QoS

Quality of Service 機能をネットワーク全体に適用すると、必要な基準に従ってネットワークトラフィックが優先順位付けされ、重要なトラフィックが優先的に処理されます。この章は、次の項で構成されています。

一般

Quality of Service（QoS）は、トラフィックを優先順位付けするスイッチの機能であり、結果として、重要なネットワークトラフィックのパフォーマンスが向上します。QoS はスイッチによって異なります。スイッチのレベルが高いほど、そのスイッチで動作するネットワーク アプリケーション レイヤが高くなります。キューの数は、優先順位付けに使用される情報の種類と同様に異なります。

QoSプロパティ

Quality of Service（QoS）はトラフィックのタイプに基づいてトラフィックフローを優先順位付けし、遅延の影響を受けやすいアプリケーション（音声やビデオなど）のトラフィックの優先順位付けに適用したり、遅延に依存しないトラフィックの影響を制御したりできます。

QoS プロパティを設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [QoS Properties] をクリックします。

ステップ 2 QoS モードを設定します。次のオプションを使用できます。

- [Disable]：デバイスで QoS が無効になります。
- [Basic]：デバイスで QoS が基本モードで有効になります。
- [Advanced]：デバイスで QoS が拡張モードで有効になります。

ステップ 3 デバイス上のすべてのポート/LAG とそれらの CoS 情報を表示または修正するには、[Port/LAG] を選択し、[Go] をクリックします。

すべてのポート/LAG について、次のフィールドが表示されます。

- [インターフェイス] : インターフェイスのタイプ。
- [デフォルト CoS] : VLAN タグが設定されていない着信パケットに対するデフォル トの VPT 値。デフォルト CoS は 0 です。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

インターフェイスの QoS を設定するには、インターフェイスを選択し、[Edit] をクリックします。

ステップ 5 パラメータを入力します。

- [インターフェイス] : ポートまたは LAG を選択します。
- [デフォルト CoS] : VLAN タグが設定されていない着信パケットに割り当てる、デ フォルト CoS 値を選択します。

ステップ 6 [Apply] をクリックします。インターフェイスのデフォルト CoS 値が実行コンフィギュレーション ファイルに保存されます。

デフォルトの CoS 値を復元するには、[Restore CoS Defaults] をクリックします。

キュー

デバイスでは、インターフェイスごとに 8 つのキューがサポートされます。キュー番号 8 は、最もプライオリティの高いキューです。キュー番号 1 は、最もプライオリティの低いキューです。

キュー内のトラフィックを処理する方式には、絶対優先 と加重ラウンド ロビン（WRR）の 2 つがあります。

- 完全優先：プライオリティが最も高いキュー内のトラフィックが最初に送出されます。それより低いキュー内のトラフィックは、プライオリティが最高のキュー内のトラフィックが創出された後にのみ送出されます。したがって、プライオリティが最高のトラフィックは最大番号のキューに格納されます。
- [Weighted Round Robin (WRR)]：WRR モードでは、キューから送出されるパケット数は、キューのウェイトに比例します（キューのウェイトが大きいほど、送出されるフレームの数が多くなる）。たとえば、許容最大数の 4 個のキューがあり、4 個のキューすべてが WRR モードに設定されていて、デフォルトのウェイト設定が使用されている場合、すべてのキューが飽和状態になっていて輻輳が発生していると仮定すると、キュー 1 では帯域幅の 1/15、キュー 2 では 2/15、キュー 3 では 4/15、キュー 4 では 8/15 がそれぞれ使用されます。このデバイスで使用される WRR アルゴリズムの種類は、一般的な Deficit WRR（DWRR）ではなく Shaped Deficit WRR（SDWRR）です。

キューイング モードは [Queue] ページで選択できます。キューイング モードが SP の場合、プライオリティによって各キューの処理順序が決まります。まず、プライオリティが最高のキューから開始し、各キューが完了すると、プライオリティが次に高いキューに移ります。

キューイング モードが加重ラウンド ロビンの場合は、キューに割り当てられた帯域幅がすべて使用されるまでキューが処理され、その後に別のキューが処理されます。プライオリティの低いキューを WRR モードに設定し、プライオリティの高いキューを SP モードに設定することもできます。この場合、SP モードのキュー内のトラフィックは常に、WRR モードのキュー内のトラフィックよりも先に送出されます。SP モードのキューが空になると、WRR モードのキュー内のトラフィックの送出が開始されます。（各 WRR キューからの相対的な送出割合は、キューのウェイトに依存する）。

プライオリティ方式を選択し、WRR データを入力するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [Queue] をクリックします。

ステップ 2 パラメータを入力します。

- [キュー]：キュー番号が表示されます。
- [Scheduling Method]：次のオプションのいずれかを選択します。
  - [Strict Priority]：選択したキューおよびそれよりプライオリティの高いすべてのキューのトラフィック スケジューリングは、厳密にそのキューのプライオリティに基づきます。
  - [WRR]：選択したキューのトラフィック スケジューリングは、WRR に基づきます。送出時間は、空でない WRR モードのキュー間で配分されます。つまり、それらのキューには出力記述子が設定されています。この配分が発生するのは、SP モードのキューが空になっている場合のみです。
  - [WRR ウェイト]：WRR を選択した場合、このキューに割り当てる WRR ウェイトを入力します。
  - [WRR 帯域幅の %]：このキューに割り当てられている帯域幅の割合が表示されます。この値は、WRR ウェイトをパーセント値で表したものです。

ステップ 3 [Apply] をクリックします。キューが設定され、実行コンフィギュレーション ファイルが更新されます。

CoS/802.1p 値のキューへのマッピング

[CoS/802.1p to Queue] ページでは、802.1p プライオリティを出力キューにマッピングできます。[CoS/802.1p 値のキューへのマッピング テーブル（CoS/802.1p to Queue Table] では、着信パケットの出力キューが、パケットの VLAN タグ内の 802.1p プライオリティに基づいて決定されます。タグなし着信パケットの場合、802.1p プライオリティは、入力ポートに割り当てられているデフォルトの CoS/802.1p プライオリティです。

キューが 8 個の場合のデフォルトのマッピングを、以下の表に示します。

802.1p 値（0 ～ 7。プライオリティは 7 が最高）	キュー（キューが 8 個（1 ～ 8）の場合。プライオリティは 8 が最高）	7 個のキュー	注記
0	1	1	バックグラウンド
1	2	1	ベスト エフォート
2	3	2	エクセレントエフォート
3	6	5	基幹アプリケーション：LVS 電話の SIP
4	5	4	ビデオ
5	8	7	音声：Cisco IP Phone のデフォルト
6	8	7	インターワーク制御 LVS 電話の RTP
7	7	6	ネットワーク制御

CoS/802.1p 値とキューのマッピング（[CoS/802.1p to Queue]）、キューのスケジュール方式と帯域割り当てを調整することにより、ネットワークでのサービス品質目標を達成できます。

CoS/802.1p 値からキューへのマッピングは、次のいずれかの場合にのみ適用されます。

- デバイスが QoS 基本モードかつ CoS/802.1p 信頼モードである場合。
- デバイスが QoS 拡張モードであり、CoS/802.1p が信頼されているフローにパケットが属する場合。

CoS 値を出力キューにマッピングするには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [CoS/802.1p to Queue] をクリックします。

ステップ 2 パラメータを入力します。

- [802.1p]：出力ポートを割り当てる 802.1p 値が表示されます。プライオリティは 0が最低、7 が最高です。
- [出力キュー] : 802.1p 値に割り当てる出力キューを選択します。サポートされる出力キュー数は 4 個または 8 個のいずれかです。キュー 4 またはキュー 8 が最高のプライオリティの出力キューで、キュー 1 が最低のプライオリティの出力キューです。

ステップ 3 それぞれの 802.1p プライオリティをマッピングする出力キューを選択します。

ステップ 4 [Apply]、[Cancel]、または [Restore Defaults] をクリックします。801.1p プライオリティ値がキューにマッピングされて実行コンフィギュレーション ファイルが更新されるか、入力された変更がキャンセルされるか、または以前に定義された値が復元されます。

DSCP値のキューへのマッピング

[DSCP (IP Differentiated Services Code Point) to Queue] ページでは、DSCP 値が出力キューにマッピングされます。[DSCP to Queue Table] では、着信パケットの出力キューが、パケットの DSCP 値に基づいて決定されます。着信パケットの元の VPT（VLAN プライオリティ タグ）値は変更されません。

DSCP 値とキューのマッピング、キューイングモード、および帯域割り当てを調整することにより、ネットワーク上でサービス品質目標を達成できます。

次の場合、DSCP 値のキューへのマッピングに IP パケットに適用できます。

- デバイスが QoS 基本モードであり、かつ DSCP が信頼モードである場合。
- デバイスが QoS 拡張モードであり、パケットが DSCP 信頼であるフローに属する場合。

非 IP パケットは、常にベスト エフォート キューに格納されます。

8 キューシステムでの DSCP からキューへのデフォルトマッピングを、以下の表に示します。7 が最高であり、8 はスタックコントロール用に使用されます。

DSCP	63	55	47	39	31	23	15	7
キュー	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
キュー	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
キュー	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
キュー	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
キュー	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
キュー	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1

キュー	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
キュー	6	6	6	7	6	6	1	1

8 キューシステムの場合の DSCP 値のキューへのデフォルトのマッピングを、以下の表に示します。8 が最高です。

DSCP	63	55	47	39	31	23	15	7
キュー	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
キュー	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
キュー	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
キュー	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
キュー	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
キュー	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
キュー	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
キュー	7	7	7	8	7	7	1	2

DSCP をキューにマッピングするには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [DSCP to Queue] をクリックします。

[DSCP値のキューへのマッピング] ページには、[入力DSCP] フィールドが含まれています。このフィールドには着信パケットの DSCP 値とその関連クラスが表示されます。

ステップ 2 [出力キュー] で、DSCP 値をマッピングする出力キュー（トラフィック フォワーディング キュー）を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。デフォルト設定に戻すには、[Restore Defaults] をクリックします。

帯域幅

（注） この設定は、[Advanced Setting] ビューでのみ使用できます。

[Bandwidth] ページには、各インターフェイスの帯域幅情報が表示されます。帯域幅情報を表示するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [Bandwidth] をクリックします。

このページのフィールドは、次のフィールドを除いて、下記の [Edit] ページで説明されています。

- **[入力レート制限]**：
  - [ステータス]：入力レート制限が有効になっているかどうかが表示されます。
  - [Rate Limit (KBits/sec)]：ポートの入力レート制限が表示されます。
  - [%]：ポートの入力レート制限を合計ポート帯域幅で割った値が表示されます。
  - [CBS (Bytes)]：データのバイトに含まれる入力インターフェイスの最大バーストデータサイズ。
- [Egress Shaping Rates]：
  - [Status]：出力シェーピング レートが有効になっているかどうかが表示されます。
  - [CIR (キロビット/秒)]：出力インターフェイスの最大帯域幅が表示されます。
  - [CBS (Bytes)]：データのバイトに含まれる出力インターフェイスの最大バーストデータサイズ。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ステップ 3 [ポート] または [LAG] インターフェイスを選択します。

ステップ 4 選択したインターフェイスに関する次のフィールドの値を入力します。

オプション	説明
入力レート制限	入力レート制限を有効にする場合、このフィールドを選択します。具体的な値はその下のフィールドで定義します（LAGとは無関係です）。
[Ingress Rate Limit (Kbits per sec)]	このインターフェイスで使用できる最大帯域幅を入力します（LAGとは無関係です）。
入力認定バーストサイズ(CBS)	データのバイトに含まれる入力インターフェイスの最大バーストデータサイズを入力します。帯域幅が一時的に許容範囲を超えて増加する

オプション	説明
	場合でも、この量を送信できます。このフィールドは、インターフェイスがポートの場合にのみ使用できます（LAG とは無関係です）。
出力シェーピングレート	このインターフェイスで出力シェーピングを有効にする場合、このフィールドを選択します。
認定情報レート（CIR）[にんていじょうほうれーとCIR]	出力インターフェイスの最大帯域幅を入力します。
出力認定バーストサイズ(CBS)	データのバイトに含まれる出力インターフェイスの最大バーストデータサイズを入力します。帯域幅が一時的に許容範囲を超えて増加する場合でも、この量を送信できます。

ステップ 5 [Apply] をクリックします。帯域幅設定は、実行コンフィギュレーション ファイルに書き込まれます。

キューあたりの出力シェーピング

この設定は、[Advanced Setting] ビューでのみ使用できます。

このデバイスでは、[Bandwidth] ページにおいてポート単位で入出力レートを制限できるだけでなく、選択した出力フレームの入出力レートをキュー単位、ポート単位で制限することもできます。出力レートを制限するには、出力負荷をシェーピングします。

このデバイスでは、管理フレーム以外のすべてのフレームを制限できます。制限されていないフレームは、レートの計算では無視されます。つまり、フレームのサイズは制限の合計に含まれません。

キューごとに出力シェーピングを設定するには、次の手順を実行します。

ステップ 1 **[Quality of Service]** > **[General]** > **[Egress Shaping per Queue]** をクリックします。

[Egress Shaping Per Queue] ページには、キューごとのレート制限（CIR）とバーストサイズ（CBS）が表示されます。

ステップ 2 インターフェイス タイプ（ポートまたは LAG）を選択し、[Go] をクリックします。

ステップ 3 ポート/LAG を選択して **[Edit]** をクリックします。

このページでは、インターフェイスごとに最大 8 個のキューに対して出力シェーピングを有効にすることができます。

ステップ 4 [Interface] を選択します。

ステップ 5 必要な各キューに関して、次のフィールドに入力します。

- [Enable Shaping]：選択すると、このキューで出力シェーピングが有効になります。

- [Committed Information Rate (CIR)]：最大レート（CIR）（Kbps 単位）を入力します。CIR は、送信できる平均最大データ量です。
- [Committed Burst Size (CBS)]：最大バースト サイズ（CBS）（バイト単位）を入力します。CBS は、バーストが CIR を超えても送信できるデータの最大バーストです。

ステップ 6 [Apply] をクリックします。帯域幅設定は、実行コンフィギュレーション ファイルに書き込まれます。

VLAN入力レート制限

この設定は、[Advanced Setting] ビューでのみ使用できます。

[VLAN 入力レート制限] ページで VLAN ごとにレート制限を実行すると、VLAN 上でのトラフィック制限が有効になります。VLAN 入力レート制限が設定されている場合、そのデバイス上のすべてのポートからの集約トラフィックが制限されます。

VLAN ごとのレート制限には、次の制約が適用されます。

- システム内で定義されている他のトラフィック ポリシングよりも低い優先度になります。たとえば、QoS レート制限と VLAN レート制限がパケットに適用されていて、それらのレート制限が競合する場合、QoS レート制限が優先されます。
- これはデバイス レベルで適用され、そのデバイス内部ではパケット プロセッサ レベルで適用されます。デバイス上に複数のパケット プロセッサがある場合、設定されている VLAN レート制限値が、各パケット プロセッサに個別に適用されます。ポート数が 24 個以下のデバイスの場合、パケット プロセッサは 1 個ですが、ポート数が 48 個以上のデバイスにはパケット プロセッサが 2 個あります。

レート制限は、ユニット中のパケット プロセッサごとに別個に計算されます。

VLAN 入力レート制限を定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [VLAN Ingress Rate Limit] をクリックします。

このページには、VLAN 入力レート制限テーブルが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [VLAN ID]：VLAN を選択します。
- [Committed Information Rate (CIR)]：VLAN に受け入れ可能な平均最大データ量（Kbps 単位）を入力します。
- [Committed Burst Size (CBS)]：出力インターフェイスの最大バースト データ サイズ（バイト単位）を入力します。帯域幅が一時的に許容範囲を超えて増加する場合でも、この量を送信できます。LAG の場合は入力できません。

ステップ 4 [Apply] をクリックします。VLAN レート制限が追加され、実行コンフィギュレーション ファイルが更新されます。

iSCSI

この設定は、[Advanced Setting] ビューでのみ使用できます。

このページでは、iSCSI最適化をアクティブにすることができます。これは、iSCSIトラフィックを他のタイプのトラフィックより優先するメカニズムのセットアップを意味します。この機能がデバイス上で有効になっている場合は、すべてのインターフェイス上のiSCSIトラフィックに定義済みの優先順位が割り当てられ、iSCSIトラフィックはインターフェイス上で設定されたACLまたはポリシールールの影響を受けなくなります。

iSCSIトラフィックは、iSCSIターゲットが要求をリッスンするTCPポートによって（また、必要に応じて、iSCSIターゲットが要求をリッスンするIPv4アドレスによっても）識別されます。デフォルトで、ウェルノウンTCPポート3260と860を使用した2つのiSCSI IPv4フローがデバイス上で定義されます。iSCSIフローの最適化は双方向に、つまり、ターゲットへとターゲットからの両方向のストリームに適用されます。

iSCSIトラフィックに優先順位を付け、必要であればマーキングするためのメカニズムを有効にして設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [iSCSI] をクリックします。

ステップ 2 [iSCSI Status] フィールドで [Enable] チェックボックスをオンにして、デバイス上の iSCSI トラフィックの処理を有効にします。

ステップ 3 [サービス設定の品質] の下のフィールドに入力します。

- [VPT Assignment]：[Unchanged] を選択してパケット内の元の VLAN プライオリティ タグ（VPT）値をそのまま使用するか、[Reassigned] フィールドに新しい値を入力します。
- [DSCP Assignment]：[Unchanged] を選択してパケット内の元の DSCP 値をそのまま使用するか、[Reassigned] フィールドに値を入力します。
- [キュー割り当て]：iSCSI トラフィックのキュー割り当てを入力します。デフォルトで、キュー 7 に割り当てられます。

ステップ 4 [Apply] をクリックして設定を保存します。

iSCSI フロー テーブルに、定義されたさまざまな iSCSI フローが表示されます。ウェルノウン TCP ポート 3260 および 860 を使用した 2 つの iSCSI フローが表示されます。これらのフローの [Flow Type] は [Default] です。新しいフローを追加すると、その [Flow Type] が [Static] になります。

新しいフローを追加するには、次の手順に従います。

ステップ 5 [Add] をクリックして、次のフィールドに入力します。

- [TCP Port]：これは、iSCSI ターゲットが要求をリッスンする TCP ポートの番号です。スイッチ上で最大 8 つのターゲット TCP ポートを設定できます。
- [Target IP Address]：iSCSI ターゲット（データの保存先）の IP アドレスを指定します。これは、iSCSI トラフィックの送信元でもあります。[Any] を選択して TCP ポートパラメータに基づいてフローを定義することも、[User-Defined] フィールドに IP アドレスを入力して特定のターゲットアドレスを定義することもできます。

ステップ 6 [Apply] をクリックして設定を保存します。

デフォルト フローを復元する場合は、[Restore Default Flows] をクリックします。

TCP 輻輳回避

この設定は、[Advanced Setting] ビューでのみ使用できます。

[TCP Congestion Avoidance] ページでは、TCP 輻輳回避アルゴリズムをアクティブにすることができます。このアルゴリズムは、さまざまな送信元が同じバイト カウントのパケットを送信しているためにノードで輻輳が発生している場合に、その輻輳ノードでの TCP グローバル同期を無効にするか、または回避します。

TCP 輻輳回避を設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [TCP Congestion Avoidance] をクリックします。

ステップ 2 [Enable] をクリックして TCP 輻輳回避を有効にして、[Apply] をクリックします。

QoS 基本モード

QoS 基本モードでは、ネットワーク内の特定のドメインを信頼できるものとして定義できます。そのドメイン内では、必要となるサービスのタイプを表すために、パケットに802.1pプライオリティやDSCPのマークが付けられます。そのドメイン内のノードでは、それらのフィールドを使用して、パケットが特定の出力キューに割り当てられます。初期パケット分類およびそれらのフィールドのマーキングは、信頼できるドメインの入力において実行されます。

QoS のグローバルな設定

[Global Settings] ページには、デバイスで信頼を有効にするための情報が含まれています（後述の [Trust Mode] フィールドを参照）。QoS モードが基本モードの場合、この設定がアクティブになります。QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。

信頼設定を定義するには、以下の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Basic Mode] > [Global Settings] の順にクリックします。

ステップ 2 デバイスが基本モードまたは拡張モードになっているときに [Trust Mode] を選択します。パケットの CoS レベルと DSCP タグが個別のキューにマッピングされる場合、信頼モードが、パケットが割り当てられるキューを決定します。

- [CoS/802.1p]：トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて（着信パケットに VLAN タグがない場合）キューにマッピングされます。VPT とキューの実際のマッピングは、[mapping CoS/802.1p to Queue] ページで設定できます。
- DSCP：すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP のキューへの実際のマッピングは、[DSCP to Queue] ページで設定できます。トラフィックが IP トラフィックではない場合、ベストエフォートキューにマッピングされます。
- [CoS/802.1p、DSCP]：CoS/802.1p と DSCP のうち、いずれか設定されているほう。

ステップ 3 着信パケット中の元の DSCP 値を、DSCP オーバーライドテーブルに入力された新しい値でオーバーライドする場合は、[Override Ingress DSCP] を選択します。[Override Ingress DSCP] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

（注） フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 4 [DSCP Override Table] をクリックして、DSCP を再設定します。（「DSCP オーバーライド テーブル」を参照）。

ステップ 5 [DSCP In] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。[DSCP Out] の値は、発信値がマッピングされることを示す場合に選択します。

ステップ 6 [Apply] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP 値で更新されます。デフォルト設定に戻るには、[Restore Defaults] をクリックします。

QoS インターフェイス設定

[Interface Settings] ページでは、次のように、デバイスのポートごとに QoS を設定できます。

- インターフェイスに対して QoS 状態を無効にした場合：そのポートの着信トラ フィックはすべて、ベスト エフォート キューに格納されます。トラフィックの分類処 理およびプライオリティ設定処理は実行されません。
- ポートに対して QoS 状態を有効にした場合：そのポートに届いたトラフィックは、システム規模でグローバルに設定された信頼モード（CoS/802.1p 信頼モードまたは DSCP 信頼モード）に基づいて処理されます。

各インターフェイスの QoS 設定を入力するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Basic Mode] > [Interface Settings] をクリックします。

ステップ 2 フィルタを使用して [Interface Type] （[Port] または [LAG]）を選択し、[Go] をクリックして現在の設定を表示します。[QoS State] に、インターフェイスの QoS 状態（有効か無効か）が表示されます。

ステップ 3 インターフェイスを選択して、[Edit] をクリックします。

ステップ 4 [ポート] または [LAG] インターフェイスを選択します。

ステップ 5 [QoS State] で、このインターフェイスの QoS 状態（有効または無効）をクリックして設定します。

ステップ 6 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

QoS拡張モード

ACL に合致して着信が許可されたフレームは、暗黙的に、着信許可を出した ACL の名前がラベルとして付けられます。その後、それらのフローに、拡張モード QoS アクションを適用できます。

QoS 拡張モードでは、フローごとの QoS をサポートするポリシーがデバイスによって使用されます。ポリシーとそのコンポーネントには、次の特徴および関係性があります。

- ポリシーには 1 つ以上のクラス マップが含まれています。
- クラス マップは、関連する 1 つ以上の ACL でフローを定義します。クラス マップの中の許可（転送）アクションをともなう ACL ルール（ACE）のみに合致するパケットは、同じフローに属するものと見なされ、同じサービス品質が適用されます。そのようにして、1 つのポリシーに 1 つ以上のフローが含まれ、そのそれぞれにユーザ定義 QoS があります。
- クラス マップ（フロー）の QoS は、関連するポリサーによって適用されます。ポリサーには、シングル ポリサーと集約ポリサーの 2 種類があります。それぞれのポリサーは、QoS 仕様により設定されます。シングル ポリサーは、そのポリサーの QoS 仕様に基づいて QoS を単一のクラス マップに、したがって単一のフローに適用します。集約ポリサーは、1 つ以上のクラス マップに、したがって 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラス マップをサポート可能です。

  2 レート 3 カラー（2R3C）機能がデバイスでサポートされます。この機能では、すべてのポリサーに 2 つのしきい値が割り当てられます。1 つ目のしきい値に到達すると、ユーザ設定の超過アクションが実行されます。2 つ目のしきい値に到達すると、ユーザー設定の違反アクションが実行されます。
- フローごとの QoS は、ポリシーを目的のポートにバインドすることによりフローに適用されます。1 つのポリシーとそのクラス マップを 1 つ以上のポートにバインドすることは可能ですが、各ポートは 1 つのポリシーにしかバインドされません。

グローバル設定

[Global Settings] ページには、デバイスで信頼を有効にするための情報が含まれています。QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。

信頼設定を定義するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Global Settings] をクリックします。

ステップ 2 デバイスが拡張モードになっているときに [Trust Mode] を選択します。パケットの CoS レベルと DSCP タグが個別のキューにマッピングされる場合、信頼モードが、パケットが割り当てられるキューを決定します。

- [CoS/802.1p]：トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて（着信パケットに VLAN タグがない場合）キューにマッピングされます。VPT とキューの実際のマッピングは、[mapping CoS/802.1p to Queue] ページで設定できます。
- DSCP：すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP のキューへの実際のマッピングは、[DSCP to Queue] ページで設定できます。トラフィックが IP トラフィックではない場合、ベストエフォートキューにマッピングされます。
- [CoS/802.1p-DSCP]：選択すると、非 IP トラフィックに信頼 CoS モードが使用され、IP トラフィックに信頼 DSCP が使用されます。

ステップ 3 [Default Mode Status] フィールドで、インターフェイスのデフォルトの拡張モード QoS 信頼モード（信頼できるかどうか）を選択します。これにより、拡張 QoS で基本 QoS の機能が提供されるため、拡張 QoS においてデフォルトで（ポリシーを作成することなく）CoS/DSCP を信頼できます。

ステップ 4 [QoS Advanced Mode] で、[Default Mode Status] が [Not Trusted] に設定されている場合、インターフェイスで設定されているデフォルトの CoS 値は無視され、すべてのトラフィックがキュー 1 に送られます。詳細については、[Quality of Service] > [QoS Advanced Mode] > [Global Settings] ページを参照してください。

ステップ 5 インターフェイス上にポリシーがある場合、デフォルトモードは無効になり、ポリシー設定に従ったアクションになって、合致しないトラフィックはドロップされます。

ステップ 6 DSCP オーバーライドテーブルに従って、着信パケット中の元の DSCP 値を新しい値でオーバーライドする場合は、[入力DSCPのオーバーライド] を選択します。[Override Ingress DSCP] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

（注） フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 7 [Override Ingress DSCP] を有効にした場合は、[DSCP Override Table] をクリックして DSCP を設定しなおします。

a) [DSCP Override Table] で、次のフィールドに入力します。

- [DSCP入力]：着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。

• [DSCP出力]：発信値がマッピングされることを示す場合に DSCP 出力値を選択します。

b) [Apply] をクリックします。デフォルト設定に戻るには、[Restore Defaults] をクリックします。

アウト オブ プロファイル DSCP リマーク

クラスマップ（フロー）にポリサーが割り当てられている場合、1 つまたは複数のフロー内のトラフィック量が QoS で指定されている制限を超えた場合に実行されるアクションを指定できます。トラフィックのうち、フローが QoS 制限を超過する原因となった部分は、アウトオブプロファイルパケットと呼ばれます。超過アクションがアウトオブプロファイル DSCP の場合、デバイスにより、アウトオブプロファイル IP パケットの元の DSCP 値が、アウトオブプロファイル DSCP リマークテーブルに基づく新しい値を使用してマッピングし直されます。デバイスは、新しい値を使用して、それらのパケットにリソースと出力キューを割り当てます。また、アウトオブプロファイルパケット中の元の DSCP 値も、デバイスによって新しい DSCP 値に物理的に置き換えられます。

アウト オブ プロファイル DSCP 超過アクションを使用するには、アウト オブ プロファイル DSCP リマーク テーブルで DSCP 値を再マッピングします。そうしない場合、アクションは空になります。これは、工場出荷時設定では、パケットが、このテーブルの DSCP 値により、その値そのものに再マッピングされるためです。この機能により、信頼 QoS ドメイン間で切り替えられる着信トラフィックの DSCP タグが変更されます。あるドメインで使用されている DSCP 値が変更されると、そのタイプのトラフィックのプライオリティが、他のドメインで使用されている DSCP 値に対して設定され、同じタイプのトラフィックが識別されるようになります。これらの設定値は、システムが QoS 拡張モードの場合にアクティブになり、一度アクティブになるとグローバルにアクティブになります。これは、QoSプロパティ （1 ページ）で設定できます。

DSCP 値をマッピングするには、次の手順を実行します。

ステップ 1 **[Quality of Service]** > **[QoS Advanced Mode]** > **[Out of Profile DSCP Remarking]** の順にクリックします。このページで、デバイスを出入りするトラフィックの DSCP 値を設定することができます。

[DSCP In] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。

ステップ 2 着信値のマッピング結果となる [DSCP Out] 値を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP リマーク テーブルで更新されます。

ステップ 4 このインターフェイスの CoS 情報を工場出荷時の設定に戻すには、[Restore Defaults] をクリックします。

クラスマッピング

クラス マップは、そこで定義されている ACL（アクセス制御リスト）を使用してトラフィック フローを定義します。MAC ACL、IP ACL、および IPv6 ACL を組み合わせて、クラス マップを作成できます。クラスマップは、すべて合致か、いずれかが合致という形でパケット条件に合致するように設定されます。パケット合致は、ファーストフィット方式で判定されます。つまり、最初に合致したクラスマップに関連付けられたアクションが、システムの実行するアクションになります。複数のパケットが同じクラスマップに合致する場合、それらのパケットは同じフローに属するものと見なされます。

（注） クラスマップの定義は QoS には影響しません。これは暫定的な手順であり、後でクラスマップを使用できるようにします。

より複雑なルールセットが必要になる場合、複数のクラスマップを、ポリシーと呼ばれるスーパーグループにまとめることができます。

同一のクラスマップでは、宛先 IPv6 アドレスがフィルタリング条件として設定されている IPv6 ACE と同時に MAC ACL を使用することはできません。

[Class Mapping] ページには、定義されているクラス マップとそのそれぞれを構成する ACL のリストが表示されます。このページで、クラスマップを追加または削除することができます。

クラスマップを定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Class Mapping] をクリックします。

クラス マップごとに、そこで定義されている ACL が、それらの ACL 間の関係とともに表示されます。最大 3 つの ACL を [Match] とともに表示できます。[Match] は [And] または [Or] のどちらかにすることができます。これは、ACL 間の関係を示しています。クラス マップは、3 つの ACL を And または Or のどちらかで結合した結果になります。

ステップ 2 [Add] をクリックします。

1 つまたは 2 つの ACL を選択し、クラス マップの名前を指定すると、新しいクラス マップが追加されます。クラス マップの ACL が 2 つの場合、フレームが両方の ACL に合致しなければならないのか、それとも選択された ACL のいずれか一方または両方に合致しなければならないのかを指定できます。

ステップ 3 パラメータを入力します。

- [Class Map Name]：新しいクラス マップの名前を入力します。
- [Match ACL Type]：クラス マップで定義されているフローに属すると見なされるためにパケットが合致しなければならない条件。次のオプションがあります。
  - [IP]：パケットは、クラスマップの IP ベース ACL のいずれかに合致しなければなりません。
  - [MAC]：パケットは、クラスマップの MAC ベース ACL のいずれかに合致しなければなりません。

- [IP and MAC]：パケットは、クラスマップの IP ベース ACL と MAC ベース ACL に合致しなければなりません。
- [IP or MAC]：パケットは、クラスマップの IP ベース ACL または MAC ベース ACL のいずれかに合致しなければなりません。

- [IP]：クラス マップの IPv4 ベース ACL または IPv6 ベース ACL を選択します。
- [MAC]：クラスマップの MAC ベースの ACL を選択します。
- [Preferred ACL]：パケットを IP と MAC のどちらと最初に照合するのかを選択します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

集約ポリサー

定義済みのルールセットに一致するトラフィックのレートを測定できます。制限を適用するには、1 つ以上のクラスマップで ACL を使用して目的のトラフィックに一致させ、ポリサーを使用して照合トラフィックに QoS を適用します。

ポリサーは、QoS 仕様により設定されます。ポリサーには、次の 2 種類があります。

- シングル（標準）ポリサー：シングル ポリサーは、そのポリサー QoS 仕様に基づいて QoS を単一のクラスマップに、そして単一のフローに適用します。シングルポリサーを使用するクラスマップが複数のポートにバインドされている場合、各ポートにはそのシングルポリサーの独自のインスタンスがあります。したがって、それぞれが互いに独立したポートで、クラスマップ（フロー）に QoS を適用します。シングル ポリサーは、[Policy Table] ページで作成されます。
- 集約ポリサー：集約ポリサーは、1 つ以上のクラス マップに、そして 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラスマップをサポート可能です。集約ポリサーは、ポリシーやポートに関係なく、集約されたすべてのフローに QoS を適用します。集約ポリサーは、[Aggregate Policer] ページで作成されます。

  集約ポリサーは、ポリサーを複数のクラスで共有する場合に定義されます。あるポートのポリサーを、別のデバイスの他のポリサーと共有することはできません。

各ポリサーは、次のパラメータを組み合わせたそれぞれ独自の QoS 仕様により定義されます。

- [Peak Enforcement]：選択すると、ピーク バースト サイズを超えた場合のアクションが有効になります。
- [Peak Information Rate (PIR)]：ピーク トラフィック レート（PIR）をキロビット/秒（kbps）単位で入力します。
- [Peak Burst Size (PBS)]：ピークバーストサイズ（PIR）をバイト単位で入力します。
- [Violate Action]：ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。

- [Drop]：ピーク サイズに違反したフレームをドロップします。
- [Out-of-Profile DSCP]：事前に設定したDSCP値でピークサイズを超えているフレームをマークします。

- 最大許容レート（「認定情報レート（CIR）」と呼ばれる）（Kbps 単位）。
- トラフィック量（「認定バースト サイズ（CBS）」と呼ばれる）（バイト単位）。これは、定義されている最大レートを超える場合にも一時的なバーストとして通過を許可されるトラフィックです。
- 制限を超えるフレーム（「アウト オブ プロファイル トラフィック」と呼ばれる）に適用されるアクション。そのようなフレームは、そのまま通過させられるか、ドロップされるか、あるいは通過させられた上で新しいDSCP値に再マッピングされ、そのデバイス内の以降のすべての処理ではプライオリティが低いフレームとなるようにマークされます。
- 指定されたレートに基づいてトラフィックポリシングを設定し、オプションのアクションを実行します。 CIR とそれらのオプションの値およびアクションを入力します。

ポリサーをクラス マップに割り当てる処理は、クラス マップがポリシーに追加される時点で実行されます。ポリサーが集約ポリサーの場合は、[Aggregate Policer]ページを使用してそれを作成する必要があります。

集約ポリサーを定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Aggregate Policer] をクリックします。

このページには、既存の集約ポリサーが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [集約ポリサー名]：集約ポリサーの名前を入力します。
- [Ingress Committed Information Rate (CIR)]：許可される最大帯域幅（bps単位）を入力します。帯域幅（7 ページ）の説明を参照してください。
- [Ingress Committed Burst Size (CBS)]：CIR を超えていても通過を許可される最大バースト サイズ（バイト単位）を入力します。帯域幅 （7 ページ）の説明を参照してください。
- [超過アクション]：CIR を超える着信パケットに対して実行するアクションを選択します。値は次のとおりです。
  - ドロップ（Drop）：定義済みの CIR 値を超えるパケットはドロップされます。
  - [Out of Profile DSCP]：定義されている CIR 値を超えるパケットの DSCP 値は、アウト オブ プロファイル DSCP リマーク テーブルに基づく値に再マッピングされます。
- [Peak Enforcement]：選択すると、ピーク バースト サイズを超えた場合のアクションが有効になります。

- [Peak Information Rate (PIR)]：ピーク トラフィック レート（PIR）をキロビット/秒（kbps）単位で入力します。
- [Peak Burst Size (PBS)]：ピークバーストサイズ（PIR）をバイト単位で入力します。
- [Violate Action]：ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。
  - [Drop]：ピーク サイズに違反したフレームをドロップします。
  - [Out-of-Profile DSCP]：事前に設定した DSCP 値でピークサイズを超えているフレームをマークします。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ポリシーテーブル

[Policy Table Map] ページには、システム内で定義されている拡張 QoS ポリシーのリストが表示されます。このページでは、ポリシーを作成および削除できます。インターフェイスにバインドされているポリシーのみがアクティブになります（ポリシーバインディング （22 ページ）を参照）。

各ポリシーは、次のもので構成されます。

- ポリシーでトラフィック フローを定義する ACL の 1 つ以上のクラス マップ。
- ポリシーでトラフィック フローに QoS を適用する 1 つ以上の集約。

ポリシーが追加された後、[Policy Table] ページを使用してクラスマップを追加することができます。QoS ポリシーを追加するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Table] をクリックします。

このページには、定義されているポリシーのリストが表示されます。

ステップ 2 [Policy Class Map Table] をクリックして、[Policy Class Maps] ページを表示するか、または [Add] をクリックして、[Add Policy Table] ページを表示します。

ステップ 3 [New Policy Name] フィールドに、新しいポリシーの名前を入力します。

ステップ 4 [Apply] をクリックします。QoS ポリシー プロファイルが追加され、実行コンフィギュレーション ファイルが更新されます。

ポリシークラスマップ

ポリシーには 1 つ以上のクラス マップを追加できます。クラス マップは、同じトラフィック フローに属すると見なされるパケットのタイプを定義します。

クラス マップをポリシーに追加するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Class Maps] をクリックします。

ステップ 2 [Filter] でポリシーを選択し、[Go] をクリックします。そのポリシー内のすべてのクラスマップが表示されます。

ステップ 3 新しいクラス マップを追加するには、[Add] をクリックします。

ステップ 4 次のパラメータを入力します。

[Policy Name]	クラスマップの追加先のポリシーが表示されます。
クラス マップ名	ポリシーに関連付ける既存のクラスマップを選択します。クラスマップは[Class Mapping] ページで作成されます。
アクション タイプ	一致するすべてのパケットの入力CoS/802.1pやDSCPの値に関するアクションを選択します。 • [Use default trust mode]：このオプションが選択されている場合は、グローバル信頼モードでデフォルトモードステータスを使用します。デフォルトモード ステータスが「Not Trusted」（信頼できない）の場合は、入力CoS/802.1pやDSCPの値が無視され、合致したパケットはベストエフォートとして送信されます。 • [Always Trust]：このオプションが選択されている場合は、デバイスがグローバル信頼モード（[Global Settings] ページで選択）に基づいて一致したパケットを信頼します。デフォルト モード ステータス（[Global Settings] ページで選択）は無視されます。 • [設定]：このオプションが選択されている場合は、[新しい値] ボックスに入力された値を使用することにより、合致パケットの出力キューが以下のように判別されます。 新しい値 (0..7) が CoS/802.1p プライオリティである場合は、そのプライオリティ値と [CoS/802.1p to Queue Table] を使用して、すべての合致パケットの出力キューを判別します。 新しい値 (0..63) が DSCP である場合は、新しい DSCP と [DSCP to Queue Table] を使用して、合致するIPパケットの出力キューを判別します。これら以外の場合は、新しい値 (1..8) を、すべての合致パケットの出力キュー番号として使用します。
トラフィックリダイレクト	一致するトラフィックをリダイレクトするかどうかを選択します。リダイレクトする場合は、トラフィックをリダイレクトするユニット/ポートを選択します。

トラフィックミラー	トラフィックフローをアナライザ イーサネット ポートにミラーリングするように設定します。このオプションが選択されている場合、トラフィックはSPANセッション ID 1 で指定された宛先ポートにミラーリングされます。SPAN セッション ID 1 でターゲットポートが指定されていない場合、ミラーアクションは無効です。トラフィック ミラー アクションをともなうポリシー クラス マップがインターフェイスに適用され、その同じインターフェイスが SPAN セッション 1 の送信元ポートとして定義されている場合は、特定のフローだけでなく、すべてのトラフィックがミラーリングされます。 トラフィック ミラー アクションが設定されている場合でも、インターフェイスに適用されたポリシー（およびACL）の追加のルールとアクションは依然として適用されます。次に例を示します。 • ミラー対象フローの ACL アクションが許可されている場合は、ミラーリングに加えて、フロートラフィックも転送されます。フロー ACL のアクションが拒否になっている場合、フロートラフィックはミラーリングされますが、出力ネットワークインターフェイスに転送されません（ドロップ動作）。 • ポリシーが適用されるインターフェイス上のトラフィックフローがミラー対象のクラスマップ分類と一致しない場合は、デフォルトポリシーのデフォルトアクションに従います。
ポリシングタイプ	ポリシーのポリサー タイプを選択します。次のオプションがあります。 • [None]：ポリシーは使用されません。 • [Single]：ポリシーのポリサーはシングル ポリサーです。 • [集約]：ポリシーのポリサーは集約ポリサーです。

ステップ 5 [Police Type] が [Aggregate] の場合は、[Aggregate Policer] を選択します。

ステップ 6 [Police Type] が [Single] である場合は、次の QoS パラメータを入力します。

入力認定情報レート(CIR)	CIR を Kbps 単位で入力します。この説明については、帯域幅ページを参照してください。
入力認定バーストサイズ(CBS)	CBS をバイト単位で入力します。この説明については、帯域幅ページを参照してください。
超過アクション	CIR を超える着信パケットに割り当てるアクションを選択します。次のオプションがあります。 • ドロップ（Drop）：定義済みの CIR 値を超えるパケットはドロップされます。 • [Out of Profile DSCP]：定義されている CIR 値を超える IP パケットは、アウト オブ プロファイル DSCP リマーク テーブルに由来する新しい DSCP を使用して転送されます。

ピーク強制	ピークバーストサイズを超えたときにアクションを有効にする場合に選択します。
最大情報レート(PIR)	ピークトラフィックレート（PIR）をキロビット/秒（kbps）単位で入力します。
最大バーストサイズ(PBS)	ピークバーストサイズ（PIR）をキロビット/秒（kbps）単位で入力します。
違反アクション	ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。 • [Drop]：ピーク サイズに違反したフレームをドロップします。 • [Out of Profile DSCP]：事前に設定した DSCP 値でピークサイズを超えているフレームをマークします。

ステップ 7 [Apply] をクリックします。

ポリシーバインディング

[Policy Binding] ページには、どのポリシープロファイルがどのポートにバインドされているかが表示されます。ポリシーは入力ポリシーまたは出力ポリシーとしてインターフェイスにバインドできます。ポリシープロファイルは、特定のポートにバインドされている場合、そのポートでアクティブになっています。ポートごとおよび方向ごとに設定できるポリシープロファイルは 1 つだけです。ただし、1 つのポリシーを複数のポートにバインドできます。

ポリシーがポートにバインドされている場合、ポリシーで定義されているフローに属するトラフィックがフィルタリングされ、それに QoS が適用されます。

ポリシーを編集するには、まず、バインド先のすべてのポートからそのポリシーを削除（アンバインド）する必要があります。

（注） ポートは、ポリシーまたは ACL にバインドできますが、両方にバインドすることはできません。

ポリシーバインディングを定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Binding] をクリックします。

ステップ 2 必要に応じて、[Interface Type] を選択します。

ステップ 3 [Go] をクリックします。そのインターフェイスのポリシーが表示されます。

ステップ 4 [Edit] をクリックします。

ステップ 5 入力ポリシー/インターフェイスに関して次の項目を選択します。

- [Input Policy Binding]：入力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]：バインドする入力ポリシーを選択します。

- [Default Action]：パケットがポリシーと合致した場合のアクションを選択します。
  - [Deny Any]：インターフェイス上のパケットがいずれかのポリシーと合致するときに転送する場合に選択します。
  - [Permit Any]：インターフェイス上のパケットがいずれのポリシーにも一致しないときに転送する場合に選択します。

    （注） [Permit Any] を定義できるのは、IP ソースガードがインターフェイス上でアクティブでない場合のみです。

ステップ 6 出力ポリシー/インターフェイスに関して次の項目を選択します。

- [Output Policy Binding]：出力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]：バインドする出力ポリシーを選択します。
- [Default Action]：パケットがポリシーと合致した場合のアクションを選択します。
  - [Deny Any]：インターフェイス上のパケットがいずれかのポリシーと合致するときに転送する場合に選択します。
  - [Permit Any]：インターフェイス上のパケットがいずれのポリシーにも一致しないときに転送する場合に選択します。

    （注） [Permit Any] を定義できるのは、IP ソースガードがインターフェイス上でアクティブでない場合のみです。

ステップ 7 [Apply] をクリックします。QoS ポリシー バインディングが定義され、実行コンフィギュレーション ファイルが更新されます。

QoS 統計情報

QoS 統計情報機能により、パケットがキューから転送される速度の統計情報と、デバイス上で認定パケット、適合パケット、または超過パケットがドロップされる速度の統計情報を収集できます。

シングルポリサー統計

[Single Policer Statistics] ページには、インターフェイスから受信したプロファイル内パケットおよびアウト オブ プロファイル パケットのうち、ポリシーのクラス マップで定義されている条件を満たすものの数が示されます。

（注） デバイスがレイヤ 3 モードの場合、このページは表示されません。

ポリサー統計情報を表示するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Single Policer Statistics] の順にクリックします。

このページには、次のフィールドが表示されます。

- [Interface]：このインターフェイスに関する統計情報が表示されます。
- [ポリシー]：このポリシーに関する統計情報が表示されます。
- [Class Map]：このクラス マップに関する統計情報が表示されます。
- [プロファイル内バイト]：受信したプロファイル内バイトの数。
- [Out-of-Profile Bytes]：受信したアウト オブ プロファイル バイトの数。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：統計情報を収集する対象のインターフェイスを選択します。
- [Policy Name]：ポリシー名を選択します。
- [Class Map Name]：クラス名を選択します。

ステップ 4 [Apply] をクリックします。統計情報に関する追加の要求が作成され、実行コンフィギュレーション ファイルが更新されます。

集約ポリサー統計

集約ポリサー統計情報を表示するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Aggregate Policer Statistics] をクリックします。

このページには、次のフィールドが表示されます。

- [集約ポリサー名]：統計の対象となるポリサー。
- [In-Profile Bytes]：受信されたプロファイル内パケットの数。
- [Out-of-Profile Bytes]：受信されたアウト オブ プロファイル パケットの数。

ステップ 2 [Add] をクリックします。

ステップ 3 [Aggregate Policer Name] で、統計情報表示の対象となる作成済みの集約ポリサーの 1 つを選択します。

ステップ 4 [Apply] をクリックします。統計情報に関する追加の要求が作成され、実行コンフィギュレーション ファイルが更新されます。

ステップ 5 特定の統計情報を削除するには、[Delete] をクリックします。

ステップ 6 選択したポリサーをクリアするには、[Clear Counters] をクリックします。

キュー統計情報

[Queues Statistics] ページには、転送されたパケットやドロップされたパケットなどに関する統計情報が、インターフェイスごと、キューごと、およびドロップ優先順位ごとに表示されます。

キュー統計情報を表示したり、表示する統計情報（カウンタセット）を定義したりするには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Queues Statistics] の順にクリックします。

このページには、次のフィールドが表示されます。

- [リフレッシュレート] : インターフェイスイーサネット統計情報がリフレッシュされるまでの時間を選択します。次のオプションを使用できます。
  - [No Refresh]：統計情報は更新されません。
  - [15 秒]：統計情報は 15 秒ごとにリフレッシュされます。
  - [30 Sec]：統計情報は 30 秒ごとに更新されます。
  - [60 Sec]：統計情報は 60 秒ごとに更新されます。

特定のユニットやインターフェイスを表示するには、フィルタでユニット/インターフェイスを選択して、[Go] をクリックします。

特定のインターフェイスを表示するには、フィルタでインターフェイスを選択して、[実行] をクリックします。

キュー統計情報テーブルに、各キューに関する次のフィールドが表示されます。

- [Queue]：このキューから転送またはテール ドロップされたパケット。
- [Transmitted Packets]：送信されたパケットの数。
- [テールドロップパケット数]：テール ドロップされたパケットの数。
- [送信バイト数]：送信されたバイトの数。
- [テールドロップバイト数]：テール ドロップされたバイトの数。

ステップ 2 選択したインターフェイスの統計情報カウンタをクリアするには、[Clear Interface Counters] をクリックします。

ステップ 3 すべてのインターフェイスの統計情報カウンタをクリアするには、[Clear All Interface Counters] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。