS=1 PRIORITY=7 ↵
```

■ ハードウェアパケットフィルターを使用するために、必ずしも IP モジュールを有効にする必要はありません。純粋なレイヤー 2 スイッチとして本製品を使用する場合であっても、ハードウェアパケットフィルターを使えば、IP アドレスやプロトコルに応じたフィルタリングが可能です。

■ どのようなハードウェアパケットフィルター（マッチ条件）が作成されているかを確認するには、SHOW SWITCH L3FILTER コマンド（44 ページ）を使います。

```
Manager > show switch l3filter

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Match Entry ................ 3 / 16
Entry Block 0 (Port1-8) .... 3 / 254
Entry Block 1 (Port9-16) ... 2 / 254
Entry Block 2 (Port17-24) .. 2 / 254

Filter ................. 1
Matched fields ......... sip
Type ................... ETHII
Source MAC addr. mask .. ff-ff-ff-ff-ff-ff
Dest. MAC addr. mask ... ff-ff-ff-ff-ff-ff
Source IP addr. mask ... 255.255.255.0
Dest. IP addr. mask .... 0.0.0.0
Ingress port mask ...... true
Egress port mask ....... false

Manager > show switch l3filter=1 entry

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Match Entry ................ 3 / 16
Entry Block 0 (Port1-8) .... 3 / 254
Entry Block 1 (Port9-16) ... 2 / 254
Entry Block 2 (Port17-24) .. 2 / 254

Filter ................. 1
Matched fields ......... sip
Type ................... ETHII
Source MAC addr. mask .. ff-ff-ff-ff-ff-ff
Dest. MAC addr. mask ... ff-ff-ff-ff-ff-ff
Source IP addr. mask ... 255.255.255.0
Dest. IP addr. mask .... 0.0.0.0
```

```
Ingress port mask ...... true
Egress port mask ....... false
Filter Entries:
--------------------------------------------------------------------------------
  Entry ................ 1
  Ingress Port ......... 1
  Egress Port .......... None
  Source MAC Address ... 00-00-00-00-00-00
  Source MAC Mask ...... ff-ff-ff-ff-ff-ff
  Dest MAC Address ..... 00-00-00-00-00-00
  Dest MAC Mask ........ ff-ff-ff-ff-ff-ff
  Source Address ....... 192.168.10.0
  Source Mask .......... 255.255.255.0
  Dest Address ......... 0.0.0.0
  Dest Mask ............ 0.0.0.0
  Protocol ............. 0
  TTL .................. 0
  TOS .................. 0
  IPDSCP ............... 0
  Type ................. 0800(ETHII)
  Action ............... DENY
--------------------------------------------------------------------------------
```

■ ハードウェアパケットフィルターのフィルターエントリーを確認するには、SHOW SWITCH L3FILTER コマンド（44 ページ）に ENTRY オプションを付けます。このときは、フィルター番号を必ず指定しなくてはなりません。

```
Manager > show switch l3filter=1 entry

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Filter ................ 1
Matched fields ......... type
Type ................... ETHII
Source MAC addr. mask .. ff-ff-ff-ff-ff-ff
Dest. MAC addr. mask ... ff-ff-ff-ff-ff-ff
Source IP addr. mask ... 0.0.0.0
Dest. IP addr. mask .... 0.0.0.0
Ingress port mask ...... false
Egress port mask ....... false
Filter Entries:
--------------------------------------------------------------------------------
  Entry ................ 1
  Ingress Port ......... None
  Egress Port .......... None
  Source MAC Address ... 00-00-00-00-00-00
  Source MAC Mask ...... ff-ff-ff-ff-ff-ff
  Dest MAC Address ..... 00-00-00-00-00-00
  Dest MAC Mask ........ ff-ff-ff-ff-ff-ff
```

```
  Source Address ....... 0.0.0.0
  Source Mask .......... 0.0.0.0
  Dest Address ......... 0.0.0.0
  Dest Mask ............ 0.0.0.0
  Protocol ............. 0
  TTL .................. 0
  TOS .................. 0
  IPDSCP ............... 0
  Type ................. 0017(ETHII)
  Action ............... DENY
------------------------------------------------------------------------------
```

■ ハードウェアパケットフィルターからエントリーを削除するには、DELETE SWITCH L3FILTER コマンド（32 ページ）の ENTRY パラメーターでエントリー番号を指定します。

```
DELETE SWITCH L3FILTER=1 ENTRY=1 ↵
```

✎ エントリー番号は可変です。エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれるので注意してください。コマンド中でエントリー番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（44 ページ）に ENTRY パラメーターを付けて実行し、希望のエントリーの番号を確認してから指定してください。

■ フィルター（マッチ条件）を削除するには、エントリーをすべて削除したあとで次のように実行します。

```
DELETE SWITCH L3FILTER=1 ↵
```

✎ フィルター番号は可変です。フィルター（マッチ条件）を削除すると、後続のフィルター番号が 1 つずつ前にずれるので注意してください。コマンド中でフィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（44 ページ）で希望するフィルターの番号を確認してから指定してください。

■ ハードウェアパケットフィルターはデフォルトで有効になっています。無効に設定していた場合は、ENABLE SWITCH L3FILTER コマンド（35 ページ）で有効にしてください。

```
ENABLE SWITCH L3FILTER ↵
```

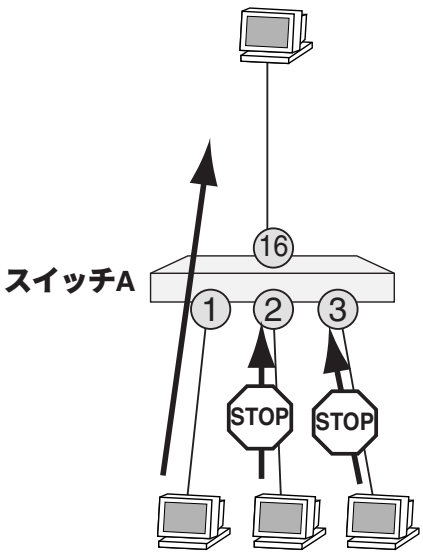
設定例

特定スイッチポートからのみ UDP 通信を許可

ハードウェアパケットフィルターを利用して、特定ポートからのみ UDP 通信を許可する設定例を示します。ここでは、次のようなネットワーク構成を例に説明します。

VLAN 名（VID）	untagged ポート	tagged ポート
default（1）	1-16	なし

表 4:



ここでは、次のようなフィルタリング条件を考えます。

- UDP トラフィックは原則として拒否する。
- ただし、ポート 1 からは UDP 通信を許可する。

ポート単位でのフィルタリングには、DHCP クライアントの IP アドレスが変更された場合でも対応できるメリットがあります。

✎ ハードウェアパケットフィルターには「許可」のアクションがありません。そのため、ハードウェアパケットフィルターをトラフィック制限に使用する場合は、拒否するトラフィックのパターンを指定していくことになります。

スイッチ A の設定

■ ハードウェアパケットフィルターの設定を行います。

- フィルターを作成しマッチ条件を指定します。ここでは UDP トラフィックだけを対象とするため、IP プロトコルフィールド（PROTOCOL）を条件として指定します。また、入力ポート単位でフィルタリングを行うため「IMPORT=TRUE」も指定します。

```
ADD SWITCH L3FILTER MATCH=PROTOCOL IMPORT=TRUE ↵
```

- 具体的な条件値とアクションを指定します。ここではプロトコルが UDP で、受信ポートが 2 か 3 のトラフィックを破棄するよう指定します。

```
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=UDP IPORT=2 ACTION=DENY ↵
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=UDP IPORT=3 ACTION=DENY ↵
```

- ハードウェアパケットフィルターを有効にします。

```
ENABLE SWITCH L3FILTER ↵
```

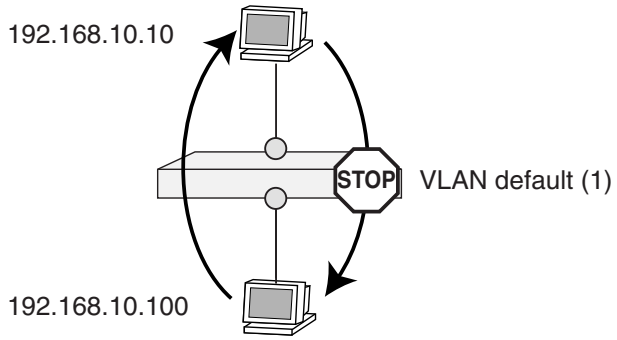
設定は以上です。

TCP 片方向通信

マッチ条件として TCP の制御フラグ Syn と Ack を使用し、192.168.10.100 からのみ TCP の通信を開始できるように設定します。

VLAN 名（VID）	untagged ポート	tagged ポート	IP アドレス
default（1）	1〜16	なし	192.168.10.1

表 5:



ここでは、次のようなフィルタリング条件を考えます。

- TCP は 192.168.10.100 から 192.168.10.10 への通信（セッション開始）のみを許可。192.168.10.10 から 192.168.10.100 への通信は拒否する。
- その他のプロトコルはすべて許可する。

✎ ハードウェアパケットフィルターには「許可」のアクションがありません。そのため、ハードウェアパケットフィルターをトラフィック制限に使用する場合は、拒否するトラフィックのパターンを指定していくことになります。

スイッチの設定

1. IP モジュールを有効にします。

```
ENABLE IP ↵
```

2. インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-default IP=192.168.10.1 MASK=255.255.255.0 ↵
```

3. ハードウェアパケットフィルターの設定を行います。
   - フィルターを作成しマッチ条件を指定します。ここではIPヘッダーの始点・終点IPアドレスとプロトコルフィールド、TCPヘッダーのSyn、Ackフラグを条件として指定します。サブネット単位でアドレスを指定するため、SCLASS、DCLASSにはC（クラスC＝24ビットマスク）を指定します。

     ```
     ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR,PROTOCOL,TCPACK,TCPSYN
       SCLASS=C DCLASS=C ↵
     ```

   - 具体的な条件値とアクションを指定します。ここでは192.168.10.10から192.168.10.100へのTCPセッション開始要求（Synパケット）を破棄するよう設定します。

     ```
     ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.10
       DIPADDR=192.168.10.100 PROTOCOL=TCP TCPSYN=TRUE TCPACK=FALSE
       ACTION=DENY ↵
     ```

   - ハードウェアパケットフィルターを有効にします。

     ```
     ENABLE SWITCH L3FILTER ↵
     ```

設定は以上です。

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

ADD SWITCH L3FILTER ENTRY

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

ADD SWITCH L3FILTER=*filter-id* ENTRY [IPORT=*port-number*]
[EPORT=*port-number*] [TYPE=*protocoltype*] [MACDADDR=*macadd*]
[MACSADDR=*macadd*] [TOS=*0..7*] [IPDSCP=*0..63*] [TTL=*0..255*] [PROTOCOL={TCP|UDP|ICMP|IGMP|*protocol*}] [SIPADDR=*ipadd*] [DIPADDR=*ipadd*] [TCPSPORT={*port*|*port-name*}] [TCPDPORT={*port*|*port-name*}] [TCPSYN={TRUE|FALSE}]
[TCPACK={TRUE|FALSE}] [TCPFIN={TRUE|FALSE}] [UDPSPORT={*port*|*port-name*}]
[UDPDPORT={*port*|*port-name*}] [ACTION={SETPRIORITY|SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|MOVETOSTOPRIO|MOVEPRITOTOS|NODROP|SETIPDSCP|SENDNONUNICASTTOPORT|FORWARD}[,...]] [PRIORITY=*0..7*] [NEWTOS=*0..7*]
[PORT=*port-number*] [NEWIPDSCP=*0..63*]

filter-id: フィルター番号（1〜16）
protocol: IP プロトコル番号（0〜255）
ipadd: IP アドレス
port: TCP/UDP ポート番号（0〜65535）
port-name: サービス名
protocoltype: L3 プロトコル番号（16 進数）
port-number: スイッチポート番号（1〜）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

ハードウェアパケットフィルターにフィルターエントリーを追加する。
ADD SWITCH L3FILTER MATCH コマンドで指定したすべてのパケットフィールドに対して、フィルタリング条件を実際の値で指定し、マッチ時のアクション（複数可）を指定する。
エントリー番号はコマンド実行時にシステムが自動で割り当てる。この番号は可変なので、エントリーの追加や削除によって前後にずれる可能性がある。他のコマンドでエントリー番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンドに ENTRY パラメーターを付けて実行し、希望するエントリーであることを確認してから指定すること。
フィルターエントリーは、10/100M ポートで最大 252 個まで（IGMP Snooping および MLD Snooping 無効時は 254 個）、1000M ポートで最大 124 個まで（IGMP Snooping および MLD Snooping 無効時は 126 個）まで設定可能。なお、LDF 検出機能を有効にした場合は、10/100M ポートおよび 1000M ポートで 1 個エントリーを消費する。

パラメーター

L3FILTER　フィルター（マッチ条件）番号。この番号は可変なので、SHOW SWITCH L3FILTER コマンドで確認してから指定すること
IPORT　（フィルタリング条件）対象パケットの入力スイッチポート。指定ポートから入力されたパケットだ

けがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで IMPORT=TRUE を指定した場合にのみ有効。

EPORT （フィルタリング条件）対象パケットの出力スイッチポート。指定ポートから出力されるパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで EMPORT=TRUE を指定した場合にのみ有効。ただし、EPORT パラメーターを指定した場合は、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットにはフィルターが適用されなくなるので注意すること。

TYPE （フィルタリング条件）対象パケット（フレーム）のレイヤー 3 プロトコルタイプフィールド値（16 進数）。本パラメーターを指定した場合、他のフィルタリング条件パラメーターは無効となる。また、ACTION に SETTOS を指定することはできない。プロトコル番号は、ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームタイプにおけるものを指定すること。Ethernet Version 2 と 802.2 LLC(DSAP、SSAP）におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長で指定する。

MACDADDR （フィルタリング条件）対象パケットの宛先 MAC アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの MACDADDR オプションで指定したマスクが適用される。

MACSADDR （フィルタリング条件）対象パケットの送信元 MAC アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの MACSADDR オプションで指定したマスクが適用される。

TOS （フィルタリング条件）対象パケットの IP TOS 優先度（TOS オクテットの precedence）フィールド値。有効範囲は 0〜7。

IPDSCP （フィルタリング条件）対象パケットの IP DSCP（DiffServ Code Point）フィールド値。有効範囲は 0〜63。

TTL （フィルタリング条件）対象パケットの IP TTL（生存時間）フィールド値。有効範囲は 0〜255。

PROTOCOL （フィルタリング条件）対象パケットの IP プロトコルフィールド値。TCP、UDP、CMP、IGMP については名前でも指定できる。その他プロトコルの場合は IP プロトコル番号で指定する。

SIPADDR （フィルタリング条件）対象パケットの始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される。

DIPADDR （フィルタリング条件）対象パケットの終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される。

TCPSPORT （フィルタリング条件）対象パケットの TCP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。

TCPDPORT （フィルタリング条件）対象パケットの TCP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。

TCPSYN （フィルタリング条件）対象パケットの TCP 制御フラグ「Syn」の値（オン・オフ）。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。

TCPACK （フィルタリング条件）対象パケットの TCP 制御フラグ「Ack」の値（オン・オフ）。TRUE、YES、ON はフラグが立っていることを、FALSE、NO、OFF はフラグが立っていないことを示す。

TCPFIN （フィルタリング条件）対象パケットの TCP 制御フラグ「Fin」の値（オン・オフ）。TRUE、

YES、ON はフラグが立っていることを、FALSE、NO、OFF はフラグが立っていないことを示す。

UDPSPORT （フィルタリング条件）対象パケットの UDP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL オプションに UDP を指定したときのみ有効。

UDPDPORT （フィルタリング条件）対象パケットの UDP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL オプションに UDP を指定したときのみ有効。

ACTION パケットがフィルターの条件に一致したときのアクション。カンマ区切りで複数のアクションを指定可能。

PRIORITY （アクションパラメーター）対象パケットに適用する 802.1p ユーザープライオリティー（0〜7）値。ACTION オプションに SETPRIORITY か SENDCOS を指定したときのみ有効。ACTION=SETPRIORITY のときは、パケットのユーザープライオリティーフィールドに PRIORITY オプションで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないと意味を持たない）。ACTION=SENDCOS のときは、パケットを PRIORITY オプションで指定したユーザープライオリティーに対応する送信キューに入れる。省略時は 0。

NEWTOS （アクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。ACTION オプションに SETTOS を指定したときのみ有効。

PORT （アクションパラメーター）対象パケットを出力するスイッチポート。ACTION オプションに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみ有効。入力ポートと出力ポートが同一 VLAN になるよう注意すること。

NEWIPDSCP （アクションパラメーター）パケット送信時に IP ヘッダーの DSCP（DiffServ Code Point）フィールドにセットする値。ACTION オプションに SETDSCP を指定したときのみ有効。

SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない。
SENDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる。
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効。
DENY	パケットを破棄する。もっとも効力の強いアクションであり、マッチしたエントリーの中に DENY アクションが含まれている場合は、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）。

SENDEPORT	パケットの出力先を PORT パラメーターで指定されたポートに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。
MOVETOSTOPRIO	IP ヘッダーの TOS オクテットの優先度フィールドを、VLAN タグフレームの 802.1p ユーザープライオリティー値に置き換える。
MOVEPRIOTOTOS	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを、IP ヘッダーの TOS オクテットの優先度値に置き換える。
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う。
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド値に、NEWIPDSCP オプションで指定された値を書き込む。
SENDNONUNICASTTOPORT	Unknown、M/C、B/C パケットなどの送出先を、PORT オプションで指定したスイッチポートからのみ出力する。
FORWARD	パケットを転送する。

表 6: ACTION パラメーターに指定できるオプション

例

■ポート 1〜3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY
```

■192.168.10.100 からの TCP コネクション確立要求を拒否（片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる）

```
ADD SWITCH L3FILTER MATCH=SIPADDR,PROTOCOL,TCPSYN,TCPACK SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
  TCPSYN=TRUE TCPACK=FALSE ACTION=DENY
```

■192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4
  ACTION=SETPRIORITY
```

備考・注意事項

フィルタリング条件として EPORT（出力スイッチポート）を指定した場合、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットにはフィルターが適用されなくなる。したがって、TCP 制御フラグによるフィルタリング（TCPSYN、TCPACK、TCPFIN パラメーター）を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないこと。

IGMP Snooping を有効にすると、IGMP Snooping 用にハードウェアパケットフィルターのエントリーが 1 つ作成され、ハードウェアパケットフィルター機能が有効化される。そのため、ユーザーが定義できるフィルターエントリーの数は 1 つ減少する。また、すでに最大数までフィルターエントリーを作成している場合は、IGMP Snooping を有効にできない。その場合は、先にエントリーを削除し、IGMP Snooping 用エントリーの空きを作る必要がある（DELETE SWITCH L3FILTER ENTRY コマンド）。IGMP Snooping 用エントリーはユーザーには見えない。

MLD Snooping を有効にすると、MLD Snooping 用にハードウェアパケットフィルターのエントリーが 1 つ作成され、ハードウェアパケットフィルター機能が有効化される。そのため、ユーザーが定義できるフィルターエントリーの数は 1 つ減少する。また、すでに最大数までフィルターエントリーを作成している場合は、MLD Snooping を有効にできない。その場合は、先にエントリーを削除し、MLD Snooping 用エントリーの空きを作る必要がある（DELETE SWITCH L3FILTER ENTRY コマンド）。MLD Snooping 用エントリーはユーザーには見えない。

関連コマンド

DELETE SWITCH L3FILTER ENTRY（33 ページ）
SET SWITCH L3FILTER ENTRY（36 ページ）
SHOW SWITCH L3FILTER（44 ページ）

ADD SWITCH L3FILTER MATCH

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

```
ADD SWITCH L3FILTER MATCH={NONE|TYPE|MACDADDR|MACSADDR|TOS|IPDSCP|TTL|
    PROTOCOL|SIPADDR|DIPADDR|TCPSPORT|TCPDPORT|TCPSYN|TCPACK|TCPFIN|UDPSPORT|
    UDPDPORT} [,… ] [IMPORT={YES|NO|ON|OFF|TRUE|FALSE}] [EMPORT={YES|NO|ON
    |OFF|TRUE|FALSE}] [MACDADDR=macadd] [MACSADDR=macadd] [SCLASS={A|B|C|HOST
    |1..32}] [DCLASS={A|B|C|HOST|1..32}] [TYPE={ETHII|ETHII-TAGGED
    |ETHII-UNTAGGED|802|802.2-TAGGED|802.2-UNTAGGED|SNAP|SNAP-TAGGED
    |SNAP-UNTAGGED}] [NOMATCHACTION={SETPRIORITY|SENDCOS|SETTOS|DENY
    |SENDEPORT|SENDMIRROR|MOVETOSTOPRIO|MOVEPRIOTOTOS|SETIPDSCP
    |SENDNONUNICASTTOPORT|FORWARD} [,… ] ] [NOMATCHPRIORITY=0..7
    ] [NOMATCHPORT=port-number] [NOMATCHDSCP=0..63] [NOMATCHTOS=0..
```

macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
port-number: スイッチポート番号（1〜）

解説

ハードウェアパケットフィルター（L3 フィルター）を作成する。
このコマンドでは、どのパケットフィールドをフィルタリング条件（マッチ条件）として使用するかを指定する。実際のフィルタリング条件（フィルターエントリー）は ADD SWITCH L3FILTER ENTRY コマンドで指定する。フィルター（マッチ条件）はシステム全体で 14 個まで（IGMP Snooping および MLD Snooping 無効時は 16 個まで）設定可能。
フィルター番号はコマンド実行時にシステムが自動で割り当てる。この番号は可変なので、他のフィルターの削除により変更される可能性がある。他のコマンドでフィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること。

パラメーター

MATCH　フィルタリング条件として使用するパケットフィールドを指定する。カンマ区切りで複数指定が可能。詳細は別表を参照。

IMPORT　特定のスイッチポートから入力されたパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの IPORT パラメーターで指定する（指定ポートから入力されたパケットだけがフィルタリングの対象となる）。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

EMPORT　特定のスイッチポートから出力されるパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターで指定する（指定ポートから出力されるパケットだけがフィルタリングの対象となる。ただし、本パラメーターに TRUE を指定した場合は、FDB に登録されていない MAC アドレス宛てのパケットがフィルタリング対象にならないという制限がある。詳細は ADD SWITCH L3FILTER

ENTRY コマンドの EPORT パラメーターの説明を参照)。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

MACDADDR MACDADDR（宛先 MAC アドレス）のパケットマッチング時に適用する、MAC アドレスのマスクパターンを指定する。省略時はフルマスク（ff-ff-ff-ff-ff-ff）

MACSADDR MACSADDR（送信元 MAC アドレス）のパケットマッチング時に適用する、MAC アドレスのマスクパターンを指定する。省略時はフルマスク（ff-ff-ff-ff-ff-ff）

SCLASS SIPADDR（始点 IP アドレス）のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A（8 ビット)、B（16 ビット)、C（24 ビット）の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1〜32 の任意長のマスクを指定できる。

DCLASS DIPADDR（終点 IP アドレス）のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A（8 ビット)、B（16 ビット)、C（24 ビット）の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1〜32 の任意長のマスクを指定できる。

TYPE フィルタリング条件として TYPE を指定した場合に、フレームフォーマット（エンキャプセレーション）を指定する。802（802.2 LLC)、ETHII（Ethernet Version 2)、SNAP（802.2 LLC + SNAP）から選択する。また、タグ付き（TAGGED)、タグ無し（UNTAGGED）も選択可能。指定しないときは、タグの有無に関係なく適用。ADD SWITCH L3FILTER ENTRY コマンドの TYPE パラメーターには、ここで指定したフレームタイプのプロトコル番号を指定する。

NOMATCHACTION マッチングしなかったときのアクションを指定。カンマ区切りで複数指定可能。

NOMATCHPRIORITY NONMATCHACTION=SETPRIORITY のとき、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、本オプションで指定したプライオリティー値を書き込む。NONMATCHACTION=SENDCOS のとき、本オプションで指定したプライオリティーに対応するレベルの送信キュー（CoS）に入れる。

NOMATCHTOS IP ヘッダーの TOS 優先度（precedence）フィールド値。有効範囲は、0〜7。

NOMATCHPORT パケットの出力先ポート番号を指定。

NOMATCHDSCP IP ヘッダーの DSCP（DiffServ Code Point）フィールド値。有効範囲は、1〜63。

NONE	下記 MATCH 条件を適用せず、入力ポートあるいは出力ポートのみでマッチングしたい場合に使用
TYPE	Ethernet フレームの L3 プロトコルタイプフィールド。本オプションを指定するときは、TYPE パラメーターでフレームタイプも指定する必要がある。MACDADDR/MACSADDR 以外のオプションとの併用はできない。
MACDADDR	宛先 MAC アドレスフィールド
MACSADDR	送信元 MAC アドレスフィールド
TOS	IP ヘッダーの TOS オクテットの優先度（precedence）フィールド
IPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド
TTL	IP ヘッダーの TTL（生存時間）フィールド
PROTOCOL	IP ヘッダーのプロトコルフィールド
SIPADDR	IP ヘッダーの始点 IP アドレス。本オプションを指定するときは、SCLASS パラメーターの指定も必要。
DIPADDR	IP ヘッダーの終点 IP アドレス。本オプションを指定するときは、DCLASS パラメーターの指定も必要。

TCPSPORT	TCP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPDPORT	TCP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPSYN	TCP ヘッダーの制御フラグ「Syn」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPACK	TCP ヘッダーの制御フラグ「Ack」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPFIN	TCP ヘッダーの制御フラグ「Fin」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
UDPSPORT	UDP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
UDPDPORT	UDP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。

表 7: MATCH パラメーターに指定できるオプション

SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、NOMATCHPRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない。
SENDCOS	パケットを NOMATCHPRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる。
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NOMATCHTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効。
DENY	パケットを破棄する。もっとも効力の強いアクションであり、マッチしたエントリーの中に DENY アクションが含まれている場合は、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）。
SENDEPORT	パケットの出力先を NOMATCHPORT パラメーターで指定されたポートに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。

MOVETOSTOPRIO	IP ヘッダーの TOS オクテットの優先度フィールドを、VLAN タグフレームの 802.1p ユーザープライオリティー値に置き換える。
MOVEPRIOTOTOS	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを、IP ヘッダーの TOS オクテットの優先度値に置き換える。
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド値に、NOMATCHDSCP オプションで指定された値を書き込む。
SENDNONUNICASTTOPORT	Unknown、M/C、B/C パケットなどの送出先を、NOMATCH-PORT オプションで指定したスイッチポートからのみ出力する。
FORWARD	パケットを転送する。

表 8: NOMATCHACTION パラメーターに指定できるオプション

例

■ポート 1〜3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY
```

■192.168.10.100 からの TCP コネクション確立要求を拒否（片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる）

```
ADD SWITCH L3FILTER MATCH=SIPADDR,PROTOCOL,TCPSYN,TCPACK SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
  TCPSYN=TRUE TCPACK=FALSE ACTION=DENY
```

■192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4
  ACTION=SETPRIORITY
```

■NetBEUI パケットをすべて破棄する。

```
ADD SWITCH L3FILTER MATCH=TYPE TYPE=802
ADD SWITCH L3FILTER=1 ENTRY TYPE=F0F0 ACTION=DENY
```

備考・注意事項

NOMATCHACTION パラメーターでデフォルトのアクションを指定したハードウェアパケットフィルターが存在する場合、その他のフィルターにマッチするパケットに対して、このアクションが実行さる。
複数のマッチ条件を指定したとき、マッチ条件の型が一致するような場合には、本製品のソフトウェアでマッチ条件が一つにまとめられる場合がある。同じパケットに対する処理でも、複数のマッチ条件がまとめられた場合と、一つ一つ実行された場合で、結果が異なることがある。

関連コマンド

ADD SWITCH L3FILTER ENTRY（22 ページ）
DELETE SWITCH L3FILTER（32 ページ）
SET SWITCH L3FILTER MATCH（40 ページ）
SHOW SWITCH L3FILTER（44 ページ）

DELETE SWITCH L3FILTER

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

DELETE SWITCH L3FILTER=*filter-id*

filter-id: フィルター番号（1〜16）

解説

ハードウェアパケットフィルターを削除する。
該当フィルターにエントリーが登録されている場合は削除できない。その場合は、DELETE SWITCH L3FILTER ENTRY コマンドですべてのエントリーを削除してから本コマンドを実行する。
フィルター番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること。
フィルターを削除すると、後続のフィルター（削除したフィルターより番号が大きいもの）の番号が 1 つずつ前にずれるので注意。

パラメーター

L3FILTER　フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

関連コマンド

ADD SWITCH L3FILTER MATCH（27 ページ）
SET SWITCH L3FILTER MATCH（40 ページ）
SHOW SWITCH L3FILTER（44 ページ）

DELETE SWITCH L3FILTER ENTRY

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

DELETE SWITCH L3FILTER=*filter-id* ENTRY=*entry-id*

filter-id: フィルター番号（1〜16）
entry-id: エントリー番号（1〜）

解説

ハードウェアパケットフィルターから指定したフィルターエントリーを削除する。
フィルター番号、エントリー番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること。エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれるので注意。

パラメーター

L3FILTER　フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

ENTRY　エントリー番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドに ENTRY オプションを付けて実行し、希望のエントリーを確認してから指定すること。

関連コマンド

ADD SWITCH L3FILTER ENTRY（22 ページ）
SET SWITCH L3FILTER ENTRY（36 ページ）
SHOW SWITCH L3FILTER（44 ページ）

DISABLE SWITCH L3FILTER

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 SWITCH L3FILTER

解説

ハードウェアパケットフィルター（L3 フィルター）機能を無効にする。デフォルトは有効（デフォルト有効の IGMP Snooping および MLD Snooping がハードウェアパケットフィルターを内部的に使用しているため）。

関連コマンド

ENABLE SWITCH L3FILTER（35 ページ）
SHOW SWITCH L3FILTER（44 ページ）

ENABLE SWITCH L3FILTER

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 SWITCH L3FILTER

解説

ハードウェアパケットフィルター（L3 フィルター）機能を有効にする。デフォルトは有効（デフォルト有効の IGMP Snooping および MLD Snooping がハードウェアパケットフィルターを内部的に使用しているため）。

関連コマンド

DISABLE SWITCH L3FILTER（34 ページ）
SHOW SWITCH L3FILTER（44 ページ）

SET SWITCH L3FILTER ENTRY

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 SWITCH L3FILTER=*filter-id* ENTRY=*entry-id* [IPORT=*port-number*]
[EPORT=*port-number*] [TYPE=*protocoltype*] [MACDADDR=*macadd*]
[MACSADDR=*macadd*] [TOS=*0..7*] [IPDSCP=*0..63*] [TTL=*0..255*] [PROTOCOL={TCP|UDP|ICMP|IGMP|*protocol*}] [SIPADDR=*ipadd*] [DIPADDR=*ipadd*] [TCPSPORT={*port*|*portname*}] [TCPDPORT={*port*|*portname*}] [TCPSYN={TRUE|FALSE}]
[TCPACK={TRUE|FALSE}] [TCPFIN={TRUE|FALSE}] [UDPSPORT={*port*|*portname*}]
[UDPDPORT={*port*|*portname*}] [ACTION={SETPRIORITY|SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|MOVETOSTOPRIO|MOVEPRITOTOS|NODROP|SETIPDSCP|SENDNONUNICASTTOPORT|FORWARD}[,...]] [PRIORITY=*0..7*] [NEWTOS=*0..7*]
[PORT=*port-number*] [NEWIPDSCP=*0..63*]

filter-id: フィルター番号（1〜16）
entry-id: エントリー番号（1〜）
protocol: IP プロトコル番号（0〜255）
ipadd: IP アドレス
port: TCP/UDP ポート番号（0〜65535）
portname: サービス名
protocoltype: L3 プロトコル番号（16 進数）
port-number: スイッチポート番号（1〜）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

ハードウェアパケットフィルターのフィルターエントリー（フィルタリング条件およびマッチ時のアクション）を変更する。
フィルタリングに使用するパケットフィールドの変更は、SET SWITCH L3FILTER MATCH コマンドで行う。

パラメーター

L3FILTER　フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

ENTRY　エントリー番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドに ENTRY パラメーターを付けて実行し、希望のエントリーを確認してから指定すること

IPORT　（フィルタリング条件）対象パケットの入力スイッチポート。指定ポートから入力されたパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで IMPORT=TRUE を指定した場合にのみ有効。

EPORT　（フィルタリング条件）対象パケットの出力スイッチポート。指定ポートから出力されるパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで EMPORT=TRUE

を指定した場合にのみ有効。ただし、EPORT パラメーターを指定した場合は、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットにはフィルターが適用されなくなるので注意すること。

TYPE （フィルタリング条件）対象パケット（フレーム）のレイヤー 3 プロトコルタイプフィールド値（16 進数）。本パラメーターを指定した場合、他のフィルタリング条件パラメーターは無効となる。また、ACTION に SETTOS を指定することはできない。プロトコル番号は、ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームタイプにおけるものを指定すること。Ethernet Version 2 と 802.2 LLC(DSAP、SSAP）におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長で指定する。

MACDADDR （フィルタリング条件）対象パケットの宛先 MAC アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの MACDADDR オプションで指定したマスクが適用される。

MACSADDR （フィルタリング条件）対象パケットの送信元 MAC アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの MACSADDR オプションで指定したマスクが適用される。

TOS （フィルタリング条件）対象パケットの IP TOS 優先度（TOS オクテットの precedence）フィールド値。有効範囲は 0～7。

IPDSCP （フィルタリング条件）対象パケットの IP DSCP（DiffServ Code Point）フィールド値。有効範囲は 0～63。

TTL （フィルタリング条件）対象パケットの IP TTL（生存時間）フィールド値。有効範囲は 0～255。

PROTOCOL （フィルタリング条件）対象パケットの IP プロトコルフィールド値。TCP、UDP、ICMP、IGMP については名前でも指定できる。その他プロトコルの場合は IP プロトコル番号で指定する。

SIPADDR （フィルタリング条件）対象パケットの始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される。

DIPADDR （フィルタリング条件）対象パケットの終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される。

TCPSPORT （フィルタリング条件）対象パケットの TCP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。

TCPDPORT （フィルタリング条件）対象パケットの TCP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。

TCPSYN （フィルタリング条件）対象パケットの TCP 制御フラグ「Syn」の値（オン・オフ）。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。

TCPACK （フィルタリング条件）対象パケットの TCP 制御フラグ「Ack」の値（オン・オフ）。TRUE、YES、ON はフラグが立っていることを、FALSE、NO、OFF はフラグが立っていないことを示す。

TCPFIN （フィルタリング条件）対象パケットの TCP 制御フラグ「Fin」の値（オン・オフ）。TRUE、YES、ON はフラグが立っていることを、FALSE、NO、OFF はフラグが立っていないことを示す。

UDPSPORT （フィルタリング条件）対象パケットの UDP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL オプションに UDP を指定したときのみ有効。

UDPDPORT （フィルタリング条件）対象パケットの UDP 終点ポート。ポート番号かサービス名で指定

する。PROTOCOL オプションに UDP を指定したときのみ有効。

ACTION パケットがフィルターの条件に一致したときのアクション。カンマ区切りで複数のアクションを指定可能。

PRIORITY （アクションパラメーター）対象パケットに適用する 802.1p ユーザープライオリティー（0〜7）値。ACTION オプションに SETPRIORITY か SENDCOS を指定したときのみ有効。ACTION=SETPRIORITY のときは、パケットのユーザープライオリティーフィールドに PRIORITY オプションで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないと意味を持たない）。ACTION=SENDCOS のときは、パケットを PRIORITY オプションで指定したユーザープライオリティーに対応する送信キューに入れる。省略時は 0。

NEWTOS （アクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。ACTION オプションに SETTOS を指定したときのみ有効。

PORT （アクションパラメーター）対象パケットを出力するスイッチポート。ACTION オプションに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみ有効。入力ポートと出力ポートが同一 VLAN になるよう注意すること。

NEWIPDSCP （アクションパラメーター）パケット送信時に IP ヘッダーの DSCP（DiffServ Code Point）フィールドにセットする値。ACTION オプションに SETDSCP を指定したときのみ有効。

SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない。
SENDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる。
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効。
DENY	パケットを破棄する。もっとも効力の強いアクションであり、マッチしたエントリーの中に DENY アクションが含まれている場合は、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）。

SENDEPORT	パケットの出力先を PORT パラメーターで指定されたポートに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。
MOVETOSTOPRIO	IP ヘッダーの TOS オクテットの優先度フィールドを、VLAN タグフレームの 802.1p ユーザープライオリティー値に置き換える。
MOVEPRIOTOTOS	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを、IP ヘッダーの TOS オクテットの優先度値に置き換える。
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド値に、NEWIPDSCP オプションで指定された値を書き込む。
SENDNONUNICASTTOPORT	Unknown、M/C、B/C パケットなどの送出先を、PORT オプションで指定したスイッチポートからのみ出力する。
FORWARD	パケットを転送する。

表 9: ACTION パラメーターに指定できるオプション

備考・注意事項

フィルタリング条件として EPORT（出力スイッチポート）を指定した場合、FDB に登録されていない MAC アドレス（ブロードキャスト、マルチキャスト、未学習のユニキャスト）宛てのパケットにはフィルターが適用されなくなる。したがって、TCP 制御フラグによるフィルタリング（TCPSYN、TCPACK、TCPFIN パラメーター）を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないこと。

関連コマンド

ADD SWITCH L3FILTER ENTRY（22 ページ）
ADD SWITCH L3FILTER MATCH（27 ページ）
DELETE SWITCH L3FILTER ENTRY（33 ページ）
SET SWITCH L3FILTER MATCH（40 ページ）
SHOW SWITCH L3FILTER（44 ページ）

SET SWITCH L3FILTER MATCH

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 SWITCH L3FILTER=*filter-id* MATCH={**NONE**|**TYPE**|**MACDADDR**|**MACSADDR**|**TOS**|
IPDSCP|**TTL**|**PROTOCOL**|**SIPADDR**|**DIPADDR**|**TCPSPORT**|**TCPDPORT**|**TCPSYN**|**TCPACK**|
TCPFIN|**UDPSPORT**|**UDPDPORT**} [,…] [IMPORT={YES|NO|ON|OFF|TRUE|FALSE}]
[EMPORT={YES|NO|ON|OFF|TRUE|FALSE}] [MACDADDR=*macadd*] [MACSADDR=*macadd*]
[SCLASS={A|B|C|HOST|*1..32*}] [DCLASS={A|B|C|HOST|*1..32*}] [TYPE={ETHII
|ETHII-TAGGED|ETHII-UNTAGGED|*802*|*802*.2-TAGGED|*802*.2-UNTAGGED|SNAP
|SNAP-TAGGED|SNAP-UNTAGGED}] [NOMATCHACTION={SETPRIORITY|SENDCOS|SETTOS
|DENY|SENDEPORT|SENDMIRROR|MOVETOSTOPRIO|MOVEPRIOTOTOS| SETIPDSCP
|SENDNONUNICASTTOPORT|FORWARD} [,…]] [NOMATCHPRIORITY=*0..7*
] [NOMATCHPORT=*port-number*] [NOMATCHDSCP=*0..63*] [NOMATCHTOS=*0..*

filter-id: フィルター番号（1〜16）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
port-number: スイッチポート番号（1〜）

解説

ハードウェアパケットフィルター（L3 フィルター）の設定を変更する。
本コマンドでは、フィルタリング条件（マッチ条件）として使用するパケットフィールドの指定を変更できる。具体的な条件値（エントリー）は SET SWITCH L3FILTER ENTRY コマンドで変更する。
該当フィルターにエントリーが登録されている場合は設定を変更できない。その場合は、DELETE SWITCH L3FILTER ENTRY コマンドですべてのエントリーを削除してから本コマンドを実行し、新しいマッチ条件に適合するよう再度エントリーを登録すること。

パラメーター

L3FILTER　フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

MATCH　フィルタリング条件として使用するパケットフィールドを指定する。カンマ区切りで複数指定が可能。詳細は別表を参照。

IMPORT　特定のスイッチポートから入力されたパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの IPORT パラメーターで指定する（指定ポートから入力されたパケットだけがフィルタリングの対象となる）。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

EMPORT　特定のスイッチポートから出力されるパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターで指定する（指定ポートから出力されるパケットだけがフィルタリングの対象となる。ただし、本パラメーターに TRUE を指定した場合は、FDB に登録されていない MAC アドレス宛て

のパケットがフィルタリング対象にならないという制限がある。詳細は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターの説明を参照)。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

MACDADDR MACDADDR（宛先 MAC アドレス）のパケットマッチング時に適用する、MAC アドレスのマスクパターンを指定する。省略時はフルマスク（ff-ff-ff-ff-ff-ff）

MACSADDR MACSADDR（送信元 MAC アドレス）のパケットマッチング時に適用する、MAC アドレスのマスクパターンを指定する。省略時はフルマスク（ff-ff-ff-ff-ff-ff）

SCLASS SIPADDR（始点 IP アドレス）のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A（8 ビット)、B（16 ビット)、C（24 ビット）の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1〜32 の任意長のマスクを指定できる。

DCLASS DIPADDR（終点 IP アドレス）のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A（8 ビット)、B（16 ビット)、C（24 ビット）の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1〜32 の任意長のマスクを指定できる。

TYPE フィルタリング条件として TYPE を指定した場合に、フレームフォーマット（エンキャプセレーション）を指定する。802（802.2 LLC)、ETHII（Ethernet Version 2)、SNAP（802.2 LLC + SNAP）から選択する。また、タグ付き（TAGGED)、タグ無し（UNTAGGED）も選択可能。指定しないときは、タグの有無に関係なく適用。ADD SWITCH L3FILTER ENTRY コマンドの TYPE パラメーターには、ここで指定したフレームタイプのプロトコル番号を指定する。

NOMATCHACTION マッチングしなかったときのアクションを指定。カンマ区切りで複数指定可能。

NOMATCHPRIORITY NONMATCHACTION=SETPRIORITYのとき、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、本オプションで指定したプライオリティー値を書き込む。NONMATCHACTION=SENDCOS のとき、本オプションで指定したプライオリティーに対応するレベルの送信キュー（CoS）に入れる。

NOMATCHTOS IP ヘッダーの TOS 優先度（precedence）フィールド値。有効範囲は、0〜7。

NOMATCHPORT パケットの出力先ポート番号を指定。

NOMATCHDSCP IP ヘッダーの DSCP（DiffServ Code Point）フィールド値。有効範囲は、1〜63。

NONE	下記 MATCH 条件を適用せず、入力ポートあるいは出力ポートのみでマッチングしたい場合に使用
TYPE	Ethernet フレームの L3 プロトコルタイプフィールド。本オプションを指定するときは、TYPE パラメーターでフレームタイプも指定する必要がある。MACDADDR/MACSADDR 以外のオプションとの併用はできない。
MACDADDR	宛先 MAC アドレスフィールドフィールド
MACSADDR	送信元 MAC アドレスフィールドフィールド
TOS	IP ヘッダーの TOS オクテットの優先度（precedence）フィールド
IPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド
TTL	IP ヘッダーの TTL（生存時間）フィールド
PROTOCOL	IP ヘッダーのプロトコルフィールド
SIPADDR	IP ヘッダーの始点 IP アドレス。本オプションを指定するときは、SCLASS パラメーターの指定も必要。

DIPADDR	IP ヘッダーの終点 IP アドレス。本オプションを指定するときは、DCLASS パラメーターの指定も必要。
TCPSPORT	TCP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPDPORT	TCP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPSYN	TCP ヘッダーの制御フラグ「Syn」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPACK	TCP ヘッダーの制御フラグ「Ack」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPFIN	TCP ヘッダーの制御フラグ「Fin」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
UDPSPORT	UDP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
UDPDPORT	UDP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。

表 10: MATCH パラメーターに指定できるオプション

SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、NOMATCHPRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない。
SENDCOS	パケットを NOMATCHPRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる。
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NOMATCHTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効。
DENY	パケットを破棄する。もっとも効力の強いアクションであり、マッチしたエントリーの中に DENY アクションが含まれている場合は、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）。

SENDEPORT	パケットの出力先を NOMATCHPORT パラメーターで指定されたポートに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。
MOVETOSTOPRIO	IP ヘッダーの TOS オクテットの優先度フィールドを、VLAN タグフレームの 802.1p ユーザープライオリティー値に置き換える。
MOVEPRIOTOTOS	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを、IP ヘッダーの TOS オクテットの優先度値に置き換える。
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド値に、NOMATCHDSCP オプションで指定された値を書き込む。
SENDNONUNICASTTOPORT	Unknown、M/C、B/C パケットなどの送出先を、NOMATCH-PORT オプションで指定したスイッチポートからのみ出力する。
FORWARD	パケットを転送する。

表 11: NOMATCHACTION パラメーターに指定できるオプション

関連コマンド

ADD SWITCH L3FILTER ENTRY（22 ページ）
ADD SWITCH L3FILTER MATCH（27 ページ）
DELETE SWITCH L3FILTER（32 ページ）
SET SWITCH L3FILTER ENTRY（36 ページ）
SHOW SWITCH L3FILTER（44 ページ）

SHOW SWITCH L3FILTER

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 SWITCH L3FILTER[=*filter-id* [ENTRY[=*entry-id*]]]

filter-id: フィルター番号（1〜16）
entry-id: エントリー番号（1〜）

解説

ハードウェアパケットフィルター（L3 フィルター）の設定内容を表示する。

パラメーター

L3FILTER　フィルター番号。番号を省略した場合は、フィルターの一覧が表示される。フィルター番号は可変なので、指定するときは SHOW SWITCH L3FILTER コマンドで確認してから指定すること。

ENTRY　エントリー番号。番号を省略した場合は、L3FILTER パラメーターで指定したフィルター内の全エントリーが表示される。エントリー番号は可変なので、指定するときは SHOW SWITCH L3FILTER コマンドに ENTRY パラメーターを付けて実行し、希望のエントリーを確認してから指定すること。本パラメーターを指定するときは、L3FILTER パラメーターでフィルター番号を指定しなくてはならない。

入力・出力・画面例

```
Manager > show switch l3filter

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Match Entry ................ 3 / 16
Entry Block 0 (Port1-8) .... 3 / 254
Entry Block 1 (Port9-16) ... 2 / 254
Entry Block 2 (Port17-24) .. 2 / 254

Filter ................. 1
Matched fields ......... sip
Type ................... ETHII
Source MAC addr. mask .. ff-ff-ff-ff-ff-ff
Dest. MAC addr. mask ... ff-ff-ff-ff-ff-ff
Source IP addr. mask ... 255.255.255.0
Dest. IP addr. mask .... 0.0.0.0
Ingress port mask ...... true
Egress port mask ....... false
```

```
Manager > show switch l3filter=1 entry

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Match Entry ................ 3 / 16
Entry Block 0 (Port1-8) .... 3 / 254
Entry Block 1 (Port9-16) ... 2 / 254
Entry Block 2 (Port17-24) .. 2 / 254

Filter ................. 1
Matched fields ......... sip
Type ................... ETHII
Source MAC addr. mask .. ff-ff-ff-ff-ff-ff
Dest. MAC addr. mask ... ff-ff-ff-ff-ff-ff
Source IP addr. mask ... 255.255.255.0
Dest. IP addr. mask .... 0.0.0.0
Ingress port mask ...... true
Egress port mask ....... false
Filter Entries:
--------------------------------------------------------------------------------
  Entry ................ 1
  Ingress Port ......... 1
  Egress Port .......... None
  Source MAC Address ... 00-00-00-00-00-00
  Source MAC Mask ...... ff-ff-ff-ff-ff-ff
  Dest MAC Address ..... 00-00-00-00-00-00
  Dest MAC Mask ........ ff-ff-ff-ff-ff-ff
  Source Address ....... 192.168.10.0
  Source Mask .......... 255.255.255.0
  Dest Address ......... 0.0.0.0
  Dest Mask ............ 0.0.0.0
  Protocol ............. 0
  TTL .................. 0
  TOS .................. 0
  IPDSCP ............... 0
  Type ................. 0800(ETHII)
  Action ............... DENY
--------------------------------------------------------------------------------
```

Hardware based filtering	ハードウェアパケットフィルター機能の有効/無効
Match Entry	マッチ条件エントリー数（システム単位）
Entry Block n	フィルターエントリー数（ブロック単位）
Matched fields	フィルタリング条件として用いるパケットフィールドの一覧。type0、macdaddr、macsaddr、tos、ipdscp、ttl、protocol、sipaddr、dipaddr、tcpsport、tcpdport、tcpsyn、tcpack、tcpfin、udpsport、udpdport の組み合わせ

Type	フレームタイプ
Source Mac addr. mask	送信元 MAC アドレスのマッチング時に適用するアドレスマスク
Dest. Mac addr. mask	宛先 MAC アドレスのマッチング時に適用するアドレスマスク
Source address mask	始点 IP アドレスのマッチング時に適用するアドレスマスク
Dest. address mask	終点 IP アドレスのマッチング時に適用するアドレスマスク
Ingress port mask	入力パケットに対するフィルタリングを指定ポートだけに限定するかどうか。
Egress port mask	出力パケットに対するフィルタリングを指定ポートだけに限定するかどうか。
Entry	フィルターエントリー番号
Ingress Port	フィルタリングを適用する入力ポート
Egress Port	フィルタリングを適用する出力ポート
Source MAC Address	送信元 MAC アドレスのマッチング時に適用する MAC アドレス
Source MAC Mask	送信元 MAC アドレスのマッチング時に適用するアドレスマスク
Dest MAC Address	宛先 MAC アドレスのマッチング時に適用する MAC アドレス
Dest MAC Mask	宛先 MAC アドレスのマッチング時に適用するアドレスマスク
Source Address	始点 IP アドレスのマッチング時に適用する IP アドレス
Source Mask	始点 IP アドレスのマッチング時に適用するアドレスマスク
Dest Address	始点 IP アドレスのマッチング時に適用する IP アドレス
Dest Mask	始点 IP アドレスのマッチング時に適用するアドレスマスク
Protocol	IP プロトコル番号
TTL	TTL（生存時間）フィールド値
TOS	TOS（サービスタイプ）優先度（precedence）値
IPDSCP	IPDSCP 値
Type	プロトコルタイプ（フレームタイプ）
Action	マッチ時のアクション。DENY、SETPRIORITY、SENDCOS、SETTOS、SENDEPORT、SENDMIRROR がある

表 12:

関連コマンド

ADD SWITCH L3FILTER ENTRY（22 ページ）
ADD SWITCH L3FILTER MATCH（27 ページ）
DELETE SWITCH L3FILTER（32 ページ）
DELETE SWITCH L3FILTER ENTRY（33 ページ）
DISABLE SWITCH L3FILTER（34 ページ）
ENABLE SWITCH L3FILTER（35 ページ）
SET SWITCH L3FILTER ENTRY（36 ページ）
SET SWITCH L3FILTER MATCH（40 ページ）