

日立電線スイッチングハブ

Apresia13000/13100/13200/15000 シリーズ

AEOS Ver. 8 アプリケーションノート

(パケットフィルター2 編)

制定・改訂履歴表

No.	年 月 日	内 容
-	2010年9月13日	<ul style="list-style-type: none"> •新規作成
A	2011年3月30日	<ul style="list-style-type: none"> •タイトルを修正 •適用機種一覧表を修正 •表 1-1 パケットフィルタ-2のグループ数を修正 •表 1-2 グループあたりのルール/帯域制限エントリ-/カウンター数を修正 •表 1-3 コンディションタイプと関係するコマンドを削除 •表 1-4 コンディションタイプと関連コマンドおよびフィルタ-条件(コンディション)を修正 •表 1-5 IPv4 関連のフィルタ-条件(コンディション)を修正 •表 1-6 IPv6 関連のフィルタ-条件(コンディション)を修正 •表 1-11 占有するグループ数と算出値の関係を修正 •表 1-12 占有するグループ数とポート数を修正 •表 1-13 最大ルール数と占有するグループ数を修正 •表 1-14 識別条件(アサイン)の設定項目を修正 •表 1-16 アクションの設定項目を修正 •表 1-18 各機能が占有するグループ数を削除 •1.3.2.7 クラス ID 条件を追加 •1.4.3 qos アクションを修正 •1.4.12 none アクションを修正 •1.9 TCP/UDP ポート番号範囲指定エントリ-を修正 •1.10 ワイドモードを追加 •1.11.1 IP アドレス機能を修正 •1.11.2 ユーザーループ検知機能を修正 •1.11.3 MMRP-Plus 機能を修正 •1.11.4 AccessDefender 機能を修正 •1.11.5 Flush FDB 機能を修正 •1.13.2 手順(2) フィルタ-条件(コンディション)の設定を修正
B	2012年6月8日	<ul style="list-style-type: none"> •全体の章構成を変更 •はじめにの説明文を修正 •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を設定した場合の動作図(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を設定した場合の動作図(CPU 宛フィルタ-グループ)を追加 •図 11-1 IPv6 パケット構成を追加 •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-条件(コン

No.	年 月 日	内 容
		<p>ディション)を修正</p> <ul style="list-style-type: none"> •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を設定した場合の注意点を修正 •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を修正 •表 14-2 フィルター条件(コンディション)の設定項目を修正 •表 14-3 アクションの設定項目を修正 •表 14-4 その他の設定項目を修正 •表 17-1 各 AEOS8 バージョンでの機能追加、変更点を修正 <ul style="list-style-type: none"> •1 概要を修正 •3.2.2 VLAN ID 条件を修正 •3.2.3 Customer VLAN ID 条件を追加 •3.2.4 VLAN priority 条件を追加 •3.2.5 Ethernet Type 条件を修正 •3.2.6 ARP 送信元 IP アドレス(arp-sender-ip)条件を修正 •3.2.7 IPv4 関連の条件を修正 •3.2.8 IPv6 関連の条件を修正 •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 •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 アクションを修正 •4.5 block-cpu-control アクションを追加 •4.10 policing アクションを修正 •4.13 mirror アクションを修正 •5 CPU 宛フィルター機能を追加 •6 同一ルールに複数アクションを設定した場合の注意を修正 •6.1 通常グループを追加 •6.2 CPU 宛フィルターグループを追加 •11 IPv6 ヘッダーNext Header フィールドの対象箇所を追加 •12 ワイドモードを修正 •13.1 IP アドレス機能を修正 •13.4 MMRP-Plus transmit-fdb-flush 受信機能を追加 •13.7 BFS 機能を追加 •13.8 FCoE Forwarder 機能を追加 •13.9 MLAG 機能を追加 •15.2 手順(2) フィルター条件(コンディション)の設定を修正 •15.3 手順(3) アクションの設定を修正 •24. 受信時の CPU 宛フィルター機能を追加

No.	年 月 日	内 容
		<ul style="list-style-type: none">•24.1 設定例を追加•24.1.1 設定手順を追加

目次

制定・改訂履歴表	1
はじめに	7
1. 概要	8
2. グループ	9
3. ルール	10
3.1 識別条件(アサイン)	10
3.2 フィルター条件(コンディション)	11
3.2.1 宛先MACアドレス条件、送信元MACアドレス条件	13
3.2.2 VLAN ID条件	13
3.2.3 Customer VLAN ID条件	14
3.2.4 VLAN priority条件	15
3.2.5 Ethernet Type条件	15
3.2.6 ARP送信元IPアドレス(arp-sender-ip)条件	15
3.2.7 IPv4 関連の条件	16
3.2.8 IPv6 関連の条件	18
3.2.9 クラスID条件	19
3.3 マスク指定	20
3.3.1 16進設定値に対するマスク指定	20
3.3.2 10進設定値に対するマスク指定	21
4. アクション(動作)	24
4.1 permitアクション	24
4.2 denyアクション	24
4.3 noneアクション	24
4.4 authentication-bypassアクション	26
4.5 block-cpu-controlアクション	26
4.6 qosアクション	26
4.7 priorityアクション	27
4.8 ip-tos-dscpアクション	27
4.9 ip-tos-precedenceアクション	28
4.10 policingアクション	28
4.11 redirectアクション	29
4.12 counterアクション	30
4.13 mirrorアクション	30
4.14 exceeded-action denyアクション	30
5. CPU宛フィルター機能	31
6. 同一ルールに複数アクションを設定した場合の注意	33
6.1 通常グループ	33
6.2 CPU宛フィルターグループ	36

7. 複数のグループにマッチした場合の注意	37
8. 帯域制限エントリー	38
9. カウンター	39
10. TCP/UDPポート番号範囲指定エントリー	40
11. IPv6 ヘッダーNext Headerフィールドの対象箇所	42
12. ワイドモード	44
13. パケットフィルタ2のリソースを自動的に占有する機能	45
13.1 IPアドレス機能	45
13.2 ユーザループ検知機能	47
13.3 MMRP-Plus機能	48
13.4 MMRP-Plus transmit-fdb-flush受信機能	49
13.5 AccessDefender機能	50
13.6 Flush FDB機能	52
13.7 BFS機能	53
13.8 FCoE Forwarder機能	54
13.9 MLAG機能	55
14. 設定項目	56
15. 設定手順	60
15.1 手順(1) 識別条件(アサイン)の設定	60
15.2 手順(2) フィルタ条件(コンディション)の設定	60
15.3 手順(3) アクションの設定	64
15.4 手順(4) exceeded-action denyの設定	66
15.5 手順(5) ルール毎の有効/無効設定	66
16. 制限事項および注意事項	67
17. 各AEOS8バージョンでの機能追加、変更点	68
18. 受信時のフィルタリング機能	73
18.1 設定例(1) 破棄対象を記述する方法	74
18.1.1 設定手順	74
18.2 設定例(2) 許可対象を記述する方法	77
18.2.1 設定手順	77
19. 受信時のQPマッピング機能	80
19.1 設定例(1) IP Precedence値からのQPマッピング	80
19.1.1 設定手順	80
20. 送信フレームの802.1p優先度変更機能	84
20.1 設定例(1) 送信フレームの802.1p優先度変更機能	84
20.1.1 設定手順	84
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	87
21.1 設定例(1) 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	87
21.1.1 設定手順	87
22. 送信パケットのDSCP値/IP Precedence値変更機能	91


22.1 設定例(1) 送信パケットのDSCP値/IP Precedence値変更機能	91
22.1.1 設定手順	91
23. 受信時の帯域制限機能	94
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	94
23.1.1 設定手順	94
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	95
23.2.1 設定手順	96
24. 受信時のCPU宛フィルター機能	99
24.1 設定例	99
24.1.1 設定手順	99

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. 8 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
Apresia13000 シリーズ	Apresia13000-X24-PSR	8.15.01
Apresia13100 シリーズ	Apresia13100-48X-PSR	
Apresia13200 シリーズ	Apresia13200-48X-PSR	
	Apresia13200-52GT-PSR	
	Apresia13200-52GT	
Apresia15000 シリーズ	Apresia15000-32XL-PSR	
	Apresia15000-64XL-PSR	

 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。

Apresia は、日立電線株式会社の登録商標です。

AEOS は、日立電線株式会社の登録商標です。

MMRP は、日立電線株式会社の登録商標です。

AccessDefender は、日立電線株式会社の登録商標です。

イーサネットは、富士ゼロックス株式会社の登録商標です。

その他の社名、ブランド名および商品名は、各所有者の商標もしくは登録商標です。

1. 概要

パケットフィルタ-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-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 RPVST+機能が有効な場合の PVST フレーム、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 が無効かつ BPDU 転送制限機能が無効な場合の BPDU フレーム、RPVST+機能が有効かつ BPDU 転送制限機能が無効な場合の PVST フレーム)。
 - 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(装置宛での 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-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宛フィルタ機能」

これらはパケットフィルタ-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-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「13 パケットフィルタ-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-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/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-2のグループ数

No.	製品種別	グループ数
1	Apresia13000-X24-PSR	11
2	Apresia13100-48X-PSR Apresia13200 シリーズ	14
3	Apresia15000 シリーズ	9

表 2-2 グループあたりのルール/帯域制限エントリ/カウンター数

No.	製品種別	ルール数	帯域制限 エントリ数	カウンター数
1	Apresia13000-X24-PSR	グループ 1-3 : 256 グループ 4-11 : 128	64	64
2	Apresia13100-48X-PSR Apresia13200 シリーズ	512	64	64
3	Apresia15000 シリーズ	グループ 1-5 : 256 グループ 6-9 : 128	64	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条件に用いるコンディショントイプを共有します。このコンディショントイプとは、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、コンディショント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。

コンディショント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条件を設定した際に自動的にコンディショントイプが定義されます。それぞれのコンディショントイプでどのようなフィルタ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。

グループ毎に異なるコンディショント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 複数のグループにマッチした場合の注意」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	-	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	-	-	-	<ul style="list-style-type: none"> 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	-	-	<ul style="list-style-type: none"> 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	-	-	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 「受信ポート」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

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	
					ては当該ルールのみ対象となります。
8	-	設定有	設定有	-	<ul style="list-style-type: none"> 「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ついては表 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・Customer VLAN ID・Ethernet Type・宛先 IPv4 アドレス <ul style="list-style-type: none"> 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・Customer VLAN ID・Ethernet Type・送信元 IPv4 アドレス・ARP 送信元 IP アドレス <ul style="list-style-type: none"> 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・Customer 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
		<ul style="list-style-type: none"> 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 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ります。 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	<p><GROUP> <RULE> condition ipv4 src tcp/udp 関連コマンド</p> <ul style="list-style-type: none"> 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	<p><GROUP> <RULE> condition ipv4 dst tcp/udp 関連コマンド</p> <ul style="list-style-type: none"> 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	<p><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</p> <ul style="list-style-type: none"> 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ります。 wide-mode 使用時のみ指定可能です。
8	ipv6-any	<p><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</p> <ul style="list-style-type: none"> 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	<p><GROUP> <RULE> condition ipv6 src ip 関連コマンド 送信元 IPv6 アドレス</p> <ul style="list-style-type: none"> 送信元 IPv6 アドレス条件は、対象が IPv6 パケット(Ethernet Type = 0x86DD)

No.	タイプ	関連コマンドおよびコンディション
		の場合に有効です。
10	ipv6-dst-ip	<GROUP> <RULE> condition ipv6 dst ip 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-src-tcp /udp-range	<GROUP> <RULE> condition ipv6 src tcp/udp 関連コマンド 送信元 TCP/UDP ポート番号 •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。 •wide-mode 使用時のみ指定可能です。
12	ipv6-dst-tcp /udp-range	<GROUP> <RULE> condition ipv6 dst tcp/udp 関連コマンド 宛先 TCP/UDP ポート番号 •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。 •wide-mode 使用時のみ指定可能です。
13	class	<GROUP> <RULE> condition class 認証端末のクラス ID

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-2の VLAN ID 条件」が一致した場合に対象となります。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-2の VLAN ID 条件」が一致した場合に対象となります。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-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-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 Customer VLAN ID条件

Customer 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。「c-vid 指定」と「none 指定」による 2 種類の設定方法が存在します。

「VLAN ID 条件」がサービスタグの VLAN ID を対象とするのに対し、「Customer VLAN ID 条件」ではカスタマータグの VLAN ID を対象とします。本装置ではカスタマータグの TPID が 0x8100 のフレームのみをカスタマータグ付きフレームとして認識します。

「c-vid 指定」では、「受信トラフィックのカスタマータグ(inner tag)の VID 情報」と「パケットフィルタ-2 の Customer VLAN ID 条件」が一致した場合に対象となります。

「none 指定」では、「カスタマータグ無しフレーム(カスタマータグの TPID が 0x8100 ではないフレームを含む)」がフィルタの対象となります。

ただし、「VLAN ID 条件」に記載の “ignore-tag enable” を設定した装置のアクセスポートに対する VLAN タグ付きフレームの受信時や、装置の TPID と異なる VLAN タグ付きフレームの受信時のように、受信トラフィックを装置が Untag フレームとして認識するような場合には、「受信トラフィックのサービスタグ(Outer Tag)の VID 情報」がフィルタの対象となることに注意してください。

なお、同一ルール内では「c-vid 指定」と「none 指定」の Customer VLAN ID 条件を併用して設定は

できません。

Customer 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。

3.2.4 VLAN priority条件

VLAN priority 条件は、「VLAN ID 条件」または「Customer VLAN ID 条件」のオプションとして使用可能です。

指定した「VLAN ID 条件」または「Customer VLAN ID 条件」に加え、「対象トラフィックの 802.1p VLAN プライオリティ情報」と「パケットフィルタ-2 の VLAN priority 条件」も一致した場合に対象となります。

VLAN priority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。

3.2.5 Ethernet Type条件

Ethernet Type 条件は dst、src、ethernet コンディショント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。

3.2.6 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 コンディショント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。

3.2.7 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	<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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。

No.	condition	概要
		<p>す。</p> <ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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)	<ul style="list-style-type: none"> •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。 •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)	<ul style="list-style-type: none"> •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

No.	condition	概要
		<p>ては自動的に任意の値としてマスクが設定されます。</p> <ul style="list-style-type: none"> •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。

3.2.8 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)	<ul style="list-style-type: none"> •ipv6-any 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)	<ul style="list-style-type: none"> •ipv6-any 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)	<ul style="list-style-type: none"> •ipv6-any 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 フィールドの対象箇所に関しては「11 IPv6 ヘッダーNext Header フィールドの対象箇所」を参照してください。 •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)	<ul style="list-style-type: none"> •ipv6-any 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 (icmp type)	<ul style="list-style-type: none"> •ipv6-any 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	<ul style="list-style-type: none"> •ipv6-src-ip コンディションタイプのルールで使用可能です。

No.	condition	概要
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> ipv6-dst-ip 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	<ul style="list-style-type: none"> ipv6、ipv6-src-tcp/udp-range コンディションタイプのルールで使用可能です。 ipv6 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。ipv6-src-tcp/udp-range コンディションタイプの場合は範囲指定します。 オプションで TCP 指定もしくは UDP 指定が可能です。 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	<ul style="list-style-type: none"> ipv6、ipv6-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。 ipv6 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。ipv6-dst-tcp/udp-range コンディションタイプの場合は範囲指定します。 オプションで TCP 指定もしくは UDP 指定が可能です。 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。

3.2.9 クラスID条件

指定したクラス ID 条件が認証端末のクラス ID 情報と一致した場合に対象となります。

AccessDefender で認証された端末に対してクラス ID が付与されている場合、クラス ID をフィルター条件に指定することができ、認証端末毎のパケットフィルター2 適用が可能となります(ユーザーポリシーコントロール)。クラス ID は RADIUS サーバーまたはローカルデータベースに設定することにより端末へ付与されます。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。

クラス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。

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 Ethernet 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 条件や VLAN priority 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 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 0xffff 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を設定した場合の注意」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 複数のグループにマッチした場合の注意」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。

 除外したいフィルター条件には、他のルール番号よりも若番のルールを設定する必要があります。

例 1

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

この場合、port 1/1 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 pbr にすれば、特定端末を PBR 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
1 2 action deny
1 2 condition src vid 1
1 2 assign port 1/1
```

access-defender

packet-filter2 group 6

packet-filter2 max-rule 100

mac-authentication port 1/1

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 には認証バイパス動作をしません(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 には認証バイパス動作をします(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-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-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-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-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 exceeded-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。

policing アクションを設定可能なパケットフィルター2 のグループ数は Apresia13000/15000 シリーズが 4 グループ、Apresia13100/13200 シリーズが 14 グループです。

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	<ul style="list-style-type: none">•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。•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	<ul style="list-style-type: none">•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>

No.	設定方法	概要
		<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •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」	<ul style="list-style-type: none"> •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中継するトラフィック」	<ul style="list-style-type: none"> •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。 •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 exceeded-action denyアクション

exceeded-actionは帯域制限エントリ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。

「12 ワイドモード」との併用時は、wide-mode設定のあるグループ同士を、CPU宛フィルター機能で使用するグループに指定してください。ワイドモードはグループを連番で2つ使用するため、CPU宛フィルター機能の設定には、パケットフィルター2 のグループが4個必要になります。ワイドモードを複数設定できない、Apresia13000 シリーズではワイドモードと併用できません。

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/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
```

```
-----
```

```
1/1  Packet-filter2 (block-cpu-control with  1/2 )
```

```
1/2  Packet-filter2 (block-cpu-control with  1/1 )
```

```
(中略)
```

グループ 1、3 を CPU 宛フィルターグループに指定 (ワイドモード併用時)

```
wide-mode 1
```

```
wide-mode 3
```

```
block-cpu-control 1 3 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 wide-mode pf2 (block-cpu-control with X/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

1/1	wide-mode pf2 (block-cpu-control with 1/3)
1/2	wide-mode pf2
1/3	wide-mode pf2 (block-cpu-control with 1/1)
1/4	wide-mode pf2
(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。

6. 同ルールに複数アクションを設定した場合の注意

アクションは同ルールに複数設定することが可能(" 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。

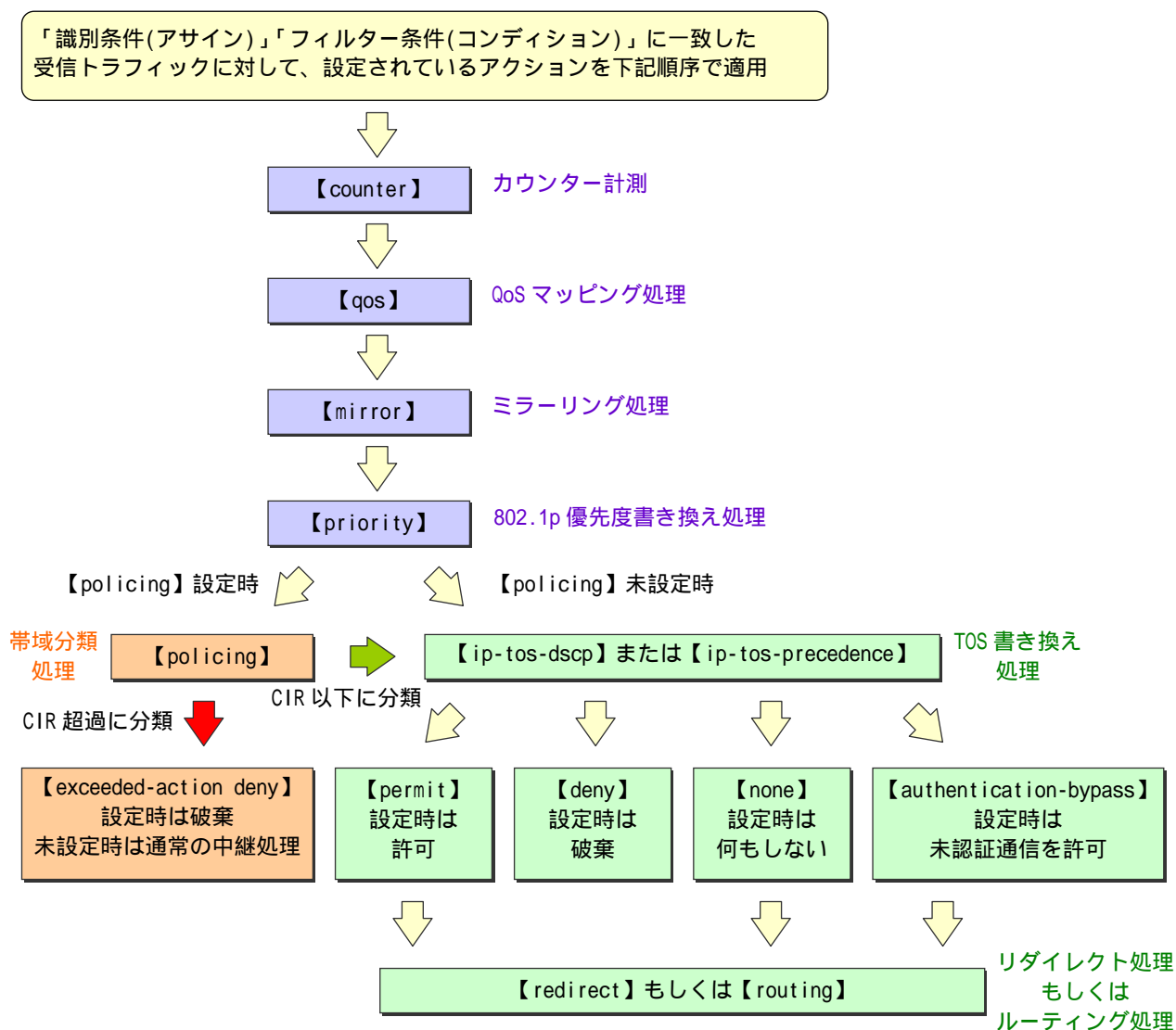


図 6-1 同ルールに複数アクションを設定した場合の動作図(通常グループ)

表 6-1 に同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を設定した場合の注意点

No.	Action	注意点
1	permit	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【permit】【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
3	none	<ul style="list-style-type: none"> •【block-cpu-control】【counter】を除く、他のアクションとの併用は未サポート
4	authentication-bypass	<ul style="list-style-type: none"> •【permit】【deny】【none】と併用設定は不可 •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
5	block-cpu-control	<ul style="list-style-type: none"> •【none】【counter】を除く、他のアクションとの併用設定は不可
6	qos	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •他の全てのアクションと併用設定が可能
13	mirror	<ul style="list-style-type: none"> •【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

No.	Action	注意点
		•【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。

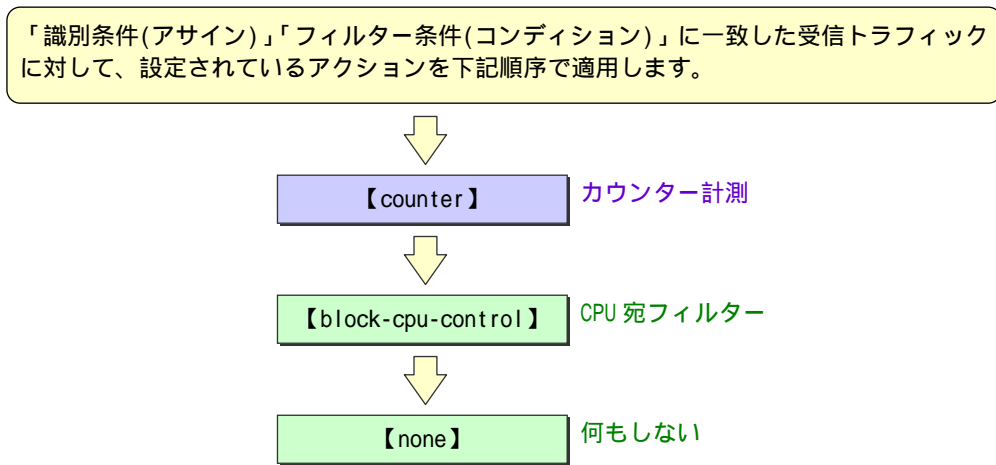


図 6-2 同一ルールに複数アクションを設定した場合の動作図(CPU 宛フィルターグループ)

7. 複数のグループにマッチした場合の注意

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を設定した場合の注意」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	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •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/老番グループの両方が動作します。
3	policing とその他のアクション	<ul style="list-style-type: none"> •【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	<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •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 exceeded-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。

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-dst-tcp/udp-range、ipv6-src-tcp/udp-range コンディショント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。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. IPv6 ヘッダーNext Headerフィールドの対象箇所

conditionコマンドのipv6 next-headerでは、図 11-1に示す次ヘッダーの値を対象として動作します。次ヘッダーは基本ヘッダー部と言われるもので、必要に応じて拡張ヘッダー部がこの後に追加されます。この拡張ヘッダー部の追加される数により、対象とする箇所が機種により異なります。

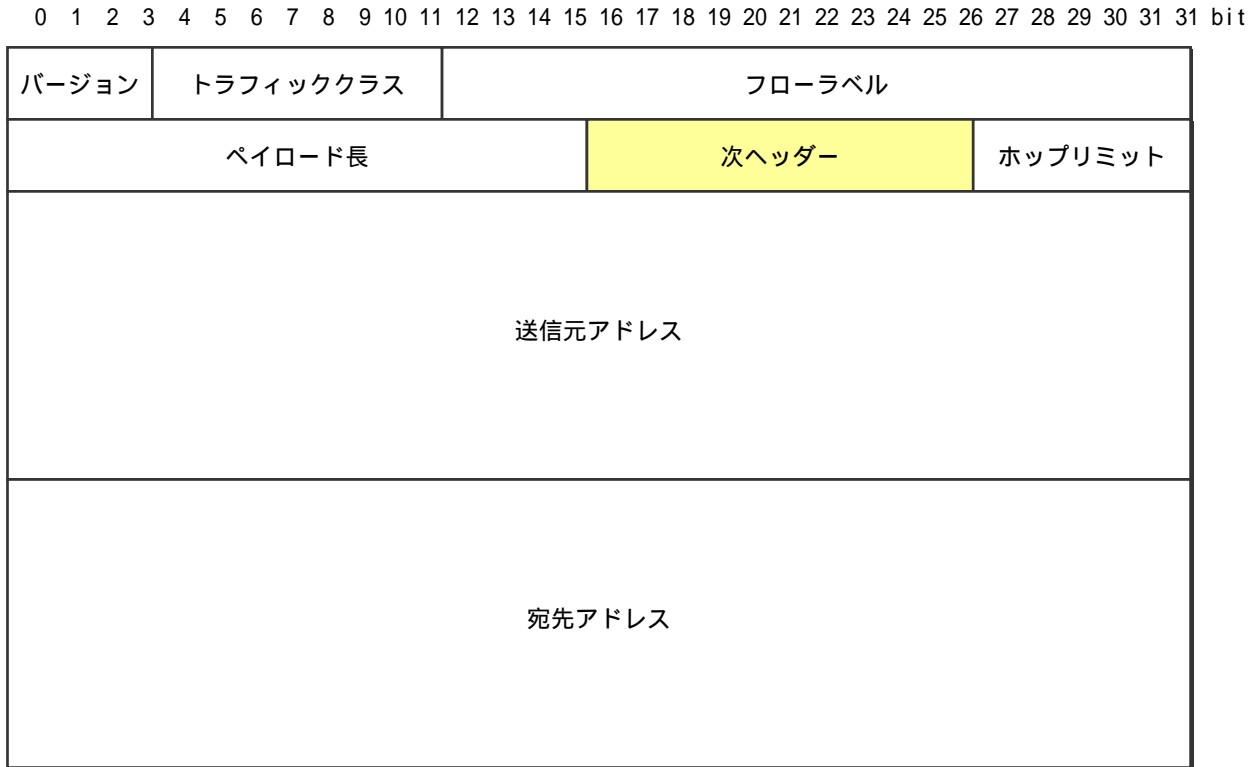
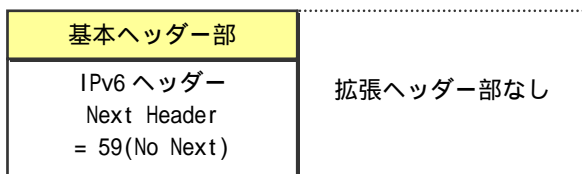


図 11-1 IPv6 パケット構成

パターン1 基本ヘッダー部のみで、拡張ヘッダーがない場合



全機種共通

基本ヘッダー部内のNext Header の値

上記の例では、基本ヘッダー部内のNext Header の値：59を対象とします。

パターン 2 基本ヘッダー部 + 拡張ヘッダー部 1 の場合

基本ヘッダー部	拡張ヘッダー部 1
IPv6 ヘッダー Next Header = 6(TCP)	6(TCP)ヘッダー Next Header = 59(No Next)

全機種共通

拡張ヘッダー部 1 内の Next Header の値

上記の例では、拡張ヘッダー部 1 内の Next Header の値 : 59 を対象とします。

パターン 3 基本ヘッダー部 + 拡張ヘッダー部 1、2 の場合

基本ヘッダー部	拡張ヘッダー部 1	拡張ヘッダー部 2
IPv6 ヘッダー Next Header = 43(Routing)	43(Routing)ヘッダー Next Header = 6(TCP)	6(TCP)ヘッダー Next Header = 59(No Next)

Apresia13000/13100/13200 シリーズの場合

拡張ヘッダー部 1 内の Next Header の値

上記の例では、拡張ヘッダー部 1 内の Next Header の値 : 6 を対象とします。

Apresia15000 シリーズの場合

拡張ヘッダー部 2 内の Next Header の値

上記の例では、拡張ヘッダー部 2 内の Next Header の値 : 59 を対象とします。

パターン 4 基本ヘッダー部 + 拡張ヘッダー部 1~3 の場合

基本ヘッダー部	拡張ヘッダー部 1	拡張ヘッダー部 2	拡張ヘッダー部 3
IPv6 ヘッダー Next Header = 43(Routing)	43(Routing)ヘッダー Next Header = 44(Fragment)	44(Fragment)ヘッダー Next Header = 6(TCP)	6(TCP)ヘッダー Next Header = 59(No Next)

Apresia13000/13100/13200 シリーズの場合

拡張ヘッダー部 1 内の Next Header の値

上記の例では、拡張ヘッダー部 1 内の Next Header の値 : 44 を対象とします。

Apresia15000 シリーズの場合

拡張ヘッダー部 2 内の Next Header の値

上記の例では、拡張ヘッダー部 2 内の Next Header の値 : 6 を対象とします。

以降、拡張ヘッダーが 3 以上追加された場合もパターン 4 の動作となります。

12. 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。Apresia13000/13100/13200シリーズのワイドモード使用時の最大ルール数は指定したグループの最大ルール数の1/2です。

ワイドモードの設定

```
wide-mode <GROUP>
```

```
GROUP ..... グループ番号
```

```
Apresia13000 シリーズ : <2>
```

```
Apresia13100/13200 シリーズ : <奇数グループ>
```

```
Apresia15000 シリーズ : <偶数グループ>
```

設定例

```
(config-filter)# wide-mode 2
```

```
(config-filter)# 2 1 condition ipv6 dst ip 3ffe:506::1/128
```

```
(config-filter)# 2 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)を同一ルールに設定可能です。

13. パケットフィルタ-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-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-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-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-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。

13.1 IPアドレス機能

VLANインターフェース/ループバック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13-1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プライマリーIPアドレス設定の数) + (VLANインターフェースのセカンダリーIPアドレス設定の数) + (ループバックインターフェースに設定したIPアドレスの数) + 3(装置予約 ¹⁾)

1) AEOS8.08.01以降は3、それ以前のバージョンでは7です。

表 13-1 占有するグループ数と算出値の関係

占有するグループ数	算出値		
	Apresia13000シリーズ	Apresia13100/13200シリーズ	Apresia15000シリーズ
0	0-256	0-1024	0-256
1	257-512	1025-1536	257-512
2	513-768	-	513-768
3	769-1024	-	769-1024
4	1025-1152	-	1025-1280
5	1153-1280	-	-

以下にIPアドレスの最大設定数を示します。

- ループバックインターフェースに設定可能なIPアドレスは最大14個(CLI禁則あり)

- Apresia13000/13100/13200 シリーズにおける、VLAN インターフェースに設定可能なプライマリ IP アドレス設定は最大 1024 個 (CLI 禁則あり)
- Apresia15000 シリーズにおける、VLAN インターフェースに設定可能なプライマリ IP アドレス設定は最大 255 個 (CLI 禁則あり)
- VLAN インターフェースにセカンダリ IP アドレス設定する場合、最大 1000 個以下を推奨 (CLI 禁則なし)

装置に登録可能な IP アドレス総数(プライマリ/セカンダリ/ループバック)は 1269 個までのため、最大設定数は各 IP アドレスの設定数により変動します。

13.2 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若番のグループが 1 個占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。

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
```

```
Apresia13000 シリーズ : <1-11>
```

```
Apresia13100/13200 シリーズ : <1-14>
```

```
Apresia15000 シリーズ : <1-9>
```


13.3 MMRP-Plus機能

MMRP-Plus 機能の設定を行うと 1-3 グループ占有します。“ show packet-filter2 reserved-group ”では「MMRP」と表示されます。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。指定しない場合は自動的にまだ他の機能で使用されていない最若番のグループが 1 個占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。表 13-2 に占有するグループ数と設定可能なRing数を示します。

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
	Apresia13000 シリーズ : <1-11>
	Apresia13100/13200 シリーズ : <1-14>
	Apresia15000 シリーズ : <1-9>
NUMBER	占有するグループ数指定オプション
	Apresia13000 シリーズ : <1-2>(デフォルト 1)
	Apresia13100/13200 シリーズ : <1>(デフォルト 1)
	Apresia15000 シリーズ : <1-3>(デフォルト 1)

表 13-2 占有するグループ数とポート数

占有する グループ 数	MMRP-Plus ポート総数		
	Apresia13000 シリーズ	Apresia13100/ 13200 シリーズ	Apresia15000 シリーズ
1	1-24	1-52	1-24
2	25-28	-	25-48
3	-	-	49-64

MMRP-Plus ポート総数の算出方法は下記を参照

<p>MMRP-Plus ポート総数</p> <p>= (マスタースイッチとして設定する MMRP-Plus Ring¹の数 × 2 ポート)</p> <p>+ (アウェアスイッチとして設定する MMRP-Plus Ring²の数 × 2 ポート)</p> <p>+ (分散マスタースイッチの Master ポートを設定する MMRP-Plus Ring³の数)</p> <p>+ (分散シャドウスイッチの Slave ポートを設定する MMRP-Plus Ring⁴の数)</p> <p>1) “ mmrp-plus ring <RINGID> master ” で設定する Ring</p> <p>2) “ mmrp-plus ring <RINGID> aware ” で設定する Ring</p> <p>3) “ mmrp-plus ring <RINDID> divided-master ” で設定する Ring</p> <p>4) “ mmrp-plus ring <RINDID> divided-slave ” で設定する Ring</p>

13.4 MMRP-Plus transmit-fdb-flush受信機能

MMRP-Plus transmit-fdb-flush 受信機能(“ mmrp-plus receive-flush-fdb enable ”)の設定を行うと1グループ占有します。“ show packet-filter2 reserved-group ” では「MMRP」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若番のグループが1個占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。

MMRP-Plus transmit-fdb-flush 受信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

Apresia13000 シリーズ : <1-11>

Apresia13100/13200 シリーズ : <1-14>

Apresia15000 シリーズ : <1-9>

NUMBER 占有するグループ数指定オプション

指定したグループ数に関わらず、1グループ占有

13.5 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、使用する最大ルール数を最初に設定します。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。オプション機能である認証拒否機能(“ deny-rule ”を設定)を利用する場合、専用に1グループを占有します。

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801端末目以降(Apresia13000シリーズでは201端末目以降)、1端末につき2ルール使用します。表 13-3 に最大ルール数と占有するグループ数を示します。

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-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 13-3 参照。
 RULE2 …… AccessDefender 機能の認証拒否機能が占有するパケットフィルタ-2の最大ルール数。本設定を行った場合、1グループを占有。

表 13-3 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	最大ルール数	
	Apresia13000 シリーズ	Apresia13100/ 13200 シリーズ
4	1-128	1-512
5	129-256	513-1024
6	257-384	1025-1536
7	385-512	1537-2048
8	513-640	2049-2560
9	641-768	2561-3072
10	769-896	3073-3584
11	897-1024	3585-4096
12	-	4097-4608
13	-	4609-5120
14	-	5121-5632

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
 Apresia13000 シリーズ : <1-11>
 Apresia13100/13200 シリーズ : <1-14>

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 1024 ” 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 (Aprasia13100/13200 シリーズの場合)。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 1024 ” は設定できません。

13.6 Flush FDB機能

「Flush FDB rp-e 機能」「Flush FDB rp-g 機能」の設定を行うとパケットフィルタ-2のリソースをそれぞれ1個占有します。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。指定しない場合は、他の機能で使用されていない最若番のグループが自動的に1個占有されます。“show packet-filter2 reserved-group”では「Flush FDB rp-e 機能」が「Flush FDB rp-e」、「Flush FDB rp-g 機能」が「Flush FDB rp-g」と表示されます。

13.7 BFS機能

BFS(BoxCore Fabric System)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「BoxCore Fabric System」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若番のグループが 1 個占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。

BFS 機能が占有するグループ番号指定コマンド

```
bfs group <GROUP>
```

```
GROUP ..... 指定するグループ番号
```

```
Apresia15000 シリーズ : <1-9>
```

13.8 FCoE Forwarder機能

FCoE(Fibre Channel over Ethernet) Forwarder 機能の設定を行うと最小で1グループ占有します。占有するグループ数が多ければ多いほど収容可能端末数も増加します。“ show packet-filter2 reserved-group ”では「FCoE Forwarder」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最初と最後を除くグループが自動的に占有されます。他機能で予約されているグループが存在する場合、連続した未使用グループが自動的に占有されます。連続した未使用グループが複数ある場合は、未使用グループ数が大きい番号が占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。表 13-4 に占有するグループ数と収容可能端末を示します。

表 13-4 占有するグループ数と収容可能端末

占有する グループ 数	収容可能端末
	Aprasia15000 シリーズ
1	1-216
2	217-472
3	473-728
4	729-984
5	985-1240
6	1241-1368
7	1369-1496
8	1497-1624
9	1625-1700

```
FCoE Forwarder 機能が占有するグループ番号指定コマンド
fcoe group <GROUP> <NUMBER>
    GROUP ..... 指定するグループ番号
                  Aprasia15000 シリーズ : <1-9>
    NUMBER ..... 占有するグループ数指定オプション
                  Aprasia15000 シリーズ : <1-9>
```

13.9 MLAG機能

MLAG 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「MLAG」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若番のグループが 1 個占有されます。このグループ番号は、構成情報(“ show running-config ”)にグループ番号指定設定として自動的に反映されます。

MLAG 機能が占有するグループ番号指定コマンド

```
mlag group <GROUP>
```

GROUP 指定するグループ番号

Apresia13100/13200 シリーズ : <1-14>

Apresia15000 シリーズ : <1-9>

14. 設定項目

パケットフィルタ-2 の設定項目を表 14-1～表 14-4 に示します。

表 14-1 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	Apresia13000-X24-PSR : 1-28 Apresia13100-48X-PSR : 1-52 Apresia13200 シリーズ : 1-52 Apresia15000-32XL-PSR : 1-32 Apresia15000-64XL-PSR : 1-64
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 14-2 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> 0x0-0xffff ¹ <MASK>省略時は 0xfff
4	Customer VLAN ID	なし	<VID> 1-4094 <MASK> 0x0-0xffff ¹ <MASK>省略時は 0xfff
5	IEEE802.1Q プライオリ ティ値	なし	<VID> 1-4094 <MASK> 0x0-0xffff <PRIORITY> 0-7
6	Ethernet Type	なし	<TYPE> 0x0-0xffff <MASK> 0x0-0xffff ¹ <MASK>省略時は 0xffff
7	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

8	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
9	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
10	TOS フィールド (tos)	なし	<VALUE> 0x0-0xff <MASK> 0x0-0xff ¹ <MASK>省略時は 0xff
11	DSCP 値 (tos-dscp)	なし	<VALUE> 0-63 <MASK> 0x0-0x3f ¹ <MASK>省略時は 0x3f
12	IP Precedence 値 (tos-precedence)	なし	<VALUE> 0-7 <MASK> 0x0-0x7 ¹ <MASK>省略時は 0x7
13	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
14	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
15	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
16	TCP ヘッダーの制御 Flag フィールド (tcp-flag)	なし	<ul style="list-style-type: none"> 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。
17	Traffic Class フィールド (traffic-class)	なし	<VALUE> 0-255 <MASK> 0x0-0xff ¹ <MASK>省略時は 0xff
18	Flow Label フィールド (flow-label)	なし	<VALUE> 0-1048575 <MASK> 0x0-0xffffffff ¹ <MASK>省略時は 0xffffffff
19	Next Header フィールド (next-header)	なし	<VALUE> 0-255 <MASK> 0x0-0xff ¹ <MASK>省略時は 0xff
20	Hop Limit フィールド (hop-limit)	なし	<VALUE> 0-255 <MASK> 0x0-0xff ¹ <MASK>省略時は 0xff
21	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

22	送信元 IPv6 アドレス	なし	<IPv6> ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <LENGTH> ³ 0-128
23	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 14-3 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 : 40000000Kbps cbs : 4Kbyte	<設定方法 1 の場合> cir : 64-40000000(Kbps)、64Kbps 刻み ² cbs : 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16380(Kbyte) ³ <設定方法 2 の場合> group : 1-64
11	redirect	なし	Apresia13000-X24-PSR : 1-28 Apresia13100-48X-PSR : 1-52 Apresia13200 シリーズ : 1-52 Apresia15000-32XL-PSR : 1-32 Apresia15000-64XL-PSR : 1-64
12	counter	なし	1-64 オプションで[unit byte]指定可
13	mirror	なし	Apresia13000-X24-PSR : 1-28 Apresia13100-48X-PSR : 1-52 Apresia13200 シリーズ : 1-52

		Apresia15000-32XL-PSR : 1-32 Apresia15000-64XL-PSR : 1-64
--	--	--

- 1) 二通りの設定方法に関しては「4.10 policingアクション」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 14-4 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	40000000Kbps	64-40000000(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, 16380(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。

15. 設定手順

パケットフィルタ-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-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

15.1 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 14-1 参照

VID …… VLAN ID 1-4094

MASK …… VLAN ID に対するマスク 0x0¹-0xfff 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。

15.2 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「15.1 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>]

<p>ethernet コンディショントイプの場合</p> <pre><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:ff¹ 省略時は ff:ff:ff:ff:ff:ff</pre>
<p>送信元 MAC アドレス条件の設定</p> <p>src コンディショントイプの場合</p> <pre><GROUP> <RULE> condition src mac <MAC> [mask <MASK>]</pre> <p>ethernet コンディショントイプの場合</p> <pre><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:ff¹ 省略時は ff:ff:ff:ff:ff:ff</pre>
<p>VLAN ID 条件の設定</p> <p>dst コンディショントイプの場合</p> <pre><GROUP> <RULE> condition dst vid <VID> [mask <MASK>]</pre> <p>src コンディショントイプの場合</p> <pre><GROUP> <RULE> condition src vid <VID> [mask <MASK>]</pre> <p>ethernet コンディショントイプの場合</p> <pre><GROUP> <RULE> condition ethernet vid <VID> [mask <MASK>] VID VLAN ID 1-4094 MASK <VID>に対するマスク 0x0-0xfff¹ 省略時は 0xffff</pre>
<p>Customer VLAN ID 条件の設定</p> <p>dst コンディショントイプの場合</p> <pre><GROUP> <RULE> condition dst c-vid <VID> [mask <MASK>] <GROUP> <RULE> condition dst c-vid none</pre> <p>src コンディショントイプの場合</p> <pre><GROUP> <RULE> condition src c-vid <VID> [mask <MASK>] <GROUP> <RULE> condition src c-vid none</pre> <p>ethernet コンディショントイプの場合</p> <pre><GROUP> <RULE> condition ethernet c-vid <VID> [mask <MASK>] <GROUP> <RULE> condition ethernet c-vid none VID VLAN ID 1-4094 MASK <VID>に対するマスク 0x0-0xfff¹ 省略時は 0xffff none カスタマータグなしフレーム (カスタマータグの TPID が 0x8100 ではないフレームを含む)が対象</pre>
<p>VLAN priority 条件の設定</p> <p>dst コンディショントイプの場合</p> <pre><GROUP> <RULE> condition dst vid <VID> mask <MASK> priority <VALUE> <GROUP> <RULE> condition dst c-vid <VID> mask <MASK> priority <VALUE></pre> <p>src コンディショントイプの場合</p> <pre><GROUP> <RULE> condition src vid <VID> mask <MASK> priority <VALUE> <GROUP> <RULE> condition src c-vid <VID> mask <MASK> priority <VALUE></pre>

<p>ethernet コンディションタイプの場合</p> <p><GROUP> <RULE> condition ethernet vid <VID> mask <MASK> priority <VALUE></p> <p><GROUP> <RULE> condition ethernet c-vid <VID> mask <MASK> priority <VALUE></p> <p>VID VLAN ID 1-4094</p> <p>MASK <VID>に対するマスク 0x0-0xfff (入力必須)</p> <p>0x0 を指定した場合は、全ての VLAN(VLAN ID 0 を含む)が対象</p> <p>PRIORITY ...802.1p VLAN プライオリティの値 0-7</p>
<p>Ethernet Type 条件の設定</p> <p>dst コンディションタイプの場合</p> <p><GROUP> <RULE> condition dst type <TYPE> [mask <MASK>]</p> <p>src コンディションタイプの場合</p> <p><GROUP> <RULE> condition src type <TYPE> [mask <MASK>]</p> <p>ethernet コンディションタイプの場合</p> <p><GROUP> <RULE> condition ethernet type <TYPE> [mask <MASK>]</p> <p>TYPE Ethernet Type 0x0-0xffff</p> <p>MASK <TYPE>に対するマスク 0x0-0xffff¹ 省略時は 0xffff</p>
<p>ARP 送信元 IP アドレス(arp-sender-ip)条件の設定</p> <p><GROUP> <RULE> condition src arp-sender-ip <IPv4>[/<NETMSAK>]</p> <p>IPv4 ARP パケットの Sender protocol address フィールド</p> <p>0.0.0.0-255.255.255.255</p> <p>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</p>
<p>送信元 IPv4 アドレス条件の設定</p> <p>src コンディションタイプの場合</p> <p><GROUP> <RULE> condition src ip <IPv4>[/<NETMASK>]</p> <p>ipv4, ipv4-src-tcp/udp-range, ipv4-dst-tcp/udp-range コンディションタイプの場合</p> <p><GROUP> <RULE> condition ipv4 src ip <IPv4>[/<NETMSAK>]</p> <p>IPv4 送信元 IPv4 アドレス 0.0.0.0-255.255.255.255</p> <p>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</p>
<p>宛先 IPv4 アドレス条件の設定</p> <p>dst コンディションタイプの場合</p> <p><GROUP> <RULE> condition dst ip <IPv4>[/<NETMASK>]</p> <p>ipv4, ipv4-src-tcp/udp-range, ipv4-dst-tcp/udp-range コンディションタイプの場合</p> <p><GROUP> <RULE> condition ipv4 dst ip <IPv4>[/<NETMSAK>]</p> <p>IPv4 宛先 IPv4 アドレス 0.0.0.0-255.255.255.255</p> <p>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</p>
<p>TOS フィールド(tos)条件の設定</p> <p><GROUP> <RULE> condition ipv4 tos <VALUE> [mask <MASK>]</p> <p>VALUE IPv4 ヘッダーの TOS フィールド 0x0-0xff</p> <p>MASK <VALUE>に対するマスク 0x0-0xff¹ 省略時は 0xff</p>
<p>DSCP 値(tos-dscp)条件の設定</p> <p><GROUP> <RULE> condition ipv4 tos-dscp <VALUE> [mask <MASK>]</p> <p>VALUE IPv4 ヘッダーの DSCP 値 0-63</p>

<p>MASK …… <VALUE>に対するマスク 0x0-0x3f¹ 省略時は 0x3f</p>
<p>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 0x0-0x7¹ 省略時は 0x7</p>
<p>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 0x0-0xff¹ 省略時は 0xff</p>
<p>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</p>
<p>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</p>
<p>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</p>
<p>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 0x0-0xff¹ 省略時は 0xff</p>
<p>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 0x0-0xffff¹ 省略時は 0xffff</p>
<p>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 0x0-0xff¹ 省略時は 0xff</p>
<p>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 0x0-0xff¹ 省略時は 0xff</p>
<p>ICMPv6 ヘッダーType フィールド icmp type)条件の設定</p>

<p><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 0x0-0xff¹ 省略時は 0xff</p>
<p>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</p>
<p>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</p>
<p>クラス ID 条件の設定 <GROUP> <RULE> condition class <CLASSID> CLASSID …… クラス ID 1-4095</p>

- 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。

15.3 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。

<p>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</p>
<p>permit アクションの設定 <GROUP> <RULE> action permit</p>
<p>deny アクションの設定 <GROUP> <RULE> action deny</p>
<p>none アクションの設定 <GROUP> <RULE> action none</p>
<p>authentication-bypass アクションの設定 <GROUP> <RULE> action authentication-bypass</p>
<p>block-cpu-control アクションの設定 <GROUP> <RULE> action block-cpu-control</p>

<p>qos アクションの設定</p> <p><GROUP> <RULE> action qos <QOSPROFILE> QOSPROFILE … マッピングする QoS プロファイル qp1-qp8</p>
<p>priority アクションの設定</p> <p><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</p>
<p>ip-tos-dscp アクションの設定</p> <p><GROUP> <RULE> action ip-tos-dscp <DSCP> DSCP …… 書き換える DSCP 値 0-63</p>
<p>ip-tos-precedence アクションの設定</p> <p><GROUP> <RULE> action ip-tos-precedence <PRECEDENCE> PRECEDENCE … 書き換える IP Precedence 値 0-7</p>
<p>設定方法 1 による policing アクションの設定(表 4-1 参照)</p> <p><GROUP> <RULE> action policing cir <RATE> <GROUP> <RULE> action policing cbs <BURST> RATE …… CIR(Committed Information Rate) 64-40000000(Kbps)、64Kbps 刻み¹ BURST …… CBS(Committed Burst Size) 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16380(Kbyte)²</p>
<p>設定方法 2 による policing アクションの設定(表 4-1 参照)</p> <p><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) 64-40000000(Kbps)、64Kbps 刻み¹ BURST …… CBS(Committed Burst Size) 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16380(Kbyte)²</p>
<p>redirect アクションの設定</p> <p><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 14-3 参照</p>
<p>counter アクションの設定</p> <p><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</p>
<p>mirror アクションの設定</p> <p><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 14-3 参照</p>

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。

15.4 手順(4) exceeded-action denyの設定

パケットフィルタ-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

15.5 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

16. 制限事項および注意事項

パケットフィルタ-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ティスを参照して下さい。

表 16-1 パケットフィルタ-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	<ul style="list-style-type: none">•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。
2	設定関連	<ul style="list-style-type: none">•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を設定した場合の注意」を参照して下さい。•パケットフィルタ-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「13 パケットフィルタ-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	<ul style="list-style-type: none">•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AEOS8 バージョンでの機能追加、変更点

パケットフィルタ-2 に関する各AEOS8 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ティスを参照して下さい。

表 17-1 各 AEOS8 バージョンでの機能追加、変更点

Version	管理番号	内容
8.03.01	AEOS-80301-RC006	パケットフィルタ 2 機能において、condition 設定時に MASK を省略した場合、構成情報表示から MASK 表示を省略するように仕様を変更しました。
	AEOS-80301-RC007	パケットフィルタ 2 機能において、“ show packet-filter2 policing ” 表示を AEOS7 と同一表示に変更しました。
8.04.01	AEOS-80401-RC020	パケットフィルタ 2 機能において、複数 action 設定時、no action deny で permit 設定が消えないようにしました。
	AEOS-80401-RC021	パケットフィルタ 2 機能において、show packet-filter2 counter において、rule 部の表示を変更(AEOS7 と共通化)しました。
8.07.01	AEOS-80701-RC024 AEOS-80601-ER006	パケットフィルタ-2 機能において、同一グループに “ condition ” の設定がない場合、 “ <GROUP> <RULE> assign port ” 又は “ <GROUP> <RULE> assign vlan ” “ no action ” “ condition ” の順に設定すると、“ condition ” の設定が反映されず、 の設定もすべて消去される問題を修正しました。
8.08.01	AEOS-80801-RC015	パケットフィルタ-2 機能において、VLAN の priority を指定できる condition コマンドをサポートしました。 ・ “ <GROUP> <RULE> condition (dst src) vid <VID> mask <MASK> priority <VALUE> ” ・ “ <GROUP> <RULE> condition ethernet vid <VID> mask <MASK> priority <VALUE> ”
	AEOS-80801-RC016	パケットフィルタ-2 機能において、フィルター条件を満たしても何もしない action コマンドをサポートしました。 ・ “ <GROUP> <RULE> action none ” AccessDefender 機能の認証成功端末からのフレームにパケットフィルタ-2 機能を適用する場合に使用します。
	AEOS-80801-RC023	IP アドレス機能において、IP アドレスで使うパケットフィルターのルール数がプライマリー/セカンダリー/Loopback の各 IP アドレス数の総和に 7 を足した値から、各 IP アドレス数の総和に 3 足した値に仕様を変更しました。
	AEOS-80801-RC030	パケットフィルタ-2 機能において、設定していない action に対して no コマンドを受け付けないように仕様を変更しました。実施した場合はエラーメッセージ(“ % Mismatch action delete mode. ”)が出力されません。

	AEOS-80801-RC050 AEOS-80602-ER002	パケットフィルタ-2 機能において、 " <GROUP> <RULE> assign port vlan " を設定した後に、同一グループ内の別ルールにて " action " " condition " のみを設定すると、ルール内に " assign " 設定がないにもかかわらず、設定した " action " " condition " が全 port、全 vlan で不正に有効となる問題を修正しました。
	AEOS-80801-RC051 AEOS-80701-ER003	パケットフィルタ-2 機能において、 " condition " 設定 tcp/udp のレンジ指定を上書き設定すると、tcp/udp の設定値が内部的に不正になる問題を修正しました。
	AEOS-80801-RC063	AccessDefender 機能において、 " no web-authentication http-port " コマンドを行っても内部で利用していたパケットフィルタ-2 のルールが削除されないためコマンドで設定した http-port でアクセスできる問題を修正しました。
8.08.02	AEOS-80802-RC008	SNMP 機能において、パケットフィルタ-2 のカウンター情報を MIB で取得できる機能をサポートしました。
	AEOS-80802-RC011	IP アドレス機能において、セカンダリー IP アドレスを削除してもパケットフィルタ-2 のグループが開放されない問題を修正しました。
	AEOS-80802-RC022	Egress シェーピング機能において、 " egress-shape count-mode include-ifg-pa " の設定がある場合、パケットフィルタ-2 機能の policing 設定通りの転送レートにならない問題を修正しました。
8.08.03	AEOS-80803-RC009	パケットフィルタ-2 機能において、パケットフィルタ-2 のグループを利用している機能で、複数機能の参照/変更が全く同時に行われた場合に、機能が停止する可能性がある問題を修正しました。
8.09.02	AEOS-80902-RC006	パケットフィルタ-2 機能において、パケットフィルタ-2 のグループを利用している機能で、複数機能の参照/変更が全く同時に行われた場合に、機能が停止する可能性がある問題を修正しました。
8.09.03	AEOS-80903-RC014 AEOS-80803-ER007	パケットフィルタ-2 機能において、 " condition ipv6 src dst ip " 設定時に、同一グループ、別ルールに " action " だけを設定すると " condition ipv6 src ip ::/0 " 誤表示される問題を修正しました。
	AEOS-80903-RC015 AEOS-80803-ER008	パケットフィルタ-2 機能において、 " condition ipv4 dst tcp/udp range " を同一ルール内に再度設定すると condition 設定が削除される問題が修正しました。
	AEOS-80903-RC016 AEOS-80803-ER009	パケットフィルタ-2 機能において、同一ルール内に " condition ipv4 src tcp/udp " と " condition ipv4 dst tcp/udp " 設定後、どちらか一方のルールを削除すると " show packet-filter2 " で表示されるプロトコル番号(tcp/udp)が0と誤表示される問題を修正しました。
8.09.06	AEOS-80906-RC006 AEOS-80903-ER010	QoS 機能において、Aprasia15000 シリーズで " qos qosprofile " とパケットフィルタ-2 機能の " action qos " 設定後に、 " no qos qosprofile " コマンドを実行するとエラーメッセージが出力される問題を修正しました。
8.10.01	AEOS-81001-RC002	AccessDefender 機能において、認証機能(ゲートウェイ認証以外)でユー

		ザー毎にパケットフィルタ-2 機能を適用拡張できる機能をサポートしました。
	AEOS-81001-RC003	パケットフィルタ-2 機能において、特定フィルター条件(コンディション)の同一ルール内複数設定を可能にする " wide-mode <GROUP> " コマンドに対応しました。
	AEOS-81001-RC013 AEOS-80803-ER005	パケットフィルタ-2 機能において、assign をグループに設定した状態で " no <GROUP> <RULE> action " " no <GROUP> <RULE> condition " コマンドを実施すると、 " show running-config " 上では削除されているが内部的に設定が残る問題を修正しました。
	AEOS-81001-RC014 AEOS-80803-ER006	パケットフィルタ-2 機能において、 " condition dst ip " と " condition dst type " 設定後、 " condition dst ip " を削除すると、 " condition dst type " の値が 0x0 mask 0x0 と不正に変更される問題を修正しました。
	AEOS-81001-RC015 AEOS-80803-ER007	パケットフィルタ-2 機能において、 " condition ipv6 src dst ip " 設定時に、同一グループ、別ルールに " action " だけを設定すると " condition ipv6 src ip ::/0 " と誤表示される問題を修正しました。
	AEOS-81001-RC016 AEOS-80803-ER008	パケットフィルタ-2 機能において、 " condition ipv4 dst tcp/udp range " を同一ルール内に再度設定すると condition が削除される問題を修正しました。
	AEOS-81001-RC017 AEOS-80803-ER009	パケットフィルタ-2 機能において、同一ルール内に " condition ipv4 src tcp/udp " と " condition ipv4 dst tcp/udp " 設定後、どちらか一方のルールを削除すると " show packet-filter2 " で表示されるプロトコル番号(tcp/udp)が0と誤表示される問題を修正しました。
8.11.01	AEOS-81101-RC021 AEOS-81001-ER006	パケットフィルタ-2 機能において、 " action mirror " コマンドを設定すると他機能が停止、又は装置が再起動する可能性がある問題を修正しました。
8.12.01	AEOS-81201-RC023	パケットフィルタ-2 機能において、 " condition " 設定で MAC アドレスを指定してもエラーメッセージが出力されて、極稀に設定が反映されない問題を改修しました。
	AEOS-81201-RC024	パケットフィルタ-2 機能において、 " wide-mode " 設定があると極稀にパケットフィルタ-2 の設定が反映されない問題を改修しました。
8.13.01	AEOS-81301-RC025	パケットフィルタ-2 機能において、 " condition " 設定で MAC アドレスを指定してもエラーメッセージが出力されて、極稀に設定が反映されない問題を改修しました。
8.14.01	AEOS-81401-RC007	パケットフィルタ-2 機能において、 ICMPv6 ヘッダーの Type 値を指定できるコンディションコマンドをサポートしました。 ・ "<GROUP> <RULE> condition ipv6 icmp type"
	AEOS-81401-RC008	Aprasia15000 シリーズのパケットフィルタ-2 機能において、特定フィルター条件(コンディション)の同一ルール内複数設定を可能にするコマンドに対応しました。

		<ul style="list-style-type: none"> ・"wide-mode <GROUP>"
	AEOS-81401-RC029	パケットフィルタ-2 機能において、"packet-filter2 [<CHASSIS>]" コマンドで [<CHASSIS>] を設定できないように仕様変更をしました。
	AEOS-81401-RC036 AEOS-81202-ER004 AEOS-81303-ER006	パケットフィルタ-2 機能において、"show packet-filter2 reserved-group" を長時間連続実行すると、装置が再起動する問題を修正しました。
	AEOS-81401-RC037 AEOS-81202-ER006	パケットフィルタ-2 機能において、"wide-mode" が有効になっているグループに対し、異なる condition-type の追加/削除を繰り返すとエラーが出力され設定が反映されなくなる問題を修正しました。
	AEOS-81401-RC038 AEOS-81202-ER005 AEOS-81303-ER007	パケットフィルタ-2 機能において、MMRP-Plus 機能が設定されているポートに対して、"action mirror port" を連続設定すると同一ルールの設定変更ができなくなる問題を修正しました。
	AEOS-81401-RC039	パケットフィルタ-2 機能において、"no <group> <rule>" コマンド実行時に同じグループに所属する他 rule が一時的に無効になる問題を修正しました。
8.15.01	AEOS-81501-RC007	<p>パケットフィルタ-2 機能において、カスタムタグの VLAN ID の値を指定できるコンディションコマンドをサポートしました。</p> <ul style="list-style-type: none"> ・"<GROUP> <RULE> condition (dst src ethernet) c-vid <VID> [mask <MASK> [priority <VAULE>]]" ・"<GROUP> <RULE> condition (dst src ethernet) c-vid none"
	AEOS-81501-RC008	<p>パケットフィルタ-2 機能において、CPU 宛フィルタ-機能をサポートしました。</p> <ul style="list-style-type: none"> ・"block-cpu-control <GROUP> <GROUP> enable" ・"<GROUP> <RULE> action block-cpu-control"
	AEOS-81501-RC023	パケットフィルタ-2 機能において、"wide-mode" を複数グループ設定できるように仕様を変更しました。
	AEOS-81501-RC044 AEOS-81405-ER003	パケットフィルタ-2 機能において、"assign port vlan" の設定がある状態で condition-type を変更すると設定が反映されず正常に動作しない問題を修正しました。(AEOS8.14.01 から発生)
	AEOS-81501-RC045	パケットフィルタ-2 機能において、"assign port" "assign vlan" を両方設定してあるルールに対して"assign port"のみを削除した場合、設定ルールが動作しなくなる問題を修正しました。
	AEOS-81501-RC046	パケットフィルタ-2 機能において、"condition ipv4 tcp-flag" と "condition ipv4 (src dst) tcp/udp <TCP/UDPPORT> tcp" 設定後に、"condition ipv4 (src dst) tcp/udp <TCP/UDPPORT> tcp" を削除しようとするとエラーが出力され設定を削除できない問題を修正しました。
	AEOS-81501-RC047	パケットフィルタ-2 機能において、"wide-mode" を設定している状態で "action counter" の設定を削除すると "action counter" が再設定出来なくなる問題を修正しました。
	AEOS-81501-RC048	Aprasia13000/13100/13200 シリーズのパケットフィルタ-2 機能におい

		て、"wide-mode"を設定している状態で"action policing"設定した時に "show running-config"に設定が反映され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アクション」「4.2 denyアクション」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1/1で受信する送信元IPv4アドレスが10.0.10.0/24の packets」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1/1で受信する送信元IPv4アドレスが10.0.0.0/8の packets」に一致した場合には【deny】

と設定した場合には、「ポート1/1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 packets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 packets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

- Apresia13200-48X-PSR のポート 1/1 ~ 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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 assign port 1/1-10
```

(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。

```
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 2 assign port 1/1-10
```

(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 2 action deny
```

(8) 設定後の show コマンド結果を示します。

```
Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign port 1/1-10
 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 1/1-10
 1 2 condition ethernet src mac 00:bb:bb:bb:bb:bb
 1 2 action deny
!
~ 省略 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1 port             ethernet
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
action:
group rule deny        tos QosProf    Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
 1/1    1 Deny           -    -          -    -    -        -          -
 1/1    2 Deny           -    -          -    -    -        -          -

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

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

condition:
group rule condition  dst mac address    src mac address    Type    vid
-----
 1/1    1 ether          00:a1:00:00:00:00 -                -    -
 1/1    1 ether-m       ff:ff:ff:00:00:00 -                -    -
 1/1    2 ether          -                00:bb:bb:bb:bb:bb -    -
 1/1    2 ether-m       -                ff:ff:ff:ff:ff:ff -    -
```

~省略~

Ap132-48x#

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

- Apresia13000-X24-PSR のポート 1/1、1/3、1/5 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 コンディショント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。

```
Ap13kX24# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap13kX24(config)# packet-filter2
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 assign port 1/1,1/3,1/5
Ap13kX24(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。

```
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 1 action permit1
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。

```
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 2 action permit1
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。

```
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 3 action deny
```

(9) 設定後の show コマンド結果を示します。

```
Ap13kX24# show running-config
~ 中略 ~
packet-filter2
 1 assign port 1/1,1/3,1/5
 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 ~
Ap13kX24#
Ap13kX24# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1  port/vlan      src
Ap13kX24#
Ap13kX24# show packet-filter2 1 brief
action:
group rule deny          tos QosProf   Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
 1/1    1 Permit            -    -    -    -    -    -    -
 1/1    2 Permit            -    -    -    -    -    -    -
 1/1    3 Deny              -    -    -    -    -    -    -

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

assign:

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

condition:

group	rule	condition	src mac address	src ip address	Type	vid
1/1	1	src	-	10.1.10.0	-	-
1/1	1	src-m	-	255.255.255.0	-	-
1/1	2	src	-	10.1.20.0	-	-
1/1	2	src-m	-	255.255.255.0	-	-
1/1	3	src	00:a1:00:00:00:00	-	-	-
1/1	3	src-m	ff:ff:ff:ff:ff:ff	-	-	-

~省略~

Ap13kX24#

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ついては「4.6 qosアクション」を参照して下さい。

19.1 設定例(1) 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

- Apresia13200-48X-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 コンディショント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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 condition ipv4 tos-precedence 0 mask 0x41
```

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ついては「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。

```
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 2 condition ipv4 tos-precedence 4 mask 0x61
```

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ついては「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。

```
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 3 condition ipv4 tos-precedence 6 mask 0x61
```

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ついては「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。

```
Ap132-48x(config-filter)# 1 3 action qos qp7
```

(11) 設定後の show コマンド結果を示します。

```
Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign vlan 2000 mask 0xffff
 1 1 condition ipv4 tos-precedence 0 mask 0x4
 1 1 action qos qp1
 1 1 action permit
 1 2 assign vlan 2000 mask 0xffff
 1 2 condition ipv4 tos-precedence 4 mask 0x6
 1 2 action qos qp1
 1 2 action permit
 1 3 assign vlan 2000 mask 0xffff
 1 3 condition ipv4 tos-precedence 6 mask 0x6
 1 3 action qos qp7
 1 3 action permit
!
~ 省略 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
```

```

1/1  vlan          ipv4
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
group assign      condition-type
-----
1/1  vlan          ipv4
Ap132-48x# show packet-filter2 1 b
action:
group rule deny   tos QosProf   Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
1/1    1 Permit      -    qp1     -    -    -        -        -
1/1    2 Permit      -    qp1     -    -    -        -        -
1/1    3 Permit      -    qp7     -    -    -        -        -

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

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

condition:
group rule condition  src ip address  dst ip address  Prot  tos(P/D)
-----
1/1    1  ipv4      -              -              -    0 (P)
1/1    1  ipv4-m    -              -              -    0x4 (P)
1/1    2  ipv4      -              -              -    4 (P)
1/1    2  ipv4-m    -              -              -    0x6 (P)
1/1    3  ipv4      -              -              -    6 (P)
1/1    3  ipv4-m    -              -              -    0x6 (P)

condition tcp/udp:
group rule condition  tcp-flag s-t/u-p d-t/u-p range index
-----
1/1    1  ipv4-t/u    -        -        -
1/1    1  ipv4-t/u-m  -        -        -
1/1    2  ipv4-t/u    -        -        -
1/1    2  ipv4-t/u-m  -        -        -

```

1/1	3	ipv4-t/u	-	-	-
1/1	3	ipv4-t/u-m	-	-	-

~省略~

Ap132-48x#

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アクション」を参照して下さい。

20.1 設定例(1) 送信フレームの 802.1p優先度変更機能

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

- Apresia13200-48X-PSR のポート 1/1～1/9 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 コンディショント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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 assign port 1/1-9
```

(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。

```
Ap132-48x(config-filter)# 1 1 condition dst mac 00:aa:bb:cc:dd:ee
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 2 assign port 1/1-9
```

(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。

```
Ap132-48x(config-filter)# 1 2 condition dst mac 00:aa:bb:cc:dd:ee
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 action priority 6
```

(8) 設定後の show コマンド結果を示します。

```
Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign port 1/1-9
 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 1/1-9
 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 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1 port             dst
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
action:
group rule deny      tos QosProf   Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
1/1    1 Permit   prio      -     6    -    -         -         -
1/1    2 Permit   prio      -     6    -    -         -         -

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

assign:
```

group	rule	assign	port	vid	vid-m	

1/1	1	port	1/1-9	-	-	
1/1	2	port	1/1-9	-	-	
condition:						
group	rule	condition	dst mac address	dst ip address	Type	vid

1/1	1	dst	00:aa:bb:cc:dd:ee	-	0x0800	-
1/1	1	dst-m	ff:ff:ff:ff:ff:ff	-	0xffff	-
1/1	2	dst	00:aa:bb:cc:dd:ee	-	0x0806	-
1/1	2	dst-m	ff:ff:ff:ff:ff:ff	-	0xffff	-
~省略~						
Ap132-48x#						

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を設定した場合の注意」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つ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 複数のグループにマッチした場合の注意」を参照して下さい。

21.1 設定例(1) 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

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

- Apresia13200-48X-PSR のポート 1/1 ~ 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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 assign port 1/1-24
```

(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。

```
Ap132-48x(config-filter)# 1 1 condition ipv4 src ip 10.1.1.0/24
Ap132-48x(config-filter)# 1 1 condition ipv4 dst ip 192.168.100.0/24
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 2 1 assign port 1/1-24
```

(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。

```
Ap132-48x(config-filter)# 2 1 condition ipv4 src ip 10.1.1.0/24
Ap132-48x(config-filter)# 2 1 condition ipv4 dst ip 192.168.100.0/24
Ap132-48x(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。

```
Ap132-48x(config-filter)# 2 1 action priority 6
```

(8) 設定後の show コマンド結果を示します。

```
Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign port 1/1-24
 1 1 condition ipv4 dst ip 192.168.100.0/24
 1 1 condition ipv4 src ip 10.1.1.0/24
 1 1 condition ipv4 tos-precedence 6
 1 1 action qos qp7
 1 1 action permit

 2 1 assign port 1/1-24
 2 1 condition ipv4 dst ip 192.168.100.0/24
 2 1 condition ipv4 src ip 10.1.1.0/24
 2 1 condition ipv4 tos-precedence 6
 2 1 action priority 6
 2 1 action permit
!
~ 省略 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1 port              ipv4
  1/2 port              ipv4
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
action:
group rule deny        tos QosProf    Prio  Mirr  Redir  Polic(grp-id) counter(U)
-----
```

```

1/1    1 Permit    -    qp7    -    -    -    -    -
exceeded-action:
group rule    deny
-----
1/1    1    -
assign:
group rule assign    port                                vid vid-m
-----
1/1    1 port    1/1-24                                -    -
condition:
group rule condition    src ip address    dst ip address    Prot    tos(P/D)
-----
1/1    1 ipv4    10.1.1.0    192.168.100.0    -    6 (P)
1/1    1 ipv4-m    255.255.255.0    255.255.255.0    -    0x7 (P)
condition tcp/udp:
group rule condition    tcp-flag s-t/u-p d-t/u-p range index
-----
1/1    1 ipv4-t/u    -    -    -
1/1    1 ipv4-t/u-m    -    -    -
~省略~
Ap132-48x#
Ap132-48x# show packet-filter2 2 brief
action:
group rule deny    tos QosProf    Prio    Mirr Redir    Polic(grp-id) counter(U)
-----
1/2    1 Permit    prio    -    6    -    -    -    -
exceeded-action:
group rule    deny
-----
1/2    1    -
assign:
group rule assign    port                                vid vid-m
-----
1/2    1 port    1/1-24                                -    -
condition:
group rule condition    src ip address    dst ip address    Prot    tos(P/D)
-----
1/2    1 ipv4    10.1.1.0    192.168.100.0    -    6 (P)

```

```
1/2    1 ipv4-m      255.255.255.0  255.255.255.0  - 0x7 (P)
```

condition tcp/udp:

```
group rule condition tcp-flag s-t/u-p d-t/u-p range index
```

```
1/2    1 ipv4-t/u      -      -      -
```

```
1/2    1 ipv4-t/u-m    -      -      -
```

~省略~

Ap132-48x#

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アクション」「4.9 ip-tos-precedenceアクション」を参照して下さい。

22.1 設定例(1) 送信パケットのDSCP値/IP Precedence値変更機能

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

- Apresia13200-48X-PSR のポート 1/1 ~ 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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 assign port 1/1-24
```

(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。

```
Ap132-48x(config-filter)# 1 1 condition ipv4 dst ip 10.1.1.100/32
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 2 assign port 1/1-24
```

(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。

```
Ap132-48x(config-filter)# 1 2 condition ipv4 dst ip 10.1.1.200/32
Ap132-48x(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。

```
Ap132-48x(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。

```
Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign port 1/1-24
 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 1/1-24
 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 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1 port             ipv4-src-tcp/udp-range
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
action:
group rule deny        tos QosProf    Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
 1/1    1 Permit  dscp-48    -      -      -      -      -      -
 1/1    2 Permit  pre-1     -      -      -      -      -      -

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

assign:

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

condition:

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

condition tcp/udp:

group	rule	condition	tcp-flag	s-t/u-p	d-t/u-p	range	index
1/1	1	ipv4-t/u	-	-	-	src:1-1023	
1/1	1	ipv4-t/u-m	-	-	-		
1/1	2	ipv4-t/u	-	-	-	src:1-1023	
1/1	2	ipv4-t/u-m	-	-	-		

~省略~

Ap132-48x#

Ap132-48x# show packet-filter2 tcp/udp-range

range-id	src/dst	port-range
----------	---------	------------

1	src	1 to 1023
---	-----	-----------

Ap132-48x#

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 exceeded-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

- Apresia13200-48X-PSR のポート 1/1 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 コンディショントップ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。

```
Ap132-48x# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap132-48x(config)# packet-filter2
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 assign port 1/1
```

(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。

```
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 action policing cir 99968
Ap132-48x(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。

```
Ap132-48x(config-filter)# 1 1 exceeded-action deny
```

(6) 設定後の show コマンド結果を示します。

```

Ap132-48x# show running-config
~ 中略 ~
packet-filter2
 1 1 assign port 1/1
 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 ~
Ap132-48x#
Ap132-48x# show packet-filter2 group brief
  group assign          condition-type
-----
  1/1  port            ipv6-src-ip
Ap132-48x#
Ap132-48x# show packet-filter2 1 brief
action:
group rule deny      tos QosProf   Prio  Mirr Redir  Polic(grp-id) counter(U)
-----
 1/1    1 Permit        -    -    -    -    -    99968-128    -

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

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

condition:
group rule condition  ip address
-----
 1/1    1 ipv6-src-ip  fe80::aaaa/128
~ 省略 ~
Ap132-48x#

```

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

- Apresia13000-X24-PSR のポート 1/1 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 コンディショントイプとして使用する。帯域制限エントリ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。

```
Ap13kX24# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap13kX24(config)# packet-filter2
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 1 assign port 1/1
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 1 condition ipv4 src ip 192.168.0.100/32
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 1 action policing group 1
Ap13kX24(config-filter)# 1 policing 1 cir 49984
Ap13kX24(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。

```
Ap132-48x(config-filter)# 1 1 exceeded-action deny
```

(6) 設定後の show コマンド結果を示します。

```
Ap13kX24# show running-config
~ 中略 ~
packet-filter2
 1 policing 1 cbs 64
 1 policing 1 cir 49984

 1 1 assign port 1/1
 1 1 assign vlan 10 mask 0xffff
```

```

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~

Ap13kX24#

Ap13kX24# show packet-filter2 group brief

```

group assign          condition-type
-----

```

```

1/1 port/vlan      ipv4

```

Ap13kX24#

Ap13kX24# show packet-filter2 1 brief

action:

```

group rule deny      tos QosProf   Prio  Mirr Redir  Polic(grp-id) counter(U)
-----

```

```

1/1    1 Permit      -      -      -      -      -      1-1      -

```

exceeded-action:

```

group rule    deny
-----

```

```

1/1    1    -

```

assign:

```

group rule assign    port                                vid vid-m
-----

```

```

1/1    1 port/vlan  1/1                                10 0xfff

```

condition:

```

group rule condition  src ip address  dst ip address  Prot  tos(P/D)
-----

```

```

1/1    1 ipv4        192.168.0.100  172.21.0.0      -  -

```

```

1/1    1 ipv4-m       255.255.255.255 255.255.0.0     -  -

```

condition tcp/udp:

```

group rule condition  tcp-flag s-t/u-p d-t/u-p range index
-----

```

```

1/1    1 ipv4-t/u      -      -      -

```

```

1/1    1 ipv4-t/u-m     -      -      -

```

~省略~

Ap13kX24#

Ap13kX24# show packet-filter2 policing 1

```

group m-id          cir  cbs rule
-----

```

```

1/1    1          49984  64 1

```

1/1

2

40000000

4

~省略~

Ap13kX24#

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アクション」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

- ・ Apresia13000-X24-PSR のポート 1/1 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 1/1 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。

```
Ap13kX24# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ap13kX24(config)# packet-filter2
Ap13kX24(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。

```
Ap13kX24(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。

```
Ap13kX24(config-filter)# 1 assign port 1/1
```

(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。

```
Ap13kX24(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。

```
Ap13kX24(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。

```
Ap13kX24(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。

```
Ap13kX24(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。

```
Ap13kX24# show running-config
~ 中略 ~
packet-filter2
  block-cpu-control 1 2 enable
  1 assign port 1/1
  2 assign port 1/1
  1 1 action none
  1 1 condition ipv4 src ip 192.168.10.100/32
  1 1 condition ipv4 dst tcp/udp 23 tcp
  1 2 action none
  1 2 action block-cpu-control
  1 2 condition ipv4 src ip 192.168.10.0/24
  2 1 action none
  2 1 condition ipv4 src ip 192.168.10.100/32
  2 1 condition ipv4 dst tcp/udp 23 tcp
  2 2 action none
  2 2 action block-cpu-control
  2 2 condition ipv4 src ip 192.168.10.0/24
```

!

~ 省略 ~

```
Ap13kX24#
```

```
Ap13kX24# show packet-filter2 group brief
```

```
  group assign          condition-type
```

```
-----
  1/1 port              ipv4
  1/2 port              ipv4
```

```
Ap13kX24#
```

```
Ap13kX24# show packet-filter2 1 brief
```

```
action:
```

```
group rule deny        CPU Polic(grp-id) counter(U)
```

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

```
exceeded-action:
```

```
group rule  deny        CPU
```

```
1/1 1 - -
1/1 2 - -
```

assign:

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

condition:

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

condition tcp/udp:

group	rule	condition	tcp-flag	s-t/u-p	d-t/u-p	range	index
1/1	1	ipv4-t/u	-	-	-	23	
1/1	1	ipv4-t/u-m	-	-	-	0xffff	
1/1	2	ipv4-t/u	-	-	-	-	
1/1	2	ipv4-t/u-m	-	-	-	-	

~省略~

Ap13kX24#

AEOS Ver. 8 アプリケーションノート
(パケットフィルタ-2 編)

Copyright(c) 2012 Hitachi Cable, Ltd.

2010年9月 初版

2012年6月 第3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