APRESIA

TD61-4048F

日立電線スイッチングハブ

Apresia3400/4300/5400/13000 シリーズ

AEOS Ver. 7

アプリケーションノート(パケットフィルター2 編)

日立電線株式会社

制 定 ・ 改 訂 来 歴 表

No.	年　月　日	内　容
-	2009 年 3 月 31 日	・新規作成
A	2009 年 11 月 5 日	・Apresia3448GT、Apresia3448G-PSR、Apresia5412 シリーズを追加
B	2010 年 7 月 30 日	・Apresia3424GT-HiPoE、Apresia5428GT を追加 ・表 1-19 最大ルール数と占有するグループ数を修正 ・1.11.6 AccessDefender 機能を修正 ・1.14 フィルター条件および動作の一括設定(multi コマンド)を追加
C	2010 年 8 月 30 日	・Apresia5412GT-HRSS,Apresia5412GT-HRSS-DC48V,Apresia5412GT-HRSS-DC110V を追加
D	2011 年 7 月 24 日	・表 8-1 複数のグループにマッチした場合のアクション概要を修正 ・表 17-1 各 AEOS7 バージョンでの機能追加、変更点を修正 ・1. 概要を修正 ・4.1 permit アクションを修正 ・4.2 deny アクションを修正 ・4.3 none アクションを追加 ・4.4 block-cpu-control アクションを追加 ・4.5 qos アクションを修正 ・6. CPU 宛フィルター機能を追加 ・7. 同一ルールに複数アクション設定時の動作を修正 ・14.3 手順(3) アクションの設定を修正 ・15. フィルター条件および動作の一括設定(multi コマンド)を修正 ・16. 制限事項および注意事項を修正 ・24. 受信時の CPU 宛フィルター機能を追加
E	2012 年 3 月 23 日	・適用機種一覧表を修正 ・CONFIG-FILTER モードの用語名を PACKETFILTER2 モードに変更 ・図 6-1 同一ルールに複数アクション設定時の動作図(通常グループ)を修正 ・図 6-2 同一ルールに複数アクション設定時の動作図(CPU 宛フィルターグループ)を修正 ・表 2-3 コンディションタイプと関係するコマンドを削除 ・表 2-4 コンディションタイプとフィルター条件(コンディション)を削除 ・表 3-2 コンディションタイプと関連コマンドおよびフィルター条件(コンディション)を追加 ・表 3-3 IPv4 関連のフィルター条件(コンディション)を修正 ・表 3-4 IPv6 関連のフィルター条件(コンディション)を修正 ・表 6-1 同一ルールに複数アクション設定時の注意点を修正 ・表 13-2 フィルター条件(コンディション)の設定項目を修正 ・表 13-3 アクションの設定項目を修正 ・表 15-1 multi コマンドの設定可能フィルター条件(コンディション)を修

No.	年　月　日	内　　容
		正 ・表 17-1 各 AEOS7 バージョンでの機能追加、変更点を修正 ・4. アクション(動作)章の構成を変更 ・4.2 deny アクションを修正 ・4.3 none アクションを修正 ・4.13 mirror アクションを修正 ・6. 同一ルールに複数アクション設定時の動作を修正 ・6.1 通常グループを修正 ・10. TCP/UDP ポート番号範囲指定エントリーを修正 ・11. ワイドモードを追加 ・14.2 手順(2) フィルター条件(コンディション)の設定を修正 ・14.3 手順(3) アクションの設定を修正 ・18. 受信時のフィルタリング機能を修正 ・19. 受信時の QP マッピング機能を修正 ・20. 送信フレームの 802.1p 優先度変更機能を修正 ・21. 受信時の QP マッピング＋送信フレームの 802.1p 優先度変更機能を修正 ・22. 送信パケットの DSCP 値/IP Precedence 値変更機能を修正 ・23. 受信時の帯域制限機能を修正 ・24. 受信時の CPU 宛フィルター機能を修正
F	2012 年 6 月 8 日	・3.2.1 宛先 MAC アドレス条件、送信元 MAC アドレス条件を修正 ・3.2.2 VLAN ID 条件を修正 ・3.2.3 Ethernet Type 条件を修正 ・3.2.4 ARP 送信元 IP アドレス(arp-sender-ip)条件を修正 ・3.2.5 IPv4 関連の条件を修正 ・3.2.6 IPv6 関連の条件を修正 ・3.3 マスク指定を修正 ・3.3.1 16 進設定値に対するマスク指定を追加 ・3.3.2 10 進設定値に対するマスク指定を追加

はじめに

本書は、日立電線製 BOX 型スイッチングハブ APRESIA シリーズのファームウェア AEOS Ver. 7 の機能概要および構成・設定例を記述しています。それ以外のハードウェアに関する説明および操作方法については、ハードウェアマニュアルおよびインストレーションガイドを参照して下さい。また各種コマンドに関する説明は、最新のコマンドリファレンスを参照して下さい。

適用機種一覧表

シリーズ名称		製品名称	バージョン
Apresia 3400 シリーズ	Apresia 3424 シリーズ	Apresia3424GT-SS	Ver. 7.28
		Apresia3424GT-PoE	
		Apresia3424GT-HiPoE	
	Apresia 3448 シリーズ	Apresia3448GT	
		Apresia3448G-PSR	
Apresia 4300 シリーズ	Apresia 4328 シリーズ	Apresia4328GT	
	Apresia 4348 シリーズ	Apresia4348GT	
		Apresia4348GT-PSR	
Apresia5400 シリーズ		Apresia5412GT-PoE	
		Apresia5412GT-HRSS	
		Apresia5412GT-HRSS-DC48V	
		Apresia5412GT-HRSS-DC110V	
		Apresia5428GT	
Apresia13000 シリーズ		Apresia13000-24GX-PSR	
		Apresia13000-48X	

この注意シンボルは、そこに記述されている事項が人身の安全と直接関係しない注意書きに関するものであることを示し、注目させる為に用います。

目次

1. 概要

パケットフィルター2 とは、定義した条件に一致した受信トラフィックに対して、フィルタリングだけでなく QP マッピングや帯域制限等を実施することが可能な機能です。パケットフィルター2 が対象とする受信トラフィックは装置がハードウェア中継転送するトラフィック、および、装置の CPU 宛トラフィックです。下記の点に注意して下さい。

・管理ポートで受信したトラフィックは非対象です。
・装置の CPU 宛トラフィックは CPU 宛フィルター機能でフィルタリング可能です。CPU 宛トラフィックの例を下記に示します。
  ・STP/RSTP/MSTP が有効な場合の BPDU フレームや LLDP フレーム/LACP フレーム等の装置が中継転送することのない制御フレーム。
  ・装置がソフトウェア中継を行うフレーム(STP/RSTP/MSTP が無効でかつ BPDU 転送制限機能が無効な場合の BPDU フレーム等)。
  ・VLAN インターフェースに IP アドレスを設定している場合の制御パケット(装置宛ての ARP パケットや、RIP/OSPF を有効にしている場合の RIP/OSPF パケット等)。

パケットフィルター2 を使用することにより下記のような機能を実現できます。設定例に関しては各章を参照して下さい。

・「18.受信時のフィルタリング機能」
・「19.受信時のQPマッピング機能」
・「20.送信フレームの 802.1p優先度変更機能」
・「21.受信時のQPマッピング＋送信フレームの 802.1p優先度変更機能」
・「22.送信パケットのDSCP値/IP Precedence値変更機能」
・「23.受信時の帯域制限機能」
・「24.受信時のCPU宛フィルター機能」

これらはパケットフィルター2 をユーザーが明示的に設定して使用する機能ですが、これ以外にもパケットフィルター2 のリソースを自動的に占有する機能があります。これら機能に関する注意点については「12 パケットフィルター2 のリソースを自動的に占有する機能」を参照して下さい。

2. グループ

パケットフィルター2 は複数のグループを設定可能です。一つのグループは複数のルール/帯域制限エントリー/カウンターと呼ばれる機能要素から構成されています。それ以外に、全グループで共有して使用するTCP/UDPポート番号範囲指定エントリーという機能要素もあります。装置種別によりこれらの上限が異なることに注意して下さい(表 2-1、表 2-2 参照)。

表 2-1 パケットフィルター2 のグループ数

No.	製品種別	グループ数
1	Apresia3400 シリーズ Apresia4348 シリーズ Apresia5400 シリーズ Apresia13000-48X	14 個 (1-14)
2	Apresia13000-24GX-PSR	14 個 (1-14)
3	Apresia4328GT	7 個 (1-7)

表 2-2 グループあたりのルール/帯域制限エントリー/カウンター数

No.	製品種別	ルール数	帯域制限 エントリー数	カウンター数
1	Apresia3400 シリーズ Apresia4348 シリーズ Apresia5400 シリーズ Apresia13000-48X	128 個 (1-128)	64 個 (1-64)	64 個 (1-64)
2	Apresia13000-24GX-PSR	256 個 (1-256)	128 個 (1-128)	128 個 (1-128)
3	Apresia4328GT	128 個 (1-128)	64 個 (1-64)	64 個 (1-64)

一つのグループには複数のルールを設定することができますが、同一グループ内の全てのルールはフィルター条件に用いるコンディションタイプを共有します。このコンディションタイプとは、受信トラフィックのパターンマッチを行う際の抽出条件(送信元 MAC アドレスや、宛先 IPv4 アドレス等)としてどのフィールドの情報を抽出するのかを絞り込むために定義されます。当然、対象トラフィックの中の全ての情報を抽出できることが望ましいのですが、現実的にはそのような仕組みの実現と性能を両立することは非常に困難なため、コンディションタイプによって抽出する情報の範囲の絞り込みが必要になります。

コンディションタイプはユーザーが明示的に設定する必要はありません。使用するグループの任意のルールで最初にフィルター条件を設定した際に自動的にコンディションタイプが定義されます。それぞれのコンディションタイプでどのようなフィルター条件を使用できるかに関しては 表 3-2 を参照してください。

グループ毎に異なるコンディションタイプを定義できるため、設定によってはある対象トラフィックが複数のグループのルールにマッチして、複数のアクションが選ばれる場合も考えられます。そのよう

な場合に、最終的にどのアクションが適用されるかに関しては「7 複数グループにマッチした場合の動作」を参照して下さい。

3. ルール

各ルールではパケットフィルター2 に必要な識別条件(アサイン)・フィルター条件(コンディション)・アクション(動作)等の情報を定義します。

ある一つのグループの各ルールは若番から順番にチェックされ、マッチした場合にはそれ以降のルールはチェックしない、いわゆる First Match の規則で動作します。なお、例えば将来の拡張のために Rule_ID：10 Rule_ID：20 Rule_ID：30 …… と、ルール ID 番号を連番でない設定をすることも可能です。

以降では識別条件・フィルター条件について説明します。

3.1 識別条件(アサイン)

識別条件はルールを適用する受信ポートもしくは受信VLANを指定します。これはパケットフィルター2 を使用する場合に必ず設定する必要があります。受信ポートは複数ポート設定可能ですが、受信VLANはマスク指定による範囲指定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。なお、識別条件だけを設定してフィルター条件を設定しない場合には、識別条件に一致した全ての受信トラフィックが対象になります。

識別条件は基本的にはルール毎に設定しますが、同一グループの全てのルールにおいて同じ識別条件を使用する場合には、そのグループ全体に対して識別条件を設定することも可能です。使用可能な識別条件の組み合わせとその概要を 表 3-1 に示します。

表 3-1 識別条件(アサイン)の設定可能な組み合わせ

No.	識別条件の組み合わせ				概要
	グループ全体指定		ルール毎指定		
	Port	VLAN	Port	VLAN	
1	―	―	設定有	―	・対象は当該ルールのみとなります。 ・指定したポートで受信したトラフィックが対象です。
2	―	―	―	設定有	・対象は当該ルールのみとなります。 ・指定した VLAN で受信したトラフィックが対象です。
3	―	―	設定有	設定有	・対象は当該ルールのみとなります。 ・指定したポートの指定したVLANで受信したトラフィックが対象です。
4	設定有	―	―	―	・対象は当該グループの全ルールとなります。 ・指定したポートで受信したトラフィックが対象です。
5	―	設定有	―	―	・対象は当該グループの全ルールとなります。 ・指定した VLAN で受信したトラフィックが対象です。
6	設定有	設定有	―	―	・対象は当該グループの全ルールとなります。 ・指定したポートの指定したVLANで受信したトラフィックが対象です。
7	設定有	―	―	設定有	・「受信ポート」条件に関しては当該グループの全ルー

No.	識別条件の組み合わせ				概要
	グループ全体指定		ルール毎指定		
	Port	VLAN	Port	VLAN	
					ルが対象ですが、「受信ポート＋受信 VLAN」条件に関しては当該ルールのみ対象となります。
8	－	設定有	設定有	－	・「受信 VLAN」条件に関しては当該グループの全ルールが対象ですが、「受信ポート＋受信 VLAN」条件に関しては当該ルールのみ対象となります。

3.2 フィルター条件(コンディション)

フィルター条件はルールを適用するトラフィックの詳細な情報を定義します。各ルールで設定できるフィルター条件はコンディションタイプにより異なります。それぞれのコンディションタイプでどのようなフィルター条件を使用できるかに関しては 表 3-2 を参照して下さい。

表 3-2 コンディションタイプと関連コマンドおよびフィルター条件(コンディション)

No.	タイプ	関連コマンドおよびコンディション
1	dst	<GROUP> <RULE> condition dst 関連コマンド全て 宛先 MAC アドレス・VLAN ID・Ethernet Type・宛先 IPv4 アドレス
		・宛先 IPv4 アドレス条件は、対象が IPv4 パケット(Ethernet Type = 0x0800)の場合に有効です。 ・Ethernet Type 条件で 0x0806(ARP)を指定したとしても、ARP パケットの Target protocol address フィールドの指定のために宛先 IPv4 アドレス条件は使用できないことに注意してください。
2	src	<GROUP> <RULE> condition src 関連コマンド全て 送信元 MAC アドレス・VLAN ID・Ethernet Type・送信元 IPv4 アドレス・ARP 送信元 IP アドレス
		・送信元 IPv4 アドレス条件は、対象が IPv4 パケット(Ethernet Type = 0x0800)の場合に有効です。 ・Ethernet Type 条件で 0x0806(ARP)を指定したとしても、ARP パケットの Sender protocol address フィールドの指定のために送信元 IPv4 アドレス条件は使用できないことに注意してください。 ・同一ルール内では「送信元 IPv4 アドレス＋Ethernet Type 条件」と「ARP 送信元 IP アドレス条件」の併用設定は不可です。
3	ethernet	<GROUP> <RULE> condition ethernet 関連コマンド全て 宛先 MAC アドレス・送信元 MAC アドレス・VLAN ID・Ethernet Type
4	ipv4	<GROUP> <RULE> condition ipv4 関連の全コマンド 送信元 IPv4 アドレス・宛先 IPv4 アドレス・TOS フィールド・DSCP 値・IP Precedence 値・プロトコルフィールド・送信元 TCP/UDP ポート番号・宛先 TCP/UDP ポート番号・TCP ヘッダーの制御 Flag フィールド

No.	タイプ	関連コマンドおよびコンディション
		•TCP/UDP ポート番号指定は、単一の TCP/UDP ポート番号を指定した場合です。
		•IPv4 関連の条件は対象が IPv4 パケット(Ethernet Type = 0x0800)の場合に有効です。 •TCP/UDP ポート番号条件は対象が TCP もしくは UDP パケットの場合に有効です。 •TCP ヘッダーの制御 Flag フィールド条件は対象が TCP パケットの場合に有効です。 •TCP/UDP ポート番号は単一の TCP/UDP ポート番号のみ指定可能です。範囲指定した場合はコンディションタイプが変わることに注意してください。 •同一ルールでの併用設定の注意点に関しては 表 3-3 を参照してください。
5	ipv4-src-tcp /udp-range	<GROUP> <RULE> condition ipv4 src tcp/udp 関連コマンド
		•基本的には ipv4 コンディションの場合と同じです。 •送信元 TCP/UDP ポート番号の範囲指定が可能です。単一指定した場合はコンディションタイプが変わります。 •範囲指定時の注意点は「10 TCP/UDPポート番号範囲指定エントリー」を参照してください。
6	ipv4-dst-tcp /udp-range	<GROUP> <RULE> condition ipv4 dst tcp/udp 関連コマンド
		•基本的には ipv4 コンディションの場合と同じです。 •宛先 TCP/UDP ポート番号の範囲指定が可能です。単一指定した場合はコンディションタイプが変わります。 •範囲指定時の注意点は「10 TCP/UDPポート番号範囲指定エントリー」を参照してください。
7	ipv6	<GROUP> <RULE> condition ipv6 src 関連コマンド <GROUP> <RULE> condition ipv6 dst 関連コマンド
		•基本的には ipv6-src-ip、ipv6-dst-ip コンディションの場合と同じです。 •IPv6 アドレス条件は、wide-mode 使用時かつ、TCP/UDP ポート番号条件と同一グループに設定していない場合に ipv6 コンディションタイプが定義されます。TCP/UDP ポート番号条件と同一グループに設定した場合はコンディションタイプが変わることに注意してください。
8	ipv6-header	<GROUP> <RULE> condition ipv6 {flow-label|hop-limit|next-header|traffic-class|icmp type} Traffic Class フィールド・Flow Label フィールド・Next Header フィールド・Hop Limit フィールド・ICMPv6 ヘッダーType フィールド
		•IPv6 ヘッダー関連の条件は、対象が IPv6 パケット(Ethernet Type = 0x86DD)の場合に有効です。 •icmp type は wide-mode 使用時のみ指定可能です。 •同一ルール内では「Next Header フィールド条件」と「ICMPv6 ヘッダーType フィールド」の併用設定は不可です。
9	ipv6-src-ip	<GROUP> <RULE> condition ipv6 src 関連コマンド 送信元 IPv6 アドレス

No.	タイプ	関連コマンドおよびコンディション
		・送信元 IPv6 アドレス条件は、対象が IPv6 パケット(Ethernet Type = 0x86DD)の場合に有効です。
10	ipv6-dst-ip	<GROUP> <RULE> condition ipv6 dst 関連コマンド 宛先 IPv6 アドレス
		・宛先 IPv6 アドレス条件は、対象が IPv6 パケット(Ethernet Type = 0x86DD)の場合に有効です。
11	ipv6-tcp/udp-range	<GROUP> <RULE> condition ipv6 src tcp/udp 関連コマンド <GROUP> <RULE> condition ipv6 dst tcp/udp 関連コマンド 送信元 TCP/UDP ポート番号・宛先 TCP/UDP ポート番号
		・TCP/UDP ポート番号指定は対象が TCP もしくは UDP パケットの場合に有効です。 ・TCP/UDP ポート番号の範囲指定が可能です。 ・TCP/UDPポート番号指定時の注意点については「10 TCP/UDPポート番号範囲指定エントリー」を参照してください。 ・wide-mode 使用時のみ指定可能です。

3.2.1 宛先MACアドレス条件、送信元MACアドレス条件

宛先 MAC アドレス条件は dst、ethernet コンディションタイプのルールで使用可能です。送信元 MAC アドレス条件は src、ethernet コンディションタイプのルールで使用可能です。

指定した宛先 MAC アドレス条件もしくは送信元 MAC アドレス条件が、受信トラフィックの宛先 MAC アドレスもしくは送信元 MAC アドレスと一致した場合に対象となります。

MACアドレス条件はマスク指定での設定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

3.2.2 VLAN ID条件

VLAN ID 条件は dst、src、ethernet コンディションタイプのルールで使用可能です。

VLAN ID 条件は受信トラフィックの種類によって動作が異なります。受信トラフィックを装置が Untag フレームと認識した場合には、「ポートに設定した VLAN ID」と「パケットフィルター2 の VLAN ID 条件」が一致した場合に対象になります。受信トラフィックを装置が Tag フレームと認識した場合には、「受信トラフィックの VLAN タグの VID 情報」と「パケットフィルター2 の VLAN ID 条件」が一致した場合に対象になります。ただし例外として、“ ignore-tag enable ”を設定した装置のアクセスポートで Tag フレームを受信した場合には、Untag フレームとして認識した場合と同様の動作になることに注意して下さい。

VLAN ID条件はマスク指定での設定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

“ tag-type ”で設定した TPID(Tag Protocol Identifier)と受信した VLAN タグ付きフレームの TPID が等しい場合に、装置はその受信フレームを Tag フレームとして認識します。TPID のデフォルト設定は 0x8100。装置の TPID と異なる VLAN タグ付きフ

レームを受信した場合には、その受信フレームは Untag フレームとして認識します。

“ switchport access vlan <VID> ” で設定したアクセスポート、“ switchport trunk native <VID> ”で設定した Native VLAN のポート、“ switchport trunk protocol <VID> ” で設定した Protocol VLAN のポートで VLAN タグ無しフレームを受信した場合に、装置はその受信フレームを Untag フレームとして認識します。

“ switchport access vlan <VID> ” で設定したアクセスポートで TPID が等しい VLAN タグ付きフレームを受信した場合には、その VLAN タグの VID 情報とアクセスポートに設定した VLAN ID が等しければ VLAN タグを外して受信し中継します(IEEE802.1Q 準拠)。この場合、パケットフィルター2 ではその受信トラフィックを Tag フレームとして認識することに注意して下さい。

“ ignore-tag enable ” を設定した装置のアクセスポートでは TPID が等しい VLAN タグ付きフレームを受信した場合でも、あたかも Untag フレームと同様に受信して中継するようになります。しかしながら「VLAN ID 条件の場合の例外」を除いて、パケットフィルター2 ではその受信トラフィックを Tag フレームとして認識することに注意して下さい。

3.2.3 Ethernet Type条件

Ethernet Type 条件は dst、src、ethernet コンディションタイプのルールで使用可能です。

指定した Ethernet Type 条件が受信トラフィックの Ethernet Type と一致した場合に対象となります。

Ethernet Type 条件は受信トラフィックを装置が Untag フレームと認識した場合だけでなく、受信トラフィックを Tag フレームと認識した場合でも適用可能です。ただし、装置の TPID と異なる VLAN タグ付きフレームを Untag フレームと認識して受信した場合には適用することはできません。もし適用した場合には、その受信フレームの TPID(4byte)と Ethernet Type 条件が一致した場合に対象となります。

Ethernet Type条件はマスク指定での設定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

3.2.4 ARP送信元IPアドレス(arp-sender-ip)条件

ARP 送信元 IP アドレス条件は src コンディションタイプのルールでのみ使用可能で、ARP ヘッダーの中の Sender protocol address フィールドを対象とする唯一のフィルター条件です。

指定した ARP 送信元 IP アドレス条件が受信 ARP パケットの Sender protocol address フィールドと一致した場合に対象となります。

ARP 送信元 IP アドレス条件は受信トラフィックを装置が Untag フレームと認識した場合だけでなく、受信トラフィックを Tag フレームと認識した場合でも適用可能です。ただし、装置の TPID と異なる VLAN タグ付きフレームを Untag フレームと認識して受信した場合には適用することはできません。

なお、同一ルール内では「送信元 IPv4 アドレス条件＋Ethernet Type 条件」と「ARP 送信元 IP アドレス条件」を併用して設定はできないことに注意して下さい。

ARP送信元IPアドレス条件はプレフィックス表記によるマスク指定での設定が可能です。マスク指定

の詳細に関しては「3.3 マスク指定」を参照して下さい。

ARP 送信元 IP アドレス条件を使用しても、deny アクションを使用して装置宛て ARP パケットの CPU 処理を抑止することはできないことに注意して下さい。ただし、同じ VLAN の他のポートにフラッディング中継することに対して deny アクションは動作します。

3.2.5 IPv4 関連の条件

指定した IPv4 関連の条件が受信トラフィックの情報と一致した場合に対象となります。

IPv4 関連の条件は受信トラフィックを装置が Untag フレームと認識した場合だけでなく、受信トラフィックを Tag フレームと認識した場合でも適用可能です。ただし、装置の TPID と異なる VLAN タグ付きフレームを Untag フレームと認識して受信した場合には適用することはできません。

いくつかのIPv4 関連の条件はマスク指定での設定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

IPv4 関連のフィルター条件について 表 3-3 に示します。

表 3-3 IPv4 関連のフィルター条件(コンディション)

No.	condition	概要
1	送信元 IPv4 アドレス	・src、ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・送信元 IPv4 アドレスを指定します。プレフィックス表記によるマスク指定が可能です。
2	宛先 IPv4 アドレス	・dst、ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・宛先 IPv4 アドレスを指定します。プレフィックス表記によるマスク指定が可能です。
3	TOS フィールド (tos)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・IPv4 ヘッダーの TOS フィールド(8bit)を指定します。マスク指定が可能です。 ・TOS フィールド条件を設定したルールでは DSCP 値・IP Precedence 値条件の併用設定は不可となります。
4	DSCP 値 (tos-dscp)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・IPv4 ヘッダーの DSCP 値(6bit)を指定します。マスク指定が可能です。 ・DSCP 値条件を設定したルールでは TOS フィールド・IP Precedence 値条件の併用設定は不可となります。
5	IP Precedence 値 (tos-precedence)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・IPv4 ヘッダーの IP Precedence 値(3bit)を指定します。マスク指定が可能

No.	condition	概要
		です。 ・IP Precedence 値条件を設定したルールでは TOS フィールド・DSCP 値条件の併用設定は不可となります。
6	プロトコルフィールド (protocol)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・IPv4 ヘッダーのプロトコルフィールドを指定します。マスク指定が可能です。 ・プロトコルフィールド条件を設定したルールでは TCP/UDP ポート番号・TCP ヘッダーの制御 Flag フィールド条件の併用設定は不可となります。
7	送信元 TCP/UDP ポート番号 (src tcp/udp)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・ipv4、ipv4-dst-tcp/udp-range コンディションタイプの場合は単一の送信元 TCP/UDP ポート番号を指定します。ipv4-src-tcp/udp-range コンディションタイプの場合は連続範囲指定します。 ・オプションで TCP 指定もしくは UDP 指定が可能です。 ・指定可能な連続範囲指定パターンは装置全体で 16 パターンまで可能です。この際にTCP/UDPポート番号範囲指定エントリーが自動的に設定されます。TCP/UDPポート番号範囲指定エントリーに関しては「10 TCP/UDPポート番号範囲指定エントリー」を参照してください。 ・TCP/UDP ポート番号条件を設定したルールではプロトコルフィールド・TCP ヘッダーの制御 Flag フィールド条件の併用設定は不可となります。ただし例外としてオプション TCP 指定で設定した場合には TCP ヘッダーの制御 Flag フィールド条件は併用設定可能です。 ・オプションで TCP を指定したルールは宛先 TCP/UDP ポートも TCP 指定のみ設定可能です。オプション UDP 指定の場合も同様です。
8	宛先 TCP/UDP ポート番号 (dst tcp/udp)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・ipv4、ipv4-src-tcp/udp-range コンディションタイプの場合は単一の宛先 TCP/UDP ポート番号を指定します。ipv4-dst-tcp/udp-range コンディションタイプの場合は連続範囲指定します。 ・オプションで TCP 指定もしくは UDP 指定が可能です。 ・指定可能な連続範囲指定パターンは装置全体で 16 パターンまで可能です。この際にTCP/UDPポート番号範囲指定エントリーが自動的に設定されます。TCP/UDPポート番号範囲指定エントリーに関しては「10 TCP/UDPポート番号範囲指定エントリー」を参照してください。 ・TCP/UDP ポート番号条件を設定したルールではプロトコルフィールド・TCP ヘッダーの制御 Flag フィールド条件の併用設定は不可となります。ただし例外としてオプション TCP 指定で設定した場合には TCP ヘッダーの制御 Flag フィールド条件は併用設定は可能です。

No.	condition	概要
		・オプションで TCP を指定したルールは送信元 TCP/UDP ポートも TCP 指定のみ設定可能です。オプション UDP 指定の場合も同様です。
9	TCP ヘッダーの制御 Flag フィールド (tcp-flag)	・ipv4、ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range コンディションタイプのルールで使用可能です。 ・TCP ヘッダーの制御 Flag フィールド(6bit)の各制御コード(FIN、SYN、RST、PSH、ACK、URG)のビットを指定します(0 or 1)。指定しないビットに関しては自動的に任意の値としてマスクが設定されます。 ・TCP ヘッダーの制御 Flag フィールド条件を設定したルールではプロトコルフィールド・TCP/UDP ポート番号条件の併用設定は不可となります。ただし例外として TCP/UDP ポート番号条件をオプション TCP 指定で設定した場合には併用設定は可能です。

3.2.6 IPv6 関連の条件

指定した IPv6 関連の条件が受信トラフィックの情報と一致した場合に対象となります。

IPv6 関連の条件は受信トラフィックを装置が Untag フレームと認識した場合だけでなく、受信トラフィックを Tag フレームと認識した場合でも適用可能です。ただし、装置の TPID と異なる VLAN タグ付きフレームを Untag フレームと認識して受信した場合には適用することはできません。

IPv6 関連の条件はマスク指定での設定が可能です。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

IPv6 関連のフィルター条件について 表 3-4 に示します。

表 3-4 IPv6 関連のフィルター条件(コンディション)

No.	condition	概要
1	Traffic Class フィールド (traffic-class)	・ipv6-header コンディションタイプのルールで使用可能です。 ・IPv6 ヘッダーの Traffic Class フィールド(8bit)を指定します。マスク指定が可能です。
2	Flow Label フィールド (flow-label)	・ipv6-header コンディションタイプのルールで使用可能です。 ・IPv6 ヘッダーの Flow Label フィールド(20bit)を指定します。マスク指定が可能です。
3	Next Header フィールド (next-header)	・ipv6-header コンディションタイプのルールで使用可能です。 ・IPv6 ヘッダーの Next Header フィールド(8bit)を指定します。マスク指定が可能です。 ・Next Header フィールド条件を設定したルールでは ICMPv6 ヘッダー Type フィールド条件の併用設定は不可となります。
4	Hop Limit フィールド (hop-limit)	・ipv6-header コンディションタイプのルールで使用可能です。 ・IPv6 ヘッダーの Hop Limit フィールド(8bit)を指定します。マスク指定が可能です。
5	ICMPv6 ヘッダー Type フィールド	・ipv6-header コンディションタイプのルールで使用可能です。 ・ICMPv6 ヘッダーの Type フィールド(8bit)を指定します。マスク指定

No.	condition	概要
	(icmp type)	が可能です。 ・ICMPv6 ヘッダーType フィールド条件を設定したルールでは Next Header フィールド条件の併用設定は不可となります。
6	送信元 IPv6 アドレス	・ipv6、ipv6-src-ip、ipv6-tcp/udp-range コンディションタイプのルールで使用可能です。 ・送信元 IPv6 アドレスを指定します。プレフィックス長によるマスク指定が可能です。
7	宛先 IPv6 アドレス	・ipv6、ipv6-dst-ip、ipv6-tcp/udp-range コンディションタイプのルールで使用可能です。 ・宛先 IPv6 アドレスを指定します。プレフィックス長によるマスク指定が可能です。
8	送信元 TCP/UDP ポート	・ipv6-tcp/udp-range コンディションタイプのルールで使用可能です。 ・オプションで TCP 指定もしくは UDP 指定が可能です。 ・オプションで TCP を指定したルールは宛先 TCP/UDP ポートも TCP 指定のみ設定可能です。オプション UDP 指定の場合も同様です。
9	宛先 TCP/UDP ポート	・ipv6-tcp/udp-range コンディションタイプのルールで使用可能です。 ・オプションで TCP 指定もしくは UDP 指定が可能です。 ・オプションで TCP を指定したルールは送信元 TCP/UDP ポートも TCP 指定のみ設定可能です。オプション UDP 指定の場合も同様です。

3.3 マスク指定

フィルター条件の多くはマスク指定が可能で、これによりフィルター条件を範囲指定することができます。マスク指定はマスクのビットが 0 か 1 かによって次のような動作になります。

マスクが 1 のビット ⇒ 元の値のビットは固定。
マスクが 0 のビット ⇒ 元の値のビットに関わらず、0 と 1 の両方を対象とする。

3.3.1 16 進設定値に対するマスク指定

以下に、宛先 MAC アドレス条件や Ethenet Type 条件など、16 進数で条件を設定する値に対して、マスク指定を使用した場合の例を示します。この例 1 と例 2 の設定内容は異なりますが、結果的に得られる動作は同じであることに注意して下さい。なお、基本的には例 1 のようにマスク指定するビットに関しては元の値も 0 になるように設定することを推奨します。

■ 例 1
・送信元 MAC アドレス条件に 00:11:22:33:00:00～00:11:22:33:ff:ff を指定したい場合(1)

```
<GROUP> <RULE> condition ethernet src mac 00:11:22:33:00:00 mask ff:ff:ff:ff:00:00

元の値   00:11:22:33:00:00 → 00000000-00010001-00100010-00110011-00000000-00000000
マスク   ff:ff:ff:ff:00:00 → 11111111-11111111-11111111-11111111-00000000-00000000
                                        ↓
         00:11:22:33:00:00 → 00000000-00010001-00100010-00110011-00000000-00000000)
         00:11:22:33:ff:ff → 00000000-00010001-00100010-00110011-11111111-11111111)
                                        ↓
結果     00:11:22:33:00:00～00:11:22:33:ff:ff を指定したことになります。
```

■ 例 2
・送信元 MAC アドレス条件に 00:11:22:33:00:00～00:11:22:33:ff:ff を指定したい場合(2)

```
<GROUP> <RULE> condition ethernet src mac 00:11:22:33:44:55 mask ff:ff:ff:ff:00:00

元の値   00:11:22:33:44:55 → 00000000-00010001-00100010-00110011-01000100-01010101
マスク   ff:ff:ff:ff:00:00 → 11111111-11111111-11111111-11111111-00000000-00000000
                                        ↓
         00:11:22:33:00:00 → 00000000-00010001-00100010-00110011-00000000-00000000)
         00:11:22:33:ff:ff → 00000000-00010001-00100010-00110011-11111111-11111111)
                                        ↓
結果     00:11:22:33:00:00～00:11:22:33:ff:ff を指定したことになります。
```

3.3.2 10 進設定値に対するマスク指定

以下に、VLAN ID 条件など、10 進数で条件を設定する値に対して、マスク指定を使用した場合の例を示します。マスクのビットが 0 か 1 かによるマスク指定の動作は変わりませんが、元の値が 10 進数のため、任意の範囲に対してマスク指定をする場合には、例 4 のように複数のルールに分けて設定する必要があることに注意して下さい。

■ 例 1
・VLAN ID 条件に VLAN ID：10 のみを指定したい場合

```
<GROUP> <RULE> condition dst vid 10 mask 0xfff

元の値      10 → 0000-0000-1010
マスク  0xfff → 1111-1111-1111
                          ↓
            10 → 0000-0000-1010
                          ↓
結果     10 のみを指定したことになります。マスク未指定時の動作に該当します。
```

■ 例 2
・VLAN ID 条件に VLAN ID：8～11 を指定したい場合

```
<GROUP> <RULE> condition dst vid 10 mask 0xffc

元の値      10 → 0000-0000-1010
マスク  0xffc → 1111-1111-1100
                          ↓
             8 → 0000-0000-1000
             9 → 0000-0000-1001
            10 → 0000-0000-1010
            11 → 0000-0000-1011
                          ↓
結果     8～11 を指定したことになります。
```

■ 例 3
・VLAN ID 条件に全ての VLAN(VLAN ID：1～4094)を指定したい場合
※ マスクに 0x0 を設定した場合は、フィルター条件設定値に関わらず、
全ての範囲を指定したことになります。

```
<GROUP> <RULE> condition dst vid 10 mask 0x0
```

元の値　　10 → 0000-0000-1010
マスク　0xfff → 0000-0000-0000
　　↓
　　0 → 0000-0000-0000
　　4094 → 1111-1111-1111
　　↓
結果　　全ての VLAN(VLAN ID：1～4094)を指定したことになります。

■ 例 4
・VLAN ID 条件に VLAN ID：100～200 を指定したい場合
　※ 例 2 のような任意の範囲を単一ルールで指定できるパターンは限られます。
　　任意の範囲を指定する場合は、指定したい範囲のフィルター条件設定値を 2 進数に置き換え、
　　必要となる設定値とマスクの指定範囲を考慮した上で、複数のルールに分けて設定します。

<GROUP> <RULE1> condition dst vid 100 mask 0xffc
<GROUP> <RULE2> condition dst vid 104 mask 0xff8
<GROUP> <RULE3> condition dst vid 112 mask 0xff0
<GROUP> <RULE4> condition dst vid 128 mask 0xfc0
<GROUP> <RULE5> condition dst vid 192 mask 0xff8
<GROUP> <RULE6> condition dst vid 200 mask 0xfff

元の値　　100 → 0000-0110-0100
マスク　0xffc → 1111-1111-1100
　　↓
　　100 → 0000-0110-0100
　　103 → 0000-0110-0111
　　↓
<RULE1>では 100～103 を指定したことになります。

元の値　　104 → 0000-0110-1000
マスク　0xffc → 1111-1111-1000
　　↓
　　104 → 0000-0110-1000
　　111 → 0000-0110-1111
　　↓
<RULE2>では 104～111 を指定したことになります。

元の値　　112 → 0000-0111-0000

マスク　0xff0 → 1111-1111-0000
↓
112 → 0000-0111-0000
127 → 0000-0111-1111
↓
<RULE3>では 112～127 を指定したことになります。

元の値　　128 → 0000-1000-0000
マスク　0xfc0 → 1111-1100-0000
↓
128 → 0000-1000-0000
191 → 0000-1011-1111
↓
<RULE4>では 128～191 を指定したことになります。

元の値　　192 → 0000-1100-0000
マスク　0xff8 → 1111-1111-1000
↓
192 → 0000-1100-0000
199 → 0000-1100-0111
↓
<RULE5>では 192～199 を指定したことになります。

元の値　　200 → 0000-1100-1000
マスク　0xfff → 1111-1111-1111
↓
200 → 0000-1100-1000
↓
<RULE6>では 200 を指定したことになります。

結果　　同一グループ内において、100～200 を指定したことになります。

4. アクション(動作)

アクションは識別条件・フィルター条件に一致した受信トラフィックに対してどのような動作を行わせるのかを定義します。同一ルールに複数種類のアクションを設定することは可能ですが、組み合わせによっては併用設定できないアクションもあることに注意して下さい。同一ルールに複数種類のアクションを設定した場合の注意に関しては「6 同一ルールに複数アクション設定時の動作」を参照して下さい。また、複数のグループにマッチした場合の注意に関しては「7 複数グループにマッチした場合の動作」を参照して下さい。

4.1 permitアクション

【permit】を設定した場合には、「対象となる受信トラフィックの中継を許可する」という動作になります。【permit】はルールのデフォルトアクションのため、新規にルールを作成した場合には自動的に設定されます。

【deny】、【none】、【authentication-bypass】以外のアクションを設定した場合、必ず【permit】が設定されます。【deny】、【none】、【authentication-bypass】を設定した場合は【permit】は自動的に削除されますが、【deny】、【none】、【authentication-bypass】を削除すると再度【permit】が設定されます。

4.2 denyアクション

【deny】を設定した場合には、「対象となる受信トラフィックを破棄する」という動作になります。【deny】はフィルタリング目的で使用する場合に有効で、設定例に関しては「18.受信時のフィルタリング機能」を参照して下さい。なお、ある一つのルールにおいて【deny】は【permit】【none】【authentication-bypass】以外のアクションと併用して設定可能ですが、最終的に得られる動作は「破棄」になることに注意して下さい。ただし、【counter】【mirror】だけは例外で「破棄」「カウンター」「ミラーリング」は全て同時に動作します。

4.3 noneアクション

【none】を設定した場合には、「対象となる受信トラフィックに何もしない」という動作になります。【none】により同一グループ、別ルールのフィルター条件から【none】で指定したフィルター条件を除外することが可能です。別グループのフィルター条件からは除外されません。CPU フィルター機能の指定グループでactionコマンドや、assign、conditionコマンドを使用してルールを新規に作成するとき、【none】が自動的に設定されます。

none アクションを使用する場合、同一ルールに他のアクションを設定しないでください。

除外するフィルター条件は、他のルール番号よりも若番ルールを設定してください。

■ 例 1

```
1 1 action none
1 1 condition src mac 00:40:66:33:ae:e8
1 1 assign port 1
1 2 action deny
1 2 condition src vid 1
1 2 assign port 1
```

この場合、port 1 が受信した VID=1 のフレームは破棄されますが(1 2 action deny が動作)、送信元 MAC アドレスが 00:40:66:33:ae:e8 のフレームは破棄されません(1 1 action none が動作)。

1 2 を action counter にすれば、特定端末をカウンター条件から外す。
1 2 を action authentication-bypass にすれば、特定端末を認証バイパスから外す。
1 2 を action block-cpu-control にすれば、特定端末を CPU 宛フィルターから外す。
のような運用が可能です。

■ 例 2

```
1 1 action none
1 1 condition src mac 00:40:66:33:ae:e8
1 1 assign port 1
1 2 action deny
1 2 condition src vid 1
1 2 assign port 1

access-defender
packet-filter2 group 6
packet-filter2 max-rule 100
mac-authentication port 1
mac-authentication enable
```

この場合、送信元 MAC アドレスが 00:40:66:33:ae:e8 のフレームは AccessDefender 機能による認証成功後は中継し、認証に失敗した場合は AccessDefender 機能によりフレームを破棄します。
送信元 MAC アドレスが 00:40:66:33:ae:e8 以外の VID=1 のフレームは破棄されます(1 2 action deny が動作)。

【permit】と【none】の違いを以下に示します。

【permit】の場合

```
1 1 action permit
1 1 condition src mac 00:40:66:33:ae:e8
1 1 assign port 1/1
2 1 action authentication-bypass
2 1 condition src vid 1
2 1 assign port 1/1
```

端末 00:40:66:33:ae:e8 には認証バイパスは適用されません(1 1 action permit が有効)。

【none】の場合

```
1 1 action none
1 1 condition src mac 00:40:66:33:ae:e8
1 1 assign port 1/1
2 1 action authentication-bypass
2 1 condition src vid 1
2 1 assign port 1/1
```

端末 00:40:66:33:ae:e8 には認証バイパスが適用されます(グループ番号が異なるため、2 1 action authentication-bypass が有効)。

4.4 authentication-bypassアクション

【authentication-bypass】は、「AccessDefender 機能の認証ポートにおいて認証を行わずに通信を許可する認証バイパス機能」のために使用される専用のアクションです。詳細に関しては AccessDefender 機能のアプリケーションノートを参照して下さい。

authentication-bypass アクションを使用する場合には、AccessDefender 機能が占有するグループ番号よりも若番のグループで設定する必要があります。詳細に関しては AccessDefender 機能のアプリケーションノートを参照して下さい。

4.5 block-cpu-controlアクション

【block-cpu-control】を設定した場合、「対象となる CPU 宛フレームを CPU へ転送しない」という動作になります。CPU へ転送され、かつ、他ポートへも転送されるフレームは CPU 宛のみフィルタリングされます。

【block-cpu-control】を設定するには 2 つのグループが必要です。設定例は「24.受信時のCPU宛フィルター機能」を参照して下さい。

4.6 qosアクション

【qos】を設定した場合には、「対象となる受信トラフィックのQoSプロファイル(qp1-qp8)へのマッピングルールを変更」という動作になります。設定例に関しては「19.受信時のQPマッピング機能」「21 受信時のQPマッピング＋送信フレームの 802.1p優先度変更機能」を参照して下さい。なお、ある一つのルールにおいて【qos】は【priority】と併用設定できないことに注意して下さい。

「受信トラフィックの QoS プロファイル(qp1-qp8)へのマッピングルール」はデフォルトでは下記のように動作しますが、パケットフィルター2 の【qos】を使用することにより特定のトラフィック種類に対してマッピングルールを変更するといったことが可能になります。なお、“ qos qosprofile <qp1-qp8> mapping <802.1p> ”よりもパケットフィルター2 の【qos】の方が優先されることに注意して下さい。

■ 受信トラフィックの QoS プロファイル(qp1-qp8)へのデフォルトマッピングルール
・Untag フレームと認識した場合には qp3 にマッピングされる。
・Tag フレームと認識した場合には、“ qos qosprofile <qp1-qp8> mapping <802.1p> ”の設定に従って 802.1p 優先度(0-7)から QoS プロファイル(qp1-qp8)にマッピングされる。

4.7 priorityアクション

【priority】を設定した場合には、「対象となる受信トラフィックを別のトランクポートからTagフレームとして送信する際に 802.1p優先度の値を書き換える」という動作になります。値を指定して設定した場合には指定した 802.1p優先度(0-7)に書き換えますが、【from ip-tos-precedence】オプションを指定して設定した場合にはIP Precedence値(0-7)と同じ値に 802.1p優先度を書き換えます。設定例に関しては「20.送信フレームの 802.1p優先度変更機能」「21 受信時のQPマッピング＋送信フレームの 802.1p優先度変更機能」を参照して下さい。なお、ある一つのルールにおいて【priority】は【qos】と併用設定できないことに注意して下さい。

「装置が送信する Tag フレームの 802.1p 優先度」はデフォルトでは下記のように動作しますが、パケットフィルター2 の【priority】を使用することにより特定のトラフィック種類に対して 802.1p 優先度を変更するといったことが可能になります。

■ 送信 Tag フレームの 802.1p 優先度のデフォルトルール
・受信時に Untag フレームと認識した場合には、802.1p 優先度は 0 で送信される。
・受信時に Tag フレームと認識した場合には、元の 802.1p 優先度を変更することなくそのままの値で送信される。
・“ ignore-tag enable ”を設定した装置のアクセスポートで Tag フレームを受信して、別のトランクポートから Tag フレームとして送信する場合(つまり、ダブル Tag フレームとして送信する場合)には、新たに付加される一番外側の Tag の 802.1p 優先度は 0 で送信される。

4.8 ip-tos-dscpアクション

【ip-tos-dscp】を設定した場合には、「対象となる受信トラフィックを別のポートから送信する際に

IPv4 ヘッダーのDSCP値を書き換える」という動作になります。設定例に関しては「22.送信パケットのDSCP値/IP Precedence値変更機能」を参照して下さい。なお、ある一つのルールにおいて【ip-tos-dscp】は【ip-tos-precedence】と併用設定できないことに注意して下さい。

装置はデフォルトでは DSCP 値を変更せずに中継しますが、パケットフィルター2 の【ip-tos-dscp】を使用することにより変更することが可能になります。

ip-tos-dscp アクションを適用する対象が IPv6 パケットの場合には、Traffic Class フィールドの先頭 6bit に反映されます。

4.9 ip-tos-precedenceアクション

【ip-tos-precedence】を設定した場合には、「対象となる受信トラフィックを別のポートから送信する際にIPv4 ヘッダーのIP Precedence値を書き換える」という動作になります。設定例に関しては「22.送信パケットのDSCP値/IP Precedence値変更機能」を参照して下さい。なお、ある一つのルールにおいて【ip-tos-precedence】は【ip-tos-dscp】と併用設定できないことに注意して下さい。

装置はデフォルトでは IP Precedence 値を変更せずに中継しますが、パケットフィルター2 の【ip-tos-precedence】を使用することにより変更することが可能になります。

ip-tos-precedence アクションを適用する対象が IPv6 パケットの場合には、Traffic Class フィールドの先頭 3bit に反映されます。

4.10 policingアクション

【policing】を設定した場合には、「対象となる受信トラフィックを帯域制限エントリーによって 2 段階に分類する」という動作になります。別途「4.14 exceed-action denyアクション」を設定することにより、受信時の帯域制限機能として使用することが可能です。設定例に関しては「23.受信時の帯域制限機能」を参照して下さい。また、帯域制限エントリーに関しては「8 帯域制限エントリー」を参照して下さい。

【policing】の設定は二通りの方法で設定可能ですが、装置全体でどちらか一方の方法でしか設定できないことに注意して下さい。それぞれの設定方法の特徴について 表 4-1 に示します。

表 4-1 policing アクションの設定方法

No.	設定方法	概要
1	帯域制限エントリーを自動的に割り当てる方法	・使用するコマンドは下記。 <GROUP> <RULE> action policing cir <RATE> <GROUP> <RULE> action policing cbs <BURSTSIZE> ・この設定方法の場合には、1 個の帯域制限エントリーを 1 個のルールで占有して使用します。帯域制限エントリーはまだ未使用なエントリーが内部で自動的に割り当てられます。

No.	設定方法	概要
		・この設定方法の場合には、“ show packet-filter2 ”等で設定した CIR/CBS を確認することができますが、“ show packet-filter2 policing ”は使用できなくなることに注意して下さい。
2	帯域制限エントリーを明示的に割り当てる方法	・使用するコマンドは下記。 <GROUP> <RULE> action policing group <INDEX> <GROUP> policing <INDEX> cir <RATE> <GROUP> policing <INDEX> cbs <BURSTSIZE> ・この設定方法の場合には、1 個の帯域制限エントリーを 1 個のルールで占有して使用することも、1 個の帯域制限エントリーを複数のルールで共有して使用することも可能です。帯域制限エントリーの<INDEX>はユーザーが指定して設定します。 ・この設定方法の場合には、“ show packet-filter2 policing ”で設定した CIR/CBS を確認することができますが、“ show packet-filter2 ”等では指定した帯域制限エントリーの<INDEX>が表示されることに注意して下さい。

4.11 redirectアクション

【redirect】を設定した場合には、「対象となる受信トラフィックを本来中継する宛先ポートではなく指定したポートに強制的に中継(リダイレクト)する」という動作になります。この際、本来中継すべき宛先ポートには中継されなくなることに注意して下さい。ある一つのルールにおいて指定可能なリダイレクト先ポートは 1 ポートです。

【redirect】は設定を間違えると正常な通信へ悪影響を及ぼすことも考えられるため、設定する場合には十分に検討した上で使用して下さい。表 4-2 に【redirect】に関する注意点を示します。

表 4-2 redirect アクションの注意点

No.	対象	注意点
1	共通	・redirect アクションが適用されたトラフィックは本来中継すべき宛先ポートには中継されなくなります。 ・リダイレクト先のポートが「対象となるトラフィックを受信したポート」の場合でもリダイレクトされます。
2	対象が「その装置で L2 中継するトラフィック」	・リダイレクト先のポートには「対象となるトラフィックを受信した VLAN」と同じ VLAN が割り当てられている必要があります。 ・対象となるトラフィックがブロードキャスト/マルチキャスト/Unknown ユニキャストのようなフラッディングフレームの場合でもリダイレクトされ、本来中継すべき宛先ポート(同じ VLAN の受信ポート以外の全ポート)にはフラッディングされなくなることに注意して下さい。
3	対象が「その装置で Routing 中継す	・リダイレクト先のポートには「対象となるトラフィックが本来 Routing 中継された後の VLAN」が割り当てられている必要があります。

No.	対象	注意点
	るトラフィック」	・リダイレクトされた後のパケットは Routing 処理(宛先/送信元 MAC アドレスの付け替えや TTL の減算処理等)が行われた後のパケットになっていることに注意して下さい。 ・対象となるトラフィックが本来 Routing 中継される際の宛先 ARP エントリー(Route Cache)が未登録な場合にはリダイレクトされません。

リダイレクト先のポートが「対象となるトラフィックを受信したポート」であり、かつ対象にフラッディングフレームが含まれるような条件で使用する場合には十分に注意して下さい。そのように設定した装置を同じ VLAN に 2 台以上接続してしまうとトラフィックの増幅事象が発生し正常な通信への悪影響が考えられます。

4.12 counterアクション

【counter】を設定した場合には、「対象となる受信トラフィックをカウンターで計測する」という動作になります。デフォルトでは受信パケット数での計測になりますが、【unit byte】オプションを指定して設定した場合には受信バイト数での計測になります。カウンターに関しては「9 カウンター」を参照して下さい。なお、ある一つのルールにおいて【counter】は他の全てのアクションと併用して設定可能です。

4.13 mirrorアクション

【mirror】を設定した場合には、「対象となる受信トラフィックをミラーリングする」という動作になります。ミラーリングされた後のトラフィック形式はミラーリング先ポートのポート種別や VLAN 設定には関係しません。受信トラフィックを装置が Untag フレームと認識した場合にはその Untag フレーム形式のままミラーリングされ、受信トラフィックを Tag フレームと認識した場合にはその Tag フレーム形式のままミラーリングされます。ある一つのルールにおいて指定可能なミラーリング先ポートは 1 ポートですが、装置全体では最大 2 ポートまでミラーリング先ポートを指定可能です。

ある一つのルールにおいて【mirror】は【none】【block-cpu-control】を除く、他の全てのアクションと併用して設定可能です。ミラーリングされた後のトラフィックは基本的には他のアクションが適用される前のトラフィック形式のままミラーリングされますが、【qos】だけは【mirror】よりも先に適用されることに注意して下さい。

mirror アクションは、対象となる受信トラフィックを指定ポートにミラーリングしてフレームを解析するための機能です。従って、ミラーリング先に設定したポートでは他機能を動作させず、アナライザー等のネットワーク解析装置以外は接続しないでください。

4.14 exceed-action denyアクション

exceeded-actionは帯域制限エントリーを使用するルールにおいて、CIR(Committed Information Rate)を超えた受信トラフィックに対しての動作を設定するアクションです。設定可能なアクションとしては【deny】のみが適用可能で、これを設定することにより受信時の帯域制限機能として使用することが可能です。帯域制限機能の設定例に関しては「23.受信時の帯域制限機能」を参照して下さい。

5. CPU宛フィルター機能

CPU 宛フィルター機能はフィルター条件に合致した CPU 宛フレームを【block-cpu-control】アクションでフィルタリングする機能です。CPU 宛フィルター機能はパケットフィルター2 のグループを 2 個使用します。"block-cpu-control <GROUP> <GROUP> enable"コマンドにて CPU 宛フィルター機能で使用するグループ(CPU 宛フィルターグループと呼びます)を指定してください。CPU 宛フィルターグループへのパケットフィルター2 関連の設定/削除は、自動的にもう一方の指定グループへ設定/削除されます。

指定グループで使用可能なアクションは【none】、【block-cpu-control】、【counter】です。

■ グループ 1、2 を CPU 宛フィルターグループに指定

```
block-cpu-control 1 2 enable
```

パケットフィルター2 のグループ 1、2 を CPU 宛フィルターグループに指定します。CPU 宛フィルターグループは"show packet-filter2 reserved-group"で Packet-filter2 (block-cpu-control with X) と表示されます。

■ "show packet-filter2 reserved-group"の表示結果

```
# show packet-filter2 reserved-group
 Group   Function
--------------------------------------------------------------------------------
     1   Packet-filter2 (block-cpu-control with 2)
     2   Packet-filter2 (block-cpu-control with 1)
   (中略)
```

CPU 宛フィルター機能はアクション設定前に必ずフィルター条件(コンディション)を設定してください。フィルター条件が設定されていない場合、CPU 宛ての全パケットがフィルターされます。

"no ip icmp redirect send disable"コマンド設定時の ICMP リダイレクト対象パケットはフィルターできません。

sFlow 有効時は sFlow パケットをフィルターできません。

Apresia3448 シリーズにおいて、以下の組み合わせ(*1 または*2)でアクション block-cpu-control を設定した場合、パケット数を 2 倍にカウントする可能性があるため、アクション counter を使用できません。
(*1)ポート 1-24、49-50 のいずれかを assign port で指定
ポート 25-48、51-52 のいずれかを assign port で指定
(*2)ポート 1-24、49-50 のいずれかの所属 vlan を assign vlan で指定

ポート 25-48、51-52 のいずれかの所属 vlan を assign vlan で指定

6. 同一ルールに複数アクション設定時の動作

アクションは同一ルールに複数設定することが可能です(”action none ” の場合を除く)。CPU 宛フィルター機能を使用するグループと、それ以外のグループ(通常グループ)で設定可能アクションが異なります。

6.1 通常グループ

図 6-1 に通常グループの同一ルールに複数アクションを設定した場合の動作を示します。

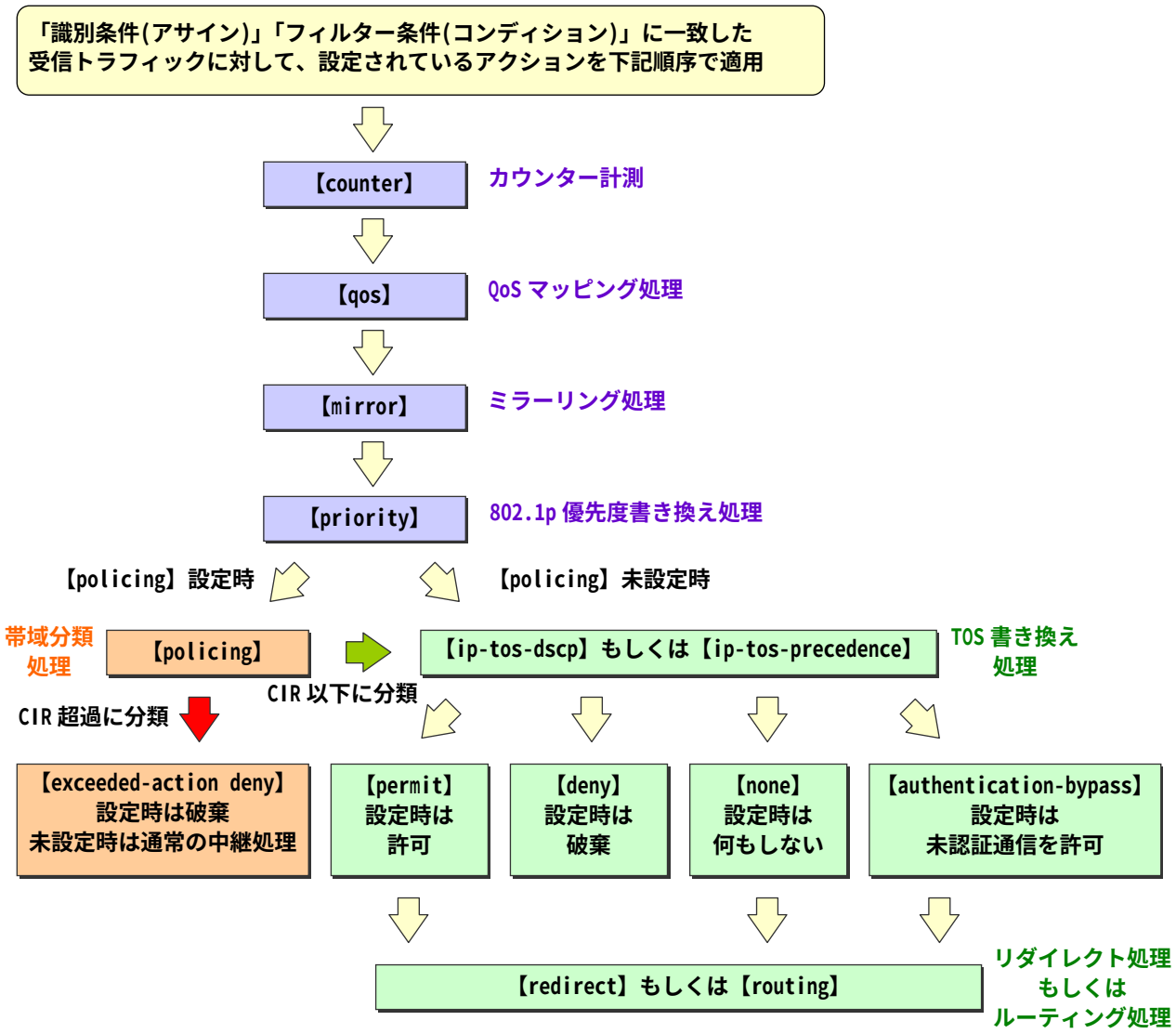

図 6-1 同一ルールに複数アクション設定時の動作図(通常グループ)

表 6-1 に同一ルールに複数アクション設定時の注意点を示します。

表 6-1 同一ルールに複数アクション設定時の注意点

No.	action	注意点
1	permit	・【deny】【none】【authentication-bypass】と併用設定は不可 ・【policing】併用設定時には、CIR 以内に分類されたトラフィックが対象
2	deny	・【permit】【none】と併用設定は不可 ・【authentication-bypass】との併用設定は未サポート ・【policing】併用設定時には、CIR 以内に分類されたトラフィックが対象
3	none	・【block-cpu-control】【counter】以外の、他のアクションとの併用は未サポート
4	block-cpu-control	・【none】【counter】を除く、他のアクションとの併用設定は不可
5	authentication-bypass	・【permit】と併用設定は不可 ・【deny】【none】との併用設定は未サポート ・基本的には「AccessDefender 機能の認証ポートにおいて認証を行わずに通信を許可する認証バイパス機能」のために使用される専用のアクション
6	qos	・【priority】と併用設定は不可 ・【policing】併用設定時でも、【policing】適用前の全てのトラフィックに対して【qos】が適用
7	priority	・【qos】と併用設定不可 ・【policing】併用設定時でも、【policing】適用前の全てのトラフィックに対して【priority】が適用 ・【from ip-tos-precedence】オプションを指定して設定した場合でかつ【ip-tos-precedence】併用設定時には、【ip-tos-precedence】適用前の IP Precedence 値で【priority from ip-tos-precedence】が適用
8	ip-tos-dscp	・【ip-tos-precedence】と併用設定は不可 ・【policing】併用設定時には、CIR 以内に分類されたトラフィックが対象
9	ip-tos-precedence	・【ip-tos-dscp】と併用設定は不可 ・【policing】併用設定時には、CIR 以内に分類されたトラフィックが対象
10	policing	・【none】【block-cpu-control】を除く、他の全てのアクションと併用設定が可能 ・【counter】【qos】【mirror】【priority】は【policing】適用前のトラフィックに対して適用 ・【ip-tos-dscp】【ip-tos-precedence】【permit】【deny】【redirect】は【policing】適用後の CIR 以下に分類されたトラフィックに対して適用 ・【exceeded-action deny】は【policing】適用後の CIR 超過に分類されたトラフィックに対して適用
11	redirect	・【none】【block-cpu-control】を除く、他の全てのアクションと併用設定が可能 ・他の全てのアクション適用後のトラフィックがリダイレクト ・ただし【deny】併用設定時にはリダイレクト不可
12	counter	・他の全てのアクションと併用設定が可能

No.	action	注意点
13	mirror	・【none】【block-cpu-control】を除く、他の全てのアクションと併用設定が可能 ・【qos】を除く、他の全てのアクション適用前のトラフィックがミラーリング

6.2 CPU宛フィルターグループ

図 6-2 にCPU宛フィルターグループの同一ルールに複数アクションを設定した場合の動作を示します。

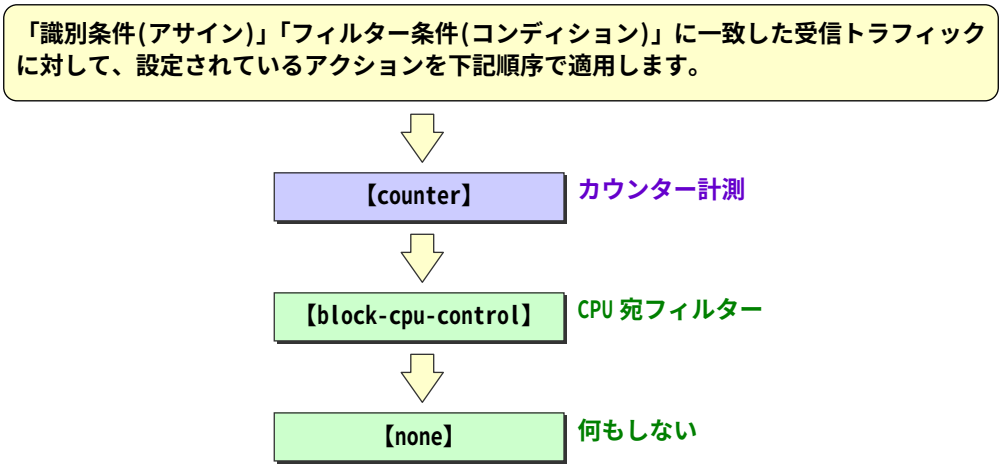

図 6-2 同一ルールに複数アクション設定時の動作図(CPU 宛フィルターグループ)

7. 複数グループにマッチした場合の動作

例えばグループ 1 のルール 1 では「送信元 MAC アドレスが 00:00:00:00:00:A1」の受信フレームを対象にするように設定し、グループ 2 のルール 1 では「送信元 IP アドレスが 10.1.1.0/24」の受信パケットを対象にするように設定した場合を想定します。この際に、「送信元 MAC アドレスが 00:00:00:00:00:A1 で送信元 IP アドレスが 10.1.1.0/24 の IPv4 パケット」を受信した場合には、この受信パケットは両方のグループにマッチすることになります。

このような場合には複数のアクションが候補になることが考えられますが、基本的には競合しないアクションであれば「6 同一ルールに複数アクション設定時の動作」と同様に全てのアクションが適用されますが、競合するアクションの場合には注意が必要です。また競合しないアクションでも例外があることに注意して下さい。複数のグループにマッチした場合に最終的にどのアクションが適用されるかについて 表 7-1 に示します。

表 7-1 複数のグループにマッチした場合のアクション概要

No.	action	概要
1	deny とその他のアクション	・【deny】が若番グループの場合、「破棄」の動作。老番グループに設定された【block-cpu-control】【mirror】【counter】も動作しますが、それ以外のアクションは動作しません。 ・【deny】が老番グループの場合、若番グループに設定されたアクションが動作。「破棄」の動作は適用されません。若番グループのアクションが【none】【block-cpu-control】の場合、「破棄」の動作も適用されます。
2	同一アクションが複数	・基本的には若番グループのアクションが適用され、老番グループのアクションは適用されません。例えば、若番グループが【priority 3】で老番グループが【priority 7】の場合は、若番グループの【priority 3】が適用されます。 ・【none】【block-cpu-control】【counter】は若番/老番グループ両方が動作します。
3	policing とその他のアクション	・【policing】が若番グループの場合には【policing】もその他のアクションも動作します。 ・【policing】が老番グループの場合には【policing】は動作しません。【none】の場合、【policing】も適用されます。
4	ip-tos-dscp と ip-tos-precedence	・若番/老番グループに関係なく、常に【ip-tos-dscp】が適用されます。【ip-tos-precedence】は動作しません。
5	それ以外の競合しないアクションの組み合わせ	・全てのアクションが動作します。 ・アクションの適用順序に関しては 図 6-1 を参照してください。

8. 帯域制限エントリー

帯域制限エントリーはトラフィック計測分類機能です。帯域制限エントリーは必ず設定しなければならない要素ではなくオプション的に使用するものであり、トラフィックを帯域に基づいて分類したい場合に使用します。帯域制限エントリーはグループ毎に複数用意されていますが、装置種別によりその上限が異なることに注意して下さい(表 2-2 参照)。なお、1 個の帯域制限エントリーを複数のルールで共有して使用することもでき、例えば複数のルールに一致した受信トラフィックの総和をある帯域に制限するといったことも可能です。

帯域制限エントリーを使用した場合には、識別条件・フィルター条件に一致した受信トラフィックは 2 段階に分類されます。設定したCIR(Committed Information Rate)を超過しない受信トラフィックに対しては「4 アクション(動作)」の一部のアクションを除いたアクションが適用されます。CIRを超過した受信トラフィックに対しては「4.14 exceed-action denyアクション」が適用されます。このexceeded-actionとしてはdenyアクションのみが適用可能で、これを設定することにより受信時の帯域制限機能として使用することが可能になります。

帯域制限エントリーはフレームの DA(宛先 MAC アドレス)～FCS(Frame Check Sequence)までのサイズを対象として計測します。これには Preamble/SFD(Start Frame Delimiter)と IFG(Inter Frame Gap)は含まれていないことに注意して下さい。また、受信トラフィックを Tag フレームとして認識した場合には、Tag(4byte)もサイズに含むことに注意して下さい。

Apresia13000-48X では帯域制限エントリーは二つのポートブロック(port 1-24, 50 と port 25-48, 49)毎に独立して適用されます。そのため、対象となる受信トラフィックが両方のポートブロックに跨っている場合には、計測する CIR が設定値の最大 2 倍まで上回ることがあります。Apresia13000-48X で帯域制限エントリーを使用する場合には、対象となる受信トラフィックが二つのポートブロックを跨がないようにしてご使用下さい。

9. カウンター

カウンターは定義した条件に一致した受信パケット数もしくは受信バイト数を計測する統計情報機能です。カウンターは必ず設定しなければならない要素ではなくオプション的に使用するものです。カウンターはグループ毎に複数用意されていますが、装置種別によりその上限が異なることに注意して下さい(表 2-2 参照)。なお、1 個のカウンターを複数のルールで共有して使用することもできますが、その際には「パケット数でカウントする」もしくは「バイト数でカウントする」という使い方が一致している必要があります。

カウンターはフレームの DA(宛先 MAC アドレス)～FCS(Frame Check Sequence)までのサイズを対象として計測します。これには Preamble/SFD(Start Frame Delimiter)と IFG(Inter Frame Gap)は含まれていないことに注意して下さい。また、受信トラフィックを Tag フレームとして認識した場合には Tag(4byte)もサイズに含むことに注意して下さい。

10. TCP/UDPポート番号範囲指定エントリー

TCP/UDP ポート番号範囲指定エントリーは TCP/UDP ポート番号を連続範囲指定でチェックできるようにする機能要素です。ipv4-src-tcp/udp-range、ipv4-dst-tcp/udp-range、ipv6-tcp/udp-range コンディションタイプのルールを定義した際に自動的に設定されます。装置全体で 16 個使用可能で、一つのエントリーは「送信元 or 宛先」と「TCP/UDP ポート番号の連続範囲」の二つの要素で構成されます。ipv6-tcp/udp-range コンディションタイプのルールでは、単一の「TCP/UDP ポート番号」指定時においても、エントリーを一つ消費します。なお、同じパターンのエントリーを複数のルールで共有して使用することが可能です。

以下にフィルター条件と自動的に設定される TCP/UDP ポート番号範囲指定エントリーの例を示します。

■ 例 1

```
1 10 condition ipv4 src tcp/udp 49152-50000
1 20 condition ipv4 src tcp/udp 49152-60000
```

この場合には「送信元ポート番号」であることは同じですが指定しているポート番号範囲が異なるため、それぞれの TCP/UDP ポート番号範囲指定エントリーが自動的に設定されます。つまり 2 個のエントリーを消費します。

■ “show packet-filter2 tcp/udp-range”の表示結果

```
 range-id   src/dst       port-range
------------------------------------------------------------------------------
        1       src   49152 to 50000
        2       src   49152 to 60000
```

■ 例 2

```
1 10 condition ipv4 src tcp/udp 1-1023
2 10 condition ipv4 dst tcp/udp 1-1023
```

この場合にはポート番号範囲は同じですが「送信元ポート番号」と「宛先ポート番号」を対象にしていることが異なるため、それぞれの TCP/UDP ポート番号範囲指定エントリーが自動的に設定されます。つまり 2 個のエントリーを消費します。

■ “show packet-filter2 tcp/udp-range”の表示結果

```
 range-id   src/dst       port-range
------------------------------------------------------------------------------
        1       src       1 to   1023
        2       dst       1 to   1023
```

■ 例 3

```
1 10 condition ipv4 dst tcp/udp 10000-10010
1 20 condition ipv4 dst tcp/udp 10000-10010
```

この場合にはパターンが同じ条件のため、自動的に設定される TCP/UDP ポート番号範囲指定エントリーは 1 個です。

■ “ show packet-filter2 tcp/udp-range ”の表示結果

```
 range-id  src/dst      port-range
-------------------------------------------------------------------------------
        1      dst  10000 to 10010
```

■ 例 4

```
1 10 condition ipv4 dst tcp/udp 10000-10010 tcp
1 20 condition ipv4 dst tcp/udp 10000-10010 udp
```

オプション TCP/UDP 指定が異なる場合でも、「送信元 or 宛先」と「TCP/UDP ポート番号の連続範囲」の二つの要素が同じパターンであれば、自動的に設定される TCP/UDP ポート番号範囲指定エントリーは 1 個です。

■ “ show packet-filter2 tcp/udp-range ”の表示結果

```
 range-id  src/dst      port-range
-------------------------------------------------------------------------------
        1      dst  10000 to 10010
```

11. ワイドモード

ワイドモードは同一ルール内のフィルター条件(コンディション)に宛先 IPv6 アドレス、送信元 IPv6 アドレス、宛先 TCP/UDP ポート、送信元 TCP/UDP ポートを複数設定可能とします。これらのフィルター条件は、コンディションタイプが異なっていてもワイドモードにより同一ルール内に設定可能となります。ワイドモードはグループを連番で 2 つ使用します。

■ ワイドモードの設定

```
wide-mode <GROUP>
        GROUP ····· グループ番号
                    Apresia3400/4348/5400/13000 シリーズ：<奇数グループ>
                    Apresia4328 シリーズ：<偶数グループ>
```

■ 設定例

```
(config-filter)# wide-mode 1
(config-filter)# 1 1 condition ipv6 dst ip 3ffe:506::1/128
(config-filter)# 1 1 condition ipv6 dst tcp/udp 21
```

ワイドモードを指定することにより、コンディションタイプが異なるフィルター条件(ipv6-dst-ip と ipv6-tcp/udp-range)を同一ルールに設定可能です。

12. パケットフィルター2 のリソースを自動的に占有する機能

設定を行うとパケットフィルター2 のリソースを自動的に占有する機能がいくつかあります。他の機能によって占有されたグループはパケットフィルター2 としてユーザーが使用できなくなることに注意して下さい。どのグループがどの機能によって占有されているかは“ show packet-filter2 reserved-group ”によって確認可能です。ユーザーがパケットフィルター2 として設定したグループは「Packet-filter2」と表示されます。

以降では、どのような機能がどれだけパケットフィルター2 のリソースを占有するかについて説明します。各機能の詳細に関してはコマンドリファレンスや各アプリケーションノートを参照して下さい。

12.1 IPアドレス機能

VLAN インターフェース/Loopback インターフェースに設定する IP アドレスの総数が少ない場合には占有されませんが、多くの IP アドレスを設定する場合には占有が発生します。IP アドレス機能が占有した場合には“ show packet-filter2 reserved-group ”に「Netif」と表示されます。

IP アドレス機能が占有するグループ番号をユーザーが指定することはできません。また、占有する場合には自動的にグループ 1 番から順番に占有されます。もしも他の機能によってグループ 1 番が既に使用されている場合には、多くの IP アドレスの設定ができないことに注意して下さい。

どのぐらいの数のIPアドレスを設定した場合に占有が発生するかは下記の計算によって算出できます。装置種別と算出値を元に 表 12-1 を参照して占有するグループ番号が判断可能です。

算出値 ＝ (VLAN インターフェースの Primary IP アドレス設定の数×3)
＋(VLAN インターフェースの Secondary IP アドレス設定の数)
＋(Loopback インターフェースに設定した IP アドレスの数)

表 12-1 占有するグループ番号と算出値の関係

占有するグループ番号	算出値				
	Apresia3400 /5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
1 番	252-379	129-256	257-384	508-763	257-384
1～2 番	380-507	257-384	385-512	764-1019	385-512
1～3 番	508-635	385-512	513-640	1020-1275	513-640
1～4 番	636-763	513-640	641-768	1276-1531[1]	641-768
1～5 番	764-891[1]	641-768	769-896[1]	—[1]	769-896
1～6 番	—[1]	769-896[1]	—[1]	—[1]	897-1024
1～7 番	—[1]	—[1]	—[1]	—[1]	1025-1152
1～8 番	—[1]	×[2]	—[1]	—[1]	1153-1280
1～9 番	—[1]	×[2]	—[1]	—[1]	1281-1408[1]

1) これより多くの算出値になるような IP アドレスを設定して更に多くのグループを占有することも可

能ですが、仕様としてこれ以上占有するような IP アドレス設定を推奨しません。
2) Apresia4328GTの最大グループ数は 7 個です。表 2-1 参照。

参考までに、例えば「Loopbackインターフェースに IPアドレスを 1 個と各VLANインターフェースに Primary IPアドレスを 1 個設定する」という条件の場合に、IPアドレス機能による占有が発生しない最大VLAN数を 表 12-2 に示します。

表 12-2 占有しない範囲で IP アドレスを設定可能な最大 VLAN 数の例

上段：VLAN 数　下段：(算出値)				
Apresia3400/5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24 GX-PSR	Apresia13000-48X
83VLAN (250)	42VLAN (127)	85VLAN (256)	168VLAN (505)	85VLAN (256)

* Loopback インターフェースには 1 個の IP アドレスを設定し、各 VLAN インターフェースには 1 個の Primary IP アドレスを設定するという条件の場合。

表 12-3 にあらためてIPアドレス機能が占有するグループ数に関してまとめます。このパケットフィルター2 のリソースとしての仕様上限以外にも、下記のようなIPアドレス機能としての仕様上限があることに注意して下さい。IPアドレス機能を使用する場合には、これらのいずれの仕様上限の制約を受けない範囲でご使用下さい。

・Loopback インターフェースに設定可能な IP アドレスは最大 14 個です(CLI 禁則あり)。
・VLAN インターフェースに設定可能な Primary IP アドレス設定は最大 255 個です(CLI 禁則あり)。
・Apresia13000 シリーズにおいて VLAN インターフェースに Secondary IP アドレス設定を行う場合には、総数を最大 1000 個以下で使用することを推奨します(CLI 禁則なし)。
・Apresia3400/4300/5400 シリーズにおいて VLAN インターフェースに Secondary IP アドレス設定を行う場合には、総数を最大 100 個以下で使用することを推奨します(CLI 禁則なし)。

表 12-3 IP アドレス機能が占有するグループ数

表示名称[1]	Apresia3400/ 5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
Netif	0～5 個[2]	0～6 個[2]	0～5 個[2]	0～4 個[2]	0～9 個[2]

1) “ show packet-filter2 reserved-group ”での表示名称。
2) これより多くのグループを IP アドレス機能で占有することも可能ですが、仕様としてこれ以上占有するような IP アドレス設定は推奨しません。

12.2 ユーザーループ検知機能

ユーザーループ検知機能の設定を行うと 1 グループ占有します。“ show packet-filter2 reserved-group ”では「Loop watch」と表示されます。占有するグループ番号をユーザーが指定するこ

とも可能です。指定しない場合には自動的にまだ他の機能で使用されていない最老番のグループが 1 個占有されます。ユーザーループ検知機能が占有するグループ数に関して 表 12-4 にまとめます。

■ ユーザーループ検知機能が占有するグループ番号指定コマンド
loop-watch group <GROUP>
GROUP ····· 指定するグループ番号。Apresia4328GT の場合は<1-7>、それ以外の装置の場合には<1-14>。

表 12-4 ユーザーループ検知機能が占有するグループ数

表示名称[1]	Apresia3400/5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
Loop watch	1 個	1 個	1 個	1 個	1 個

1) “ show packet-filter2 reserved-group ”での表示名称です。

12.3 MMRP機能

MMRP 機能において Apresia13000-48X では全ての機能が使用可能となりますが、それ以外の装置ではアウェアスイッチとして使用時のみ、全ての機能が使用可能となることに注意して下さい。

Apresia13000-24GX-PSR/5412GT-PoE では MMRP 機能の設定を行うと 1 グループ占有します。Apresia3424 シリーズ/4300 シリーズ/5428GT/13000-48X では 1 グループもしくは連番で 2 グループ占有します。Apresia3448 シリーズでは 1 グループもしくは連番で 2～3 グループ占有します。“ show packet-filter2 reserved-group ”では「MMRP」と表示されます。

MMRP 機能が占有するグループ番号をユーザーが指定することも可能です。指定しない場合には自動的にグループ 1 番、グループ 1～2 番もしくはグループ 1～3 番が占有されます。もしも他の機能によってグループ 1～2 番が既に使用されている場合には、別の空いているグループを指定しない限り MMRP 機能を使用できないことに注意して下さい。

■ MMRP 機能が占有するグループ番号指定コマンド
mmrp group <GROUP> [NUMBER]
GROUP ····· 指定するグループ番号。Apresia4328GT の場合は<1-7>、それ以外の装置の場合には<1-14>。
NUMBER ···· 占有するグループ数指定オプション。
Apresia3424 シリーズ/4328GT/5428GT：<1-2>(デフォルト 1)
Apresia3448 シリーズ：<1-3>(デフォルト設定 1)
Apresia4348 シリーズ/13000-48X：<1-2>(デフォルト 2)
Apresia13000-24GX-PSR/5412GT-PoE：<1>(デフォルト 1)

Apresia13000-24GX-PSR/5412GT-PoE以外の装置では、設定するRingの数が少ない場合には 1 グループだけの占有でも動作可能ですが、装置の最大数までRingを設定するには 2 グループもしくは 3 グループの占有が必要です。占有するグループ数と設定可能なRing数に関して 表 12-5 にまとめます。

表 12-5 占有グループ数と MMRP 機能の設定可能な Ring 数の関係

No.	対象	概要
1	Apresia3424 シリーズ	・物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 ・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。
2	Apresia3448 シリーズ	・物理ポートが最大 52 ポートのため、仕様としてはアウェアスイッチとして最大 26 個の Ring を設定可能です。この場合は 3 グループ占有の設定が必要です。 ・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。 ・2 グループ占有設定の場合には、最大 25 個の Ring を設定可能です。
3	Apresia4328GT	・物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 ・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。
4	Apresia4348 シリーズ	・物理ポートが最大 48 ポートのため、仕様としてはアウェアスイッチとして最大 24 個の Ring を設定可能です。この場合は 2 グループ占有設定が必要です。 ・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。
5	Apresia5412GT -PoE[1]	・物理ポートが最大 12 ポートのため、仕様としてはアウェアスイッチとして最大 6 個の Ring を設定可能です。
6	Apresia5428GT	・物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 ・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。
7	Apresia13000-24GX-PSR[1]	・物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。
8	Apresia13000-48X	・物理ポートが最大 50 ポートのため、仕様としては最大 50 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 ・1 グループ占有設定の場合には、MMRP ポートの総数[2]が 25 ポートを超過しない範囲の Ring を設定可能です。全て分散マスタースイッチとする場合は最大 25 個の Ring を設定可能です。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能です。

1) Apresia13000-24GX-PSR/5412GT-PoE は 1 グループを占有する設定のみとなります。

2) MMRP ポートの総数の算出方法は下記を参照してください。

MMRP ポートの総数 ＝ (マスタースイッチとして設定する MMRP Ring[1] の数×2 ポート)
＋(アウェアスイッチとして設定する MMRP Ring[2] の数×2 ポート)
＋(分散マスタースイッチの Master ポートを設定する MMRP Ring[3] の数)
＋(分散シャドウスイッチの Slave ポートを設定する MMRP Ring[4] の数)

1) “mmrp ring <NAME> master”で設定する Ring。
2) “mmrp ring <NAME> aware”で設定する Ring。
3) “mmrp ring <NAME> divided-master”で設定する Ring。
4) “mmrp ring <NAME> divided-shadow”で設定する Ring。

12.4 MMRP-Plus機能

Apresia13000-24GX-PSR/5412GT-PoE では MMRP-Plus 機能の設定を行うと 1 グループ占有します。Apresia3424 シリーズ/4300 シリーズ/5428GT/13000-48X では 1 グループもしくは連番で 2 グループ占有します。Apresia3448 シリーズでは 1 グループもしくは連番で 2～3 グループ占有します。“ show packet-filter2 reserved-group ”では「MMRP」と表示されます。「MMRP-Plus」と表示されないことに注意して下さい。

MMRP-Plus 機能が占有するグループ番号をユーザーが指定することも可能です。指定しない場合には自動的にグループ 1 番、グループ 1～2 番もしくはグループ 1～3 番が占有されます。もしも他の機能によってグループ 1～2 番が既に使用されている場合には、別の空いているグループを指定しない限り MMRP-Plus 機能を使用できないことに注意して下さい。

■ MMRP-Plus 機能が占有するグループ番号指定コマンド
mmrp-plus group <GROUP> [NUMBER]
GROUP ····· 指定するグループ番号。Apresia4328GT の場合は<1-7>、それ以外の装置の場合には<1-14>。
NUMBER ···· 占有するグループ数指定オプション。
Apresia3424 シリーズ/4328GT/5428GT：<1-2>(デフォルト 1)
Apresia3448 シリーズ：<1-3>(デフォルト設定 1)
Apresia4348 シリーズ/Apresia13000-48X：<1-2>(デフォルト 2)
Apresia13000-24GX-PSR/5412GT-PoE：<1>(デフォルト 1)

Apresia13000-24GX-PSR/5412GT-PoE以外の装置では、設定するRingの数が少ない場合には 1 グループだけの占有でも動作可能ですが、装置の最大数までRingを設定するには 2 グループもしくは 3 グループの占有が必要です。占有するグループ数と設定可能なRing数に関して 表 12-6 にまとめます。

表 12-6 占有グループ数と MMRP-Plus 機能の設定可能な Ring 数の関係

No.	対象	概要
1	Apresia3424 シリーズ	・物理ポートが最大 28 ポートのため、仕様としては最大 28 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 ・1 グループ占有の設定の場合には、MMRP-Plus ポートの総数[2]が 25 ポートを超過しない範囲の Ring を設定可能。全て分散マススイッチとする場合は最大 25 個の Ring を設定可能です。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能です。
2	Apresia3448 シリーズ	・物理ポートが最大 52 ポートのため、仕様としては最大 52 個の Ring を設定可能。この場合は 3 グループ占有設定が必要。 ・1 グループ占有設定の場合には、MMRP-Plus ポートの総数[2]が 25 ポートを超えない範囲の Ring を設定可能。全て分散マススイッチとする場合は最大 25 個の Ring を設定可能。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能。

No.	対象	概要
		•2 グループ占有設定の場合には、MMRP-Plus ポートの総数[2]が 50 ポートを超えない範囲の Ring を設定可能。全て分散マススイッチとする場合は最大 50 個の Ring を設定可能。全てアウェアスイッチとする場合は最大 25 個の Ring を設定可能。
3	Apresia4328GT	•物理ポートが最大 28 ポートのため、仕様としては最大 28 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 •1 グループ占有設定の場合には、MMRP-Plus ポートの総数[2]が 25 ポートを超えない範囲の Ring を設定可能です。全て分散マススイッチとする場合は最大 25 個の Ring を設定可能です。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能です。
4	Apresia4348 シリーズ	•物理ポートが最大 48 ポートのため、仕様としては最大 48 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 •1 グループ占有設定の場合には、MMRP-Plus ポートの総数[2]が 25 ポートを超えない範囲の Ring を設定可能です。全て分散マススイッチとする場合は最大 25 個の Ring を設定可能です。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能です。
5	Apresia5412GT -PoE[1]	•物理ポートが最大 12 ポートのため、仕様としてはアウェアスイッチとして最大 6 個の Ring を設定可能です。
6	Apresia5428GT	•物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 •1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。
7	Apresia13000-24GX-PSR[1]	•物理ポートが最大 28 ポートのため、仕様としては最大 28 個の Ring を設定可能です。
8	Apresia13000-48X	•物理ポートが最大 50 ポートのため、仕様としては最大 50 個の Ring を設定可能です。この場合は 2 グループ占有の設定が必要です。 •1 グループ占有設定の場合には、MMRP-Plus ポートの総数[2]が 25 ポートを超えない範囲の Ring を設定可能です。全て分散マススイッチとする場合は最大 25 個の Ring を設定可能です。全てアウェアスイッチとする場合は最大 12 個の Ring を設定可能です。

1) Apresia13000-24GX-PSR/5412GT-PoE は 1 グループを占有する設定のみとなります。

2) MMRP-Plus ポートの総数の算出方法は下記を参照してください。

MMRP-Plus ポートの総数
　＝ (マススイッチとして設定する MMRP-Plus Ring[1]の数×2 ポート)
　　＋(アウェアスイッチとして設定する MMRP-Plus Ring[2]の数×2 ポート)
　　＋(分散マススイッチの Master ポートを設定する MMRP-Plus Ring[3]の数)
　　＋(分散シャドウスイッチの Slave ポートを設定する MMRP-Plus Ring[4]の数)

1) “mmrp-plus ring <RINGID> master”で設定する Ring。
2) “mmrp-plus ring <RINGID> aware”で設定する Ring。

3) “mmrp-plus ring <RINDID> divided-master”で設定する Ring。
4) “mmrp-plus ring <RINDID> divided-shadow”で設定する Ring。

12.5 MMRP2 Aware機能

MMRP2 Aware 機能は Apresia13000-24GX-PSR と Apresia13000-48X でのみ使用可能です。

この機能は同一装置の別ポートならば MMRP 機能と併用設定可能ですが、この場合には MMRP2 Aware 機能が占有するグループと MMRP 機能が占有するグループが同じになるように指定して下さい。同様に同一装置の別ポートならば MMRP-Plus 機能と併用設定可能ですが、この場合には MMRP2 Aware 機能が占有するグループと MMRP-Plus 機能が占有するグループが同じになるように指定して下さい。なお、MMRP 機能と MMRP-Plus 機能は同一装置で併用できないことに注意して下さい。

上述のような併用設定で使用する場合には同じパケットフィルター2 のリソースを消費することになるため、それぞれの機能で説明している設定可能な最大 Ring 数は減ることに注意して下さい。以降では、MMRP2 Aware 機能だけを設定した場合について説明します。

Apresia13000-24GX-PSR では MMRP2 Aware 機能を設定すると 1 グループ占有します。Apresia13000-48X では 1 グループもしくは連番で 2 グループ占有します。“show packet-filter2 reserved-group”では「MMRP」と表示されます。「MMRP2 Aware」と表示されないことに注意して下さい。

MMRP2 Aware 機能が占有するグループ番号をユーザーが指定することも可能です。指定しない場合には自動的にグループ 1 番もしくはグループ 1～2 番が占有されます。もしも他の機能によってグループ 1～2 番が既に使用されている場合には、別の空いているグループを指定しない限り MMRP2 Aware 機能を使用できないことに注意して下さい。

■ MMRP2 Aware 機能が占有するグループ番号指定コマンド
mmrp2 group <GROUP> [NUMBER]
GROUP ····· 指定するグループ番号。<1-14>。
NUMBER ···· 占有するグループ数指定オプション。
Apresia13000-48X：<1-2>(デフォルト 2)
Apresia13000-24GX-PSR：<1>(デフォルト 1)

Apresia13000-48Xでは、設定するRingの数が少ない場合には 1 グループだけの占有でも動作可能ですが、装置の最大数までRingを設定するには 2 グループの占有が必要です。占有するグループ数と設定可能なRing数に関して 表 12-7 にまとめます。

表 12-7 占有グループ数と MMRP2 Aware 機能の設定可能な Ring 数の関係

No.	対象	概要
1	Apresia13000-24GX-PSR[1]	・物理ポートが最大 28 ポートのため、仕様としてはアウェアスイッチとして最大 14 個の Ring を設定可能です。
2	Apresia13000-48X	・物理ポートが最大 50 ポートのため、仕様としてはアウェアスイッチとして最大 25 個の Ring を設定可能です。この場合は 2 グループ占有設定が必要です。

No.	対象	概要
		・1 グループ占有設定の場合には、最大 12 個の Ring を設定可能です。

1) Apresia13000-24GX-PSR は 1 グループを占有する設定のみとなります。

12.6 AccessDefender機能

AccessDefender 機能の設定を行うと最少でも連番で 4 グループ占有します。認証端末数が多ければ多いほど占有するグループ数も増加します。“ show packet-filter2 reserved-group ”では「AccessDefender」と表示されます。

AccessDefender 機能では、最大認証端末数に応じて使用する最大ルール数を最初に設定する必要があります。最大ルール数の設定により、未使用の最老番グループから連番で降順に必要なグループ数だけ自動的に占有されます。

使用ルール数はWeb認証、MAC認証、802.1X認証では 1 端末につき 1 ルール使用します。DHCPスヌーピングでは 201 端末目以降(Apresia13000-24GXは 401 端末目以降)、1 端末につき 2 ルール使用します。表 12-8 に最大ルール数と占有するグループ数の関係を示します。

■ AccessDefender 機能の認証端末の最大数を設定するコマンド
packet-filter2 max-rule <RULE1> [deny-rule <RULE2>]
RULE1 …… AccessDefender 機能が占有するパケットフィルター2 の最大ルール数
設定可能範囲は装置種別により異なります。表 12-8 参照。
RULE2 …… 認証拒否機能が占有するパケットフィルター2 の最大ルール数
本オプションを設定した場合、1 グループを占有します。

表 12-8 最大ルール数と占有するグループ数

占有するグループ数	“ paceket-filter2 max-rule <RULE> ”で指定する最大ルール数[3]				
	Apresia3400/5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
4 個	1-128	1-128	1-128	1-256	1-128
5 個	129-256	129-256	129-256	257-512	129-256
6 個	257-384	257-384	257-384	513-768	257-384
7 個	385-512	385-512[1]	385-512	769-1024	385-512
8 個	513-640	×[2]	513-640	1025-1280	513-640
9 個	641-768	×[2]	641-768	1281-1536	641-768
10 個	769-896	×[2]	769-896	1537-1792	769-896
11 個	897-1024	×[2]	897-1024	1793-2048	897-1024
12 個	1025-1152	×[2]	1025-1152	2049-2304	1025-1152
13 個	1153-1280	×[2]	1153-1280	2305-2560	1153-1280
14 個[1]	1281-1408[1]	×[2]	1281-1408[1]	2561-2816[1]	1281-1408[1]

1) この場合には AccessDefender 機能によってパケットフィルター2 のリソースを全て占有することに注意して下さい。例えば、認証バイパス機能を併用する場合には認証バイパスの設定を行うグルー

プ数を考慮して最大数を検討して下さい。

2) Apresia4328GTの最大グループ数は 7 個です。表 2-1 参照。

3) Web 認証、MAC 認証、802.1X 認証では 1 端末につき 1 ルール使用します。DHCP スヌーピングでは 201 端末目以降(Apresia13000-24GX は 401 端末目以降)、1 端末につき 2 ルール使用します。

例えば Apresia13000-48X で“ packet-filter2 max-rule 256 ”により 5 グループ占有する場合を考えます。他の機能によってまだどのグループも占有されていない場合にはグループ 10～14 番の 5 個が占有されますが、他の機能によって既にグループ 13～14 が占有されている場合には 8～12 番の 5 個が占有されます。ただし、他の機能によって既にグループ 13 は占有されているがグループ 14 は占有されていないような場合には、「まだ他の機能で使用されていない最老番のグループから連番で降順に必要なグループ数だけ占有」することができないため、このままでは設定できません。この場合には、AccessDefender 機能が占有するグループの先頭番号を指定するコマンドを併用設定して下さい。

■ AccessDefender 機能が占有するグループの先頭番号を指定するコマンド
packet-filter2 group <NUMBER>
NUMBER ・・・・ 指定するグループ番号です。Apresia4328GT の場合は<1-4>、それ以外の装置の場合には<1-11>となります。

上述の例において、最初に“ packet-filter2 group 3 ”により占有する先頭のグループ番号を 3 番に指定することとします。この場合に“ packet-filter2 max-rule 256 ”を実施すると、グループ 3～7 番が他の機能によって占有されていなければグループ 3～7 番の 5 個が占有されます。グループ 3～7 番が他の機能によって占有されている場合には“ packet-filter2 max-rule 256 ”は設定できません。

12.7 その他の機能

これまで説明した機能以外では、「Flush FDB rp-e 機能」「Flush FDB rp-g 機能」「NA 機能」がパケットフィルター2 のリソースを占有します。なお、「NA 機能」は Apresia13000-48X のみ使用可能なことに注意して下さい。

これらの機能が占有するグループ番号をユーザーが指定することはできません。占有する場合には自動的にまだ他の機能で使用されていない最老番のグループから必要なグループ数だけ占有されます。表 12-9 にこれらの機能が占有するグループ数に関してまとめます。

表 12-9 各機能が占有するグループ数

表示名称[1]	Apresia3400/5400 シリーズ	Apresia4328GT	Apresia4348 シリーズ	Apresia13000-24GX-PSR	Apresia13000-48X
Flush FDB rp-e	1 個	1 個	1 個	1 個	1 個
Flush FDB rp-g	1 個	1 個	1 個	1 個	1 個
NA	×[3]	×[3]	×[3]	×[3]	1～3 個[4]

1) “ show packet-filter2 reserved-group ”での表示名称。

2) NA 機能は Apresia13000-48X のみ使用可能です。

3) NA 機能の使用方法により占有するグループ数は異なります。詳細に関してはコマンドリファレンスを参照して下さい。

13. 設定項目

パケットフィルター2 の設定項目を 表 13-1～表 13-4 に示します。

表 13-1 識別条件(アサイン)の設定項目

No.	項目	default 設定	可変項目
1	port 指定	なし	Apresia3424 シリーズ：1-28 Apresia3448 シリーズ：1-52 Apresia4328GT：1-28 Apresia4348 シリーズ：1-48 Apresia5412GT-PoE：1-12 Apresia5428GT：1-28 Apresia13000-24GX-PSR：1-28 Apresia13000-48X：1-50
2	VLAN 指定	なし	<VID> 1-4094 <MASK> 0x0[1]-0xfff <MASK>省略時は 0xfff

1) <MASK>を 0x0 指定で設定した場合には、結果的に全ての VLAN を対象にすることになるため VLAN 指定の設定が削除される動作になります。

表 13-2 フィルター条件(コンディション)の設定項目

No.	項目	default 設定	可変項目
1	宛先 MAC アドレス	なし	<MAC> 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff <MASK> 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff[1] <MASK>省略時は ff:ff:ff:ff:ff:ff
2	送信元 MAC アドレス	なし	<MAC> 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff <MASK> 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff[1] <MASK>省略時は ff:ff:ff:ff:ff:ff
3	VLAN ID	なし	<VID> 1-4094 <MASK> 0x0-0xfff[1] <MASK>省略時は 0xfff
4	Ethernet Type	なし	<TYPE> 0x0-0xffff <MASK> 0x0-0xffff[1] <MASK>省略時は 0xffff
5	ARP 送信元 IP アドレス (arp-sender-ip)	なし	<IPv4> 0.0.0.0-255.255.255.255 <NETMASK>[2] 0-32 <NETMASK>省略時は 32
6	送信元 IPv4 アドレス	なし	<IPv4> 0.0.0.0-255.255.255.255 <NETMASK>[2] 0-32

			<NETMASK>省略時は 32
7	宛先 IPv4 アドレス	なし	<IPv4> 0.0.0.0-255.255.255.255 <NETMASK>[2] 0-32 <NETMASK>省略時は 32
8	TOS フィールド(tos)	なし	<VALUE> 0x0-0xff <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
9	DSCP 値(tos-dscp)	なし	<VALUE> 0-63 <MASK> 0x0-0x3f[1] <MASK>省略時は 0x3f
10	IP Precedence 値 (tos-precedence)	なし	<VALUE> 0-7 <MASK> 0x0-0x7[1] <MASK>省略時は 0x7
11	プロトコルフィールド (protocol)	なし	<VALUE> 0-255 <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
12	送信元 TCP/UDP ポート番号 (src tcp/udp)	なし	<VALUE> 0-65535 オプションで[tcp|udp]指定可
13	宛先 TCP/UDP ポート番号 (dst tcp/udp)	なし	<VALUE> 0-65535 オプションで[tcp|udp]指定可
14	TCP ヘッダーの制御 Flag フィールド(tcp-flag)	なし	・各制御 Flag(FIN、SYN、RST、PSH、ACK、URG)に関して 0 or 1 を指定します。 ・未設定の Flag に関しては任意の値になるように自動的にマスク設定が調整されます。
15	Traffic Class フィールド (traffic-class)	なし	<VALUE> 0-255 <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
16	Flow Label フィールド (flow-label)	なし	<VALUE> 0-1048575 <MASK> 0x0-0xfffff[1] <MASK>省略時は 0xfffff
17	Next Header フィールド (next-header)	なし	<VALUE> 0-255 <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
18	Hop Limit フィールド (hop-limit)	なし	<VALUE> 0-255 <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
19	ICMPv6 ヘッダー Type フィールド (icmp type)	なし	<VALUE> 0-255 <MASK> 0x0-0xff[1] <MASK>省略時は 0xff
20	送信元 IPv6 アドレス	なし	<IPv6> ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

			<LENGTH>[3] 0-128
21	宛先 IPv6 アドレス	なし	<IPv6> ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <LENGTH>[3] 0-128

1) <MASK>を全てのビットが 1 になるように指定して設定した場合には、構成情報では<MASK>指定が省略された形式で表示されることに注意して下さい。
2) <NETMASK>指定値によっては<IPv4>指定値が自動的に修正されます。例えば「192.168.1.100/24」と指定した場合には自動的に「192.168.1.0/24」に修正されます。
3) <LENGTH>の省略設定はできません。

表 13-3 アクションの設定項目

No.	項目	default 設定	可変項目
1	permit	なし	－
2	deny	なし	－
3	none	なし	－
4	authentication-bypass	なし	－
5	block-cpu-control	なし	－
6	qos	なし	qp1-qp8
7	priority	なし	0-7, [from ip-tos-precedence]
8	ip-tos-dscp	なし	0-63
9	ip-tos-precedence	なし	0-7
10	policing[1]	cir： 33554368Kbps cbs：4Kbyte	<設定方法 1 の場合> cir：64-33554368(Kbps)、64Kbps 刻み[2] cbs：4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384(Kbyte)[3] <設定方法 2 の場合> group：1-64(Apresia13000-24GX-PSR 以外の装置) 1-128(Apresia13000-24GX-PSR)
11	redirect	なし	Apresia3424 シリーズ：1-28 Apresia3448 シリーズ：1-52 Apresia4328GT：1-28 Apresia4348 シリーズ：1-48 Apresia5412GT-PoE：1-12 Apresia5428GT：1-28 Apresia13000-24GX-PSR：1-28 Apresia13000-48X：1-50
12	counter	なし	1-64(Apresia13000-24GX-PSR 以外の装置) 1-128(Apresia13000-24GX-PSR) オプションで[unit byte]指定可

13	mirror	なし	Apresia3424 シリーズ：1-28 Apresia3448 シリーズ：1-52 Apresia4328GT：1-28 Apresia4348 シリーズ：1-48 Apresia5412GT-PoE：1-12 Apresia5428GT：1-28 Apresia13000-24GX-PSR：1-28 Apresia13000-48X：1-50

1) 二通りの設定方法に関しては「4.10 policing」を参照して下さい。
2) CIR は設定可能範囲の任意の値を指定して設定できますが、実際の動作は 64Kbps 刻みになります。設定値が 64Kbps 刻みの値ではない場合には、その設定値を超えない一番近い 64Kbps 刻みの値として動作します。CIR の設定は有効値を指定して設定することを推奨します。
3) CBS は設定可能範囲の任意の値を指定して設定できますが、実際に有効な値はこの表に示す 13 通りです。設定値が有効値ではない場合には、その設定値を超えない一番近い有効値として動作します。CBS の設定は有効値を指定して設定することを推奨します。

表 13-4 その他の設定項目

No.	項目	default 設定	可変項目
1	exceeded-action	なし	deny
2	ルールの有効/無効	有効	(enable[1]), disable
3	帯域制限エントリーの CIR 設定	33554368Kbps	64-33554368(Kbps)、64Kbps 刻み [2]
4	帯域制限エントリーの CBS 設定	4Kbyte	4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384(Kbyte)[3]

1) コマンドとして選択項目には含まれないので、デフォルト設定に戻す場合には no 指定で設定を削除します。
2) CIR は設定可能範囲の任意の値を指定して設定できますが、実際の動作は 64Kbps 刻みになります。設定値が 64Kbps 刻みの値ではない場合には、その設定値を超えない一番近い 64Kbps 刻みの値として動作します。CIR の設定は有効値を指定して設定することを推奨します。
3) CBS は設定可能範囲の任意の値を指定して設定できますが、実際に有効な値はこの表に示す 13 通りです。設定値が有効値ではない場合には、その設定値を超えない一番近い有効値として動作します。CBS の設定は有効値を指定して設定することを推奨します。

14. 設定手順

パケットフィルター2 の設定手順を説明します。各コマンドの詳細に関してはコマンドリファレンスを参照して下さい。なお、パケットフィルター2 は PACKETFILTER2 モードで設定を行います。

■ PACKETFILTER2 モードへの移行コマンド
packet-filter2

14.1 手順(1) 識別条件(アサイン)の設定

最初に識別条件を設定します。識別条件は必ず設定する必要があります。識別条件はルールを適用する受信ポートもしくは受信VLANを指定します。識別条件の詳細に関しては「3.1 識別条件(アサイン)」を参照して下さい。

■ 識別条件(アサイン)の設定
<GROUP> assign port <PORT>
<GROUP> assign vlan <VID> [mask <MASK>]
<GROUP> <RULE> assign port <PORT>
<GROUP> <RULE> assign vlan <VID> [mask <MASK>]
GROUP ····· グループ番号 設定可能範囲は装置種別により異なります 表 2-1 参照
RULE ····· ルール番号 設定可能範囲は装置種別により異なります 表 2-2 参照
PORT ····· ポート番号 複数指定可能。設定可能範囲は装置種別により異なります 表 13-1 参照
VID ····· VLAN ID 1-4094
MASK ····· VLAN ID に対するマスク 0x0[1]-0xfff 省略時は 0xfff

1) <MASK>を 0x0 指定で設定した場合には、結果的に全ての VLAN を対象にすることになるため vlan 指定の設定が削除される動作になります。

14.2 手順(2) フィルター条件(コンディション)の設定

次にフィルター条件を設定します。フィルター条件を設定しない場合には「14.1 手順(1) 識別条件(アサイン)の設定」で設定した条件に一致する全ての受信トラフィックが対象になります。

フィルター条件はルールを適用するトラフィックの詳細な情報を定義します。コンディションタイプによって使用可能なフィルター条件が異なることに注意して下さい。また、フィルター条件の組み合わせによっては併用設定できない組み合わせがあることに注意して下さい。フィルター条件の詳細に関しては「3.2 フィルター条件(コンディション)」を参照して下さい。

■ フィルター条件(コンディション)設定コマンドの共通項目
GROUP ····· グループ番号 設定可能範囲は装置種別により異なります 表 2-1 参照
RULE ····· ルール番号 設定可能範囲は装置種別により異なります 表 2-2 参照

■ 宛先 MAC アドレス条件の設定
dst コンディションタイプの場合
  <GROUP> <RULE> condition dst mac <MAC> [mask <MASK>]
ethernet コンディションタイプの場合
  <GROUP> <RULE> condition ethernet dst mac <MAC> [mask <MASK>]
          MAC ・・・・・・・ 宛先 MAC アドレス 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff
          MASK ・・・・・・ <MAC>に対するマスク 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff[1]
                      省略時は ff:ff:ff:ff:ff:ff

■ 送信元 MAC アドレス条件の設定
src コンディションタイプの場合
  <GROUP> <RULE> condition src mac <MAC> [mask <MASK>]
ethernet コンディションタイプの場合
  <GROUP> <RULE> condition ethernet src mac <MAC> [mask <MASK>]
          MAC ・・・・・・・ 送信元 MAC アドレス 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff
          MASK ・・・・・・ <MAC>に対するマスク 00:00:00:00:00:00-ff:ff:ff:ff:ff:ff[1]
                      省略時は ff:ff:ff:ff:ff:ff

■ VLAN ID 条件の設定
dst コンディションタイプの場合
  <GROUP> <RULE> condition dst vid <VID> [mask <MASK>]
src コンディションタイプの場合
  <GROUP> <RULE> condition src vid <VID> [mask <MASK>]
ethernet コンディションタイプの場合
  <GROUP> <RULE> condition ethernet vid <VID> [mask <MASK>]
          VID ・・・・・・・ VLAN ID 1-4094
          MASK ・・・・・・ <VID>に対するマスク 0x0-0xfff[1] 省略時は 0xfff

■ Ethernet Type 条件の設定
dst コンディションタイプの場合
  <GROUP> <RULE> condition dst type <TYPE> [mask <MASK>]
src コンディションタイプの場合
  <GROUP> <RULE> condition src type <TYPE> [mask <MASK>]
ethernet コンディションタイプの場合
  <GROUP> <RULE> condition ethernet type <TYPE> [mask <MASK>]
          TYPE ・・・・・・ Ethernet Type 0x0-0xffff
          MASK ・・・・・・ <TYPE>に対するマスク 0x0-0xffff[1] 省略時は 0xffff

■ ARP 送信元 IP アドレス(arp-sender-ip)条件の設定
  <GROUP> <RULE> condition src arp-sender-ip <IPv4>[/<NETMSAK>]
          IPv4 ・・・・・・ ARP パケットの Sender protocol address フィールド
                      0.0.0.0-255.255.255.255
          NETMASK ・・・ <IPv4>に対するマスク(プレフィックス表記)[2] 0-32 省略時は 32

■ 送信元 IPv4 アドレス条件の設定
src コンディションタイプの場合
  <GROUP> <RULE> condition src ip <IPv4>[/<NETMASK>]
ipv4, ipv4-src-tcp/udp-range, ipv4-dst-tcp/udp-range コンディションタイプの場合

<GROUP> <RULE> condition ipv4 src ip <IPv4>[/<NETMSAK>]
IPv4 ・・・・・・ 送信元 IPv4 アドレス 0.0.0.0-255.255.255.255
NETMASK ・・・ <IPv4>に対するマスク(プレフィックス表記)[2] 0-32 省略時は 32

■ 宛先 IPv4 アドレス条件の設定
dst コンディションタイプの場合
<GROUP> <RULE> condition dst ip <IPv4>[/<NETMASK>]
ipv4, ipv4-src-tcp/udp-range, ipv4-dst-tcp/udp-range コンディションタイプの場合
<GROUP> <RULE> condition ipv4 dst ip <IPv4>[/<NETMSAK>]
IPv4 ・・・・・・ 宛先 IPv4 アドレス 0.0.0.0-255.255.255.255
NETMASK ・・・ <IPv4>に対するマスク(プレフィックス表記)[2] 0-32 省略時は 32

■ TOS フィールド(tos)条件の設定
<GROUP> <RULE> condition ipv4 tos <VALUE> [mask <MASK>]
VALUE ・・・・・ IPv4 ヘッダーの TOS フィールド 0x0-0xff
MASK ・・・・・・ <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ DSCP 値(tos-dscp)条件の設定
<GROUP> <RULE> condition ipv4 tos-dscp <VALUE> [mask <MASK>]
VALUE ・・・・・ IPv4 ヘッダーの DSCP 値 0-63
MASK ・・・・・・ <VALUE>に対するマスク 0x0-0x3f[1] 省略時は 0x3f

■ IP Precedence 値(tos-precedence)条件の設定
<GROUP> <RULE> condition ipv4 tos-precedence <VALUE> [mask <MASK>]
VALUE ・・・・・ IPv4 ヘッダーの IP Precedence 値 0-7
MASK ・・・・・・ <VALUE>に対するマスク 0x0-0x7[1] 省略時は 0x7

■ プロトコルフィールド(protocol)条件の設定
<GROUP> <RULE> condition ipv4 protocol <VALUE> [mask <MASK>]
VALUE ・・・・・ IPv4 ヘッダーのプロトコルフィールド 0-255
MASK ・・・・・・ <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ 送信元 TCP/UDP ポート番号(src tcp/udp)条件の設定
<GROUP> <RULE> condition ipv4 src tcp/udp <VALUE> [tcp|udp]
<GROUP> <RULE> condition ipv6 src tcp/udp <VALUE> [tcp|udp]
VALUE ・・・・・ 送信元 TCP/UDP ポート番号 0-65535
tcp ・・・・・・・ オプション TCP 指定
udp ・・・・・・・ オプション UDP 指定

■ 宛先 TCP/UDP ポート番号(dst tcp/udp)条件の設定
<GROUP> <RULE> condition ipv4 dst tcp/udp <VALUE> [tcp|udp]
<GROUP> <RULE> condition ipv6 dst tcp/udp <VALUE> [tcp|udp]
VALUE ・・・・・ 宛先 TCP/UDP ポート番号 0-65535
tcp ・・・・・・・ オプション TCP 指定
udp ・・・・・・・ オプション UDP 指定

■ TCP ヘッダーの制御 Flag フィールド(tcp-flag)条件の設定
<GROUP> <RULE> condition ipv4 tcp-flag {fin|syn|rst|psh|ack|urt} <VALUE>
VALUE ・・・・・ 0-1

■ Traffic Class フィールド(traffic-class)条件の設定
<GROUP> <RULE> condition ipv6 traffic-class <VALUE> [mask <MASK>]
VALUE ····· IPv6 ヘッダーの Traffic Class フィールド 0-255
MASK ····· <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ Flow Label フィールド(flow-label)条件の設定
<GROUP> <RULE> condition ipv6 flow-label <VALUE> [mask <MASK>]
VALUE ····· IPv6 ヘッダーの Flow Label フィールド 0-1048575
MASK ····· <VALUE>に対するマスク 0x0-0xfffff[1] 省略時は 0xfffff

■ Next Header フィールド(next-header)条件の設定
<GROUP> <RULE> condition ipv6 next-header <VALUE> [mask <MASK>]
VALUE ····· IPv6 ヘッダーの Next Header フィールド 0-255
MASK ····· <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ Hop Limit フィールド(hop-limit)条件の設定
<GROUP> <RULE> condition ipv6 hop-limit <VALUE> [mask <MASK>]
VALUE ····· IPv6 ヘッダーの Hop Limit フィールド 0-255
MASK ····· <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ ICMPv6 ヘッダーType フィールド(icmp type)条件の設定
<GROUP> <RULE> condition ipv6 icmp type <VALUE> [mask <MASK>]
VALUE ····· ICMPv6 ヘッダーの Type フィールド 0-255
MASK ····· <VALUE>に対するマスク 0x0-0xff[1] 省略時は 0xff

■ 送信元 IPv6 アドレス条件の設定
<GROUP> <RULE> condition ipv6 src ip <IPv6>[/<LENGTH>]
IPv6 ····· 送信元 IPv6 アドレス ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
LENGTH ···· <IPv6>に対するプレフィックス長[3] 0-128

■ 宛先 IPv6 アドレス条件の設定
<GROUP> <RULE> condition ipv6 dst ip <IPv6>[/<LENGTH>]
IPv6 ····· 宛先 IPv6 アドレス ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
LENGTH ···· <IPv6>に対するプレフィックス長[3] 0-128

1) <MASK>を全てのビットが 1 になるように指定して設定した場合には、構成情報では<MASK>指定が省略された形式で表示されることに注意して下さい。
2) <NETMASK>指定値によっては<IPv4>指定値が自動的に修正されます。例えば「192.168.1.100/24」と指定した場合には自動的に「192.168.1.0/24」に修正されます。
3) <LENGTH>の省略設定はできません。

14.3 手順(3) アクションの設定

次にアクションを設定します。アクションは識別条件・フィルター条件に一致した受信トラフィックに対してどのような操作を行うのかを定義します。同一ルールに複数のアクションを設定することは可能ですが、競合するアクションの場合には設定できないことに注意して下さい。アクションの詳細に関しては「4 アクション(動作)」を参照して下さい。

■ アクションの設定コマンド共通項目

GROUP ····· グループ番号 設定可能範囲は装置種別により異なります 表 2-1 参照

RULE ····· ルール番号 設定可能範囲は装置種別により異なります 表 2-2 参照

■ permit アクションの設定

<GROUP> <RULE> action permit

■ deny アクションの設定

<GROUP> <RULE> action deny

■ none アクションの設定

<GROUP> <RULE> action none

■ authentication-bypass アクションの設定

<GROUP> <RULE> action authentication-bypass

■ block-cpu-control アクションの設定

<GROUP> <RULE> action block-cpu-control

■ qos アクションの設定

<GROUP> <RULE> action qos <QOSPROFILE>

QOSPROFILE ··· マッピングする QoS プロファイル qp1-qp8

■ priority アクションの設定

<GROUP> <RULE> action priority <PRIORITY>

<GROUP> <RULE> action priority from ip-tos-precedence

PRIORITY ····· 書き換える 802.1p 優先度の値 0-7

from ip-tos-precedence ··· IP Precedence 値(0-7)からの書き換え機能

■ ip-tos-dscp アクションの設定

<GROUP> <RULE> action ip-tos-dscp <DSCP>

DSCP ····· 書き換える DSCP 値 0-63

■ ip-tos-precedence アクションの設定

<GROUP> <RULE> action ip-tos-precedence <PRECEDENCE>

PRECEDENCE ··· 書き換える IP Precedence 値 0-7

■ 設定方法 1 によるpolicingアクションの設定(表 4-1 参照)

<GROUP> <RULE> action policing cir <RATE>

<GROUP> <RULE> action policing cbs <BURST>

RATE ····· CIR(Committed Information Rate) 64-33554368(Kbps)、64Kbps 刻み[1]

BURST ····· CBS(Committed Burst Size)

4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384(Kbyte)[2]

■ 設定方法 2 によるpolicingアクションの設定(表 4-1 参照)

<GROUP> <RULE> action policing group <P_INDEX>

<GROUP> policing <P_INDEX> cir <RATE>

<GROUP> policing <P_INDEX> cbs <BURST>

P_INDEX ··· 帯域制限エントリーの番号。設定可能範囲は装置種別により異なります 表 2-2 参照

RATE ····· CIR(Committed Information Rate) 64-33554368(Kbps)、64Kbps 刻み[1]

BURST ····· CBS(Committed Burst Size)
4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384(Kbyte)[2]

■ redirect アクションの設定
<GROUP> <RULE> action redirect <PORT>
PORT ····· リダイレクト先ポート 設定範囲は装置種別により異なります 表 13-3 参照

■ counter アクションの設定
<GROUP> <RULE> action counter <C_INDEX>
<GROUP> <RULE> action counter unit byte
C_INDEX ····· カウンター番号 設定可能範囲は装置種別により異なります 表 2-2 参照
unit byte ··· オプション受信バイト指定します

■ mirror アクションの設定
<GROUP> <RULE> action mirror <PORT>
PORT ····· ミラーリング先ポート 設定範囲は装置種別により異なります 表 13-3 参照

1) CIR は設定可能範囲の任意の値を指定して設定できますが、実際の動作は 64Kbps 刻みになります。設定値が 64Kbps 刻みの値ではない場合には、その設定値を超えない一番近い 64Kbps 刻みの値として動作します。CIR の設定は有効値を指定して設定することを推奨します。
2) CBS は設定可能範囲の任意の値を指定して設定できますが、実際に有効な値はこの表に示す 13 通りです。設定値が有効値ではない場合には、その設定値を超えない一番近い有効値として動作します。CBS の設定は有効値を指定して設定することを推奨します。

14.4 手順(4) exceeded-action denyの設定

パケットフィルター2 を受信時の帯域制限機能として使用する場合に設定します。exceeded-action は帯域制限エントリーを使用するルールにおいて、CIR(Committed Information Rate)を超えた受信トラフィックに対しての操作を設定するアクションです。設定可能なアクションとしては deny アクションのみが適用可能で、これを設定することにより受信時の帯域制限機能として使用することが可能です。

■ exceeded-action deny の設定
<GROUP> <RULE> exceeded-action deny
GROUP ····· グループ番号 設定可能範囲は装置種別により異なります 表 2-1 参照
RULE ····· ルール番号 設定可能範囲は装置種別により異なります 表 2-2 参照

14.5 手順(5) ルール毎の有効/無効設定

任意のルールを無効にしたい場合に設定します。デフォルト設定では各ルールは有効です。

■ ルール毎の有効/無効
<GROUP> <RULE> state disable
GROUP ····· グループ番号 設定可能範囲は装置種別により異なります 表 2-1 参照
RULE ····· ルール番号 設定可能範囲は装置種別により異なります 表 2-2 参照

15. フィルター条件および動作の一括設定(multiコマンド)

パケットフィルター2 のmultiコマンドを使用することによりフィルター条件(コンディション)、動作(アクション)の一括設定が可能です。multiコマンドで指定可能なフィルター条件(コンディション)を 表 15-1 に、動作(アクション)を 表 15-2 に示します。フィルター条件(コンディション)を複数指定する場合、表 15-1 の順番に従って設定してください(src-ipの後にdst-ipは設定できません)。

設定コマンドは以下です。一括設定表示を解除するには no <GROUP> <RULE> multi コマンドを使用して下さい。設定したコンディション、アクションのみを削除する場合は no コマンド使用時にコンディション、アクションを指定してください。

CPU 宛フィルターグループでは設定できません。

■ multi コマンド

[no] <GROUP> <RULE> multi [condition ipv4 <*CONDITIONS*> [<*CONDITIONS*>] [<*CONDITIONS*>] [<*CONDITIONS*>]] [action <*ACTIONS*> [<*ACTIONS*>]]

no <GROUP> <RULE> multi

GROUP ····· グループ番号 設定可能範囲は装置種別により異なります

RULE ····· ルール番号 設定可能範囲は装置種別により異なります

CONDITIONS ····· 表 15-1 に示すコンディションを設定します

ACTIONS ····· 表 15-2 に示すアクションを設定します

表 15-1 multi コマンドの設定可能フィルター条件(コンディション)

condition		内容
ipv4	src-ip <IPV4ADDR> | <IPV4ADDR/NETMASK>	送信元 IP アドレスを指定します。 <NETMASK>の入力を省略した場合は、自動で設定されます。
	dst-ip <IPV4ADDR> | <IPV4ADDR/NETMASK>	宛先 IP アドレスを指定します。 <NETMASK>の入力を省略した場合は、自動で設定されます。
	protocol <PROTOCOL> [mask <MASK>]	IPv4 ヘッダーのプロトコル値を指定します。
	src-tcp <TCPPORT>	送信元 TCP ポート番号を指定します。
	dst-tcp <TCPPORT>	宛先 TCP ポート番号を指定します。
	src-udp <UDPPORT>	送信元 UDP ポート番号を指定します。
	dst-udp <UDPPORT>	宛先 UDP ポート番号を指定します。

表 15-2 動作(アクション)

動作(アクション)	内容
permit	フレームの中継を許可します。permit はルールのデフォルトアクションです。

	アクションに counter を設定した場合、自動的に permit が設定されます。 アクションに counter が設定された状態で no コマンドを使用しても permit は削除できません。
deny	フレームの中継を拒否します。permit と deny は同一ルールで使用できません。 アクションに deny および counter が設定されている状態において no コマンドで deny を削除すると、自動的に permit が設定されます。
counter <INDEX>	ルールにマッチしたフレーム数をカウントします。 カウンターはグループ毎に複数個(注)用意されており、ルール毎にカウンターを設定、または、同一カウンターを複数ルール(グループ内)に設定可能です。 (注)：1 グループあたりの index 数 Apresia3400/4300/5400 シリーズ/13000-48X：64 個 Apresia13000-24GX：128 個

16. 制限事項および注意事項

パケットフィルター2 の制限事項および注意事項を 表 16-1 に示します。最新の情報に関しては、リリースノートやフィールドノーティスを参照して下さい。

表 16-1 パケットフィルター2 の制限事項および注意事項

No.	項目	制限事項および注意事項
1	装置種別関連	・装置種別によって、使用可能なグループ数/ルール数/帯域制限エントリー数/カウンター数が異なります。表 2-1 と 表 2-2 を参照して下さい。 ・Apresia13000-48X で帯域制限エントリーを使用する場合には、対象となる受信トラフィックが二つのポートブロック(port 1-24, 50 と port 25-48, 49)を跨がないようにしてご使用下さい。
2	設定関連	・識別条件には併用設定ができない組み合わせがあります。「3.1 識別条件(アサイン)」を参照して下さい。 ・同一ルールに複数のフィルター条件を設定可能ですが、併用設定ができない組み合わせがあります。「3.2 フィルター条件(コンディション)」を参照して下さい。 ・同一ルールに複数のアクションを設定可能ですが、併用設定ができない組み合わせがあります。「4 アクション(動作)」および「6 同一ルールに複数アクション設定時の動作」を参照して下さい。 ・パケットフィルター2 のリソースを自動的に占有する機能がいくつかあります。そのような機能に関する注意点については「12 パケットフィルター2 のリソースを自動的に占有する機能」を参照して下さい。
3	運用関連	・mirror アクションでミラーリング先ポートに指定したポートでトラフィックを受信しても中継しません。これはその mirror アクションを設定しているルールを無効にしても変わらないことに注意して下さい。

17. 各AEOS7 バージョンでの機能追加、変更点

パケットフィルター2 に関する各AEOS7 バージョンでの機能追加、変更点を 表 17-1 にまとめます。最新の情報に関しては、リリースノートやフィールドノーティスを参照して下さい。

表 17-1 各 AEOS7 バージョンでの機能追加、変更点

Version	管理番号	内容
7.02.01	AEOS-70201-RC007	・Apresia13000-48X において、パケットフィルター2 の一部の機能をサポートしました。
7.03.01	AEOS-70301-RC010	・Apresia13000-48X において、パケットフィルター2 の全ての機能をサポートしました。
7.03.01	AEOS-70301-RC012	・パケットフィルター2 において、いくつかの仕様変更/問題修正を行いました。
7.06.01	AEOS-70601-RC020	・Secondary IP アドレスおよび Loopback インターフェースの IP アドレス設定時に占有されるパケットフィルター2 のリソースの数を変更しました。
7.08.01	AEOS-70801-RC001	・Apresia4328GT に対応しました。
7.08.01	AEOS-70801-RC005	・パケットフィルター2 の各グループの占有状況を参照するコマンド“ show packet-filter2 reserved-group ”を追加しました。
7.09.01	AEOS-70901-RC001	・Apresia4348 シリーズに対応しました。
7.10.01	AEOS-71001-RC001	・Apresia13000-24GX-PSR に対応しました(ただし、PIM-SM 除く)。
7.12.01	AEOS-71201-RC001	・Apresia3424 シリーズに対応しました(ただし、L3 機能を除く)。
7.12.01	AEOS-71201-RC002	・パケットフィルター2 のフィルター条件に ARP 送信元 IP アドレス条件(arp-sender-ip)を追加しました。
7.12.01	AEOS-71201-RC005	・MMRP 機能が占有するパケットフィルター2 のリソースを、設定する Ring 数に応じて選択可能にしました(1 グループ占有での利用可能)。
7.12.01	AEOS-71201-RC006	・MMRP-Plus 機能が占有するパケットフィルター2 のリソースを、設定する Ring 数に応じて選択可能にしました(1 グループ占有での利用可能)。
7.14.01	AEOS-71401-RC003	・Apresia4328GT において、IGMP スヌーピング機能及び MLD スヌーピング機能が packet-filter2 のグループを使用しないように変更しました。
7.17.01	AEOS-71701-RC002	・パケットフィルター2 機能において、複数設定を一括して行うコマンド”<GROUP> <RULE> multi”に対応しました。
7.17.01	AEOS-71701-RC008	・IGMP Proxy 機能を packet-filter2 のグループを利用しない方法に変更しました。
7.21.01	AEOS-72101-RC001	・Apresia5412GT-HRSS,Apresia5412GT-HRSS-DC48V,Apresia5412GT-HRSS-DC110V に対応しました。

7.24.01	AEOS-72401-RC002	・パケットフィルター2 機能において、Apresia3400/4328/5400 シリーズで CPU 宛フィルター機能をサポートしました。
7.26.01	AEOS-72601-RC011	・パケットフィルター2 機能において、Apresia3448 シリーズで ”block-cpu-control “ 設定を ”assign port ”で指定しても CPU 宛フィルターが有効にならない問題を修正しました。

18. 受信時のフィルタリング機能

受信時のフィルタリング機能は、識別条件・フィルター条件で指定した対象の受信トラフィックに対してpermitもしくはdenyアクションを適用することにより動作します。アクションの詳細に関しては「4.1 permit」「4.2 deny」を参照して下さい。

フィルタリング機能の簡単な設定方法としては、次の 2 種類の方法が考えられます。

■ 破棄対象を記述する方法
(1) グループ X のルール a において、条件 A に一致した場合は【deny】
(2) グループ X のルール b において、条件 B に一致した場合は【deny】
(3) グループ X のルール c において、条件 C に一致した場合は【deny】

この設定方法の場合は条件 A or B or C に一致した受信トラフィックは破棄されて、それ以外の受信トラフィックは許可されます。

■ 許可対象を記述する方法
(1) グループ X のルール a において、条件 A に一致した場合は【permit】
(2) グループ X のルール b において、条件 B に一致した場合は【permit】
(3) グループ X のルール c において、条件 C に一致した場合は【permit】
(4) グループ X の a, b, c よりも老番のルール n において、全てを【deny】

この設定方法の場合は条件 A or B or C に一致した受信トラフィックは許可されて、それ以外の受信トラフィックは破棄されます。
なお、必ずしも最後のルールにおいて全てを【deny】と定義する必要はありません。例えば、
(1) グループ X のルール a において、「ポート 1 で受信する送信元 IPv4 アドレスが 10.0.10.0/24 のパケット」に一致した場合には【permit】
(2) グループ X のルール a よりも老番のルール n において、「ポート 1 で受信する送信元 IPv4 アドレスが 10.0.0.0/8 のパケット」に一致した場合には【deny】
と設定した場合には、「ポート 1 で受信するトラフィックのうち、送信元 IPv4 アドレスが 10.0.10.0/24 のパケットは許可され、それ以外の送信元 IPv4 アドレスが 10.0.0.0/8 のパケットは破棄されます。更にそれ以外の受信トラフィックは全て許可。」という動作にすることも可能です。

18.1 設定例(1) 破棄対象を記述する方法

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「宛先 MAC アドレス条件と送信元 MAC アドレス条件」を用いた設定例を示します。

■ 設定例内容

・Apresia13000-48X のポート 1～10 で受信するフレームのうち、宛先 MAC アドレスが 00:a1:00:00:00:00～00:a1:00:ff:ff:ff のフレームは破棄、送信元 MAC アドレスが 00:bb:bb:bb:bb:bb のフレームも破棄して、それ以外の受信トラフィックは許可する。
・グループは 1 番を、ルールは若番から順番に使用することとする。また、ethernet コンディションタイプとして使用する。

18.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap13k-48x# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap13k-48x(config)# packet-filter2
Ap13k-48x(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-48x(config-filter)# 1 1 assign port 1-10
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-48x(config-filter)# 1 1 condition ethernet dst mac 00:a1:00:00:00:00
                                                    mask ff:ff:ff:00:00:00
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap13k-48x(config-filter)# 1 1 action deny
```

(5) グループ 1 のルール 2 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-48x(config-filter)# 1 2 assign port 1-10
```

(6) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-48x(config-filter)# 1 2 condition ethernet src mac 00:bb:bb:bb:bb:bb
```

(7) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap13k-48x(config-filter)# 1 2 action deny
```

(8) 設定後の show コマンド結果を示します。

```
Ap13k-48x# show running-config
～中略～
packet-filter2
 1 1 assign port 1-10
```

```
 1 1 condition ethernet dst mac 00:a1:00:00:00:00 mask ff:ff:ff:00:00:00
 1 1 action deny
 1 2 assign port 1-10
 1 2 condition ethernet src mac 00:bb:bb:bb:bb:bb
 1 2 action deny
!
～省略～
Ap13k-48x#
Ap13k-48x# show packet-filter2 group brief
  group assign         condition-type
------------------------------------------------------------------------------
     1 -               ethernet
Ap13k-48x#
Ap13k-48x# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
------------------------------------------------------------------------------
   1    1    Deny       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
------------------------------------------------------------------------------
                           -               -     -
   1    2    Deny       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
------------------------------------------------------------------------------
                           -               -     -

exceeded-action:
group rule    deny
------------------------------------------------------------------------------
   1    1       -
   1    2       -

assign:
group rule assign     port                                        vid vid-m
------------------------------------------------------------------------------
   1    1 port       1-10                                          -     -
   1    2 port       1-10                                          -     -

condition:
group rule condition     dst mac address    src mac address     Type    vid
------------------------------------------------------------------------------
   1    1 ether       00:a1:00:00:00:00                 -        -      -
   1    1 ether-m     ff:ff:ff:00:00:00                 -        -      -
```

```
    1     2 ether                         -  00:bb:bb:bb:bb:bb        -       -
    1     2 ether-m                       -  ff:ff:ff:ff:ff:ff        -       -
～省略～
Ap13k-48x#
```

18.2 設定例(2) 許可対象を記述する方法

識別条件として「グループ全体指定の受信ポートと受信 VLAN」を、フィルター条件として「送信元 MAC アドレスと送信元 IPv4 アドレス」を用いた設定例を示します。

■ 設定例内容

- Apresia3424GT-SS のポート 1, 3, 5 の VLAN 100 で受信するトラフィックのうち、送信元 MAC アドレスが 00:a1:00:00:00:00 のフレームは破棄する。ただし、その中でも送信元 IPv4 アドレスが 10.1.10.0/24 と 10.1.20.0/24 のパケットの場合だけは許可する。それ以外の受信トラフィックは全て許可する。
- グループは 1 番を、ルールは若番から順番に使用することとする。また、src コンディションタイプとして使用する。

18.2.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap3424GT# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap3424GT(config)# packet-filter2
Ap3424GT(config-filter)#
```

(2) グループ 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap3424GT(config-filter)# 1 assign port 1,3,5
Ap3424GT(config-filter)# 1 assign vlan 100
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3424GT(config-filter)# 1 1 condition src ip 10.1.10.0/24
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap3424GT(config-filter)# 1 1 action permit[1]
1) permit アクションは新規にルールを作成した場合には自動的に設定されますが、ここでは例として実施します。実施してもしなくてもどちらでも問題はありません。
```

(5) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3424GT(config-filter)# 1 2 condition src ip 10.1.20.0/24
```

(6) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap3424GT(config-filter)# 1 2 action permit[1]
1) permit アクションは新規にルールを作成した場合には自動的に設定されますが、ここでは例とし
```

て実施します。実施してもしなくてもどちらでも問題はありません。

(7) グループ 1 のルール 3 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3424GT(config-filter)# 1 3 condition src mac 00:a1:00:00:00:00
```

(8) グループ 1 のルール 3 において、「手順(3) アクションの設定」をします。

```
Ap3424GT(config-filter)# 1 3 action deny
```

(9) 設定後の show コマンド結果を示します。

```
Ap3424GT# show running-config
～中略～
packet-filter2
 1 assign port 1,3,5
 1 assign vlan 100 mask 0xfff

 1 1 condition src ip 10.1.10.0/24
 1 1 action permit
 1 2 condition src ip 10.1.20.0/24
 1 2 action permit
 1 3 condition src mac 00:a1:00:00:00:00
 1 3 action deny
!
～省略～
Ap3424GT#
Ap3424GT# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 port/vlan      src
Ap3424GT#
Ap3424GT# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -
    1    2  Permit       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -
```

```
    1    3    Deny       -       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                              -               -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -
    1    2       -
    1    3       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    1    1 port/vlan  1,3,5                                       100 0xfff
    1    2 port/vlan  1,3,5                                       100 0xfff
    1    3 port/vlan  1,3,5                                       100 0xfff

condition:
group rule condition     src mac address   src ip address     Type    vid
-------------------------------------------------------------------------------
    1    1 src                         -        10.1.10.0        -      -
    1    1 src-m                       -    255.255.255.0        -      -
    1    2 src                         -        10.1.20.0        -      -
    1    2 src-m                       -    255.255.255.0        -      -
    1    3 src         00:a1:00:00:00:00                -        -      -
    1    3 src-m       ff:ff:ff:ff:ff:ff                -        -      -
～省略～
Ap3424GT#
```

19. 受信時のQPマッピング機能

受信時のQPマッピング機能は、識別条件・フィルター条件で指定した対象の受信トラフィックに対してqosアクションを適用することにより動作します。これにより特定のトラフィック種類に対してマッピングルールを変更するといったことが可能になります。アクションの詳細に関しては「4.6 qos」を参照して下さい。

19.1 設定例 IP Precedence値からのQPマッピング

識別条件として「ルール毎指定の受信 VLAN」を、フィルター条件として「IP Precedence 値」を用いた設定例を示します。

■ 設定例内容
- Apresia13000-24GX-PSR の全ポートの VLAN 2000 で受信するトラフィックのうち、受信 IPv4 パケットの IP Precedence 値が 0～5 の場合は QoS プロファイル qp1、IP Precedence 値が 6～7 の場合は QoS プロファイル qp7 へマッピングする。
- グループは 1 番を、ルールは若番から順番に使用することとする。また、ipv4 コンディションタイプとして使用する。

19.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap13k-24gx# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap13k-24gx(config)# packet-filter2
Ap13k-24gx(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 assign vlan 2000
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 condition ipv4 tos-precedence 0 mask 0x4[1]
```
1) このマスク指定により 0～3 を指定したことになります。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 action qos qp1
```

(5) グループ 1 のルール 2 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 2 assign vlan 2000
```

(6) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 2 condition ipv4 tos-precedence 4 mask 0x6[1]
```

1) このマスク指定により 4～5 を指定したことになります。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

(7) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap13k-24gx(config-filter)# 1 2 action qos qp1
```

(8) グループ 1 のルール 3 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 3 assign vlan 2000
```

(9) グループ 1 のルール 3 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 3 condition ipv4 tos-precedence 6 mask 0x6[1]
```

1) このマスク指定により 6～7 を指定したことになります。マスク指定の詳細に関しては「3.3 マスク指定」を参照して下さい。

(10)グループ 1 のルール 3 において、「手順(3) アクションの設定」をします。

```
Ap13k-24gx(config-filter)# 1 3 action qos qp7
```

(11)設定後の show コマンド結果を示します。

```
Ap13k-24gx# show running-config
～中略～
packet-filter2
 1 1 assign vlan 2000 mask 0xfff
 1 1 condition ipv4 tos-precedence 0 mask 0x4
 1 1 action qos qp1
 1 1 action permit
 1 2 assign vlan 2000 mask 0xfff
 1 2 condition ipv4 tos-precedence 4 mask 0x6
 1 2 action qos qp1
 1 2 action permit
 1 3 assign vlan 2000 mask 0xfff
 1 3 condition ipv4 tos-precedence 6 mask 0x6
 1 3 action qos qp7
 1 3 action permit
!
～省略～
```

```
Ap13k-24gx#
Ap13k-24gx# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 -              ipv4
Ap13k-24gx#
Ap13k-24gx# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -     qp1       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -              -     -
    1    2  Permit       -     qp1       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -              -     -
    1    3  Permit       -     qp7       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -              -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -
    1    2       -
    1    3       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    1    1 vlan       -                                        2000 0xfff
    1    2 vlan       -                                        2000 0xfff
    1    3 vlan       -                                        2000 0xfff

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    1    1 ipv4                    -              -    -    0 (P)
    1    1 ipv4-m                  -              -    -  0x4 (P)
```

```
    1    2 ipv4                    -               -    -    4 (P)
    1    2 ipv4-m                  -               -    -  0x6 (P)
    1    3 ipv4                    -               -    -    6 (P)
    1    3 ipv4-m                  -               -    -  0x6 (P)

condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 1   1 c    -       -       -
 1   1 m    -       -       -
 1   2 c    -       -       -
 1   2 m    -       -       -
 1   3 c    -       -       -
 1   3 m    -       -       -
～省略～
Ap13k-24gx#
```

20. 送信フレームの 802.1p優先度変更機能

送信フレームの 802.1p優先度変更機能は、識別条件・フィルター条件で指定した対象の受信トラフィックに対してpriorityアクションを適用することにより動作します。これにより、「対象となる受信トラフィックを別のトランクポートからTagフレームとして送信する際に 802.1p優先度の値を書き換える」ことが可能になります。アクションの詳細に関しては「4.7 priority」を参照して下さい。

20.1 設定例

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「宛先MACアドレスとEthernet Type」を用いた設定例を示します。

■ 設定例内容

- Apresia4348GT のポート 1～9 で受信するトラフィックのうち、宛先 MAC アドレスが 00:aa:bb:cc:dd:ee でかつ Ethernet Type が 0x0800(IPv4)と 0x0806(ARP)の場合は、別のトランクポートから Tag フレームとして送信する際に 802.1p 優先度の値を 6 に書き換える。
- グループは 1 番を、ルールは若番から順番に使用することとする。また、dst コンディションタイプとして使用する。

20.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap4348GT# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap4348GT(config)# packet-filter2
Ap4348GT(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap4348GT(config-filter)# 1 1 assign port 1-9
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap4348GT(config-filter)# 1 1 condition dst mac 00:aa:bb:cc:dd:ee
Ap4348GT(config-filter)# 1 1 condition dst type 0x0800
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap4348GT(config-filter)# 1 1 action priority 6
```

(5) グループ 1 のルール 2 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap4348GT(config-filter)# 1 2 assign port 1-9
```

(6) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap4348GT(config-filter)# 1 2 condition dst mac 00:aa:bb:cc:dd:ee
Ap4348GT(config-filter)# 1 2 condition dst type 0x0806
```

(7) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap4348GT(config-filter)# 1 1 action priority 6
```

(8) 設定後の show コマンド結果を示します。

```
Ap4348GT# show running-config
～中略～
packet-filter2
 1 1 assign port 1-9
 1 1 condition dst type 0x800
 1 1 condition dst mac 00:aa:bb:cc:dd:ee
 1 1 action priority 6
 1 1 action permit
 1 2 assign port 1-9
 1 2 condition dst type 0x806
 1 2 condition dst mac 00:aa:bb:cc:dd:ee
 1 2 action priority 6
 1 2 action permit
!
～省略～
Ap4348GT#
Ap4348GT# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 -              dst
Ap4348GT#
Ap4348GT# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -       -       6    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                              -               -     -
    1    2  Permit       -       -       6    -     -              -          -

       routing(        Nexthop        Tracking drop)
```

```
--------------------------------------------------------------------------------
                            -               -     -


exceeded-action:
group rule    deny
--------------------------------------------------------------------------------
    1    1       -
    1    2       -

assign:
group rule assign     port                                      vid vid-m
--------------------------------------------------------------------------------
    1    1 port       1-9                                         -     -
    1    2 port       1-9                                         -     -

condition:
group rule condition     dst mac address   dst ip address     Type    vid
--------------------------------------------------------------------------------
    1    1 dst         00:aa:bb:cc:dd:ee               -    0x800      -
    1    1 dst-m       ff:ff:ff:ff:ff:ff               -   0xffff      -
    1    2 dst         00:aa:bb:cc:dd:ee               -    0x806      -
    1    2 dst-m       ff:ff:ff:ff:ff:ff               -   0xffff      -
～省略～
Ap4348GT#
```

21. 受信時のQPマッピング＋送信フレームの 802.1p優先度変更機能

受信時のQPマッピング機能はqosアクションを使用し、送信フレームの 802.1p優先度変更機能はpriorityアクションを使用してそれぞれ実施可能ですが、qosアクションとpriorityアクションは同一ルールで併用設定できないことに注意して下さい。同一ルールに複数アクションを設定する場合の注意は「6 同一ルールに複数アクション設定時の動作」を参照して下さい。

そのため、これらの機能を同じ対象トラフィックに同時に適用したい場合には 2 個のグループを使用する必要があります。複数グループにマッチした場合の注意に関しては「7 複数グループにマッチした場合の動作」を参照して下さい。

21.1 設定例

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「送信元 IPv4 アドレスと宛先 IPv4 アドレスと IP Precedence 値」を用いた設定例を示します。

■ 設定例内容

- Apresia13000-24GX-PSR のポート 1～24 で受信するトラフィックのうち、送信元 IPv4 アドレスが 10.1.1.0/24 でかつ宛先 IPv4 アドレスが 192.168.100.0/24 でかつ IPv4 ヘッダーの IP Precedence 値が 6 の場合は QoS プロファイル qp7 にマッピングする。さらに、別のトランクポートから Tag フレームとして送信する際に 802.1p 優先度の値を 6 に書き換える。
- グループは 1～2 番を、ルールは若番から順番に使用することとする。また、ipv4 コンディションタイプとして使用する。

21.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap13k-24gx# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap13k-24gx(config)# packet-filter2
Ap13k-24gx(config-filter)#
```

(2) グループ 1 のルール 1 において、手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 assign port 1-24
```

(3) グループ 1 のルール 1 において、手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 condition ipv4 src ip 10.1.1.0/24
Ap13k-24gx(config-filter)# 1 1 condition ipv4 dst ip 192.168.100.0/24
Ap13k-24gx(config-filter)# 1 1 condition ipv4 tos-precedence 6
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap13k-24gx(config-filter)# 1 1 action qos qp7
```

(5) グループ 2 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-24gx(config-filter)# 2 1 assign port 1-24
```

(6) グループ 2 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-24gx(config-filter)# 2 1 condition ipv4 src ip 10.1.1.0/24
Ap13k-24gx(config-filter)# 2 1 condition ipv4 dst ip 192.168.100.0/24
Ap13k-24gx(config-filter)# 2 1 condition ipv4 tos-precedence 6
```

(7) グループ 2 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap13k-24gx(config-filter)# 2 1 action priority 6
```

(8) 設定後の show コマンド結果を示します。

```
Ap13k-24gx# show running-config
～中略～
packet-filter2
 1 1 assign port 1-24
 1 1 condition ipv4 tos-precedence 6
 1 1 condition ipv4 dst ip 192.168.100.0/24
 1 1 condition ipv4 src ip 10.1.1.0/24
 1 1 action qos qp7
 1 1 action permit

 2 1 assign port 1-24
 2 1 condition ipv4 tos-precedence 6
 2 1 condition ipv4 dst ip 192.168.100.0/24
 2 1 condition ipv4 src ip 10.1.1.0/24
 2 1 action priority 6
 2 1 action permit
!
～省略～
Ap13k-24gx#
Ap13k-24gx# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 -              ipv4
      2 -              ipv4
Ap13k-24gx#
Ap13k-24gx# show packet-filter2 1 brief
```

```
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -     qp7       -    -     -             -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                             -              -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    1    1 port       1-24                                          -     -

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    1    1 ipv4              10.1.1.0   192.168.100.0    -    6 (P)
    1    1 ipv4-m       255.255.255.0   255.255.255.0    -  0x7 (P)

condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 1   1 c    -       -       -
 1   1 m    -       -       -
～省略～
Ap13k-24gx#
Ap13k-24gx# show packet-filter2 2 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    2    1  Permit       -       -       6    -     -             -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                             -              -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
```

```
    2    1       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    2    1 port       1-24                                          -     -

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    2    1 ipv4              10.1.1.0   192.168.100.0    -    6 (P)
    2    1 ipv4-m       255.255.255.0   255.255.255.0    -  0x7 (P)

condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 2   1 c    -       -       -
 2   1 m    -       -       -
～省略～
Ap13k-24gx#
```

22. 送信パケットのDSCP値/IP Precedence値変更機能

送信パケットのDSCP値/IP Precedence値変更機能は、識別条件・フィルター条件で指定した対象の受信トラフィックに対してip-tos-dscpもしくはip-tos-precedenceアクションを適用することにより動作します。これにより、「対象となる受信トラフィックを別のポートから送信する際にIPv4 ヘッダーのDSCP値もしくはIP Precedence値を書き換える」ことが可能になります。アクションの詳細に関しては「4.8 ip-tos-dscp」「4.9 ip-tos-precedence」を参照して下さい。

22.1 設定例

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「宛先 IPv4 アドレスと送信元 TCP ポート番号範囲」を用いた設定例を示します。

■ 設定例内容

・ Apresia4328GT のポート 1～24 で受信するトラフィックのうち、宛先 IPv4 アドレスが 10.1.1.100/32 でかつ送信元 TCP ポート番号範囲が 1～1023 のパケットの場合は、別のポートから送信する際に IPv4 ヘッダーの DSCP 値を 48 に書き換える。同様に、宛先 IPv4 アドレスが 10.1.1.200/32 でかつ送信元 TCP ポート番号範囲が 1～1023 のパケットの場合は、別のポートから送信する際に IPv4 ヘッダーの IP Precedence 値を 1 に書き換える。

・ グループは 1 番を、ルールは若番から順番に使用することとする。また、ipv4-src-tcp/udp-range コンディションタイプとして使用する。

22.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap4328GT# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap4328GT(config)# packet-filter2
Ap4328GT(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap4328GT(config-filter)# 1 1 assign port 1-24
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap4328GT(config-filter)# 1 1 condition ipv4 dst ip 10.1.1.100/32
Ap4328GT(config-filter)# 1 1 condition ipv4 src tcp/udp 1-1023 tcp
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap4328GT(config-filter)# 1 1 action ip-tos-dscp 48
```

(5) グループ 1 のルール 2 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap4328GT(config-filter)# 1 2 assign port 1-24
```

(6) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap4328GT(config-filter)# 1 2 condition ipv4 dst ip 10.1.1.200/32
Ap4328GT(config-filter)# 1 2 condition ipv4 src tcp/udp 1-1023 tcp
```

(7) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap4328GT(config-filter)# 1 2 action ip-tos-precedence 1
```

(8) 設定後の show コマンド結果を示します。

```
Ap4328GT# show running-config
～中略～
packet-filter2
 1 1 assign port 1-24
 1 1 condition ipv4 dst ip 10.1.1.100/32
 1 1 condition ipv4 src tcp/udp 1-1023 tcp
 1 1 action ip-tos-dscp 48
 1 1 action permit
 1 2 assign port 1-24
 1 2 condition ipv4 dst ip 10.1.1.200/32
 1 2 condition ipv4 src tcp/udp 1-1023 tcp
 1 2 action ip-tos-precedence 1
 1 2 action permit
!
～省略～
Ap4328GT#
Ap4328GT# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 -              ipv4-src-tcp/udp-range
Ap4328GT#
Ap4328GT# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit dscp-48       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
```

```
                              -               -     -
    1    2  Permit   pre-1       -       -    -     -              -          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                              -               -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -
    1    2       -

assign:
group rule assign     port                                          vid vid-m
-------------------------------------------------------------------------------
    1    1 port       1-24                                           -     -
    1    2 port       1-24                                           -     -

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    1    1 ipv4                     -      10.1.1.100    6        -
    1    1 ipv4-m                   - 255.255.255.255 0xff       -
    1    2 ipv4                     -      10.1.1.200    6        -
    1    2 ipv4-m                   - 255.255.255.255 0xff       -

condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 1   1 c    -       -       - src:1-1023
 1   1 m    -       -       -
 1   2 c    -       -       - src:1-1023
 1   2 m    -       -       -
～省略～
Ap4328GT#
Ap4328GT# show packet-filter2 tcp/udp-range
 range-id  src/dst      port-range
-------------------------------------------------------------------------------
        1      src      1 to  1023
Ap4328GT#
```

23. 受信時の帯域制限機能

受信時の帯域制限機能は、識別条件・フィルター条件で指定した対象の受信トラフィックに対してpolicingアクションとexceeded-action denyを適用することにより動作します。アクションの詳細に関しては「4.10 policingアクション」「4.14 exceed-action denyアクション」を参照して下さい。

policingアクションの設定方法には二種類の設定方法があります(表 4-1 参照)。

23.1 設定例(1) 帯域制限エントリーを自動的に割り当てる方法

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「送信元 IPv6 アドレス」を用いた設定例を示します。帯域制限エントリーは自動的に割り当てる方法を用います。

■ 設定例内容

- Apresia13000-48X のポート 1 で受信するトラフィックのうち、送信元 IPv6 アドレスがfe80::aaaa/128 のパケットを約 100Mbps(99968Kbps)に制限する。バーストサイズは 128Kbyte とする。
- グループは 1 番を、ルールは若番から順番に使用することとする。また、ipv6-src コンディションタイプとして使用する。

23.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap13k-48x# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap13k-48x(config)# packet-filter2
Ap13k-48x(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap13k-48x(config-filter)# 1 1 assign port 1
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap13k-48x(config-filter)# 1 1 condition ipv6 src ip fe80::aaaa/128
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap13k-48x(config-filter)# 1 1 action policing cir 99968
Ap13k-48x(config-filter)# 1 1 action policing cbs 128
```

(5) グループ 1 のルール 1 において、「手順(4) exceeded-action denyの設定」をします。

```
Ap13k-48x(config-filter)# 1 1 exceeded-action deny
```

(6) 設定後の show コマンド結果を示します。

```
Ap13k-48x# show running-config
～中略～
packet-filter2
 1 1 assign port 1
 1 1 condition ipv6 src ip fe80::aaaa/128
 1 1 exceeded-action deny
 1 1 action policing cbs 128
 1 1 action policing cir 99968
 1 1 action permit
!
～省略～
Ap13k-48x#
Ap13k-48x# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 -              ipv6-src-ip
Ap13k-48x#
Ap13k-48x# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir Polic(cir-cbs) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -       -       -    -     -      99968-128          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -              -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1    Deny

assign:
group rule assign     port                                      vid vid-m
-------------------------------------------------------------------------------
    1    1 port       1                                          -     -

condition:
group rule condition  ip address
-------------------------------------------------------------------------------
    1    1 ipv6-src   fe80::aaaa/128
```

```
～省略～
Ap13k-48x#
```

23.2 設定例(2) 帯域制限エントリーを明示的に設定する方法

識別条件として「ルール毎指定の受信ポートと受信 VLAN」を、フィルター条件として「送信元 IPv4 アドレスと宛先 IPv4 アドレス」を用いた設定例を示します。帯域制限エントリーは明示的に割り当てる方法を用います。

■ 設定例内容

・ Apresia3424GT-SS のポート 1 の VLAN 10 で受信するトラフィックのうち、送信元 IPv4 アドレスが 192.168.0.100/32 でかつ宛先 IPv4 アドレスが 172.21.0.0/16 のパケットを約 50Mbps(49984Kbps)に制限する。バーストサイズは 64Kbyte とする。

・ グループは 1 番を、ルールは若番から順番に使用することとする。また、ipv4 コンディションタイプとして使用する。帯域制限エントリーは若番から順番に使用することとする。

23.2.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap3424GT# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap3424GT(config)# packet-filter2
Ap3424GT(config-filter)#
```

(2) グループ 1 のルール 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap3424GT(config-filter)# 1 1 assign port 1
Ap3424GT(config-filter)# 1 1 assign vlan 10
```

(3) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3424GT(config-filter)# 1 1 condition ipv4 src ip 192.168.0.100/32
Ap3424GT(config-filter)# 1 1 condition ipv4 dst ip 172.21.0.0/16
```

(4) グループ 1 のルール 1 において、「手順(3) アクションの設定」をします。

```
Ap3424GT(config-filter)# 1 1 action policing group 1
Ap3424GT(config-filter)# 1 policing 1 cir 49984
Ap3424GT(config-filter)# 1 policing 1 cbs 64
```

(5) グループ 1 のルール 1 において、「手順(4) exceeded-action denyの設定」をします。

```
Ap13k-48x(config-filter)# 1 1 exceeded-action deny
```

(6) 設定後の show コマンド結果を示します。

```
Ap3424GT# show running-config
```

```
～中略～
packet-filter2
 1 policing 1 cbs 64
 1 policing 1 cir 49984

 1 1 assign port 1
 1 1 assign vlan 10 mask 0xfff
 1 1 condition ipv4 dst ip 172.21.0.0/16
 1 1 condition ipv4 src ip 192.168.0.100/32
 1 1 action policing group 1
 1 1 action permit
!
～省略～
Ap3424GT#
Ap3424GT# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
     1 -              ipv4
Ap3424GT#
Ap3424GT# show packet-filter2 1 brief
action:
group rule    deny     tos QosProf    Prio Mirr Redir  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
    1    1  Permit       -       -       -    -     -           1-1          -

       routing(        Nexthop        Tracking drop)
-------------------------------------------------------------------------------
                            -               -     -

exceeded-action:
group rule    deny
-------------------------------------------------------------------------------
    1    1       -

assign:
group rule assign     port                                        vid vid-m
-------------------------------------------------------------------------------
    1    1 port/vlan  1                                           10 0xfff

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    1    1 ipv4         192.168.0.100      172.21.0.0    -        -
    1    1 ipv4-m     255.255.255.255     255.255.0.0    -        -
```

```
condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 1   1 c    -       -       -
 1   1 m    -       -       -
～省略～
Ap3424GT#
Ap3424GT# show packet-filter2 policing 1
   group  m-id       cir    cbs rule
-------------------------------------------------------------------------------
       1     1     49984     64 1
       1     2  33554368      4
       1     3  33554368      4
～省略～
Ap3424GT#
```

24. 受信時のCPU宛フィルター機能

受信時のCPU宛フィルター機能は、識別条件・フィルター条件で指定した対象のCPU宛トラフィックに対してblock-cpu-controlアクションを適用することにより動作します。アクションの詳細に関しては「4.5 block-cpu-control」を参照して下さい。

24.1 設定例

識別条件として「ルール毎指定の受信ポート」を、フィルター条件として「送信元 IPv4 アドレス」を用いた設定例を示します。

■ 設定例内容
- Apresia3448GT のポート 1 で受信する CPU 宛トラフィックのうち、送信元 IPv4 アドレスが 192.168.10.0/24 のフレームをフィルタリングする。
- ポート 1 で受信する CPU 宛トラフィックのうち、送信元 IPv4 アドレスが 192.168.10.100/32 の TELNET フレームを若番ルールでの none アクションにより、フィルタリングから除外する(CPU 宛フィルターグループでルールを新規に作成するとき、noneアクションが自動的に設定されるため、明示的な設定は不要)。
- グループ 1、2 を CPU 宛フィルターグループで使用する。

24.1.1 設定手順

(1) PACKETFILTER2 モードに移行します。

```
Ap3448GT# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ap3448GT(config)# packet-filter2
Ap3448GT(config-filter)#
```

(2) グループ 1、2 を CPU 宛フィルターグループに設定します。

```
Ap3448GT(config-filter)# block-cpu-control 1 2 enable
```

(3) グループ 1 において、「手順(1) 識別条件(アサイン)の設定」をします。

```
Ap3448GT(config-filter)# 1 assign port 1
```

(4) グループ 1 のルール 2 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3448GT(config-filter)# 1 2 condition ipv4 src ip 192.168.10.0/24
```

(5) グループ 1 のルール 2 において、「手順(3) アクションの設定」をします。

```
Ap3448GT(config-filter)# 1 2 action block-cpu-control
```

(6) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3448GT(config-filter)# 1 1 condition ipv4 src ip 192.168.10.100/32
```

(7) グループ 1 のルール 1 において、「手順(2) フィルター条件(コンディション)の設定」をします。

```
Ap3448GT(config-filter)# 1 1 condition ipv4 dst tcp/udp 23 tcp
```

(8) 設定後の show コマンド結果を示します。

```
Ap3448GT# show running-config
～中略～
packet-filter2
 block-cpu-control 1 2 enable

 1 assign port 1
 2 assign port 1

 1 1 condition ipv4 dst tcp/udp 23 tcp
 1 1 condition ipv4 src ip 192.168.10.100/32
 1 1 action none
 1 2 condition ipv4 src ip 192.168.10.0/24
 1 2 action none
 1 2 action block-cpu-control

 2 1 condition ipv4 dst tcp/udp 23 tcp
 2 1 condition ipv4 src ip 192.168.10.100/32
 2 1 action none
 2 2 condition ipv4 src ip 192.168.10.0/24
 2 2 action none
 2 2 action block-cpu-control
!
～省略～
Ap3448GT#
Ap3448GT# show packet-filter2 group brief
  group assign         condition-type
-------------------------------------------------------------------------------
      1 port           ipv4
      2 port           ipv4
Ap3448GT#
Ap3448GT# show packet-filter2 1 brief
action:
group rule    deny     CPU  Polic(grp-id) counter(U)
-------------------------------------------------------------------------------
```

```
    1    1    None       -              -          -
    1    2    None    Block             -          -

exceeded-action:
group rule    deny     CPU
-------------------------------------------------------------------------------
    1    1       -       -
    1    2       -       -

assign:
group rule assign     port                                      vid vid-m
-------------------------------------------------------------------------------
    1    1 port       1                                           -     -
    1    2 port       1                                           -     -

condition:
group rule condition   src ip address  dst ip address Prot tos(P/D)
-------------------------------------------------------------------------------
    1    1 ipv4        192.168.10.100              -    6        -
    1    1 ipv4-m     255.255.255.255              - 0xff        -
    1    2 ipv4          192.168.10.0              -    -        -
    1    2 ipv4-m       255.255.255.0              -    -        -

condition tcp/udp:
 G   R T Flag S-t/u-p D-t/u-p tcp/udp-ranges(src/dst)
-------------------------------------------------------------------------------
 1   1 c    -       -      23
 1   1 m    -       -  0xffff
 1   2 c    -       -       -
 1   2 m    -       -       -
～省略～
Ap3448GT#
```

AEOS Ver. 7 アプリケーションノート
(パケットフィルター2 編)

2009 年 11 月 初版
2012 年 6 月 第 7 版

日立電線株式会社
東京都千代田区外神田四丁目 14 番 1 号
秋葉原 UDX