Cisco Nexus 6000 シリーズ NX-OS Quality of Service コンフィギュレーション ガイド、リリース 7.x

初版：2014 年 01 月 29 日

最終更新：2014 年 05 月 09 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/

Text Part Number: OL-30919-03-J

【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。

目 次

はじめに

ここでは、次の項について説明します。

対象読者

本書は、Cisco Nexus デバイス および Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定と保守を行う、ネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screenフォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 6000 シリーズ マニュアル セットは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-release-notes-list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-and-configuration-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FCoE Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Configuration Guide*』

インストレーション ガイドおよびアップグレード ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guides*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-command-reference-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Virtual Port Channel Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 6000 Series NX-OS MIB Reference*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/mib/reference/NX6000_MIBRef.html から入手できます。

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 6000 Series NX-OS System Message Guide*』は、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 6000 Series NX-OS Troubleshooting Guide*』は、http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/tsd-products-support-troubleshoot-and-alerts.html から入手できます。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載漏れに関する報告は、vsg-docfeedback@cisco.com に送信してください。 ご協力をよろしくお願いいたします。

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

新機能および変更された機能に関する情報

次の表では、このコンフィギュレーション ガイドでの重要な変更点の概要を示します。 この表は、このマニュアルのすべての変更点、または特定のリリースのすべての新機能をまとめたリストではありません。

機能	リリース	説明	参照先
		FEX-Based ACL 分類機能では、FEX の TCAM リソースを使用し、着信パケットの ACL ベースのパケット分類をスイッチ上で実行します。	FEX-Based ACL 分類の設定
バッファ使用状況ヒストグラム	7.0(2)N1(1)	バッファ使用状況ヒストグラム機能では、リアルタイムでシステムの最大キュー深度とバッファ使用状況を分析できます。 即時またはリアルタイムバッファ使用状況情報がサポートされます。	バッファ使用状況ヒストグラムの設定, （113 ページ）

機能	リリース	説明	参照先
IPv6 ACL ロギング	7.0(1)N1(1)	IPv6 ACL ロギング機能では、ACL フローをモニタし、インターフェイスでドロップされたパケットをログに記録することができます。	IPv6 ACL ロギングの概要, （107 ページ）
マイクロバーストモニタリング	7.0(0)N1(1)	マイクロバーストモニタリング機能は、入出力ポートの両方でポートごとにトラフィックをモニタし、非常に短い時間（マイクロ秒）内で不測のデータバーストを検出できるようにするものです。これにより、データ消失の危険性があったり、追加の帯域幅を必要とするようなネットワークフローを検出できます。	マイクロバーストモニタリングの概要, （91 ページ）
スイッチレイテンシモニタリングの設定	7.0(0)N1(1)	スイッチレイテンシモニタリング機能では、タイムスタンプ値とともに各入出力パケットをマークします。システムの各パケットのレイテンシを計算するために、スイッチは入力と出力のタイムスタンプを比較します。この機能により、すべてのポートペア間の平均レイテンシの履歴とリアルタイムのレイテンシデータを表示できます。	スイッチレイテンシモニタリングの概要, （95 ページ）

機能	リリース	説明	参照先
WRED 明示的輻輳通知	7.0(0)N1(1)	Weighted Random Early Detection（WRED）および明示的輻輳通知（ECN）は、遅延やパケット損失の影響を受ける用途に輻輳の管理と回避策を提供します（例：Telnet、Web ブラウジング、音声およびビデオデータなどの双方向トラフィック転送）。	プロキシキューの送信速度, （104 ページ）

新機能および変更された機能に関する情報

第 2 章

概要

この章の内容は、次のとおりです。

QoS について

設定可能な Cisco NX-OS Quality of Service（QoS）機能を使用して、ネットワーク トラフィックを分類し、トラフィック フローに優先順位を付けて、輻輳回避を実行できます。

デバイス上のデフォルトの QoS 設定により、ファイバ チャネルおよび Fibre Channel Over Ethernet（FCoE）トラフィックのロスレス サービスと、Ethernet トラフィックのベストエフォート型サービスが提供されます。 イーサネット トラフィックのサービス クラス（CoS）を追加するよう QoS を設定できます。 Cisco NX-OS QoS 機能は、Cisco Modular QoS CLI（MQC）を使用して設定されます。

（注） 標準のイーサネットは、ベスト エフォート型のメディアであるため、どのような形のフロー制御も備えていません。 輻輳や衝突が発生した場合、イーサネットではパケットが廃棄されます。 失われたデータの検出および廃棄されたパケットの再送信は、上位プロトコルにより行われます。

ファイバチャネルには各パケットの配信を保証する信頼できる送信システムが必要です。 FCoE を適切にサポートするために、イーサネットは輻輳を回避するプライオリティ フロー制御（PFC）メカニズムで拡張されています。

モジュラ QoS CLI

Cisco MQC は、QoS を設定するための標準コマンド セットを提供します。

MQC を使用して、追加のトラフィック クラスを定義し、システム全体および個別のインターフェイスに対して QoS ポリシーを設定できます。 MQC で QoS ポリシーを設定するには、次の手順を実行します。

1. トラフィック クラスを定義します。
2. 各トラフィック クラスにポリシーおよびアクションをアソシエートします。
3. ポリシーを論理インターフェイスまたは物理インターフェイスに結合します。同様にグローバル システム レベルで結合できます。

MQC には、トラフィックのクラスとポリシーを定義するために、2 つのコマンド タイプが用意されています。

class-map

パケット一致基準に基づいて、トラフィックのクラスを表すクラス マップを定義します。クラス マップはポリシー マップ内で参照されます。

クラス マップは、IEEE 802.1p サービス クラス（CoS）値などの一致基準に基づいて、着信パケットを分類します。 ユニキャスト パケットおよびマルチキャスト パケットが分類されます。

policy-map

クラス単位でクラス マップに適用するポリシーのセットを表すポリシー マップを定義します。

ポリシー マップは、帯域幅の制限やパケットのドロップなど、アソシエートされたトラフィック クラスで実行するアクション セットを定義します。

クラス マップおよびポリシー マップを作成する場合は、次の class-map および policy-map オブジェクト タイプを定義します。

network-qos

システム レベルの関連アクションに使用できる MQC オブジェクトを定義します。

qos

分類に使用できる MQC オブジェクトを定義します。

queuing

出力でキューイングおよびスケジューリングに使用したり、使用できる MQC オブジェクトを定義します。

（注） qos タイプは、**class-map** コマンドおよび **policy-map** コマンドのデフォルトですが、タイプを明示的に指定する必要がある **service-policy** では、デフォルトではありません。

ポリシーは、**service-policy** コマンドを使用して、インターフェイスまたは EtherChannel に追加できるほか、グローバル システム レベルで追加できます。

show class-map コマンドおよび **show policy-map** コマンドを使用して、MQC オブジェクトのすべてまたは個々の値を表示できます。

MQC ターゲットは、パケットのフローを表すエンティティ（イーサネット インターフェイスなど）です。 サービス ポリシーはポリシー マップを MQC ターゲットに関連付け、着信または発信パケットでポリシーを適用するかどうかを指定します。 このマッピングにより、マーキング、帯域割り当て、バッファ割り当てなど、QoS ポリシーの設定をイネーブルにします。

CPU 方向のトラフィックの QoS

デバイスは、CPU でパケットがフラッディングしないように、CPU 方向のトラフィックに自動的に QoS ポリシーを適用します。 ブリッジ プロトコル データ ユニット（BPDU）フレームなどの制御トラフィックには、確実に配信できるように、より高いプライオリティが与えられます。

第 3 章

分類の設定

この章の内容は、次のとおりです。

分類について

分類とは、パケットをトラフィック クラスに振り分けることです。指定した分類済みトラフィックに対して特定のアクション（ポリシングやマークダウンなど）を実行するようにデバイスを設定します。

パケットの特性を分類基準と照合することによって、各トラフィック クラスを表すクラスマップを作成できます。

表 *1*：分類基準

分類基準	説明
クラス マップ	名前付きクラス マップ オブジェクト内で指定された基準。
Precedence	IP ヘッダーのタイプ オブ サービス（ToS）バイト内部の優先順位値。
Diffserv コード ポイント（DSCP）	IP ヘッダーの DIffServ フィールド内部の DSCP 値。

分類基準	説明
プロトコル	アドレス解決プロトコル（ARP）、コネクションレス型ネットワーク サービス（CLNS）などの選択済みプロトコル セット。
IP RTP	Real-time Transport Protocol（RTP）を使用しているアプリケーションを、UDP ポート番号範囲によって識別します。
ACL	トラフィックは、アクセス コントロール リスト（ACL）に定義されている基準で分類されます。

表 *2*：サポートされている *RFC*

RFC	タイトル
RFC 2474	『Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers』

入力分類ポリシー

分類は、トラフィックをクラスに区分けするのに使用します。 トラフィックは、パケット特性（CoS フィールド）またはパケット ヘッダー フィールドに基づいて分類します。パケット ヘッダー フィールドには、IP precedence、DiffServ コード ポイント（DSCP）、レイヤ 2 からレイヤ 4 までのパラメータが含まれます。 トラフィックの分類に使用する値を、一致基準と呼びます。

どのクラスにも一致しないトラフィックは、class-default と呼ばれるデフォルトのトラフィック クラスに割り当てられます。

分類のライセンス要件

この機能にはライセンスは不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

分類の設定

クラス マップの設定

class-map コマンドを使用して、クラス マップを作成または変更できます。 クラス マップは、トラフィックのクラスを表す名前付きオブジェクトです。クラスマップでは、パケットを分類する一致基準を指定します。 以降は、クラスマップをポリシーマップで参照できるようになります。

（注） クラス マップ タイプのデフォルトは type qos で、その一致基準のデフォルトは match-all です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map** [**type** {**network-qos** | **qos** | **queuing**}] *class-map name*	指定されたトラフィックのクラスを表す名前付きオブジェクトを作成するか、名前付きオブジェクトにアクセスします。 クラス マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大40文字まで設定できます。 次のように 3 つのクラス マップ コンフィギュレーション モードがあります。 • **network-qos**：ネットワーク全体（グローバル）モード。 CLI プロンプト：switch (config-cmap-nq)# • **qos**：分類モード。これがデフォルト モードです。 CLI プロンプト：switch (config-cmap-qos)# • **queuing**：キューイング モード。 CLI プロンプト：switch(config-cmap-que)#
ステップ 3	switch(config)# **class-map** [**type qos**] [**match-all** | **match-any**] *class-map name*	（任意） パケットがクラス マップに定義された基準の一部またはすべてを満たす必要があることを指定します。 • **match-all**：パケットが、指定した class map に定義されているすべての基準を満たす場合（たとえば、定義された CoS と ACL 基準の両方が一致する場合）、トラフィックを分類します。

	コマンドまたはアクション	目的
		• **match-any**：パケットが、指定した class map に定義されているいずれかの基準を満たす場合（たとえば、CoS またはACLの基準のいずれかが一致する場合）、トラフィックを分類します。 クラス マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大40文字まで設定できます。
ステップ 4	switch(config)# **no class-map** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	（任意） 指定されたクラス マップを削除します。 （注） システム定義の 2 つのクラス マップ（class-fcoe と class-default）は削除できません。 クラス マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大40文字まで設定できます。

CoS 分類の設定

IEEE 802.1Qヘッダー内のサービスクラス（CoS）フィールドに基づいてトラフィックを分類できます。 この 3 ビットのフィールドは IEEE 802.1p で QoS トラフィック クラスをサポートするために規定されています。 CoS は Virtual Local Area Network（VLAN：バーチャル LAN）ID タグ フィールドの上位 3 ビットで符号化され、*user_priority* と呼ばれます。

（注） Cisco Nexus 2148 ファブリック エクステンダは dot1p vlan 0 タグを持つフレームをサポートしません。

システム クラスに no-drop 機能が設定されている場合、**match cos** コマンドは追加目的で機能します。 スイッチは CoS 値をアダプタに送信するので、アダプタはこの CoS 値の PFC ポーズを適用します。

FCoE システム クラスのデフォルトの CoS 値は 3 です。 **match cos** 設定を FCoE システム クラスに追加して、異なる CoS 値を設定できます。 PFC ポーズは新しい値と一致するトラフィックに適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map type qos** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。 クラス マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	switch(config-cmap-qos)# **match cos** *cos-value*	パケットをこのクラスに分類する場合に照合する CoS 値を指定します。 CoS 値は、0 ～ 7 の範囲で設定できます。 （注） Cisco Nexus 2148T ファブリック エクステンダを接続して使用している場合、データ トラフィックを CoS 値 7 でマーク付けしないでください。 CoS 7 は、ファブリック エクステンダを通過する制御トラフィック用に予約されています。
ステップ 4	switch(config-cmap-qos)# **no match cos** *cos-value*	（任意） 一致するトラフィックをトラフィック クラスから削除します。

次の例は、定義された CoS 値に基づいてパケットを照合することにより、トラフィックを分類する方法を示しています。

```
switch# configure terminal
switch(config)# class-map type qos match-any class_cos
switch(config-cmap-qos)# match cos 4, 5-6
```

CoS 値のクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_cos
```

Precedence 分類の設定

IP ヘッダー（IPv4 または IPv6 のいずれか）のサービス タイプ（ToS）バイト フィールドの優先順位値に基づいてトラフィックを分類できます。 次の表に、優先順位値を示します。

表 *3*：優先順位値

値	優先順位値の一覧
<0-7>	IP precedence 値
critical	クリティカル precedence（5）
flash	フラッシュ precedence（3）
flash-override	フラッシュ上書き precedence（4）
immediate	即時 precedence（2）
internet	インターネットワーク コントロール precedence（6）
network	ネットワーク コントロール precedence（7）
priority	優先 precedence（1）
routine	ルーチン precedence（0）

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map type qos match-any** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。 クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラスマップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	switch(config-cmap-qos)#**match precedence** *precedence-values*	優先順位の値に基づいたパケットの照合により、トラフィック クラスを設定します。 優先順位値の一覧については、優先順位値の表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 4	switch((config-cmap-qos)# **no match precedence** *precedence-values*	（任意） 一致するトラフィックをトラフィック クラスから削除します。優先順位値の一覧については、優先順位値の表を参照してください。

次の例は、IP ヘッダーの ToS バイトの優先順位値に基づいてパケットを照合することにより、トラフィックを分類する方法を示しています。

```
switch# configure terminal
switch(config)# class-map type qos match-any class_precedence
switch(config-cmap-qos)# match precedence 1-2, critical
```

IP precedence 値のクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_precedence
```

DSCP 分類の設定

IP ヘッダー（IPv4 または IPv6 のいずれか）の DiffServ フィールドにある DiffServ コード ポイント（DSCP）値に基づいてトラフィックを分類できます。

表 *4*：標準の *DSCP* 値

値	DSCP 値のリスト
af11	AF11 dscp（001010）：10 進数の 10
af12	AF12 dscp（001100）：10 進数の 12
af13	AF13 dscp（001110）：10 進数の 14
af21	AF21 dscp（010010）：10 進数の 18
af22	AF22 dscp（010100）：10 進数の 20
af23	AF23 dscp（010110）：10 進数の 22
af31	AF31 dscp（011010）：10 進数の 26
af32	AF32 dscp（011100）：10 進数の 28
af33	AF33 dscp（011110）：10 進数の 30
af41	AF41 dscp（100010）：10 進数の 34

値	DSCP 値のリスト
af42	AF42 dscp（100100）：10 進数の 36
af43	AF43 dscp（100110）：10 進数の 38
cs1	CS1（優先順位 1）dscp（001000）：10 進数の 8
cs2	CS2（優先順位 2）dscp（010000）：10 進数の 16
cs3	CS3（優先順位 3）dscp（011000）：10 進数の 24
cs4	CS4（優先順位 4）dscp（100000）：10 進数の 32
cs5	CS5（優先順位 5）dscp（101000）：10 進数の 40
cs6	CS6（優先順位 6）dscp（110000）：10 進数の 48
cs7	CS7（優先順位 7）dscp（111000）：10 進数の 56
default	デフォルト dscp（000000）：10 進数の 0
ef	EF dscp（101110）：10 進数の 46

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map type qos** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	switch(config-cmap-qos)# **match dscp** *dscp-list*	*dscp-list* 変数の値に基づいて、パケットの照合によってトラフィック クラスを設定します。 DSCP 値の一

	コマンドまたはアクション	目的
		覧については、標準のDSCP値の表を参照してください。
ステップ 4	switch(config-cmap-qos)# **no match dscp** *dscp-list*	（任意） 一致するトラフィックをトラフィック クラスから削除します。 DSCP 値の一覧については、標準の DSCP 値の表を参照してください。

次の例は、IP ヘッダーの DiffServ フィールドの DSCP 値に基づいてパケットを照合することにより、トラフィックを分類する方法を示しています。

```
switch# configure terminal
switch(config)# class-map type qos match-any class_dscp
switch(config-cmap-qos)# match  dscp af21, af32
```

DSCP のクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_dscp
```

プロトコル分類の設定

IP ヘッダーの [IPv4 Protocol] フィールドまたは [IPv6 Next Header] フィールドに基づいて、トラフィックを分類できます。 次の表に、protocol 引数を示します。

表 5：***Protocol*** 引数

引数	説明
arp	アドレス解決プロトコル（ARP）
clns_es	CLNS エンド システム
clns_is	CLNS 中継システム
dhcp	Dynamic Host Configuration（DHCP）
ldp	ラベル配布プロトコル（LDP）
netbios	NetBIOS Extended User Interface（NetBEUI）

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **class-map type qos** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラスマップ名は大文字と小文字が区別され、最大40文字まで設定できます。
ステップ 3	switch(config-cmap-qos)# **match protocol** {**arp** | **clns_es** | **clns_is** | **dhcp** | **ldp** | **netbios**}	指定したプロトコルに基づいてパケットを照合することによって、トラフィック クラスを設定します。
ステップ 4	switch(config-cmap-qos)# **no match protocol** {**arp** | **clns_es** | **clns_is** | **dhcp** | **ldp** | **netbios**}	（任意） 一致するトラフィックをトラフィック クラスから削除します。

次の例は、プロトコル フィールドに基づいてパケットを照合することにより、トラフィックを分類する方法を示しています。

```
switch# configure terminal
switch(config)# class-map type qos class_protocol
switch(config-cmap-qos)# match protocol arp
```

プロトコルのクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_protocol
```

IP RTP 分類の設定

IP Real-time Transport Protocol（RTP）は、オーディオやビデオなどのデータを送信するリアルタイム アプリケーション用のトランスポート プロトコルで、Request For Comments（RFC）3550 で規定されています。 RTP では一般的な TCP ポートや UDP ポートは使用されませんが、通常はポート 16384 ～ 32767 を使用するように RTP を設定します。 偶数ポートを UDP 通信に使用し、次の上位の奇数ポートを RTP Control Protocol（RTCP）通信に使用します。

UDP ポート範囲に基づいて分類できます。UDP ポート範囲は、RTP を使用するアプリケーションを対象とする可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map type qos** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。 クラス マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	switch(config-cmap-qos)# **match ip rtp** *port-number*	UDP ポート番号の下限と上限に基づいてパケットを照合することによって、トラフィック クラスを設定します。UDP ポート番号の範囲は、RTP を使用するアプリケーションを対象とする可能性があります。値の範囲は 2000 ～ 65535 です。
ステップ 4	switch(config-cmap-qos)# **no match ip rtp** *port-number*	（任意） 一致するトラフィックをトラフィック クラスから削除します。

次に、RTP アプリケーションで一般に使用される UDP ポート範囲に基づいてパケットを照合することにより、トラフィックを分類する例を示します。

```
switch# configure terminal
switch(config)# class-map type qos match-any class_rtp
switch(config-cmap-qos)# match  ip rtp 2000-2100, 4000-4100
```

RTP のクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_rtp
```

ACL 分類の設定

既存のアクセスコントロールリスト（ACL）に基づいたパケットの照合により、トラフィックを分類できます。 ACL で定義された基準によってトラフィックが分類されます。 ACL キーワードの **permit** および **deny** は、照合時には無視されます。アクセス リストの一致基準に **deny** アクションが含まれる場合でも、そのクラスの照合では使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **class-map type qos** *class-name*	トラフィックのクラスを表す名前付きオブジェクトを作成します。 クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。クラス マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	switch(config-cmap-qos)# **match access-group name** *acl-name*	*acl-name* に基づいてパケットを照合することによって、トラフィック クラスを設定します。 ACL キーワードの **permit** および **deny** は、照合時には無視されます。 （注） 1 つのクラス マップで定義できる ACL は 1 つだけです。 **match access-group** が定義されたクラスには、その他の一致基準を追加できません。
ステップ 4	switch(config-cmap-qos)# **no match access-group name** *acl-name*	（任意） 一致するトラフィックをトラフィック クラスから削除します。

次に、既存の ACL に基づいたパケットの照合により、トラフィックを分類する例を示します。

```
switch# configure terminal
switch(config)# class-map type qos class_acl
switch(config-cmap-qos)# match access-group name acl-01
```

ACL のクラス マップ設定を表示するには、**show class-map** コマンドを使用します。

```
switch# show class-map class_acl
```

分類設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show class-map	スイッチで定義されたクラスマップを表示します。

コマンド	目的
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。指定したポリシーだけを表示することもできます。
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 4 章

ポリシー マップの設定

この章の内容は、次のとおりです。

ポリシー タイプに関する情報

このデバイスは、複数のポリシー タイプをサポートしています。 クラス マップはポリシー タイプで作成します。

3 つのポリシー タイプがあります。

- network-qos
- Queuing
- QoS

Cisco Nexus デバイス で FCoE をイネーブルにする前に、**type qos policy maps** コマンドを入力し、システム QoS に 1 つ以上の FCoE QoS ポリシーを適用することによって、3 つのタイプ QoS ポリシー（ネットワーク QoS、キューイング、および QoS）において、class-fcoe をイネーブルにする必要があります。

クラスの各タイプには、次の QoS パラメータを指定できます。

- type network-qos：network-qos ポリシーを使用して、システム クラスを配置し、システム全体のスコープを持つそれらのクラスにパラメータを関連付けます。
  - 分類：このクラスに一致するトラフィックは次のとおりです。
    - QoS グループ：type network-qos のクラス マップはシステム クラスを示し、関連付けられた qos-group によって照合されます。

- ポリシー：一致したトラフィックで実行されるアクションは次のとおりです。

（注） network-qos ポリシーは、システム qos ターゲットだけに結合できます。

  - MTU：システム クラスにマッピングされたトラフィックに適用する必要のある最大伝送単位（MTU）。 システム クラスごとにデフォルトの MTU があります。システム クラス MTU は設定可能です。
  - マルチキャスト最適化：このクラスにマッピングされているマルチキャスト トラフィックのパフォーマンスを最適化する場合に指定します。
  - pause no-drop：no drop は、システム クラスのロスレス サービスを指定します。drop は、このシステム クラスのキューが満杯である場合にテール ドロップを使用する（キューが割り当てサイズに達すると、着信パケットがドロップされる）よう指定します。

    追加のパラメータ pfc-cos を設定できます。 このパラメータは、no-drop システム クラスのトラフィックが、サービスクラス（CoS）だけに基づいてマッピングされず、輻輳が発生する場合に、プライオリティ フロー制御（PFC）をアサートする CoS 値を示します。
  - no-drop クラス用のバッファを変更できます。
  - キュー制限：このシステム クラスのキューに確保する必要があるバッファ数を指定します。 このオプションは no-drop システム クラスには設定できません。

- type queuing：type queuing ポリシーを使用して、システム クラスと関連付けられたキューのスケジューリング特性を定義します。

（注） 一部の設定パラメータは、EtherChannel に適用されていると、メンバ ポートの設定に反映されません。

  - 分類：このクラスに一致するトラフィックは次のとおりです。
    - QoS グループ：タイプ キューイングのクラス マップは、システム クラスを示し、関連付けられた QoS グループによって照合されます。
  - ポリシー：一致したトラフィックで実行されるアクションは次のとおりです。

（注） システム qos ターゲットまたは任意のインターフェイスに結合できます。 出力キューイング ポリシーを使用して、システム クラスに関連付けられた、デバイスの出力キューを設定します。 入力キューイング ポリシーを使用して、統合ネットワーク アダプタ（CNA）のキューのスケジューリングを設定します。 入力キューイング ポリシー パラメータは、DCBX プロトコルで CNA に発信されます。

- 帯域幅：保証されるスケジューリング Deficit Weighted Round Robin（DWRR）の割合（%）をシステム クラスに設定します。
- プライオリティ：システム クラスを完全プライオリティ スケジューリング用に設定します。 指定されたキューイング ポリシーで優先するシステム クラスを 1 つだけ設定できます。

- タイプ qos：タイプ QoS ポリシーを使用して、フレーム内にあるレイヤ 2、レイヤ 3、レイヤ 4 の各種フィールドに基づいたトラフィックを分類し、システム クラスにマッピングします。

（注） 一部の設定パラメータは、EtherChannel に適用されていると、メンバ ポートの設定に反映されません。

- 分類：このクラスに一致するトラフィックは次のとおりです。
  - アクセス コントロール リスト（ACL）：既存の ACL の基準に基づいてトラフィックを分類します。
  - サービス クラス：フレーム ヘッダーの CoS フィールドに基づいてトラフィックを照合します。
  - DSCP：IP ヘッダーの DiffServ フィールドにある DiffServ コード ポイント（DSCP）値に基づいてトラフィックを分類します。
  - IP リアルタイム プロトコル：リアルタイム アプリケーションで使用されるポート番号に基づいてトラフィックを分類します。
  - 優先順位：IP ヘッダーのタイプ オブ サービス（ToS）フィールドの優先順位値に基づいてトラフィックを分類します。
  - プロトコル：IP ヘッダーの [IPv4 Protocol] フィールドまたは [IPv6 Next Header] フィールドに基づいて、トラフィックを分類します。
- ポリシー：一致したトラフィックで実行されるアクションは次のとおりです。

（注） このポリシーは、システムまたは任意のインターフェイスに追加できます。このポリシーは入力トラフィックだけに適用されます。

- QoS グループ：このトラフィック フローがマッピングされたシステム クラスに対応する QoS グループを設定します。

ポリシー マップの設定

ポリシーマップの作成

policy-map コマンドを使用して、トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。

ロスレス サービス用の no-drop クラス（class-fcoe）とベストエフォート型サービス用の drop クラス（class-default）の 2 つのデフォルト システム クラスがデバイスにあります。 イーサネット トラフィックには最大 4 つの追加システム クラスを定義できます。

次の事前定義ポリシー マップがデフォルトのサービス ポリシーとして使用されます。

- network-qos：default-nq-policy
- 入力 qos：default-in-policy
- 入力キューイング：default-in-policy
- 出力キューイング：default-out-policy

- service-policy type qos input fcoe-default-in-policy
- service-policy type queuing input fcoe-default-in-policy
- service-policy type queuing output fcoe-default-out-policy
- service-policy type network-qos fcoe-default-nq-policy

class-fcoe が qos ポリシーに含まれていない場合、vFC インターフェイスはアップにならず、ドロップの増加が発生します。

ポリシー マップを作成して、任意のユーザ定義のクラスにポリシーを指定する必要があります。このポリシー マップで、各クラスに QoS パラメータを設定できます。 同じポリシー マップを使用して、デフォルト クラスの設定を変更できます。

デバイスは、接続されたネットワーク アダプタにすべてのポリシーマップ設定値を配布します。

はじめる前に

ポリシー マップを作成する前に、新しいシステム クラスごとにクラス マップを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map** [**type** {**network-qos** | **qos** | **queuing**}] *policy-name*	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。 次のように3つのポリシーマップ コンフィギュレーション モードがあります。 • network-qos：ネットワーク全体（グローバル）モード。 CLI プロンプト：switch(config-pmap-nq)# • qos：分類モード。これがデフォルト モードです。 CLI プロンプト：switch(config-pmap-qos)# • queuing：キューイング モード。 CLI プロンプト：switch(config-pmap-que)#
ステップ 3	switch(config)# **no policy-map** [**type** {**network-qos** | **qos** | **queuing**}] *policy-name*	（任意） 指定されたポリシー マップを削除します。
ステップ 4	switch(config-pmap)# **class** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	クラス マップをポリシー マップにアソシエートし、指定されたシステム クラスのコンフィギュレーション モードを開始します。 次のように 3 つのクラス マップ コンフィギュレーション モードがあります。 • network-qos：ネットワーク全体（グローバル）モード。 CLI プロンプト：switch(config-pmap-c-nq)# • qos：分類モード。これがデフォルト モードです。 CLI プロンプト：switch(config-pmap-c-qos)# • queuing：キューイング モード。 CLI プロンプト：switch(config-pmap-c-que)# （注） アソシエートされるクラス マップには、ポリシー マップ タイプと同じタイプが必要です。
ステップ 5	switch(config-pmap)# **no class** [**type** {**network-qos** | **qos** | **queuing**}] *class-name*	（任意） クラス マップの関連付けを削除します。

type qos ポリシーの設定

一意の qos グループ値で識別される特定のシステム クラスのトラフィックを分類するには、type qos ポリシーを使用します。 type qos ポリシーは、入力トラフィックに関してのみ、システムまたは個々のインターフェイス（ファブリック エクステンダのホストインターフェイスを含む）に追加できます。

入力トラフィックには最大 5 つの QoS グループを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map type qos** *policy-name*	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	switch(config-pmap-qos)# [**class** | **class-default**] **type qos** *class-name*	クラスマップをポリシーマップにアソシエートし、指定されたシステムクラスのコンフィギュレーション モードを開始します。 （注） アソシエートされるクラス マップには、ポリシー マップ タイプと同じタイプが必要です。
ステップ 4	switch(config-pmap-c-qos)# **set qos-group** *qos-group-value*	トラフィックをこのクラスマップに分類する場合に照合する 1 つまたは複数の **qos-group** 値を設定します。 次のリストに、*qos-group-value* の範囲を示します。 デフォルト値はありません。
ステップ 5	switch(config-pmap-c-qos)# **no set qos-group** *qos-group-value*	（任意） このクラスから **qos-group** 値を削除します。

次の例は、type qos ポリシー マップを定義する方法を示しています。

```
switch# configure terminal
switch(config)# policy-map type qos policy-s1
switch(config-pmap-qos)# class type qos class-s1
switch(config-pmap-c-qos)# set qos-group 2
```

type network-qos ポリシーの設定

type network-qos ポリシーは、システム qos の結合時だけで設定でき、 特定のクラス用にスイッチ全体に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map type network-qos** *policy-name*	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	switch(config-pmap-nq)# **class type network-qos** *class-name*	クラス マップをポリシー マップにアソシエートし、指定されたシステム クラスのコンフィギュレーション モードを開始します。 （注） アソシエートされるクラス マップには、ポリシー マップ タイプと同じタイプが必要です。
ステップ 4	switch(config-pmap-c-nq)# **mtu** *mtu-value*	MTU 値をバイト単位で指定します。 （注） 設定する *mtu-value* は、**system jumbomtu** コマンドで設定した値より小さくする必要があります。
ステップ 5	switch(config-pmap-c-nq)# **no mtu**	（任意） このクラスの MTU 値をリセットします。
ステップ 6	switch(config-pmap-c-nq)# **pause no-drop**	no-drop クラスを設定します。
ステップ 7	switch(config-pmap-c)# **pause no-drop** [**pfc-cos** *pfc-cos-value*]	no-drop クラスを設定します。 このコマンドを指定しなければ、デフォルト ポリシーはドロップになります。 （注） ドロップ ポリシーの動作はテール ドロップと似ています。キューが割り当てサイズまで増加すると、着信パケットはドロップされます。 *pfc-cos-value* の範囲は 0 ～ 7 です。 このオプションがサポートされるのは、ACL ベースのシステム クラス

	コマンドまたはアクション	目的
		（CoS ベース以外の一致基準を使用してトラフィックをフィルタリングします）だけです。 **注意** CoS 値のリストは、class-fcoe の FCoE トラフィックに使用される CoS 値を含む可能性があります。 ご使用のトポロジに望ましい動作かどうかを判断する必要があります。
ステップ 8	switch(config-pmap-c-nq)# **no pause no-drop**	（任意） no-drop オプションをこのクラスから削除します。
ステップ 9	switch(config-pmap-c-nq)# **set cos** *cos-value*	このインターフェイスでパケットのマーキングに使用する 802.1Q CoS 値を指定します。 値の範囲は 0 ～ 7 です。
ステップ 10	switch(config-pmap-c-nq)# **no set cos** *cos-value*	（任意） このクラスのマーキング動作をディセーブルにします。

次の例は、type network-qos ポリシー マップを定義する方法を示しています。

```
switch# configure terminal
switch(config)# policy-map type network-qos policy-que1
switch(config-pmap-nq)# class type network-qos class-que1
switch(config-pmap-c-nq)# mtu 5000
switch(config-pmap-c-nq)# set cos 4
```

type queuing ポリシーの設定

type queuing ポリシーを使用して、特定のシステム クラスのトラフィックをスケジューリングおよびバッファリングします。 type queuing ポリシーは QoS グループで識別され、入力または出力トラフィック用にシステムまたは個々のインターフェイス（ファブリック エクステンダ ホスト インターフェイスを除く）に追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map type queuing** *policy-name*	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-pmap-que)# **class type queuing** *class-name*	クラスマップをポリシーマップにアソシエートし、指定されたシステム クラスのコンフィギュレーション モードを開始します。
ステップ 4	switch(config-pmap-c-que)# **priority**	このクラスの該当するトラフィックが完全プライオリティ キューにマッピングされるよう指定します。 （注） 完全プライオリティを設定できるクラスは、各ポリシー マップで 1 つだけです。
ステップ 5	switch(config-pmap-c-que)# **no priority**	（任意） 完全プライオリティ キューイングをこのクラスのトラフィックから削除します。
ステップ 6	switch(config-pmap-c-que)# **bandwidth percent** *percentage*	このクラスに割り当てられたインターフェイスの保証帯域幅の割合を指定します。 デフォルトでは、クラスの帯域幅は指定されていません。 （注） 帯域幅をクラスに正常に割り当てるには、まず class-default および class-fcoe で帯域幅のデフォルト設定を下げる必要があります。
ステップ 7	switch(config-pmap-c-que)# **no bandwidth percent** *percentage*	（任意） 帯域幅の指定をこのクラスから削除します。

ポリシー マップ設定の確認

コマンド	目的
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。 指定したポリシーだけを表示することもできます。
show policy-map interface [*interface number*]	1 つまたはすべてのインターフェイスのポリシーマップ設定を表示します。
show policy-map system	システム qos に結合されたポリシー マップ設定を表示します。
show policy-map type {**network-qos** | **qos** | **queuing**} [*name*]	特定のポリシー タイプのポリシー マップ設定を表示します。 指定したポリシーだけを表示することもできます。

コマンド	目的
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 5 章

マーキングの設定

この章の内容は、次のとおりです。

マーキングについて

マーキングは、着信および発信パケットの Quality of Service（QoS）フィールドを変更するために使用する方式です。

マーキングのコマンドは、ポリシーマップ内で参照されるトラフィッククラスで使用できます。設定できるマーキング機能を次に示します。

- DSCP
- IP precedence
- CoS

マーキングの設定

DSCP マーキングの設定

Cisco Nexus デバイスでは、IP ヘッダーの DiffServ フィールドの上位 6 ビットで、DSCP 値を指定の値に設定できます。 次の表に示す標準の DSCP 値のほか、0 ～ 63 の数値も入力できます。

（注） DSCP と IP precedence のいずれかの値は設定できますが、IP パケットの同じフィールドを変更するため、両方の値は設定できません。

表 *6*：標準の *DSCP* 値

値	DSCP 値のリスト
af11	AF11 dscp（001010）：10 進数の 10
af12	AF12 dscp（001100）：10 進数の 12
af13	AF13 dscp（001110）：10 進数の 14
af21	AF21 dscp（010010）：10 進数の 18
af22	AF22 dscp（010100）：10 進数の 20
af23	AF23 dscp（010110）：10 進数の 22
af31	AF31 dscp（011010）：10 進数の 26
af32	AF40 dscp（011100）：10 進数の 28
af33	AF33 dscp（011110）：10 進数の 30
af41	AF41 dscp（100010）：10 進数の 34
af42	AF42 dscp（100100）：10 進数の 36
af43	AF43 dscp（100110）：10 進数の 38
cs1	CS1（優先順位 1）dscp（001000）：10 進数の 8
cs2	CS2（優先順位 2）dscp（010000）：10 進数の 16
cs3	CS3（優先順位 3）dscp（011000）：10 進数の 24
cs4	CS4（優先順位 4）dscp（100000）：10 進数の 32
cs5	CS5（優先順位 5）dscp（101000）：10 進数の 40

値	DSCP 値のリスト
cs6	CS6（優先順位 6）dscp（110000）：10 進数の 48
cs7	CS7（優先順位 7）dscp（111000）：10 進数の 56
default	デフォルト dscp（000000）：10 進数の 0
ef	EF dscp（101110）：10 進数の 46

手順

	コマンドまたはアクション	目的
ステップ 1	**config t**	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 type qos** *qos-policy-map-name*	policy-map-name という名前のポリシー マップを作成するか、そのポリシー マップにアクセスし、ポリシー マップ モードを開始します。 ポリシー マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。ポリシー マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	**class** [**type qos**] {*class-map-name* | **class-default**}	class-map-name への参照を作成し、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。 ポリシー マップ内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。
ステップ 4	**set dscp** *dscp-value*	DSCP 値を dscp-value に設定します。 標準の DSCP 値の表を参照してください。
ステップ 5	**set qos-group** *y*	qos-group を指定します。 グループ値には 1 ～ 5 を指定できます。 （注） class-default システム クラス（qos-group 0）のトラフィックを DSCP でマーキングすることはできません。

次に、DSCP 値を 10 に設定し、qos-group を 2 に指定する例を示します。

```
policy-map type qos test-bulkdata
   class type qos bulkdata
```

```
set dscp 10
set qos-group 2
```

IP precedence マーキングの設定

IP precedence のフィールドの値を、サービス（ToS）フィールド、または IP ヘッダーの IPv6 の同等の [Traffic Class] フィールドの IPv4 タイプの 0 ～ 2 ビットに設定できます。 次の表に、優先順位値を示します。

（注） IP precedence と DSCP のいずれかの値は設定できますが、IP パケットの同じフィールドを変更するため、両方の値は設定できません。

表 7: 優先順位値

値	優先順位値の一覧
<0-7>	IP precedence 値
critical	クリティカル precedence（5）
flash	フラッシュ precedence（3）
flash-override	フラッシュ上書き precedence（4）
immediate	即時 precedence（2）
internet	インターネットワーク コントロール precedence（6）
network	ネットワーク コントロール precedence（7）
priority	優先 precedence（1）
routine	ルーチン precedence（0）

手順

	コマンドまたはアクション	目的
ステップ 1	**config t**	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	**policy-map** [**type qos**] *qos-policy-map-name*	policy-map-name という名前のポリシー マップを作成するか、そのポリシーマップにアクセスし、ポリシーマップ モードを開始します。 ポリシー マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。ポリシーマップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。
ステップ 3	**class** [**type qos**] {*class-map-name* | **class-default**}	class-map-name への参照を作成し、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。 ポリシーマップ内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。
ステップ 4	**set precedence** *precedence-value*	IP precedence 値を precedence-value に設定します。 優先順位値の表に示す値のいずれか 1 つを入力できます。

```
switch(config)# policy-map type qos my_policy
switch(config-pmap-qos)# class type qos my_class
switch(config-pmap-c-qos)# set precedence 5
switch(config-pmap-c-qos)#
```

CoS マーキングの設定

CoS フィールドの値は、IEEE 802.1Q ヘッダーの VLAN ID タグ フィールドの上位 3 ビットに記録されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config) # **policy-map** [**type network-qos**] *policy-map name*	*policy-map-name* という名前のポリシー マップを作成するか、そのポリシーマップにアクセスし、ポリシーマップ モードを開始します。 ポリシーマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。ポリシーマップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-pmap-nq) # **class** [**type network-qos**] {*class-map name* |**class-default**}	*class-map-name* への参照を作成し、ポリシー マップ クラス設定モードを開始します。 ポリシーマップ内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。
ステップ 4	switch(config-pmap-c-nq) # **set cos** *cos-value*	CoS 値を cos-value に指定します。 *cos-value* 値は、0 ～ 7 の範囲で指定します。 （注） このコマンドは、出力ポリシーに対してのみサポートされます。

レイヤ 3 トポロジの必須の CoS マーキング設定

レイヤ 3 トポロジでは、一意の cos 値でネットワーク QoS ポリシーに各 QoS グループ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	switch# **show policy-map system**	設定済みのポリシーマップおよびCoS値を表示します。 レイヤ 3 トポロジでは、各 qosgroup に一意の CoS 値が必要です。 **show policy-map system** コマンドを使用して、使用されている CoS 値と、QoS グループには使用できない CoS 値を表示します。
ステップ 2	switch# **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 3	switch(config) # **policy-map** [**type network-qos**] *policy-map name*	*policy-map-name* という名前のポリシー マップを作成するか、そのポリシーマップにアクセスし、ポリシーマップ モードを開始します。 ポリシー マップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。ポリシー マップ名は大文字と小文字が区別され、最大 40 文字まで設定できます。

	コマンドまたはアクション	目的
ステップ 4	switch(config-pmap-nq) # **class** [**type network-qos**] {*class-map name* |**class-default**}	class-map-name への参照を作成し、ポリシー マップ クラス設定モードを開始します。 ポリシー マップ内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。
ステップ 5	switch(config-pmap-nq-c) # **set cos** *cos-value*	CoS 値を指定します。 値の範囲は 0 ～ 7 です。 （注） このコマンドは出力ポリシーだけで使用できます。 レイヤ 3 トポロジでは、各 qos-group に固有の cos 設定が必要です。

次に、レイヤ 3 トポロジで、CoS 値を 4 に設定する例を示します。

```
switch# show policy-map system
  Type network-qos policy-maps
  ============================

  policy-map type network-qos pn-01
    class type network-qos cn-01      match qos-group 1
      mtu 8500
      pause no-drop
      set cos 2
    class type network-qos cn-02      match qos-group 2
      set cos 4
      mtu 9216
    class type network-qos cn-03      match qos-group 3
      mtu 8000
      set cos 6
    class type network-qos cn-04      match qos-group 4
      mtu 8750
      set cos 7
    class type network-qos cn-ip-multicast      match qos-group 5
      set cos 5
      mtu 7500
    class type network-qos class-default      match qos-group 0
      mtu 1500
      multicast-optimize
      set cos 1
...
switch# configure terminal
switch(config)# policy-map type network-qos pn-01
switch(config-pmap-nq)# class type network-qos cn-05
switch(config-pmap-c-nq)# set cos 3
```

マーキング設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show class-map	スイッチで定義されたクラスマップを表示します。
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。指定したポリシーだけを表示することもできます。
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 6 章

システムでの QoS の設定

この章の内容は、次のとおりです。

システム クラスの概要

システム クラス

システム qos は一種の MQC ターゲットです。 service-policy を使用して、ポリシー マップをシステム qos ターゲットに関連付けます。 特定のインターフェイスでサービス ポリシー設定を上書きしない限り、システム qos ポリシーはスイッチのインターフェイス全体に適用されます。 システム qos ポリシーは、システム クラスやスイッチ全体のトラフィック クラスのほか、それらの属性を定義するために使用します。 QoS 一貫性の確保（および設定の利便性）の目的で、デバイスは、Data Center Bridging Exchange（DCBX）プロトコルを使用して、システム クラス パラメータ値を接続されたすべてのネットワーク アダプタに配布します。

サービス ポリシーがインターフェイス レベルで設定されている場合、インターフェイス レベルのポリシーは常にシステム クラス設定またはデフォルト値よりも優先されます。

Cisco Nexus デバイスでは、システム クラスは qos-group 値によって一意に識別されます。 全体で 6 つのシステム クラスがサポートされています。 6 つのシステム クラスのうち 2 つはデフォルトで、必ずデバイスに存在します。 最大 4 つの追加システム クラスを管理者が作成できます。

デフォルトのシステム クラス

デバイスは、次のシステム クラスを提供します。

- ドロップ システム クラス

  デフォルトでは、すべてのユニキャストおよびマルチキャスト イーサネット トラフィックは、デフォルトのドロップ システム クラスに分類されます。 このクラスは qos-group 0 で識別されます。

  システムの起動時にこのクラスは自動的に作成されます（クラス名は CLI で **class-default** です）。 このクラスは削除できません。このデフォルト クラスに関連付けられた一致基準も変更できません。

（注） データ トラフィック（class-default）と FCoE トラフィック（class-fcoe）が同時にフローしているときに輻輳が発生した場合、キューイングのパーセンテージ設定が開始されます。

FCoE トラフィックは no-drop クラスであり、キューイング クラスによって割り当てられた帯域幅にポリシングされません。 FCoE トラフィックはロスレスメディアを想定しているため、ドロップすることはできません。 輻輳が発生すると、PFC フレームが FCoE の入力インターフェイスで生成されます。また、データ トラフィックが割り当てられた帯域幅を下回っていても、ドロップはデータ トラフィックでのみ行われます。

スループットを最適化するために、より長い期間、データ トラフィックの負荷を分散することができます。

MTU

Cisco Nexus デバイスはレイヤ 2 スイッチで、パケット フラグメンテーションをサポートしません。 入力インターフェイスと出力インターフェイスの間で最大伝送単位（MTU）の設定が一致していない場合、パケットが切り捨てられることがあります。

MTU を設定する場合は、次の注意事項に従ってください。

- MTU はシステム クラス単位で指定されます。 システム クラスではトラフィック クラスごとに異なる MTU を指定できますが、スイッチ全体のすべてのポートで矛盾しないようにする必要があります。 インターフェイスでは MTU を設定できません。
- ファイバ チャネルおよび FCoE ペイロード MTU は、スイッチで 2158 バイトです。 その結果、ファイバ チャネル インターフェイスの rxbufsize は 2158 バイトに固定されます。 Cisco Nexus デバイスが 2158 バイトではない rxbufsize をピアから受信すると、Exchange Link Parameter（ELP）ネゴシエーションに失敗し、リンクはアップ状態になりません。
- **system jumbomtu** コマンドを入力すると、システム内の MTU の上限が定義されます。 システム ジャンボ MTU のデフォルト値は 9216 バイトです。 最小 MTU は 2158 バイトで、最大 MTU は 9216 バイトです。
- システム クラス MTU はクラス内のすべてのパケットの MTU を設定します。 システム クラス MTU を、グローバル ジャンボ MTU よりも大きく設定できません。

- FCoE システム クラス（ファイバ チャネルおよび FCoE トラフィックの場合）のデフォルト MTU は 2158 バイトです。 この値は変更できません。
- スイッチは、DCBX をサポートするネットワーク アダプタに MTU 設定を送信します。

（注） MTU は DCBX の Converged Enhanced Ethernet（CEE）モードではサポートされません。

システム QoS の設定

システム サービス ポリシーの追加

service-policy コマンドは、システムのサービス ポリシーとしてシステム クラス ポリシー マップを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **system qos**	システム クラス 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	switch(config-sys-qos)# **service-policy type** {**network-qos** | **qos** | **queuing**} [**input** | **output**] *policy-name*	ポリシー マップをシステムのサービス ポリシーとして使用するよう指定します。 3 つのポリシー マップ コンフィギュレーション モードがあります。 • network-qos：ネットワーク全体（system qos）モード。 • qos：分類モード（システム qos の input またはインターフェイスの input のみ）。 • queuing：キューイング モード（システム qos およびインターフェイスの input と output）。

	コマンドまたはアクション	目的
		（注） デフォルトのポリシー マップ コンフィギュレーション モードはありません。**type** を指定してください。 **input** キーワードは、そのポリシー マップがインターフェイスの受信トラフィックに適用されることを示します。 **output** キーワードは、そのポリシー マップがインターフェイスの送信トラフィックに適用されることを示します。 qos ポリシーには **input** だけを、queuing ポリシーには **input** と **output** の両方を適用できます。
ステップ 4	switch(config-sys-qos)# **service-policy type** {**network-qos** | **qos** | **queuing**} [**input** | **output**] *fcoe default policy-name*	（任意） デフォルトの FCoE ポリシー マップをシステムのサービス ポリシーとして使用するよう指定します。 FCoE には次の 4 つの定義済みポリシー マップがあります。 • service-policy type qos input fcoe-default-in-policy • service-policy type queuing input fcoe-default-in-policy • service-policy type queuing output fcoe-default-out-policy • service-policy type network-qos fcoe-default-nq-policy （注） Cisco Nexus デバイスで FCoE をイネーブルにする前に、type qos、type network-qos、および type queuing の各ポリシー マップに、定義済みの FCoE ポリシー マップを追加する必要があります。

次の例は、no-drop イーサネット ポリシー マップをシステム クラスとして設定する方法を示しています。

```
switch(config)# class-map type network-qos ethCoS4
switch(config-cmap-nq)# match qos-group
switch(config-cmap-nq)# exit
switch(config)# policy-map type network-qos ethNoDrop
switch(config-pmap-nq)# class type network-qos ethCoS4
switch(config-pmap-c-nq)# pause no-drop
switch(config-pmap-c-nq)# exit
switch(config-pmap-nq)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos ethNoDrop
```

デフォルト システム サービス ポリシーの復元

新しいポリシーを作成して、それをシステム QoS コンフィギュレーションに追加した場合、コマンドの **no** フォームを入力して、デフォルト ポリシーを再適用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **system qos**	システム クラス 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	switch(config-sys-qos)# **no service-policy type qos input** *policy-map name*	分類モードのポリシーマップをリセットします。 このポリシー マップ設定はシステム qos 入力またはインターフェイス入力のみに使用します。
ステップ 4	switch(config-sys-qos)# **no service-policy type network-qos** *policy-map name*	ネットワーク全体のポリシー マップをリセットします。
ステップ 5	switch(config-sys-qos)# **no service-policy type queuing output** *policy-map name*	出力キューイング モードのポリシー マップをリセットします。
ステップ 6	switch(config-sys-qos)# **no service-policy type queuing input** *policy-map name*	入力キューイングモードのポリシーマップをリセットします。

次に、システム QoS 設定をリセットする方法の例を示します。

```
switch# configure terminal
switch(config)# system qos
switch(config-sys-qos)# no service-policy type qos input my-in-policy
switch(config-sys-qos)# no service-policy type network-qos my-nq-policy
switch(config-sys-qos)# no service-policy type queuing output my-out-policy
switch(config-sys-qos)# no service-policy type queuing input my-in-policy
```

指定したファブリック エクステンダのキュー制限の設定

ファブリック エクステンダ コンフィギュレーション レベルで、出方向（ネットワークからホストへ）の指定ファブリック エクステンダのキュー制限を制御できます。 ファブリック エクステンダに低いキュー制限値を使用することにより、1 つのブロックされたレシーバが他の非輻輳レシーバに送信されるトラフィックに影響を与えること（「行頭ブロッキング」）を防止できます。より高いキュー制限値では、バースト吸収が改善され、行頭ブロッキング保護が少なくなります。ファブリック エクステンダがすべての使用可能なハードウェア領域を使用できるようにするには、このコマンドの **no** 形式を使用します。

（注） システム レベルで、**fex queue-limit** コマンドを使用してファブリック エクステンダのキュー制限を設定できます。 ただし、特定のファブリック エクステンダのキュー制限を設定すると、そのファブリック エクステンダのシステム レベルで設定されたキュー制限設定が上書きされます。

次のファブリック エクステンダのキュー制限を指定できます。

- Cisco Nexus 2148T ファブリック エクステンダ（48x1G 4x10G SFP+ モジュール）
- Cisco Nexus 2224TP ファブリック エクステンダ（24x1G 2x10G SFP+ モジュール）
- Cisco Nexus 2232P ファブリック エクステンダ（32x10G SFP+ 8x10G SFP+ モジュール）
- Cisco Nexus 2248T ファブリック エクステンダ（48x1G 4x10G SFP+ モジュール）
- Cisco Nexus N2248TP-E ファブリック エクステンダ（48x1G 4x10G モジュール）

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **fex** *fex-id*	ファブリック エクステンダを指定し、ファブリック エクステンダ モードを開始します。
ステップ 3	switch(config-fex)# **hardware** *fex_card_type* **queue-limit** *queue-limit*	指定ファブリック エクステンダのキュー制限を設定します。 キュー制限はバイト単位で指定します。 有効な範囲は、Cisco Nexus 2148T ファブリック エクステンダの場合は 81920 ～ 652800、その他すべてのサポート対象のファブリック エクステンダの場合は 2560 ～ 652800 です。

次に、Cisco Nexus 2248T ファブリック エクステンダのデフォルト キュー制限を復元する例を示します。

```
switch# configure terminal
switch(config-if)# fex 101
switch(config-fex)# hardware N2248T queue-limit 327680
```

次に、Cisco Nexus 2248T ファブリック エクステンダ上でデフォルトで設定されているキュー制限を削除する例を示します。

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no hardware N2248T queue-limit 327680
```

ジャンボ MTU のイネーブル化

スイッチ全体のジャンボ最大伝送単位（MTU）は、デフォルトのイーサネット システム クラス（class-default）のポリシー マップで MTU を最大サイズ（9216 バイト）に設定することによって、イネーブルにできます。

Cisco Nexus デバイスのレイヤ 3 ルーティングでは、下のグローバルな QoS 設定に加えて、レイヤ 3 インターフェイス（IP アドレスを持つ SVI および物理インターフェイス）の MTU を設定する必要があります。

次の例は、ジャンボ MTU をサポートするようにデフォルトのイーサネット システム クラスを設定する方法を示しています。

```
switch(config)# policy-map type network-qos jumbo
switch(config-pmap-nq)# class type network-qos class-default
switch(config-pmap-c-nq)# mtu 9216
switch(config-pmap-c-nq)# exit
switch(config-pmap-nq)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos jumbo
```

（注） **system jumbomtu** コマンドは、スイッチの最大 MTU サイズを定義します。 ただし、ジャンボ MTU は MTU が設定されたシステム クラスだけにサポートされます。

ジャンボ MTU の確認

Cisco Nexus デバイスでは、トラフィックは 8 つの QoS グループのいずれか 1 つに分類されます。 MTU は、QoS グループ レベルで設定されます。 デフォルトでは、すべてのイーサネット トラフィックは、QoS グループ 0 にあります。 イーサネット トラフィックに対するジャンボ MTU を確認するには、**show queueing interface ethernet** *slot/chassis_number* コマンドを使用し、コマンド出力の「HW MTU」で QoS グループ 0 の MTU を確認します。 値は 9216 である必要があります。

show interface コマンドは、MTU サイズとして 1500 を常に表示します。 Cisco Nexus デバイスでは、異なる QoS グループで異なる MTU をサポートしているため、インターフェイス レベルで MTU を 1 つの値で表すことはできません。

（注） Cisco Nexus デバイスでのレイヤ 3 ルーティングでは、グローバル QoS MTU に加えて、レイヤ 3 インターフェイス（IP アドレスを持つ SVI および物理インターフェイス）の MTU を確認する必要があります。 **show interface vlan** *vlan_number* または **show interface** *slot/chassis_number* を使用して、レイヤ 3 MTU を確認できます。

次に、Ethernet 1/19 のジャンボ MTU 情報を表示する例を示します。

```
switch# show queuing interface ethernet1/19
Ethernet1/19 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR             50
```

```
      1       WRR             50

RX Queuing
  qos-group 0
  q-size: 243200, HW MTU: 9280 (9216 configured)
  drop-type: drop, xon: 0, xoff: 1520
  Statistics:
      Pkts received over the port             : 2119963420
      Ucast pkts sent to the cross-bar        : 2115648336
      Mcast pkts sent to the cross-bar        : 4315084
      Ucast pkts received from the cross-bar  : 2592447431
      Pkts sent to the port                   : 2672878113
      Pkts discarded on ingress               : 0
      Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

  qos-group 1
  q-size: 76800, HW MTU: 2240 (2158 configured)
  drop-type: no-drop, xon: 128, xoff: 240
  Statistics:
      Pkts received over the port             : 0
      Ucast pkts sent to the cross-bar        : 0
      Mcast pkts sent to the cross-bar        : 0
      Ucast pkts received from the cross-bar  : 0
      Pkts sent to the port                   : 0
      Pkts discarded on ingress               : 0
      Per-priority-pause status               : Rx (Inactive), Tx (Inactive)

Total Multicast crossbar statistics:
  Mcast pkts received from the cross-bar      : 80430744
```

システム QoS 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show policy-map system	システム QoS に結合されたポリシー マップ設定を表示します。
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。指定したポリシーだけを表示することもできます。
show class-map	スイッチで定義されたクラスマップを表示します。
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 7 章

インターフェイスでの QoS の設定

この章の内容は、次のとおりです。

インターフェイス QoS の概要

信頼境界

信頼境界は、次のように着信インターフェイスによって実行されます。

- すべてのファイバチャネルおよび仮想ファイバチャネルインターフェイスは、FCoE システム クラスに自動的に分類されます。
- デフォルトでは、すべてのイーサネットインターフェイスは信頼できるインターフェイスです。マーキングが設定されている場合を除き、802.1p CoS および DSCP は保持されます。CoS および DSCP のデフォルトのキューマッピングはありません。 これらのマッピングを作成するポリシーを定義し、適用できます。 デフォルトでは、ユーザ定義のポリシーがない場合、すべてのトラフィックがデフォルト キューに割り当てられます。
- 802.1p CoS 値でタグ付けされていないパケットは、デフォルトのドロップ システム クラスに分類されます。 タグなしパケットがトランク上で送信される場合、このパケットにはデフォルトのタグなし CoS 値 0 がタグ付けされます。
- イーサネット インターフェイスまたはポート チャネルのデフォルトのタグなし Cos 値は上書きできます。
- イーサネット インターフェイスまたはポート チャネル インターフェイスのデフォルトのタグなし Cos 値を上書きするには、**untagged cos** *cos-value* コマンドを使用します。

- イーサネットまたはレイヤ 3 インターフェイスまたはポート チャネル インターフェイスのデフォルトのタグなし CoS 値を上書きするには、**untagged cos** *cos-value* コマンドを使用します。

システムがタグなし CoS 値を適用しても、QoS は、CoS 値がタグ付けされたシステムに入るパケットと同様に機能します。

ファイバ チャネル インターフェイスのポリシー

出力キューは、ネイティブ ファイバ チャネル インターフェイスに設定できません。 次のように 2 つのキューが使用できます。

- ハイプライオリティ制御トラフィックを処理する完全プライオリティ キュー。
- すべてのデータ トラフィックとロー プライオリティ制御トラフィックを処理するキュー。

マルチキャスト トラフィックの QoS

Cisco Nexus デバイスには、インターフェイスごとに 128 のマルチキャスト入力キューがあります。 各スイッチには、システム クラスごとに 1 つのキューが割り当てられます。

デフォルトでは、すべてのマルチキャストイーサネットトラフィックは、デフォルトのドロップ システム クラスに分類されます。 このトラフィックは、1 つのマルチキャスト キューで処理されます。

最適化マルチキャスティングにより、未使用のマルチキャスト キューを使用して、マルチキャストフレームのスループットを向上させることができます。 最適化マルチキャストがデフォルトのドロップ システム クラスでイネーブルにされると、システムはマルチキャスト トラフィックを処理するため、6 つのキューすべてを使用します。 最適化マルチキャストがデフォルトのドロップ システム クラスでイネーブルにされると、6 つすべてのキューには同等のプライオリティが与えられます。

新しいシステムクラスを定義すると、専用のマルチキャストキューがこのクラスに割り当てられます。 このキューは、最適化マルチキャストクラスで利用できるキューのセットから除外されます。

システムは、ブロードキャストトラフィックまたはマルチキャストトラフィックを照合するための定義済みのクラス マップを 2 つ備えています。 これらのクラス マップは、ユニキャスト トラフィックとマルチキャスト トラフィックに別々のポリシー マップを作成する場合に便利です。

定義済みのクラス マップは、次のとおりです。

class-all-flood

class-all-flood クラス マップは、すべてのブロードキャスト トラフィック、マルチキャスト トラフィック、および未知のユニキャスト トラフィックを（すべての Cos 値で）照合します。 class-all-flood クラス マップでポリシー マップを設定した場合、システムはこのトラフィックに利用できるすべてのマルチキャスト キューを自動的に使用します。

class-ip-multicast

class-ip-multicast クラスマップは、すべての IP マルチキャスト トラフィックを照合します。 このクラス マップに設定されたポリシー オプションが、すべてのイーサネット CoS 値でトラフィックに適用されます。 たとえば、このクラスの最適化マルチキャストをイネーブルにすると、IP マルチキャスト トラフィックはすべての CoS 値で最適化されます。

（注） これら定義済みのクラス マップのいずれかを no-drop クラスとして設定すると、プライオリティ フロー制御機能がすべてのイーサネット CoS 値に適用されます。 この設定では、ポーズがユニキャスト トラフィックおよびマルチキャスト トラフィックに適用されます。

インターフェイス QoS の設定

タグなし CoS の設定

802.1p CoS 値でタグ付けされていない着信パケットは、デフォルトのタグなし CoS 値（0）に割り当てられます（これはデフォルトのイーサネット ドロップ システム クラスにマッピングされます）。 イーサネットまたは EtherChannel インターフェイスのデフォルトのタグなし Cos 値は上書きできます。

レイヤ 2 またはレイヤ 3 インターフェイスにフロー制御を設定できます。 レイヤ 3 インターフェイスを設定するには、**no switchport** コマンドを使用します。

Cisco Nexus デバイスでは、同じインターフェイスに QoS タイプのポリシー マップおよびタグなし CoS を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	指定されたインターフェイスまたはポートチャネルの設定モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **no switchport**	（任意） レイヤ 3 インターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **untagged cos** *cos-value*	タグなし CoS 値を設定します。 指定できる値は 1 ～ 7 です。

次に、インターフェイスで受信するタグなしフレームに CoS 値 4 を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# untagged cos 4
```

次に、レイヤ 3 インターフェイスで受信するタグなしフレームに CoS 値 3 を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if) no switchport
switch(config-if)# untagged cos 3
switch(config-if)#
```

インターフェイス サービス ポリシーの設定

入力 qos ポリシーは、イーサネット インターフェイスの着信トラフィックに適用される分類用のサービス ポリシーです。 type queuing の場合、出力ポリシーは、指定されたクラスに一致するすべての発信トラフィックに適用されます。 インターフェイスまたは EtherChannel で入力キューイング ポリシーを設定すると、スイッチは DCBX プロトコルを使用して設定データをアダプタに送信します。

（注） type qos ポリシーは、Cisco Nexus デバイス インターフェイスおよび Cisco Nexus ファブリック エクステンダ インターフェイスだけでアクティブにできます。 ファブリック エクステンダ ファブリック インターフェイスまたはファブリック エクステンダ ファブリック EtherChannel インターフェイスでは、Cisco NX-OS CLI で設定を拒否しなくても type qos ポリシーは使用されません。

ハードウェア リソースを浪費しないために、ファブリック エクステンダ ファブリック インターフェイスまたは ファブリック エクステンダ ファブリック EtherChannel インターフェイスで type qos ポリシー マップを設定しないことを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	指定したインターフェイスの設定モードを開始します。 （注） ポート チャネルのサービス ポリシーはすべてのメンバーインターフェイスに適用されます。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **service-policy** [**type** {**qos** | **queuing**}] [**input** | **output**]*policy-name*	ポリシー マップをシステムのサービス ポリシーとして使用するよう指定します。 2 つのポリシー マップ コンフィギュレーション モードがあります。 • qos：分類モード。これがデフォルト モードです。 • queuing：キューイング モード。 （注） **input** キーワードは、そのポリシー マップがインターフェイスの受信トラフィックに適用されることを示します。 **output** キーワードは、そのポリシーマップがインターフェイスの送信トラフィックに適用されることを示します。 qos ポリシーには **input** だけを、queuing ポリシーには **input** と **output** の両方を適用できます。
ステップ 4	switch(config-if)# **service-policy input** *policy-name*	インターフェイスにポリシー マップを適用します。 （注） 制約事項として、システム type qos ポリシーは、インターフェイスや EtherChannel に適用される type qos ポリシーと同じものにできません。

次の例は、イーサネット インターフェイスにポリシーを適用する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type qos input policy1
```

レイヤ 3 インターフェイスのサービス ポリシーの設定

レイヤ 3 インターフェイスのサービス ポリシーを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface ethernet** *slot*/*port*	指定したインターフェイスの設定モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **no switchport**	レイヤ 3 インターフェイスを選択します。
ステップ 4	switch(config-if)# **service-policy** [**type** {**qos** | **queuing**} [**input** | **output**]*policy-name*	ポリシー マップをレイヤ 3 インターフェイスのサービス ポリシーとして使用するように指定します。 2 つのポリシー マップ コンフィギュレーション モードがあります。 • qos：分類モード（これはデフォルト モードです）。 • queuing：キューイング モード。 （注） **input** キーワードは、そのポリシー マップがインターフェイスの受信トラフィックに適用されることを示します。 **output** キーワードは、そのポリシー マップがインターフェイスの送信トラフィックに適用されることを示します。qos ポリシーには **input** だけを、queuing ポリシーには **input** と **output** の両方を適用できます。

次に、キューイング ポリシー マップをレイヤ 3 インターフェイスに関連付ける例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# service-policy type queuing output my_output_q_policy
switch(config-if)#
```

次に、入力 qos ポリシー マップをレイヤ 3 インターフェイスに付加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# service-policy type qos input my_input_qos_policy
switch(config-if)#
```

ユニキャストおよびマルチキャストトラフィックに割り当てられた帯域幅の変更

重み付けラウンドロビン（WRR）の重み付けをインターフェイスデータ レートの割合（%）として出力キューに割り当てることにより、ユニキャストおよびマルチキャスト トラフィックに割り当てられた帯域幅を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface ethernet** *slot*/*port*	指定されたインターフェイスのコンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **wrr unicast-bandwidth** percentage-value	ユニキャストおよびマルチキャスト トラフィックに割り当てられたトラフィック輻輳時の帯域幅を変更します。 帯域幅値のパーセンテージ範囲は 0 ～ 100% です。

次に、キューイング ポリシー マップをレイヤ 3 インターフェイスに関連付ける例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# wrr unicast-bandwidth 75
switch(config-if)#
```

インターフェイス QoS 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show class-map	スイッチで定義されたクラスマップを表示します。
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。 指定したポリシーだけを表示することもできます。

コマンド	目的
show policy-map interface [*interface number*]	1つまたはすべてのインターフェイスのポリシーマップ設定を表示します。
show queuing interface *[interface slot/\port*]	キューの設定および統計情報を表示します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface flowcontrol [**module** *numbef*]	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。
show interface [*interface slot/port*] **priority-flow-control** [**module** *number*]	指定されたインターフェイスのプライオリティフロー制御詳細を表示します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface untagged-cos [**module** *number*]	すべてのインターフェイスのタグなし CoS 値を表示します。
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 8 章

VLAN での QoS の設定

この章の内容は、次のとおりです。

VLAN QoS の概要

Cisco Nexus デバイスでは、VLAN での分類およびマーキング用の Quality of Service（QoS）ポリシーを設定できます。 VLAN に適用されるポリシーは、VLAN のレイヤ 2 およびスイッチ仮想インターフェイス（SVI）ポートのトラフィックに適用されます。

QoS ポリシーの優先順位

QoS ポリシーのマーキング要件によって優先順位が決まります。 インターフェイス QoS ポリシーが最優先され、VLAN QoS ポリシーがその次になり、システム QoS ポリシーが最も低い優先順位になります。

ただし、VLAN に VLAN QoS ポリシーと VLAN ACL（VACL）の両方が割り当てられている場合、VACL が最優先されます。

インターフェイス、システム、および VLAN ポリシーの優先順位例

次に、CoS 5 のインターフェイス 1/1 のトラフィックが qos-group 3 に送信される設定例を示します。 VLAN 10 および CoS 5 の他のインターフェイスのトラフィックは qos-group 4 に送信されます。 VLAN 10 および CoS 5 以外のインターフェイスのトラフィックは qos-group 5 に送信されます。

```
class-map type qos match-all cm1
  match cos 5
policy-map type qos pm-ifc
  class cm1
    set qos-group 3
  class class-default
policy-map type qos pm-vlan
  class cm1
    set qos-group 4
  class class-default
policy-map type qos pm-sys
  class cm1
    set qos-group 5
  class class-default

system qos
  service-policy type qos input pm-sys
vlan configuration 10
  service-policy type qos input pm-vlan
interface Ethernet1/1
  service-policy type qos input pm-ifc
```

インターフェイスおよびシステム QoS ポリシーの優先順位例

次に、CoS 5 のインターフェイス 1/1 のトラフィックが qos-group 3 に送信される設定例を示します。 CoS 5 の他のインターフェイスのトラフィックは qos-group 5 に送信されます。

```
class-map type qos match-all cm1
  match cos 5
policy-map type qos pm-ifc
  class cm1
    set qos-group 3
  class class-default
policy-map type qos pm-sys
  class cm1
    set qos-group 5
  class class-default

system qos
  service-policy type qos input pm-sys

interface Ethernet1/1
  service-policy type qos input pm-ifc
```

システムおよび VLAN ポリシーの優先順位例

次に、CoS 5 の VLAN 10 のトラフィックが qos-group 4 に送信される設定例を示します。 CoS 5 の他の VLAN のトラフィックは qos-group 5 に送信されます。

```
class-map type qos match-all cm1
```

```
  match cos 5
policy-map type qos pm-vlan
  class cm1
    set qos-group 4
  class class-default
policy-map type qos pm-sys
  class cm1
    set qos-group 5
  class class-default

system qos
  service-policy type qos input pm-sys
vlan configuration 10
  service-policy type qos input pm-vlan
```

VLAN QoS および VACL ポリシーの優先順位例

この例では、送信元 IP アドレスが 10.10.10.1 のパケットはドロップされます。 ただし、VLAN 10 および CoS 5 の他のパケットは qos-group 4 に送信されます。

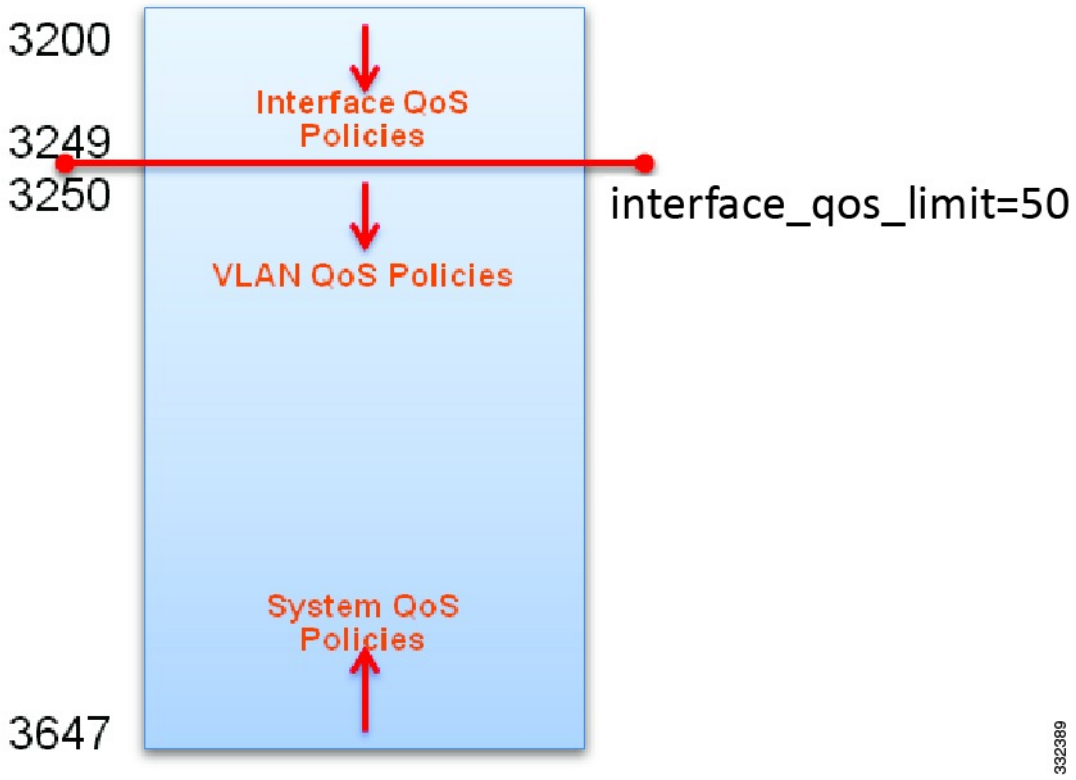
```
ip access-list al1
  10 permit ip 10.10.10.1/24 any
vlan access-map v-am1
  match ip address al1
  action drop
vlan filter v-am1 vlan-list 10

class-map type qos match-all cm1
  match cos 5
policy-map type qos pm-vlan
  class cm1
    set qos-group 4
  class class-default

vlan configuration 10
  service-policy type qos input pm-vlan
```

VLAN QoS の TCAM エントリの制限

QoS TCAM リージョンは、インターフェイス QoS、システム QoS、および VLAN QoS ポリシーによって共有されます。 VLAN QoS ポリシーを定義するために、インターフェイス QoS ポリシーの

TCAMエントリの数を制限する必要があります。 この制限を設定するには、**hardware profile tcam feature interface-qos limit** *tcam-size* を使用します。

図 *1*：*QoS TCAM* リージョン



VLAN QoS の注意事項および制約事項

- VLAN には、設定するサービス ポリシーに対して少なくとも 1 個のアクティブ メンバ ポートが必要です。 VLANに少なくとも1個のアクティブ メンバがない場合にサービスポリシーを設定すると、設定は受け入れられますが、TCAM はプログラミングされません。
- **no vlan** *number* コマンドを使用して VLAN を削除した場合、その VLAN に設定されたサービス ポリシーは残りますが、非アクティブになります。
- TCAM には VLAN でのサービス ポリシーの設定に十分な空きエントリが必要です。
- ロールバックは、インターフェイス QoS 制限がロール バック設定と実行コンフィギュレーションで異なる場合は、失敗する可能性があります。
- QoS ポリシーが設定された VLAN が QoS ポリシーがないインターフェイスで設定されている場合、**show policy-map interface** *number* コマンドは VLAN 上に設定された QoS ポリシーを表示しません。

- インターフェイス QoS 制限を変更する前に、すべてのインターフェイスの QoS ポリシーを削除します。

VLAN QoS の設定

インターフェイス QoS TCAM 制限の設定または変更

interface_qos_limit を特定の数に設定する場合、すべての ASIC の TCAM の QoS リージョンにその数のオフセットを超えるインターフェイス ポリシーを設定することはできません。 たとえば、interface_qos_limit を 1000 に設定する場合、すべての ASIC の TCAM の QoS リージョンにオフセット 1000 を超えるインターフェイス ポリシーを設定できません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **hardware profile tcam feature interface-qos limit** *tcam-size*	インターフェイス QoS TCAM 制限を設定します。 *tcam-size* の範囲は 7 ～ 446 エントリです。
ステップ 3	switch(config)# **show hardware profile tcam feature qos**	QoS TCAM の制限を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、インターフェイス QoS TCAM 制限を 20 エントリに設定する例を示します。

```
switch(config)# configure terminal
switch(config)# hardware profile tcam feature interface-qos limit 20
switch(config)# show hardware profile tcam feature qos
Feature                  Limit (number of tcam entries)
-------------------------------------------------------
interface-qos              20
vlan-qos + global-qos     428

switch(config)# copy running-config startup-config
```

TCAM からのインターフェイス QoS 制限の削除

はじめる前に

- すべての VLAN QoS ポリシーを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **show hardware profile tcam feature qos**	QoS TCAM の制限を表示します。
ステップ 3	switch(config)# **no hardware profile tcam feature interface-qos limit** *tcam-size*	インターフェイス QoS TCAM 制限を設定します。 *tcam-size* の範囲は 7 ～ 446 エントリです。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、インターフェイス QoS TCAM 制限を削除する例を示します。

```
switch(config)# configure terminal
switch(config)# show hardware profile tcam feature qos
Feature                  Limit (number of tcam entries)
-------------------------------------------------------
interface-qos              20
vlan-qos + global-qos     428

switch(config)# no hardware profile tcam feature interface-qos limit 20
switch(config)# copy running-config startup-config
```

VLAN のサービス ポリシーの設定

はじめる前に

- インターフェイス QoS 制限を設定する必要があります。
- ポリシー マップを設定する必要があります。
- TCAM には VLAN でのサービス ポリシーの設定に十分な空きエントリが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **vlan configuration** *vlan-number*	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。 *vlan-number* の範囲は 1 ～ 4094 です。
ステップ 3	switch(config-vlan)# **service-policy type qos input** *policy-name*	VLAN にポリシー マップを割り当てます。 *policy-name* は、ポリシー マップに割り当てられた名前です。 名前には最大 40 文字までの英数字を指定できます。
ステップ 4	switch(config-vlan)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、サービス ポリシーを作成し、VLAN 10 に割り当てる例を示します。

```
switch# configure terminal
switch(config)# class-map type qos cm1
switch(config-cmap-qos)# match cos 5
switch(config-cmap-qos)# policy-map type qos pm-vlan
switch(config-pmap-qos)# class cm1
switch(config-pmap-c-qos)# set qos-group 4
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
switch(config)# vlan configuration 10
switch(config-vlan-config)# service-policy type qos input pm-vlan
switch(config-vlan-config)#
```

VLAN からのサービス ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **vlan configuration** *vlan-number*	指定された VLAN の VLAN コンフィギュレーション モードが開始されます。 *vlan-number* の範囲は 1 ～ 4094 です。
ステップ 3	switch(config-vlan-config)#**no service-policy type qos input** *policy-name*	VLAN からポリシーを削除します。 *policy-name* は、ポリシーマップに割り当てられた名前です。名前には最大 40 文字までの英数字を指定できます。
ステップ 4	switch(config-vlan-config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、VLAN 10 から pm-vlan ポリシー マップを削除する例を示します。

```
swtich# configure terminal
switch(config)# vlan configuration 10
switch(config-vlan-config)# no service-policy type qos input pm-vlan
switch(config-vlan-config)# copy running-config startup-config
```

VLAN QoS 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show policy-map vlan *vlan-number*	指定する VLAN に設定されている QoS ポリシーを表示します。
show policy-map [*name*]	スイッチで定義されたポリシーマップを表示します。 指定したポリシーだけを表示することもできます。
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

VLAN QoS 機能の履歴

表 *8* : ***VLAN QoS*** 機能の履歴

機能名	リリース	機能情報
VLAN QoS	5.1(3)N2(1)	この機能が導入されました。

第 9 章

キューイングおよびフロー制御の設定

この章の内容は、次のとおりです。

キューの概要

入力キューイング ポリシー

入力ポリシー マップをイーサネット インターフェイスに関連付けて、指定されたトラフィック クラスの帯域幅を確保したり、プライオリティ キューを指定したりできます。

アダプタの入力ポリシーは、指定された Cos 値と一致するすべての発信トラフィックに適用されます。

インターフェイスの入力ポリシーを設定すると、スイッチはアダプタに設定データを送信します。アダプタが DCBX プロトコルや入力ポリシー Type-Length-Value（TLV）をサポートしていない場合、入力ポリシーの設定は無視されます。

出力キューイング ポリシー

出力ポリシーマップをイーサネットインターフェイスにアソシエートし、指定されたトラフィック クラスの帯域幅を保証したり、出力キューを設定したりできます。

帯域割り当ての制限は、FCoE トラフィックなど、インターフェイス上のすべてのトラフィックに適用されます。

イーサネット インターフェイスごとに最大 8 つのキュー（システム クラスごとに 1 つ）をサポートします。 キューには次のデフォルト設定があります。

- これらのキューに加え、CPU に転送される制御トラフィックは完全プライオリティ キューを使用します。 ユーザ設定ではこのキューにはアクセスできません。
- FCoE トラフィック（FCoE システム クラスにマッピングされるトラフィック）にキューが割り当てられます。 このキューは、帯域幅の 50% で重み付けラウンドロビン（WRR）スケジューリングを使用します。
- デフォルトのドロップ システム クラスの標準イーサネット トラフィックにキューが割り当てられます。 このキューは、帯域幅の 100 % で WRR スケジューリングを使用します。

システム クラスを追加すると、キューがクラスに割り当てられます。影響を受けたすべてのインターフェイスで帯域割り当てを再設定する必要があります。 帯域幅は、自動的にユーザ定義のシステム クラス専用にはなりません。

設定可能な完全プライオリティ キューは 1 つです。 このキューは、制御トラフィック キュー（データ トラフィックではなく制御トラフィックを伝送）以外の他のすべてのキューより先に処理されます。

Cisco Nexus デバイスのバッファとキューの制限

Cisco Nexus デバイスでは、ポートごとのパケット バッファは 640KB です。 ASIC 単位のすべてのポートでの入力は 16MB です。 ASIC 単位のすべてのポートでの出力は 9MB です。

Cisco Nexus デバイスには、ポートごとに次のデフォルトのバッファ割り当てがあります。

表 *9*：ポートごとの *Cisco Nexus* デバイスのデフォルトのバッファ割り当て

トラフィック クラス	入力バッファ サイズ（KB）
10G ポートに対する 300M の class-fcoe	161.25
40G ポートに対する 300M の class-fcoe	182.5
10G ポートに対する 3000M の class-fcoe	412.5
40G ポートに対する 3000M の class-fcoe	1300
10G ポートに対する 300M のユーザ定義の no-drop	160
40G ポートに対する 300M のユーザ定義の no-drop	181.25
10G ポートに対する 3000M のユーザ定義の no-drop	411.875

トラフィック クラス	入力バッファ サイズ（KB）
40G ポートに対する 3000M のユーザ定義の no-drop	1298.125

デフォルトのバッファ割り当てはクラスのタイプによって異なります。 たとえば、通常のテールドロップ トラフィック クラスを作成するときのデフォルトの割り当ては、**queue-limit** コマンドを使用して大規模なサイズを指定しない場合、22.7KB です。

network-qos policy-map から、user-created qos-group に使用可能な入力バッファ スペースを増やすには、**queue-limit** コマンドを使用します。

各ユーザ作成 qos-group に割り当てられる入力バッファに加えて、qos-group ごとに出力で必要になる追加の 28.6KB バッファがあります。

デフォルトの QoS 設定では、使用可能なすべてのバッファ（470KB）が class-default に割り当てられます。 新しい qos-group を作成すると、新しい qos-group に必要なバッファが class-default から削除されます。 class-default に残されるバッファ サイズは、470 から他の qos-group で使用される入力バッファを減算し、さらにそれから 28.6KB を減算したものに、qos-group の数を乗算したものと同じになります。

（注） 各新規クラスにはさらに 28.6KB が必要になるため、class default に残っているバッファの正確な量は、478 から他の qos-group によって使用されるバッファを減算し、さらにそれから 18.880KB を減算したものに qos-group の数を乗算したものと同じになります。

Cisco Nexus デバイスのデフォルト QoS ポリシーは、class-fcoe を作成せず、FCoE トラフィック用にバッファおよび qos-group を予約しません。

show queuing interface コマンドは、qos-group ごとに割り当てられた入力バッファの量を表示できます。

フロー制御の概要

リンク レベル フロー制御

IEEE 802.3x リンク レベル フロー制御により、輻輳レシーバはリンクのもう一方の端にあるトランスミッタと通信して、短時間の間データの転送を停止できます。 リンク レベル フロー制御機能は、リンク上のすべてのトラフィックに適用されます。

送受信方向は個別に設定できます。 デフォルトでは、リンク レベル フロー制御は両方向でディセーブルです。

Cisco Nexus デバイスでは、イーサネット インターフェイスはリンク レベル フロー制御機能を自動検出しません。 イーサネット インターフェイスでこの機能を明示的に設定する必要があります。

各イーサネットインターフェイスで、スイッチはプライオリティフロー制御またはリンクレベルフロー制御のいずれか（両方は不可）をイネーブルにできます。

プライオリティ フロー制御

プライオリティ フロー制御（PFC）により、ポーズ機能をリンク上のすべてのトラフィックではなく、リンク上の特定のトラフィック クラスに適用できます。 PFC は、IEEE 802.1p CoS 値に基づいて、ポーズ機能を適用します。 スイッチが PFC をイネーブルにすると、ポーズ機能を適用する CoS 値をアダプタに伝えます。

イーサネットインターフェイスは PFC を使用して、ロスレス サービスを no-drop システム クラスに提供します。 PFC はクラス単位でポーズ フレームを実装し、IEEE 802.1p CoS 値を使用してロスレス サービスを必要とするクラスを特定します。

スイッチにおいて各システム クラスには、関連付けられた IEEE 802.1p CoS 値があります。この CoS 値はデフォルトで割り当てられるか、システム クラスで設定されます。 PFC をイネーブルにすると、スイッチは no-drop CoS 値をアダプタに送信し、PFC をこれらの CoS 値に適用します。

FCoE システム クラスのデフォルトの CoS 値は 3 です。 この値は設定可能です。

デフォルトでは、スイッチは PFC 機能をイネーブルにするためのネゴシエーションを行います。ネゴシエーションが成功すると、設定に関係なく、PFC はイネーブルになり、リンクレベル フロー制御はディセーブルのままです。 PFC ネゴシエーションに失敗した場合は、PFC をインターフェイスで強制的にイネーブルにするか、IEEE 802.x リンクレベル フロー制御をイネーブルにできます。

PFC をインターフェイスでイネーブルにしていない場合、IEEE 802.3X リンクレベル ポーズをイネーブルにできます。 デフォルトでは、リンクレベル ポーズはディセーブルです。

キューイングの設定

指定したファブリック エクステンダのキュー制限の設定

ファブリック エクステンダ コンフィギュレーション レベルで、出方向（ネットワークからホストへ）の指定ファブリック エクステンダのキュー制限を制御できます。 ファブリック エクステンダに低いキュー制限値を使用することにより、1 つのブロックされたレシーバが他の非輻輳レシーバに送信されるトラフィックに影響を与えること（「行頭ブロッキング」）を防止できます。より高いキュー制限値では、バースト吸収が改善され、行頭ブロッキング保護が少なくなります。ファブリック エクステンダがすべての使用可能なハードウェア領域を使用できるようにするには、このコマンドの **no** 形式を使用します。

（注） システム レベルで、**fex queue-limit** コマンドを使用してファブリック エクステンダのキュー制限を設定できます。 ただし、特定のファブリック エクステンダのキュー制限を設定すると、そのファブリック エクステンダのシステム レベルで設定されたキュー制限設定が上書きされます。

次のファブリック エクステンダのキュー制限を指定できます。

- Cisco Nexus 2148T ファブリック エクステンダ（48x1G 4x10G SFP+ モジュール）
- Cisco Nexus 2224TP ファブリック エクステンダ（24x1G 2x10G SFP+ モジュール）
- Cisco Nexus 2232P ファブリック エクステンダ（32x10G SFP+ 8x10G SFP+ モジュール）
- Cisco Nexus 2248T ファブリック エクステンダ（48x1G 4x10G SFP+ モジュール）
- Cisco Nexus N2248TP-E ファブリック エクステンダ（48x1G 4x10G モジュール）

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **fex** *fex-id*	ファブリック エクステンダを指定し、ファブリック エクステンダ モードを開始します。
ステップ 3	switch(config-fex)# **hardware** *fex_card_type* **queue-limit** *queue-limit*	指定ファブリック エクステンダのキュー制限を設定します。 キュー制限はバイト単位で指定します。 有効な範囲は、Cisco Nexus 2148T ファブリック エクステンダの場合は 81920 ～ 652800、その他すべてのサポート対象のファブリック エクステンダの場合は 2560 ～ 652800 です。

次に、Cisco Nexus 2248T ファブリック エクステンダのデフォルト キュー制限を復元する例を示します。

```
switch# configure terminal
switch(config-if)# fex 101
switch(config-fex)# hardware N2248T queue-limit 327680
```

次に、Cisco Nexus 2248T ファブリック エクステンダ上でデフォルトで設定されているキュー制限を削除する例を示します。

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no hardware N2248T queue-limit 327680
```

no-drop バッファしきい値の設定

3000m ロスレス イーサネットの no-drop バッファしきい値を設定できます。

（注） 両方向でロスレス イーサネットを実現するためには、Cisco Nexus デバイスに接続されているデバイスに同様の機能が必要です。 no-drop 用のデフォルトのバッファおよびしきい値により、最大 300 メートルまでロスレス イーサネットを保証できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map type network-qos** *policy-map name*	policy-map network-qos クラス モードを開始し、type network-qos ポリシー マップに割り当てられたポリシー マップを特定します。
ステップ 3	switch(config-pmap-nq)# **class type network-qos** *class-map name*	ポリシー マップの既存のネットワーク QoS クラスマップを参照し、クラスモードを開始します。
ステップ 4	switch(config-pmap-nq-c)# **pause no-drop buffer-size** *buffer-size* **pause-threshold** *xoff-size* **resume-threshold** *xon-size*	3000m ロスレスイーサネットの一時停止および再開のためのバッファしきい値設定を指定します。 • buffer-size：バイト単位の入力トラフィックのバッファ サイズ。 有効な値の範囲は 10240 ～ 490880 です。 • pause-threshold：ポートがピアを一時停止するバッファ制限を指定します。 • xoff-size：一時停止するバッファ制限を表すバイト数。 有効な値の範囲は 0 ～ 490880 です。 • resume-threshold：ポートがピアを再開するバッファ制限を指定します。 • xon-size：再開するバッファ制限を表すバイト数。 有効な値の範囲は 0 ～ 490880 です。
ステップ 5	switch(config-pmap-nq-c)# **no pause no-drop buffer-size** *buffer-size* **pause-threshold** *xoff-size* **resume-threshold** *xon-size*	（任意） 3000m ロスレスイーサネットの一時停止および再開のためのバッファしきい値設定を削除します。

	コマンドまたはアクション	目的
ステップ 6	switch(config-pmap-nq-c)# **exit**	クラス モードを終了します。
ステップ 7	switch(config-pmap-nq)# **exit**	policy-map network-qos モードを終了します。

次に、3000 メートルの Cisco Nexus デバイスに対する no-drop バッファしきい値の設定方法を示します。

```
switch(config-pmap-nq)# policy-map type network-qos nqos_policy
switch(config-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-nq-c)# pause no-drop buffer-size 152000 pause-threshold 103360
resume-threshold 83520
switch(config-pmap-nq-c)# exit
switch(config-pmap-nq)# exit
switch(config)# exit
switch#
```

Cisco Nexus 2148T ファブリック エクステンダのバッファしきい値の設定

ファブリック エクステンダ コンフィギュレーション モードで、Cisco Nexus 2148T ファブリック エクステンダのバッファしきい値を設定できます。バッファしきい値は、出力キューにテール ドロップしきい値の観測を開始するように指示が送信される前に、入力バッファの消費レベルを設定します。バッファ使用量が設定されたバッファしきい値よりも低い場合、テール ドロップしきい値は無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **fex** *fex-id*	ファブリック エクステンダを指定し、ファブリック エクステンダ モードを開始します。
ステップ 3	switch(config-fex)# **hardware N2148T buffer-threshold** *buffer limit*	Cisco Nexus 2148T ファブリック エクステンダのバッファしきい値を設定します。 バッファしきい値はバイト単位で指定します。 有効な範囲は、Cisco Nexus 2148T ファブリック エクステンダの場合、81920 ～ 316160 です。

次に、Cisco Nexus 2148T ファブリック エクステンダのバッファしきい値をデフォルトに戻す例を示します。

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# hardware N2148T buffer-threshold 163840
```

次に、Cisco Nexus 2148T ファブリック エクステンダのデフォルトのバッファしきい値を削除する例を示します。

```
switch# configure terminal
switch(config)# fex 101
switch(config-fex)# no hardware N2148T buffer-threshold
```

CiscoNexusデバイスでのユニキャストトラフィックの仮想出力キュー制限のイネーブル化

ユニキャスト トラフィックの仮想出力キュー（VOQ）の制限をイネーブルにできます。 輻輳とブロッキングを軽減するために、VOQ を使用して、1 つのブロックされたレシーバが、他の非輻輳ブロッキング レシーバに送信されるトラフィックに影響を与えることを防止します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **hardware unicast voq-limit**	ユニキャスト トラフィックの VOQ 制限をイネーブルにします。 デフォルトでは無効になっています。
ステップ 3	switch(config)# **no hardware unicast voq-limit**	ユニキャスト トラフィックの VOQ 制限をディセーブルにします。

次に、スイッチ上でユニキャスト パケットに対する VOQ 制限をイネーブルにする例を示します。

```
switch(config)# hardware unicast voq-limit
switch(config)#
```

フロー制御の設定

リンク レベル フロー制御

IEEE 802.3x リンク レベル フロー制御により、輻輳レシーバはリンクのもう一方の端にあるトランスミッタと通信して、短時間の間データの転送を停止できます。 リンク レベル フロー制御機能は、リンク上のすべてのトラフィックに適用されます。

送受信方向は個別に設定できます。 デフォルトでは、リンクレベル フロー制御は両方向でディセーブルです。

Cisco Nexus デバイスでは、イーサネット インターフェイスはリンクレベル フロー制御機能を自動検出しません。 イーサネット インターフェイスでこの機能を明示的に設定する必要があります。

各イーサネットインターフェイスで、スイッチはプライオリティフロー制御またはリンクレベルフロー制御のいずれか（両方は不可）をイネーブルにできます。

プライオリティ フロー制御の設定

デフォルトでは、イーサネット インターフェイスは、DCBX プロトコルを使用してネットワークアダプタと PFC についてネゴシエーションします。 PFC がイネーブルの場合、PFC は、no-drop クラスに設定された CoS 値と一致するトラフィックに適用されます。

インターフェイスの PFC を強制的にイネーブルにすることで、ネゴシエーション結果を上書きできます。

Cisco NX-OS Release 5.0(3)N1(1) から、レイヤ 2 またはレイヤ 3 インターフェイスのプライオリティ フロー制御を設定できます。

（注） インターフェイスをレイヤ3インターフェイスとして設定するには、**no switchport** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** *type slot/port*	変更するインターフェイスを指定します。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	switch(config-if)# **no switchport**	（任意） レイヤ 3 インターフェイスを選択します。
ステップ 4	switch(config-if)# **priority-flow-control mode** {**auto** | **on**}	選択したインターフェイスの PFC モードを設定します。 PFC 機能についてネゴシエーションを行うには、auto を指定します。 これはデフォルトです。 PFC を強制的にイネーブルにするには、on を指定します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **no priority-flow-control mode on**	（任意） 選択したインターフェイスのPFC設定をディセーブルにします。

次に、インターフェイス上で PFC を強制的にイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# priority-flow-control mode on
```

次に、レイヤ 3 インターフェイスで PFC を強制的にイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# priority-flow-control mode on
```

リンクレベル フロー制御の設定

イーサネット インターフェイスの LLC は、デフォルトでディセーブルです。 送受信方向で LLC をイネーブルにできます。

レイヤ 2 またはレイヤ 3 インターフェイスにフロー制御を設定できます。

（注） インターフェイスをレイヤ3インターフェイスとして設定するには、**no switchport** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** *type slot/port*	変更するインターフェイスを指定します。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	switch(config-if)# **no switchport**	（任意） レイヤ 3 インターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **flowcontrol** [**receive** {**on** | **off**}] [**transmit** {**on** | **off**}]	選択されたインターフェイスの LLC をイネーブルにします。 **receive** および **transmit** の **on** または **off** を設定します。
ステップ 5	switch(config-if)# **no flowcontrol** [**receive** {**on** | **off**}] [**transmit** {**on** | **off**}]	（任意） 選択されたインターフェイスの LLC をディセーブルにします。

次に、インターフェイス上で LLC をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# flowcontrol receive on transmit on
```

次に、レイヤ 3 インターフェイスで LLC をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no switchport
switch(config-if)# flowcontrol receive on transmit on
```

キューおよびフロー制御設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show queuing interface *[interface slot/\port]*	キューの設定および統計情報を表示します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show interface flowcontrol [**module** *numbef*]	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。
show interface [*interface slot/port*] **priority-flow-control** [**module** *number*]	指定されたインターフェイスのプライオリティフロー制御詳細を表示します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show wrr-queue cos-map [*var*]	
running-config ipqos	QoS の実行コンフィギュレーションに関する情報を表示します。

コマンド	目的
startup-config ipqos	QoS のスタートアップ コンフィギュレーションに関する情報を表示します。

第 10 章

入力ポリシングの設定

この章の内容は、次のとおりです。

入力ポリシングに関する情報

ポリシングでは、特定のクラスのトラフィックについて、そのデータ レートをモニタできます。データ レートがユーザ設定値を超えると、スイッチはパケットをただちにドロップします。ポリシングではトラフィックがバッファリングされないため、伝搬遅延への影響はありません。トラフィックが特定のクラスのデータ レートを超えると、スイッチはパケットをドロップします。

1 レート 2 カラーの入力ポリシングを定義できます。

1 レートの入力ポリシングは、トラフィックの認定情報レート（CIR）をモニタします。

（注） 認定情報レート（CIR）は、1～80000000000 のビット レートまたはリンク レートの割合として指定される値です。

さらに、入力ポリシングは、関連付けられたパケットのバースト サイズをモニタできます。2 カラー（条件）は、指定されたデータ レートパラメータに応じて、各パケットの入力ポリシングによって決定されます。

各条件について設定できるアクションは 1 つだけです。 たとえば、最大 200 ミリ秒のバーストで、256,000 bps のデータ レートに適合するように、クラス内のトラフィックをポリシングするとします。

カラー対応入力ポリシングは、トラフィックが以前にカラーによってすでにマーキングされているものとみなします。

表 *10*：サポートされるポリサーの最大ハードウェア設定

	Nexus 5500 シリーズ	Nexus 2232	Nexus 2248TP-E	Nexus 6000 シリーズ
バースト サイズ	64 MB	32 MB	32 MB	64 MB
最高レート	96 Gbps	12 Gbps	8 Gbps	8 Gbps
粒度	732 kbps	732 kbps	488 kbps	122 kbps

入力ポリシングの注意事項と制約事項

- 入力ポリシングの設定は、Quality of Service (QoS) ポリシー設定の一部です。 次に対する入力ポリシングを含む QoS ポリシーを設定できます。
  - レイヤ 2 スイッチ ポート
  - ホスト インターフェイス（HIF）ポート
  - スイッチ ポートを持つポート チャネル
  - HIF ポートを持つポート チャネル
  - レイヤ 3 インターフェイス（サブインターフェースまたはスイッチ仮想インターフェイス（SVI）は対象外）
  - 仮想ポートチャネル（vPC）
- 入力ポリシングの統計情報が提供されます。 統計情報には、ドロップ数と許可数が含まれます。 **show policy-map interface ethernet** コマンドを入力して統計情報を表示できます。
- 添付ファイルに対して設定する QoS ポリシーは、Ternary Content Addressable Memory（TCAM）にインストールされ、スイッチによって入力ポリシングが適用されます。
- HIF ポートまたはポート チャネルに対して入力ポリシングを含む QoS ポリシーを設定した場合、入力ポリシングはファブリック エクステンダ（FEX）にオフロードされます。 ポリシーの書き換えはスイッチ内でのみ発生します。
- QoS ポリシーでサポートされるすべての一致/設定基準は、ポリシーに入力ポリシングが含まれる場合でもサポートされます。 ファブリック エクステンダ（FEX）は、レイヤ 3 の操作

（フラグメント）およびレイヤ 4 の操作（送信元ポートと宛先ポートの範囲）をサポートしますが、伝送制御プロトコル（TCP）フラグおよびレイヤ 2 の操作はサポートしません。

- 制御プロトコル トラフィックと一致するように QoS ポリシーの一致基準を定義できます。ポリシーのタイプが HIF ポートに対する入力ポリシングを含むように設定されている場合は、制御トラフィックもポリシングされます。 したがって、一致基準は、目的のトラフィック フローに固有にする必要があります。
- **police** コマンドは、Cisco Nexus デバイスの ASIC ではサポートされません。
- スイッチは、仮想イーサネットインターフェイスが接続されている HIF ポートには入力ポリシングを含む QoS ポリシーを適用できません。
- スイッチが HIF ポートに入力ポリシングを適用する場合、ポリサーは、仮想ネットワーク タグ（VNTAG）を持たないトラフィックに適用されます。
- 入力ポリシングを含むポリシーは、スイッチ ポート、HIF ポート、および switch/HIF ポートを持つポート チャネルだけに使用できます。
- 一致基準の中にレイヤ 2 の操作と TCP フラグを含む入力ポリシングは、FEX インターフェイスでは使用できません。
- 入力ポリシングは、Enhanced VPC（2LayerVPC）ポートではサポートされません。
- デュアル ホーム（AA）HIF インターフェイスで同じ入力ポリシングを適用することが推奨されます。
- **police** コマンドは、system qos ポリシーではサポートされません。
- **show policy-map interface** コマンドを使用して、入力レート リミッタが適合していることをチェックし、違反統計情報を表示することが推奨されます。 CLI は、HIF インターフェイス（port-channel と同じように標準的）の認定/違反パケットおよび秒単位のパケット統計情報を表示します。一方、スイッチ ポート（port-channel と同じように標準的）では、このコマンドは、認定/違反パケットおよびビット/秒（bps）を表示します。

認定情報レートを使用するポリシー マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map** [**type qos**] [*qos-policy-map-name*]	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **class-default**}	クラス マップをポリシー マップに関連付け、指定したシステム クラスのコンフィギュレーション モードを開始します。 ポリシー マップ内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。 *class-map-name* 引数には、最大 40 文字の英数字を指定できます。名前は大文字と小文字が区別され、英数字、ハイフン、下線だけを含めることができます。
ステップ 4	switch(config-pmap-c-qos)# **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc**] {*committed-burst-rate*}][**conform**{**transmit**} [**violate** {**drop**}]]]	**cir** を、ビット、kbps、mbps、または gbps 単位でポリシングします。 データ レートが **cir** 以下の場合は、**conform** アクションが適用されます。それ以外の場合は、**violate** アクションが適用されます。 **cir** キーワードは、認定情報レート（つまり、望ましい帯域幅）を、ビット レートまたはリンク レートの割合として使用するように指定します。 *committed-rate* 値は、1 ～ 80 の範囲で指定します。 *data-rate* の値は次のいずれかになります。 • bps：ビット/秒 • kbps：1000 ビット/秒 • mbps：1,000,000 ビット/秒 • Gbps：1,000,000,000 ビット/秒 *committed-burst-rate* の値は次のとおりです。 • bytes：バイト • キロバイト：1000 バイト • メガバイト：1,000,000 バイト • ms：ミリ秒 • us：マイクロ秒 次は、入力ポリシング アクションです。

	コマンドまたはアクション	目的
		• **conform**：トラフィックのデータ レートが制限内に収まっている場合に実行されるアクション。 デフォルト アクションは、**transmit** です。 • **transmit**：パケットを送信します。 このアクションは、パケットがパラメータに適合している場合にだけ使用できます。 • **violate**：トラフィックのデータ レートが設定済みのレート値に違反した場合に実行されるアクション。 基本のデフォルト アクションは、**drop** です。 • **drop**：パケットをドロップします。 このアクションは、パケットがパラメータを超過した場合またはパラメータに違反した場合にだけ使用できます。

ステップ 5	switch(config-pmap-c-qos)# **set** {{**dscp** {*dscp-val* | *dscp-enum*}} | {**precedence** {*prec-val* | *prec-enum*}} | {**qos-group** *qos-grp-val*}}	（任意）
		dscp、**precedence**、または **qos-group** アクションを設定します。
		引数は次のとおりです。
		• *dscp-val*：このトラフィック クラスに割り当てるDSCP値またはパラメータを指定します。 有効値の範囲は 0 ～ 63 です。
		• *dscp-enum*：有効な値は 0～63 です。
		`af11 AF11 dscp (001010)`
		`af12 AF12 dscp (001100)`
		`af13 AF13 dscp (001110)`
		`af21 AF21 dscp (010010)`
		`af22 AF22 dscp (010100)`
		`af23 AF23 dscp (010110)`
		`af31 AF31 dscp (011010)`
		`af32 AF32 dscp (011100)`
		`af33 AF33 dscp (011110)`
		`af41 AF41 dscp (100010)`
		`af42 AF42 dscp (100100)`
		`af43 AF43 dscp (100110)`
		`cs1 CS1(precedence 1) dscp (001000)`
		`cs2 CS2(precedence 2) dscp (010000)`
		`cs3 CS3(precedence 3) dscp (011000)`
		`cs4 CS4(precedence 4) dscp (100000)`
		`cs5 CS5(precedence 5) dscp (101000)`
		`cs6 CS6(precedence 6) dscp (110000)`
		`cs7 CS7(precedence 7) dscp (111000)`

	コマンドまたはアクション	目的

		`default Default dscp (000000)`
		`ef EF dscp (101110)`
		• *prec-val*：このトラフィック クラスに割り当てる IP の優先順位の値。 有効な値の範囲は 0 ～ 7 です。
		• 0：routine
		• 1：priority
		• 2：immediate
		• 3：flash
		• 4：flash-override
		• 5：critical
		• 6：internet
		• 7：network
		（注） 数字だけを入力します。
		prec-enum：有効な値は次のとおりです。
		• routine
		• priority
		• immediate
		• flash
		• flash-override
		• critical
		• internet
		• network
		qos-grp-val：このトラフィック クラスに割り当てる QoS グループの値。 範囲は 1 ～ 5 です。

ステップ 6	switch(config-pmap-c-qos)# **exit**	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ モードを開始します。
ステップ 7	switch(config-pmap-qos)# **exit**	ポリシーマップモードを終了し、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 8	switch(config)# **show policy-map** [**type qos**] [*policy-map-name*]	（任意） 設定済みのすべてのポリシーマップ、または選択した **type qos** ポリシー マップについて情報を表示します。

次に、認定情報レートを使用する入力ポリシングを含むポリシー マップを作成する例を示します。

```
switch# configure terminal
switch(config)# policy-map type qos pm1
switch(config-pmap-qos)# class type qos cm1
switch(config-pmap-c-qos)# police cir 10 mbps bc 20 kbytes
switch(config-pmap-c-qos)# set qos-group 4
switch(config-pmap-c-qos)# end
switch# show policy-map type qos pm1

 Type qos policy-maps
  ====================

  policy-map type qos pm1
  class type qos cm1
  set qos-group 4
  police cir 20 mbytes conform transmit violate drop
  set qos-group 4
  class type qos class-default
  set qos-group 1
  switch#
```

インターフェイスレートの割合を使用するポリシーマップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **policy-map** [**type qos**] [*qos-policy-map-name*]	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。 ポリシーマップ名は、最大40文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	switch(config-pmap-qos)# **class** [**type qos**] {*class-map-name* | **class-default**}	クラスマップをポリシーマップに関連付け、指定したシステム クラスのコンフィギュレーション モードを開始します。 ポリシーマップ

	コマンドまたはアクション	目的
		内のクラスと現在一致していないトラフィックをすべて選択するには、**class-default** キーワードを使用します。 *class-map-name* 引数には、最大 40 文字の英数字を指定できます。 名前は大文字と小文字が区別され、英数字、ハイフン、下線だけを含めることができます。
ステップ 4	switch(config-pmap-c-qos)# **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc**] {*committed-burst-rate*}][**conform**{**transmit**} [**violate** {**drop**}]]]	**cir** を、ビット、kbps、mbps、または gbps 単位でポリシングします。 データ レートが **cir** 以下の場合は、**conform** アクションが適用されます。それ以外の場合は、**violate** アクションが適用されます。 **cir** キーワードは、認定情報レート（つまり、望ましい帯域幅）を、ビット レートまたはリンク レートの割合として使用するように指定します。 *cir-link-percent* 値は、1～100 パーセントの範囲で指定できます。 *committed-burst-rate* の値は次のとおりです。 • bytes：バイト • キロバイト：1000 バイト • メガバイト：1,000,000 バイト 次は、入力ポリシング アクションです。 • **conform**：トラフィックのデータ レートが制限内に収まっている場合に実行されるアクション。 デフォルト アクションは、**transmit** です。 • **transmit**：パケットを送信します。 このアクションは、パケットがパラメータに適合している場合にだけ使用できます。 • **violate**：トラフィックのデータ レートが設定済みのレート値に違反した場合に実行されるアクション。 基本のデフォルト アクションは、**drop** です。 • **drop**：パケットをドロップします。 これは、パケットがパラメータを超過した場

	コマンドまたはアクション	目的
		合またはパラメータに違反した場合にだけ使用できます。
ステップ 5	switch(config-pmap-c-qos)# **set** {{**dscp** {*dscp-val* | *dscp-enum*}} | {**precedence** {*prec-val* | *prec-enum*}} | {**qos-group** *qos-grp-val*}}	（任意） **dscp**、**precedence**、または **qos-group** アクションを設定します。 *dscp-val*：このトラフィック クラスに割り当てる DSCP 値またはパラメータを指定します。有効値の範囲は 0 ～ 63 です。 *prec-val*：このトラフィック クラスに割り当てる IP の優先順位の値。 有効な値は 0 ～ 7 です。 *qos-grp-val*：このトラフィック クラスに割り当てる QoS グループの値。 範囲は 1 ～ 5 です。
ステップ 6	switch(config-pmap-c-qos)# **exit**	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ モードを開始します。
ステップ 7	switch(config-pmap-qos)# **exit**	ポリシー マップ モードを終了し、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	switch(config)# **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]	（任意） 設定済みのすべてのポリシー マップ、または選択した **type qos** ポリシー マップについて情報を表示します。

次に、インターフェイス レートの割合を使用する入力ポリシングを含むポリシーマップを作成する例を示します。

```
switch# configure terminal
switch(config)# policy-map type qos pm-test1
switch(config-pmap-qos)# class type qos cm-cos4
switch(config-pmap-c-qos)# police cir percent 10 bc 40 kbytes conform transmit violate drop
switch(config-pmap-c-qos)# end
switch# show policy-map type qos pm-test1

Type qos policy-maps
====================

policy-map type qos pm-test1
class type qos cm-cos4
set qos-group 4
police cir percent 10 bc 40 kbytes conform transmit violate drop
class type qos class-default
set qos-group 1
switch#
```

入力ポリシング設定の確認

入力ポリシングの設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show policy-map interface** [*interface number*]	1つまたはすべてのインターフェイスのポリシーマップ設定を表示します。
switch# **show policy-map** [**type qos**] [*policy-map-name*]	設定済みのすべてのポリシーマップ、または選択した **type qos** ポリシーマップについて情報を表示します。

入力ポリシングの設定例

次に、入力ポリシング レートが port/port-channel 速度に基づいて計算される場所で、割合として指定される認定情報レートの例を示します。

```
switch(config)# policy-map type qos pm-cos
switch(config-pmap-qos)# class cm-cos
switch(config-pmap-c-qos)# police cir percent 10 bc 20 mbytes conform transmit violate drop

switch(config-pmap-c-qos)#
```

次に、入力ポリシングが設定された **show monitor session** コマンドの出力の例を示します。

```
switch(config-pmap-c-qos)# show policy-map pm-cos


  Type qos policy-maps
  ====================

  policy-map type qos pm-cos
    class type qos cm-cos
      set qos-group 4
      police cir percent 10 bc 20 mbytes conform transmit violate drop
    class type qos class-default
      set qos-group 1
switch(config-pmap-c-qos)#
```

次に、**service-policy** コマンドを使用して インターフェイスに適用されるポリシーの例を示します。

```
switch(config)# interface ethernet 1/1
switch(config-if)# service-policy type qos input pm-cos
```

次に、**show policy-map** コマンドによって表示されるポリシー統計情報の例を示します。

```
switch(config-if)# show policy-map interface ethernet 1/1
Global statistics status :   disabled

Ethernet1/1

  Service-policy (qos) input:   qos-police
    policy statistics status:   disabled

    Class-map (qos):   qos-police (match-all)
      0 packets
```

```
Match: dscp 10
police cir percent 100 bc 200 ms
  conformed 0 bytes, 0 bps action: transmit
  violated 0 bytes, 0 bps action: drop
```

第 11 章

マイクロバースト モニタリング

この章の内容は、次のとおりです。

マイクロバースト モニタリング

マイクロバースト モニタリングに関する情報

マイクロバースト モニタリングの概要

マイクロバースト モニタリング機能は、入出力ポートの両方でポートごとにトラフィックをモニタし、非常に短い時間（マイクロ秒）内で不測のデータ バーストを検出できるようにするものです。 これにより、データ消失の危険性があったり、追加の帯域幅を必要とするようなネットワーク フローを検出できます。

マイクロバーストは、所定の時間間隔で一定量のデータ（単位：バイト）を超過した場合に発生します。マイクロバーストモニタリング機能では、これらの制限を絶対値として（データおよびバーストサイズの場合）、またはリンク速度の割合として指定できます。 これらのしきい値を超えると、システムは Syslog アラーム メッセージを生成します。

マイクロバースト モニタリングの使用方法

マイクロバーストモニタリング機能は、バーストをリアルタイムでモニタします。 モニタリングプロセスはデータ パス問題の概要を示すので、ネットワーク内の潜在的な容量問題の特定に役立ちます。 バーストが設定値を超えると、Syslog メッセージが生成されます。

マイクロバースト モニタリングは、以下の目的のためにリアルタイムのバースト情報を提供します。

- ネットワークのマイクロバーストをモニタする

- 輻輳検出とレイテンシ プロセスをトリガする

マイクロバースト モニタリングの注意事項と制約事項

- マイクロバーストの検出はリンクごとを基準にして実行され、ポートチャネルは考慮されません。
- マイクロバーストの検出はイーサネット ポート上だけでサポートされ、ファブリック エクステンダ テクノロジ（FEX）、ポート チャネル、仮想イーサネット（VETH）、仮想ファイバ チャネル（VFC）などのポートではサポートされていません。

マイクロバースト モニタリングの設定方法

マイクロバースト モニタリングの設定

マイクロバースト モニタリングを設定するには、インターフェイスのマイクロバーストしきい値を設定してから、インターフェイスで許容されるマイクロバーストの最大数を設定します。 入力ポートと出力ポートの設定は別々に行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 3	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/1`	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 4	**burst threshold ingress limit** *percent* **interval** *interval_time* 例： `switch(config-if)# burst threshold ingress limit 60 interval 10000000`	インターフェイスの入力トラフィックのマイクロバーストしきい値を設定します。

	コマンドまたはアクション	目的
ステップ 5	**burst threshold egress size** *max_bytes* **interval** *interval_time* 例： `switch(config-if)# burst threshold egress size 500000 interval 16000`	インターフェイスの出力トラフィックのマイクロバーストしきい値を設定します。
ステップ 6	**burst maximum egress burst-count** *max_bytes* 例： `switch(config-if)# burst maximum egress burst-count 50000`	出力方向のポートの中断が生成されるまでの時間間隔内で許容される、マイクロバーストの最大数を設定します。 この時間間隔は、マイクロバーストしきい値間隔（単位：秒）に 10 を掛けた値と等しくなります。
ステップ 7	**burst maximum ingress burst-count** *max_bytes* 例： `switch(config-if)# burst maximum ingress burst-count 600000`	入力方向のポートの中断が生成されるまでの時間間隔内で許容される、マイクロバーストの最大数を設定します。 この時間間隔は、マイクロバーストしきい値間隔（単位：秒）に 10 を掛けた値と等しくなります。
ステップ 8	**exit** 例： `switch(config-if)# exit`	設定を更新し、インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

マイクロバースト モニタリングの確認

マイクロバースト モニタリング情報を表示するには、次の show コマンドを入力します。

コマンド	目的
show interface burst-counters	マイクロバースト モニタリングが設定されているすべてのインターフェイスのマイクロバースト カウンタ情報を表示します。

マイクロバースト モニタリングの例

マイクロバースト モニタリングの設定例

次の例は、イーサネットインターフェイス上でのマイクロバーストモニタリングの設定方法を示しています。

```
switch# configuration terminal
switch(config)# interface ethernet 1/1
switch(config-if)# burst threshold egress limit 50 interval 30
switch(config-if)# burst threshold ingress size 500000 interval 16000
switch(config-if)# burst maximum egress burst-count 50000
switch(config-if)# burst maximum ingress burst-count 600000
switch(config-if)# exit
switch(config)# copy running-config startup-config
```

第 12 章

スイッチ レイテンシ モニタリングの設定

この章の内容は、次のとおりです。

スイッチ レイテンシ モニタリングに関する情報

スイッチ レイテンシ モニタリングの概要

スイッチレイテンシモニタリング機能では、タイムスタンプ値とともに各入出力パケットをマークします。 システムの各パケットのレイテンシを計算するために、スイッチは入力と出力のタイムスタンプを比較します。 この機能により、すべてのポートペア間の平均レイテンシの履歴とリアルタイムのレイテンシ データを表示できます。

レイテンシ測定値を使用して、どのフローがレイテンシの問題の影響を受けているかを特定できます。 さらにスイッチ レイテンシ モニタリング機能が生成する統計情報によって、ネットワーク トポロジの計画やインシデント対応の管理、ネットワークのアプリケーション問題の根本原因を特定することができます。 この統計情報を使用して、レイテンシ重視のアプリケーションに Service Level Agreement（SLA）を提供することもできます。

スイッチ レイテンシ モニタリングの使用方法

スイッチ レイテンシ モニタリング機能は、パケット レイテンシをナノ秒単位で測定します。 以下のモードで情報を提供します。

- リアルタイム モードでは、入出力ポート ペア間の全パケットの最小、最大、平均遅延値を維持します。

- 履歴モードでは、フローベースのレイテンシ分布ヒストグラムを維持し、線形、指数、またはカスタムの値域を提供します。

スイッチ レイテンシ モニタリングの注意事項と制約事項

スイッチ レイテンシ モニタリングには、次のような制約事項と注意事項があります。

- 入出力ポートのペア間では、一度に 1 つのモードだけを設定できます（即時、線形ヒストグラム、指数ヒストグラム、またはカスタム ヒストグラム）。 即時モードはデフォルトでイネーブルになっています。
- いずれかのヒストグラム モードがポートのペア間で設定されていると、即時モードはディセーブルになります。
- ヒストグラム モードがポートのペア間で削除されると、即時モードがイネーブルになります。
- 基準値を変更すると、スイッチ レイテンシ ヒストグラムの統計情報はすべて失われます。
- 入力ポートと出力ポートのペア間のレイテンシモニタリング モードを変更すると、そのポート ペア間のスイッチ レイテンシ統計情報は失われます。
- スイッチ レイテンシ モニタリングの記録は、スイッチのリロードまたは ISSU の実行時には維持されません。
- スイッチ レイテンシ モニタリング機能は、イーサネット インターフェイスだけでサポートされています。
- スイッチがリロードされたり、新しいモジュールの電源が投入される場合は、**clear hardware profile latency monitor all** コマンドを発行する必要があります。

スイッチ レイテンシ モニタリング モード

スイッチ レイテンシ モニタリングは、次の 4 種類のモードでサポートされます。

- 即時モード

  このモードはデフォルトでイネーブルであり、入力ポートと出力ポート間を流れるすべてのパケットの最小、最大、平均レイテンシ値を収集することができます。

- 線形ヒストグラム

  このモードは、レイテンシの範囲（単位：ナノ秒）ごとにパケット数を数えることができるので、一定範囲のレイテンシにいくつのパケットが含まれているかがカウントされます。 たとえば、800 ～ 848、848 ～ 896、 896 ～ 944、944 ～ 992 などの各レイテンシ範囲でパケット数がいくつかを数えるように、線形ヒストグラムを設定できます。 線形ヒストグラムのモニタリング モードを設定するには、表の基準値（この例では 800 ナノ秒）を指定してから、刻み値を指定します（この例では 50 ナノ秒）。

- 指数ヒストグラム

このモードでは、指数関数的に増加する範囲に対して、レイテンシの値域を指定できます。たとえば、レイテンシ範囲 848 ～ 896、896 ～ 992、992 ～ 1184、1184 ～ 1568 でパケット数を数えるには、指数モードとしてモードを指定し、基準値を 800 ナノ秒とし、50 ナノ秒で刻むように設定します。

- カスタム ヒストグラム

  このモードでは、指定範囲内のパケット数を数えたり、指定範囲外のパケット数を数えたりすることができます。

スイッチ レイテンシ モニタリングの設定方法

スイッチ レイテンシ モニタリングの設定

スイッチ レイテンシ モニタリングを設定するには、最初にモニタリングの基準値を設定してから、入出力ポートのペアとモニタリング モードを設定します。

（注） デフォルトでは、即時モードのスイッチ レイテンシ モニタリングがイネーブルになっています。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**clear hardware profile latency monitor all** 例： `switch# clear hardware profile latency monitor all`	システム内のすべての入出力ポート ペアの統計情報をクリアします。

ステップ 3	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 4	**hardware profile latency monitor base** *nanoseconds* 例： `switch(config)# hardware profile latency monitor base 800`	スイッチ レイテンシ モニタリング ヒストグラムの作成に使用される基準値を指定します。 有効な値は、8 ～ 2147483640 ナノ秒の範囲内の 8 の倍数です。
ステップ 5	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/1`	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。 このインターフェイスは、入出力ポート ペアの出力インターフェイスです。
ステップ 6	**packet latency interface ethernet** *ingress-interface-slot/port* **mode linear step** *step-value* 例： `switch(config-if)# packet latency ethernet 1/2 mode linear step 40`	出力イーサネット インターフェイスと、この指定された入力イーサネットインターフェイスの間で線形モード モニタリングを設定します。
ステップ 7	**packet latency interface ethernet** *ingress-interface-slot/port* **mode exponential step** *step-value* 例： `switch(config-if)# packet latency ethernet 1/3-4 mode exponential step 40`	出力イーサネット インターフェイスと、指定された入力イーサネット インターフェイス ポートの間で指数モード モニタリングを設定します。
ステップ 8	**packet latency interface ethernet** *ingress-interface-slot/port* **mode customer low-latency** *low-value* **high-latency** *high-value* 例： `switch(config-if)# packet latency ethernet 1/5 mode customer low-latency 40 high-latency 1200`	出力イーサネット インターフェイスと、指定された入力イーサネット インターフェイスの間でカスタム モード モニタリングを設定します。
ステップ 9	**exit** 例： `switch(config-if)# exit`	設定を更新し、インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

スイッチ レイテンシ モニタリング統計情報の確認

スイッチ レイテンシ モニタリング統計情報を表示するには、次のタスクを実行します。

コマンド	目的
show hardware profile latency monitor interface ethernet *egress-interface-slot/port* **interface ethernet** *ingress-interface-slot/port*	指定された入出力ポート ペアのスイッチ レイテンシ統計情報を表示します。

スイッチ レイテンシ モニタリングの設定例

スイッチ レイテンシ モニタリングの設定例

次に、スイッチ レイテンシ モニタリング設定方法の例を示します。

```
switch(config)# hardware profile latency monitor base 800
switch(config)# interface ethernet 1/1
switch(config-if)# packet latency interface ethernet 1/2 mode linear step 40
switch(config-if)# packet latency interface ethernet 1/3-4 mode exponential step 40
switch(config-if)# packet latency interface ethernet 1/5 mode custom low 40 high 1200
switch(config)# interface ethernet 2/1
switch(config-if)# packet latency interface ethernet 1/1 mode exponential step 80
```

第 13 章

WRED 明示的輻輳通知

この章の内容は、次のとおりです。

WRED 明示的輻輳通知

WRED 明示的輻輳通知に関する情報

WRED - 明示的輻輳通知機能の概要

現在、Transmission Control Protocol（TCP）の輻輳管理と回避アルゴリズムは、ベストエフォート型サービス モデルを使用してデータを送信するネットワークの輻輳を適切に示すのはパケット損失であるという概念に基づいています。 ネットワークがベストエフォート型サービスモデルを使用する場合、ネットワークは信頼性、遅延限界、スループットを保証せずに、可能であればデータを配信します。 ただし、これらのアルゴリズムとベストエフォート型サービスモデルは、遅延やパケット損失の影響を受ける用途には適していません（例：Telnet、Web ブラウジング、音声およびビデオ データなどの双方向トラフィック転送）。 Weighted Random Early Detection（WRED）および明示的輻輳通知（ECN）は、この問題の解決に役立ちます。

RFC 3168「*IP* への明示的輻輳通知（*ECN*）の追加（*The Addition of Explicit Congestion Notification (ECN) to IP*）」は、インターネット インフラにアクティブ キュー管理（例：WRED）を追加すると、ルータは輻輳の兆候としてパケット損失に限定されなくなることを示しています。

WRED 明示的輻輳通知の注意事項と制約事項

- 明示的輻輳通知（ECN）パラメータは、システム レベルでのみ設定できます。
- Weighted Random Early Detection（WRED）は、Quality of Service（QoS）グループ上で単独で設定することはできません。 ECN はデフォルトでイネーブルになっています。

- インターフェイスがない場合でも、10 G インターフェイスおよび 40 G インターフェイスの WRED しきい値を設定する必要があります。
- WRED ECN は、マルチキャストまたはブロードキャスト トラフィックには適用されません。
- WRED ECN は、Nexus 5000 シリーズ スイッチではサポートされません。

WRED の仕組み

WRED は、輻輳の早期検出を可能にし、複数のトラフィック クラスを処理する手段を提供します。 WRED では、ルータで輻輳が発生し始めると、よりプライオリティが低いトラフィックを選択的に廃棄し、異なるサービス クラスに対して差別化したパフォーマンス特性を提供できます。また、グローバル同期に対して保護されます。 グローバル同期は輻輳の波が頂点に達すると発生し、その後は転送リンクが容量いっぱいまで使用されない時間が続きます。 そのため、WRED は輻輳の発生が予測される出力インターフェイスやルータで役立ちます。

WRED はネットワークのコア ルータで実行されます。 エッジ ルータは、パケットがネットワークに入ると IP 優先順位をパケットに割り当てます。 WRED では、コア ルータはこれらの優先順位を使用して、異なる種類のトラフィックの処理方法を決定します。 WRED は個別のしきい値と重み付けを、それぞれの IP 優先順位に使用し、ネットワークは異なるトラフィックの種類でのパケットのドロップに対し、異なるサービス品質を実現できます。 標準的なトラフィックは、輻輳時には、優先度の高いトラフィックよりも頻繁にドロップされる可能性があります。

WRED の詳細情報については、『Congestion Avoidance Overview（輻輳回避の概要）』モジュールを参照してください。

ECN による WRED 機能の拡張

WRED は、輻輳を示す、特定のしきい値を超える平均キュー長に基づいてパケットをドロップします。 ECN は WRED の拡張で、平均キュー長が特定のしきい値を超えた場合にパケットをドロップせずにマーキングします。 WRED 明示的輻輳通知機能を設定すると、ルータとエンド ホストは、このマーキングをネットワークの輻輳によってパケットの送信速度が低下していることを示す警告として使用します。

RFC 3168『*The Addition of Explicit Congestion Notification (ECN) to IP*』に記述されているように、ECN を実装するには、ECN 専用フィールドで ECN 対応転送（ECT）ビットと CE（Congestion Experienced）ビットの 2 つのビットが IP ヘッダに含まれている必要があります。 ECT ビットと CE ビットを使用して、00 から 11 の 4 つの ECN フィールドの組み合わせを作成できます。 最初の数字は ECT ビットで、2 番目の数字は CE ビットです。 次の表は、ECN フィールドの ECT と CE ビットの組み合わせの設定一覧と、その組み合わせの意味を示しています。

表 *11*：*ECN* ビットの設定

ECT ビット	CE ビット	組み合わせが示す内容
0	0	ECN 対応ではない

ECT ビット	CE ビット	組み合わせが示す内容
0	1	転送プロトコルのエンドポイントが ECN 対応
1	0	転送プロトコルのエンドポイントが ECN 対応
1	1	Congestion experienced

ECN のフィールドの組み合わせ 00 は、パケットが ECN を使用していないことを示します。

ECN のフィールドの組み合わせ 01 と 10（それぞれ着信側 ECT（1）と ECT（0））は、データの送信側によって設定され、転送プロトコルのエンドポイントがECN対応であることを示します。ルータは、これらの 2 つのフィールドの組み合わせを同様に取り扱います。 データの送信元は、これらの 2 つの組み合わせの 1 つまたは両方を使用できます。 これらの 2 つのフィールドの組み合わせ、および組み合わせて使用する意味の詳細については、RFC 3168『*The Addition of Explicit Congestion Notification (ECN) to IP*』を参照してください。

ECN フィールドの組み合わせ 11 は、エンド ポイントに対する輻輳を示します。 ルータの満杯のキューに到着するパケットはドロップされます。

ECN がイネーブルのときパケットはどのように処理されるか

- キュー内のパケット数が最小しきい値未満の場合、パケットが送信されます。 これは ECN がイネーブルになっているかどうかに関係なく実行されます。この処理は、ネットワーク上で WRED だけが使用されている場合、パケットが受けるのと同一の処理です。
- キュー内のパケット数が最小しきい値と最大しきい値の間の場合、次の 3 つのシナリオのいずれかになる可能性があります。
  - パケットの ECN のフィールドにエンドポイントが ECN 対応であることが示されている（つまり、ECT ビットが 1 および CE ビットが 0 に設定されているか、または ECT ビットが 0 および CE ビットが 1 に設定されている）場合、および WRED アルゴリズムによってパケットが廃棄確率に基づいてドロップされると判断される場合には、パケットの ECT ビットと CE ビットが 1 に変更され、パケットが送信されます。 これは、ECN がイネーブルであり、パケットがドロップされる代わりにマークされているために発生します。
  - パケットの ECN のフィールドによって、どちらのエンドポイントも ECN 対応ではないことが示されている（つまり、ECT ビットが 0 に設定され、CE ビットが 0 に設定されている）場合、パケットは、WRED廃棄確率に基づいてドロップされる可能性があります。 これは、ルータ上で ECN を設定せずに WRED がイネーブル化されている場合に、パケットが受けるのと同一の処理です。

- パケットの ECN のフィールドに、ネットワークで輻輳が発生していることが示されている（つまり、ECT ビットと CE ビットの両方が 1 に設定されている）場合、パケットが送信されます。 これ以上のマーキングは必要ありません。

- キュー内のパケット数が最小しきい値を上回っている場合、パケットはドロップ確率に基づいてドロップされます。 これは、ルータ上で ECN を設定せずに WRED がイネーブル化されている場合に、パケットが受けるのと同一の処理です。

プロキシ キューの送信速度

プロキシ キューが輻輳を示すしきい値に達すると、明示的輻輳通知（ECN）マーキングが実行され、パケット受信者は送信者に輻輳表示をエコーします。 送信者は、輻輳がパケットドロップによって示されたかのように応答する必要があります。 プロキシキューの送信速度は、出力ポートでの輻輳時に一定量のパケットだけを送信するように設定されます。 たとえば、10 ギガビットポートでは、9900 Mbps の送信速度を設定して、一部のパケットが送信されないようにできます。

ECN 推奨しきい値およびプロキシ キューの送信速度

次の表は、推奨されるプロキシ キューの送信速度と、明示的輻輳通知（ECN）の最大および最小しきい値を説明しています。

パラメータ	10 ギガビット ポート	40 ギガビット ポート
ECN の最小しきい値	64000 バイト	4000 バイト
ECN の最大しきい値	128000 バイト	256000 バイト
プロキシ キューの送信速度	9900 Mbps	39900 Mbps

WRED 明示的輻輳通知を設定する方法

WRED - 明示的輻輳通知の設定

WRED-ECN を設定するには、インターフェイスのしきい値を指定し、ECN をイネーブルにして、プロキシ キュー送信速度を指定します。

はじめる前に

デバイスの Weighted Random Early Detection（WRED）の明示的輻輳通知（ECN）を設定する前に、Quality of Service（QoS）グループを設定する必要があります。 さらに、次の制限事項が適用されます。

- 明示的輻輳通知（ECN）パラメータは、システム レベルでのみ設定できます。

- Weighted Random Early Detection（WRED）は、Quality of Service（QoS）グループ上で単独で設定することはできません。 ECN はデフォルトでイネーブルになっています。
- インターフェイスがない場合でも、10 G インターフェイスおよび 40 G インターフェイスの WRED しきい値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	switch# **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	switch(config)# **hardware random-detect min-thresh 10g** *10g-min-threshold* **40g** *40g-min-threshold* **max-thresh 10g** *10g-max-threshold* **40g** *40g-max-threshold* **ecn qos-group** *qos-group-number*	10 ギガビットおよび 40 ギガビット インターフェイスの最小および最大しきい値を設定し、特定の QoS グループで ECN をイネーブルにします。 10 G と 40 G の両方のインターフェイスのしきい値は、1 ～ 67108863 バイトの範囲内です。 QoS グループ番号はどの QoS グループが設定されているかを指定します。範囲は0（クラスデフォルト）～ 5 です。
ステップ 3	switch(config)# **hardware pq-drain 10g** *10g-drain-rate* **40g** *40g-drain-rate*	10 ギガビットおよび 40 ギガビット ポートのプロキシキュー送信速度を設定します。 出力ポートで輻輳が発生した場合、送信速度値は送信可能な最大パケット数を指定します。 10 G インターフェイスの送信速度の範囲は 1 ～ 20000 Mbps です。 40 G インターフェイスの送信速度の範囲は 1 ～ 80000 Mbps です。

WRED 明示的輻輳通知の例

WRED 明示的輻輳通知の設定例

次に、Weighted Random Early Detection（WRED）の明示的輻輳通知（ECN）を設定する方法の例を示します。

```
switch# configuration terminal
switch(config)# hardware random-detect min-thresh 10g 64000 40g 4000 max-thresh 10g 128000
 40g 256000 ecn qos-group 2
switch(config)# hardware pq-drain 10g 9900 40g 39900
switch(config)# exit
switch(config)# copy running-config startup-config
```

第 14 章

ACL ロギングの設定

この章の内容は、次のとおりです。

ACL ロギングに関する情報

ACL ロギング機能では、ACL フローをモニタし、インターフェイスでドロップされたパケットをログに記録することができます。

IPv6 ACL ロギングの概要

ACL ロギング機能を設定すると、システムは ACL のフローをモニタし、ACL エントリの拒否条件に一致する各フローのドロップ パケットと統計情報をログに記録します。

統計情報とドロップパケットのログは、フローごとに生成されます。 フローは、送信元インターフェイス、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート値によって定義されます。 一致するフローについて維持される統計情報は、指定された時間間隔での ACL エントリによるフローの拒否件数です。

新しいフローが拒否されると（システム上ではすでにアクティブではないフロー）、システムはヒット カウント値 1 の 最初の Syslog メッセージを生成します。 次に、フローが拒否されるたびにシステムはフロー エントリを作成し、ヒット カウント値を増やします。

既存のフローが拒否されると、システムは各間隔の終了時に Syslog メッセージを生成し、現在の間隔でのフローに対するヒット カウント値を報告します。 Syslog メッセージの生成後、フローの

ヒットカウント値は次の間隔の間にゼロにリセットされます。この間隔の間に一度もヒットした記録がない場合は、フローが削除され、Syslog メッセージは生成されません。

ACL ロギングの注意事項と制約事項

ACL ロギングには次の設定上の注意事項と制約事項があります。

- 拒否 ACE 条件のみに一致するシステム ログ パケット。 許可 ACE 条件のロギングはサポートしていません。
- ロギング オプションは ACL 拒否エントリに適用される可能性があります。 ロギング オプションを暗黙的に拒否されたトラフィックに適用するには、特定のすべて拒否 ACL エントリのロギング オプションを設定する必要があります。
- ACL ロギングは、**ipv6 port traffic-filter** コマンドによって設定されたポート ACL （PACL）と、**ipv6 traffic-filter** コマンドのみによって設定されたルーテッド ACL （RACL）に適用されます。
- フローと拒否フローの総数は、DOS 攻撃を避けるためにユーザ定義の最大値に 限定されます。 この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- CPU 使用率に影響を与えずに多数のフローをサポートできるようにするため、システムはハッシュ テーブルを使用してフローの場所を特定します。 システムはタイマー キューを使用して、多数のフローのエージング管理を効率よく行います。
- ACL ロギング プロセスによって生成される Syslog エントリ数は、ACL ロギング プロセスで設定されたロギング レベルによって制限されています。 Syslogエントリの数がこの制限を超えると、ロギング機能が一部のロギング メッセージをドロップする場合があります。 したがって、ACL ロギングは課金ツールやアクセス リストとの一致数を正確に把握するための情報源として使用しないでください。
- ハードウェアの速度リミッタはパケット単位でトラフィックの速度を制限しますが、コントロール プレーン ポリシング（COPP）は、バイト単位でトラフィックの速度を制限します。パケット サイズとハードウェア速度リミッタの両方の値が大きい場合、COPP のデフォルト値を上回り、システムがパケットをドロップ する可能性があります。 この制限を回避するには、デフォルトの CIR 値（64000 バイト）を 2560000 バイトなどの大きな値に増やします。デフォルト CIR を増やすと、通常はパケットのロギングが発生します。
- IPv6 ロギングは管理または VTY （端末）ポートではサポートされていません
- IPv6 ロギングは出力 RACL ではサポートされません（ASIC の制約事項のため）。
- IPv6 ロギングは出力 VACL ではサポートされません（ASIC の制約事項のため）。

ACL ロギングの設定

ACL ロギング プロセスを設定するには、まずアクセス リストを作成し、指定された ACL を使用してインターフェイスで IPv6 トラフィックのフィルタリングをイネーブルにし、最後に ACL ロギング プロセス パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	**ipv6 access-list** *name* 例： `switch(config)# ipv6 access-list logging-test`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト 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	**deny ipv6 any** *destination-address* **log** 例： `switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log`	IPv6 アクセス リストに拒否条件を設定します。このエントリに対する一致をシステムがログに記録するようにするには、拒否条件を設定するときに **log** キーワードを使用する必要があります。
ステップ 4	**exit** 例： `switch(config-ipv6-acl)# exit`	設定を更新し、IPv6 アクセス リスト コンフィギュレーション モードを終了します。
ステップ 5	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/1`	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 6	**ipv6 traffic-filter logging-test** {**in** | **out**} 例： `switch(config-if)# ipv6 traffic-filter logging-test in`	指定された ACL を使用して、インターフェイス上で IPv6 トラフィックのフィルタリングをイネーブルにします。 発信または着信トラフィックに ACL を適用できます。
ステップ 7	**exit** 例： `switch(config-if)# exit`	設定を更新し、インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**logging ip access-list cache interval** *interval* 例： `switch(config)# logging ip access-list cache interval 490`	ACL ロギング プロセスのログ更新間隔を秒数で設定します。 デフォルト値は 300 秒です。 指定できる範囲は 5 ～ 86400 秒です。
ステップ 9	**logging ip access-list cache entries** *number-of-flows* 例： `switch(config)# logging ip access-list cache entries 8001`	ACL ロギング プロセスによってモニタリングするフローの最大数を指定します。 デフォルト値は 8000 です。 指定できる値の範囲は、0 ～ 1048576 です。
ステップ 10	**logging ip access-list cache threshold** *threshold* 例： `switch(config)# logging ip access-list cache threshold 490`	アラート間隔の期限が満了する前に規定のパケット数がログ記録されると、システムは Syslog メッセージを生成します。
ステップ 11	**hardware rate-limiter access-list-log** *packets* 例： `switch(config)# hardware rate-limiter access-list-log 200`	アクセス リスト ロギングのためにスーパーバイザモジュールにコピーされるパケットのレート制限を pps で設定します。 範囲は 0 ～ 30000 です。
ステップ 12	**acllog match-log-level** *severity-level* 例： `switch(config)# acllog match-log-level 5`	ACL 一致をログ記録する最小の重大度を指定します。 デフォルト値は 6（情報）です。 0（緊急）～7（デバッグ）までの範囲があります。

ACL ロギング設定の確認

ACL ロギング設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show logging ip access-list status	拒否フローの最大数、現在の有効なログ間隔と現在の有効なしきい値を表示します。
show logging ip access-list cache	送信元 IP アドレスと宛先 IP アドレス、S ポートおよび D ポート情報などのアクティブ ログ フロー情報を表示します。

ACL ロギングの設定例

次に、ACL ロギング プロセスの設定方法の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list logging-test
switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log
switch(config-ipv6-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ipv6 traffic-filter logging-test in
switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold 900
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 5
switch(config)# exit
switch#
```

次の例は、一般的な PACL ロギングの設定を示しています。

```
switch(config)# interface ethernet 8/11
switch(config-if)# ipv6 port traffic-filter v6log-pacl in
switch(config-if)# switchport access vlan 4064
switch(config-if)# speed 1000

switch(config)# interface Vlan 4064
switch(config-if)# no shutdown
switch(config-if)# no ip redirects
switch(config-if)# ipv6 address 4064::1/64


Switch# show vlan filter
vlan map v6-vaclmap:
Configured on VLANs: 4064

Switch# show vlan access-map v6-vaclmap
Vlan access-map v6-vaclmap
match ipv6: v6-vacl
action: drop
statistics per-entry
```

第 15 章

バッファ使用状況ヒストグラムの設定

この章の内容は、次のとおりです。

バッファ使用状況ヒストグラム機能に関する情報

バッファ使用状況ヒストグラム機能では、リアルタイムでシステムの最大キュー深度とバッファ使用状況を分析できます。 即時またはリアルタイムのバッファ使用状況情報は、ハードウェアでサポートされます。 ソフトウェアを使用して、ハードウェアを定期的にポーリングすることで、バッファ使用量の履歴を取得できます。 バッファ使用量の履歴を取得すると、システムのトラフィック パターンがより具体的にわかるので、トラフィック エンジニアリングに役立ちます。 その結果、ハードウェア バッファ リソースをより効果的に使えます。

Cisco Nexus デバイスでは、 40 ギガビット イーサネット 3 ポートごと、または 10 ギガビット イーサネット 12 ポートごとに、共有の 25 Mb パケット バッファにアクセスできます。 15.6 Mb は入力用に、8.6 Mb は出力用に予約されています。 残りの容量は SPAN および制御パケットに使用されます。

バッファ使用状況ヒストグラムによって、以下を行うことができます。

- 希望するポートのバッファ使用状況履歴の測定値を設定します。
- 一定時間、バッファ使用状況を確認します。
- 低速または高速のポーリング モードを設定します。

- 後で分析できるように、収集した統計情報を 1 時間ごとにブートフラッシュ ドライブの `buffer_util_stats` ファイルにコピーします。 収集した統計情報は 1 時間後にファイルの末尾に追加され、インターフェイス名があるヘッダーにタイムスタンプが付けられます。

バッファ使用状況ヒストグラムの注意事項と制約事項

バッファ使用状況ヒストグラムには次の注意事項と制約事項があります。

- データは、アップグレード時に維持されるわけではありません。 新しいリリースの後でスイッチがオンラインになると、新たな統計情報の学習が再起動します。
- ユニキャストおよびマルチキャスト バッファの使用状況は、出力方向で確認できます。 入力方向では、バッファの使用状況は結合されます。
- この機能は、物理ポート上でのみサポートされます。 この機能は、仮想インターフェイス、サブ インターフェイス、FEX ホスト インターフェイス（HIF）ポート、およびポート チャネルではサポートされていません。 ファブリック エクステンダ（FEX）のファブリック ポートとポート チャネル メンバ ポートがサポートされています。
- **show hardware profile buffer monitor** {**all** | **interface** *intf*} **history** {**brief** | **detail**} | **xml** > *filename***.xml** コマンドを使用して、XML 出力を取得できます。

  このコマンドは、CLI 上の XML ファイルの内容を表示します。 これは XML ファイルに転送できます。 ファイルは任意の XML アナライザ ツールにフェッチして、詳細な解析ができます。 XML サポートはリアルタイムのバッファ使用状況には使用できないので、ご注意ください。 これはつまり、**history** オプションのないコマンドを使用することです。

高速ポーリング

デフォルトでは、ソフトウェアは 1 秒ごとにバッファの使用状況をポーリングします。 高速ポーリングでは、250 ミリ秒間隔でバッファの使用状況をポーリングします。 ポーリング モードを低速（デフォルト値）から高速に変更しても、低速のポーリング モードで取得した古いヒストグラムの記録はクリアされません。 高速ポーリング モードを使用し、新しいデータの入力が続くと、古いデータは表の最後に移動していきます。 ポーリング モードが高速から低速に変更されると、同じシナリオが逆のケースであてはまります。 高速ポーリング モードではポーリング間隔は 250 ミリ秒ですが、CPU 使用率に影響はありません。

高速ポーリングでは、より詳細なデータが結果として得られます。 ポーリング モードが変更されると、そのポーリング モードはバッファ使用状況ヒストグラム機能がイネーブルになっているすべてのポートに適用されます。

バッファ使用状況ヒストグラムのデフォルト設定

次の表は、バッファ使用状況ヒストグラム パラメータのデフォルト設定の一覧です。

パラメータ（Parameters）	デフォルト
バッファ使用状況ヒストグラム	ディセーブル
ポーリング モード	遅い

バッファ使用状況ヒストグラムの設定

バッファ使用状況ヒストグラムのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** [**ethernet** [*chassis*/]*slot*/*port*]	指定したインターフェイスの設定モードを開始します。
ステップ 3	switch(config-if)# **hardware profile buffer monitor**	ポートのバッファ使用状況ヒストグラム統計情報の収集をイネーブルにします。
ステップ 4	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、バッファ使用状況ヒストグラム収集機能をイネーブルにする方法の例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# hardware profile buffer monitor
```

高速ポーリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **hardware profile buffer monitor sampling fast**	250 ミリ秒間隔で高速ポーリングを設定します。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、高速ポーリングの設定方法を示しています。

```
switch# configure terminal
switch(config)# hardware profile buffer monitor sampling fast
```

低速ポーリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **no hardware profile buffer monitor sampling fast**	1 秒間隔で低速ポーリングを設定します。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、低速ポーリングの設定方法を示しています。

```
switch# configure terminal
switch(confg)# no hardware profile buffer monitor sampling fast
```

バッファ使用状況ヒストグラム機能のディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface** [**ethernet** [*chassis*/]*slot*/*port*]	指定したインターフェイスの設定モードを開始します。
ステップ 3	switch(config-if)# **no hardware profile buffer monitor**	ポートのバッファ使用状況ヒストグラム統計情報の収集をディセーブルにします。
ステップ 4	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、バッファ使用状況ヒストグラム機能をディセーブルにする方法の例を示します。

```
switch# configure terminal
switch)config)# interface ethernet 1/1
switch(config-if)# no hardware profile buffer monitor
```

バッファ使用状況ヒストグラムの履歴のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **clear hardware profile buffer monitor** [**interface** *ifid*]	提供されたパラメータに基づいて、1つまたはすべてのポートのバッファ使用状況ヒストグラムの情報をクリアします。 インターフェイスなしでコマンドを入力すると、すべてのポートのバッファ使用状況の統計情報がクリアされます。

次に、バッファ使用状況ヒストグラムの履歴をクリアする方法の例を示します。

```
switch# configure terminal
swtich(config)# clear hardware profile buffer monitor
```

バッファ使用状況ヒストグラム機能の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show hardware profile buffer monitor {**all** | **interface** *intf*}	各ポートのユニキャストおよびマルチキャストキューのバッファ使用状況に関する統計情報と、全体のバッファ空き容量と使用済みバッファの統計情報を表示します。 このコマンドは即時（現在時刻）ベースで、バッファ使用状況の統計情報を取得するために使用されます。
show hardware profile buffer monitor {**all** | **interface** *intf*} **history** {**brief** | **detail**}	すべてのポートまたは指定されたポートのバッファ使用状況の履歴統計を表示します。 このコマンドは簡潔および詳細な表現をサポートします。 簡潔な表現は時系列の平均使用状況のみを表示するために使用されますが、詳細な表現は最大、最小、および平均の使用状況を時系列で表示します。

バッファ使用状況ヒストグラムの出力例

次に、ポーリング モードが低速に設定されている場合の出力例を示します。 バッファ使用状況データは、1 秒ごとに取得されます。 1 sec 列のデータには、最小/最大/平均は使用できません。 1 sec 列からサンプリングした 5 つのデータが 5 sec 列の最初のエントリになります（1 sec 列からサンプリングした 5 つのデータから最小/最大/平均値を計算）。 5 sec 列からサンプリングした 12 のデータが 1 min 列の最初のエントリになります。 1 min 列からサンプリングした 5 つのデータが 5 min 列の最初のエントリになります。 5 min 列からサンプリングした 12 のデータが 1 hour 列の最初のエントリになります。 この情報は、ブートフラッシュ上のファイルにコピーされます。 データは循環式に表内でプロパゲートされます。

```
switch(config)# show hardware profile buffer monitor interface ethernet 1/1 history detail
--------------------------------------------------------------------------------
                                        Interface : Eth1/1
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
                                 Sampling Mode : Slow (1 second)
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
           Ingress Buffer Utilization Detected(Min|Max|Avg)(in KB)
                 Per asic Ingress Total Usage (15.628800MB)
--------------------------------------------------------------------------------
     1 sec     |     5 sec     |     1 min     |     5 min     |     1 hour    |
```

```
-------------------------------------------------------------------------------
16.3|  -  | -  |12.5|18.9| 14.9| 9.3|22.7| 15.7| 0.0|23.0| 13.7|      N/A      |
21.4|  -  | -  |13.4|22.7| 17.5| 0.0|22.1|  5.8| 6.7|23.0| 16.3|      N/A      |
12.5|  -  | -  |10.2|21.4| 15.0| 0.0| 0.0|  0.0| 9.3|23.0| 15.8|      N/A      |
13.8|† -  | -  | 9.9|22.1| 13.0| 0.0|22.7|  5.5|      N/A      |      N/A      |
12.8|† -  | -  |10.2|15.4| 12.4| 9.3|23.0| 15.7|      N/A      |      N/A      |
      N/A      |10.9|20.5| 17.4|      N/A      |      N/A      |      N/A      |
      N/A      | 9.3|22.1| 18.0|      N/A      |      N/A      |      N/A      |
      N/A      |14.7|22.4| 17.7|      N/A      |      N/A      |      N/A      |
      N/A      | 9.9|21.1| 16.5|      N/A      |      N/A      |      N/A      |
      N/A      |11.2|20.8| 15.9|      N/A      |      N/A      |      N/A      |
      N/A      | 9.9|18.2| 14.7|      N/A      |      N/A      |      N/A      |
      N/A      |10.2|22.7| 16.1|      N/A      |      N/A      |      N/A      |
-------------------------------------------------------------------------------
         Egress Unicast Buffer Utilization Detected(Min|Max|Avg)(in KB)
                     Per asic Egress Total Usage (8.611850MB)
-------------------------------------------------------------------------------
     1 sec     |     5 sec     |     1 min     |     5 min     |     1 hour    |
-------------------------------------------------------------------------------
0.0|  -  | -  | 0.0|19.8|† 7.9| 0.0|19.8| 13.0| 0.0|19.8| 10.6|      N/A      |
1.0|  -  | -  | 0.0|19.8| 11.9| 0.0|19.8|  0.4| 0.0|19.8| 12.2|      N/A      |
0.0|  -  | -  | 0.0|19.8| 15.9| 0.0| 0.0|  0.0| 0.0|19.8| 11.9|      N/A      |
19.8|  -  | -  | 0.0|19.8| 15.9| 0.0|19.8| 4.0|      N/A      |      N/A      |
0.0|  -  | -  |19.8|19.8| 19.8| 0.0|19.8| 13.0|      N/A      |      N/A      |
      N/A      | 0.0|19.8| 11.9|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0|19.8| 15.9|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0|19.8| 11.9|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0|19.8|  7.9|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0|19.8| 15.9|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0|19.8|  8.6|      N/A      |      N/A      |      N/A      |
      N/A      |19.8|19.8| 19.8|      N/A      |      N/A      |      N/A      |
-------------------------------------------------------------------------------
         Egress Multicast Buffer Utilization Detected(Min|Max|Avg)(in KB)
                     Per asic Egress Total Usage (8.611850MB)
-------------------------------------------------------------------------------
     1 sec     |     5 sec     |     1 min     |     5 min     |     1 hour    |
-------------------------------------------------------------------------------
0.0|  -  | -  | 0.0| 0.0|  0.0| 0.0| 0.0|  0.0| 0.0| 0.0|  0.0|      N/A      |
0.0|  -  | -  | 0.0| 0.0|  0.0| 0.0| 0.0|  0.0| 0.0| 0.0|  0.0|      N/A      |
0.0|  -  | -  | 0.0| 0.0|  0.0| 0.0| 0.0|  0.0| 0.0| 0.0|  0.0|      N/A      |
0.0|  -  | -  | 0.0| 0.0|  0.0| 0.0| 0.0|  0.0|      N/A      |      N/A      |
0.0|  -  | -  | 0.0| 0.0|  0.0| 0.0| 0.0|  0.0|      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
      N/A      | 0.0| 0.0|  0.0|      N/A      |      N/A      |      N/A      |
-------------------------------------------------------------------------------
```

この例には、該当するタイムラインの平均バッファ使用量値だけが含まれます。 詳細出力の 1 行目だけが出力されます。

```
switch# show hardware profile buffer monitor interface e1/1 history brief
-------------------------------------------------------------------------------
                              Interface : Eth1/1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
                       Sampling Mode : Slow (1 second)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
                      Ingress Buffer Utilization Detected(in KB)
                      Per asic Ingress Total Usage (15.628800MB)
-------------------------------------------------------------------------------
     1 sec     |     5 sec     |     1 min     |     5 min     |     1 hour    |
-------------------------------------------------------------------------------
            0.0|            0.0|            0.0|            0.0|            0.0|
-------------------------------------------------------------------------------
        Egress Buffer Utilization Detected(Unicast|Multicast)(in KB)
                     Per asic Egress Total Usage (8.611850MB)
-------------------------------------------------------------------------------
```

```
     1 sec      |      5 sec      |      1 min      |      5 min      |      1 hour     |
-------------------------------------------------------------------------------------------
    0.0|    0.0|    0.0|    0.0|    0.0|    0.0|    0.0|    0.0|    0.0|    0.0|
-------------------------------------------------------------------------------------------
```

第 16 章

QoS 設定例

この章の内容は、次のとおりです。

QoS 例 1

次の例は、システム全体でアクセス コントロール リストに一致するトラフィックに対して、フレームの CoS フィールドを 5 に書き換えるように設定する方法を示しています。

手順

	コマンドまたはアクション	目的
ステップ 1	入力分類ポリシーを設定します（アクセス コントロール リストは定義済みです）。	(config)# **class-map type qos cmap-qos-acl** (config-cmap-qos)# **match access-group ACL-CoS** (config-cmap-qos)# **exit** (config)# **policy-map type qos pmap-qos-acl** (config-pmap-qos)# **class cmap-qos-acl** (config-pmap-c-qos)# **set qos-group 4** (config-pmap-c-qos)# **exit** (config-pmap-qos)# **exit**
ステップ 2	分類ポリシーをシステムに追加します。	(config)# **system qos** (config-sys-qos)# **service-policy type qos input pmap-qos-acl** (config-sys-qos)# **exit**
ステップ 3	システム クラスの割り当てを設定し、ポリシーを書き換えます。システム クラスを qos-group 4 に割り当て、書き換えアクションを定義します。	(config)# **class-map type network-qos cmap-nq-acl** (config-cmap-nq)# **match qos-group 4** (config-cmap-nq)# **exit** (config)# **policy-map type network-qos pmap-nq-acl** (config-pmap-nq)# **class type network-qos cmap-nq-acl** (config-pmap-c-nq)# **set cos 5** (config-pmap-c-nq)# **exit** (config-pmap-nq)# **exit**
ステップ 4	割り当ておよび書き換えポリシーをシステムに追加します。	(config)# **system qos** (config-sys-qos)# **service-policy type network-qos pmap-nq-acl** (config-sys-qos)# **exit**

QoS 例 2

次の例は、アクセス コントロール リストを使用して、イーサネット インターフェイス 1/1 のトラフィックに一致するイーサネット インターフェイス 1/3 のトラフィックに、50% の帯域幅を適用する方法を示しています。

手順

	コマンドまたはアクション	目的

ステップ 1	入力分類ポリシーを設定します。	`(config)# class-map type qos cmap-qos-bandwidth`
		`(config-cmap-qos)# match access-group ACL-bandwidth`
		`(config-cmap-qos)# exit`
		`(config)# policy-map type qos pmap-qos-eth1-1`
		`(config-pmap-qos)# class cmap-qos-bandwidth`
		`(config-pmap-c-qos)# set qos-group 2`
		`(config-pmap-c-qos)# exit`
		`(config-pmap-qos)# exit`

ステップ 2	イーサネットインターフェイス 1/1 に分類ポリシーを結合します。	`(config)# interface ethernet 1/1`
		`(config-if)# service-policy type qos input pmap-qos-eth1-1`
		`(config-if)# exit`

ステップ 3	初めにシステム全体で qos-group の定義を設定します。	`(config)# class-map type queuing cmap-que-bandwidth`
		`(config-cmap-que)# match qos-group 2`
		`(config-cmap-que)# exit`

ステップ 4	出力帯域幅ポリシーを設定します。	**（注）** まず class-default と class-fcoe のデフォルトの帯域幅設定を小さくすれば、ユーザ定義のクラス cmap-que-bandwidth に帯域幅を正常に割り当てることができます。
		`(config)# policy-map type queuing pmap-que-eth1-2`
		`(config-pmap-que)# class type queuing class-default`
		`(config-pmap-c-que)# bandwidth percent 10`
		`(config-pmap-c-que)# exit`
		`(config-pmap-que)# class type queuing class-fcoe`
		`(config-pmap-c-que)# bandwidth percent 40`
		`(config-pmap-c-que)# exit`
		`(config-pmap-que)# class type queuing cmap-que-bandwidth`
		`(config-pmap-c-que)# bandwidth percent 50`
		`(config-pmap-c-que)# exit`
		`(config-pmap-que)# exit`

	コマンドまたはアクション	目的
ステップ 5	帯域幅ポリシーを出力インターフェイスに追加します。	(config)# **interface ethernet 1/3** (config-if)# **service-policy type queuing output pmap-que-eth1-2** (config-if)# **exit**
ステップ 6	システム クラスを qos-group 2 に割り当てます。	(config)# **class-map type network-qos cmap-nq-bandwidth** (config-cmap-nq)# **match qos-group 2** (config-cmap-nq)# **exit**
ステップ 7	network-qos ポリシーを設定します。	(config)# **policy-map type network-qos pmap-nq-bandwidth** (config-pmap-nq)# **class type network-qos cmap-nq-bandwidth** (config-pmap-c-nq)# **exit** (config-pmap-nq)# **exit**
ステップ 8	network-qos ポリシーをシステムに追加します。	(config)# **system qos** (config-sys-qos)# **service-policy type network-qos pmap-nq-bandwidth** (config-sys-qos)# **exit**

QoS 例 3

次の例は、CoS 値 3 の 802.1p タグを着信タグなしパケットに追加し、イーサネット インターフェイス 1/15 にプライオリティ フロー制御ネゴシエーションを強制的に設定する方法を示しています。

手順

	コマンドまたはアクション	目的
ステップ 1	入力分類ポリシーを設定します（アクセス コントロール リストは定義済みです）。	(config)# **interface Ethernet 1/15** (config-if)# **untagged cos 3** (config-if)# **priority-flow-control mode on** (config-if)# **exit**

索 引

W

い

か

き

く

こ

さ

し

す

せ

た

ち

て

に

ふ

ほ

ま

も

ゆ

ら

れ