



Cisco IOS XE Gibraltar 16.12.x (Catalyst 9300 スイッチ) Quality of Service コンフィギュレーションガイド

初版：2019年7月31日

最終更新：2019年8月8日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

自動 QoS の設定 1

自動 QoS の前提条件 1

自動 QoS の制約事項 1

自動 QoS の設定に関する情報 2

自動 QoS の概要 2

自動 QoS 短縮機能の概要 3

自動 QoS グローバル設定テンプレート 3

自動 QoS ポリシーとクラスマップ 3

実行コンフィギュレーションでの自動 QoS の影響 3

実行コンフィギュレーションでの自動 QoS 短縮機能の影響 4

自動 QoS の設定方法 5

自動 QoS の設定 5

自動 QoS のアップグレード 8

自動 QoS 短縮機能のイネーブル化 10

自動 QoS の監視 11

自動 QoS に関するトラブルシューティング 11

自動 QoS の設定例 12

例 : auto qos trust cos 12

例 : auto qos trust dscp 14

例 : auto qos video cts 16

例 : auto qos video ip-camera 19

例 : auto qos video media-player 21

例 : auto qos voip trust 23

例 : auto qos voip cisco-phone 25

例 : auto qos voip cisco-software 28

例 : auto qos global compact 32

自動 QoS の関連情報 32

自動 QoS の機能履歴 33

第 2 章

QoS の設定 35

QoS の前提条件 35

QoS コンポーネント 36

QoS の用語 37

QoS の概要 37

モジュラ QoS コマンドライン インターフェイス 37

有線アクセスでサポートされる QoS 機能 38

階層型 QoS 38

QoS の実装 39

レイヤ 2 フレームのプライオリティ ビット 40

レイヤ 3 パケットのプライオリティ ビット 41

分類を使用したエンドツーエンドの QoS ソリューション 41

パケット分類 41

パケットと合わせて伝搬される情報に基づく分類 42

デバイス固有の情報に基づく分類 44

QoS 有線モデル 44

入力ポートのアクティビティ 44

出力ポートのアクティビティ 45

分類 45

アクセス コントロール リスト 45

クラス マップ 46

存続可能時間 (TTL) 分類 47

レイヤ 3 パケット長分類 48

レイヤ 2 SRC-Miss または DST-Miss の分類 49

ポリシー マップ 49

物理ポートのポリシー マップ 50

VLAN のポリシー マップ	51
QoS プロファイル	51
セキュリティグループ分類	51
SGT ベースの QoS	52
SGACL との DGID の共有	52
SGT ベースの QoS の制限	52
入力ポート FIFO (IPF) パーサー	53
ポリシング	55
トークンバケット アルゴリズム	55
マーキング	56
パケット ヘッダーのマーキング	56
スイッチ固有の情報のマーキング	57
テーブル マップのマーキング	57
トラフィックの調整	58
ポリシング	59
シングルレート 2 カラー ポリシング	59
デュアルレート 3 カラー ポリシング	60
シェーピング	60
クラスベース トラフィック シェーピング	61
キューイングおよびスケジューリング	61
帯域幅	63
帯域幅の割合	63
残存帯域幅の割合	63
重み付けテール ドロップ	64
重み付けテール ドロップのデフォルト値	64
プライオリティ キュー	65
プライオリティ キュー ポリサー	66
キュー バッファ	66
キュー バッファの割り当て	68
ダイナミック なしきい値および拡張	68
重み付けランダム早期検出	69

信頼動作	69
Cisco IP Phone の信頼境界機能のポート セキュリティ	69
有線ポートの信頼動作	70
標準 QoS のデフォルト設定	71
デフォルトの有線 QoS 設定	71
DSCP マップ	71
有線ターゲットの QoS に関する制約事項	73
QoS の設定方法	76
クラス、ポリシー、およびマップの設定	76
トラフィック クラスの作成	76
トラフィック ポリシーの作成	79
クラスベース パケット マーキングの設定	83
トラフィック ポリシーのインターフェイスへの適用	88
ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング	91
ポリシーマップによるトラフィックの分類およびマーキング	95
テーブル マップの設定	98
QoS の特性と機能の設定	101
帯域幅の設定	101
ポリシングの設定	103
プライオリティの設定	106
SGT ベースの QoS の設定	108
キューとシェーピングの設定	111
出力キューの特性の設定	111
キュー バッファの設定	111
キュー制限の設定	114
シェーピングの設定	117
シャープ プロファイル キューイングの設定	119
QoS のモニタリング	121
QoS の設定例	122
例 : TCP プロトコル分類	122

例：UDP プロトコル分類	123
例：RTP プロトコル分類	124
例：アクセス コントロール リストによる分類	124
例：サービス クラス レイヤ 2 の分類	125
例：サービス クラス DSCP の分類	125
例：VLAN ID レイヤ 2 の分類	125
例：DSCP 値または precedence 値による分類	125
例：階層型分類	126
例：階層型ポリシーの設定	126
例：音声およびビデオの分類	127
例：平均レート シェーピングの設定	128
例：キュー制限の設定	129
例：キュー バッファの設定	130
例：ポリシング アクションの設定	130
例：ポリサーの VLAN 設定	131
例：ポリシングの単位	131
例：シングルレート 2 カラー ポリシング設定	132
例：デュアルレート 3 カラー ポリシング設定	132
例：テーブル マップのマーキング設定	133
例：CoS マーキングを保持するテーブル マップの設定	133
次の作業	134
QoS に関する追加情報	134
QoS の機能履歴	134

第 3 章

重み付けランダム早期検出の設定	137
ネットワーク輻輳の回避	137
テール ドロップ	137
重み付けランダム早期検出	138
WRED の仕組み	138
WRED 重み計算	138
WRED 設定の制限	139

WRED 使用上の注意事項	139
WRED の設定	140
DSCP 値に基づく WRED の設定	140
サービス クラス値に基づく WRED の設定	141
IP プレシデンス値に基づく WRED の設定	143
WRED の設定例	144
階層化 QoS を使用した WRED のサポート	144
WRED 設定の確認	145
WRED 設定のベストプラクティス	146
重み付けランダム早期検出の機能履歴	148



第 1 章

自動 QoS の設定

- [自動 QoS の前提条件](#) (1 ページ)
- [自動 QoS の制約事項](#) (1 ページ)
- [自動 QoS の設定に関する情報](#) (2 ページ)
- [自動 QoS の設定方法](#) (5 ページ)
- [自動 QoS の監視](#) (11 ページ)
- [自動 QoS に関するトラブルシューティング](#) (11 ページ)
- [自動 QoS の設定例](#) (12 ページ)
- [自動 QoS の関連情報](#) (32 ページ)
- [自動 QoS の機能履歴](#) (33 ページ)

自動 QoS の前提条件

自動 QoS の前提条件は標準 QoS の前提条件と同じです。

自動 QoS の制約事項

次に、自動 QoS の制約事項を示します。

- 自動 QoS は、SVI インターフェイスではサポートされません。
- ビデオをサポートしている IP フォンには、**auto qos voip cisco-phone** オプションを設定しないでください。ビデオパケットには Expedited Forwarding (EF; 完全優先転送) プライオリティが設定されていないため、このオプションを使用すると、ビデオパケットの DSCP マーキングが上書きされ、これらのパケットが **class-default** クラスに分類されます。
- 自動 QoS が **auto qos voip cisco-phone** コマンドを使用するスタートアップ コンフィギュレーションから実行コンフィギュレーションにプッシュされた場合、自動 QoS によって設定は生成されません。これは予期された動作であり、これにより、**auto qos voip cisco-phone** コマンドがスタートアップ コンフィギュレーションからプッシュされるたびに、ユーザーが作成したカスタマイズ済みの QoS ポリシーがデフォルト設定 (ある場合) で上書きされないようにします。

この制限に対し、次のいずれかの回避策を使用できます。

- スイッチのインターフェイスで **auto qos voip cisco-phone** コマンドを手動で設定します。
- 新しいスイッチでは、スタートアップ コンフィギュレーションから自動 QoS コマンドをプッシュする場合は、コマンドに標準テンプレートの一部として次の項目をそれぞれ含める必要があります。
 1. インターフェイス レベル：
 - **trust device cisco-phone**
 - **auto qos voip cisco-phone**
 - **service-policy input** AutoQos-4.0-CiscoPhone-Input-Policy
 - **service-policy output** AutoQos-4.0-Output-Policy
 2. グローバル レベル：
 - クラスマップ
 - ポリシーマップ
 - ACL (ACE)
- **auto qos voip cisco-phone** コマンドがインターフェイスですでに設定されているが、ポリシーが生成されていない場合は、すべてのインターフェイスからコマンドを無効にして、各インターフェイスでコマンドを手動で再設定します。

自動 QoS の設定に関する情報

自動 QoS の概要

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。

スイッチはMQCモデルを採用しています。これは、特定のグローバルコンフィギュレーションを使用する代わりに、スイッチ上のインターフェイスに適用された自動QoSが複数のグローバルクラスマップとポリシーマップを設定することを意味します。

自動 QoS はトラフィックを照合し、各一致パケットを **qos-group** に割り当てます。これにより、出力ポリシーマップは、プライオリティ キューを含む特定のキューに、特定の **qos-group** を配置できます。

QoS は、着信と発信の両方向で必要です。着信時に、スイッチ ポートは、パケットの DSCP を信頼する必要があります (デフォルトで実行されます)。発信時に、スイッチポートは、音

声パケットに「front of line」プライオリティを付与する必要があります。音声が発信キューの他のパケットの後ろで待機して、遅延が長くなりすぎる場合、パケットの受信時間の範囲外となるため、エンドホストは、そのパケットをドロップします。

自動 QoS 短縮機能の概要

自動 QoS コマンドを入力すると、CLI からコマンドを入力する場合と同様に、生成されたすべてのコマンドがスイッチにより表示されます。自動 QoS 短縮機能を使用して、実行コンフィギュレーションから自動 QoS が生成したコマンドを非表示にできます。これにより、実行コンフィギュレーションを容易に把握でき、またメモリをより効率的に使用できるようになります。

自動 QoS グローバル設定テンプレート

一般に、自動 QoS コマンドは、ACL または DSCP で一致する、またはアプリケーションクラスに送信されるトラフィックを識別する CoS 値で一致する一連のクラスマップを生成します。また、生成されたクラスに一致する入力ポリシーや、設定されている帯域幅にクラスをポリシングする入力ポリシーも生成されます。8つの出力キュークラスマップが生成されます。実際の出力の出力ポリシーは、この8つの出力キュークラスマップのそれぞれにキューを割り当てます。

自動 QoS コマンドは、必要なテンプレートだけを生成します。たとえば、新しい自動 QoS コマンドを初めて使用するときに、8つのキュー出力サービスポリシーを定義するグローバル設定が生成されます。この時点から、他のインターフェイスに適用された自動 QoS コマンドは、出力キューのテンプレートを生成しません。これは、新しい自動 QoS コマンドが最初に使用されてから生成された同じ8つのキューモデルに、すべての自動 QoS コマンドが依存しているためです。

自動 QoS ポリシーとクラスマップ

適切な自動 QoS コマンドを入力すると、次のアクションが実行されます。

- 特定のクラスマップが作成されます。
- 特定のポリシーマップ（入力および出力）が作成されます。
- 指定したインターフェイスにポリシーマップが適用されます。
- インターフェイスの信頼レベルが設定されます。

実行コンフィギュレーションでの自動 QoS の影響

自動 QoS がイネーブルになると、**auto qos** インターフェイスコンフィギュレーションコマンドおよび生成されたグローバルコンフィギュレーションが実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザー設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションが警告なしで発生する可能性があります。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザー入力の設定は実行コンフィギュレーション内に残ります。上書きされなかったユーザー入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できません。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

実行コンフィギュレーションでの自動 QoS 短縮機能の影響

自動 QoS 短縮機能をイネーブルにした場合：

- CLI から入力された自動 QoS コマンドだけが実行コンフィギュレーションに表示されません。
- 生成されるグローバルコンフィギュレーションおよびインターフェイスコンフィギュレーションは表示されません。
- コンフィギュレーションを保存するときに、入力した自動 QoS コマンドだけが保存されます（非表示のコンフィギュレーションは保存されません）。
- スイッチをリロードすると、保存された自動 QoS コマンドがシステムにより検出、再実行され、AutoQoS SRND4.0 に準拠したコンフィギュレーションセットが生成されます。



(注) 自動 QoS 短縮機能がイネーブルである場合は、自動 QoS 生成コマンドを変更しないでください。これは、スイッチのリロード時にユーザー変更がオーバーライドされるためです。

自動 QoS グローバル短縮機能をイネーブルにした場合：

- **show derived-config** 非表示の AQC 派生コマンドを表示するには、コマンドを使用します。
- AQC コマンドはメモリに保存されません。これらは、スイッチがリロードされるたびに再生成されます。
- 短縮機能がイネーブルである場合、自動 QoS により生成されたコマンドは変更しないでください。
- 自動 QoS でインターフェイスが設定されており、AQC をディセーブルにする必要がある場合は、最初に自動 QoS をインターフェイス レベルでディセーブルにする必要があります。

自動 QoS の設定方法

自動 QoS の設定

QoS パフォーマンスを最適化するには、ネットワーク内のすべてのデバイスで自動 QoS を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id 例 : Device(config)# interface HundredGigE 1/0/1	VoIP ポートやビデオ デバイスに接続されているポート、またはネットワーク内部の他の信頼できるスイッチまたはルータに接続されているアップリンク ポートを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	自動 QoS 設定によって、次のコマンドの 1 つを使用します。 <ul style="list-style-type: none"> • auto qos voip {cisco-phone cisco-softphone trust} • auto qos video {cts ip-camera media-player} • auto qos classify [police] • auto qos trust {cos dscp} 例 :	次のコマンドによって、VoIP 用の自動 QoS が有効になります。 <ul style="list-style-type: none"> • auto qos voip cisco-phone : ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話機が検出された場合だけ信頼されます (CDP を介して条件付き信頼)。

	コマンドまたはアクション	目的
	Device (config-if) # auto qos trust dscp	<p>(注) ビデオをサポートしている IP フォンには、auto qos voip cisco-phone オプションを設定しないでください。ビデオ パケットには Expedited Forwarding (EF; 完全優先転送) プライオリティが設定されていないため、このオプションを使用すると、ビデオ パケットの DSCP マーキングが上書きされ、これらのパケットが class-default クラスに分類されます。</p> <ul style="list-style-type: none"> • auto qos voip cisco-softphone : ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。このコマンドによって Cisco IP SoftPhone アプリケーションおよびマーキングを実行する PC に接続しているインターフェイスの QoS 設定が生成され、そのようなインターフェイスからのトラフィックをマーキングおよびポリシングします。このコマンドで設定されたポートは、信頼できないと見なされます。 • auto qos voip trust : アップリンクポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。 <p>次のコマンドは、指定されたビデオデバイス (システム、カメラ、メディアプレーヤー) 用の自動 QoS を有効にします。</p> <ul style="list-style-type: none"> • auto qos video cts : Cisco Telepresence System に接続されているポート。着信パケットの QoS ラベルは Cisco TelePresence が検出された場合だけ

	コマンドまたはアクション	目的
		<p>信頼されます (CDP を介した条件付き信頼)</p> <ul style="list-style-type: none"> • auto qos video ip-camera : Cisco ビデオ監視カメラに接続されているポート。着信パケットの QoS ラベルは Cisco カメラが検出された場合だけ信頼されます (CDP を介した条件付き信頼) • auto qos video media-player : CDP 対応 Cisco Digital Media Player に接続されているポート。着信パケットの QoS ラベルはデジタルメディアプレイヤーが検出された場合だけ信頼されます (CDP を介した条件付き信頼)。 <p>次のコマンドは、分類の自動 QoS を有効にします。</p> <ul style="list-style-type: none"> • auto qos classify police : このコマンドは、信頼できないインターフェイスの QoS 設定を生成します。この設定では、信頼できないデスクトップ/デバイスから着信するトラフィックを分類してマークするため、サービス ポリシーがインターフェイスに適用されます。生成されたサービス ポリシーは、ポリシングを実行します。 <p>次のコマンドによって、信頼できるインターフェイス用の自動 QoS が有効になります。</p> <ul style="list-style-type: none"> • auto qos trust cos : サービス クラス • auto qos trust dscp : DiffServ コードポイント。
ステップ 4	<p>end</p> <p>例 :</p> <pre>Device(config-if) # end</pre>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 5	show auto qos interface <i>interface-id</i> 例 : Device# show auto qos interface HundredGigE 1/0/1	(任意) 自動 QoS がイネーブルである インターフェイス上の自動 QoS コマ ンドを表示します。自動 QoS 設定および ユーザー変更を表示する場合は、 show running-config コマンドを使用します。

自動 QoS のアップグレード

始める前に

アップグレードを行う前に、スイッチ上のすべての自動 QoS 設定を削除する必要があります。この例では、その手順について説明します。

この例の手順を実行した後で、新しいソフトウェアイメージまたはアップグレード後のソフトウェアイメージのスイッチをリブートし、自動 QoS を再設定する必要があります。

手順

ステップ 1 show auto qos

例 :

```
Device# show auto qos

TwentyFiveGigE1/0/1
auto qos trust dscp

TwentyFiveGigE1/0/2
auto qos trust cos
```

特権 EXEC モードでこのコマンドを入力して、現在の自動 QoS 設定をすべて記録します。

ステップ 2 no auto qos

例 :

```
Device(config-if)#no auto qos
```

インターフェイス コンフィギュレーションモードで、自動 QoS 設定が行われている各インターフェイスで適切な **no auto qos** コマンドを実行します。

ステップ 3 show running-config | i autoQos

例 :

```
Device# show running-config | i autoQos
```


特権 EXEC モードに戻り、このコマンドを入力して、残りの自動 QoS マップ、クラスマップ、ポリシーマップ、アクセスリスト、テーブルマップ、またはその他の設定を記録します。

ステップ 4 **no policy-map** *policy-map_name*

例：

```
Device(config)# no policy-map pmap_101
Device(config)# no class-map cmap_101
Device(config)# no ip access-list extended AutoQos-101
Device(config)# no table-map 101
Device(config)# no table-map policed-dscp
```

グローバル コンフィギュレーション モードでこのコマンドを入力して、QoS クラス マップ、ポリシーマップ、アクセスリスト、テーブルマップ、およびその他の自動 QoS 設定を削除します。

- **no policy-map** *policy-map-name*
- **no class-map** *class-map-name*
- **no ip access-list extended** *Auto-QoS-x*
- **no table-map** *table-map-name*
- **no table-map** *policed-dscp*

ステップ 5 **show running-config | i autoQos**

例：

```
Device#show running-config | i autoQos
```

特権 EXEC モードに戻り、このコマンドを実行して、自動 QoS 設定がないこと、または自動 QoS 設定の残りの部分がないことを確認します。

ステップ 6 **show auto qos**

例：

```
Device# show auto qos
```

このコマンドを実行して、自動 QoS 設定がないこと、または設定の残りの部分がないことを確認します。

ステップ 7 **write memory**

例：

```
Device# write memory
```

write memory コマンドを入力して、自動 QoS 設定に対する変更を NV メモリに書き込みます。

次のタスク

新しいソフトウェア イメージまたはアップグレード後のソフトウェア イメージでスイッチをリブートします。

新しいソフトウェアイメージまたはアップグレード後のソフトウェアイメージでリブートしたら、ステップ 1 で説明した **show auto qos** コマンドを実行した結果に基づいて、適切なスイッチ インターフェイスの自動 QoS を再設定します。



- (注) スイッチまたはスタックごとに、マークダウンの超過用に1つのテーブルマップ、マークダウンの違反用に1つのテーブルマップが存在します。超過アクションのテーブルマップがスイッチにすでに存在している場合は、自動 QoS ポリシーを適用できません。

自動 QoS 短縮機能のイネーブル化

自動 QoS 短縮機能をイネーブルにするには、次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	auto qos global compact 例 : Device(config)# auto qos global compact	自動 QoS 短縮機能がイネーブルになり、自動 QoS のグローバル コンフィギュレーション (非表示) が生成されます。 その後、インターフェイス コンフィギュレーション モードで設定する自動 QoS コマンドを入力できます。システムにより生成されるインターフェイス コマンドも非表示になります。 適用された自動 QoS 設定を表示するには、次の特権 EXEC コマンドを使用します。 <ul style="list-style-type: none"> • show derived-config • show policy-map • show access-list • show class-map

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • show table-map • show auto qos • show policy-map interface • show ip access-lists <p>これらのコマンドにはキーワード「AutoQos-」が含まれます。</p>

次のタスク

自動 QoS 短縮機能をディセーブルにするには、対応する自動 QoS コマンドの **no** 形式を入力して自動 QoS インスタンスをすべてのインターフェイスから削除し、次に **no auto qos global compact** グローバル コンフィギュレーション コマンドを実行します。

自動 QoS の監視

表 1: 自動 QoS の監視用コマンド

コマンド	説明
show auto qos [interface [interface-id]]	最初の自動 QoS 設定を表示します。 show auto qos コマンド出力と show running-config コマンド出力を比較してユーザー定義の QoS 設定を比較できます。
show running-config	自動 QoS によって影響されるかもしれない QoS 設定に関する情報を表示します。 show auto qos コマンド出力と show running-config コマンド出力を比較してユーザー定義の QoS 設定を比較できます。
show derived-config	自動 qos テンプレートにより実行コンフィギュレーションとともに設定される非表示の mls qos コマンドを表示します。

自動 QoS に関するトラブルシューティング

自動 QoS のトラブルシューティングを行うには、**debug auto qos** 特権 EXEC コマンドを使用します。詳細については、このリリースに対応するコマンドリファレンスにある **debug auto qos** コマンドを参照してください。

ポートで自動 QoS を無効にするには、**auto qos** インターフェイス コンフィギュレーション コマンドの **no** 形式 (**no auto qos voip** など) を使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます (グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため)。

自動 QoS の設定例

例 : auto qos trust cos

次に、**auto qos trust cos** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigE1/0/2
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface HundredGigE1/0/2

HundredGigE1/0/2

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
  QoS Set
  dscp dscp table AutoQos-4.0-Trust-Dscp-Table
```

```
Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (30000000 kbps), burst bytes 75000000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing

  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
```

例 : auto qos trust dscp

```

bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
 Match: dscp cs1 (8)
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 1%
 queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
 Match: dscp af31 (26) af32 (28) af33 (30)
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 10%
 queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
 Match: any
 Queueing

 (total drops) 0
 (bytes output) 0
 bandwidth remaining 25%
 queue-buffers ratio 25

```

例 : auto qos trust dscp

次に、**auto qos trust dscp** コマンドと、適用されるポリシーとクラスマップの例を示します。
このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)

• AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigE1/0/2
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#show policy-map interface HundredGigE1/0/2

HundredGigE1/0/2

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (30000000 kbps), burst bytes 750000000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
```

```

Match: dscp af21 (18) af22 (20) af23 (22)
Match: cos 2
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
Match: cos 1
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

例 : auto qos video cts

次に、**auto qos video cts** コマンドと、適用されるポリシーとクラスマップの例を示します。
このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigabitEthernet1/0/2
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface HundredGigabitEthernet1/0/2

HundredGigabitEthernet1/0/2

Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

Class-map: class-default (match-any)
  Match: any
  QoS Set
    cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  Match: dscp cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
```

```
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  Match: dscp cs1 (8)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例 : auto qos video ip-camera

次に、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigabitE1/0/2
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface HundredGigabitE1/0/2

HundredGigabitE1/0/2

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

  Class-map: class-default (match-any)
    Match: any
    QoS Set
      dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (300000 kbps), burst bytes 7500000,
  Priority Level: 1
```

```
Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  Match: dscp cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  Match: dscp cs1 (8)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
```

```
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

例 : auto qos video media-player

次に、**auto qos video media-player** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigabitE1/0/2
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface HundredGigabitE1/0/2

HundredGigabitE1/0/2

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
  Match: any
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
Queueing
```

```
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  Match: dscp cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  Match: dscp cs1 (8)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10
```

```
Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

例 : auto qos voip trust

次に、**auto qos voip trust** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigabitE1/0/3
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface HundredGigabitE1/0/3

HundredGigabitE1/0/3

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy
```

```
Class-map: class-default (match-any)
  Match: any
  QoS Set
    cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  Match: dscp cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10
```



```
Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  Match: dscp cs1 (8)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

例 : auto qos voip cisco-phone

次に、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-CiscoPhone-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)

- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```

Device(config)# interface HundredGigabitE1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface HundredGigabitE1/0/5

HundredGigabitE1/0/5

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
Match: ip dscp ef (46)
QoS Set
  ip dscp ef
police:
  cir 128000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
Match: ip dscp cs3 (24)
QoS Set
  ip dscp cs3
police:
  cir 32000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
Match: access-group name AutoQos-4.0-Acl-Default
QoS Set
  dscp default
police:
  cir 10000000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: class-default (match-any)
Match: any

Service-policy output: AutoQos-4.0-Output-Policy

```

```
queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
Match: dscp cs4 (32) cs5 (40) ef (46)
Match: cos 5
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
Match: dscp cs3 (24) cs6 (48) cs7 (56)
Match: cos 3
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
Match: dscp af41 (34) af42 (36) af43 (38)
Match: cos 4
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
Match: dscp af21 (18) af22 (20) af23 (22)
Match: cos 2
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
Match: dscp af11 (10) af12 (12) af13 (14)
Match: cos 1
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
Match: dscp cs1 (8)
Queueing

(total drops) 0
(bytes output) 0
```

```

bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25

```

例 : auto qos voip cisco-softphone

次に、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラスマップの例を示します。

このコマンドを実行すると、次のポリシー マップが作成されて適用されます。

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

このコマンドを実行すると、次のクラス マップが作成されて適用されます。

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)

- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

```
Device(config)# interface HundredGigE1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface HundredGigE1/0/20

HundredGigE1/0/20

Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
  Match: ip dscp ef (46)
  QoS Set
    ip dscp ef
  police:
    cir 128000 bps, bc 8000 bytes, be 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    violated 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  Match: ip dscp cs3 (24)
  QoS Set
    ip dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes, be 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    violated 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
  QoS Set
    dscp af41
  police:
    cir 5000000 bps, bc 8000 bytes, be 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    violated 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
  QoS Set
```

```
dscp af11
police:
  cir 10000000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
Match: access-group name AutoQos-4.0-Acl-Transactional-Data
QoS Set
  dscp af21
police:
  cir 10000000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
Match: access-group name AutoQos-4.0-Acl-Scavanger
QoS Set
  dscp cs1
police:
  cir 10000000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
Match: access-group name AutoQos-4.0-Acl-Signaling
QoS Set
  dscp cs3
police:
  cir 32000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
Match: access-group name AutoQos-4.0-Acl-Default
QoS Set
  dscp default
police:
  cir 10000000 bps, bc 8000 bytes, be 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  violated 0 bytes; actions:
```

```
        drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: class-default (match-any)
  Match: any

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  Match: dscp cs4 (32) cs5 (40) ef (46)
  Match: cos 5
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  Match: dscp cs3 (24) cs6 (48) cs7 (56)
  Match: cos 3
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  Match: dscp af41 (34) af42 (36) af43 (38)
  Match: cos 4
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  Match: dscp af21 (18) af22 (20) af23 (22)
  Match: cos 2
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  Match: dscp af11 (10) af12 (12) af13 (14)
  Match: cos 1
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
```

例 : auto qos global compact

```

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  Match: dscp cs1 (8)
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  Match: dscp af31 (26) af32 (28) af33 (30)
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  Match: any
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25

```

例 : auto qos global compact

次に、**auto qos global compact** コマンドの例を示します。

```

Device# configure terminal
Device(config)# auto qos global compact
Device(config)# interface HundredGigE1/0/2
Device(config-if)# auto qos voip cisco-phone

Device# show auto qos
HundredGigE1/0/2
auto qos voip cisco-phone

Device# show running-config interface HundredGigE1/0/2
interface HundredGigE1/0/2
auto qos voip cisco-phone
end

```

自動 QoS の関連情報

自動 QoS 設定で特定の QoS の変更をする必要がある場合は、QoS のマニュアルを確認してください。

自動 QoS の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	自動 QoS	自動 QoS 機能により、QoS 機能の導入が簡素化されます。この機能は、ネットワーク設計を確認し、スイッチがさまざまなトラフィックフローに優先度を指定できるように QoS 設定をイネーブルにします。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 2 章

QoS の設定

- QoS の前提条件 (35 ページ)
- QoS コンポーネント (36 ページ)
- QoS の用語 (37 ページ)
- QoS の概要 (37 ページ)
- QoS の実装 (39 ページ)
- QoS 有線モデル (44 ページ)
- 分類 (45 ページ)
- 入力ポート FIFO (IPF) パーサー (53 ページ)
- ポリシング (55 ページ)
- マーキング (56 ページ)
- トラフィックの調整 (58 ページ)
- キューイングおよびスケジューリング (61 ページ)
- 信頼動作 (69 ページ)
- 標準 QoS のデフォルト設定 (71 ページ)
- 有線ターゲットの QoS に関する制約事項 (73 ページ)
- QoS の設定方法 (76 ページ)
- QoS の特性と機能の設定 (101 ページ)
- キューとシェーピングの設定 (111 ページ)
- QoS のモニタリング (121 ページ)
- QoS の設定例 (122 ページ)
- 次の作業 (134 ページ)
- QoS に関する追加情報 (134 ページ)
- QoS の機能履歴 (134 ページ)

QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 標準 QoS の概念

- 従来の Cisco IOS QoS。
- モジュラ QoS CLI (MQC)
- QoS 実装について。
- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- トラフィックの特性およびネットワークのニーズ。たとえば、ネットワークのトラフィックがバーストであるかどうか。音声およびビデオスリム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

QoS コンポーネント

Quality of Service (QoS) は、次の主要コンポーネントで構成されています。

- 分類：分類は、アクセス コントロール リスト (ACL)、DiffServ コード ポイント (DSCP)、サービス クラス (CoS)、およびその他の要因に基づいて、トラフィックの 1 つのタイプを区別するプロセスです。
- マーキングと変換：マーキングは、特定の情報をネットワークのダウンストリームデバイスに伝送するか、デバイス内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するためにトラフィック上で使用されます。トラフィックをマークすると、そのトラフィックの QoS 動作が適用されます。これは、**set** コマンドを直接使用するか、テーブルマップ経由で入力値を受け取って出力の値に直接変換することで実行します。
- シェーピングとポリシング：シェーピングはダウンストリームデバイスで輻輳が発生しないようにトラフィック レートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。ポリシングは、トラフィック クラスに最大レートを強制するために使用されます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。
- キューイング：キューイングは、トラフィックの輻輳を防止するために使用されます。トラフィックは、帯域割り当てに基づいて処理およびスケジューリングするために、特定のキューに送信されます。次に、トラフィックはポートを介してスケジュールまたは送信されます。
- 帯域幅：帯域幅の割り当てにより、QoS ポリシーが適用されるトラフィックで使用可能な容量が決まります。
- 信頼：信頼により、トラフィックがデバイスを通過できるようになります。明示的なポリシー設定がない場合、エンドポイントから、またはエンドポイントへの DiffServ コードポイント (DSCP) 値、プレシデンス値、または CoS 値は保持されます。

QoS の用語

この QoS コンフィギュレーション ガイドでは、次の用語が同じ意味で使用されます。

- アップストリーム（デバイスに対する方向）は、入力と同じ意味です。
- ダウンストリーム（デバイスに対する方向）は、出力と同じ意味です。

QoS の概要

Quality of Service (QoS) を設定することで、他のトラフィック タイプの代わりに特定のトラフィック タイプを優先的に処理できます。QoS を設定しない場合、デバイスはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。デバイスは信頼性、遅延限界、スループットを保証せずにパケットを送信します。

次に、QoS が提供する具体的な機能を示します。

- 低遅延
- 帯域幅保証
- バッファリング能力とドロップ分野
- トラフィック ポリシング
- フレームまたはパケット ヘッダーの属性変更のイネーブル化
- 関連サービス

モジュラ QoS コマンドライン インターフェイス

デバイスでは、QoS 機能はモジュラ QoS コマンドライン インターフェイス (MQC) を使用してイネーブルにできます。MQC はコマンドライン インターフェイス (CLI) 構造を採用しています。これを使用すると、トラフィック ポリシーを作成し、作成したポリシーをインターフェイスにアタッチできます。1つのトラフィック ポリシーには、1つのトラフィック クラスと1つ以上の QoS 機能が含まれます。トラフィック クラスがトラフィックを分類するために使用されるのに対して、トラフィック ポリシーの QoS 機能は分類されたトラフィックの処理方法を決定します。MQC の主な目的の1つは、プラットフォームに依存しないインターフェイスを提供することにより、シスコプラットフォーム全体の QoS を設定することです。

有線アクセスでサポートされる QoS 機能

次の表に、有線アクセスでサポートされる QoS 機能について説明します。

表 2: 有線アクセスでサポートされる QoS 機能

機能	説明
サポートされるターゲット	<ul style="list-style-type: none"> • ギガビットイーサネット • 10 ギガビットイーサネット • 40 ギガビットイーサネット • VLAN
設定手順	service-policy コマンドを使用してインストールされる QoS ポリシー。
ポート レベルでサポートされるキューの数	ポートでは最大 8 つのキューがサポートされます。
サポートされる分類メカニズム	<ul style="list-style-type: none"> • DSCP • IP precedence • CoS • QoS-group • 次を含む ACL のメンバーシップ： <ul style="list-style-type: none"> • IPv4 ACL • IPv6 ACL • MAC ACL

階層型 QoS

デバイスは階層型 QoS (HQoS) をサポートします。HQoS を使用すると、次の作業を実行できます。

- 階層型分類：トラフィック分類は、他のクラスに基づいています。
- 階層型ポリシング：階層型ポリシーの複数のレベルでポリシングを設定するプロセス。
- 階層型シェーピング：シェーピングは、階層の複数のレベルで設定できます。



-
- (注) 階層型シェーピングは、ポートシェーパードのみサポートされません。ポートシェーパードでは、親に対してクラスデフォルトの設定だけが可能で、クラスデフォルトのアクションはシェーピングだけです。
-

QoS の実装

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

QoS 機能を設定すると、特定のネットワークトラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワークパフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

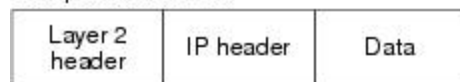
QoS は、インターネット技術特別調査委員会 (IETF) の規格である Differentiated Services (Diff-Serv) アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケットヘッダーに格納され、推奨されない IP タイプオブサービス (ToS) フィールドの 6 ビットを使用して、分類 (クラス) 情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。

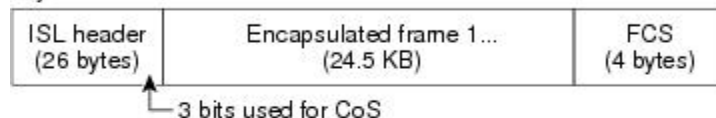
図 1: フレームおよびパケットにおける QoS 分類レイヤ

次の図にレイヤ2フレームまたはレイヤ3パケットの特殊ビットを示します。

Encapsulated Packet



Layer 2 ISL Frame



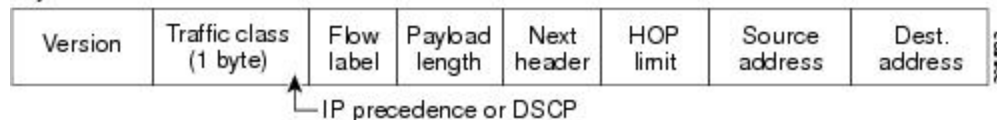
Layer 2 802.1Q and 802.1p Frame



Layer 3 IPv4 Packet



Layer 3 IPv6 Packet



レイヤ2フレームのプライオリティビット

レイヤ2のISL（スイッチ間リンク）フレームヘッダーには、下位3ビットでIEEE 802.1p サービスクラス（CoS）値を伝達する1バイトのユーザフィールドがあります。レイヤ2 ISL トランクとして設定されたポートでは、すべてのトラフィックがISLフレームに収められます。

レイヤ2 802.1Q フレームヘッダーには、2バイトのタグ制御情報フィールドがあり、上位3ビット（ユーザプライオリティビット）でCoS値が伝達されます。レイヤ2 802.1Q トランクとして設定されたポートでは、ネイティブVirtual LAN（VLAN）のトラフィックを除くすべてのトラフィックが802.1Qフレームに収められます。

他のフレームタイプでレイヤ2 CoS値を伝達することはできません。

レイヤ2 CoS値の範囲は、0（ロープライオリティ）～7（ハイプライオリティ）です。

レイヤ3パケットのプライオリティビット

レイヤ3 IP パケットは、IP precedence 値または Diffserv コードポイント (DSCP) 値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ~ 7 です。DSCP 値の範囲は 0 ~ 63 です。

分類を使用したエンドツーエンドの QoS ソリューション

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コアスイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィッククラスに割り当てるリソースの量を制限できます。Diff-Serv アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキングデバイスが提供する QoS 機能、ネットワークのトラフィックタイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

パケット分類

パケット分類は、特定の基準に基づいて定義したポリシーの複数のクラスの1つに属するものとしてパケットを識別するプロセスです。モジュラ QoS CLI (MQC) は、ポリシークラスベースの言語です。ポリシー クラスの言語は、次の定義に使用されています。

- 1つまたは複数の一致基準があるクラス マップ テンプレート
- 1つまたは複数のクラスがポリシー マップに関連付けられているポリシーマップ テンプレート

ポリシーマップテンプレートは、デバイスの1つまたは複数のインターフェイスに関連付けられます。

パケット分類は、ポリシーマップで定義されたクラスの1つに属するものとしてパケットを識別するプロセスです。分類プロセスは、処理されるパケットがクラス内の特定のフィルタに一致した場合に終了します。これは、最初の一致による終了と呼ばれます。つまり、ポリシーマップ内のクラスの順序に関係なく、パケットがポリシー内の複数のクラスに一致する場合、最初のクラスの一致後に分類プロセスが終了します。

パケットがポリシーのクラスと一致しない場合は、ポリシーのデフォルトクラスに分類されます。すべてのポリシー マップには、システム定義のクラスのデフォルトクラスがあり、どのユーザー定義クラスにも一致しないパケットに一致します。

パケット分類は次のタイプに分類できます。

- パケットと合わせて伝搬される情報に基づく分類
- デバイス固有の情報に基づく分類
- 階層型分類

パケットと合わせて伝搬される情報に基づく分類

パケットの一部としてエンドツーエンドまたはホップ間で伝搬される情報に基づく分類には、一般的に次のものがあります。

- レイヤ 3 または レイヤ 4 ヘッダーに基づく分類
- レイヤ 2 情報に基づく分類

レイヤ 3 または レイヤ 4 ヘッダーに基づく分類

これは最も一般的な導入シナリオです。レイヤ 3 および レイヤ 4 ヘッダーの多くのフィールドは、パケット分類に使用できます。

最もきめ細かいレベルでは、この分類方法はフロー全体を照合するために使用できます。この導入タイプで、アクセス コントロール リスト (ACL) を使用できます。ACL は、フローのさまざまなサブセット (送信元 IP アドレスのみ、宛先 IP アドレスのみ、または両方の組み合わせなど) に基づく照合に使用することもできます。

分類は、IP ヘッダーの precedence 値または DSCP 値に基づいて実行することもできます。IP precedence フィールドは、特定の packets を処理する必要がある相対プライオリティを示すために使用されます。これは、IP ヘッダー内のタイプ オブ サービス (ToS) バイトの 3 ビットで構成されます。

次の表に、さまざまな IP precedence ビット値と名前を示します。

表 3: IP precedence 値と名前

IP precedence 値	IP precedence ビット	IP precedence の名前
0	000	ルーチン
1	001	プライオリティ
2	010	即時
3	011	フラッシュ
4	100	フラッシュ オーバーライド

IP precedence 値	IP precedence ビット	IP precedence の名前
5	101	重大
6	110	インターネットワーク制御
7	111	ネットワーク制御



- (注) ネットワークのルーティング制御トラフィックすべては、IP precedence 値 6 をデフォルトで使用します。また、IP precedence 値 7 は、ネットワーク制御トラフィック用に予約されています。したがって、IP precedence 値 6 および 7 はユーザー トラフィック用に推奨されません。

DSCP フィールドは、IP ヘッダーの 6 ビットで構成され、インターネット技術特別調査委員会 (IETF) の DiffServ ワーキンググループにより標準化されています。DSCP ビットが含まれた元の ToS バイトは、DSCP バイトの名前を変更しました。DSCP フィールドは、IP precedence と同様に IP ヘッダーの一部です。DSCP フィールドは、IP precedence フィールドのスーパーセットです。したがって、DSCP フィールドは、IP precedence に関連して説明した内容と同様の方法で使用され、設定されます。



- (注) DSCP フィールド定義は IP precedence 値と下位互換性があります。
レイヤ2ヘッダー内の一部のフィールドは、ポリシーを使用して設定することもできます。

レイヤ2ヘッダーに基づく分類

レイヤ2ヘッダー情報に基づく分類は、さまざまな方法で実行できます。最も一般的な方法は次のとおりです。

- MAC アドレスベースの分類 (アクセス グループの場合のみ) : 分類は送信元 MAC アドレス (入力方向のポリシー用) および宛先 MAC アドレス (出力方向のポリシー用) に基づいています。
- サービス クラス : 分類は、IEEE 802.1p 標準に基づくレイヤ2ヘッダーの3ビットに基づいて行われます。これは通常、IP ヘッダーの ToS バイトにマッピングします。
- VLAN ID : 分類は、パケットの VLAN ID に基づいて行われます。



- (注) レイヤ2ヘッダー内のこれらフィールドの一部は、ポリシーを使用して設定することもできます。

デバイス固有の情報に基づく分類

デバイスは分類がパケットヘッダーまたはペイロードの情報に基づいていない場合に使用できる分類メカニズムを提供します。

複数の入力インターフェイスから出力インターフェイスの特定のクラスに送信されるトラフィックを集約する必要が生じる場合があります。たとえば、複数のカスタマーエッジルータが、異なるインターフェイスの同じアクセスデバイスに接続される可能性があります。サービスプロバイダは、特定のレートでコアに送信されるすべての集約音声トラフィックをポリシングする場合があります。ただし、異なるカスタマーからの音声トラフィックには、異なる ToS 設定がなされている可能性があります。QoS グループベースの分類は、次のシナリオで役立つ機能です。

入力インターフェイスで設定されたポリシーは、QoS グループを特定の値に設定します。この値は出力インターフェイスでイネーブルになっているポリシーのパケットの分類に使用できません。

QoS グループは、デバイス内部のパケットデータ構造内のフィールドです。QoS グループは、デバイスの内部ラベルであり、パケットヘッダーの一部ではないことに注意してください。

QoS 有線モデル

QoS を実装するには、デバイスで次のタスクを実行する必要があります。

- **トラフィック分類**：パケットまたはフローを相互に区別します。
- **トラフィックマーキングおよびポリシング**：パケットがデバイスを移動するときに、特定の QoS を示すラベルを割り当て、パケットが設定されたリソース使用率制限に準拠するようにします。
- **キューイングおよびスケジューリング**：リソース競合があるすべての状況で、異なる処理を行います。
- **シェーピング**：デバイスから送信されるトラフィックが、特定のトラフィックプロファイルに適合するようにします。

入力ポートのアクティビティ

次のアクティビティはデバイスの入力ポートで発生します。

- **分類**：パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。たとえば、デバイスは、ある種類のトラフィックを別の種類のトラフィックと区別するためにパケット内の CoS または DSCP を QoS ラベルにマッピングします。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。
- **ポリシング**：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィックフローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。

- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。

出力ポートのアクティビティ

次のアクティビティはデバイスの出力ポートで発生します。

- ポリシング：ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィックフローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。
- マーキング：マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。
- キューイング：キューイングでは、使用する出力キューを選択する前に、QoS パケットラベルと対応する DSCP 値または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、重み付けテールドロップ (WTD) によってトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS がデバイス上でイネーブルになっている場合にのみ、分類はイネーブルです。デフォルトにより、QoS はデバイスでイネーブルになっています。

分類時に、デバイスは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

アクセスコントロールリスト

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケットグループ（クラス）を定義できます。また IPv6 ACL に基づいて IP トラフィックを分類することもできます。

QoS のコンテキストでは、アクセスコントロールエントリ (ACE) の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。

- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、デバイスがベストエフォート型サービスを実行します。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかり、それ以降の検索処理は中止され、QoS 処理が開始されます。



- (注) アクセスリストを作成するときは、アクセスリストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する (DSCP を割り当てるなど) コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバルコンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバルコンフィギュレーション コマンドを使用します。

クラス マップ

クラス マップは、特定のトラフィック フロー (またはクラス) に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラスマップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合や、DSCP 値または IP precedence 値あるいは CoS 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。



- (注) 同じクラスマップに IPv4 と IPv6 の分類基準を同時に設定することはできません。ただし、同じポリシー内の異なるクラスマップで設定することは可能です。

クラスマップを作成するには、**class-map** グローバルコンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。複数のポリシー間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、デバイスによってクラスマップ コンフィギュレーション モードが開始されます。

class class-default ポリシーマップ コンフィギュレーション コマンドを使用して、デフォルトクラスを作成できます。デフォルトクラスはシステム定義であり、設定することはできません。分類されていないトラフィック（トラフィッククラスで指定された一致基準を満たさないトラフィック）は、デフォルトトラフィックとして処理されます。

存続可能時間 (TTL) 分類

ACL マップに基づいてパケットを分類できます。ACL リストの基準として TTL を設定し、着信パケットの TTL チェックを実行できます。アクセス コントロール エントリは、IPv4 TTL をチェックし、着信パケットの値を照合するために使用されます。分類されたパケットは、ポリシーマップアクションに基づいてマーキングまたはポリシングされます。この分類ではキューイングを設定できません。

次に、TTL 分類の例を示します。

```
policy-map TTL_MATCH
  class IPV4_TTL
    police rate 6000000000
    set dscp af23

ip access-list extended IPV4_TTL
  permit ip any any ttl eq 100
  permit tcp any any ttl ne 150

!
Device#show run class-map IPV4_TTL
class-map match-all IPV4_TTL
  match access-group name IPV4_TTL
!

Device#show policy-map interface hun1/0/47

HundredGigE1/0/47

Service-policy output: TTL_MATCH

Class-map: IPV4_TTL (match-all)
553567424 packets
Match: access-group name IPV4_TTL
police:
rate 6000000000 bps, burst 187500000 bytes
conformed 22983406600 bytes; actions:
transmit
exceeded 32375773000 bytes; actions:
drop
conformed 588922000 bps, exceeded 830894000 bps
QoS Set
dscp af23

Class-map: class-default (match-any)
2184433710 packets
Match: any
```

レイヤ3パケット長分類

この機能は、IPヘッダーのレイヤ3パケット長に基づいて、トラフィックを照合して分類する機能を提供します。レイヤ3パケット長とは、IPデータグラム長とIPヘッダー長の合計です。クラスポリシーマップの一致基準としてパケット長を設定し、着信パケットで値を照合することができます。分類されたパケットは、ポリシーマップアクションに基づいてマーキングまたはポリシングされます。この機能は、IPv6パケットでは機能しません。

次に、レイヤ3パケット長の分類の例を示します。

```
Service-policy output: PACKET_MATCH1

Class-map: class-default (match-any)
 16281588 packets
  Match: any

Service-policy : L3_MATCH

Class-map: PACKET_LENGTH_1 (match-any)
 9910510 packets
  Match: packet length 7582
  Match: packet length 5000
  QoS Set
  dscp cs2
  police:
  rate 3 %
  rate 1200000000 bps, burst 37500000 bytes
  conformed 10000 bytes; actions:
    transmit
  exceeded 112121 bytes; actions:
    drop
  conformed 500 bps, exceeded 3434 bps

Class-map: PACKET_LENGTH_2 (match-all)
 6371042 packets
  Match: dscp cs4 (32)
  Match: packet length 7759
  police:
  rate 12000000000 bps, burst 375000000 bytes
  conformed 44545 bytes; actions:
    transmit
  exceeded 34343 bytes; actions:
    drop
  conformed 1211 bps, exceeded 11211 bps

Class-map: class-default (match-any)
 36 packets
  Match: any
  QoS Set
  precedence 3
Device#

class-map match-any PACKET_LENGTH_1
match packet length min 7582 max 7582
match packet length min 5000 max 5000

class-map match-all PACKET_LENGTH_2
match dscp cs4
match packet length min 7759 max 7759
```


レイヤ 2 SRC-Miss または DST-Miss の分類

トラフィックは、送信元 MAC アドレスまたは宛先 MAC アドレスについて、MAC アドレステーブルに見つからない MAC アドレスで分類できます。L2-Miss 分類によるポリシーマップは、入力方向でレイヤ 2 インターフェイスに適用できます。ポリシング、マーキング、または再マーキングアクションは、この分類を使用して適用できます。L2-Miss 分類は、レイヤ 3 インターフェイスには適用できません。この分類ではキューイングを設定できません。

次に、L2-Miss 分類の例を示します。

```
Device #show run class-map DST-MISS
      class-map match-any DST-MISS
      match l2 dst-mac miss
```

```
Device #show run class-map SRC-MISS
      class-map match-all SRC-MISS
      match l2 src-mac miss
```

```
Device #show policy-map L2-MISS
Policy Map L2-MISS
  Class DST-MISS
    set dscp af22
  police cir percent 10
    conform-action transmit
    exceed-action drop
  Class SRC-MISS
    set precedence 1
  police rate percent 20
    conform-action transmit
    exceed-action drop
```

```
!
end
```

```
Device#
```

ポリシー マップ

ポリシー マップでは、作用対象のトラフィック クラスを指定します。アクションには次が含まれます。

- トラフィック クラスに特定の DSCP 値または IP precedence 値を設定する
- トラフィック クラスに CoS 値を設定する
- QoS グループを設定する
- トラフィックがアウト オブ プロファイルになった場合の、トラフィックの帯域幅制限やアクションを指定する

ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

ポリシーマップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、デバイスはポリシーマップ コンフィギュレーション モードを開始します。このモードでは、**class** または **set** ポリシーマップ コンフィ

キューレーション コマンドおよびポリシーマップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシーマップは、ポリシーマップ クラス コンフィギュレーション コマンド **police** と **bandwidth** を使用して設定することもできます。これらのコマンドは、ポリサー、トラフィックの帯域幅制限、および制限を超過した場合のアクションを定義します。加えて、ポリシーマップは、**priority** ポリシーマップ クラス コンフィギュレーション コマンド（クラスの優先順位をスケジューリングする）、またはキューイング ポリシーマップ クラス コンフィギュレーション コマンド（**queue-buffers** および **queue-limit**）を使用すると、より詳細に設定できます。

ポリシーマップを有効にするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。



- (注) **priority** と **set** の両方をポリシーマップに設定することはできません。これらのコマンド両方をポリシーマップに設定すると、ポリシーマップをインターフェイスに適用した際に、エラーメッセージが表示されます。次に、この制限の例を示します。

```
Device# configure terminal
Device(config)# class-map cmap
Device(config-cmap)# exit
Device(config)# class-map classmap1
Device(config-cmap)# exit
Device(config)# policy-map pmap
Device(config-pmap)# class cmap
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# exit
Device(config-pmap)# class classmap1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface HundredGigE1/0/2
Device(config-if)# service-policy output pmap

Non-queuing action only is unsupported in a queuing policy!!!
%QOS-6-POLICY_INST_FAILED:
Service policy installation failed
```

物理ポートのポリシー マップ

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。アクションには、特定の DSCP あるいはトラフィック クラスでの IP プレゼンダンス値または QoS の値の設定、一致する各トラフィック クラス（ポリサー）に対するトラフィックの帯域幅限度の指定、トラフィックがアウト オブ プロファイル（マーキング）の場合の処理などが含まれます。

ポリシー マップには、次の特性もあります。

- 1つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に定義されたデフォルトのトラフィック クラスを含めることができます。デフォルトのトラフィック クラスはマップの末尾に明示的に配置されます。

class class-default ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィッククラスを設定すると、未分類トラフィック（トラフィッククラスで指定された一致基準に一致しないトラフィック）はデフォルトのトラフィッククラス（**class-default**）として処理されます。

- 1つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

VLAN のポリシー マップ

デバイスは、VLAN の QoS 機能をサポートします。これにより、ユーザーは、着信フレームの VLAN 情報を使用して VLAN レベルで QoS 処理（分類と QoS アクション）を実行できます。VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。VLAN ポリシー マップに属するすべての物理インターフェイスは、ポートベースのポリシー マップの代わりに VLAN ベースのポリシー マップが表示されるようにプログラムする必要があります。

ポリシーマップはVLANSVIに適用されますが、ポート単位で実行できるのはマーキングまたは再マーキングアクションのみです。複数の物理ポートからのトラフィックの合計が認識されるようにポリサーを設定できません。各ポートは、そのポートに着信するトラフィックを制御する別のポリサーを必要とします。

QoS プロファイル

デバイスは、Ternary Content Addressable Memory (TCAM) を使用して分類ルールを保存します。TCAM リソースの使用を最適化するには、QoS プロファイルを使用して、使用頻度の低い機能の一部をオフにし、必要に応じてオンにします。

qos profile {default | extended} コマンドを使用して、必要な分類機能セットを選択できます。**default** キーワードは、共通の分類機能のみをロードします。**extended** キーワードは、デバイスで使用可能な完全な分類機能セット（ただしスケールは縮小されています）をロードします。デフォルトでは、一般的に使用される分類機能のみがデバイスに設定されます。

qos profile extended は、共通の分類機能とともに TCP フラグを有効にします。

show platform software fed active qos profile コマンドを使用して、デバイスに設定されている QoS プロファイルを確認できます。

例

```
device# show platform software fed active qos profile
Using default - Common Classification Features
```

セキュリティグループ分類

セキュリティグループの分類には、送信元セキュリティグループタグ (SGT) と宛先セキュリティグループタグ (DGT) によって指定される送信元グループと宛先グループの両方が含まれます。

SGT QoS 分類の目的は、ユーザーグループを活用してポリシーの粒度を高めることです。これにより、ポリシーはアプリケーションに対応するだけでなく、ユーザーアイデンティティ（またはユーザーが属するユーザーのグループ）に基づいて差別化されたサービスを提供します。

SGT または DGT に基づく出力 QoS 分類はサポートされていません。

SGT ベースの QoS

SGT ベースの QoS 機能は、定義されたユーザーグループまたはデバイスに対して、QoS ポリシーおよびアクションに基づくトラフィックのクラスに特別な処理を提供します。この機能により、異なるユーザーグループによって開始されたアプリケーションやトラフィックに複数の QoS ポリシーを割り当てることができます。各ユーザーグループは一意的 SGT 値によって定義され、MQC ベースの QoS 構成をサポートできます。

SGT ベースの QoS 機能は、SGT-DGT ベースの packets 分類に使用するユーザーグループおよびデバイスベースの QoS サービスレベルの両方に適用できます。これは、QoS ポリシーの優先度設定に使用するコンテキスト情報に基づくユーザーグループの定義をサポートできる可能性もあります。

SGACL との DGID の共有

リソースの制限により、4096 のセキュリティグループ宛先タグ (DGT) のみがサポートされます。DGT に基づく分類は、DGID と呼ばれるセキュリティ宛先タグ ID によって実現されます。DGID はグローバルリソースであり、SGACL と共有されます。DGID 割り当ては、検出された順序で行われます。デバイスでは、起動時に、QoS ポリシー設定の前に SGACL 設定が適用されます。したがって、DGID は最初に SGACL に割り当てられ、次に QoS ポリシーに割り当てられます。

`show platform software fed sw active sgacl detail` コマンドは、DGT から DGID へのマッピングを表示します。

例

```
device# show platform software fed active sgacl detail

Global Enforcement: On
*Refcnt: for the non-SGACL feature
===== DGID Table =====
SGT/Refcnt   DGT   DGID  hash  test_cell  monitor  permitted  denied
=====
*/1          24    1     24
24           24    1     24      Off      Off       0          0
```

SGT ベースの QoS の制限

次に、SGT ベースの QoS 機能の制限事項を示します。

- SGT ベースの QoS は、トンネルインターフェイスではサポートされません。
- 4096 のセキュリティ宛先タグと 65539 のセキュリティ送信元タグのみがサポートされます。

- SGT ベースのポリシーは、インターフェイスの入力方向にのみ適用できます。

アップグレードまたはダウングレードの制約事項

- 以前のリリースから Cisco IOS XE リリース 16.12.x 以降にアップグレードする場合、サポートされる DGID の最大数は 256 です。この問題を解決するには、スイッチをリロードします。
- Cisco IOS XE リリース 17.1.x から IOS XE 16.12.x リリースへのダウングレードの場合、割り当てられた DGID は 4096 と表示されますが、256 個の DGID のみがサポートされます。この問題を解決するには、スイッチをリロードします。
- tcp フラグがポリシーで設定されている場合、In-Service Software Upgrade (ISSU) は失敗します。ISSU を実行するには、最初に tcp フラグ設定を削除します。
- インターフェイスにアタッチされているポリシーマップが tcp フラグに基づいてトラフィックを分類すると、ISSU のアップグレードは失敗します。ISSU を実行するには、ポリシーマップをインターフェイスから切り離すか、tcp フラグの分類を削除します。

入力ポート FIFO (IPF) パーサー

IPF は、着信ネットワークトラフィックを解析して、フレームをさまざまなプライオリティレベルに分類します。トラフィッククラスはさまざまなパケット形式から抽出されます。たとえば、トラフィッククラスは、IP パケットの場合は Differentiated Services Code Point (DSCP; DiffServ コードポイント) から、dot1q タグパケットの場合はサービスクラス (CoS) から抽出できます。これらのトラフィッククラスはさらにプライオリティレベルにマッピングされます。このプライオリティレベルは、輻輳発生時にドロップを決定するために使用されます。

IPF パーサーは、グローバルモードと分離モード（ポートレベルでのハイおよびロープライオリティ設定）で使用できます。デフォルトでは、分離モードです。分離モードでは、プライオリティの区別はシステムレベルではなくポートレベルで行われます。

IPF パーサーをグローバルモードで設定するには、次のコマンドを使用します。

```
configure port-ingress-fifo mode global
```

次に、トラフィッククラスとプライオリティのマッピングを表示する show コマンドの例を示します。

```
Device# show platform hardware fed active qos ipf interface twentyFiveGigE 1/0/1 cos-map
```

```
IPF cos to traffic class map for Interface [cos : traffic-class]:
```

```
-----
0 : 0          1 : 1          2 : 2          3 : 3
4 : 4          5 : 5          6 : 6          7 : 7
8 : 4          9 : 4         10 : 4         11 : 4
12 : 4         13 : 4         14 : 4         15 : 4
```

```
Device# show platform hardware fed active qos ipf interface twentyFiveGigE 1/0/1 dscp-map
```

```
IPF dscp to traffic class map for Interface [dscp : traffic-class]:
```

```
-----
```

```

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

```

```
Device#show platform hardware fed active qos ipf interface twentyFiveGigE 1/0/1 exp-map
```

```
IPF exp to traffic class map for Interface [exp : traffic-class]:
```

```
-----
0 : 0          1 : 1          2 : 2          3 : 3
4 : 4          5 : 5          6 : 6          7 : 7

```

```
Device#show platform hardware qos ipf interface twentyFiveGigE 1/0/1 ipf-parse-cfg
IPF configuration for Interface:
```

```
-----
Port Trust:           Enabled
Default TC:           0
Dscp based parsing:   Disabled
Exp based parsing:    Disabled
Fdcos based parsing: Enabled
cos based parsing:    Disabled

```

```
Device#show platform hardware fed active qos ipf tc-to-pri asic 0
IPF traffic class to priority for[Asic:Core:TlaInst]::[0:0:0]
```

```
-----
Priority              Traffic Classes
-----
Low Pri :             0 1 4
High Pri:             2 3 5 6 7
IPF traffic class to priority for[Asic:Core:TlaInst]::[0:0:1]
```

```
-----
Priority              Traffic Classes
-----
Low Pri :             0 1 4
High Pri:             2 3 5 6 7

```

統計情報の show コマンド :

```
Device#show platform hardware fed active qos ipf statistics asic 0
IpF Statistics:[Asic|Core|Tla] : [0 | 0 | 0] - Global Mode
```

```
-----
IpF misc packet drops:                               0
IpF Drop Statistics
-----
low pri Frames drop:                                0
low pri mop Frames drop:                             0
high pri Frames drop:                                0
almost full Frames drop:                             0
RCP Frames drop:                                     0

```

```
IpF Statistics:[Asic|Core|Tla] : [0 | 0 | 1] - Global Mode
```

```
-----
IpF misc packet drops:                               0
IpF Drop Statistics

```

```

-----
low pri Frames drop:          0
low pri mop Frames drop:     0
high pri Frames drop:        0
almost full Frames drop:     0
RCP Frames drop:             0

```

ポリシング

パケットが分類され、DSCP ベース、CoS ベース、または QoS グループのラベルが割り当てられると、ポリシングおよびマーキング プロセスを開始できます。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「アウトオブプロファイル」または「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP または CoS 値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。

パケットの混乱を避けるため、通常、適合トラフィックも不適合トラフィックも同じキューを通過します。



- (注) すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートでのみポリシングを設定できます。

ポリシーマップおよびポリシングアクションを設定したら、**service-policy** インターフェイス コンフィギュレーションコマンドを使用して、入力ポートまたは出力ポートにポリシーマップを付加します。

トークンバケット アルゴリズム

ポリシングはトークンバケット アルゴリズムを使用します。各フレームがデバイスに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。バケットにトークンが追加されるたびに、デバイスは、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサーアクション（ドロップまたはマークダウン）が実行されます。

バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限され

ます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィックフローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシングアクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシーマップクラス コンフィギュレーション コマンドの **burst-byte** オプションを使用します。トークンがバケットから削除される速度（平均レート）を設定するには、**police** ポリシーマップクラス コンフィギュレーション コマンドの **rate** オプションを使用します。

マーキング

マーキングは、特定の情報をネットワークのダウンストリームデバイスに伝送するか、デバイス内の 1 つのインターフェイスから別のインターフェイスに情報を伝送するために使用します。

マーキングは、パケットヘッダーの特定のフィールド/ビットを設定するか、デバイス内部のパケット構造内の特定のフィールドを設定するために使用できます。さらに、マーキング機能はフィールド間のマッピングの定義に使用できます。QoS では次のマーキング方法を使用できます。

- パケットヘッダー
- デバイス固有の情報
- テーブルマップ

パケットヘッダーのマーキング

パケットヘッダーフィールドのマーキングは 2 種類の一般的なカテゴリに分類できます。

- IPv4/v6 ヘッダービットマーキング
- レイヤ 2 ヘッダービットマーキング

IP レベルのマーキング機能は、**precedence** を設定したり、IP ヘッダー内の DSCP を特定の値に設定したりして、ダウンストリームデバイス（スイッチまたはルータ）で特定のホップごとの動作を実行するために使用されます。また、異なる入力インターフェイスからのトラフィックを、出力インターフェイス内の単一のクラスに集約するためにも使用できます。この機能は現在、IPv4 および IPv6 ヘッダーでサポートされています。

レイヤ 2 ヘッダーのマーキングは、通常、ダウンストリームデバイス（スイッチまたはルータ）のドロップ動作に影響を与えるために使用されます。これは、レイヤ 2 ヘッダーの一致と並行して動作します。ポリシーマップを使用して設定されるレイヤ 2 ヘッダーのビットはサービスクラスです。

スイッチ固有の情報のマーキング

この形式のマーキングには、パケットヘッダーの一部ではないパケットデータ構造内のフィールドのマーキングが含まれます。これにより、後でデータパスでマーキングを使用できるようになります。これはスイッチ間で伝搬されません。QoS グループのマーキングはこのカテゴリに分類されます。この形式のマーキングは、入力インターフェイスで有効になっているポリシーだけでサポートされます。対応する照合機能を同じスイッチの出力インターフェイスでイネーブルにし、適切な QoS アクションを適用することができます。

テーブル マップのマーキング

テーブル マップ マーキングは変換表を使用したフィールド間のマッピングおよび変換を可能にします。この変換表はテーブル マップと呼ばれます。

インターフェイスに接続されているテーブルマップに応じて、パケット内の CoS、DSCP、および Precedence 値が書き換えられます。デバイスにより、入力テーブルマップポリシーと出力テーブルマップポリシーの両方を設定できます。

たとえば、テーブルマップは、レイヤ 2 CoS 設定をレイヤ 3 の precedence 値にマッピングするのに使用できます。この機能により、マッピングを実行する方法を示す 1 つのテーブルに複数の **set** コマンドを組み合わせて使用することができます。このテーブルは複数のポリシーで参照するか、または同じポリシー内で複数回参照することができます。

テーブル マップ ベースのポリシーでは、次の機能がサポートされています。

- 変換：1 つの DSCP 値セットから別の DSCP 値セットにマッピングするテーブル マップを利用できます。また、このテーブル マップは出力ポートに付加できます。
- 書き換え：入力パケットは設定されたテーブル マップに基づいて書き換えられます。
- マッピング：テーブル マップ ベースのポリシーは、set ポリシーの代わりに使用できます。

テーブル マップ マーキングには、次の手順が必要です。

1. テーブルマップの定義：**table-map** グローバル コンフィギュレーション コマンドを使用して値をマッピングします。テーブルが使用されるクラスまたはポリシーは認識されません。テーブルマップのデフォルトのコマンドは、「from」フィールドで一致がない場合に値が「to」フィールドにコピーされることを示すために使用されます。
2. ポリシー マップの定義：テーブル マップを使用するポリシー マップを定義します。
3. ポリシーをインターフェイスに関連付けます。



- (注) 入力ポートのテーブル マップ ポリシーによって、そのポートの信頼設定が qos-marking の「from」タイプに変更されます。



(注) dscp 値以外の値を信頼するには、テーブルマップを入力方向でデフォルトのコピーとともに使用します。



(注) 出力のテーブルマップポリシーで QoS グループを DSCP 値にマッピングすると、QoS グループは DSCP に対応する同等の COS 値をマッピングしません。QoS グループをゼロ以外の COS 値に定義する場合は、COS テーブルマップに別の QoS グループを設定します。

トラフィックの調整

ネットワークで QoS をサポートするには、サービスプロバイダネットワークに入るトラフィックをネットワーク境界ルータでポリシングし、トラフィック レートがサービス範囲内に収まるようにする必要があります。ネットワーク コアのプロビジョニングで処理できるように設定されているトラフィックよりも多くのトラフィックがネットワーク境界のいくつかのルータから送信開始されると、トラフィック 負荷の増加によってネットワーク 輻輳が発生します。ネットワークのパフォーマンスが低下すると、すべてのネットワーク トラフィックで QoS を提供することが困難になります。

トラフィック ポリシング機能（ポリシング機能を使用）およびシェーピング機能（トラフィックシェーピング機能を使用）はトラフィック レートを管理しますが、トークンが不足した場合のトラフィックの処理方法が異なります。トークンの概念は、トークンバケット方式、トラフィック測定機能に基づいています。



(注) ネットワーク トラフィックで QoS テストを実行すると、シェーパーデータとポリシングデータで異なる結果が生じることがあります。シェーピングからのネットワーク トラフィックデータの方が、より正確な結果が得られます。

この表は、ポリシングとシェーピングの機能を比較します。

表 4: ポリシングとシェーピングの機能の比較

ポリシング機能	シェーピング機能
適合するトラフィックをライン レートで送信し、バーストを許可します。	トラフィックが固定レートでスムーズに送信されます。
トークンが不足すると、アクションがただちに実行されます。	トークンが不足すると、パケットをバッファし、後でトークンが使用可能になった時点で送信します。シェーピングを使用するクラスにはキューが関連付けられており、このキューを使用してパケットがバッファされます。

ポリシング機能	シェーピング機能
ポリシングは、ビット/秒、パケット/秒、およびセル/秒など複数の単位で設定できます。	シェーピングの設定単位はビット/秒だけです。
ポリシングには、イベントに複数の可能なアクションが関連付けられています。このようなアクションの例としては、イベント、マーキング、ドロッピングなどがあります。	シェーピングはプロファイルを満たさないパケットをマークできません。
入出力両方のトラフィックで機能します。	出力トラフィックに対してのみ実装されます。
ウィンドウサイズを小さくしたためにパケットドロップが発生すると、伝送制御プロトコル (TCP) は、回線速度でラインを検出しますが、設定されたレートに適合します。	TCP は低速回線があることを検出し、再送信タイマーを適切に調整できます。これにより、再送信の範囲が狭くなり、TCP に負担をかけません。

ポリシング

QoS ポリシング機能は、トラフィック クラスに最大レートを強制するために使用されます。QoS ポリシング機能は、プライオリティ機能と合わせて、プライオリティトラフィックを制限するためにも使用できます。レートを超過した場合は、イベント発生直後に特定のアクションが実行されます。レート (認定情報レート [CIR] および最大情報レート [PIR]) とバーストパラメータ (適合バースト サイズ [B_c] および拡張バースト サイズ [B_e]) は、すべてバイト/秒で設定されます。

QoS では次のポリシング形式またはポリサーがサポートされます。

- シングルレート 2 カラー ポリシング
- デュアルレート 3 カラー ポリシング



(注) シングルレート 3 カラー ポリシングはサポートされません。

シングルレート 2 カラー ポリシング

シングルレート 2 カラー ポリサーは、CIR と B_c だけを設定するモードです。

B_c は任意のパラメータであり、これが指定されていない場合、デフォルトで計算されます。このモードでは、着信パケットに十分なトークンがある場合、パケットは適合すると見なされます。パケットの到着時に、十分なトークンが B_c の範囲内で使用できない場合、パケットは設定レートを越えたと見なされます。



- (注) トークンバケットアルゴリズムの詳細については、[トークンバケットアルゴリズム \(55 ページ\)](#) を参照してください。

デュアルレート 3 カラー ポリシング

デュアルレートポリサーでは、デバイスはカラーブラインドモードのみをサポートします。このモードでは、認定情報レート (CIR) および最大情報レート (PIR) を設定します。名前からわかるように、この場合、最大レート用に 1 つ、認定レート用に 1 つの、合わせて 2 つのトークンバケットがあります。



- (注) トークンバケットアルゴリズムの詳細については、[トークンバケットアルゴリズム \(55 ページ\)](#) を参照してください。

カラーブラインドモードでは、最大レートのバケットの着信パケットが最初にチェックされます。十分な数のトークンがない場合、パケットはレートに違反していると思なされます。十分な数のトークンがある場合、次に適合レートのバケットのトークンをチェックして、十分な数のトークンがあるかどうかを判別します。最大レートのバケットにあるトークンは、バケットのサイズによって減少します。十分な数のトークンがない場合、パケットが設定されているレートを超過していると思なされます。十分な数のトークンがある場合、パケットは適合すると思なされ、両方のバケットのトークンは、バケットのサイズによって減少します。

トークン補充レートは着信パケットによって異なります。あるパケットが時間 T1 に着信し、次のパケットが時間 T2 に着信したとします。T1 と T2 間の時間間隔は、トークンバケットに追加される必要があるトークンの数を決定します。これは次のように計算されます。

パケットの時間間隔 (T2-T1) * CIR) / 8 バイト

シェーピング

シェーピングは、ダウンストリームスイッチおよびルータで輻輳が発生しないようにトラフィックレートを調整しながら、トラフィックの最大レートを強制するプロセスのことです。最も一般的な形式のシェーピングは、物理または論理インターフェイスから送信されるトラフィックを制限するために使用されます。

シェーピングにはバッファが関連付けられており、十分なトークンがないパケットがすぐにドロップされずにバッファされます。シェーピングされるトラフィックのサブセットで使用可能なバッファ数は制限され、さまざまな要因に基づいて計算されます。使用可能なバッファの数は、特定の QoS コマンドを使用して調整できます。パケットはドロップされずに、バッファが使用可能になった時点でバッファされます。

クラスベース トラフィック シェーピング

デバイスではクラスベースのトラフィック シェーピングを使用します。このシェーピング機能は、インターフェイスに関連付けられたポリシーのクラスでイネーブルになります。シェーピングが設定されたクラスには、トークンがないパケットを保持する複数のバッファが割り当てられます。バッファされたパケットは FIFO を使用してクラスから送信されます。最も一般的な形式の使用では、クラスベースのシェーピングを使用して、全体として物理インターフェイスまたは論理インターフェイスの最大レートを強制します。クラスでは次のシェーピング形式がサポートされます。

- 平均レート シェーピング
- 階層型シェーピング

シェーピングは、トークンバケットを使用して実行されます。CIR、B_c、B_eの値は、パケットが送信されるレートと、トークンが補充されるレートを決定します。



(注) トークンバケットアルゴリズムの詳細については、[トークンバケットアルゴリズム \(55 ページ\)](#) を参照してください。

平均レート シェーピング

平均レートシェーピングを設定するには、**shape average** ポリシーマップ クラス コマンドを使用します。

このコマンドは、特定のクラスの最大帯域幅を設定します。キューの帯域幅は、ポートでさらに使用できる帯域幅があってもこの値に制限されます。デバイスでは、割合またはターゲットビットレート値でシェーピング平均を設定できます。

階層型シェーピング

シェーピングは、階層内の複数のレベルで設定することもできます。これは、シェーピングを設定した親ポリシーを作成して、追加のシェーピングを設定した子ポリシーを親ポリシーに付加することで実現できます。

ポート シェーパーでは、クラス デフォルトが使用され、親で実行できるアクションはシェーピングだけです。キューイングアクションはポート シェーパーがある子で実行されます。ユーザー設定のシェーピングを使用すると、子のキューイングアクションを設定することはできません。

キューイングおよびスケジューリング

デバイスは、トラフィックの輻輳を防止するためにキューイングおよびスケジューリングを使用します。デバイスは、次のキューイングおよびスケジューリング機能をサポートします。

- 帯域幅

- 重み付けテール ドロップ
- プライオリティ キュー
- キュー バッファ
- 重み付けランダム早期検出

ポートにキューイング ポリシーを定義すると、制御パケットは、しきい値が最も高いベスト プライオリティ キューにマッピングされます。制御パケットのキュー マッピングは、以下の状況では異なって機能します。

- Quality of Service (QoS) ポリシーなし：QoS ポリシーが設定されていない場合、DSCP 値が 16、24、48、および 56 の制御パケットは、最も高いしきい値 `threshold2` を持つキュー 0 にマッピングされます。
- ユーザー定義のポリシーあり：出力ポートに設定されているユーザー定義のキューイング ポリシーは、制御パケットのデフォルトのプライオリティ キューの設定に影響する可能性があります。



(注) 出力方向のキューイングポリシーは **match access-group** 分類をサポートしません。

制御トラフィックは、次のルールに基づいて最適なキューにリダイレクトされます。

1. ユーザー ポリシーで定義されている場合、最高レベルのプライオリティ キューがベスト キューとして常に選択されます。
2. プライオリティ キューがない場合、Cisco IOS ソフトウェアは、ベスト キューとしてキュー 0 を選択します。ソフトウェアがベスト キューとしてキュー 0 を選択した場合は、コントロールプレーン トラフィックに最適な QoS 処理を提供するために、このキューに最大帯域幅を定義する必要があります。
3. しきい値がベスト キューで設定されていない場合、Cisco IOS ソフトウェアは、DiffServ コードポイント (DSCP) 値が 16、24、48、および 56 の制御パケットを `threshold2` にマッピングされるように割り当て、ベスト キュー内の残りの制御トラフィックを `threshold1` に再割り当てします。

ポリシーが制御トラフィックに対して明示的に設定されていない場合、Cisco IOS ソフトウェアはすべての一致しない制御トラフィックを `threshold2` を持つベスト キューにマッピングし、一致する制御トラフィックはポリシーで設定されたキューにマッピングされません。



-
- (注) レイヤ3 パケットに適切な QoS を提供するために、パケットが適切なキューに明示的に分類されていることを確認する必要があります。ソフトウェアはデフォルトキューで DSCP 値を検出すると、自動的にこのキューをベストキューとして再割り当てします。
-

帯域幅

デバイスは次の帯域幅設定をサポートしています。

- 帯域幅
- 帯域幅の割合
- 残存帯域幅の割合

帯域幅の割合

特定のクラスに最小帯域幅を割り当てるには、**bandwidth percent** ポリシーマップ クラス コマンドを使用します。合計が 100% を超えることはできず、合計が 100% 未満である場合は、残りの帯域幅がすべての帯域幅キューで均等に分割されます。



-
- (注) キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。
-

ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1 つのポリシー マップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。

残存帯域幅の割合

指定されたキューでの未使用帯域幅の割合を作成するには、**bandwidth remaining percent** ポリシーマップクラス コマンドを使用します。未使用帯域幅は、これら指定されたキューにより、設定で指定されている割合で使用されます。このコマンドは、**priority** コマンドがポリシー内の特定のキューでも使用される場合に使用します。

割合を割り当てる場合には、これらの割合に従って、キューに特定の重みが割り当てられません。

0 - 100 の割合を指定できます。たとえば、1 つのクラスの帯域幅余剰割合を 2 に設定し、別のクラスで帯域幅余剰割合 4 のキューを設定できます。帯域幅余剰割合 4 は、帯域幅余剰割合 2 の 2 倍の頻度でスケジュールされます。

ポリシーの全帯域幅の割合の割り当ては 100 を超えることができます。たとえば、1 つのキューの帯域幅余剰割合を 50 に設定し、別のキューに帯域幅余剰割合 100 を設定できます。

重み付けテールドロップ

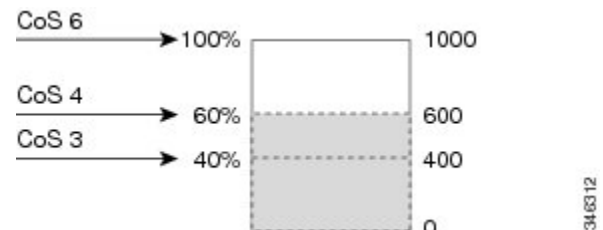
デバイス出力キューは、重み付けテールドロップ (WTD) と呼ばれるテールドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると (宛先キューの空きスペースがフレームサイズより小さくなると)、フレームはドロップされます。

各キューには 3 種類の設定可能なしきい値があります。QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。

図 2: WTD およびキューの動作

次の図は、サイズが 1000 フレームであるキューでの WTD の動作の例を示しています。ドロップ割合は次のように設定されています。40% (400 フレーム)、60% (600 フレーム)、および 100% (1000 フレーム) です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレーム



をキューイングできるという意味です。

例では、CoS 値 6 は他の CoS 値よりも重要度が高く、100% のドロップしきい値 (キューフルステート) に割り当てられます。CoS 値 4 は 60% しきい値に、CoS 値 3 は 40% しきい値に割り当てられます。これらのしきい値の割り当てはすべて、`queue-limit cos` コマンドを使用します。

600 のフレームが格納されているキューに、新しいフレームが着信したとします。これは CoS 値 4 を使用し、60% のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、フレームはドロップされます。

重み付けテールドロップのデフォルト値

次に、重み付けテールドロップ (WTD) のデフォルト値と、WTD しきい値を設定するためのルールを示します。

- WTD に対して 2 つ以下のキュー制限割合を設定する場合、WTD のデフォルト値はこれらのしきい値に割り当てられます。

次に、WTD しきい値のデフォルト値を示します。

表 5: WTD しきい値のデフォルト値

しきい値	デフォルト値の割合
0	80
1	90
2	400

- 異なる 3 つの WTD しきい値が設定されている場合、キューは設定どおりにプログラムされます。
- 2 つの WTD しきい値が設定されている場合、最大値の割合は 400 です。
- 1 つの WTD しきい値が x として設定されている場合、最大値の割合は 400 です。
 - x の値が 90 未満の場合、 $\text{threshold1} = 90$ および $\text{threshold0} = x$ です。
 - x の値が 90 の場合、 $\text{threshold1} = 90$ 、 $\text{threshold0} = 80$ です。
 - x の値が 90 より大きい場合、 $\text{threshold1} = x$ 、 $\text{threshold0} = 80$ です。

プライオリティ キュー

各ポートは 8 つの出力キューをサポートし、そのうち 2 つにプライオリティを設定できます。

2 つのクラスのプライオリティを設定するには、**priority level** ポリシー クラスマップ コマンドを使用します。1 つのクラスにプライオリティ キュー レベル 1 を設定し、別のクラスにプライオリティ キュー レベル 2 を設定する必要があります。これら 2 つのキューのペケットは、他のキューと比較して、低遅延になります。

プライオリティキューが設定されている場合は、100% のラインレートトラフィックを送信できません。プライオリティキューが設定されている場合、ラインレートトラフィックは 99.6% にしかならないため、遅延は 20 マイクロ秒未満になります。



(注) プライオリティは 1 つのレベルのみ設定できます。

1 つのポリシーマップで使用できる完全プライオリティまたはレベル付きプライオリティは 1 つだけです。kbps または割合のない同じプライオリティ レベルが設定された複数のプライオリティは、ポリシングですべてが設定された場合にのみ使用できます。

プライオリティ キュー ポリサー

このスイッチは、プライオリティキューのポリシングレートの設定をサポートします。プライオリティ キュー ポリサーは、シングルレート 2 カラーポリシングのみをサポートします。



(注) テーブルマップを使用したポリシングはサポートされません。

プライオリティ キュー ポリサーの設定例

例 1

```
Policy Map priority-1
  Class prio1
    priority level 1
    police rate percent 10
      conform-action transmit
      exceed-action drop
  Class prio2
    priority level 2
    police rate percent 5
      conform-action transmit
      exceed-action drop
  Class new
    bandwidth 20 (%)
```

例 2

```
Policy Map priority-1
  Class prio1
    priority level 1 20 (%)
    police rate percent 10
      conform-action transmit
      exceed-action drop
  Class prio2
    priority level 2 25 (%)
    police rate percent 5
      conform-action transmit
      exceed-action drop
  Class new
    bandwidth 20 (%)
```

キュー バッファ

ブート時に有線ポートでイネーブルになっているポリシーマップがない場合、デフォルトで作成される 2 つのキューがあります。有線ポートには、MQC ベースのポリシーを使用して最大 8 つのキューを設定できます。次の表に、どのパケットがどのキューに入っているかを示します。

表 6: DSCP、Precedence、CoS : キューのしきい値のマッピングテーブル

DSCP、Precedence、CoS	キュー	しきい値
制御パケット	0	2

DSCP、Precedence、CoS	キュー	しきい値
他のパケット	1	2



- (注) バッファの可用性を保証し、ドロップしきい値を設定し、キューの最大メモリ割り当てを設定できます。キューバッファを設定するには、**queue-buffers** ポリシーマップクラスコマンドを使用します。最大しきい値を設定するには、**queue-limit** ポリシーマップクラスコマンドを使用します。

バッファ割り当ては2種類あります。キューに明示的に予約される厳格なバッファと、特定のポートで未使用時に他のポートで利用可能な柔軟なバッファです。

有線ポートのデフォルトでは、キュー0には、厳格なバッファとしてインターフェイスで利用可能なバッファの40%が割り当てられます。つまり、1ギガビットポートにおいては、キュー0に対して200バッファが割り当てられ、10ギガビットポートにおいては、600バッファが割り当てられます。このキューの柔軟な最大値は厳格なバッファの4倍に設定されます。つまり、1ギガビットポートの場合は800、10ギガビットポートの場合は2400、40ギガビットポートの場合は9600に設定されます。

キュー1に割り当てられた厳格なバッファはありません。柔軟なバッファの最小割り当ては、1ギガビットポートの場合は300バッファ、10ギガビットポートの場合は900バッファ、40ギガビットポートの場合は3600バッファです。キュー1の柔軟なバッファの最大割り当ては、柔軟なバッファの最小割り当ての4倍に設定されます。つまり、1ギガビットポートの場合は1200バッファ、10ギガビットポートの場合は3600バッファ、40ギガビットポートの場合は14400バッファです。



- (注) デフォルトでは、キュー0はプライオリティキューではありません。ポリシーマップでは、**priority level** コマンドを使用して、キュー0をプライオリティキューにすることができます。キュー0にプライオリティレベル1が割り当てられている場合、このキューのソフト最大制限はハード最大制限と同じ値に自動的に設定されます。

C9300-24UB、C9300-24UXB、および C9300-48UB スイッチでのキューバッファ管理

Cisco Catalyst 9300 スイッチ、C9300-24UB、C9300-24UXB、および C9300-48UB は、C9300 シリーズの他のスイッチと比較して、速度の不一致によるマイクロバーストトラフィックおよび輻輳を処理するパケットバッファ機能を拡張するために大きなバッファがプロビジョニングされています。スタッキングモードと非スタッキングモードを選択することにより、大きなバッファサイズを有効または無効にできます。

C9300-24UB および C9300-48UB スイッチのスタッキングモードと非スタッキングモードのバッファは、**qos stack-buffer** コマンドを使用して管理できます。



- (注) C9300-24UXB は **qos stack-buffer** コマンドをサポートしていません。C9300-24UXB は常にスタッキングモードで起動します。

デフォルトでは、C9300-24UB、C9300-24UXB、C9300-48UB スイッチの起動時にスタッキングが有効になります。**qos stack-buffer disable** コマンドを実行してからスイッチをリロードすると、C9300-24UB および C9300-48UB スイッチをスタンドアロンモード（非スタッキングモード）で起動できます。スタンドアロンモードでは、スイッチのスタッキング機能は無効です。スタッキングモードに切り替えるには、**qos stack-buffer enable** コマンドを実行し、**write memory** コマンドを使用して設定を保存してから、デバイスをリロードします。



- (注) C9300-24UB、C9300-24UXB、および C9300-48UB を C9300 シリーズの他のスイッチとスタックすることはできません。C9300-24UB、C9300-24UXB、および C9300-48UB スイッチは、相互にのみスタックできます。

キューバッファの割り当て

キューに対するバッファ割り当ては、**queue-buffers ratio** ポリシーマップクラス コンフィギュレーション コマンドを使用して調整できます。

ダイナミックなしきい値および拡張

従来、予約バッファは各キューに静的に割り当てられていました。キューがアクティブかどうかにかかわらず、バッファはキューに保持されます。さらに、キューの数が増えるに従って、各キューに割り当てられた予約バッファの部分が徐々に短くなることがあります。最終的に、すべてのキューのジャンボフレームをサポートするのに十分な予約バッファがなくなる可能性があります。

デバイスは、バッファリソースを公平かつ効率的に割り当てる機能として、ダイナミックなしきい値および拡張 (DTS) をサポートしています。輻輳が発生すると、この DTS 機能はグローバル/ポートリソースの占有に基づいて、着信データにバッファを柔軟に割り当てます。概念上、DTS は、リソースを他のキューが使用できるように、キューバッファの割り当てを徐々に縮小します。逆も同様です。この柔軟な方法によって、バッファをより効率的かつ公平に利用できるようになります。

前の項で説明したように、キューには厳格な制限と柔軟な制限の2つの制限が設定されています。

厳格な制限は DTS の一部ではありません。これらのバッファはそのキューにだけ使用できます。厳格な制限の合計は、グローバルに設定された厳格な最大制限未満である必要があります。出力キューイングのために設定されたグローバルな厳格な制限は、現在 5705 に設定されています。MQC ポリシーが設定されていないデフォルトのシナリオでは、24 の 1 ギガビットポートが $24 * 67 = 1608$ を使用し、4 つの 10 ギガビットポートが $4 * 720 = 2880$ を使用し、合計 4488 のバッファを使用して、設定に基づいてより厳格なバッファを割り当てることができます。

柔軟なバッファ制限は DTS プロセスに参加します。さらに、柔軟なバッファ割り当ての一部は、グローバルな柔軟な制限の割り当てを超えることができます。出力キューイング用のグローバルな柔軟な制限は、現在 27024 に設定されています。厳格な制限と柔軟な制限の合計は 39696 になり、10.1 MB に変換されます。柔軟なバッファ割り当ての合計がグローバルな制限を超える場合があるため、システムの負荷が軽ければ、特定のキューで多数のバッファを使用できるようになります。DTS プロセスはシステムの負荷が増大するにしたがって、キュー単位の割り当てを動的に調整します。

重み付けランダム早期検出

重み付けランダム早期検出 (WRED) は、ネットワークでの輻輳を回避するメカニズムです。WRED は、出力インターフェイスにネットワーク混雑の兆候が表れた際に、選択的にパケットをドロップしてテールドロップの確率を減らし、多数のパケットが一度にドロップされないようにします。

WRED の詳細については、次を参照してください。 [重み付けランダム早期検出の設定 \(137 ページ\)](#)

信頼動作

Cisco IP Phone の信頼境界機能のポート セキュリティ

一般的なネットワークでは、デバイスポートに Cisco IP Phone を接続し、電話の背後からデータパケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイプライオリティ (CoS=5) にマーキングし、データパケットをロープライオリティ (CoS=0) にマーキングすることで、共有データリンクを通して音声品質を保証しています。電話からデバイスに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビットフィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からデバイスへ送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。 **trust device** インターフェイスコンフィギュレーションコマンドを使用して、電話の接続先のデバイスポートが受信トラフィックを信頼するように設定します。



- (注) インターフェイスコンフィギュレーションモードで使用可能な **trust device device_type** コマンドは、デバイスでのスタンドアロンコマンドです。このコマンドを AutoQoS 設定で使用するときに、接続されているピアデバイスが対応デバイス (信頼ポリシーに一致するデバイスとして定義されているデバイス) ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。接続されているピアデバイスが対応するデバイスである場合は、入力ポリシーが有効になります。

信頼設定により、ユーザが電話をバイパスして PC を直接デバイスに接続する場合に、ハイプライオリティキューの誤使用を避けるため信頼境界機能も使用できます。信頼境界機能を使用しないと、（信頼性のある CoS 設定により）PC が生成した CoS ラベルがデバイスで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してデバイスポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。電話が検出されない場合、信頼境界機能がハイプライオリティキューの誤使用を避けるためにデバイスポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がデバイスに接続されているハブに接続されている場合は機能しないことに注意してください。

有線ポートの信頼動作

次の表に、着信パケットタイプが発信パケットタイプと異なる場合の信頼動作およびキューイング動作を示します。ポートのデフォルトの信頼モードが DSCP ベースであることに注意してください。信頼モードは、着信パケットが純粋なレイヤ 2 パケットの場合、CoS に「フォールバック」します。また、信頼設定を DSCP から CoS に変更できます。この設定変更は、「set cos cos table default default-cos」アクションのクラス デフォルトがある MQC ポリシーによって実現されます。ここで、default-cos は作成されるテーブルマップ名です（デフォルトコピーだけを実行）。

デバイス（IP フォン、ラップトップ、カメラ、TelePresence ユニットなどのエンドポイント、またはその他のデバイス）に接続されている有線ポートの場合、インターフェイス上で信頼デバイス設定が有効になります。明示的なポリシー設定がない場合、これらのエンドポイントから、またはこれらエンドポイントへの DSCP 値、precedence 値、または CoS 値はデバイスで信頼されるため、保持されます。

パケットはデフォルトの初期設定ごとに適切なキューに入れられます。デフォルトでは、デバイスでのプライオリティキューイングは実行されません。これは、ユニキャストおよびマルチキャストパケットに当てはまります。

表 7: 信頼およびキューイング動作

着信パケット	発信パケット	信頼動作	キューイング動作
レイヤ 3	レイヤ 3	DSCP/Precedence の保持	DSCP に基づく
レイヤ 2	レイヤ 2	N/A	CoS に基づく
タグ付き	タグ付き	DSCP および CoS の保持	DSCP に基づく（信頼 DSCP が優先）
レイヤ 3	タグ付き	DSCP の保持、すなわち CoS が 0 に設定される	DSCP に基づく

標準 QoS のデフォルト設定

デフォルトの有線 QoS 設定

デバイスの各有線インターフェイスでは、デフォルトで2つのキューが設定されます。すべての制御トラフィックはキュー0を通過し、処理されます。その他すべてのトラフィックはキュー1を通過し、処理されます。

DSCP マップ

デフォルトの CoS/DSCP マップ

DSCP 透過モードを無効にすると、DSCP 値は次の表に従って CoS から抽出されます。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

(注) DSCP 透過モードはデフォルトでは無効になっています。これがイネーブルになっている場合 (`mls qos rewrite ip dscp` コンフィギュレーションコマンド)、DSCP の書き換えは実行されません。

表 8: デフォルトの CoS/DSCP マップ

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

デフォルトの IP Precedence/DSCP マップ

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。次の表は、

デフォルトの IP Precedence/DSCP マップを示しています。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 9: デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

デフォルトの DSCP/CoS マップ

4つの出力キューのうち1つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。次の表に、デフォルトの DSCP/CoS マップを示します。これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

表 10: デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ~ 7	0
8 ~ 15	1
16 ~ 23	2
24 ~ 31	3
32 ~ 39	4
40 ~ 47	5
48 ~ 55	6
56 ~ 63	7

有線ターゲットの QoS に関する制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線ターゲットには、ポートまたは VLAN を指定できます。

次に、QoS 機能を有線ターゲットのデバイスに適用する場合の制限事項を示します。

- 有線ターゲットのデバイスポートでは、最大 8 つのキューイングクラスがサポートされません。
- 有線ターゲットの有線ポートでは、入力または出力方向でポリシーごとに最大 63 のポリサーがサポートされます。
- Cisco IOS XE リリース 16.x.x 以降のリリースでは、ダウンリンクポートのサイズは 10 GB ですが、デフォルトでは、すべてのダウンリンクポートに 1 GB のポートバッファが割り当てられます。この変更の前は、すべての 1 GB ダウンリンクポートには 1 GB バッファが、10 GB ダウンリンクポートには 10 GB バッファが割り当てられていました。
- 最大 1599 のポリシーマップを作成できます。
- QoS 階層でサポートされるのは最大 2 レベルです。
- 階層型ポリシーでは、子ポリシーの親およびキュー機能のポリシーにポートシェーパーがある場合を除き、親子間のオーバーラップは許可されていません。
- QoS ポリシーは、EtherChannel インターフェイスに付加できません。
- 親と子の両方のポリシングは、QoS 階層ではサポートされていません。
- 親と子の両方のマーキングは、QoS 階層ではサポートされていません。
- シェーピングでは、ハードウェア内部に占める 20 バイトの IPG オーバーヘッドがすべてのパケットにあります。シェーピングの精度はこれにより向上し、とくに小さいサイズのパケットに対して効果があります。
- 空のクラスはサポートされません。
- 空のアクションによるクラスマップはサポートされません。クラスマップの順序が同じポリシーが 2 つあり、どちらかのポリシーにアクションが含まれていないクラスマップがある場合、トラフィックのドロップが起こる可能性があります。回避策として、PRIORITY_QUEUE 内のすべてのクラスに最小帯域幅を割り当てます。
- 有線ターゲットの有線ポートでは、ポリシーごとに最大 256 のクラスがサポートされません。
- Cisco UADP アーキテクチャに基づき、トラフィックは QoS ルックアップの対象となり、対応する設定済みアクションに従います。このトラフィックがたとえ Egress Global Resolution ブロックに後でドロップされて、実際のインターフェイスから送信されない場合も同様です。
- ポリシーマップ内のポリサーのアクションには、次の制限事項があります。

- 適合アクションは送信する必要があります。
- マークダウンタイプの超過/違反アクションは、`cos2cos`、`prec2prec`、`dscp2dscp` だけです。
- マークダウンタイプはポリシー内で同じである必要があります。
- SVI では、マーキングポリシーのみがサポートされます。
- ポート レベルの入力マーキング ポリシーは SVI ポリシーより優先されますが、ポート ポリシーが設定されていない場合は、SVI ポリシーが優先されます。優先するポート ポリシーに対し、ポートレベルのポリシーを定義します。SVI ポリシーが上書きされるようにするためです。
- 分類カウンタには、次の制限事項があります。
 - 分類カウンタは、バイトの代わりにパケットをカウントします。
 - フィルタ ベースの分類カウンタはサポートされません。
 - マーキングまたはポリシングによる QoS 設定だけが、分類カウンタをトリガーします。
 - 分類カウンタはポートベースではありません。これは、分類カウンタが、異なるインターフェイスに接続し、同じポリシーの同じクラスに属するすべてのパケットを集約することを意味します。
 - ポリシー内にポリシングまたはマーキングアクションがある限り、クラスは分類カウンタを保持します。
 - 分類カウンタは、どのクラスマップ下の完全なキューイングポリシーでもサポートされません。
 - クラスに複数の `match` ステートメントがある場合、トラフィックカウンタはクラスのすべての `match` ステートメントで累積されます。
 - 分類カウンタ (クラスマップ) は、帯域幅、WRED、キューバッファ、シェーピングなどのアクションを含むキューイングポリシーでは使用できません。**`show policy-map interface`** コマンド出力には、リマーキングまたはポリサーアクションのいずれかを持つポリシーの分類カウンタ (クラスマップ) のみが表示されます。
- デバイスは、ポリサー超過マークダウンでは合計 8 つのテーブルマップ、ポリサー違反マークダウンでは 8 つのテーブルマップをサポートします。
- 階層型ポリシーは次の機能で必要になります。
 - ポート シェーパー
 - 集約ポリシング機能
 - PV ポリシー
 - 親シェーピングおよび子マーキング/ポリシング

- 親シェーピングと、プライオリティ レベルキューイングおよびプライオリティ レベル ポリシングが設定された子ポリシーを含む HQoS ポリシーでは、ポリシングの統計情報は更新されません。QoS シェイパーの統計情報のみが更新されます。QoS シェイパーの統計情報を表示するには、グローバルコンフィギュレーションモードで **show policy-map interface** コマンドを使用します。
- 有線ターゲットを含むポートでは、次の階層型ポリシーだけがサポートされています。
 - 同じポリシー内でのポリシングの連結はサポートされていません。
 - 同じポリシー内で階層型キューイングはサポートされていません（ポートシェイパーは例外）。
 - 親クラスでは、すべてのフィルタが同じタイプでなければなりません。子フィルタタイプは次の例外を除き、親フィルタのタイプと一致する必要があります。
 - IP に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。
 - CoS に一致するように親クラスが設定されている場合、ACL に一致するように子クラスを設定できます。
- インターフェイス コンフィギュレーションモードで使用可能な **trust device device_type** コマンドは、デバイスでのスタンドアロンコマンドです。このコマンドを AutoQoS 設定で使用するとき、接続されているピアデバイスが対応デバイス（信頼ポリシーに一致するデバイスとして定義されているデバイス）ではない場合、CoS 値と DSCP 値の両方が「0」に設定され、いずれの入力ポリシーも有効になりません。接続されているピアデバイスが対応するデバイスである場合は、入力ポリシーが有効になります。

次に、VLAN の QoS 機能を有線ターゲットに適用する場合の制限事項を示します。

- フラットつまり非階層型ポリシーでは、マーキングまたはテーブルマップのみサポートされます。

次に、EtherChannel とチャネル メンバー インターフェイスで QoS 機能を適用するための制限事項と考慮事項を示します。

- QoS は、EtherChannel インターフェイスではサポートされません。
- QoS は、入力および出力方向の EtherChannel メンバー インターフェイスでサポートされます。すべての EtherChannel メンバーが同じ QoS ポリシーを適用する必要があります。QoS ポリシーが同じでない場合、異なるリンクの個々のポリシーは独立して機能します。
- チャネルメンバーへサービスポリシーを付加すると、EtherChannel 内のすべてのポートに同じポリシーが接続されていることを確認するようユーザーに知らせる、次の警告メッセージが表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」
- 自動 QoS は EtherChannel メンバーではサポートされません。



- (注) EtherChannel ヘサービス ポリシーを付加すると、次のメッセージがコンソールに表示されます。「Warning: add service policy will cause inconsistency with port xxx in ether channel xxx.」。この警告メッセージは予期されるメッセージです。この警告メッセージは、同じ EtherChannel 内の他のポートに同じポリシーを付加するように促すものです。同じメッセージがブートアップ中にも表示されます。このメッセージは、EtherChannel メンバーポート間に不一致があることを意味するものではありません。

QoS の設定方法

クラス、ポリシー、およびマップの設定

トラフィック クラスの作成

一致基準が含まれるトラフィッククラスを作成するには、**class-map** コマンドを使用してトラフィッククラス名を指定し、必要に応じて、次の **match** コマンドをクラスマップコンフィギュレーションモードで使用します。

始める前に

この設定作業で指定するすべての **match** コマンドの使用は任意ですが、1 つのクラスに少なくとも 1 つの一致基準を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	class-map class-map name { match-any match-all } 例： Device(config)# class-map test_1000 Device(config-cmap)#	クラス マップ コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> 名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。 match-any : トラフィッククラスで受信したトラフィックがその一部と分類されるには、一致基準のいずれかを満たす必要があります。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • match-all : トラフィック クラスで受信したトラフィックがトラフィック クラスの一部と分類されるには、すべての一致基準を満たす必要があります。 <p>(注) これはデフォルトです。match-any または match-all が明示的に定義されていない場合、デフォルトで match-all が選択されます。</p>
ステップ 3	<p>match access-group {<i>index number</i> <i>name</i>}</p> <p>例 :</p> <pre>Device (config-cmap) # match access-group 100 Device (config-cmap) #</pre>	<p>このコマンドでは次のパラメータを使用できます。</p> <ul style="list-style-type: none"> • access-group • cos • dscp • group-object • ip • mpls • non-client-nrt • precedence • protocol • qos-group • vlan • wlan <p>(任意) この例では、アクセス グループ ID を入力します。</p> <ul style="list-style-type: none"> • アクセス リスト インデックス (1 ~ 2799 の値) • 名前付きアクセス リスト

	コマンドまたはアクション	目的
ステップ 4	match cos <i>CoS</i> 値 例 : Device(config-cmap) # match cos 2 3 4 5 Device(config-cmap) #	(任意) IEEE 802.1Q または ISL サービスクラス (ユーザー) プライオリティ値に一致します。 <ul style="list-style-type: none"> 最大 4 つの CoS 値 (0 ~ 7) をスペースで区切って入力します。
ステップ 5	match dscp <i>DSCP</i> 値 例 : Device(config-cmap) # match dscp af11 af12 Device(config-cmap) #	(任意) IPv4 および IPv6 パケットの DSCP 値に一致します。
ステップ 6	match ip { dscp <i>dscp value</i> precedence <i>precedence value</i> } 例 : Device(config-cmap) # match ip dscp af11 af12 Device(config-cmap) #	(任意) 次を含む IP 値に一致します。 <ul style="list-style-type: none"> dscp : IP DSCP (DiffServ コードポイント) に一致します。 precedence : IP precedence (0 ~ 7) に一致します。 (注) CPU 生成パケットは出力時にマークされないため、パケットは設定されたクラスマップと一致しません。
ステップ 7	match qos-group <i>QoS</i> グループ値 例 : Device(config-cmap) # match qos-group 10 Device(config-cmap) #	(任意) QoS グループ値 (0 ~ 31) に一致します。
ステップ 8	match vlan <i>vlan value</i> 例 : Device(config-cmap) # match vlan 210 Device(config-cmap) #	(任意) VLAN ID (1 ~ 4095) に一致します。
ステップ 9	end 例 :	設定の変更内容を保存します。

	コマンドまたはアクション	目的
	Device(config-cmap)# end	

次のタスク

ポリシー マップを設定します。

トラフィック ポリシーの作成

トラフィックポリシーを作成するには、**policy-map** グローバル コンフィギュレーション コマンドを使用して、トラフィックポリシーの名前を指定します。

トラフィッククラスは、**class** コマンドを使用したときにトラフィックポリシーと関連付けられます。**class** コマンドは、ポリシーマップ コンフィギュレーション モードを開始した後に実行しなければなりません。**class** コマンドを入力すると、デバイスが自動的にポリシー マップ クラス コンフィギュレーション モードを開始します。ここでトラフィックポリシーの QoS ポリシーを定義します。

次のポリシー マップ クラスのアクションがサポートされます。

- **bandwidth** : 帯域幅設定オプション。
- **exit** : QoS クラス アクション コンフィギュレーション モードを終了します。
- **no** : コマンドのデフォルト値を無効にするか、設定します。
- **police** : ポリシング機能の設定オプション。
- **priority** : このクラスの完全スケジューリング プライオリティの設定オプション。
- **queue-buffers** : キューのバッファ設定オプション。
- **queue-limit** : 重み付けテールドロップ (WTD) 設定オプションのキューの最大しきい値。
- **service-policy** : QoS サービス ポリシーを設定します。
- **set** : 次のオプションを使用して QoS 値を設定します。
 - CoS 値
 - DSCP 値
 - precedence 値
 - QoS グループ値
- **shape** : トラフィック シェーピング設定オプション。

始める前に

最初にクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map <i>policy-map name</i> 例 : Device(config)# policy-map test_2000 Device(config-pmap)#	ポリシーマップ コンフィギュレーション モードを開始します。 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
ステップ 3	class {<i>class-name</i> class-default } 例 : Device(config-pmap)# class test_1000 Device(config-pmap-c)#	ポリシーを作成または変更するクラスの名前を指定します。 未分類のパケットのシステムデフォルトクラスも作成できます。
ステップ 4	bandwidth { <i>Kb/s</i> percent <i>percentage</i> remaining {<i>percent</i> <i>ratio</i>} } 例 : Device(config-pmap-c)# bandwidth 500 Device(config-pmap-c)#	(任意) 次のいずれかを使用して帯域幅を設定します。 <ul style="list-style-type: none"> • Kb/s : キロビット/秒。Kb/s に 100 ~ 100000000 の値を入力します。 • percent : このポリシーマップに使用される総帯域幅の割合を入力します。 • remaining : 残りの帯域幅の割合を入力します。 このコマンドおよび使用の詳細な例については、 帯域幅の設定 (101 ページ) を参照してください。
ステップ 5	exit 例 : Device(config-pmap-c)# exit Device(config-pmap-c)#	(任意) QoS クラス アクション コンフィギュレーションモードを終了します。
ステップ 6	no 例 :	(任意) コマンドを無効にします。

	コマンドまたはアクション	目的
	Device(config-pmap-c) # no Device(config-pmap-c) #	
ステップ 7	police { <i>target_bit_rate</i> cir rate } 例 : Device(config-pmap-c) # police 100000 Device(config-pmap-c) #	(任意) ポリサーを設定します。 <ul style="list-style-type: none"> • target_bit_rate : ビットレート/秒を入力します。8000 ~ 10000000000 の値を入力します。 • cir : 認定情報レート。 • rate : ポリシングレート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。 このコマンドおよび使用の詳細な例については、 ポリシングの設定 (103 ページ) を参照してください。
ステップ 8	priority { <i>kb/s</i> level level value percent percentage value } 例 : Device(config-pmap-c) # priority level 1 percent 50 Device(config-pmap-c) #	(任意) このクラスに完全スケジューリングプライオリティを設定します。コマンド オプションは次のとおりです。 <ul style="list-style-type: none"> • kb/s : キロビット/秒。1 ~ 2000000 の値を入力します。 • level : マルチレベル プライオリティキューを確立します。値を入力します (1 または 2)。 • percent : このプライオリティの全帯域幅の割合を入力します。 このコマンドおよび使用の詳細な例については、 プライオリティの設定 (106 ページ) を参照してください。
ステップ 9	queue-buffers ratoratio limit 例 : Device(config-pmap-c) # queue-buffers ratio 10 Device(config-pmap-c) #	(任意) クラスのキューバッファを設定します。キューバッファの割合制限 (0 ~ 100) を入力します。 このコマンドおよび使用の詳細な例については、 キューバッファの設定 (111 ページ) を参照してください。

	コマンドまたはアクション	目的
ステップ 10	<p>queue-limit {<i>packets</i> cos dscp percent}</p> <p>例 :</p> <pre>Device(config-pmap-c) # queue-limit cos 7 percent 50 Device(config-pmap-c) #</pre>	<p>(任意) テール ドロップに対してキューの最大しきい値を指定します。</p> <ul style="list-style-type: none"> • packets : デフォルトのパケット数。1 ~ 2000000 の値を入力します。 • cos : 各 CoS 値のパラメータを入力します。 • dscp : 各 DSCP 値のパラメータを入力します。 • percent : しきい値の割合を入力します。 <p>このコマンドおよび使用の詳細な例については、キュー制限の設定 (114 ページ) を参照してください。</p>
ステップ 11	<p>service-policy <i>policy-map name</i></p> <p>例 :</p> <pre>Device(config-pmap-c) # service-policy test_2000 Device(config-pmap-c) #</pre>	<p>(任意) QoS サービスポリシーを設定します。</p>
ステップ 12	<p>set {cos dscp ip precedence qos-group wlan}</p> <p>例 :</p> <pre>Device(config-pmap-c) # set cos 7 Device(config-pmap-c) #</pre>	<p>(任意) QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。</p> <ul style="list-style-type: none"> • cos : IEEE 802.1Q/ISL サービスクラスまたはユーザープライオリティを設定します。 • dscp : IP(v4) および IPv6 パケットに DSCP を設定します。 • ip : IP 固有の値を設定します。 • precedence : IP(v4)、IPv6 パケットの優先順位を設定します。 • qos-group : QoS グループを設定します。
ステップ 13	<p>shape average {<i>target_bit_rate</i> percent}</p> <p>例 :</p>	<p>(任意) トラフィックシェーピングを設定します。コマンドパラメータは次のとおりです。</p>

	コマンドまたはアクション	目的
	<pre>Device(config-pmap-c) #shape average percent 50 Device(config-pmap-c) #</pre>	<ul style="list-style-type: none"> • target_bit_rate : ターゲットビットレート。 • percent : 認定情報レートのインターフェイス帯域幅の割合。 <p>このコマンドおよび使用の詳細な例については、シェーピングの設定 (117 ページ) を参照してください。</p>
ステップ 14	<p>end</p> <p>例 :</p> <pre>Device(config-pmap-c) #end Device(config-pmap-c) #</pre>	設定の変更内容を保存します。

次のタスク

インターフェイスを設定します。

クラスベース パケット マーキングの設定

この手順は、次のクラスベース パケット マーキング機能をデバイスで設定する方法を示します。

- CoS 値
- DSCP 値
- IP 値
- precedence 値
- QoS グループ値
- WLAN 値

始める前に

この手順を開始する前にクラス マップとポリシー マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 2	<p>policy-map <i>policy name</i></p> <p>例 :</p> <pre>Device(config)# policy-map policy1 Device(config-pmap)#</pre>	<p>ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。</p>
ステップ 3	<p>class <i>class name</i></p> <p>例 :</p> <pre>Device(config-pmap)# class class1 Device(config-pmap-c)#</pre>	<p>ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。</p> <p>ポリシー クラス マップ コンフィギュレーションモードには、次のコマンド オプションが含まれます。</p> <ul style="list-style-type: none"> • bandwidth : 帯域幅設定オプション。 • exit : QoS クラス アクション コンフィギュレーションモードを終了します。 • no : コマンドのデフォルト値を無効にするか、設定します。 • police : ポリシング機能の設定オプション。 • priority : このクラスの完全スケジューリングプライオリティの設定オプション。 • queue-buffers : キューのバッファ設定オプション。 • queue-limit : 重み付けテールドロップ (WTD) 設定オプションのキューの最大しきい値。 • service-policy : QoS サービスポリシーを設定します。 • set : 次のオプションを使用して QoS 値を設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • CoS 値 • DSCP 値 • precedence 値 • QoS グループ値 • WLAN 値 <p>• shape : トラフィック シェーピング設定オプション。</p> <p>(注) この手順では、set コマンドオプションを使用して、使用可能な設定について説明します。その他のコマンドオプション (bandwidth) についてはこのマニュアルの他の項で説明します。このタスクでは、使用可能なすべての set コマンドが表示されますが、クラス単位でサポートされるのは1つの set コマンドだけです。</p>
ステップ 4	<p>例 :</p> <pre>Device(config-pmap) # set cos 5 Device(config-pmap) #</pre>	<p>(任意) 発信パケットの固有の IEEE 802.1Q レイヤ 2 CoS 値を設定します。値は 0 ~ 7 です。</p> <p>set cos コマンドを使用して次の値を設定することもできます。</p> <ul style="list-style-type: none"> • cos table : CoS 値をテーブル マップに基づいて設定します。 • dscp table : コード ポイント値をテーブルマップに基づいて設定します。 • precedence table : コード ポイント値をテーブルマップに基づいて設定します。 • qos-group table : テーブル マップに基づいて QoS グループから CoS 値を設定します。

	コマンドまたはアクション	目的
ステップ 5	<p>例 :</p> <pre>Device(config-pmap)# set dscp af11 Device(config-pmap)#</pre>	<p>(任意) DSCP 値を設定します。</p> <p>特定の DSCP 値の設定に加えて、set dscp コマンドを使用して次を設定できます。</p> <ul style="list-style-type: none"> • default : パケットをデフォルト DSCP 値 (000000) と一致させます。 • dscp table : テーブルマップに基づいて DSCP からパケットの DSCP 値を設定します。 • ef : パケットを EF DSCP 値 (101110) と一致させます。 • precedence table : テーブルマップに基づいて優先順位からパケットの DSCP 値を設定します。 • qos-group table : テーブルマップに基づいて QoS グループからパケットの DSCP 値を設定します。
ステップ 6	<p>set ip {dscp precedence}</p> <p>例 :</p> <pre>Device(config-pmap)# set ip dscp c3 Device(config-pmap)#</pre>	<p>(任意) IP 固有の値を設定します。これらの値は、IP DSCP 値または IP precedence 値です。</p> <p>set ip dscp コマンドを使用して、次の値を設定することができます。</p> <ul style="list-style-type: none"> • dscp value : 特定の DSCP の値を設定します。 • default : パケットをデフォルト DSCP 値 (000000) と一致させます。 • dscp table : テーブルマップに基づいて DSCP からパケットの DSCP 値を設定します。 • ef : パケットを EF DSCP 値 (101110) と一致させます。 • precedence table : テーブルマップに基づいて優先順位からパケットの DSCP 値を設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • qos-group table : テーブル マップに基づいて QoS グループからパケットの DSCP 値を設定します。 <p>set ip precedence コマンドを使用して、次の値を設定することができます。</p> <ul style="list-style-type: none"> • <i>precedence value</i> : precedence 値を設定します (0 ~ 7) 。 • cos table : テーブル マップに基づいてレイヤ 2 CoS からパケットの precedence 値を設定します。 • dscp table : テーブルマップに基づいて DSCP 値からパケットの precedence 値を設定します。 • precedence table : テーブルマップに基づいて優先順位から precedence 値を設定します。 • qos-group table : テーブル マップに基づいて QoS グループから precedence 値を設定します。
ステップ 7	<p>set precedence {<i>precedence value</i> cos table <i>table-map name</i> dscp table <i>table-map name</i> precedence table <i>table-map name</i> qos-group table <i>table-map name</i>}</p> <p>例 :</p> <pre>Device(config-pmap)# set precedence 5 Device(config-pmap)#</pre>	<p>(任意) IPv4 と IPv6 パケットの precedence 値を設定します。</p> <p>set precedence コマンドを使用して、次の値を設定することができます。</p> <ul style="list-style-type: none"> • <i>precedence value</i> : precedence 値を設定します (0 ~ 7) 。 • cos table : レイヤ 2 CoS からのパケットの precedence 値をテーブルマップに基づいて設定します。 • dscp table : テーブルマップに基づいて DSCP 値からパケットの precedence 値を設定します。 • precedence table : テーブルマップに基づいて優先順位から precedence 値を設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • qos-group table : テーブル マップに基づいて QoS グループから precedence 値を設定します。
ステップ 8	set qos-group { <i>qos-group value</i> dscp table <i>table-map name</i> precedence table <i>table-map name</i> } 例 : Device(config-pmap) # set qos-group 10 Device(config-pmap) #	(任意) QoS グループ値を設定します。このコマンドを使用して次の値を設定できます。 <ul style="list-style-type: none"> • <i>qos-group value</i> : 1 から 31 までの数。 • dscp table : テーブルマップに基づいて DSCP からコードポイント値を設定します。 • precedence table : テーブルマップに基づいて優先順位からコードポイント値を設定します。
ステップ 9	end 例 : Device(config-pmap) # end Device#	設定変更を保存します。
ステップ 10	show policy-map 例 : Device# show policy-map	(任意) すべてのサービスポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

service-policy コマンドを使用して、インターフェイスにトラフィック ポリシーを付加します。

トラフィック ポリシーのインターフェイスへの適用

トラフィッククラスとトラフィックポリシーの作成後、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、トラフィックポリシーをインターフェイスに付加し、ポリシーを適用する方向を指定します (インターフェイスに着信するパケットまたはインターフェイスから送信されるパケット)。

始める前に

インターフェイスにトラフィックポリシーを付加する前に、トラフィッククラスとトラフィックポリシーを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type 例 : Device(config)# interface GigabitEthernet1/0/1 Device(config-if)#	インターフェイス コンフィギュレーション モードを開始し、インターフェイスを設定します。 インターフェイス コンフィギュレーションのコマンド パラメータは次のとおりです。 <ul style="list-style-type: none"> • ANI : 自律型 ネットワーキング 仮想 インターフェイス • AccessTunnel : アクセス トンネル インターフェイス • Auto Template : 自動 テンプレート インターフェイス • CEM-PG : 保護 グループ を持つ 回線 エミュレーション インターフェイス • FortyGigabitEthernet : 40 ギガビット イーサネット • GigabitEthernet : Gigabit Ethernet IEEE 802.3z • Internal Interface : 内部 インターフェイス • LISP : ロケータ ID 分離 プロトコル 仮想 インターフェイス • Loopback : ループバック インターフェイス • Null : ノル インターフェイス • PROTECTION_GROUP : 保護 グループ コントローラ • Port-channel : インターフェイスの イーサネット チャネル

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • SDH_ACR : 仮想 SDH-ACR コントローラ • TLS-VIF : TLS 仮想インターフェイス • TenGigabitEthernet : 10 ギガビットイーサネット • Tunnel : トンネルインターフェイス • Tunnel-tp : MPLS トランスポートプロファイルインターフェイス • Vlan : Catalyst VLAN • Range : インターフェイス範囲 <p>(注) トンネルインターフェイスはサポートされていません。</p>
ステップ 3	service-policy { input <i>policy-map</i> output <i>policy-map</i> } 例 : <pre>Device(config-if)# service-policy output policy_map_01 Device(config-if)#</pre>	<p>ポリシー マップを入力または出力インターフェイスに適用します。このポリシー マップは、そのインターフェイスのサービス ポリシーとして使用されます。</p> <p>この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。</p>
ステップ 4	end 例 : <pre>Device(config-if)# end Device#</pre>	設定変更を保存します。
ステップ 5	show policy map 例 : <pre>Device# show policy map</pre>	(任意) 指定されたインターフェイスのポリシーの統計情報を表示します。

次のタスク

他のトラフィック ポリシーをインターフェイスに付加し、ポリシーを適用する方向を指定します。

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。サポートされるアクションは再マーキングとポリシングです。

始める前に

この手順を開始する前に、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて、あらかじめポリシー マップによって決定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	class-map { <i>class-map name</i> match-any match-all } 例 : Device (config)# class-map ipclass1 Device (config-cmap)# exit Device (config)#	クラスマップ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> 名前を指定したクラスとパケットとの照合に使用されるクラスマップを作成します。 match-any を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。これはデフォルトです。 match-all を指定すると、トラフィック クラスで受信したトラフィックがトラフィック クラスの一部と分類されるには、すべての一致基準を満たす必要があります。

	コマンドまたはアクション	目的
		<p>(注) これはデフォルトです。 match-any または match-all が明示的に定義されていない場合、デフォルトで match-all が選択されます。</p>
ステップ 3	<p>match access-group { <i>access list index</i> <i>access list name</i> }</p> <p>例 :</p> <pre>Device(config-cmap)# match access-group 1000 Device(config-cmap)# exit Device(config)#</pre>	<p>このコマンドでは次のパラメータを使用できます。</p> <ul style="list-style-type: none"> • access-group • cos • dscp • group-object • ip • mpls • non-client-nrt • precedence • protocol • qos-group • vlan • wlan <p>(任意) この例では、アクセスグループ ID を入力します。</p> <ul style="list-style-type: none"> • アクセス リスト インデックス (1 ~ 2799 の値) • 名前付きアクセス リスト
ステップ 4	<p>policy-map <i>policy-map-name</i></p> <p>例 :</p> <pre>Device(config)# policy-map flowit Device(config-pmap)#</pre>	<p>ポリシー マップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシーマップは定義されていません。</p>

	コマンドまたはアクション	目的
ステップ 5	<p>class {<i>class-map-name</i> class-default}</p> <p>例 :</p> <pre>Device (config-pmap) # class ipclass1 Device (config-pmap-c) #</pre>	<p>トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップ クラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p> <p>class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシー マップの最後に配置されます。暗黙の match any が class-default クラスに含まれている場合、他のトラフィック クラスと一致しないパケットはすべて class-default と一致します。</p>
ステップ 6	<p>set {cos dscp ip precedence qos-group wlan user-priority}</p> <p>例 :</p> <pre>Device (config-pmap-c) # set dscp 45 Device (config-pmap-c) #</pre>	<p>(任意) QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。</p> <ul style="list-style-type: none"> • cos : IEEE 802.1Q/ISL サービス クラスまたはユーザー プライオリティを設定します。 • dscp : IP (v4) および IPv6 パケットの DSCP を設定します。 • ip : IP 固有の値を設定します。 • precedence : IP (v4) および IPv6 パケットの precedence を設定します。 • qos-group : QoS グループを設定します。 <p>この例では、set dscp コマンドが、パケットでの新しい DSCP 値を設定して IP トラフィックを分類します。</p>
ステップ 7	<p>police {<i>target_bit_rate</i> cir rate}</p> <p>例 :</p>	<p>(任意) ポリサーを設定します。</p>

	コマンドまたはアクション	目的
	<pre>Device(config-pmap-c) # police 100000 conform-action transmit exceed-action drop Device(config-pmap-c) #</pre>	<ul style="list-style-type: none"> • target_bit_rate : ビットレート/秒を指定し、8000 ~ 10000000000 の値を入力します。 • cir : 認定情報レート。 • rate : 階層型ポリシーのポリシングレート PCR を指定します。 <p>この例では、police コマンドが 100000 セットのターゲットビットレートを超えるトラフィックがドロップされるクラスにポリサーを追加します。</p>
ステップ 8	<p>exit</p> <p>例 :</p> <pre>Device(config-pmap-c) # exit</pre>	ポリシーマップコンフィギュレーションモードに戻ります。
ステップ 9	<p>exit</p> <p>例 :</p> <pre>Device(config-pmap) # exit</pre>	グローバル コンフィギュレーションモードに戻ります。
ステップ 10	<p>interface interface-id</p> <p>例 :</p> <pre>Device(config) # interface HundredGigabitEthernet 1/0/2</pre>	<p>ポリシーマップを適用するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。</p> <p>有効なインターフェイスには、物理ポートが含まれます。</p>
ステップ 11	<p>service-policy input policy-map-name</p> <p>例 :</p> <pre>Device(config-if) # service-policy input flowit</pre>	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシーマップは、入力ポートに 1 つだけです。
ステップ 12	<p>end</p> <p>例 :</p> <pre>Device(config-if) # end</pre>	特権 EXEC モードに戻ります。
ステップ 13	<p>show policy-map [policy-map-name [class class-map-name]]</p>	(任意) 入力を確認します。

	コマンドまたはアクション	目的
	例 : Device# show policy-map	
ステップ 14	copy running-config startup-config 例 : Device# copy-running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次のタスク

必要に応じて QoS 設定は、ポリシー マップを使用して、SVI のトラフィックの分類、ポリシング、およびマーキングを設定します。

ポリシーマップによるトラフィックの分類およびマーキング

始める前に

この手順を開始する前に、ポリシー マップを使用して、ネットワーク トラフィックの分類、ポリシング、およびマーキングについて決定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	class-map {class-map name match-any match-all} 例 : Device(config)# class-map class_vlan100	クラスマップコンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> 名前を指定したクラスとパケットとの照合に使用されるクラスマップを作成します。 match-any を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • match-all を指定すると、トラフィック クラスで受信したトラフィックがトラフィッククラスの一部と分類されるには、すべての一致基準を満たす必要があります。 <p>(注) これはデフォルトです。 match-any または match-all が明示的に定義されていない場合、デフォルトで match-all が選択されます。</p>
ステップ 3	match vlan <i>vlan number</i> 例 : Device(config-cmap) # match vlan 100 Device(config-cmap) # exit Device(config) #	VLAN をクラスマップに一致するように指定します。
ステップ 4	policy-map <i>policy-map-name</i> 例 : Device(config) # policy-map policy_vlan100 Device(config-pmap) #	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーションモードを開始します。 デフォルトでは、ポリシーマップは定義されていません。
ステップ 5	description 説明 例 : Device(config-pmap) # description vlan 100	(任意) ポリシーマップの説明を入力します。
ステップ 6	class { <i>class-map-name</i> class-default } 例 : Device(config-pmap) # class class_vlan100 Device(config-pmap-c) #	トラフィック分類を定義し、ポリシーマップクラス コンフィギュレーションモードを開始します。 デフォルトでは、ポリシーマップクラスマップは定義されていません。 すでに class-map グローバル コンフィギュレーションコマンドを使用してトラフィッククラスが定義されている場

	コマンドまたはアクション	目的
		<p>合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p> <p>class-default トラフィッククラスは定義済みで、どのポリシーにも追加できます。このトラフィッククラスは、常にポリシーマップの最後に配置されます。暗黙の match any が class-default クラスに含まれている場合、他のトラフィッククラスと一致しないパケットはすべて class-default と一致します。</p>
ステップ 7	<p>set { cos dscp ip precedence qos-group wlan user-priority }</p> <p>例 :</p> <pre>Device(config-pmap-c)# set dscp af23 Device(config-pmap-c)#</pre>	<p>(任意) QoS 値を設定します。使用可能な QoS 設定値は次のとおりです。</p> <ul style="list-style-type: none"> • cos : IEEE 802.1Q/ISL サービスクラスまたはユーザープライオリティを設定します。 • dscp : IP (v4) および IPv6 パケットの DSCP を設定します。 • ip : IP 固有の値を設定します。 • precedence : IP (v4) および IPv6 パケットの precedence を設定します。 • qos-group : QoS グループを設定します。 <p>この例では、set dscp コマンドが AF23 (010010) の DSCP 値にパケットを照合することによって、IP トラフィックを分類します。</p>
ステップ 8	<p>exit</p> <p>例 :</p> <pre>Device(config-pmap-c)# exit</pre>	<p>ポリシーマップコンフィギュレーションモードに戻ります。</p>
ステップ 9	<p>exit</p> <p>例 :</p> <pre>Device(config-pmap)# exit</pre>	<p>グローバルコンフィギュレーションモードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 10	interface <i>interface-id</i> 例 : Device(config)# interface gigabitethernet 1/0/3	ポリシーマップを適用するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 11	service-policy input <i>policy-map-name</i> 例 : Device(config-if)# service-policy input policy_vlan100	ポリシーマップ名を指定し、入力ポートに適用します。サポートされるポリシーマップは、入力ポートに1つだけです。
ステップ 12	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 13	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] 例 : Device# show policy-map	(任意) 入力を確認します。
ステップ 14	copy running-config startup-config 例 : Device# copy-running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

テーブル マップの設定

テーブルマップはマーキングの形式であり、テーブルを使用してフィールド間のマッピングと変換を可能にすることもできます。たとえば、テーブルマップはレイヤ 2 の CoS 設定をレイヤ 3 の precedence 値にマッピングして変換するために使用できます。



- (注)
- テーブルマップは、複数のポリシーで、または同じポリシー内で複数回参照できます。
 - デフォルトのクラスマップでカスタム出力ポリシー用に設定されたテーブルマップは、トラフィックが分類されるクラスマップに関係なく、すべての DSCP トラフィックに影響します。回避策は、テーブルマップを削除し、デフォルトクラスで **set dscp** コマンドを設定して、分類されたトラフィックの DSCP マーキングを変更することです。ユーザー定義クラスに非キューイングアクション（ポリサーまたはマーキング）がある場合、パケットはそのユーザー定義クラス自体の値またはコメントを保持します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	table-map name {default {default value copy ignore} exit map {from from value to to value } no} 例 : Device (config)# table-map table01 Device (config-tablemap)#	テーブルマップを作成し、テーブルマップコンフィギュレーションモードを開始します。テーブルマップコンフィギュレーションモードでは、次のタスクを実行できます。 <ul style="list-style-type: none"> • default : テーブルマップのデフォルト値を設定するか、テーブルマップ内にない値についてのデフォルトの動作（コピーまたは無視）を設定します。 • exit : テーブルマップコンフィギュレーションモードを終了します。 • map : テーブルマップで <i>from</i> 値を <i>to</i> 値にマッピングします。 • no : コマンドのデフォルト値を無効にするか、設定します。
ステップ 3	map from value to value 例 : Device (config-tablemap)# map from 0 to 2	この手順では、DSCP 値が 0 のパケットを CoS 値 2 に、DSCP 値が 1 のパケットを CoS 値 4 に、DSCP 値が 24 のパケットを CoS 値 3 に、DSCP 値が 40 のパケットを CoS 値 6 に、およびそれ

	コマンドまたはアクション	目的
	<pre>Device(config-tablemap) # map from 1 to 4 Device(config-tablemap) # map from 24 to 3 Device(config-tablemap) # map from 40 to 6 Device(config-tablemap) # default 0 Device(config-tablemap) #</pre>	<p>以外のすべてのパケットを CoS 値 0 にマークします。</p> <p>(注) この例の CoS 値から DSCP 値へのマッピングは、後で説明するように、set ポリシーマップクラス コンフィギュレーションコマンドを使用して設定します。</p>
ステップ 4	<p>exit</p> <p>例 :</p> <pre>Device(config-tablemap) # exit Device(config) #</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	<p>exit</p> <p>例 :</p> <pre>Device(config) exit Device#</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show table-map</p> <p>例 :</p> <pre>Device# show table-map Table Map table01 from 0 to 2 from 1 to 4 from 24 to 3 from 40 to 6 default 0</pre>	テーブル マップ設定を表示します。
ステップ 7	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal Device(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 8	<p>policy-map</p> <p>例 :</p> <pre>Device(config) # policy-map table-policy Device(config-pmap) #</pre>	テーブルマップのポリシーマップを設定します。

	コマンドまたはアクション	目的
ステップ 9	class class-default 例 : Device (config-pmap) # class class-default Device (config-pmap-c) #	クラスをシステムデフォルトに一致させます。
ステップ 10	set cos dscp table table map name 例 : Device (config-pmap-c) # set cos dscp table table01 Device (config-pmap-c) #	このポリシーが入力ポートに適用された場合、そのポートでは trust dscp がイネーブルになり、テーブルマップに応じてマーキングが行われます。
ステップ 11	end 例 : Device (config-pmap-c) # end Device #	特権 EXEC モードに戻ります。

次のタスク

ネットワークの QoS 用の追加のポリシーマップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用してトラフィックポリシーをインターフェイスに付加します。

QoS の特性と機能の設定

帯域幅の設定

この手順は、デバイスで帯域幅を設定する方法を説明しています。

始める前に

この手順を開始する前に、帯域幅のクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 2	policy-map <i>policy name</i> 例 : Device(config)# policy-map policy_bandwidth01 Device(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class <i>class name</i> 例 : Device(config-pmap)# class class_bandwidth01 Device(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 <ul style="list-style-type: none"> • word : クラスマップ名。 • class-default : 未分類のパケットを照合するシステムデフォルトクラス。
ステップ 4	bandwidth {<i>Kb/s</i> percent <i>percentage</i> remaining { ratio <i>ratio</i> }} 例 : Device(config-pmap-c)# bandwidth 200000 Device(config-pmap-c)#	ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。 <ul style="list-style-type: none"> • Kb/s : 特定の値を kbps で設定します (100 ~ 100000000) 。 • percent : 割合に基づいて、特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。 • remaining : 特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることは

	コマンドまたはアクション	目的
		<p>できません。このコマンドは、ポリシー内の特定のキューに対して priority コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は0～100の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100を超えることができます。</p> <p>(注) ポリシー マップで帯域幅タイプを混在させることはできません。たとえば、1つのポリシー マップで帯域幅の割合と kbps の両方を使用して、帯域幅を設定することはできません。</p>
ステップ 5	end 例 : <pre>Device(config-pmap-c)# end Device#</pre>	設定変更を保存します。
ステップ 6	show policy-map 例 : <pre>Device# show policy-map</pre>	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークのQoS用の追加のポリシーマップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用して、インターフェイスにトラフィックポリシーを付加します。

ポリシングの設定

この手順は、デバイスでポリシングを設定する方法を説明しています。

始める前に

この手順を開始する前に、ポリシングのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map <i>policy name</i> 例 : Device(config)# policy-map policy_police01 Device(config-pmap) #	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class <i>class name</i> 例 : Device(config-pmap) # class class_police01 Device(config-pmap-c) #	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 <ul style="list-style-type: none"> • word : クラス マップ名。 • class-default : 未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	police {<i>target_bit_rate</i> [<i>burst bytes</i> bc conform-action pir] cir {<i>target_bit_rate</i> percent percentage} rate {<i>target_bit_rate</i> percent percentage} conform-action transmit exceed-action {drop [violate action] set-cos-transmit set-dscp-transmit set-prec-transmit transmit [violate action] } } 例 : Device(config-pmap-c) # police 8000 conform-action transmit exceed-action drop Device(config-pmap-c) #	次の police サブコマンドオプションを使用できます。 <ul style="list-style-type: none"> • target_bit_rate : ビット/秒 (8000 ~ 10000000000) 。 • burst bytes : 1000 ~ 512000000 の値を入力します。 • bc : 適合バースト。 • conform-action : レートが適合バーストより小さくなる場合に実行されるアクション。 • pir : 最大情報レート。 • cir : 認定情報レート。 • target_bit_rate : ターゲット ビット レート (8000 ~ 10000000000) 。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • percent : CIR のインターフェイス帯域幅の割合。 • rate : ポリシングレート、階層型ポリシーの PCR、またはシングルレベルの ATM 4.0 ポリサー ポリシーの SCR を指定します。 • target_bit_rate : ターゲットビットレート (8000 ~ 10000000000) 。 • percent : レートのインターフェイス帯域幅の割合。 <p>次の police conform-action transmit exceed-action サブコマンドオプションを使用できます。</p> <ul style="list-style-type: none"> • drop : パケットをドロップします。 • set-cos-transmit : CoS 値を設定して送信します。 • set-dscp-transmit : DSCP 値を設定して送信します。 • set-prec-transmit : パケットの precedence を書き換えて送信します。 • transmit : パケットを送信します。 <p>(注) ポリサー ベースのマークダウン アクションは、テーブル マップを使用する場合のみサポートされます。デバイスの各マーキングフィールドで許可されているマークダウンテーブルマップは 1 つだけです。</p>
ステップ 5	end 例 : Device(config-pmap-c) # end	設定変更を保存します。

	コマンドまたはアクション	目的
	Device#	
ステップ 6	show policy-map 例 : Device# show policy-map	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。 (注) show policy-map コマンドの出力では、適合バイトおよび超過バイトのカウンタを表示しません。

次のタスク

ネットワークの QoS 用の追加のポリシーマップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用してトラフィックポリシーをインターフェイスに付加します。

プライオリティの設定

この手順は、デバイスでプライオリティを設定する方法を説明しています。



- (注) デバイスでは、指定されたキューにプライオリティを指定できます。使用可能な2つのプライオリティ レベルがあります (1 および 2)。音声とビデオに対応するキューには、プライオリティ レベル 1 を割り当てます。

始める前に

この手順を開始する前に、プライオリティのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map policy name 例 : Device(config)# policy-map policy_priority01	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成

	コマンドまたはアクション	目的
	Device (config-pmap) #	または修正し、サービス ポリシーを指定します。
ステップ 3	<p>class class name</p> <p>例 :</p> <pre>Device (config-pmap) # class class_priority01 Device (config-pmap-c) #</pre>	<p>ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。</p> <ul style="list-style-type: none"> • word : クラス マップ 名。 • class-default : 未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	<p>priority [Kb/s [burst_in_bytes] level level_value [Kb/s [burst_in_bytes] percent percentage [burst_in_bytes]] percent percentage [burst_in_bytes]]</p> <p>例 :</p> <pre>Device (config-pmap-c) # priority level 1 Device (config-pmap-c) #</pre>	<p>(任意) priority コマンドは、クラスに完全スケジューリング プライオリティを割り当てます。</p> <p>コマンドオプションは次のとおりです。</p> <ul style="list-style-type: none"> • Kb/s : kbps を指定します (1 ~ 2000000) 。 • burst_in_bytes : バイトでバーストを指定します (32 ~ 2000000) 。 • level level_value : マルチレベル (1 ~ 2) のプライオリティキューを指定します。 • Kb/s : kbps を指定します (1 ~ 2000000) 。 • burst_in_bytes : バイトでバーストを指定します (32 ~ 2000000) 。 • percent : 総帯域幅の割合。 • burst_in_bytes : バイトでバーストを指定します (32 ~ 2000000) 。 • percent : 総帯域幅の割合。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>burst_in_bytes</i> : バイトでバーストを指定します (32 ~ 2000000)。 <p>(注) プライオリティ レベル 1 はプライオリティ レベル 2 より重要です。プライオリティ レベル 1 は、QoS に最初に処理される帯域幅を予約するため、遅延は非常に低くなります。プライオリティ レベル 1 と 2 はどちらも帯域幅を予約します。</p>
ステップ 5	end 例 : Device(config-pmap-c) # end Device#	設定変更を保存します。
ステップ 6	show policy-map 例 : Device# show policy-map	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシーマップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用してトラフィックポリシーをインターフェイスに付加します。

SGT ベースの QoS の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	class-map <i>class-map-name</i> { match-any match-all } 例 : Device (config) # class-map c1	クラスマップを指定し、クラスマップコンフィギュレーションモードを開始します。
ステップ 3	match security-group source tag <i>sgt-number</i> 例 : Device (config-cmap) # match security-group source tag 1000	security-group source security tag の値を設定します。
ステップ 4	match security-group destination tag <i>dgt-number</i> 例 : Device (config-cmap) # match security-group destination tag 2000	security-group destination security tag の値を設定します。
ステップ 5	exit 例 : Device (config-cmap) # exit Device#	ルート マップ インターフェイス コンフィギュレーション モードを終了して、グローバルコンフィギュレーションモードに戻ります。
ステップ 6	policy-map <i>policy-map-name</i> 例 : Device (config) # policy-map pin Device (config-pmap) #	<p>ポリシー マップを指定し、ポリシー マップコンフィギュレーションモードを開始します。</p> <p><i>policy-map-name</i> は子ポリシーマップの名前です。名前には最大 40 文字までの英数字を指定できます。</p>
ステップ 7	class <i>class-name</i> 例 : Device (config-pmap) # class c1 Device (config-pmap-c) #	<p>ポリシー クラス マップ コンフィギュレーションモードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシークラスマップコンフィギュレーションモードには、次のコマンドオプションが含まれます。</p> <ul style="list-style-type: none"> • word : クラス マップ名。 • class-default : 未分類のパケットを照合するシステムデフォルトクラス。

	コマンドまたはアクション	目的
ステップ 8	set dscp dscp-value 例： Device(config-pmap-c)# set dscp af11	DiffServ コードポイント (DSCP) 値を設定します。
ステップ 9	end 例： Device(config-pmap-c)# end Device#	設定変更を保存します。クラスマップコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 10	interface interface-num 例： Device(config)# interface GigabitEthernet1/0/24	インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 11	service-policy { input output } policy-map-name 例： Device(config-if)# service-policy input pin	インターフェイスの入力にポリシーマップを割り当てます。
ステップ 12	end 例： Device(config-if)# end Device#	設定変更を保存します。インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに入ります。

SGT ベースの QoS 分類の設定例

次に、インターフェイスでの SGT ベースの QoS の設定例を示します。

```
ip access-list role-based sgt_acl
 10 permit ip
cts role-based sgt-map 24.0.0.0/8 sgt 24
cts role-based enforcement
cts role-based permissions from 24 to 24 sgt_acl

class-map match-all c1
 match protocol attribute business-relevance business-relevant
 match protocol attribute traffic-class ops-admin-mgmt
 match security-group destination tag 24
 match security-group source tag 24

policy-map pin
 class c1
  set dscp af11
 class class-default
  set dscp af12
```

```
interface GigabitEthernet1/0/24
no switchport
ip address 24.1.1.2 255.255.255.0
service-policy input pin
ip nbar protocol-discovery
```

キューとシェーピングの設定

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さによっては、この項の手順をすべて実行する必要があります。次の特性を決定する必要があります。

- DSCP、CoS、または QoS グループ値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューに適用されるドロップ割合のしきい値と、トラフィックタイプで必要な予約メモリと最大メモリ
- キューに割り当てる固定バッファ スペース
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）



(注) 出力キューはデバイスでのみ設定できます。

キューバッファの設定

デバイスでは、キューにバッファを割り当てることができます。バッファが割り当てられていない場合は、すべてのキューに対して均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトで DTS (Dynamic Threshold and Scaling) はすべてのキューでアクティブになるため、これらはソフトバッファになります。



(注) queue-buffer ratio は queue-limit とともに設定することはできません。

始める前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キューバッファのクラス マップを作成する必要があります。

- キューバッファを設定する前に、ポリシー マップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map policy name 例 : Device(config)# policy-map policy_queuebuffer01 Device(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class class name 例 : Device(config-pmap)# class class_queuebuffer01 Device(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 <ul style="list-style-type: none"> • word : クラス マップ名。 • class-default : 未分類の packets を照合するシステム デフォルト クラス。
ステップ 4	bandwidth {Kb/s percent percentage remaining { ratio ratio value }} 例 : Device(config-pmap-c)# bandwidth percent 80 Device(config-pmap-c)#	ポリシーマップの帯域幅を設定します。コマンドパラメータは次のとおりです。 <ul style="list-style-type: none"> • Kb/s : 特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ~ 100000000 です。 • percent : 割合を使用して特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100% を超えることはできません。100%未満の場合、帯域幅の残りは、すべての

	コマンドまたはアクション	目的
		<p>帯域幅キュー上に均等に分割されます。</p> <ul style="list-style-type: none"> • remaining : 特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクリプすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して priority コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ~ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 <p>(注) ポリシー マップで帯域幅タイプを混在させることはできません。</p>
ステップ 5	<p>queue-buffers { ratio ratio value}</p> <p>例 :</p> <pre>Device(config-pmap-c) # queue-buffers ratio 10 Device(config-pmap-c) #</pre>	<p>キューの相対的なバッファ サイズを設定します。</p> <p>(注) ポリシーに設定されているすべてのバッファの合計が 100 % 以下である必要があります。未割り当てバッファは、残りのキューに均等に分散されます。プライオリティ キューを含むすべてのキューに十分なバッファが割り当てられるようにします。</p>

	コマンドまたはアクション	目的
		(注) スパニングツリーや LACP などのネットワーク制御プロトコルのプロトコルデータユニット (PDU) は、プライオリティ キューまたはキュー 0 (プライオリティ キューが設定されていない場合) を使用します。プロトコルが機能するには、これらのキューに十分なバッファが割り当てられるようにします。
ステップ 6	end 例 : Device(config-pmap-c)# end Device#	設定変更を保存します。
ステップ 7	show policy-map 例 : Device# show policy-map	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシーマップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用してトラフィックポリシーをインターフェイスに付加します。

キュー制限の設定

重み付けテールドロップ (WTD) を設定するためにキュー制限を使用します。WTD を使用すると、キューごとに複数のしきい値を設定できます。各サービスクラスが異なるしきい値でドロップされて QoS 差別化が実現されます。デバイスによって、3 つの明示的にプログラム可能なしきい値クラスとして各キューに 0、1、2 を指定できます。したがって、キューごとに各パケットのキューイング/ドロップの決定は、フレーム ヘッダーの DSCP、CoS、または QoS グループフィールドに指定されたパケットのしきい値クラスの割り当てによって決定されます。

WTD では柔軟な制限が使用されるため、最大 400 % (共通プールで予約されるバッファの最大 4 倍) のキュー制限を設定できます。この柔軟な制限は、他の機能に影響することなく、共通プールのオーバーランを防止します。



(注) キュー制限は、有線ポートのデバイスの出力キューでのみ設定できます。

始める前に

この手順の前提条件を次に示します。

- この手順を開始する前に、キュー制限を使用するクラス マップを作成する必要があります。
- キュー制限を設定する前に、ポリシーマップの帯域幅、シェーピング、またはプライオリティを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map policy name 例 : Device(config)# policy-map policy_queue_limit01 Device(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class class name 例 : Device(config-pmap)# class class_queue_limit01 Device(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 <ul style="list-style-type: none"> • word : クラス マップ名。 • class-default : 未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	bandwidth {Kb/s percent percentage remaining {ratio ratio value}} 例 :	ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。

	コマンドまたはアクション	目的
	<pre>Device(config-pmap-c) # bandwidth 500000 Device(config-pmap-c) #</pre>	<p>目的</p> <ul style="list-style-type: none"> • Kb/s : 特定の値を設定するには、このコマンドを使用します。指定できる範囲は 20000 ~ 100000000 です。 • percent : 特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100%未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。 • remaining : 特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して priority コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率は 0 ~ 100 の範囲で指定できます。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 <p>(注) ポリシー マップで帯域幅タイプを混在させることはできません。</p>
ステップ 5	<pre>queue-limit {<i>packets</i> packets cos {<i>cos value</i> { <i>maximum threshold value</i> percent percentage } values {<i>cos value</i> percent percentage } } dscp {<i>dscp value</i> {<i>maximum threshold value</i> percent percentage } <i>match packet</i> {<i>maximum threshold value</i> percent percentage } default {<i>maximum threshold value</i> percent percentage } ef {<i>maximum threshold value</i> percent</pre>	<p>キュー制限のしきい値の割合を設定します。</p> <p>すべてのキューで、3つのしきい値 (0、1、2) があり、それぞれのしきい値についてデフォルト値があります。デフォルトまたはその他のキュー制限しきい値設定を変更するには、このコマンドを使用します。たとえば、DSCP 3、4、および</p>

	コマンドまたはアクション	目的
	<pre>percentage} dscp values dscp value} percent percentage }}</pre> <p>例 :</p> <pre>Device (config-pmap-c) # queue-limit dscp 3 percent 20 Device (config-pmap-c) # queue-limit dscp 4 percent 30 Device (config-pmap-c) # queue-limit dscp 5 percent 40</pre>	<p>5 のパケットが設定した特定のキューに送信される場合、このコマンドは、この 3 つの DSCP 値のしきい値パーセンテージを設定できます。キュー制限しきい値に関する詳細については、重み付けテーブルドロップ (64 ページ) を参照してください。</p> <p>(注) デバイスは絶対キュー制限の割合をサポートしません。デバイスは、DSCP または CoS キュー制限の割合だけをサポートします。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device (config-pmap-c) # end Device#</pre>	設定変更を保存します。
ステップ 7	<p>show policy-map</p> <p>例 :</p> <pre>Device# show policy-map</pre>	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加ポリシー マップを設定します。ポリシーマップを作成したら、**service-policy** コマンドを使用して、トラフィックポリシーをインターフェイスに付加します。

シェーピングの設定

特定のクラスのシェーピング (最大帯域幅) を設定するには、**shape** コマンドを使用します。ポートに残っている追加帯域幅があっても、キューの帯域幅はこの値に制限されます。シェーピングは平均の割合で、または bps のシェーピングの平均値で設定できます。

始める前に

この手順を開始する前に、シェーピングのクラス マップを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map policy name 例 : Device(config)# policy-map policy_shaping01 Device(config-pmap)#	ポリシー マップ コンフィギュレーション モードを開始します。 1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class class name 例 : Device(config-pmap)# class class_shaping01 Device(config-pmap-c)#	ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。 <ul style="list-style-type: none"> • word : クラス マップ名。 • class-default : 未分類の packets を照合するシステム デフォルト クラス。
ステップ 4	shape average {target bit rate percent percentage} 例 : Device(config-pmap-c)# shape average percent 50 Device(config-pmap-c)#	平均シェーピング レートを設定します。平均シェーピング レートを、ターゲット ビット レート (bps) または認定情報 レート (CIR) のインターフェイス帯域幅の割合で設定できます。
ステップ 5	end 例 : Device(config-pmap-c)# end Device#	設定変更を保存します。

	コマンドまたはアクション	目的
ステップ 6	show policy-map 例 : Device# show policy-map	(任意) すべてのサービス ポリシーに設定されたすべてのクラスに関するポリシー設定情報を表示します。

次のタスク

ネットワークの QoS 用の追加のポリシー マップを設定します。ポリシー マップを作成したら、**service-policy** コマンドを使用してトラフィック ポリシーをインターフェイスに付加します。

シャープ プロファイル キューイングの設定

この手順は、スイッチでシャープ プロファイル キューイングを設定する方法を説明しています。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	policy-map policy name 例 : Device(config)# policy-map policy_shaping01 Device(config-pmap)#	<p>ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>1つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。</p> <p><i>policy-map-name</i> は子ポリシーマップの名前です。名前には最大 40 文字までの英数字を指定できます。</p>
ステップ 3	class class name 例 : Device(config-pmap)# class class_shaping01 Device(config-pmap-c)#	<p>ポリシー クラス マップ コンフィギュレーション モードを開始します。ポリシーを作成または変更するクラスの名前を指定します。ポリシー クラス マップ コンフィギュレーション モードには、次のコマンドオプションが含まれます。</p> <ul style="list-style-type: none"> • <i>word</i> : クラス マップ名。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • class-default : 未分類のパケットを照合するシステム デフォルト クラス。
ステップ 4	bandwidth { <i>Kb/s</i> percent <i>percentage</i> remaining { ratio <i>ratio value</i> }} 例 : Device (config-pmap-c) # bandwidth 200000 Device (config-pmap-c) #	<p>ポリシーマップの帯域幅を設定します。パラメータは次のとおりです。</p> <ul style="list-style-type: none"> • Kb/s : 特定の値を kbps で設定します (100 ~ 100000000) 。 • percent- : 割合に基づいて、特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。100 % 未満の場合、帯域幅の残りは、すべての帯域幅キュー上に均等に分割されます。 • remaining : 特定のクラスに最小帯域幅を割り当てます。キューは、他のキューが全体のポート帯域幅を使用しない場合は、帯域幅をオーバーサブスクライブすることができます。合計が 100 % を超えることはできません。このコマンドは、ポリシー内の特定のキューに対して priority コマンドが使用されている場合に使用します。各キューには、割合ではなく比率を割り当てることもできます。キューにはそれらの比率に従って、特定の重みが割り当てられます。比率の範囲は 1 ~ 65536 です。この場合のポリシーの全帯域幅での比率の割り当ては、100 を超えることができます。 <p>(注) ポリシー マップで帯域幅タイプを混在させることはできません。</p>

	コマンドまたはアクション	目的
ステップ 5	shape average { <i>target bit rate</i> percent <i>percentage</i> } 例 : Device(config-pmap-c) # shape average percent 50 Device(config-pmap-c) #	平均シェーピングレートを設定します。平均シェーピングレートを、ターゲットビットレート (bps) または認定情報レート (CIR) のインターフェイス帯域幅の割合で設定できます。
ステップ 6	end 例 : Device(config-pmap-c) # end Device#	設定変更を保存します。

シャープ プロファイル キューイングの設定

次に、シャープキューイングの例を示します。

```

Policy Map test
  Class test1
    bandwidth 20 (%)
    Average Rate Traffic Shaping
    cir 40%
  Class test3
    Average Rate Traffic Shaping
    cir 50%
  Class test2
    Average Rate Traffic Shaping
    cir 50%
  Class test4
    bandwidth 20 (%)
  Class test5
    Average Rate Traffic Shaping
    cir 70%
  Class test6
    Average Rate Traffic Shaping
    cir 60%

```

QoS のモニタリング

デバイスでの QoS のモニタリングには、次のコマンドを使用できます。

表 11: QoS のモニタリング

コマンド	説明
show class-map [<i>class_map_name</i>]	設定されているすべてのクラスマップのリストを表示します。

コマンド	説明
show policy-map [<i>policy_map_name</i>]	設定されているすべてのポリシーマップのリストを表示します。コマンドパラメータは次のとおりです。 <ul style="list-style-type: none"> • policy map name • interface • session
show policy-map session [<i>input</i> <i>output</i> <i>uid UUID</i>]	セッションの QoS ポリシーを表示します。コマンドパラメータは次のとおりです。 <ul style="list-style-type: none"> • input : 入力ポリシー • output : 出力ポリシー • uid : SSS 固有の ID に基づくポリシー
show table-map	すべてのテーブルマップと設定を表示します。

QoS の設定例

例 : TCP プロトコル分類

TCP パケットは、ポート番号に基づいて分類できます。TCP プロトコルの設定は次のとおりです。

```
Device#show ip acce tcp
Extended IP access list tcp
  10 permit tcp any any eq 80
Device #
Device #show run class-map tcp

Current configuration : 63 bytes
!
class-map match-all tcp
  match access-group name tcp
!
end
Device #
Device #show run policy-map tcp

Current configuration : 56 bytes
!
policy-map tcp
```

```
class tcp
  police 1000000000
!
end
Device #

Device #show run int tw 1/0/1

Current configuration : 93 bytes
!
interface TwentyFiveGigE1/0/1
  no ip address
  no keepalive
  service-policy output tcp
end

Device #
```

例 : UDP プロトコル分類

UDP パケットは、ポート番号に基づいて分類できます。UDP プロトコルの設定例は次のとおりです。

```
Device#show ip acce udp
Extended IP access list udp
  10 permit udp any any eq ntp
Device #

Device #show run class-map udp
Building configuration...

Current configuration : 63 bytes
!
class-map match-all udp
  match access-group name udp
!
end

Device #
Device #show run policy-map udp
Building configuration...

Current configuration : 56 bytes
!
policy-map udp
  class udp
    police 1000000000
!
end
Device #
Device #show run int tw 1/0/1

Current configuration : 93 bytes
!
interface TwentyFiveGigE1/0/1
  no ip address
  no keepalive
  service-policy output udp
end

Device #
```

例 : RTP プロトコル分類

RTP パケットは、ポート番号に基づいて分類できます。RTP プロトコルの設定例は次のとおりです。

```
Device# show ip access-list rtp
Extended IP access list rtp
  10 permit udp any any eq 554
  11 permit tcp any any eq 554
Device #
```

```
Device #show run class-map rtp

Current configuration : 63 bytes
!
class-map match-all rtp
  match access-group name rtp
!
end
```

```
Device #
Device #show run policy-map rtp

Current configuration : 56 bytes
!
policy-map rtp
  class rtp
    police 1000000000
!
end
```

```
Device #
Device #show run int tw 1/0/1

Current configuration : 93 bytes
!
interface TwentyFiveGigE1/0/1
  no ip address
  no keepalive
  service-policy output rtp
end
```

```
Device #
```

例 : アクセスコントロールリストによる分類

この例は、アクセスコントロールリスト (ACL) を使用して QoS のパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
Device(config)# class-map acl-101
Device(config-cmap)# description match on access-list 101
Device(config-cmap)# match access-group 101
Device(config-cmap)#
```

ACL を使用してクラスマップを作成した後で、クラスのポリシーマップを作成し、ポリシーマップを QoS のインターフェイスに適用します。

例：サービス クラス レイヤ2の分類

この例は、サービス クラス レイヤ2の分類を使用して QoS に対してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map cos
Device(config-cmap)# match cos ?
<0-7> Enter up to 4 class-of-service values separated by white-spaces
Device(config-cmap)# match cos 3 4 5
Device(config-cmap)#
```

CoS レイヤ2の分類を使用してクラス マップを作成したら、そのクラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：サービス クラス DSCP の分類

この例は、サービス クラス DSCP の分類を使用して、QoS に対してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map dscp
Device(config-cmap)# match dscp af21 af22 af23
Device(config-cmap)#
```

DSCP 分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：VLAN ID レイヤ2の分類

この例は、VLAN ID レイヤ2の分類を使用して QoS に分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map vlan-120
Device(config-cmap)# match vlan ?
<1-4095> VLAN id
Device(config-cmap)# match vlan 120
Device(config-cmap)#
```

VLAN レイヤ2の分類を使用してクラス マップを作成したら、クラスのポリシー マップを作成し、QoS のインターフェイスにポリシー マップを適用します。

例：DSCP 値または precedence 値による分類

この例は、DSCP 値または precedence 値を使用してパケットを分類する方法を示しています。

```
Device# configure terminal
Device(config)# class-map prec2
```

```

Device(config-cmap)# description matching precedence 2 packets
Device(config-cmap)# match ip precedence 2
Device(config-cmap)# exit
Device(config)# class-map ef
Device(config-cmap)# description EF traffic
Device(config-cmap)# match ip dscp ef
Device(config-cmap)#

```

DSCP 値または precedence 値を使用してクラスマップを作成したら、クラスのポリシーマップを作成し、QoS のインターフェイスにポリシーマップを適用します。

例：階層型分類

次の例は、child という名前の別のクラスに一致する parent という名前のクラスが作成される、階層型分類を示しています。child という名前のクラスは、2 に設定された IP precedence に基づいて照合されます。

```

Device# configure terminal
Device(config)# class-map child
Device(config-cmap)# match ip precedence 2
Device(config-cmap)# exit
Device(config)# class-map parent
Device(config-cmap)# match class child
Device(config-cmap)#

```

親クラスマップを作成したら、クラスのポリシーマップを作成し、QoS のインターフェイスにポリシーマップを適用します。

例：階層型ポリシーの設定

次の例は、階層型ポリシーを使用した設定を示しています。

```

Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# match dscp 30
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# match precedence 4
Device(config-cmap)# exit

Device(config)# class-map c3
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000

```

```
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

次の例は、テーブル マップを使用した階層型ポリシーを示しています。

```
Device(config)# table-map dscp2dscp
Device(config-tablemap)# default copy
Device(config)# policy-map ssid_child_policy
Device(config-pmap)# class voice
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 15000000
Device(config-pmap)# class video
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 10000000
Device(config)# policy-map ssid_policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 30000000
Device(config-pmap-c)# queue-buffer ratio 0
Device(config-pmap-c)# set dscp dscp table dscp2dscp
Device(config-pmap-c)# service-policy ssid_child_policy
```

例：音声およびビデオの分類

この例は、デバイス固有の情報を使用して、音声とビデオのパケットストリームを分類する方法を示しています。

この例では、音声とビデオがエンドポイント A からデバイスの GigabitEthernet1/0/1 に送信され、それぞれ precedence 値 5 と 6 を持ちます。また、音声とビデオは、エンドポイント B からデバイスの FortyGigabitEthernet1/0/2 にそれぞれ DSCP 値 EF と AF11 で送信されます。

両方のインターフェイスからのすべてのパケットがアップリンク インターフェイスに送信されます。その場合、音声は 100 Mbps にポリシングし、ビデオは 150 Mbps にポリシングする必要があります。

上記の要件ごとに分類するために、GigabitEthernet1/0/1 で送信される音声パケットに一致するクラスが作成されます。これには、precedence 5 に一致する voice-interface-1 という名前が付けられます。同様に、GigabitEthernet1/0/2 の音声パケットに一致する、voice-interface-2 という名前の音声用の別のクラスが作成されます。これらのクラスは、GigabitEthernet1/0/1 に接続される input-interface-1 と、GigabitEthernet1/0/2 に接続される input-interface-2 という 2 つの別個のポリシーに関連付けられます。このクラスのアクションは、qos-group に 10 とマーキングすることです。出力インターフェイスで QoS-group 10 のパケットを照合するために、QoS-group 10 で一致する voice という名前のクラスが作成されます。これは、output-interface という名前の別のポリシーに関連付けられ、アップリンク インターフェイスに関連付けられます。ビデオも同じ方法で処理されますが、QoS-group 20 で一致します。

例：平均レート シェーピングの設定

次の例は、上記のデバイス固有の情報を使用して分類する方法を示しています。

```

Device(config)#
Device(config)# class-map voice-interface-1
Device(config-cmap)# match ip precedence 5
Device(config-cmap)# exit

Device(config)# class-map video-interface-1
Device(config-cmap)# match ip precedence 6
Device(config-cmap)# exit

Device(config)# class-map voice-interface-2
Device(config-cmap)# match ip dscp ef
Device(config-cmap)# exit

Device(config)# class-map video-interface-2
Device(config-cmap)# match ip dscp af11
Device(config-cmap)# exit

Device(config)# policy-map input-interface-1
Device(config-pmap)# class voice-interface-1
Device(config-pmap-c)# set qos-group 10
Device(config-pmap-c)# exit

Device(config-pmap)# class video-interface-1
Device(config-pmap-c)# set qos-group 20

Device(config-pmap-c)# policy-map input-interface-2
Device(config-pmap)# class voice-interface-2
Device(config-pmap-c)# set qos-group 10
Device(config-pmap-c)# class video-interface-2
Device(config-pmap-c)# set qos-group 20
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# class-map voice
Device(config-cmap)# match qos-group 10
Device(config-cmap)# exit

Device(config)# class-map video
Device(config-cmap)# match qos-group 20
Device(config)# policy-map output-interface
Device(config-pmap)# class voice
Device(config-pmap-c)# police 256000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class video
Device(config-pmap-c)# police 1024000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

```

例：平均レート シェーピングの設定

次の例は、平均レート シェーピングを設定する方法を示しています。

```

Device# configure terminal
Device(config)# class-map prec1

```



```
Device(config-cmap) # description matching precedence 1 packets
Device(config-cmap) # match ip precedence 1
Device(config-cmap) # end

Device# configure terminal
Device(config) # class-map prec2
Device(config-cmap) # description matching precedence 2 packets
Device(config-cmap) # match ip precedence 2
Device(config-cmap) # exit

Device(config) # policy-map shaper
Device(config-pmap) # class prec1
Device(config-pmap-c) # shape average 512000
Device(config-pmap-c) # exit

Device(config-pmap) # policy-map shaper
Device(config-pmap) # class prec2
Device(config-pmap-c) # shape average 512000
Device(config-pmap-c) # exit

Device(config-pmap) # class class-default
Device(config-pmap-c) # shape average 1024000
```

クラス マップ、ポリシー マップ、シェーピング平均を設定したら、QoS のインターフェイスにポリシー マップを適用します。

例：キュー制限の設定

次の例は、DSCP 値および割合に基づいて、キュー制限ポリシーを設定する方法を示しています。

```
Device# configure terminal
Device#(config) # policy-map port-queue
Device#(config-pmap) # class dscp-1-2-3
Device#(config-pmap-c) # bandwidth percent 20
Device#(config-pmap-c) # queue-limit dscp 1 percent 80
Device#(config-pmap-c) # queue-limit dscp 2 percent 90
Device#(config-pmap-c) # queue-limit dscp 3 percent 100
Device#(config-pmap-c) # exit

Device#(config-pmap) # class dscp-4-5-6
Device#(config-pmap-c) # bandwidth percent 20
Device#(config-pmap-c) # queue-limit dscp 4 percent 20
Device#(config-pmap-c) # queue-limit dscp 5 percent 30
Device#(config-pmap-c) # queue-limit dscp 6 percent 20
Device#(config-pmap-c) # exit

Device#(config-pmap) # class dscp-7-8-9
Device#(config-pmap-c) # bandwidth percent 20
Device#(config-pmap-c) # queue-limit dscp 7 percent 20
Device#(config-pmap-c) # queue-limit dscp 8 percent 30
Device#(config-pmap-c) # queue-limit dscp 9 percent 20
Device#(config-pmap-c) # exit

Device#(config-pmap) # class dscp-10-11-12
Device#(config-pmap-c) # bandwidth percent 20
Device#(config-pmap-c) # queue-limit dscp 10 percent 20
Device#(config-pmap-c) # queue-limit dscp 11 percent 30
```

例：キューバッファの設定

```

Device# (config-pmap-c) # queue-limit dscp 12 percent 20
Device# (config-pmap-c) # exit

Device# (config-pmap) # class dscp-13-14-15
Device# (config-pmap-c) # bandwidth percent 10
Device# (config-pmap-c) # queue-limit dscp 13 percent 20
Device# (config-pmap-c) # queue-limit dscp 14 percent 30
Device# (config-pmap-c) # queue-limit dscp 15 percent 20
Device# (config-pmap-c) # end
Device#

```

上記のポリシーマップのキュー制限の設定が終了すると、QoSのインターフェイスにポリシーマップを適用することができます。

例：キューバッファの設定

次の例は、キューバッファポリシーを設定してQoSのインターフェイスに適用する方法を示しています。

```

Device# configure terminal
Device(config)# policy-map policy1001
Device(config-pmap)# class class1001
Device(config-pmap-c)# bandwidth remaining ratio 10
Device(config-pmap-c)# queue-buffer ratio ?
<0-100> Queue-buffers ratio limit
Device(config-pmap-c)# queue-buffer ratio 20
Device(config-pmap-c)# end

Device# configure terminal
Device(config)# interface HundredGigabitE1/0/3
Device(config-if)# service-policy output policy1001
Device(config-if)# end

```

例：ポリシングアクションの設定

次の例は、ポリサーに関連付けることができるさまざまなポリシングアクションを示しています。これらのアクションは、パケット設定の適合、超過、または違反によって実現されます。トラフィックプロファイルを超過または違反したパケットをドロップ、マーク付け、または送信することができます。

たとえば、1つの一般的な導入シナリオでは、エンタープライズ顧客ポリシートラフィックがネットワークからサービスプロバイダに送信され、DSCP値が異なる、適合、超過、および違反パケットをマーキングします。サービスプロバイダは、輻輳があるとDSCP値の超過および違反としてマーキングされたパケットをドロップすることができますが、使用可能な帯域幅がある場合は送信することも可能です。



(注) Layer 2 フィールドには CoS フィールドが含まれるようにマーキングでき、Layer 3 フィールドには precedence および DSCP フィールドが含まれるようにマーキングできます。

1 つの便利な機能として、複数のアクションとイベントを関連付ける機能があります。たとえば、すべての適合パケットについて、precedence ビットと CoS を設定できます。アクションを設定するサブモードは、ポリシング機能によって配信できます。

これは、ポリシングアクションの設定例を示しています。

```
Device# configure terminal
Device(config)# policy-map police
Device(config-pmap)# class class-default
Device(config-pmap-c)# police cir 1000000 pir 2000000
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
Device(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
Device(config-pmap-c-police)# end
```

この例では、exceed-markdown-table と violate-mark-down-table がテーブルマップです。



- (注) ポリサーベースのマークダウンアクションは、テーブルマップを使用する場合のみサポートされます。デバイスの各マーキングフィールドで許可されているマークダウンテーブルマップは1つだけです。

例：ポリサーの VLAN 設定

次の例では、VLAN のポリサー設定を表示します。この設定の最後に、QoS のインターフェイスに VLAN ポリシー マップを適用します。

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface HundredGigabitE1/0/5
Device(config-if)# service-policy input vlan100
```

例：ポリシングの単位

ポリシングの単位は、トークンバケットが機能する基礎となります。CIR および PIR はビット/秒で指定します。バーストパラメータはバイト単位で指定します。これはデフォルトのモードであり、単位が指定されていない場合に使用される単位です。CIR および PIR は、パーセントでも設定できます。その場合バーストパラメータをミリ秒単位で設定する必要があります。

例：シングルレート 2 カラー ポリシング設定

次の例は、ビット/秒のポリサー設定を示しています。この設定では、測定単位がビットであるデュアルレートの 3 カラーポリサーが設定されます。バーストおよびピークバーストはすべてビットに指定されます。

```
Device(config)# policy-map bps-policer
Device(config-pmap)# class class-default
Device(config-pmap-c)# police rate 100000 peak-rate 1000000
conform-action transmit exceed-action set-dscp-transmit dscp table
DSCP_EXCE violate-action drop
```

例：シングルレート 2 カラー ポリシング設定

次の例は、シングルレート 2 カラー ポリサーを設定する方法を示しています。

```
Device(config)# class-map match-any prec1
Device(config-cmap)# match ip precedence 1
Device(config-cmap)# exit
Device(config)# policy-map policer
Device(config-pmap)# class prec1
Device(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)#
```

例：デュアルレート 3 カラー ポリシング設定

次の例は、デュアルレート 3 カラー ポリサーを設定する方法を示しています。

```
Device# configure terminal
Device(config)# policy-Map dual-rate-3color-policer
Device(config-pmap)# class class-default
Device(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-markdown-table
Device(config-pmap-c-police)# violate-action set-dscp-transmit dscp table
violate-markdown-table
Device(config-pmap-c-police)# exit
Device(config-pmap-c)#
```

この例では、`exceed-markdown-table` と `violate-mark-down-table` がテーブル マップです。



(注) ポリサー ベースのマークダウンアクションは、テーブル マップを使用する場合のみサポートされます。デバイスの各マーキングフィールドで許可されているマークダウンテーブルマップは 1 つだけです。

例：テーブル マップのマーキング設定

次のステップと例は、QoS設定でテーブルマップマーキングを使用する方法を示しています。

1. テーブル マップを定義します。

table-map コマンドを使用してテーブルマップを定義し、値のマッピングを示します。このテーブルでは、テーブルが使用されるポリシーまたはクラスを認識しません。テーブルマップのデフォルトのコマンドは、一致する「from」フィールドがない場合に、「to」フィールドにコピーされる値を示します。この例では、table-map1 というテーブルマップが作成されます。定義されたマッピングでは、値 0 が 1 に、2 が 3 に変換され、デフォルト値は 4 に設定されます。

```
Device(config)# table-map table-map1
Device(config-tablemap)# map from 0 to 1
Device(config-tablemap)# map from 2 to 3
Device(config-tablemap)# default 4
Device(config-tablemap)# exit
```

2. テーブル マップが使用されるポリシー マップを定義します。

この例では、着信 CoS が table-map1 テーブルで指定されたマッピングに基づいて、DSCP にマッピングされます。この例では、着信パケットの DSCP が 0 である場合、パケット内の CoS は 1 に設定されます。テーブル マップ名が指定されていない場合、このコマンドではデフォルトの動作が実行され、値が「from」フィールド（この場合は DSCP）から「to」フィールド（この場合は CoS）にコピーされます。ただし、CoS が 3 ビットフィールドであっても DSCP は 6 ビットフィールドです。これは、DSCP 内の最初の 3 ビットに CoS がコピーされることを意味します。

```
Device(config)# policy map policy1
Device(config-pmap)# class class-default
Device(config-pmap-c)# set cos dscp table table-map1
Device(config-pmap-c)# exit
```

3. ポリシーをインターフェイスに関連付けます。

```
Device(config)# interface HundredGigabitE1/0/2
Device(config-if)# service-policy output policy1
Device(config-if)# exit
```

例：CoS マーキングを保持するテーブル マップの設定

次の例は、テーブル マップを使用して、QoS 設定のインターフェイスで CoS マーキングを保持する方法を示しています。

(例で設定されている) cos-trust-policy ポリシーは入力方向でイネーブルになり、インターフェイスに着信する CoS マーキングが保持されます。ポリシーがイネーブルになっていない場合

は、デフォルトで DSCP だけが信頼されます。純粋なレイヤ 2 パケットがインターフェイスに着信すると、CoS の入力ポートに一致するポリシーがない場合は、CoS 値が 0 に書き換えられます。

```
Device# configure terminal
Device(config)# table-map cos2cos
Device(config-tablemap)# default copy
Device(config-tablemap)# exit

Device(config)# policy map cos-trust-policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# set cos cos table cos2cos
Device(config-pmap-c)# exit

Device(config)# interface HundredGigabitE1/0/2
Device(config-if)# service-policy input cos-trust-policy
Device(config-if)# exit
```

次の作業

QoS 設定でこれらの自動機能を使用できるかどうかについては、自動 QoS のマニュアルを参照してください。

QoS に関する追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference</i> 『Cisco IOS Quality of Service Configuration Guide』

QoS の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	QoS の機能	QoS により、他のトラフィックタイプの代わりに特定のトラフィックタイプを優先的に処理できます。QoS を設定しない場合、デバイスはパケットの内容やサイズに関係なく、各パケットにベスト エフォート型のサービスを提供します。 (注) このリリースでは、コンバージドアクセスはサポートされません。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 3 章

重み付けランダム早期検出の設定

- ネットワーク輻輳の回避 (137 ページ)
- テールドロップ (137 ページ)
- 重み付けランダム早期検出 (138 ページ)
- WRED 設定の制限 (139 ページ)
- WRED 使用上の注意事項 (139 ページ)
- WRED の設定 (140 ページ)
- WRED の設定例 (144 ページ)
- 階層化 QoS を使用した WRED のサポート (144 ページ)
- WRED 設定の確認 (145 ページ)
- WRED 設定のベストプラクティス (146 ページ)
- 重み付けランダム早期検出の機能履歴 (148 ページ)

ネットワーク輻輳の回避

異種ネットワークには、アプリケーションが使用する異なるプロトコルが含まれており、これにより、ファイル転送などの時間依存が比較的少ないアプリケーションのニーズに対処しながら、タイムクリティカルなアプリケーションに応えるためにトラフィックの優先順位を付ける必要が生じています。ネットワーク内のデバイス間で単一のデータパスを共有するさまざまなタイプのトラフィックをサポートするようにネットワークが設定されている場合、輻輳回避メカニズムを実装することにより、さまざまなタイプのトラフィックを公平に処理し、共通のネットワーク ボトルネックでの輻輳を回避できます。輻輳回避メカニズムは、パケットのドロップにより実現します。

ランダム早期検出 (RED) は、ネットワークで一般的に使用される輻輳回避メカニズムです。

テールドロップ

テールドロップでは、すべてのトラフィックを平等に扱い、サービス クラス内では差別化しません。出力キューが一杯でテールドロップが有効な場合、輻輳が解消されてキューが一杯でなくなるまでパケットはドロップされます。

重み付けランダム早期検出

RED メカニズムは、TCP の輻輳制御メカニズムを利用します。輻輳が頻繁に発生する前にパケットがランダムにドロップされます。パケット送信元が TCP を使用する場合、送信元はすべてのパケットが宛先に届くようになるまで送信速度を下げます。これは輻輳が解消されたことを示します。RED を、TCP のパケットの転送速度を下げる方法として使用できます。TCP は停止するだけでなく、素早く再起動して、ネットワークがサポート可能なレートに伝送レートを対応させます。

WRED は、シスコが実装している RED です。RED アルゴリズムの機能と、IP プレゼンデンス、DiffServ コードポイント (DSCP)、またはサービスクラス (CoS) の値を組み合わせています。

WRED の仕組み

WRED は、出力インターフェイスにネットワーク混雑の兆候が表れた際に、選択的にパケットをドロップしてテールドロップの確率を減らします。WRED は、キューが一杯になるまで待機するのではなく、一部のパケットを早期にドロップします。そのため、一度に大量のパケットをドロップすることを防ぎ、TCP グローバル同期の可能性を最小限に抑えます。

Approximate Fair Drop (AFD) は、パケットのドロップ確率を決定するアクティブキュー管理 (AQM) アルゴリズムです。パケットをドロップする確率は、入力時のフローの着信レート計算と現在のキュー長によって異なります。

AFD ベースの WRED は、有線ネットワークポートに実装されます。

AFD ベースの WRED は、WRED の優先的なドロップ動作をエミュレートします。この優先的なドロップ動作は、WRED の対応するドロップしきい値に基づいて AFD サブクラスの重みを変更することで実現します。物理キュー内では、重みが大きいトラフィックのドロップ確率は、重みの小さいトラフィックよりも低くなります。

- 各 WRED 対応キューには、上限と下限のしきい値があります。
- 優先度の高いサブクラスには大きな AFD の重みが設定されます。
- サブクラスは、最も低い WRED minThreshold に基づいて昇順でソートされます。

WRED 重み計算

AFD の重みは、下限と上限のしきい値を使用して計算されます。AFD は、WRED の上限と WRED の下限のしきい値の平均を表す調整されたインデックスです。

パケットがインターフェイスに着信すると、次のイベントが発生します。

1. ドロップ確率が計算されます。AFD の重みが減少するほど、ドロップ確率は高くなります。つまり、下限と上限のしきい値の平均が小さいほど、ドロップ確率は高くなります。

2. WRED は、パケットのドロップを決定する前に、パケットフローのプライオリティとしきい値を検討します。CoS、DSCP、または IP Precedence の値は、指定されたしきい値にマッピングされます。これらのしきい値を超えると、これらのしきい値にマッピングされた設定値を持つパケットはドロップの対象になります。高いしきい値に割り当てられた CoS、DSCP、または IP Precedence 値を持つその他のパケットは、キューに入れられます。このプロセスにより、プライオリティの高いフローがそのまま維持され、パケット伝送の遅延が最小限に抑えられます。
3. パケットが WRED を使用してドロップされない場合、テールドロップされます。

WRED 設定の制限

- デフォルトでは、重み付きテールドロップ (WTD) がすべてのキューでイネーブルになっています。
- WRED はキューごとに有効または無効にできます。WRED を無効にすると、WTD がターゲットキューに適用されます。WRED プロファイルを持つポリシーマップは出力ポリシーとして物理ポート上にのみ設定されます。
- WRED は、ネットワークポートキューのみでサポートされており、内部 CPU キューとスタックキューではサポートされていません。
- 各 WRED 物理キューは、一意の WRED しきい値ペア設定を使用して 3 つのサブキューをサポートできます。
- WRED とともに、ポリシーマップで帯域幅または形状を設定することを確認します。
- すべての WRED しきい値は必ずパーセンテージモードで指定します。
- WRED しきい値ペアのマッピングは、対応する一致フィルタを使用してクラスマップフィルタをマッピングすることで行います。
「any」一致フィルタが設定されたクラスマップをお勧めします。
- プライオリティトラフィックの WRED はサポートされていません。
- WRED とキュー制限は、同じポリシーではサポートされません。
- 有線ポートは最大で 8 つの物理キューをサポートします。そのうちの 4 つの物理キューでそれぞれが 3 つのしきい値ペアを持つ WRED を設定できます。残りのキューは、WTD で設定されます。5 つ以上の WRED キューを持つポリシーは拒否されます。

WRED 使用上の注意事項

AFD ベースの WRED 機能を設定するには、ポリシーマップを指定し、クラスを追加します。**random-detect** コマンドを使用し、ドロップ確率の計算に WRED が使用する方式を (dscp-based/cos-based/cos-based 引数を使用して) 指定します。



(注) ポリシーは作業中に変更できます。AFD の重みが自動的に再計算されます。

WREDはIPv4/IPv6、マルチキャストなどのどのような種類のトラフィックにも設定できます。WRED は、8つのキューイングクラスすべてでサポートされます。

random-detect コマンドを使用して WRED を設定する場合は次の点を考慮してください。

- **dscp-based** 引数を使用する場合、WRED は DSCP 値を使用してドロップ確率を計算します。
- **cos-based** 引数を使用する場合、WRED は CoS 値を使用してドロップ確率を計算します。
- デフォルトでは、WRED はドロップ確率の計算に IP precedence 値を使用します。
precedence-based 引数がデフォルトであり、CLI には表示されません。



(注) **show run policy-map *policy-map*** コマンドは、**random-detect** コマンドで precedence が設定されていても、「precedence」を表示しません。

- **dscp-based** 引数と **precedence-based** 引数は、相互に排他的です。
- 8つの物理キューを、それぞれ異なる WRED プロファイルで設定できます。

WRED の設定

DSCP 値に基づく WRED の設定

DSCP 値に基づいて WRED プロファイルをパケット モードで設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	class-map <i>match-criteria class-name</i> 例： device(config)# class-map match-any CS	クラスマップに一致基準を設定します。 推奨する一致基準は match-any です。
ステップ 2	match <i>class-map-name</i> 例： device(config-cmap)#match dscp CS1	クラスマップを照合します。

	コマンドまたはアクション	目的
ステップ 3	policy-map <i>name</i> 例： device(config)#policy-map PWRED	作成する WRED プロファイル ポリシーの名前を指定します。
ステップ 4	class <i>class-name</i> 例： device(config-pmap)#class CS	ポリシーに関連付けるクラスの名前を指定します。
ステップ 5	Use either bandwidth { <i>kbps</i> remaining percentage percent percentage } or shape { average peak } <i>cir</i> 例： device(config-pmap-c)#bandwidth percent 10	ポリシーマップに属しているクラスに割り当てる帯域幅またはトラフィックシェーピングを指定します。
ステップ 6	random-detect <i>dscp-based</i> 例： device(config-pmap-c)#random-detect dscp-based	パケットのドロップ確率を計算する際には DSCP 値を使用するように WRED を設定します。
ステップ 7	random-detect dscp <i>dscp-value percent minThreshold maxThreshold</i> 例： device(config-pmap-c)#random-detect dscp cs1 percent 10 20	最小しきい値および最大しきい値をパーセンテージで指定します。
ステップ 8	interface <i>interface-name</i> 例： device(config)#interface HundredGigE1/0/2	インターフェイスコンフィギュレーションモードを開始します。
ステップ 9	service-policy output ポリシーマップ 例： device(config-if)#service-policy output pwred	ポリシー マップを出力インターフェイスに付加します。

サービスクラス値に基づく WRED の設定

サービスクラス (CoS) 値に基づいて WRED プロファイルをパケットモードで設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	class-map <i>match-criteria class-name</i> 例： device(config)# class-map match-any CS	クラスマップに一致基準を設定します。 推奨する一致基準は match-any です。
ステップ 2	match <i>class-map-name</i> 例： device(config-cmap)#match cos 3	クラスマップを照合します。
ステップ 3	policy-map <i>name</i> 例： device(config)#policy-map PWRED	作成する WRED プロファイル ポリシーの名前を指定します。
ステップ 4	class <i>class-name</i> 例： device(config-pmap)#class CS	ポリシーに関連付けるクラスの名前を指定します。
ステップ 5	bandwidth { <i>kbps</i> remaining percentage percent percentage } 例： device(config-pmap-c)#bandwidth percent 10	ポリシー マップに属しているクラスに割り当てる帯域幅を指定します。
ステップ 6	random-detect <i>cos-based</i> 例： device(config-pmap-c)#random-detect cos-based	パケットのドロップ確率を計算する際には CoS 値を使用するように WRED を設定します。
ステップ 7	random-detect cos <i>cos-value percent minThreshold maxThreshold</i> 例： device(config-pmap-c)#random-detect cos 3 percent 10 20	最小しきい値および最大しきい値をパーセンテージで指定します。
ステップ 8	interface <i>interface-name</i> 例： device(config)# interface HundredGigE1/0/2	インターフェイスコンフィギュレーションモードを開始します。
ステップ 9	service-policy output ポリシーマップ 例： device(config-if)#service-policy output pwred	ポリシー マップを出カインターフェイスに付加します。

IP プレシデンス値に基づく WRED の設定

IP プレシデンス値に基づいて WRED プロファイルをパケット モードで設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	class-map <i>match-criteria class-name</i> 例： device (config) # class-map match-any CS	クラスマップに一致基準を設定します。 推奨する一致基準は <i>match-any</i> です。
ステップ 2	match <i>class-map-name</i> 例： device (config-cmap) #match precedence 3	クラスマップを照合します。
ステップ 3	policy-map <i>name</i> 例： device (config) #policy-map pwred	作成する WRED プロファイル ポリシーの名前を指定します。
ステップ 4	class <i>class-name</i> 例： device (config-pmap) #class CS	ポリシーに関連付けるクラスの名称を指定します。
ステップ 5	bandwidth { <i>kbps</i> remaining percentage percent percentage } 例： device (config-pmap-c) #bandwidth percent 10	ポリシー マップに属しているクラスに割り当てる帯域幅を指定します。
ステップ 6	random-detect <i>precedence-based</i> 例： device (config-pmap-c) #random-detect precedence-based	パケットのドロップ確率を計算する際には IP プレシデンス値を使用するように WRED を設定します。
ステップ 7	random-detect precedence <i>precedence-value percent minThreshold maxThreshold</i> 例： device (config-pmap-c) #random-detect precedence 3 percent 10 20	最小しきい値および最大しきい値をパーセンテージで指定します。
ステップ 8	interface <i>interface-name</i> 例：	インターフェイスコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	device(config)#interface HundredGigE1/0/2	
ステップ 9	service-policy output ポリシーマップ 例： device(config-if)#service-policy output pwred	ポリシー マップを出カインターフェイスに付加します。

WRED の設定例

次に、クラス CS の DSCP プロファイルを使用するように WRED をイネーブルにする例を示します。この例では、cs1、cs2、および cs3 という 3 つのサブクラスを WRED の最小しきい値および最大しきい値で設定し、最終的にはポリシーを 100 ギガビットイーサネット インターフェイス 8 に適用します。

```
Device(config)# class-map match-any CS
Device(config-cmap)# match dscp cs1
Device(config-cmap)# match dscp cs2
Device(config-cmap)# match dscp cs3
Device(config-cmap)# policy-map PWRED
Device(config-pmap)# class CS
Device(config-pmap-c)# bandwidth percent 10
Device(config-pmap-c)# random-detect dscp-based
Device(config-pmap-c)# random-detect dscp cs1 percent 10 20
Device(config-pmap-c)# random-detect dscp cs2 percent 20 30
Device(config-pmap-c)# random-detect dscp cs3 percent 34 44
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface HundredGigE1/0/8
Device(config-if)# service-policy output PWRED
```

階層化 QoS を使用した WRED のサポート

階層型 QoS では、トラフィック管理をより細かい粒度で実行する、複数のポリシー レベルで QoS 動作を指定できます。

HQoS の場合、子ポリシーでのみ WRED が許可され、親ポリシーでは許可されません。親ポリシーにシェーピングを、子ポリシーに WRED を設定できます。

次に、親ポリシー **pwred-parent** を帯域幅の 10 パーセントでシェーピングしたトラフィックで設定し、それを DSCP ベースの WRED に設定されたその子ポリシー **pwred-child** に適用する例を示します。

```
policy-map PWRED-CHILD
class CWRED
  bandwidth percent 10
  random-detect dscp-based
  random-detect dscp 1 percent 10 20
  random-detect dscp 10 percent 20 30
```



```

policy-map PWRED-PARENT
  class class-default
  shape average percent 10
  service-policy PWRED-CHILD

```

次に、HQoS WRED 設定を確認する `show` コマンドを示します。

```

device# show policy-map PWRED-PARENT
policy Map PWRED-PARENT
  class class-default
    average Rate Traffic Shaping
    cir 30%
  service-policy PWRED-CHILD
policy-map PWRED-CHILD
class CWRED
  bandwidth percent 10
  random-detect dscp-based
  random-detect dscp 1 percent 10 20
  random-detect dscp 10 percent 20 30
policy-map PWRED-PARENT
class class-default
  shape average percent 30
  service-policy PWRED-CHILD

```

WRED 設定の確認

次の `show` コマンドを使用して、WRED の設定を確認します。

手順

ステップ 1 `show policy-map policy-map-name`

WRED としきい値のラベルが表示されます。

例：

```

Device# show policy-map PWRED
Policy Map PWRED
Class CS
  bandwidth 10 (%)
  percent-based wred

  dscp      min-threshold  max-threshold
  -----
  cs1 (8)   10              20
  cs2 (16)  20              30
  cs3 (24)  34              44
  default (0) -

```

ステップ 2 `show policy-map interface interface-name`

WRED AFD の重み、WRED Enq (パケット数およびバイト数)、WRED ドロップ (パケット数およびバイト数)、しきい値ペアに対して設定された DSCP ラベルが表示されます。

(注) トラフィックを開始した後にのみ、このコマンドを使用します。**show policy-map interface** は、トラフィックが送信された後にのみ、WRED 設定が更新されます。

例：

```
Device#show policy-map interface HundredGigE 1/0/2
HundredGigE1/0/2
```

```
Service-policy output: PWRED
```

```
Class-map: CS (match-any)
 0 packets
Match: dscp cs1 (8)
Match: dscp cs2 (16)
Match: dscp cs3 (24)
Queueing
```

```
(total drops) 27374016
(bytes output) 33459200081
bandwidth 10% (1000000 kbps)
```

```
AFD WRED STATS BEGIN
```

```
Virtual Class   min/max       Transmit      Random drop
AFD Weight
```

```
 0             10 / 20      (Byte) 33459183360    27374016
12
```

```
(Pkts) 522799759      427716
```

```
dscp : 8
```

```
 1             20 / 30      Byte) 0              0
20
```

```
(Pkts) 0              0
```

```
dscp : 16
```

```
 2             34 / 44      (Byte) 16721         0
31
```

```
(Pkts) 59             0
```

```
dscp : 24
```

```
Total Drops(Bytes)   : 27374016
```

```
Total Drops(Packets) : 427716
```

```
AFD WRED STATS END
```

```
Class-map: class-default (match-any)
 0 packets
Match: any
```

```
(total drops) 0
(bytes output) 192
```

WRED 設定のベストプラクティス

・3つの WRED 設定ペアのサポート

各 WRED 物理キュー（AFD キュー）は、一意の WRED しきい値ペア設定を使用して3つの WRED 設定ペアをサポートできます。

```
Policy-map P1
  Class CS
    Random-detect dscp-based
    Random-detect dscp CS1 percent 10 20 // WRED pair 1
    Random-detect dscp CS2 percent 20 30 // WRED pair 2
    Random-detect dscp CS3 percent 30 40 // WRED pair 3
  Class-map match-any CS
    match cs1
    match cs2
    match cs3
```

• WRED 設定ペアの追加

重複するしきい値ペアを WRED 設定ペアに追加できます。

```
Policy-map P1
  Class CS
    Random-detect dscp-based
    Random-detect dscp CS1 percent 10 20 // WRED pair 1
    Random-detect dscp CS2 percent 20 30 // WRED pair 2
    Random-detect dscp CS3 percent 30 40 // WRED pair 3
    Random-detect dscp CS4 percent 30 40 ==> belongs to WRED pair 3
    Random-detect dscp CS5 percent 20 30 ==> belongs to WRED pair 2
  Class-map match-any CS
    match cs1
    match cs2
    match cs3
    match cs4 >>
    match cs5 >>
```

• デフォルトの WRED ペア

2つ以下の WRED ペアが設定されている場合、WRED に参加しているどのクラスマップフィルタも最大しきい値（100, 100）でデフォルトの3番目の WRED ペアに割り当てられます。

```
Policy-map P1
  Class CS
    Random-detect dscp-based
    Random-detect dscp CS1 percent 10 20 // WRED pair 1
    Random-detect dscp CS2 percent 20 30 // WRED pair 2
  Class-map match-any CS
    match CS1
    match CS2
    match CS3
    match CS4
```

この場合は、CS3 と CS4 のクラスはしきい値（100, 100）で WRED ペア 3 にマッピングされます。

• 一致しない設定の拒否

クラスマップ内に一致フィルタがない場合に random-detect を設定すると、ポリシーのインスタールが拒否されます。

```
Class-map match-any CS
  match CS1
  match CS2
  match CS5
```

```

Policy-map P1
  Class CS
    Shape average percent 10
    Random-detect dscp-based
    Random-detect dscp CS1 percent 10 20 // WRED pair 1
    Random-detect dscp CS2 percent 20 30 // WRED pair 2
    Random-detect dscp CS3 percent 30 40 // WRED pair 3 ==> Mismatched
  sub-class.

```

このポリシーを出力側のインターフェイスに適用すると、クラスマップ値が不正であるとして、インストール時にそのポリシーは失敗します。

```

device(config)# int Fo1/0/5
device(config-if)# service-policy output P1
device(config-if)#
*Feb 20 17:33:16.964: %IOSXE-5-PLATFORM: Switch 1 R0/0: fed: WRED POLICY INSTALL
FAILURE.Invalid WRED filter mark: 24 in class-map: CS
*Feb 20 17:33:16.965: %FED_QOS_ERRMSG-3-LABEL_2_QUEUE_MAPPING_HW_ERROR: Switch 1
R0/0: fed: Failed to detach queue-map for FortyGigabitEthernet1/0/5: code 2

```

重み付けランダム早期検出の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	重み付けランダム早期検出メカニズム	<p>WRED は、ネットワーク内の輻輳を回避するメカニズムです。WRED は、出力インターフェイスにネットワーク混雑の兆候が表れた際に、選択的にパケットをドロップしてテール ドロップの確率を減らし、多数のパケットが一度にドロップされないようにします。次の値に基づいて動作するように WRED を設定できます。</p> <ul style="list-style-type: none"> • DiffServ コードポイント • IP Precedence • サービスクラス

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

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。