QoS モジュラ QoS コマンドライン インターフェイス 設定ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL:http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

MQC を使用した QoS 機能の適用 3

機能情報の確認 3

MQC を使用した QoS 機能の適用に対する制約事項 4

MQC を使用した QoS 機能の適用について 6

MQC 構造 6

トラフィック クラスの要素 6

トラフィック ポリシーの要素 9

ネストしたトラフィック クラス 12

class-map コマンドの match-all キーワードと match-any キーワード 12

service-policy コマンドの input および output キーワード 13

MQC を使用して QoS 機能を適用することの利点 13

MQC を使用した QoS 機能の適用方法 13

トラフィック クラスの作成 13

トラフィック ポリシーの作成 15

MQC を使用したインターフェイスへのトラフィック ポリシーの適用 17

トラフィック クラスとトラフィック ポリシー情報の確認 18

MQC を使用した QoS 機能の適用の設定例 19

トラフィック クラスの作成 19

ポリシー マップの作成 20

例：トラフィック ポリシーのインターフェイスへの適用 20

match not コマンドの使用 20

デフォルト トラフィック クラスの設定 21

「class-map match-any」コマンドと「class-map match-all」コマンドの違い 21

一致基準としてのトラフィック クラス（ネストしたトラフィック クラス）の確立 22

例：メンテナンスのためにネストされたトラフィック クラス 23

例：match-any 特性と match-all 特性を 1 つのトラフィック クラスで組み合わせるためのネストしたトラフィック クラス 23
例：QoS ポリシーとしてのトラフィック ポリシー（階層型トラフィック ポリシー） 24
その他の参考資料 24
MQC を使用した QoS 機能の適用の機能情報 25
3 レベルのユーザ定義キューイング ポリシーのサポート 29
機能情報の確認 29
3 レベルのユーザ定義キューイング ポリシーのサポートに関する制約事項 30
3 レベルのユーザ定義キューイング ポリシーのサポートに関する情報 30
階層型 QoS の 3 つのパラメータによるスケジューラ 30
階層型ポリシーのガイドライン 31
HQoS の最上位レベル ポリシーのユーザ定義トラフィック クラス 32
3 レベルのユーザ定義のキューイング ポリシー サポートの設定方法 32
3 レベルの階層型 QoS ポリシーの設定 32
最上位レベルのポリシーでのユーザ定義のトラフィック クラスの設定 32
3 レベルのユーザ定義のキューイング ポリシー サポートに関するその他の参考資料 33
3 レベルのユーザ定義キューイング ポリシーのサポートの機能情報 34
IP/ATM 間サービス クラスの設定 35
機能情報の確認 35
単一の ATM VC での IP/ATM 間 CoS の設定タスク リスト 36
WRED パラメータ グループの定義 36
WRED パラメータ グループの設定 36
WRED パラメータの表示 37
キューイング統計情報の表示 37
ATM バンドルでの IP/ATM 間 CoS の設定タスク リスト 37
VC バンドルの作成 37
バンドルレベルのパラメータの適用 38
バンドル レベルのパラメータの設定 38
バンドルに適用する VC クラスのパラメータの設定 39
バンドルへのクラスの適用 39

バンドルへの VC のコミット 40

個々の VC へのパラメータの適用 40

VC バンドル メンバーの直接設定 40

VC バンドル メンバーに適用する VC クラスのパラメータの設定 41

個々の VC バンドル メンバーへの VC クラスの適用 41

バンピングされたトラフィックを拒否する場合の VC の設定 42

VC バンドルとそれらの VC メンバーのモニタリングと保守 42

VC 単位の WFQ および CBWFQ の設定タスク リスト 42

クラスベースの重み付け均等化キューイングの設定 42

サービス ポリシーの適用と VC に対する CBWFQ のイネーブル化 44

スタンドアロン VC へのポリシー マップの適用と CBWFQ のイネーブル化 44

個々の VC へのポリシー マップの適用と CBWFQ のイネーブル化 44

フローベースの WFQ を使用する場合の VC の設定 44

スタンドアロン VC へのポリシー マップの適用と WFQ のイネーブル化 45

個々の VC へのポリシー マップの適用と WFQ のイネーブル化 46

VC 単位の WFQ および CBWFQ のモニタリング 46

コンソールへのエラー メッセージのロギングのイネーブル化 46

IP/TM 間 CoS の設定例 46

例：WRED グループおよび IP プレシデンスを使用した単一の ATM VC 46

例：VC クラスを使用した VC バンドルの設定 47

Bundle-Class クラス 47

Control-Class クラス 47

Premium-Class クラス 47

Priority-Class クラス 48

Basic-Class クラス 48

new-york バンドル 48

san-francisco バンドル 49

los-angeles バンドル 50

例：スタンドアロン VC での VC 単位の WFQ と CBWFQ 50

例：バンドルメンバー VC での VC 単位の WFQ と CBWFQ 51

複雑な階層型スケジュール：フラグメント化されたポリシー（ポリシー集約） 53

QoS の前提条件：ポリシー集約 54

QoS の制約事項：ポリシー集約 54
QoS について：ポリシー集約 54
クラス定義文内のフラグメント 54
Gigabit EtherChannel バンドルのフラグメント 55
ポリシー マップ内のフラグメント トラフィック クラス 56
サービス フラグメント トラフィック クラスについて 56
QoS：ポリシー集約 MQC 56
複数キュー集約の元の機能と MQC サポートの違い 57
キュー制限と WRED しきい値の変更 59
QoS の設定例：ポリシー集約 59
例 1：QoS の設定：インターフェイスのポリシー集約 59
ポリシー マップでのフラグメント トラフィック クラスの設定 59
次の作業 60
サービス フラグメントのトラフィック クラスの設定 61
トラブルシューティングのヒント 64
次の作業 64
QoS の設定：Gigabit EtherChannel でのポリシー集約 64
Gigabit EtherChannel バンドルをサポートする物理インターフェイスでのサービス フラグメントの設定 64
トラブルシューティングのヒント 66
次の作業 66
Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定 66
トラブルシューティングのヒント 69
QoS の設定方法：ポリシー集約 MQC 69
QoS のサービス ポリシーのアップグレード：ポリシー集約 MQC 69
はじめる前に 69
アップグレード作業 70
QoS の設定：ポリシー集約 MQC トラフィック クラス 71
サブスクライバ インターフェイスでのトラフィック クラスの設定 71
次の作業 72
サブインターフェイスでのフラグメント トラフィック クラスの設定 72

次の作業 72
メイン インターフェイスでのトラフィック クラスの設定 72
次の作業 74
メイン インターフェイスでのサービス フラグメント トラフィック クラスの設定 74
次の作業 74
QoS の設定：ポリシー集約 MQC サポート 74
トラフィック ポリシー クラスのポリシー情報とドロップ統計情報の確認 74
QoS の設定例：ポリシー集約 75
例：QoS：ポリシー集約 75
例：Gigabit EtherChannel QoS ポリシー集約 76
例：メイン インターフェイスでの QoS ポリシー集約 77
その他の参考資料 79
QoS の機能情報：ポリシー集約 80
レガシー QoS コマンドの廃止予定 83
機能情報の確認 83
レガシー QoS コマンドの廃止予定に関する情報 84
MQC を使用して適用した QoS 機能 84
隠しレガシー コマンド 84
その他の参考資料 94
レガシー QoS コマンドの廃止予定に関する機能情報 95
QoS パケット マーキング 103
QoS パケット分類について 103
マーキングの定義 103
パケットをマーキングする理由 104
マーキング パケットに対するアプローチ 105
マーキング アクションの範囲 106
複数の set ステートメント 106
内部指定子のマーキング 107
入力マーキング アクションと出力マーキング アクション 107
インポジション マーキング 107
QoS パケット マーキングの設定例 109

例 1：入力マーキングの設定 109
例 2：出力マーキングの設定 109
例 3：MPLS EXP インポジションの設定 110
例 4：トンネル インポジション マーキングの設定 110
例 5：QoS グループ マーキングの設定 111
例 6：discard-class マーキングの設定 112
QoS パケット マーキングの確認 112
show policy-map interface コマンドでの確認 113
QoS パケット マーキング統計情報での確認 114
QoS パケット マーキング統計情報のイネーブル化 115
QoS パケット マーキング統計情報の表示 115
データプレーン設定の検証 116
ネットワーク レベルの設定例 117
例 1：ネットワーク全体にわたるサービス クラス情報の伝達 118
例 2：ネットワークのエッジでのマーキングによるサービス クラスの指定 119
例 3：サービス プロバイダーの要件に一致させるためのトラフィックの再マーキング 121
例 4：SP ネットワークに対するトンネル インターフェイスでの再マーキング □ Gotcha の可能性 123
例 5：トンネル インポジション マーキングを使用した SP ネットワークに対する再マーキング 125
コマンド リファレンス 126
platform qos marker-statistics 126
set atm-clp 127
set cos 128
set cos-inner 128
set discard-class 129
set dscp 130
set dscp tunnel 131
set fr-de 132
set ip dscp 132
set ip dscp tunnel 133
set ip precedence 133

set ip precedence tunnel 133
set mpls experimental imposition 133
set mpls experimental topmost 134
set precedence 135
set precedence tunnel 136
set qos-group 136
QoS パケット一致統計情報の設定 139
機能情報の確認 139
QoS パケット一致統計情報機能の前提条件 140
QoS パケット一致統計情報機能の制約事項 140
QoS パケット一致統計情報に関する情報 141
QoS パケット一致統計情報：フィルタ単位の機能の概要 141
QoS パケット一致統計情報：ACE 単位の機能の概要 142
QoS パケット一致統計情報の設定方法 143
QoS パケット一致統計情報の設定：フィルタ単位 144
QoS パケット一致統計情報の設定：ACE 単位 147
トラブルシューティングのヒント 151
例：QoS パケット一致統計情報の設定：フィルタ単位 151
その他の参考資料 152
QoS パケット一致統計情報の機能情報 153
ポリサーを使用した ATM CLP 設定ビット 155
機能情報の確認 155
ポリサーを使用した ATM CLP 設定ビットの前提条件 156
ポリサーを使用した ATM CLP 設定ビットに関する情報 156
ATM CLP ビット 156
ポリサーを使用した ATM CLP ビットの設定方法 157
PPPoA ブロードバンドのトラフィック ポリシングの設定 157
ATM CLP ビットのマーキング 159
ポリサーを使用した ATM CLP 設定ビットの設定例 161
例：クラスに一致するポリサー アクションによる ATM CLP のマーキング 161
例：ポリサー アクションのポリシングされたしきい値による ATM CLP のマーキング 162
その他の参考資料 162

ポリサーを使用した ATM CLP 設定ビットの機能情報 164
EVC Quality of Service 165
機能情報の確認 165
EVC での Quality of Service に関する情報 166
EVC Quality of Service と MQC 166
QoS 対応イーサネット フロー ポイント（EFP） 166
QoS 機能と EVC 167
EVC QoS がサポートするトラフィック分類の match コマンド 167
1 つのトラフィック クラスでの複数の match コマンド 168
EVC で QoS 機能をイネーブルにするために使用するコマンド 169
service-policy コマンドの input および output キーワード 171
EVC での Quality of Service 機能の設定方法 172
EVC で使用するトラフィック クラスの作成 172
EVC で使用するポリシー マップの作成 173
EVC の設定および EVC へのトラフィック ポリシーの適用 175
EVC QoS の設定例 177
例：EVC で使用するトラフィック クラスの作成 177
例：EVC で使用するポリシー マップの作成 178
例：EVC の設定と EVC へのトラフィック ポリシーの適用 178
例：EVC のトラフィック クラスおよびトラフィック ポリシー情報の確認 179
その他の参考資料 179
EVC QoS を設定するための機能情報 180
EtherChannel インターフェイスの QoS 183
機能情報の確認 183
EtherChannel の QoS に関する情報 184
QoS 機能を備えた EtherChannel の進化 184
クラス定義文内のフラグメントについて 185
Gigabit EtherChannel バンドルのフラグメント 186
QoS：ポリシー集約 MQC 186
元の機能と複数キューの集約に対する MQC サポートとの違い ポリシー集約の違い：サブインターフェイスでの出力MQCキューイングとメインインターフェイスでの複数キューの集約に対する MQC サポート 187

EtherChannel 用の QoS の設定方法 188
ポートチャネルのサブインターフェイスでの出力 MQC キューイングの設定 188
ポートチャネルのメンバー リンクでの出力 MQC キューイングの設定 189
QoS のポリシー集約の設定：サブインターフェイスでの出力 MQC キューイング 191
ポリシー マップでのフラグメント トラフィック クラスの設定 192
次の作業 193
サービス フラグメントのトラフィック クラスの設定 193
トラブルシューティングのヒント 197
次の作業 197
Gigabit EtherChannel バンドルをサポートする物理インターフェイスでのサービス フラグメントの設定 197
Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定 199
ポートチャネル サブインターフェイスでの入力ポリシングとマーキングの設定 200
ポートチャネルのメンバー リンクでの出力ポリシングとマーキングの設定 202
ポリシー集約の設定：メイン インターフェイスでの複数キュー集約に対する MQC サポート 204
ポートチャネルのメンバー リンクでの MQC キューイング設定：EtherChannel ロード バランシングなし 205
ポートチャネルのメンバー リンクでの MQC キューイング設定の設定：EtherChannel ロード バランシング 207
EtherChannels の QoS の設定例 209
例：QoS ポリシー集約の設定：サブインターフェイスでの出力 MQC キューイング 209
例：QoS ポリシー集約の設定：メイン インターフェイスでの複数キュー集約に対する MQC サポート 210
その他の参考資料 211
EtherChannel インターフェイスの QoS の機能情報 211
集約 EtherChannel QoS 215
集約 EtherChannel QoS の制約事項 215
集約 EtherChannel QoS に関する情報 216
集約 EtherChannel QoS のサポート対象機能 216

集約 EtherChannel QoS のサポート対象外機能の組み合わせ 216
集約 EtherChannel QoS のスケーラビリティ 217
集約 EtherChannel QoS の設定方法 217
集約 EtherChannel QoS の設定解除方法 219
集約 EtherChannel QoS の設定例 219
例：集約ポートチャネル インターフェイスの設定 219
例：QoS に対するクラス マップの設定 220
例：QoS に対するポリシー マップの設定 220
例：ポート チャネル インターフェイスへの QoS の適用 221
集約 EtherChannel サブインターフェイス QoS の設定方法 221
集約 EtherChannel サブインターフェイス QoS の設定解除方法 223
集約 EtherChannel サブインターフェイス QoS の設定例 224
例：集約ポートチャネル インターフェイスとサブインターフェイスの設定 224
例：QoS に対するクラス マップの設定 224
例：QoS に対するポリシー マップの設定 224
例：ポート チャネル サブインターフェイスへの QoS の適用 225
その他の参考資料 225
集約 EtherChannel QoS の機能情報 226
PPPoGEC のセッション単位の QoS 229
機能情報の確認 229
PPPoGEC のセッション単位の QoS について 230
PPPoGEC のセッション単位の QoS に関する制約事項 230
アクティブ/スタンバイ EtherChannel による PPPoGEC 230
PPPoGEC のセッション単位の QoS の設定方法 231
EtherChannel アクティブ/スタンバイによる PPPoE セッションでの QoS の設定 231
PPPoGEC のセッション単位の QoS の設定例 232
例：EtherChannel アクティブ/スタンバイによる PPPoE セッションでの QoS 232
PPPoGEC のセッション単位の QoS のその他の参考資料 233
PPPoGEC のセッション単位の QoS の機能情報 234
IPv6 選択的パケット廃棄 237
機能情報の確認 237
IPv6 選択的パケット廃棄に関する情報 238

IPv6 での SPD の概要 238
SPD ステート チェック 238
SPD モード 238
SPD ヘッドルーム 238
IPv6 選択的パケット廃棄の設定方法 239
SPD プロセス入力キューの設定 239
SPD モードの設定 240
SPD ヘッドルームの設定 241
IPv6 選択的パケット廃棄の設定例 242
例：SPD プロセス入力キューの設定 242
その他の参考資料 243
IPv6 選択的パケット廃棄の機能情報 243
ACE 単位の QoS 統計情報 245
機能情報の確認 245
ACE 単位の QoS 統計情報の前提条件 246
ACE 単位の QoS 統計情報の制約事項 246
ACE 単位の QoS 統計情報に関する情報 246
ACE 単位の QoS 統計情報の概要 246
ACE 単位の QoS 統計情報の設定方法 248
ACE 単位の QoS 統計情報の設定 248
ACE 単位の QoS 統計情報のその他の参考資料 249
ACE 単位の QoS 統計情報の機能情報 250

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

MQC を使用した QoS 機能の適用

ここでは、トラフィック クラスとそれらのクラスに適用される処理を定義するためのシスコ全体にわたる標準であるモジュラ Quality of Service（QoS）コマンドラインインターフェイス（CLI）（MQC）について説明します。

- 機能情報の確認，3 ページ
- MQC を使用した QoS 機能の適用に対する制約事項，4 ページ
- MQC を使用した QoS 機能の適用について，6 ページ
- MQC を使用した QoS 機能の適用方法，13 ページ
- MQC を使用した QoS 機能の適用の設定例，19 ページ
- その他の参考資料，24 ページ
- MQC を使用した QoS 機能の適用の機能情報，25 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MQC を使用した QoS 機能の適用に対する制約事項

MQC ベースの QoS は、Internetwork Packet Exchange（IPX）、DECnet、AppleTalk などとは異なり、レガシー レイヤ 2 プロトコル パケットの分類をサポートしません。このタイプのパケットが一般的なレイヤ 2 トンネリング メカニズムによって転送されると、パケットは MQC により処理されますが、プロトコル分類はされません。その結果、レイヤ 2 トンネルのレガシー プロトコル トラフィックは、「match any」クラスまたは class-default によってのみ照合されます。

サポートされる QoS ポリシー マップとクラス マップの数は、プラットフォームとリリースにより異なります。

（注） ポリシーマップの制限は、適用されるポリシーマップのインスタンスの数ではなく、ポリシーマップの定義を参照します。

次の制限は、Cisco ASR 903 ルータ用 Cisco IOS XE リリース 3.5S に適用されます。

- QoS ポリシー マップはセッションではサポートされません。
- ネストしたトラフィック マップはサポートされません。

Cisco ASR 903 ルータの制約事項の詳細については、『Quality of Service Configuration Guidelines for Cisco ASR 903 Router』を参照してください。

表 *1*：*Cisco ASR 903* のポリシーとクラス マップのサポート

	Cisco IOS XE 3.5S、3.6S、3.7S、3.8S	**Cisco IOS XE 3.9S 以上**
固有のポリシー マップの数	1024	1024
固有のクラス マップの数	4096	4096
1 ポリシーマップあたりのクラス数	512	4096
1 クラスマップあたりのフィルタ数	16	16

表 *2*：*Cisco ASR 1000* シリーズのポリシーとクラス マップのサポート

	Cisco IOS XE 2.0S、2.1S、2.2S	**Cisco IOS XE 2.3S**	**Cisco IOS XE 3.5S、3.6S、3.7S、3.8S、3.9S**	**Cisco IOS XE 3.10S 以上**
固有のポリシー マップの数	1024	4096	4096	4096 16000（RP2、ESP40、ESP100、ESP200 モデルのみ）
固有のクラスマップの数	4096	4096	4096	4096
1 ポリシー マップあたりのクラス数	8	256	1000	1000
1 クラス マップあたりのフィルタ数	16	16	32	32

表 *3*：*Cisco CSR 1000V* のポリシーとクラス マップのサポート

	Cisco IOS XE 3.10S、3.11S、3.12S	**Cisco IOS XE 3.13S 以上**
固有のポリシー マップの数	30	256
固有のクラス マップの数	256	512
1ポリシーマップあたりのクラス数	32	512
1 クラス マップあたりのフィルタ数	8	16

表 *4*：*Cisco ISR 4000* シリーズ サービス統合型ルータのポリシーとクラス マップのサポート

	Cisco IOS XE 3.9.1S、3.9.2	**Cisco IOS XE 3.10S（ISR 4451のみ）**
固有のポリシー マップの数	4096	4000
固有のクラス マップの数	4096	4096

	Cisco IOS XE 3.9.1S、3.9.2	Cisco IOS XE 3.10S（ISR 4451のみ）
1 ポリシーマップあたりのクラス数	1000	256
1 クラスマップあたりのフィルタ数	32	32

MQC を使用した QoS 機能の適用について

MQC 構造

MQC（モジュラ QoS コマンドライン インターフェイス（CLI））では、QoS グループ値に基づいてパケット分類とマーキングを設定できます。MQC CLI では、トラフィック クラスおよびポリシーを作成し、QoS機能（パケット分類など）をイネーブルにして、それらのポリシーをインターフェイスに適用することができます。

MQC 構造は、大きく次の 3 つの手順からなります。

トラフィック クラスの要素

トラフィック クラスに含まれる 3 つの主な要素は、トラフィック クラス名、一連の **match** コマンド、およびトラフィック クラスで複数の **match** コマンドが使用される場合にそれらの **match** コマンドを評価する方法です。

match コマンドは、パケットを分類するために使用します。パケットがチェックされ、**match** コマンドで指定された条件を満たすかどうかが判断されます。パケットが指定された条件を満たしている場合、パケットはそのクラスのメンバーと見なされます。一致条件を満たしていないパケットは、デフォルト トラフィック クラスのメンバーとして分類されます。

利用可能な match コマンド

次の表に、MQC で使用できる **match** コマンドの一部を示します。使用可能な **match** コマンドは、Cisco IOS XE のリリースによって異なります。コマンドおよびコマンド シンタックスの詳細については、『*Cisco IOS Quality of Service Solutions* Command Reference』を参照してください。

表 *5*：*MQC* で使用可能な *match* コマンド

コマンド	目的
matchaccess-group	指定したアクセスコントロールリスト（ACL）に基づいて、クラスマップの一致基準を設定します。
matchany	すべてのパケットに対して適切に一致する基準となる、クラス マップの一致基準を設定します。
matchcos	レイヤ 2 サービス クラス（CoS）マーキングに基づいてパケットを照合します。
matchdestination-addressmac	宛先 MAC アドレスを一致条件として使用します。
matchdiscard-class	特定の廃棄クラスのパケットを照合します。
match [**ip**] **dscp**	特定の IP Diffserv コード ポイント（DSCP）値を一致条件として識別します。1 つの match 文に最大 8 つの DSCP 値を含めることができます。
matchfr-dlci	クラスマップで一致基準としてフレーム リレーデータリンク接続識別子（DLCI）番号を指定します。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchiprtp	Real-Time Transport Protocol（RTP）ポートを一致条件として使用するようにクラスマップを設定します。
matchmplsexperimental	指定されたマルチプロトコル ラベル スイッチング（MPLS）の EXP フィールドの値を一致基準として使用するクラスマップを設定します。
matchmplsexperimentaltopmost	最上位ラベル内の MPLS EXP 値を照合します。

コマンド	目的
matchnot	成功しない一致基準として使用する、1 つの一致基準値を指定します。 （注） **matchnot** コマンドは、一致基準として使用する特定の match パラメータを指定する代わりに、パケットがクラスのメンバーとして分類されるのを防ぐ一致基準を指定するために使用します。たとえば、トラフィック クラスの設定中に **matchnotqos-group6** コマンドを発行すると、QoS グループ 6 だけが、成功する一致基準として考慮されない QoS グループ値となります。他の QoS グループ値は成功する一致基準となります。
matchpacketlength	IP ヘッダー中のレイヤ 3 パケット長をクラスマップ中の一致条件として指定します。
matchport-type	トラフィックを、クラス マップのポート タイプに基づいて照合します。
match [ip] precedence	IP precedence 値を一致基準として識別します。
matchprotocol	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。 （注） 個別の **matchprotocol** (NBAR) コマンドを使用すると、Network-Based Application Recognition（NBAR）が認識しているプロトコル タイプでトラフィックを照合するように NBAR を設定できます。
matchprotocolfasttrack	FastTrack ピアツーピア トラフィックを照合するように NBAR を設定します。
matchprotocolgnutella	Gnutella ピアツーピア トラフィックを照合するように NBAR を設定します。
matchprotocolhttp	URL、ホスト、多目的インターネット メール拡張（MIME）タイプ、HTTP パケット ヘッダー内のフィールドによってハイパーテキスト転送プロトコル（HTTP）トラフィックを照合するように NBAR を設定します。

コマンド	目的
matchprotocolrtp	RTP トラフィックを照合するように NBAR を設定します。
matchqos-group	特定の QoS グループ値を一致基準として識別します。
matchsource-addressmac	送信元 MAC アドレスを一致基準として使用します。

1 つのトラフィック クラスでの複数の match コマンド

トラフィック クラスに複数の **match** コマンドが含まれている場合、それらの **match** コマンドの評価方法を指定する必要があります。指定するには、**class-map** コマンドの **match-any** キーワードまたは **match-all** キーワードを使用します。**match-any** キーワードと **match-all** キーワードついては、次の点に注意してください。

- **match-any** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した基準の *1* つに一致する必要があります。
- **match-all** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した基準のすべてに一致する必要があります。
- どちらのキーワードも指定しなかった場合、トラフィック クラスによって評価されるトラフィックは、指定した基準のすべてに一致する必要があります（つまり、**match-all** キーワードの動作が使用されます）。

トラフィック ポリシーの要素

トラフィック ポリシーには、トラフィック ポリシー名、トラフィック クラス（**class** コマンドで指定）、QoS 機能をイネーブルにするために使用するコマンドの 3 つの要素が含まれています。

ポリシー マップをインターフェイスに適用すると（**service-policy** コマンドを使用）、トラフィック ポリシー（ポリシー マップ）は、イネーブルにした QoS 機能をトラフィック クラスに適用します。

（注） パケットは、トラフィック ポリシー内のいずれかのトラフィック クラスだけに一致します。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義されている最初のトラフィック クラスが使用されます。

QoS 機能をイネーブルにするために使用するコマンド

QoS 機能をイネーブルにするために使用するコマンドは、Cisco IOS XE リリースごとに異なります。以下の表に、使用可能なコマンドとそれによってイネーブルになる QoS 機能の一部を示します。コマンド構文の詳細については、『*Cisco IOS QoS Command Reference*』を参照してください。

イネーブルにする特定の QoS 機能の詳細については、『Cisco IOS XE Quality of Service Solutions Configuration Guide』の適切なモジュールを参照してください。

表 *6*：*QoS* 機能をイネーブルにするために使用するコマンド

コマンド	目的
bandwidth	クラスの最小帯域幅保証を設定します。
bandwidthremaining	クラスの過剰重量を設定します。
fair-queue	トラフィック クラス内のフローベースのキューイング機能をイネーブルにします。
drop	指定したトラフィック クラスのパケットを廃棄します。
police	トラフィック ポリシングを設定します。
police(percent)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police(tworates)	認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートを使用したトラフィック ポリシングを設定します。
priority	ポリシーマップに属するトラフィックのクラスにプライオリティを与えます。
queue-limit	ポリシーマップで設定されているクラスに対してキューが保持できるパケットの最大数を指定または変更します。
random-detect	重み付けランダム早期検出（WRED）をイネーブルにします。
random-detectdiscard-class	ポリシー マップ内のクラスの discard-class 値に対し、WRED パラメータを設定します。
random-detectdiscard-class-based	パケットの廃棄クラス値に基づく WRED を設定します。

コマンド	目的
random-detectexponential-weighting-constant	クラス用に予約されたキューの平均キューサイズ計算用の指数加重係数を設定します。
random-detectprecedence	ポリシーマップ内のクラスポリシーに対する、特定の IP precedence の WRED パラメータを設定します。
service-policy	一致基準として使用するトラフィックポリシーの名前を指定します（トラフィックポリシーを互いにネストさせるため（階層型トラフィックポリシー））。
setatm-clp	ポリシーマップを設定するときのセル損失率優先度（CLP）ビットを設定します。
setcos	送信パケットのレイヤ 2 サービス クラス（CoS）値を設定します。
setdiscard-class	discard-class 値でパケットをマークします。
set[**ip**] **dscp**	タイプ オブ サービス（ToS）バイト内の DiffServ コード ポイント（DSCP）値を設定することでパケットをマークします。
setfr-de	インターフェイスから送信されるすべてのトラフィックに対し、フレームリレーフレームのアドレス フィールドの廃棄適性（DE）ビット設定を 1 に変更します。
setmplsexperimental	パケットが指定したポリシーマップに一致する場合に MPLS ビットを設定する値を指定します。
setprecedence	パケット ヘッダーに precedence 値を設定します。
setqos-group	後でパケットを分類するために使用できる QoS グループ ID を設定します。
shape	指定したアルゴリズムに従って、指示されたビット レートまでトラフィックをシェーピングします。

ネストしたトラフィック クラス

MQC では、必ずしも 1 つのトラフィック クラスだけを 1 つのトラフィック ポリシーに関連付ける必要はありません。

パケットが複数の一致基準を満たしているシナリオでは、MQC により複数のトラフィック クラスを 1 つのトラフィック ポリシー（ネストしたトラフィック クラスとも呼ぶ）に関連付けることができます。これを行うには、**matchclass-map** コマンドを使用します（これらをネストしたクラス マップまたは *MQC* 階層型クラス マップと呼びます）。 このコマンドで、1 つのトラフィック クラス内で match-any 特性と match-all 特性を組み合わせる唯一の方法が提供されます。これを実行することにより、1 つの一致基準評価命令（match-any と match-all のどちらか）を使用してトラフィック クラスを作成して、そのトラフィック クラスを別の一致基準タイプを使用するトラフィック クラス内に一致基準として使用できます。たとえば、match-any 命令を使用して作成したトラフィック クラスは match-all 命令を一致基準として使用して設定したクラスを使用する必要があり、その逆の場合も同様です。

考えられるシナリオは次のとおりです。A、B、C、および D が、すべて異なる一致基準であるとし、A、B、または C かつ D（A または B または（C かつ D））に一致するトラフィックをトラフィック クラスに属するものとして分類するとします。ネストしたトラフィック クラスがない場合、トラフィックがトラフィック クラスの一部であると見なされるためには、4 つの一致基準すべてに一致するか（A かつ B かつ C かつ D）、いずれかの一致基準に一致する必要があります（A または B または C または D）。「かつ」（match-all）文と「または」（match-any）文をトラフィック クラス内で組み合わせることはできないため、目的の設定を実現できません。

解決策：C と D に対して match-all を使用する 1 つのトラフィック クラスを作成し（これを条件 E と呼びます）、A、B、E を使用して新しい match-any トラフィック クラスを作成します。新しいトラフィック クラスの評価順序は正しくなります（A または B または E、つまり A または B または（C かつ D））。

class-map コマンドの match-all キーワードと match-any キーワード

トラフィック クラスを作成するときに使用するコマンドの 1 つが **class-map** コマンドです。**class-map** コマンドのコマンド シンタックスには、2 つのキーワード **match-all** と **match-any** が含まれています。**match-all** キーワードと **match-any** キーワードの指定が必要になるのは、トラフィック クラスで複数の一致条件を設定する場合だけです。これらのキーワードについて、次の点に注意してください。

- **match-all** キーワードは、パケットを指定したトラフィック クラスに分類するために、トラフィック クラス内のすべての一致基準に一致する必要がある場合に使用します。
- **match-any** キーワードは、パケットを指定したトラフィック クラスに分類するために、トラフィック クラス内の *1* つの一致基準だけに一致する必要がある場合に使用します。
- **match-all** キーワードも **match-any** キーワードも指定しない場合、トラフィック クラスの動作は、**match-all** キーワードを指定した場合と同じになります。

service-policy コマンドの input および output キーワード

一般的な規則として、トラフィック ポリシーで設定する QoS 機能は、インターフェイスで受信されるパケットか、インターフェイスで送信されるパケットに適用できます。そのため、**service-policy** コマンドを使用する場合は、**input** キーワードまたは **output** キーワードを使用してトラフィック ポリシーの方向を指定する必要があります。

たとえば、**service-policyoutputpolicy-map1** コマンドは、トラフィック ポリシーの QoS 機能を出力方向のインターフェイスに適用します。インターフェイス（出力）から送信されるすべてのパケットが、policy-map1 という名前のトラフィック ポリシーで指定された基準に従って評価されます。

（注） Cisco のリリースでは、キューイング メカニズムは入力方向ではサポートされていません。非キューイング メカニズム（トラフィック ポリシングやトラフィック マーキングなど）は、入力方向でサポートされています。また、送信元 MAC アドレスに基づくトラフィックの分類（**matchsource-addressmac** コマンドを使用）は、入力方向でのみサポートされています。

MQC を使用して QoS 機能を適用することの利点

MQC 構造では、一度トラフィック ポリシー（ポリシー マップ）を作成すると、必要な数のトラフィック クラスに適用できます。また、トラフィック ポリシーを必要な数のインターフェイスに適用できます。

MQC を使用した QoS 機能の適用方法

トラフィック クラスの作成

トラフィック クラスを作成するには、**class-map** コマンドを使用してトラフィック クラス名を指定します。次に、1 つ以上の **match** コマンドを使用して、適切な一致基準を指定します。指定した基準に一致するパケットがトラフィック クラスに分類されます。class-map コマンドの **match-all** キーワードと **match-any** キーワードの詳細については、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。

（注） **matchcos** コマンドはステップ 4 に記載されています。**matchcos** コマンドは、使用できる **match** コマンドの 1 つに過ぎません。他の利用可能な **match** コマンドについては、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **matchcos***cos-number*
5. 必要に応じて追加の match コマンドを入力します。追加のコマンドが不要な場合はステップ 6 に進みます。
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Router(config)# class-map match-any class1`	クラス マップで使用するクラスを作成し、クラス マップ コンフィギュレーション モードを開始します。 • クラスマップは、パケットを指定したクラスに照合するために使用します。 • クラス名を入力します。 （注） **match-all** キーワードは、すべての一致基準が満たされることが必要であることを指定します。**match-any** キーワードは、いずれかの一致条件が満たされることが必要であることを指定します。これらのキーワードは、複数の **match** コマンドを指定する場合にだけ使用します。
ステップ 4	**matchcos***cos-number* 例： `Router(config-cmap)# match cos 2`	レイヤ 2 サービスクラス（CoS）番号に基づいてパケットを照合します。 • CoS 番号を入力します。

	コマンドまたはアクション	目的
		（注） **matchcos** コマンドは、使用できる **match** コマンドの一例です。他の利用可能な **match** コマンドについては、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。
ステップ 5	必要に応じて追加の match コマンドを入力します。追加のコマンドが不要な場合はステップ 6 に進みます。	--
ステップ 6	**end** 例： `Router(config-cmap)# end`	（任意）QoS class-map コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラフィック ポリシーの作成

（注） **bandwidth** コマンドはステップ 5 に記載されています。**bandwidth** コマンドは、QoS 機能を有効にするためにポリシー マップで使用できるコマンドの一例です（ここでは、クラスベース均等化キューイング（CBWFQ））。利用可能なその他のコマンドの詳細については、「トラフィック ポリシーの要素」セクションを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **percent***percent*}
6. イネーブルにする追加の QoS 機能に対するコマンドを入力します。他に QoS 機能が必要ない場合は、ステップ 7 に進みます。
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map policy1`	トラフィック ポリシーの名前を作成または指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class class1`	トラフィック クラスの名前を指定し、QoS 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。 （注） この手順により、トラフィック クラスがトラフィック ポリシーに関連付けられます。
ステップ 5	**bandwidth** {*bandwidth-kbps* | **percent***percent*} 例： `Router(config-pmap-c)# bandwidth 3000`	（任意）トラフィック クラスに対する輻輳期間中の最小帯域幅保証を指定します。 • 最小帯域幅保証は、kb/s 単位か、使用可能な全帯域幅のパーセンテージで指定します。 （注） **bandwidth** コマンドを使用すると CBWFQ がイネーブルになります。**bandwidth** コマンドは、QoS 機能をイネーブルにするためにポリシーマップで使用できるコマンドの一例です。利用可能なその他のコマンドの詳細については、「トラフィック ポリシーの要素」セクションを参照してください。
ステップ 6	イネーブルにする追加の QoS 機能に対するコマンドを入力します。他に QoS 機能が必要ない場合は、ステップ 7 に進みます。	--
ステップ 7	**end** 例： `Router(config-pmap-c)# end`	（任意）QoS 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、特権 EXEC モードに戻ります。

MQC を使用したインターフェイスへのトラフィック ポリシーの適用

（注）

（注） Cisco IOS XE リリース 2.3.0 以降では、VC または仮想パス（VP）のデフォルト モードとして未指定ビット レート（UBR）を設定した ATM インターフェイスへのポリシーの追加をサポートしていません。この設定を使用すると、UBR を設定した ATM インターフェイスではサポートされていないことを示すエラー メッセージ（CBWFQ）が表示されます。また、デフォルト UBR 値を使用しない場合は、UBR 設定で任意の UBR を指定することもできます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **service-policy**{**input** | **output**} *policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**interface***typenumber* 例： `Router(config)# interface serial 0/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイス タイプとインターフェイス番号を入力します。

	コマンドまたはアクション	目的
ステップ 4	**service-policy**{**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input policy1`	ポリシー マップをインターフェイスに付加します。 • **input** キーワードまたは **output** キーワードとポリシー マップ名を入力します。
ステップ 5	**end** 例： `Router(config-if)# end`	（任意）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、特権 EXEC モードに戻ります。

トラフィック クラスとトラフィック ポリシー情報の確認

ここで取り上げる show コマンドはいずれも任意で使用します。また、入力順も任意です。

手順の概要

1. **enable**
2. **showclass-map**
3. **showpolicy-map***policy-map-name***class***class-name*
4. **showpolicy-map**
5. **showpolicy-mapinterface***typenumber*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**showclass-map** 例： `Router# show class-map`	（任意）すべてのクラス マップとその一致条件を表示します。

	コマンドまたはアクション	目的

ステップ 3	**showpolicy-map***policy-map-name***class***class-name*
	
	例：
	
	`Router#`
	
	`show policy-map policy1 class class1`
		（任意）指定したポリシー マップの指定したクラスの設定を表示します。
		
		• ポリシー マップ名とクラス名を入力します。

ステップ 4	**showpolicy-map** 例： `Router# show policy-map`	（任意）存在するすべてのポリシー マップのすべてのクラスの設定を表示します。
ステップ 5	**showpolicy-mapinterface***typenumber* 例： `Router# show policy-map interface serial 0/0/1`	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。 • インターフェイス タイプと番号を入力します。
ステップ 6	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

MQC を使用した QoS 機能の適用の設定例

トラフィック クラスの作成

次の例では、トラフィック クラスを作成し、一致基準を定義します。最初のトラフィック クラス（class1）では、アクセス コントロール リスト（ACL）101 を使用し、2 つめのトラフィック クラス（class2）では ACL 102 を使用します。パケットとこれらの ACL のコンテンツを照合し、そのクラスに属しているかどうかを判断します。

```
class-map class1
  match access-group 101
  exit
class-map class2
  match access-group 102
  end
```

ポリシー マップの作成

次の例では、class1 と class2 の 2 つのクラスに適用する QoS 機能を含むトラフィック ポリシー（policy1）を定義します。これらのクラスの一致基準は、トラフィック クラスの作成, （19 ページ）ですでに定義されています。

class1 では、帯域幅割り当て要求と、そのクラス用に予約されるキューの最大パケット数の制限がポリシーに含まれています。class2 では、帯域幅割り当て要求だけがポリシーで指定されています。

```
policy-map policy1
  class class1
    bandwidth 3000
    queue-limit 30
    exit
  class class2
    bandwidth 2000
    end
```

例：トラフィック ポリシーのインターフェイスへの適用

次に、既存のトラフィック ポリシーをインターフェイスに適用する例を示します。**policy-map** コマンドを使用してトラフィック ポリシーを定義した後、**service-policy** コマンドをインターフェイス コンフィギュレーション モードで使用して、1 つ以上のインターフェイスに適用できます。同じトラフィック ポリシーを複数のインターフェイスに割り当てることができますが、各インターフェイスには、入力方向と出力方向に対して、それぞれトラフィック ポリシーを 1 つだけ割り当てることができます。

```
Router(config)# interface fastethernet 1/1/1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
Router(config)# interface fastethernet 1/0/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

match not コマンドの使用

matchnot コマンドを使用して、一致基準として使用していない QoS ポリシー値を指定します。その QoS ポリシーの他のすべての値が成功する一致基準となります。たとえば、QoS クラスマップ コンフィギュレーション モードで **matchnotqos-group4** コマンドを発行すると、指定したクラスは、成功する一致基準として 4 を除くすべての QoS グループ値を受け入れます。

次のトラフィック クラスでは、IP 以外のすべてのプロトコルが成功する一致条件と見なされます。

```
class-map noip
  match not protocol ip
  end
```

デフォルト トラフィック クラスの設定

トラフィック クラスで指定された一致条件を満たさないトラフィック（つまり、未分類のトラフィック）は、デフォルト トラフィック クラスに属するものとして扱われます。

デフォルト クラスを設定しない場合でも、パケットはそのクラスのメンバーとして扱われます。デフォルト クラスにはイネーブルになっている QoS 機能がないため、このクラスに属するパケットには QoS 機能がありません。そのようなパケットをテール ドロップが管理する先入先出（FIFO）キューに配置します。テール ドロップは、すべてのトラフィックを等しく扱ってサービス クラス間での区別はせずに輻輳を回避する手段です。輻輳期間中はキューが一杯になります。出力キューが一杯でテール ドロップがアクティブな場合、輻輳が解消されてキューが一杯でなくなるまでパケットはドロップされます。

次の例では、次の特性を持つデフォルト クラス（常に class-default という名前になります）のポリシー マップ（policy1）を設定します。ポリシーがクラス ポリシー policy1 で定義されている他のクラスの一致基準を満たさないトラフィック用に 10 個のキューがあり、キューあたり 20 個のパケットを超えると、追加でキューに格納されるパケットを処理するためにテール ドロップが実施されます。

```
policy-map policy1
  class class-default
    fair-queue
    queue-limit 20
```

次の例では、次の特性を持つデフォルト クラス（常に class-default という名前になる）のポリシー マップ（policy1）を設定します。ポリシーがトラフィック ポリシー policy1 で定義されている他のクラスの一致基準を満たさないトラフィック用に 10 個のキューがあります。

```
policy-map policy1
  class class-default
    shape average 100m
```

「class-map match-any」コマンドと「class-map match-all」コマンドの違い

次に、複数の一致条件がある場合にパケットを評価する例を示します。この例で、**class-mapmatch-any** コマンドと **class-mapmatch-all** コマンドの違いを示します。トラフィック クラスのメンバーと見なされるためには、パケットが一致基準のすべて（**match-all**）を満たすか、または一致基準のいずれか 1 つ（**match-any**）を満たす必要があります。

次に、**class-map match-all** コマンドを使用してトラフィック クラスを設定する例を示します。

```
class-map match-all cisco1
  match protocol ip
  match qos-group 4
  match access-group 101
```

インターフェイス上に設定されているトラフィック クラス cisco1 を持つルータにパケットが到着した場合、そのパケットが IP プロトコル、QoS グループ 4、およびアクセス グループ 101 に一致

するかどうかが評価されます。これらの一致基準がすべて満たされると、パケットはトラフィック クラス cisco1 のメンバーとして分類されます（論理 AND 演算子：IP プロトコル AND QoS グループ 4 AND アクセス グループ 101）。

```
class-map match-all vlan
  match vlan 1
  match vlan inner 1
```

次に、**class-map match-any** コマンドを使用する例を示します。パケットがトラフィック クラスのメンバーとして分類されるには、一致基準の 1 つのみを満たす必要があります（つまり、論理OR 演算子：プロトコル IP OR QoS グループ 4 OR アクセス グループ 101）。

```
class-map match-any cisco2
  match protocol ip
  match qos-group 4
  match access-group 101
```

トラフィック クラス cisco2 では、成功する一致が見つかるまで連続的に一致基準が評価されます。パケットは、まず IP プロトコルを一致基準として使用できるかどうかを判断するために評価されます。使用できる場合、パケットはトラフィック クラス cisco2 に一致します。使用できない場合、QoS グループ 4 は一致基準として評価され、以降も同様に評価されます。パケットが指定したどの条件にも一致しない場合、パケットはデフォルト トラフィック クラス（*class default-class*）のメンバーとして分類されます。

一致基準としてのトラフィック クラス（ネストしたトラフィック クラス）の確立

matchclass-map コマンドを使用する理由は 2 つあります。1 つの理由はメンテナンスです。現在大規模なトラフィック クラスが存在している場合、トラフィック クラス一致基準を使用するほうが、同じトラフィック クラス設定を再入力するよりも簡単です。2 つめのより一般的な理由としては、1 つのポリシー内で match-all と match-any の特性を組み合わせるためです。これより、1 つの一致基準評価命令（match-any と match-all のどちらか）を使用したトラフィック クラスを作成し、このトラフィック クラスを、異なるタイプの一致基準を使用するトラフィック クラスで一致条件として使用します。

考えられるシナリオは次のとおりです。A、B、C、および D が、すべて異なる一致基準であるとし、A、B、または C かつ D（A または B または（C かつ D））に一致するトラフィックをトラフィック クラスに属するものとして分類するとします。ネストしたトラフィック クラスがない場合、トラフィックがトラフィック クラスの一部であると見なされるためには、4 つの一致基準すべてに一致するか（A かつ B かつ C かつ D）、いずれかの一致基準に一致する必要があります（A または B または C または D）。「かつ」（match-all）文と「または」（match-any）文をトラフィック クラス内で組み合わせることはできないため、目的の設定を実現できません。

解決策：C と D に対して match-all を使用する 1 つのトラフィック クラスを作成し（これを条件 E と呼びます）、A、B、E を使用して新しい match-any トラフィック クラスを作成します。新しいトラフィック クラスの評価順序は正しくなります（A または B または E、つまり A または B または（C かつ D））。

例：メンテナンスのためにネストされたトラフィック クラス

次の例で、トラフィック クラス class1 の特性は、トラフィック クラス class2 の特性と同じですが、トラフィック クラス class1 では、一致基準として宛先アドレスが追加されています。トラフィック クラス class1 をゼロから設定する代わりに、**matchclass-mapclass2** コマンドを入力できます。このコマンドを使用すると、class2 というトラフィック クラスのすべての特性をトラフィック クラス class1 に取り込み、トラフィック クラス全体を再設定することなく、新しい宛先アドレスの一致基準を追加できます。

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 00.00.00.00.00.00
Router(config-cmap)# exit
```

例：match-any 特性と match-all 特性を 1 つのトラフィック クラスで組み合わせるためのネストしたトラフィック クラス

1 つのトラフィック クラスで match-any 特性と match-all 特性を使用するための唯一の方法は、**matchclass-map** コマンドを使用することです。1 つのクラスに match-any と match-all の特性を組み合わせるには、一致基準に match-all 命令を使用して設定されたクラスを使用するトラフィック クラスを作成する match-any 命令を使用します（**matchclass-map** コマンドを使用）。

次に、2 つのトラフィック クラスの特性を組み合わせる例を示します。1 つは match-any 特性を使用し、1 つは match-all 特性を使用しています。これを、**matchclass-map** コマンドで 1 つのトラフィック クラスとして設定します。その結果、パケットがトラフィック クラス class4 のメンバーと見なされるためには、次の 3 つの一致基準のいずれかを満たしている必要があります。IP プロトコルかつ QoS グループ 4、宛先 MAC アドレス 00.00.00.00.00.00、またはアクセス グループ 2。

この例で、トラフィック クラス class4 だけがトラフィック ポリシー policy1 と共に使用されています。

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 00.00.00.00.00.00
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# end
```

例：QoS ポリシーとしてのトラフィック ポリシー（階層型トラフィック ポリシー）

QoS ポリシー マップ クラス コンフィギュレーション モードで **service-policy** コマンドを使用すると、トラフィック ポリシーを QoS ポリシー内に含めることができます。トラフィック ポリシーを含むトラフィック ポリシーは、階層型トラフィック ポリシーと呼びます。

階層型トラフィック ポリシーには、1 つの子ポリシーと 1 つの親ポリシーが含まれています。子ポリシーは、以前に定義したトラフィック ポリシーであり、**service-policy** コマンドを使用して新しいトラフィック ポリシーに関連付けられます。既存のトラフィック ポリシーを使用する新しいトラフィック ポリシーが親ポリシーです。ここに示す例では、トラフィック ポリシー child が子ポリシーであり、トラフィック ポリシー parent が親ポリシーです。

階層型トラフィック ポリシーは、サブインターフェイスと ATM PVC に適用できます。階層型トラフィック ポリシーを使用すると、1 つのトラフィック ポリシー（1 つの子ポリシーと 1 つの親ポリシーを持つ）を使用して、相手先固定接続（PVC）トラフィックのシェーピングと優先順位付けを行うことができます。次の例で、子ポリシーはトラフィックの優先順位付けを行い、親ポリシーはトラフィックのシェーピングを行います。この設定で、親ポリシーは、パケットがインターフェイスから送信されるのを許可し、子ポリシーは、パケットが送信される順序を決定します。

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

shape コマンドで使用する値は、サービスプロバイダーから通知された認定情報レート（CIR）値からプロビジョニングします。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
パケット分類	「Classifying Network Traffic」モジュール
フレーム リレー フラグメンテーション（FRF）PVC	「FRF .20 Support」モジュール

関連項目	マニュアル タイトル
選択的パケット廃棄	「IPv6 Selective Packet Discard」モジュール
スケーリングとパフォーマンスの情報	『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』の「Broadband Scalability and Performance」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MQC を使用した QoS 機能の適用の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：*MQC* を使用した *QoS* 機能の適用の機能情報

機能名	リリース	機能情報
クラスベース重み付け均等化キューイング（CBWFQ）	Cisco IOS XE リリース 2.1 Cisco IOS XE リリース 3.5S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。
モジュラ QoS CLI（MQC）	Cisco IOS XE リリース 2.1 Cisco IOS XE リリース 3.5S	このモジュールでは、モジュラ QoS CLI（MQC）を使用して QoS を適用し、設定する方法について説明します。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシー マップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する QoS 機能が含まれます。 この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能は、Cisco IOS XE リリース 2.3 に付属する他の機能に対してインフラストラクチャサポートを提供するように拡張されています。 Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。

機能名	リリース	機能情報
MQC 階層型クラス マップ	Cisco IOS XE リリース 3.2	MQC では、複数のトラフィック クラス（ネストしたトラフィック クラス、ネストしたクラスマップ、またはMQC階層型クラス マップとも呼ぶ）を、1つのトラフィック クラスとして設定できます。この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。
プライオリティ キューイング	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。
重み付けランダム早期検出	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。

第 3 章

3レベルのユーザ定義キューイングポリシーのサポート

3 レベルのユーザ定義キューイング ポリシーのサポート機能を使用して、最上位レイヤのユーザ定義クラスが含まれる 3 レベル ポリシーで、階層内のトラフィック クラスの柔軟性をサポートし、強化することができます。

- 機能情報の確認，29 ページ
- 3 レベルのユーザ定義キューイング ポリシーのサポートに関する制約事項，30 ページ
- 3 レベルのユーザ定義キューイング ポリシーのサポートに関する情報，30 ページ
- 3 レベルのユーザ定義のキューイング ポリシー サポートの設定方法，32 ページ
- 3 レベルのユーザ定義のキューイング ポリシー サポートに関するその他の参考資料，33 ページ
- 3 レベルのユーザ定義キューイング ポリシーのサポートの機能情報，34 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

3 レベルのユーザ定義キューイング ポリシーのサポートに関する制約事項

- 3 レベルの階層型キューイング ポリシーの最上位レイヤのユーザ定義クラスは、ポートチャネルのメイン インターフェイスではサポートされません。

  最上位レイヤのユーザ定義クラスは、論理ターゲットではサポートされません。論理ターゲットには、サービス グループ、トンネル、セッション、ディーラー インターフェイスなどがあります。

3 レベルのユーザ定義キューイング ポリシーのサポートに関する情報

階層型 QoS の 3 つのパラメータによるスケジューラ

従来の IOS は、最大値（shape）と最小（bandwidth）を使用して、トラフィックの輻輳が発生した場合の各スケジューラ ノードの動作を定義します。つまり、2 つのパラメータによるスケジューラです。

ASR 1000 は、3 つのパラメータ、最大値（shape）、最小値（bandwidth）、および超過帯域幅の共有を調整する超過値（bandwidth remaining）による別のスケジューラです。2 つのパラメータによるスケジューラでは、超過帯域幅は比例的に（各クラスの帯域幅率と同じに）クラス間で共有されます。しかし、3つのパラメータによるスケジューラでは、最小帯域幅の要件が満たされると、デフォルトによって超過帯域幅は等分に共有されますが、これは、「bandwidth remaining」コマンドを使用すると調整できます。ISR 4000 プラットフォームは、同じ設計を共有しています。

従来の IOS では、階層のリーフと中間ノードで帯域幅を設定することができます。IOS XE では、階層のリーフ ノードでのみ、bandwidth（bandwidth rate または bandwidth percent）が許可されます。つまり、bandwidth（bandwidth rate または bandwidth percent）クラスは、キューイング機能を含んでいる子ポリシー マップに対応付けることはできません。これはソフトウェアでの制約であるため、将来、解除される可能性があります。

従来の IOS QoS ポリシー マップを IOS XE プラットフォームに移行する現在の導入の場合、中間ノードの bandwidth コマンドを bandwidth remaining コマンドに変換することが最良の選択肢です。bandwidth remaining percent コマンドまたは bandwidth remaining ratio コマンドを使用すると、非常によく似た動作を実現できます。

階層型ポリシーのガイドライン

一般に、階層の 3 つのレベルが ASR 1000 でサポートされています。階層型ポリシーは QoS をサポートするほとんどの物理ターゲットと論理ターゲットに適用できます。

キューイング ポリシーと非キューイング ポリシーが階層に混在している場合、非キューイング ポリシーマップは、そのポリシーマップのリーフ レベル（親の親および親キューイング ポリシー下の子ポリシーなど）にする必要があります。

ポリシー マップを仮想インターフェイス（トンネルまたはセッションなど）に適用すると、構成によっては階層を 2 つのキューイングの レベルに制限する追加制約がある場合があります。

- キューイング機能：shape、bandwidth、bandwidth remaining、random-detect、fair-queue、queue limit、および priority。
- 非キューイング機能：police、mark、および account。

階層機能の組み合わせ	入力ポリシー サポート	出力ポリシー サポート
1 レベルの非キューイング ポリシー	はい	はい
2 レベルの非キューイング ポリシー（カラー対応ポリシングを含む）	はい	はい
3 レベルの非キューイング ポリシー（階層型カラー対応ポリシングを含む）	はい	はい
1 レベルのキューイング ポリシー	-	はい
2 レベルのキューイング ポリシー	-	はい
3 レベルのキューイング ポリシー	-	はい
2 レベルの混合ポリシー、親レベルでのキューイング機能	-	はい
3 レベルの混在ポリシー、親の親レベルまたは親の親+親レベルでのキューイング機能	-	はい

HQoS の最上位レベル ポリシーのユーザ定義トラフィック クラス

「クラスマップ」によって明示的に設定されたどのトラフィッククラスも「ユーザ定義クラス」と呼ばれます。class-default クラスは設定する必要はなく、これらのクラスをポリシー内に使用して、ユーザ定義クラスに属していないすべてのトラフィックに一致させることができます。

Polaris 16.3 リリースまでは、3 レベルのキューイング ポリシーで最上位レベルに設定できるのは class-default クラスのみです。Polaris 16.3 以降は、3 レベルの階層型ポリシーの最上位レベルでユーザ定義クラスがサポートされています。

3 レベルのユーザ定義のキューイング ポリシー サポートの設定方法

3 レベルの階層型 QoS ポリシーの設定

```
enable
configure terminal
class-map vlan10
 match vlan10
class-map vlan20
 match vlan 20
class-map ef
 match dscp ef
policy-map child
 class ef
  priority
  police 1000000
 class class-default
 police 3000000
policy-map parent
 class vlan10
  shape average 4000000
  service-policy child
 class vlan20
  shape average 8000000
  service-policy child
policy-map grand-parent
 class class-default
  shape average 10000000
  service-policy parent
end
```

最上位レベルのポリシーでのユーザ定義のトラフィッククラスの設定

```
ip access-list extended PEER
permit ip host 200.0.0.2 any

class-map match-all ef
 match dscp ef
class-map match-all vlan100
 match vlan 100
class-map match-all vlan101
 match vlan 101
```

```
class-map match-all PEER
 match access-group name PEER

policy-map child
 class ef
  bandwidth remaining percent 15
 class class-default
  fair-queue
  queue-limit 512 packets
  bandwidth remaining percent 85

policy-map parent
 class PEER
  shape average 8000000
  bandwidth remaining percent 10
  service-policy child
class class-default
 shape average 8000000

policy-map grandparent
 class vlan100
  shape average 8000000
  bandwidth remaining ratio 1000
  service-policy parent
 class vlan101
  shape average 8000000
  bandwidth remaining ratio 1000
  service-policy parent
 class class-default
  bandwidth remaining ratio 1
  shape average 10000000
end
```

3 レベルのユーザ定義のキューイング ポリシー サポートに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

3 レベルのユーザ定義キューイング ポリシーのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8* : *3* レベルのユーザ定義キューイング ポリシーのサポートの機能情報

機能名	リリース	機能情報
3 レベルのユーザ定義キューイング ポリシーのサポート	Cisco IOS XE Denali 16.3.1.	この機能は、Cisco ASR 1000、ISR4000、CSR1000v のプラットフォームに導入されました。ユーザ定義クラスは、3 レベル階層型ポリシーの最上位レイヤで設定できます。

第 4 章

IP/ATM 間サービス クラスの設定

ここでは、IP/ATM 間サービス クラス（CoS）の設定作業について説明します。IP-ATM CoS とは、IP と ATM の間に QoS 特性をマップする機能セットです。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

- 機能情報の確認，35 ページ
- 単一の ATM VC での IP/ATM 間 CoS の設定タスク リスト，36 ページ
- ATM バンドルでの IP/ATM 間 CoS の設定タスク リスト，37 ページ
- VC 単位の WFQ および CBWFQ の設定タスク リスト，42 ページ
- IP/TM 間 CoS の設定例，46 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

単一の ATM VC での IP/ATM 間 CoS の設定タスク リスト

単一の ATM 仮想回線（VC）に IP/ATM 間 CoS を設定するには、次の項で説明する作業を実行します。最初の 2 つの項の作業は必須です。残りの項の作業は任意です。

IP/ATM 間 CoS 機能には、ATM 相手先固定接続（PVC）の管理が必要です。

WRED パラメータ グループの定義

コマンド	目的
`Router(config)#` **random-detect-group** *group-name*	WRED または VIP 分散 WRED（DWRED）グループ パラメータを定義します。

WRED パラメータ グループの設定

手順の概要

1. Device(config)#**random-detect-group***group-name*
2. Device(config)# **exponential-weighting-constant***exponent*
3. Device(config)# **precedence***precedencemin-thresholdmax-thresholdmark-probability-denominator*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)#**random-detect-group***group-name*	WRED または DWRED のパラメータ グループを指定します。
ステップ 2	Device(config)# **exponential-weighting-constant***exponent*	WRED または DWRED の指定したパラメータ グループの平均キューサイズ計算のための指数加重係数を設定します。 または
ステップ 3	Device(config)# **precedence***precedencemin-thresholdmax-thresholdmark-probability-denominator*	特定の IP precedence の指定された WRED または DWRED パラメータ グループを設定します。

WRED パラメータの表示

コマンド	目的
Router# **show queueing random-detect** [**interface** *atm_subinterface* [**vc** [[*vpi*/] *vci*]]]	指定された ATM サブインターフェイスで、WRED または DWRED がイネーブルであるすべての VC のパラメータを表示します。

キューイング統計情報の表示

コマンド	目的
Router# **show queueing interface** *interface-number* [**vc** [[*vpi*/] *vci*]]	インターフェイスの特定の VC のキューイングの統計情報を表示します。

ATM バンドルでの IP/ATM 間 CoS の設定タスク リスト

ATM バンドルで IP/ATM 間 CoS を設定するには、次の項に示されているタスクを実行します。

IP/ATM 間 CoS 機能には、ATM PVC の管理が必要です。

VC バンドルの作成

コマンド	目的
Router(config-subif)# **bundle** *bundle-name*	指定されたバンドルを作成し、バンドル コンフィギュレーション モードを開始します。

バンドルレベルのパラメータの適用

バンドル レベルのパラメータの設定

コマンド	目的
`Device(config-atm-bundle)#` **protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**]	スタティック マップを設定するか、バンドルの Inverse Address Resolution Protocol（Inverse ARP）または Inverse ARP ブロードキャストをイネーブルにします。 （注） バンドルレベルのパラメータは、VC クラスを割り当てるか、またはバンドルにそれらのクラスを直接適用することによって、適用できます。バンドルに割り当てられた VC クラスを使用して適用されたパラメータは、バンドルレベルで適用されたパラメータに置き換えられます。バンドルレベルのパラメータは、個々の VC に適用されるパラメータで置換されます。
`Device(config-atm-bundle)#` **encapsulation** *aal-encap*	ATM アダプテーション層（AAL）およびそのバンドルのカプセル化のタイプを設定します。
`Device(config-atm-bundle)#` **inarp** *minutes*	すべての VC バンドル メンバの Inverse ARP 期間を設定します。
`Device(config-atm-bundle)#` **broadcast**	すべての VC バンドル メンバのブロードキャスト転送をイネーブルにします。
`Device(config-atm-bundle)#` **oam retry** `up-count down-count retry frequency`	運用管理および保守（OAM）の管理に関連する VC バンドル パラメータを設定します。
`Device(config-atm-bundle)#` **oam-bundle** [**manage**] [*frequency*]	エンドツーエンドの F5 OAM ループバック セルの生成と、バンドルのすべての VC の OAM 管理をイネーブルにします。

バンドルに適用する VC クラスのパラメータの設定

コマンド	目的
`Router(config-vc-class)#` **oam-bundle** [**manage**] [*frequency*]	エンドツーエンドの F5 OAM ループバック セルの生成と、バンドルのすべての VC の OAM 管理をイネーブルにします。 （注） VC クラスを使用すると、クラス自体をバンドルに適用できるため、一度に複数の属性を適用するようにバンドルを設定できます。クラスを使用すると、すべての VC でパラメータを一般化することができます。一部のパラメータについては、その後で個々の VC のパラメータを変更できます（詳細については、「個々の VC へのパラメータの適用」の項を参照してください）。

バンドルへのクラスの適用

コマンド	目的
`(config-atm-bundle)#` **class-bundle** *vc-class-name*	指定された VC クラスに含まれるバンドル レベルのコマンドでバンドルを設定します。 （注） VC クラスに含まれるバンドル レベル コマンドを使用して設定されたパラメータは、バンドルとそのすべての VC メンバに適用されます。バンドル上に直接設定されたコマンドを通じて適用されたバンドルレベルのパラメータは、VC クラスを通じて適用されたパラメータよりも優先されます。VC クラスを通じて適用されたバンドルレベルのパラメータやバンドルに直接適用されたバンドルレベルのパラメータの一部は、バンドル VC コンフィギュレーション モードで個々の VC に直接適用されたコマンドによって置き換えることができます。

バンドルへの VC のコミット

コマンド	目的
`Device(config-atm-bundle)#` **pvc-bundle** *pvc-name* [*vpi*/] [*vci*]	指定された VC をバンドルに追加し、指定された VC バンドル メンバを設定するためにバンドル VC コンフィギュレーション モードを開始します。

個々の VC へのパラメータの適用

VC バンドル メンバーの直接設定

コマンド	目的
`Device(config-if-atm-member)#` **ubr** *output-pcr* [*input-pcr*]	未指定ビット レート（UBR）の QoS の VC を設定し、出力のピーク セル レート（PCR）を指定します。
`Device(config-if-atm-member)#` **ubr+** *output-pcr output-mcr* [*input-pcr*] [*input-mcr*]	UBR の QoS の VC を設定し、出力の PCR と出力の最低保証セル レートを指定します。
`Device(config-if-atm-member)#` **vbr-nrt** *output-pcr output-scr output-mbs* [*input-pcr*] [*input-scr*] [*input-mbs*]	可変ビット レート非リアルタイム（VBR-NRT）の VC を設定し、出力の PCR、出力の平均セル レート、および出力の最大バースト セル サイズを指定します。
`Device(config-if-atm-member)#` **precedence** [**other** | *range*]	VC の Precedence レベルを設定します。
`Device(config-if-atm-member)#` **bump** {**implicit** | **explicit** *precedence-level* | **traffic**}	VC のバンピング ルールを設定します。
`Device(config-if-atm-member)#` **protect** {**group** | **vc**}	VC がバンドルの保護されたグループに所属するか、個別に保護された VC バンドル メンバになるように設定します。

VC バンドル メンバーに適用する VC クラスのパラメータの設定

コマンド	目的
`Device(config-vc-class)#` **bump** {**implicit** | **explicit** *precedence-level* | **traffic**}	クラスを適用する VC メンバのバンピング ルールを指定します。これらのルールは、キャリアの VC バンドル メンバがダウンした場合に、バンドル トラフィックの VC を送信するルールを決定します。 （注） また、**ubr** コマンド、**ubr+** コマンド、および **vbr-nrt** コマンドを VC クラスに追加すると、VC バンドル メンバーの設定に使用できます。VC が VC バンドルのメンバーである場合、VC クラス モードでの VC の設定に **encapsulation** コマンド、**protocol** コマンド、**inarp** コマンド、および **broadcast** コマンドを使用することはできません。これらのコマンドは、バンドル メンバ レベルではなくバンドル レベルでのみ使用できます。個々の VC に対する設定は、VC クラスをバンドルに適用することによってすべての VC バンドル メンバに適用された共有の設定を上書きします。
`Device(config-vc-class)#` **precedence** *precedence min-threshold max-threshold mark-probability-denominator*	クラスを適用する VC メンバの Precedence レベルを定義します。
`Device(config-vc-class)#` **protect** {**group** | **vc**}	VC をバンドルの保護されたグループのメンバとして設定するか、個別に保護された VC として設定します。

個々の VC バンドル メンバーへの VC クラスの適用

コマンド	目的
`Device(config-if-atm-member)#` **class-vc** *vc-class-name*	VC クラスを VC バンドル メンバーに割り当てます。

バンピングされたトラフィックを拒否する場合の VC の設定

コマンド	目的
`Device(config-if-atm-member)#` **no bump traffic**	リダイレクトされる可能性のあるバンピングされたトラフィックを受け入れないように VC を設定します。

VC バンドルとそれらの VC メンバーのモニタリングと保守

コマンド	目的
`Device#` **show atm bundle** *bundle-name*	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
`Device#` **show atm bundle** *bundle-name* **statistics** [**detail**]	指定されたバンドルの統計情報または詳細な統計情報を表示します。
`Device#` **show atm map**	ATM ネットワークおよび ATM バンドル マップのリモートホストに対するすべての設定済みの ATM スタティック マップのリストを表示します。
`Device#` **debug atm bundle errors**	バンドルのエラーに関する情報を表示します。
`Device#` **debug atm bundle events**	バンドルのイベントの記録を表示します。

VC 単位の WFQ および CBWFQ の設定タスク リスト

VC 単位の WFQ および CBWFQ に IP/ATM 間 CoS を設定するには、次の項で説明するタスクを実行します。

IP/ATM 間 CoS 機能には、ATM PVC の管理が必要です。

クラスベースの重み付け均等化キューイングの設定

VC の CBWFQ を設定する前に、標準の CBWFQ コマンドを使用して次の作業を実行する必要があります。

- VC 間で送信されるトラフィックの分類に使用される 1 つまたは複数のクラスを作成する
- サービス ポリシーとして使用するクラスを含むポリシー マップを定義する

（注） クラス ポリシーはルータで定義可能な数だけ設定できます（最大 64 個）。ただし、VC に適用されるポリシー マップに含まれ、すべてのクラスに割り当てられている帯域幅の合計は、VC の使用可能な帯域幅の 75 % を超えてはいけません。使用可能な帯域幅の残りの 25 % は、ATM セルのオーバーヘッド（ATM セル タックスとも呼ばれる）、ルーティングとベストエフォート型のトラフィック、およびオーバーヘッドが想定されるその他の機能などのカプセル化に使用されます。帯域幅割り当ての詳細については、「輻輳管理の概要」モジュールを参照してください。

CBWFQ では最小帯域幅のみを保証するため、使用可能ビット レート（ABR）および可変ビット レート（VBR）のサービス クラスを持つ VC のみに CBWQF を適用できます。UBR および未指定ビット レート プラス（UBR+）には VC 単位の WFQ および CBWFQ を適用できません。これは、両方のサービス クラスはどちらもベストエフォート型のクラスであり、最小帯域幅が保証されないためです。VC の CBWFQ がイネーブルの場合、サービス ポリシーの一部として設定されているすべてのクラスは、均等化キューイング システムに組み込まれます。

VC レベルで CBWFQ を設定するほかに、IP to ATM CoS 機能を使用すると、VC レベルでフローベースの WFQ を設定できます。フローベースの WFQ はベストエフォート型のサービス クラスを提供する（つまり、最小帯域幅が保証されない）ため、すべてのタイプの CoS VC（ABR、VBR、UBR、および UBR+）に VC 単位の WFQ を設定できます。

VC 単位の WQF では class-default クラスを使用します。そのため、VC 単位の WFQ を設定するには、最初にポリシー マップを作成してから class-default クラスを設定する必要があります（事前に設定されているため、class-default クラスを作成する必要はありませんが、設定する必要はあります）。VC 単位の WFQ の場合、class-default クラスは **fair-queue** ポリシーマップ クラス コンフィギュレーション コマンドを使用して設定する必要があります。

fair-queue ポリシー マップ クラス コンフィギュレーション コマンドの設定に加えて、**queue-limit** コマンドまたは **random-detect** コマンドの両方ではなく、どちらか一方を使用して、デフォルト クラスを設定できます。さらに、デフォルト クラスでフローベースの WFQ を使用する場合は、**bandwidth** ポリシー マップ クラス コンフィギュレーション コマンドを使用してデフォルト クラスを設定することはできません。このコマンドを使用すると、デフォルト クラスがフローベースの WFQ として見なされないため、そのクラスを含むサービス ポリシーの適用が ABR および VBR の VC に制限されます。

サービス ポリシーの適用と VC に対する CBWFQ のイネーブル化

スタンドアロン VC へのポリシー マップの適用と CBWFQ のイネーブル化

コマンド	目的
`Router(config-if-atm-vc)#` **service-policy output** *policy-map*	CBWFQ をイネーブルにし、指定されたサービス ポリシー マップを作成または変更する VC にアタッチします。

個々の VC へのポリシー マップの適用と CBWFQ のイネーブル化

コマンド	目的
`Router(config-if-atm-member)#` **service-policy output** *policy-map*	CBWFQ をイネーブルにし、指定されたサービス ポリシー マップを作成または変更する VC にアタッチします。

（注） **service-policy output** コマンドと **random-detect-group** コマンドは同時に使用できません。サービス ポリシーを適用することによって CBWFQ をイネーブルにした VC に WRED グループを適用することはできません。さらに、1 つのコマンドが設定されている場合に、他のコマンドを設定できるようにするには、他のコマンドをディセーブルにする必要があります。

フローベースの WFQ を使用する場合の VC の設定

手順の概要

1. Device(config)# **policy-map***policy-map*
2. Device(config-pmap)# **classclass-default***default-class-name*
3. Device(config-pmap-c)# **fair-queue***number-of-dynamic-queues*
4. 次のいずれかを実行します。
   - Device(config-pmap-c)# **queue-limit***number-of-packets*
   - Device(config-pmap-c)# **random-detect**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **policy-map***policy-map*	作成または変更するポリシー マップの名前を指定します。
ステップ 2	Device(config-pmap)# **classclass-default***default-class-name*	ポリシーを設定または変更できるようデフォルトクラスを指定します。 （注） フローベースのWFQクラスを含むポリシーマップと同じポリシー マップに他のクラスを含めることができます。他の方法では一致しなかったパケットが、デフォルトの class-default クラスの一致基準によって選択されます。
ステップ 3	Device(config-pmap-c)# **fair-queue***number-of-dynamic-queues*	デフォルト クラスで実行するフローベースの WFQ が使用するために予約する、ダイナミック キューの数を指定します。 （注） デフォルトでは（つまり、**fair-queue** ポリシー マップ クラス コンフィギュレーション コマンドを使用して class-default クラスを設定しておらず、**bandwidth** ポリシー マップ クラス コンフィギュレーション コマンドを使用して class-default クラスを設定していない場合でも）、デフォルトクラスはフローベースのWFQとして定義されます。
ステップ 4	次のいずれかを実行します。 • Device(config-pmap-c)# **queue-limit***number-of-packets* • Device(config-pmap-c)# **random-detect**	そのクラスのキューに投入できるパケットの最大数を指定します。 WRED をイネーブルにします。クラス ポリシーは、テール ドロップではなく WRED を使用してパケットをドロップします。

スタンドアロン VC へのポリシー マップの適用と WFQ のイネーブル化

コマンド	目的
`Device(config-if-atm-vc)#` **service-policy output** *policy-map*	作成または変更される VC に class-default クラスを含む指定されたポリシーマップをアタッチすることで、VC の WFQ をイネーブルにします。

個々の VC へのポリシー マップの適用と WFQ のイネーブル化

コマンド	目的
`Device(config-if-atm-member)#` **service-policy output** *policy-map*	class-default クラスを含む指定されたポリシー マップを VC バンドル メンバにアタッチすることで、VC バンドル メンバの WFQ をイネーブルにします。

VC 単位の WFQ および CBWFQ のモニタリング

コマンド	目的
`Device#` **show policy-map** *interface interface-number* [**vc** [*vpi*/] *vci*]]	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。

コンソールへのエラー メッセージのロギングのイネーブル化

コマンド	目的
`Router(config)#` **logging console** *level*	コンソールに記録されるメッセージを重大度に基づいて制限します。

IP/TM 間 CoS の設定例

例：WRED グループおよび IP プレシデンスを使用した単一の ATM VC

次に、ATM インターフェイスに PVC を作成し、その PVC に sanjose という WRED パラメータ グループを適用します。次に、WRED パラメータ グループ sanjose の IP Precedence の値を設定します。

```
interface ATM1/1/0.46 multipoint
 ip address 200.126.186.2 255.255.255.0
 no ip mroute-cache
 shutdown
pvc 46
 encapsulation aal5nlpid
 random-detect attach sanjose
!
random-detect-group sanjose
```

```
 precedence 0  200   1000 10
 precedence 1  300   1000 10
 precedence 2  400   1000 10
 precedence 3  500   1000 10
 precedence 4  600   1000 10
 precedence 5  700   1000 10
 precedence 6  800   1000 10
 precedence 7  900   1000 10
```

例：VC クラスを使用した VC バンドルの設定

この例では、Intermediate System-to-Intermediate System（IS-IS）を IP ルーティング プロトコルとして使用するルータに VC バンドル管理を設定します。

Bundle-Class クラス

最初に、この設定では、VC パラメータのコンフィギュレーション コマンドを含む bundle-class という名前の VC クラスを定義します。bundle-class クラスがバンドル レベルで適用されると、そのバンドルに属しているすべての VC にこれらのパラメータが適用されます。バンドル VC モードのバンドルの個々の VC に直接適用されたコマンドは、バンドル レベルでグローバルに適用されたコマンドよりも優先されます。階層の優先ルールを考慮すると、クラス bundle-class が適用されるバンドルに属する VC は、aal5snap カプセル化、ブロードキャスト オン、Inverse ARP を使用した IP アドレスの解決、OAM のイネーブル化などのパラメータを特性として持ちます。

```
router isis
 net 49.0000.0000.0000.1111.00
vc-class atm bundle-class
 encapsulation aal5snap
 broadcast
 protocol ip inarp
 oam-bundle manage 3
 oam retry 4 3 10
```

次の設定のセクションで、その VC にクラスを割り当てることによって、バンドル内の個々の VC に適用可能なパラメータを指定するコマンドを含んだ VC クラスを定義します。

Control-Class クラス

control-class という名前のクラスを VC に適用すると、VC は IP プレシデンス レベルが 7 のトラフィックを伝送します。このクラスを割り当てた VC がダウンした場合はバンドルも一緒にダウンします。これは、このクラスが VC を保護された VC にするためです。このクラスを使用する VC の QoS タイプは vbr-nrt です。

```
vc-class atm control-class
 precedence 7
 protect vc
 vbr-nrt 10000 5000 32
```

Premium-Class クラス

premium-class という名前のクラスを VC に適用すると、その VC は IP プレシデンス レベルが 6 と 5 のトラフィックを伝送します。この VC では他のトラフィックのバンピングを許可しません。こ

のクラスが適用された VC がダウンした場合、バンピングされたトラフィックは IP プレシデンスレベルが 7 の VC にリダイレクトされます。このクラスは、VC をバンドルの保護されたグループのメンバにします。保護されたグループのすべてのメンバがダウンした場合は、バンドルもダウンします。このクラスを使用する VC の QoS タイプは vbr-nrt です。

```
vc-class atm premium-class
 precedence 6-5
 no bump traffic
 protect group
 bump explicitly 7
 vbr-nrt 20000 10000 32
```

Priority-Class クラス

priority-class という名前のクラスを VC に適用すると、VC は IP Precedence の範囲が 4 ～2 のトラフィックを伝送するように設定されます。この VC は明示的なバンピング ルールを使用し、トラフィックをバンプできるようにします。この VC はバンドルの保護されたグループに属しています。このクラスを使用する VC の QoS タイプは ubr+ です。

```
vc-class atm priority-class
 precedence 4-2
 protect group
 ubr+ 10000 3000
```

Basic-Class クラス

basic-class という名前のクラスを VC に適用すると、その VC は **precedence other** コマンドを使用して設定され、プロファイルに指定されていない IP プレシデンス レベルを持つトラフィックを伝送します。このクラスを使用する VC は、バンドルの保護されたグループに所属します。このクラスを使用する VC の QoS タイプは ubr です。

```
vc-class atm basic-class
 precedence other
 protect group
 ubr 10000
```

次のコマンド セットは、ルータのサブインターフェイスが 3 つのネイバーへの接続に使用する 3 つのバンドルを設定します。これらのバンドルは new-york、san-francisco、および los-angeles と呼ばれます。バンドル new-york には 4 つの VC メンバ、バンドル san-francisco には 4 つの VC メンバ、バンドル los-angeles には 3 つの VC メンバがあります。

new-york バンドル

この例の最初の部分では、サブインターフェイスの IP アドレスとルータのプロトコル（ルータは IP ルーティング プロトコルとして IS-IS を使用）を指定します。また、1 つめのバンドル new-york を作成し、バンドル コンフィギュレーション モードを開始します。

```
interface atm 1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip router isis
 bundle new-york
```

バンドル コンフィギュレーション モード内から、コンフィギュレーションの次の部分では 2 つのプロトコル コマンドを使用して IP と開放型システム間相互接続（OSI）のトラフィック フローをバンドル内で有効にします。OSI ルーティング パケットは、バンドルで一番優先度の高い VC を使用します。OSI データ パケットがある場合は、バンドル内の最下位の先行 VC を使用します。設定されている場合、IPX や AppleTalk などの他のプロトコルは常にバンドル内の最下位の先行 VC を使用します

先行するコマンドと後続のコマンドのインデント レベルが示すように、new-york バンドルの下位には、プロトコルを設定するコマンドと、bundle-class というクラスをそれに適用するコマンドがあります。

```
protocol ip 1.1.1.2 broadcast
protocol clns 49.0000.0000.2222.00 broadcast
class-bundle bundle-class
```

bundle-class というクラスは、バンドル new-york に適用され、**protocol ip inarp** コマンドを含んでいます。継承ルールに従って、バンドル レベルで設定される **protocol ip** は、bundle-class クラスに指定された **protocol ip inarp** よりも優先されます。

pvc-bundle ny-control 207 で始まる次の一連の下位コマンドは、（ny-control、ny-premium、ny-priority、および ny-basic という）4 つの VC をバンドル new-york に追加します。特定のクラス（この設定例で事前に定義したクラスの 1 つ）が各 VC に適用され、そのクラスに含まれているコマンドによって指定されたパラメータで設定されます。

この設定の場合と同様、バンドルに属する個々の VC を設定するには、ルータがマザー バンドルに対してバンドル モードである必要があります。バンドルに所属する各 VC では、下位のモードは特定の VC の pvc モードです。

次のコマンドでは、バンドル new-york の個々の VC を設定します。

```
pvc-bundle ny-control 207
 class-vc control-class
pvc-bundle ny-premium 206
 class-vc premium-class
pvc-bundle ny-priority 204
 class-vc priority-class
pvc-bundle ny-basic 201
 class-vc basic-class
```

san-francisco バンドル

次のコマンド セットは、san-francisco という名前のバンドルを作成し、設定します。バンドル コンフィギュレーション レベルでは、bundle-class クラスに含まれるコンフィギュレーション コマンドは、バンドル san-francisco およびバンドルに所属する個々の VC に属します。そのため、**pvc-bundle** コマンドはバンドルに追加するために個々の VC に対して実行されます。VC が追加され、バンドル VC コンフィギュレーション モードが開始されると、特定の事前設定済みのクラスが VC に割り当てられます。そのクラスを構成するコンフィギュレーション コマンドは、VC の設定に使用されます。この時点で階層のルールが適用されます。適用されたクラスに含まれているコマンド パラメータは、バンドル コンフィギュレーション レベルで適用された同じパラメータによって置き換えられ、それらのパラメータは VC に直接適用された同じパラメータによって置き換えられます。

```
bundle san-francisco
```

```
 protocol clns 49.0000.0000.0000.333.00 broadcast
 inarp 1
 class-bundle bundle-class
 pvc-bundle sf-control 307
  class-vc control-class
 pvc-bundle sf-premium 306
  class-vc premium-class
 pvc-bundle sf-priority 304
  class-vc priority-class
 pvc-bundle sf-basic 301
  class-vc basic-class
```

los-angeles バンドル

次のコマンド セットは、los-angeles という名前のバンドルを作成して設定します。バンドル コンフィギュレーション レベルでは、bundle-class クラスに含まれるコンフィギュレーション コマンドは、バンドル los-angeles およびバンドルに所属する個々の VC に属します。そのため、**pvc-bundle** コマンドはバンドルに追加するために個々の VC に対して実行されます。VC が追加され、バンドル VC コンフィギュレーション モードが開始されると、VC に優先度が設定され、その VC は保護されたグループ（protect グループ）のメンバとして設定されるか、個別に保護された VC として設定されます。特定のクラスが各 VC に割り当てられて、さらに特徴付けられます。階層のルールが適用されます。バンドル コンフィギュレーション レベルでバンドル全体に適用したパラメータよりもバンドル VC コンフィギュレーション レベルで VC にクラス内で適用した同じパラメータのほうが優先され、さらに、それらのパラメータよりも VC に直接かつ個別に適用したコマンドのパラメータが優先されます。

```
bundle los-angeles
 protocol ip 1.1.1.4 broadcast
 protocol clns 49.0000.0000.4444.00 broadcast
 inarp 1
 class-bundle bundle-class
 pvc-bundle la-high 407
  precedence 7-5
  protect vc
  class-vc premium-class
 pvc-bundle la-mid 404
  precedence 4-2
  protect group
  class-vc priority-class
 pvc-bundle la-low 401
  precedence other
  protect group
  class-vc basic-class
```

例：スタンドアロン VC での VC 単位の WFQ と CBWFQ

次に、2 つのクラス マップを作成し、それらの一致基準を定義する例を示します。最初のマップ クラス class1 では、番号付きのアクセス コントロール リスト（ACL）101 を一致条件として使用します。2 つめのマップ クラス class2 では、番号付きの ACL 102 を一致基準として使用します。

次に、policy1 というポリシー マップにこれらのクラスを組み込む例を示します。class1 のポリシーでは、このクラスのために予約されたキューに対して、最小帯域幅の割り当て要求に 500 kbps、最大パケット数の制限が 30 と指定されています。class2 のポリシーでは、最小帯域幅の割り当て要求に 1000 kbps のみが指定されているため、デフォルトのキュー制限は 64 パケットであると想

定されます。policy1 を構成する 2 つのクラスの帯域幅要求の合計が、ポリシー マップがアタッチされた cisco という名前の PVC の総帯域幅（2000 kbps）の 75 % になることに注意してください。

この例では、policy1 というポリシー マップを PVC に適用します。ポリシー マップ policy1 が PVC に適用されると、そのクラスによってその PVC の CBWFQ サービス ポリシーが構成されます。この PVC で送信されるパケットの一致基準を ACL 101 および 102 と照合して確認し、それに応じて分類します。

class-default コマンドはこのポリシー マップに対して明示的に設定されていないため、サービス ポリシーを構成している 2 つのクラスの一致基準を満たさないすべてのトラフィックが事前定義された class-default クラスによって処理されます。これによって、ベストエフォートのフローベースの WFQ が実現します。

```
class-map class1
 match access-group 101
class-map class2
 match access-group 102
policy-map policy1
 class class1
  bandwidth 500
  queue-limit 30
 class class2
  bandwidth 1000
interface ATM1/1/0.46 multipoint
 ip address 200.126.186.2 255.255.255.0
 pvc 46
  vbr-nrt 2000 2000
  encap aal5snap
  service policy output policy1
```

例：バンドルメンバー VC での VC 単位の WFQ と CBWFQ

次の例では、VC 単位の WFQ および CBWFQ がイネーブルであり、サービス ポリシーが設定されているメンバを持つ san-francisco という名前の PVC バンドルを示します。次の例では、次のポリシー マップに含まれているクラスが定義されており、ポリシー マップの policy1、policy2、および policy4 が作成されていると想定しています。各 PVC では、IP/ATM 間 CoS **pvc-bundle** コマンドを使用して、指定されたポリシー マップを適用する PVC を指定します。

PVC 0/34 および 0/31 には、同じポリシー マップ policy2 がアタッチされていることに注意してください。同じポリシー マップを複数の VC に割り当てることはできますが、各 VC に割り当てることができるのは、出力 PVC で適用されるポリシー マップ 1 つのみです。

```
bundle san-francisco
 protocol ip 1.0.2.20 broadcast
 encapsulation aal5snap
 pvc-bundle 0/35
  service policy output policy1
  vbr-nrt 5000 3000 500
  precedence 4-7
 pvc-bundle 0/34
  service policy output policy2
  vbr-nrt 5000 3000 500
  precedence 2-3
 pvc-bundle 0/33
  vbr-nrt 4000 3000 500
  precedence 2-3
  service policy output policy4
 pvc-bundle 0/31
  service policy output policy2
```

第 5 章

複雑な階層型スケジュール：フラグメント化されたポリシー（ポリシー集約）

QoS のポリシー集約機能は、異なるサブインターフェイス上のポリシー マップにあるデフォルトのトラフィック クラスのモジュラ QoS CLI（MQC）設定をサポートし、1 つのユーザ定義トラフィック クラスとしてメインインターフェイスのポリシー マップのキューに投入されます。これは、同じ物理インターフェイス上に複数のサブインターフェイス ポリシー マップがあり、それらのサブインターフェイス上でデフォルトのトラフィック クラスに同じ処理をする QoS 設定に最も適しています。

Cisco IOS XE リリース 2.6 以降、QoS のポリシー集約機能が強化され、DiffServ コード ポイント（DSCP）トラフィック クラスなど、完全優先転送（EF）、相対的優先転送 1（AF1）、および AF4 トラフィック クラスなどの他のトラフィック クラス用のプライマリ インターフェイスでのキューイング集約をサポートしています。この強化により、VLAN サブインターフェイスからのどのようなトラフィック クラスも、メインインターフェイスのポリシーマップでそのトラフィック クラス用の共通キューを共有できます。強化の内容には、これらのクラスの集約レベルで行われるドロップの統計情報を設定および表示できる機能も含まれています。

- QoS の前提条件：ポリシー集約，54 ページ
- QoS の制約事項：ポリシー集約，54 ページ
- QoS について：ポリシー集約，54 ページ
- QoS の設定例：ポリシー集約，59 ページ
- QoS の設定方法：ポリシー集約 MQC，69 ページ
- QoS の設定例：ポリシー集約，75 ページ
- その他の参考資料，79 ページ
- QoS の機能情報：ポリシー集約，80 ページ

QoS の前提条件：ポリシー集約

- この機能は MQC を使用して設定されます。
- メイン インターフェイス上のすべてのトラフィックは、1 つ以上のサブインターフェイスを通じて着信する必要があります。

QoS の制約事項：ポリシー集約

- 複数のポリシー マップを含む複数のサブインターフェイスを同じ物理インターフェイスに適用する場合にのみ適用します。この機能を使用して、異なる物理インターフェイス上のポリシー マップのデフォルトのトラフィック クラスやその他のトラフィック クラスをまとめて分類することはできません。
- Cisco IOS XE リリース 2.6 よりも前のサブインターフェイス ポリシー マップとメインインターフェイスポリシーマップでの特定のトラフィック クラスの設定には異なる動作があり、キューイングの結果も異なります。3 ページの「QoS ポリシー集約 MQC の概要」の項と、4 ページの「複数キューの集約に対する元の機能と MQC サポートの違い」の項を参照してください。
- ギガビット イーサネット インターフェイスでは **service-fragment** キーワードのみがサポートされています。ファスト イーサネット インターフェイスではサポートされていません。

QoS について：ポリシー集約

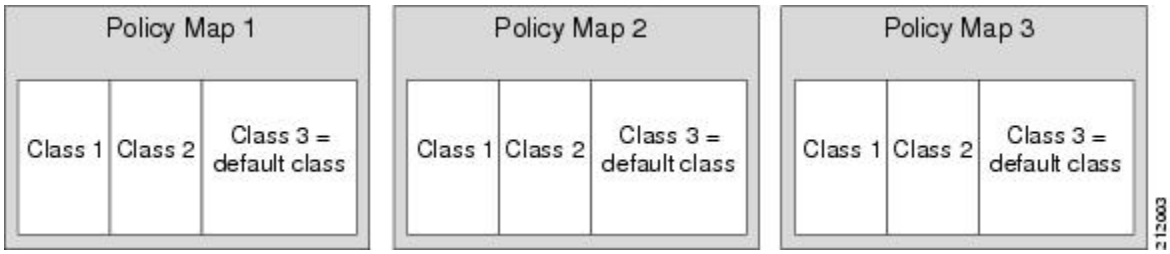
クラス定義文内のフラグメント

QoS のポリシー集約は、クラス定義文にフラグメントという発想を取り入れています。ポリシー マップ中で、デフォルト トラフィック クラス定義文をフラグメントとしてマークできます。同じインターフェイス上の他のポリシー マップでも、必要に応じてそのデフォルト トラフィック クラス文をフラグメントとして定義できます。その後、サービスフラグメントクラス定義ステートメントを使用して個別のポリシー マップを作成し、すべてのフラグメントに 1 つのグループとして QoS を割り当てるために使用できます。

次の図に、フラグメントを使用していない 3 つのポリシー マップが適用された 1 つの物理インターフェイスの例を示します。各ポリシー マップには、独自のポリシー マップ内でデフォルト

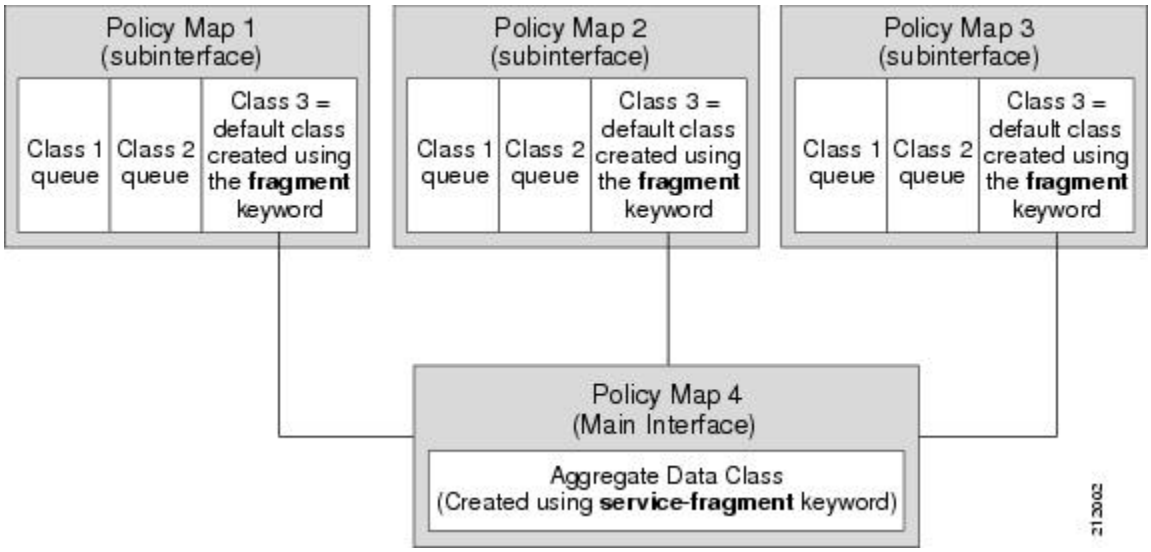
トラフィックのトラフィックのみを分類できるデフォルトのトラフィック クラスがあることに注意してください。

図 *1*：フラグメントなしで設定した *3* つのポリシー マップ



次の図にフラグメントを使用して設定した同じ設定を示し、フラグメントをまとめて分類するクラス定義文を使用して 4 つめのポリシー マップを追加します。デフォルトのトラフィック クラスは、個々のポリシー マップ内の 3 つの個別のデフォルトのトラフィック クラスとしてではなく、1 つのサービス フラグメント グループとして分類されます。

図 *2*：フラグメントを使用して設定した *3* つのポリシー マップ



Gigabit EtherChannel バンドルのフラグメント

Gigabit Etherchannel バンドルに対してフラグメントを設定すると、**fragment** キーワードを使用して設定したデフォルトのトラフィック クラスを持つポリシーマップがメンバーサブインターフェイスのリンクに適用され、フラグメントをまとめて分類するように **service-fragment** キーワードを使用して設定したトラフィック クラスを持つポリシーマップが物理インターフェイスに適用されます。

特定のポートチャネルのメンバー リンクで現在アクティブなフラグメントを使用して設定したすべてのポートチャネル サブインターフェイスは、そのメンバー リンクに集約サービス フラグメント クラスを使用します。メンバー リンクがダウンすると、セカンダリ メンバー リンクに切り替わる必要があるポートチャネルのサブインターフェイスは、新しいインターフェイスに集約サービス フラグメントを使用します。

ポリシー マップ内のフラグメント トラフィック クラス

ポリシー マップのデフォルトの class ステートメントのみがフラグメントとして設定できます。

フラグメントは、複数のポリシー マップが同じ物理インターフェイスに適用されている場合にのみ機能します。このプロセスを使用して、異なる物理インターフェイス上のポリシー マップのフラグメントとしてデフォルトのトラフィック クラスを分類することはできません。

fragment キーワードが入力されているクラスではキューイング機能だけが許可され、**fragment** キーワードが使用されているクラスでは1つ以上のキューイング機能を入力する必要があります。

fragment キーワードを使用したクラスがあるポリシーマップは、インターフェイスから出て行くトラフィックのみに適用できます（**service-policyoutput** コマンドを使用してインターフェイスに適用したポリシー マップ）。

fragments キーワードは、子ポリシー マップには入力できません。

サービス フラグメント トラフィック クラスについて

サービス フラグメントを使用すると、同じ物理インターフェイスからのフラグメントのみをまとめて分類できます。同じサービス フラグメントを使用して、別のインターフェイスからのフラグメントを分類することはできません。

service-fragment キーワードが入力されているクラスではキューイング機能だけが許可され、**service-fragment** キーワードが使用されているクラスでは1つ以上のキューイング機能を入力する必要があります。

service-fragment キーワードを使用したクラスがあるポリシー マップは、インターフェイスから出て行くトラフィックのみに適用できます（**service-policyoutput** コマンドを使用してインターフェイスに適用したポリシー マップ）。

service-fragment キーワードを使用して設定したクラスは、インターフェイス上にまだ設定されているフラグメントに QoS をまとめて適用するために使用中である場合は削除できません。**service-fragment** キーワードを使用して設定したクラスを削除するには、そのサービス フラグメントを削除する前にフラグメント トラフィックのクラスを削除します。

service-fragment キーワードは、子ポリシー マップに入力できません。

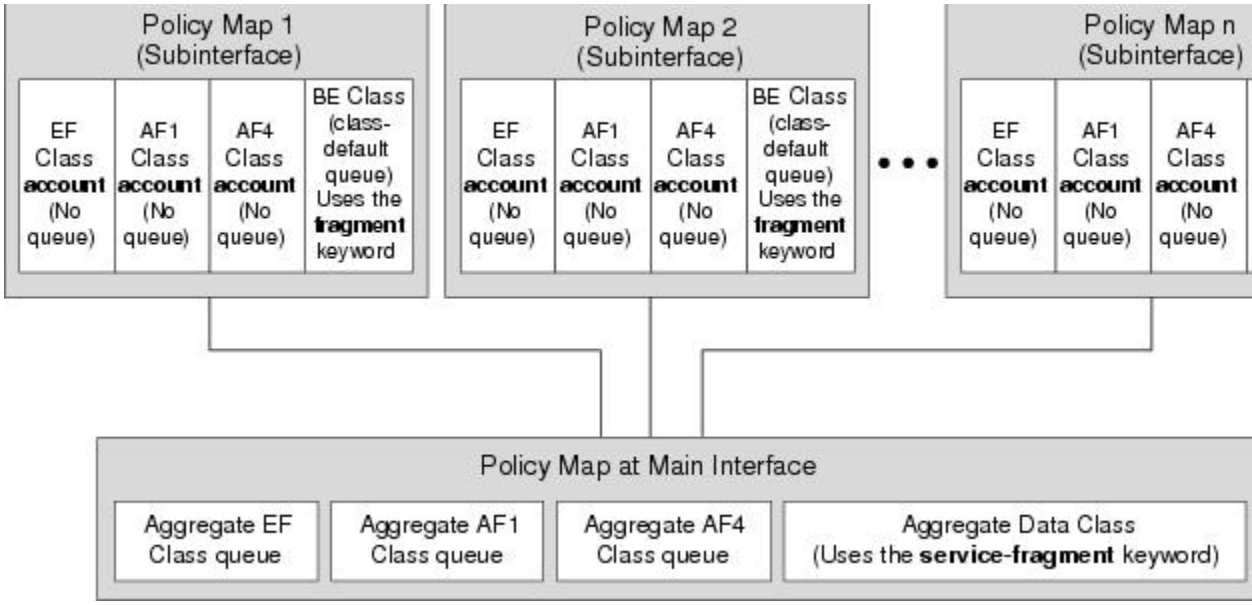
QoS：ポリシー集約 MQC

メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能は、**フラグメント**の設定と**サービス フラグメント**の設定を使用した class-default トラフィックの

以前の集約のサポートを、次の図に示すように、メインインターフェイスのポリシー マップで集約されたDSCPベースのトラフィック クラスなどのサブインターフェイスのポリシー マップ内のユーザ定義の他のトラフィック クラスに拡張します。

キューイングがサブインターフェイスのポリシーマップのトラフィック クラスに設定されていない場合は、**account** コマンドを使用して、これらのクラスの集約レベルで行われるキューイングのドロップを追跡でき、**show policy-map interface** コマンドを使用して表示できます。

図 *3*：メイン インターフェイスでの複数のキュー集約に対する *MQC* サポート機能のポリシー マップの概要



複数キュー集約の元の機能と MQC サポートの違い

元の QoS ポリシー集約機能と、メイン インターフェイスでの複数キュー集約に対する MQC サポート機能での機能拡張間の設定の一部は似ているように見えますが、キューイング動作と内部データの処理に重要ないくつかの違いがあります。

たとえば、どちらの設定も、サブスクライバ ポリシー マップの **classclass-default** コマンドの **fragment** キーワードを共有し、これを使用する必要があるだけでなく、集約トラフィックに対して共通のポリシー処理を実現するために、メインインターフェイスのポリシーマップのユーザ定義クラスに **service-fragment** キーワードを設定する必要があります。ただし、この設定を使用すると、元のQoSポリシー集約の実装と、強化されたQoSポリシー集約の実装とでは動作に違いが生じます。

- フラグメントとサービス フラグメント アーキテクチャを使用した元の実装（Cisco IOS XE リリース 2.6 よりも前）では、すべてのデフォルト クラスのトラフィックと、サブインターフェイスで定義されたキューイング機能を備えていないクラスのすべてのトラフィックが class-default キューに移動し、メイン ポリシー マップで定義されている共通のユーザ定義のキューとポリシーに集約されます。サブインターフェイスの（同じ物理インターフェイス上

の複数のサブスクライバからなどの）トラフィック集約は、最終的には、デフォルトクラスである 1 つのクラスに対してのみ発生します。

機能の特性は次のとおりです。

- すべてのサブインターフェイスのトラフィック クラスにキューがあります。ただし、キューイング機能（**priority**、**shape**、**bandwidth**、**queue-limit**、**fair-queue**、**random-detect** などのコマンドは設定されていない）を使用してトラフィック クラスがサブインターフェイスのポリシーマップに設定されていない場合、トラフィックはclass-defaultキューに割り当てられます。
- **fragment** キーワードをサブインターフェイス **classclass-default** の設定と、**service-fragment** 設定をメイン インターフェイス クラスで使用するときに、複数のサブインターフェイスからのデフォルト クラスのトラフィックをメイン インターフェイスの共通ポリシーマップに集約できます。
- **fragment** と **service-fragment** の設定を使用しないサブインターフェイスのトラフィック クラスに対しては、メインインターフェイスのポリシーマップでの分類は行われず、サポートもされていません。
- キューイングは、サブインターフェイスのポリシーマップでキューイング機能を使用して定義した他のトラフィック クラスのサブインターフェイスで実行されます。

• フラグメントとサービス フラグメント機能を使用するメイン インターフェイスでの複数キューの集約に対する MQC サポート機能が強化された実装（Cisco IOS XE リリース 2.6 以降）でも、デフォルトのすべてのクラスのトラフィックも class-default キューに移動し、メイン ポリシー マップで定義された共通のユーザ定義キューとポリシーに集約されます。ただし、集約ポリシーについては、DSCP ベースのサブスクライバ トラフィック クラスなどの他のクラスもサポートされています。これらのトラフィック クラスは、サブスクライバ ポリシー マップの **account** 以外のキューやキューイング機能をサポートしていません。フラグメントとサービス フラグメント アーキテクチャを使用することによって、（同じ物理インターフェイス上の複数のサブスクライバからの）これらの他のサブスクライバ トラフィック クラスがメイン ポリシー マップでこれらの同じクラスに対して定義されている集約トラフィックに対して共通のポリシー処理が実現します。

機能の特性は次のとおりです。

- 設定されたキューイング機能がないサブインターフェイスのトラフィック クラスには、サブスクライバ レベルのキューがありません。
- **fragment** キーワードをサブインターフェイス **classclass-default** の設定と、**service-fragment** 設定をメイン インターフェイス クラスで使用するときに、複数のサブインターフェイスからのデフォルト クラスのトラフィックをメイン インターフェイスの共通ポリシーマップに集約できます。この設定ではさらに、メインインターフェイスの共通ポリシーマップに集約する他のサブインターフェイスのトラフィック クラス（DSCP ベースのクラスなど）に対するサポートをイネーブルにします。
- 次の設定要件に従って、他のクラス トラフィックを複数のサブインターフェイスからメイン インターフェイスの共通ポリシー マップに集約できます。

- **fragment** キーワードをサブインターフェイスの **classclass-default** 設定で使用し、**service-fragment** 設定をメインインターフェイス クラスに使用することで、この動作が有効になります（これは、デフォルト クラスの集約もイネーブルにします）。
- 他のトラフィック クラスについては、サブインターフェイスのポリシーマップでキューイング機能を設定しません。
- 他のサブインターフェイスのトラフィック クラスについては、メインインターフェイスのポリシー マップで集約としてキューイングが実行されます。
- 統計情報の任意のトラッキングをサポートするには、サブインターフェイスのポリシーマップに **account** コマンドを使用します。

キュー制限と WRED しきい値の変更

Cisco IOS XE リリース 2.6 の Cisco ASR 1000 シリーズ ルータでは、キュー制限と WRED しきい値の両方に対する設定単位としてバイト単位の追加を行えます。したがって、このリリースでは、いくつかの制限がありますが、パケットベースとバイトベースの両方の制限を設定できます。

QoS の設定例：ポリシー集約

例 1：QoS の設定：インターフェイスのポリシー集約

ポリシー マップでのフラグメント トラフィック クラスの設定

はじめる前に

この手順では、ポリシー マップ内にデフォルト トラフィック クラスをフラグメントとして設定する方法のみを示します。これには、ポリシー マップ内の他のクラスや、デバイス上の他のポリシー マップの設定に関する手順は含まれていません。

例

（注） この例では、Cisco IOS XE リリース 2.6 よりも前のリリースでサポートされている設定例を示します。

次の例では、BestEffort というフラグメントがポリシー マップ subscriber1 とポリシー マップ subscriber 2 に作成されます。この例では、他のトラフィック クラスのキューイング機能はサブインターフェイスのポリシー マップでサポートされます。

```
policy-map subscriber1
 class voice
```

```
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber 2
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

（注） この例では、Cisco IOS XE リリース 2.6 以降のリリースでサポートされている設定を示します。

また、次に、メイン インターフェイスの実装で、複数キューの集約に対する QoS ポリシー集約 MQC サポートを使用して、サブインターフェイスのポリシーマップにデフォルト クラスとして BestEffort というフラグメントを設定する例を示します。この例では、ポリシーマップの他のクラスに対してキューイング機能がサポートされていないことに注意してください。

```
policy-map subscriber1
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

default class ステートメントを複数のサブインターフェイス ポリシー マップにフラグメントとして設定した後、service-fragment キーワードを使用した class ステートメントを持つ個別のポリシー マップを設定し、フラグメントとして設定した class ステートメントに QoS を適用する必要があります。

次の作業

デフォルトの class ステートメントを複数のサブインターフェイス ポリシー マップのフラグメントとして設定した後に、**service-fragment** キーワードを使用して class ステートメントの個別のポリシー マップを設定し、フラグメントとして設定した class ステートメントに QoS を適用する必要があります。

このタスクについては、8 ページの「サービス フラグメント トラフィック クラスの設定」の項を参照してください。

サービス フラグメントのトラフィック クラスの設定

はじめる前に

次に、ポリシー マップ内にサービス フラグメント トラフィックの class ステートメントを設定するタスクを示します。サービスフラグメントトラフィッククラスを使用して、他のポリシーマップを以前にフラグメントとして設定した default class ステートメントのコレクションに QoS を適用します。

この手順では、フラグメントのデフォルトトラフィッククラスがすでに作成されていると想定しています。フラグメントのデフォルト トラフィック クラスの作成手順については、「ポリシーマップでのフラグメント トラフィック クラスの設定」の項を参照してください。

すべてのポリシーマップと同様に、設定はインターフェイスに適用されるまで、ネットワーク トラフィックを管理しません。この手順では、インターフェイスへのポリシー マップの適用プロセスは扱いません。

（注） サービス フラグメントを使用すると、同じ物理インターフェイスからのフラグメントのみをまとめて分類できます。同じサービス フラグメントを使用して、別のインターフェイスからのフラグメントを分類することはできません。

service-fragment キーワードが入力されているクラスではキューイング機能だけが許可され、**service-fragment** キーワードが使用されているクラスでは 1 つ以上のキューイング機能を入力する必要があります。

service-fragment キーワードを使用したクラスがあるポリシー マップは、インターフェイスから出て行くトラフィックのみに適用できます（**service-policyoutput** コマンドを使用してインターフェイスに適用したポリシー マップ）。

service-fragment キーワードを使用して設定したクラスは、インターフェイス上にまだ設定されているフラグメントにQoSをまとめて適用するために使用中である場合は削除できません。**service-fragment** キーワードを使用して設定したクラスを削除するには、そのサービス フラグメントを削除する前にフラグメント トラフィックのクラスを削除します。

service-fragment キーワードは、子ポリシー マップに入力できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-name***service-fragment***fragment-class-name*
5. **shapeaveragepercent***percent*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Device(config)# policy-map BestEffortFragments`	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class***class-name***service-fragment***fragment-class-name* 例： `Device(config-pmap)# class data service-fragment BestEffort`	*fragment-class-name* に一致するすべてのフラグメントを合わせたトラフィックのクラスを指定します。他のポリシーマップでフラグメントを定義する場合、サービス フラグメント クラスを正しく設定するには、*fragment-class-name* がこのコマンド ラインの *fragment-class-name* に一致する必要があります。
ステップ 5	**shapeaveragepercent***percent* 例： `Device(config-pmap-c)# shape average percent 50`	QoS コンフィギュレーションコマンドを入力します。フラグメントとして設定されたデフォルトのトラフィック クラスでは、キューイング機能のみがサポートされます。 サポートされているキューイング機能は、**bandwidth**、**shape**、および **random-detectexponential-weighting-constant** です。 複数の QoS キューイング コマンドを入力できます。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	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、特権 EXEC モードに戻ります。

例

（注） この例では、Cisco IOS XE リリース 2.6 よりも前のリリースでサポートされている設定例を示します。

次の例では、BestEffort という名前のすべてのフラグメントに QoS を適用するために、ポリシーマップが作成されます。

```
policy-map main-interface
 class data service-fragment BestEffort
  shape average 400000000
```

次の例では、2 つのフラグメントを作成し、サービス フラグメントを使用してまとめて分類します。

```
policy-map subscriber1
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber 2
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

（注） この例では、Cisco IOS XE リリース 2.6 以降のリリースでサポートされている設定を示します。

次に、サブ インターフェイス ポリシー マップに BestEffort という 2 つのフラグメントを作成し、BestEffort という**サービス フラグメント**を設定してメイン インターフェイスのポリシー マップでキューを集約する例を示します。

```
policy-map subscriber1
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber2
 class voice
  set cos 5
  account
 class video
```

```
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map main-interface
 class voice
  priority level 1
 class video
  priority level 2
 class AF1
  bandwidth remaining ratio 90
 class data service-fragment BestEffort
  shape average 400000000
  bandwidth remaining ratio 1
```

トラブルシューティングのヒント

同じサービス フラグメントの一部であると思われるすべての class ステートメントが同じフラグメントクラス名を共有していることを確認します。

次の作業

ポリシーマップ（トラフィック ポリシー）をインターフェイスに適用する必要があります。このタスクについては、「MQC を使用した QoS 機能の適用」の章の「MQC を使用したインターフェイスへのトラフィック ポリシーの適用」の項を参照してください。

QoS の設定：Gigabit EtherChannel でのポリシー集約

QoS の Gigabit EtherChannel バンドルでのポリシー集約を適切に設定するには、次のアクションを実行する必要があります。

- サービス フラグメント トラフィック クラスを設定し、主要な物理インターフェイスに適用する必要があります。
- フラグメント トラフィック クラスを設定し、メンバー リンクのサブインターフェイスに適用する必要があります。

Gigabit EtherChannel バンドルをサポートする物理インターフェイスでのサービス フラグメントの設定

はじめる前に

この手順では、サービス フラグメント トラフィック クラスがすでに作成されている必要があります。フラグメント クラスを設定しないと、サービス フラグメントのトラフィック クラスは設定できません。フラグメントのクラスを作成する手順については、「ポリシー マップでのフラグメントのトラフィック クラスの設定」の項を参照してください。サービスフラグメントのクラスを作成する手順については、「サービスフラグメントのトラフィック クラスの設定」の項を参照してください。

これらの手順には、Gigabit EtherChannel のメンバー リンクのサブインターフェイスに設定可能なオプションに関する詳細は示されていません。これらの手順では、フラグメントのトラフィッククラスをすでに持っているポリシーマップをメンバーリンクのサブインターフェイスに適用する手順のみが説明されています。

（注） 正しく動作させるには、ポートチャネルのメンバー リンクがダウンしたときに、すべてのメンバー リンクに同じポリシー マップが適用されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface GigabitEthernet***card*/*bay*/*port*
4. **service-policyoutput***service-fragment-class-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface GigabitEthernet***card*/*bay*/*port* 例： `Device(config)# interface GigabitEthernet 0/1/0`	サービス ポリシー設定を受け取るメンバー リンクの物理インターフェイスを指定します。
ステップ 4	**service-policyoutput***service-fragment-class-name* 例： `Device(config-if)# service-policy output aggregate-member-link`	サービス フラグメントのデフォルトのトラフィッククラスを含むサービス ポリシーを物理ギガビット イーサネット インターフェイスに適用します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

例

次に、ポリシー マップの集約メンバーリンクを物理インターフェイスに適用する例を示します。

```
interface GigabitEthernet1/1/1
 service-policy output aggregate-member-link
!
interface GigabitEthernet1/1/2
 service-policy output aggregate-member-link
```

次の作業

service-fragment の定義と fragment-class の定義で、フラグメント クラス名が整合していることを確認します。「Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定」の項に進みます。

トラブルシューティングのヒント

service-fragment の定義と fragment-class の定義で、サービスフラグメント名が整合していることを確認します。

次の作業

Gigabit EtherChannel のメンバー リンクのサブインターフェイスにフラグメント サービス ポリシーを適用します。このタスクについては、14 ページの「Gigabit EtherChannel のメンバー リンク サブインターフェイスでのフラグメントの設定」の項を参照してください。

Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定

はじめる前に

このタスクでは、サービスフラグメントのトラフィック クラスがすでに作成されている必要があります。フラグメント クラスを設定しないと、サービス フラグメントのトラフィック クラスは設定できません。フラグメントのクラスを作成する手順については、6 ページの「ポリシー マップでのフラグメントのトラフィック クラスの設定」の項を参照してください。サービスフラグメ

ントのクラスを作成する手順については、8 ページの「サービス フラグメントのトラフィック クラスの設定」の項を参照してください。

これらの手順には、Gigabit EtherChannel のメンバー リンクのサブインターフェイスに設定可能なオプションに関する詳細は示されていません。これらの手順では、フラグメントのトラフィック クラスをすでに持っているポリシーマップをメンバー リンクのサブインターフェイスに適用する手順のみが説明されています。

（注） フラグメントは、2 つ以上の物理インターフェイスのトラフィックに使用できません。この設定を正しく機能させるには、GEC が同じ物理インターフェイス上にすべて存在していなければなりません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceport-channel***port-channel-interface-number.port-channel-subinterface-number*
4. **service-policyoutput***fragment-class-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**interfaceport-channel***port-channel-interface-number.port-channel-subinterface-number* 例： `Router(config)# interface port-channel 1.100`	サブインターフェイス コンフィギュレーション モードを開始し、EtherChannel メンバー リンクのサブインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**service-policyoutput***fragment-class-name* 例： `Router(config-subif)# service-policy output subscriber`	EtherChannel メンバー リンクのサブインターフェイスに対し、フラグメントのデフォルトのトラフィック クラスが含まれているサービス ポリシーを適用します。

例

（注） 次に、Cisco IOS XE リリース 2.6 よりも前のリリースの元の QoS のポリシー集約機能に対してサポートされている設定例を示します。Cisco IOS XE リリース 2.6 での更新に関する新しいポリシーマップの設定ガイドラインに従うことで、メイン インターフェイスでの複数キュー集約に対する QoS ポリシー集約 MQC サポート機能に適応できます。

次の例では、subscriber というサービス ポリシーにフラグメントのデフォルトのトラフィック クラスがあり、このサービス ポリシーが Gigabit EtherChannel バンドルのメンバー リンクのサブインターフェイスに適用されます。

（注） この例には、フラグメントのデフォルトのトラフィック クラスを Gigabit EtherChannel バンドルのメンバー リンクのサブインターフェイスに適用する方法のみが示されています。この設定は完全ではなく、物理インターフェイスが設定され、サービスフラグメント トラフィック クラスをサポートするようになるまではデフォルトのトラフィックを適切に分類しません。

```
policy-map subscriber
 class voice
  priority level 1
 class video
  priority level 2
 class class-default fragment BE
  shape average 100000000
  bandwidth remaining ratios 80
policy-map aggregate-member-link
 class BestEffort service-fragment BE
  shape average 100000000
!
interface Port-channel1
 ip address 172.16.2.3 255.255.0.0
!
interface Port-channel1.100
 encapsulation dot1Q 100
 ip address 192.168.2.100 255.255.255.0
 service-policy output subscriber
!
```

トラブルシューティングのヒント

この設定は、サービスフラグメントのデフォルトのトラフィックが作成されてフラグメントとしてマークされたデフォルトのトラフィック クラスを分類するまでは機能しません。このサービスフラグメント トラフィック クラスは、ネットワーク トラフィックに影響を与えるように、この設定に対して設定する必要があります。

QoS の設定方法：ポリシー集約 MQC

Cisco IOS XE リリース 2.6 とそれ以前の Cisco IOS XE ソフトウェア リリースでのポリシー集約機能の設定のサポートにはある程度の下位互換性があります。ただし、QoS に移行する場合、物理インターフェイスに関するアップグレードガイドライン（メインインターフェイスでの複数キューの集約に対するポリシー集約 MQC サポート機能の設定）を順守してください。

最適な結果を得るには、Cisco IOS XE リリース 2.6 よりも前に実装したサービス ポリシー設定がある場合は、サポート対象の最新の設定にアップグレードする必要があります。

元の QoS と強化された QoS のポリシー集約機能の設定は、同じ物理インターフェイス上に混在設定がない場合は、同じ Cisco ASR 1000 シリーズ ルータ上にのみ存在することができます。つまり、1 つの物理インターフェイスで元の設定をサポートし、別の物理インターフェイスで強化された設定をサポートできます。

QoS のメイン インターフェイスでの複数キューの集約に対するポリシー集約 MQC サポート機能には、元の機能のフラグメント トラフィック クラスと同じ設定が必要です。**classclass-defaultfragment** コマンドを使用して有効にしてから、デフォルトのトラフィック クラスと別のトラフィック クラスの両方に対してすべてのサブインターフェイス ポリシー集約を定義します。

QoS のメインインターフェイスでの複数キュー集約に対するポリシー集約 MQC サポート機能では、集約クラス キューに対するキューイング機能（サブインターフェイスで定義されている対応するクラスからのトラフィック）はメインインターフェイスのポリシー マップで設定されます。

QoS のサービス ポリシーのアップグレード：ポリシー集約 MQC

はじめる前に

QoS をサポートするためのサービス ポリシーのアップグレード：メイン インターフェイスでの複数キューの集約に対するポリシー集約 MQC サポート機能では、次のネットワーク条件を前提としています。

- ネットワークに適した対応する class-map ステートメントがすでに設定されている。
- Cisco IOS XE リリース 2.6 より前のデフォルト トラフィック クラスについては、QoS サービス ポリシーの集約が前もって設定されており、所定の物理インターフェイスとそれに対応するサブインターフェイス、あるいはサブスクライバインターフェイスのメイン インターフェイス ポリシーに適用されている。

- Cisco IOS XE リリース 2.6 より前のサービス ポリシー集約機能を設定した物理インターフェイスと同じインターフェイス上のポートは、「QoS：メイン インターフェイスでの複数キューの集約に対するポリシー集約 MQS のサポート」の設定をサポートする必要がある。

アップグレード作業

手順の概要

1. メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能にサービス ポリシーを設定します。
2. 以前に設定したポリシー集約機能に対する Cisco IOS XE リリース 2.6 よりも前に設定したサービス ポリシーを **noservice-policy** コマンドと **nopolicy-map** コマンドを使用して削除します。
3. メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能に対し、**service-policyoutput** コマンドを次のように使用して、サービス ポリシーを適用します。

手順の詳細

ステップ 1 メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能にサービス ポリシーを設定します。
18 ページの「QoS の設定：ポリシー集約 MQC トラフィック クラス」に記載されているタスクを参照してください。

ステップ 2 以前に設定したポリシー集約機能に対する Cisco IOS XE リリース 2.6 よりも前に設定したサービス ポリシーを **noservice-policy** コマンドと **nopolicy-map** コマンドを使用して削除します。

a) 各サブインターフェイスで、**noservice-policy** コマンドを設定します。最初にサブインターフェイスでポリシーを削除してください。
b) 物理インターフェイスで、**noservice-policy** コマンドを設定します。

ステップ 3 メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能に対し、**service-policyoutput** コマンドを次のように使用して、サービス ポリシーを適用します。

a) 物理インターフェイスで、**service-policyoutput** コマンドを設定します。
b) 各サブインターフェイスで、**service-policyoutput** コマンドを設定します。

QoS の設定：ポリシー集約 MQC トラフィック クラス

サブスクライバ インターフェイスでのトラフィック クラスの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-name*
5. **account** [**drop**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map subscriber1`	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class***class-name* 例： `Router(config-pmap)# class EF`	メインインターフェイス ポリシー マップで集約するトラフィック クラスの名前を指定し、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。 （注） このクラスに対してはキューイング機能を設定しないでください。このクラスと物理インターフェイスに関連付けられたすべてのサブインターフェイスに対してメインインターフェイス ポリシーマップでキューイングが設定され、集約されます。

	コマンドまたはアクション	目的
ステップ 5	**account** [**drop**] 例： `Router(config-pmap-c)# account`	（任意）**drop** キーワードですべてのパケット ドロップ統計情報を収集する場合、このコマンドが設定さたトラフィック クラスに一致するパケットの統計情報の収集をイネーブルにします。ドロップ統計情報の収集はデフォルトです。

例

次に、ドロップ統計情報の収集を行うサブスクライバ サブインターフェイスでのポリシー集約に EF トラフィック クラスを設定する例を示します。

```
policy-map subscriber1
 class EF
 account
```

次の作業

集約するすべてのトラフィック クラスに対して次のタスクを実行してから、19ページの「サブインターフェイスでのフラグメント トラフィック クラスの設定」の項のタスクを実行します。

サブインターフェイスでのフラグメント トラフィック クラスの設定

次の作業

サブインターフェイスのポリシーマップ設定を初期の QoS のポリシー集約機能の実装からアップグレードする場合は、**noservice-policy** コマンドを使用してサブインターフェイスから現在のサービスポリシーを削除します。

service-policyoutput コマンドを使用して、サブインターフェイスの発信トラフィックに新しいポリシー マップを適用します。

メイン インターフェイスでのトラフィック クラスの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-name*
5. **prioritylevel***level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map main-interface`	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class***class-name* 例： `Router(config-pmap)# class EF`	メインインターフェイスポリシーマップで集約するトラフィック クラスの名前を指定し、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。
ステップ 5	**prioritylevel***level* 例： `Router(config-pmap-c)# priority level 1`	QoS コンフィギュレーション コマンドを入力します。 現在サポートされているキューイング機能は、**bandwidth**、**priority**、**shape**、and **random-detectexponential-weighting-constant** です。 複数の QoS キューイング コマンドを入力できます。

例

次に、集約サービスフラグメント データ クラスとともに、3 つのトラフィック クラスをメインインターフェイス ポリシー マップで設定する例を示します。

```
policy-map main-interface
 class voice
  priority level 1
 class video
  priority level 2
 class AF1
  bandwidth remaining ratio 90
 class data service-fragment BestEffort
  shape average 400000000
  bandwidth remaining ratio 1
```

次の作業

次のタスクを実行して集約するすべてのトラフィック クラスに対してキューイング機能を定義してから、21 ページの「メイン インターフェイスでのサービス フラグメント トラフィック クラスの設定」の項のタスクを実行します。

メイン インターフェイスでのサービス フラグメント トラフィック クラスの設定

次の作業

デフォルトの複数の class ステートメントをポリシーマップのフラグメントとして設定した後に、**service-fragment** キーワードを使用して class ステートメントの個別のポリシー マップを設定し、フラグメントとして設定した class ステートメントに QoS を適用する必要があります。

このプロセスについては、「サービス フラグメント トラフィック クラスの設定」の項を参照してください。

QoS の設定：ポリシー集約 MQC サポート

QoS のメイン インターフェイスでの複数キューの集約に対するポリシー集約 MQC サポート機能は、この拡張機能について記載されたサブスクライバおよびメインインターフェイスの設定ガイドラインに従って、強化されたサービス ポリシーの設定も Gigabit EtherChannel 上でサポートします。

詳細については、次の項を参照してください。

トラフィック ポリシー クラスのポリシー情報とドロップ統計情報の確認

account コマンドを使用してイネーブルになったポリシーマップの設定とサブスクライバのドロップ統計に関する情報を表示するには、**show policy-map interface** コマンドを使用します。

```
Router# show policy-map interface port-channel 1.1
Port-channel1.1
   Service-policy input: input_policy
     Class-map: class-default (match-any)
       0 packets, 0 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: any
       QoS Set
       dscp default
       No packet marking statistics available
   Service-policy output: Port-channel_1_subscriber
     Class-map: EF (match-any)
       105233 packets, 6734912 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp ef (46)
       Match: access-group name VLAN_REMARK_EF
       Match: qos-group 3
       Account QoS statistics
```

```
    Queueing
      Packets dropped 0 packets/0 bytes
  QoS Set
  cos 5
  No packet marking statistics available
  dscp ef
  No packet marking statistics available
Class-map: AF4 (match-all)
  105234 packets, 6734976 bytes
  5 minute offered rate 134000 bps, drop rate 0000 bps
  Match: dscp cs4 (32)
  Account QoS statistics
    Queueing
      Packets dropped 0 packets/0 bytes
  QoS Set
  cos 4
  No packet marking statistics available
Class-map: AF1 (match-any)
  315690 packets, 20204160 bytes
  5 minute offered rate 402000 bps, drop rate 0000 bps
  Match: dscp cs1 (8)
  Match: dscp af11 (10)
  Match: dscp af12 (12)
  Account QoS statistics
    Queueing
      Packets dropped 0 packets/0 bytes
  QoS Set
  cos 1
  No packet marking statistics available
Class-map: class-default (match-any) fragment Port-channel_BE
  315677 packets, 20203328 bytes
  5 minute offered rate 402000 bps, drop rate 0000 bps
  Match: any
  Queueing
    queue limit 31250 bytes
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 315679/20203482
    bandwidth remaining ratio 1
```

QoS の設定例：ポリシー集約

例：QoS：ポリシー集約

（注） 次の例には、Cisco IOS XE リリース 2.6 より前の元の QoS ポリシー集約機能でサポートされている設定が示されています。

次に、QoS のポリシー集約を使用してトラフィックのフラグメント クラスを定義し、BestEffort という名前のデフォルトのトラフィック クラスを使用してデフォルトのトラフィックを分類する例を示します。subscriber1 と subscriber2 というポリシー マップからのすべてのデフォルトのトラフィックは、BestEffort というフラグメント デフォルトのトラフィック クラスの一部です。このデフォルトのトラフィックが、**service-fragment** キーワードと **shape** コマンドを使用する、data というクラスを作成することによってまとめてシェーピングされます。

この例では、次の点に注意してください。

- 各フラグメント デフォルトのトラフィック クラスのクラス名は「BestEffort」です。

- クラス名の「BestEffort」は、**service-fragment** キーワードが入力されるクラスの定義にも使用します。このクラスは、「BestEffort」というフラグメント デフォルトのトラフィック クラスを使用して転送されるすべてのトラフィックにシェーピング ポリシーを適用します。

```
policy-map subscriber1
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber 2
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map input_policy
 class class-default
  set dscp default
policy-map main-interface
 class data service-fragment BestEffort
  shape average 400000000
interface portchannel1.1001
 encapsulation dot1q 1001
 service-policy output subscriber1
 service-policy input input_policy
interface portchannel1.1002
 encapsulation dot1q 1002
 service-policy output subscriber2
 service-policy input input_policy
interface gigabitethernet 0/1
 description member-link1
 port channel 1
 service-policy output main-interface
interface gigabitethernet 0/2
 description member-link2
 port channel 1
service-policy output main-interface
```

例：Gigabit EtherChannel QoS ポリシー集約

（注） 次の例には、Cisco IOS XE リリース 2.6 より前の元の QoS ポリシー集約機能でサポートされている設定が示されています。

次に、BE という名前のフラグメント クラスを使用してポリシー マップ サブスクライバを設定する例を示します。フラグメントは、aggregate-member-link という名前のポリシーの一部として設定します。ポリシー マップ サブスクライバがバンドルのサブインターフェイスに適用され、ポリシー マップ aggregate-member-link が物理インターフェイスに関連付けられます。

```
port-channel load-balancing vlan-manual
class-map match-all BestEffort
```

```
!
class-map match-all video
!
class-map match-all voice
!
policy-map subscriber
 class voice
  priority level 1
 class video
  priority level 2
 class class-default fragment BE
  shape average 100000000
  bandwidth remaining ratios 80
policy-map aggregate-member-link
 class BestEffort service-fragment BE
  shape average 100000000
!
interface Port-channel1
 ip address 10.1.1.3 255.255.0.0
!
interface Port-channel1.100
 encapsulation dot1Q 100
 ip address 10.1.2.1 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.200
 encapsulation dot1Q 200
 ip address 10.1.2.2 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.1.2.3 255.255.255.0
 service-policy output subscriber
!
interface GigabitEthernet1/1/1
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
!
interface GigabitEthernet1/1/2
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
```

例：メイン インターフェイスでの QoS ポリシー集約

（注） この例では、Cisco IOS XE リリース 2.6 以降にサポートされている設定例を示します。

Port-channel_1_main_policy というメインインターフェイス ポリシー マップで、DSCP ベースのサブスクライバ トラフィック クラスのキューイング機能を設定します。また、メインインターフェイス キューに実装されているバイトベースのキュー制限とランダム検出のしきい値の使用法も確認できます。

サブスクライバクラスのデフォルトのフラグメントクラスからのトラフィックを集約するように Port-channel_BE というサービス フラグメントも設定します。

```
policy-map Port-channel_1_main_policy
 class EF
  priority level 1
  queue-limit 547500 bytes
 class AF4
```

```
  priority level 2
  queue-limit 4037500 bytes
 class AF1
  bandwidth remaining ratio 90
  queue-limit 750000 bytes
  random-detect dscp-based
  random-detect dscp 8 750000 bytes 750000 bytes
  random-detect dscp 10 750000 bytes 750000 bytes
  random-detect dscp 12 600000 bytes 675000 bytes
 class data service-fragment Port-channel_BE
  shape average 250000000
  bandwidth remaining ratio 1
!
```

この例では、Port-channel_BE というフラグメント クラスを使用してポリシー マップ Port-channel_1_subscriber を設定します（簡単にするために、単一のサブインターフェイス ポリシーのみを示します）。これにより、サブスクライバ トラフィック クラスのキューイングとポリシー集約がメインインターフェイス ポリシー マップでイネーブルになります。

Port-channel_1_subscriber ポリシー マップは、EF、AF4、および AF1 の DSCP ベースのトラフィック クラスを特定し、これらのクラスのドロップ統計情報の収集をイネーブルにします。

```
policy-map Port-channel_1_subscriber
 class EF
  account
  set cos 5
  set dscp ef
 class AF4
  account
  set cos 4
 class AF1
  account
  set cos 1
 class class-default fragment Port-channel_BE
  bandwidth remaining ratio 1
  queue-limit 31250 bytes
!
port-channel load-balancing vlan-manual
!
interface Port-channel1
 no ip address
 no negotiation auto
!
```

サービス ポリシーは、次に示すように、最初に物理インターフェイスに適用されてから、サブインターフェイスに適用されます。

```
interface GigabitEthernet1/2/0
 no ip address
 negotiation auto
 no cdp enable
 service-policy output Port-channel_1_main_policy
 channel-group 1
!
interface GigabitEthernet2/2/0
 no ip address
 negotiation auto
 service-policy output Port-channel_1_main_policy
 channel-group 1
!
interface Port-channel1.1
 encapsulation dot1Q 2 primary GigabitEthernet1/2/0 secondary GigabitEthernet2/2/0
 ip address 10.0.0.2 255.255.255.0
 service-policy output Port-channel_1_subscriber
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
モジュラ QoS コマンドライン インターフェイス	「Applying QoS Features Using the MQC」モジュール
比率を使用した余剰帯域幅配分	「比率を使用した余剰帯域幅配分」モジュール
クラスベースのシェーピング	「トラフィック シェーピングを使用したパケット フローの制御」モジュール

標準

規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	

MIB

MIB	MIB のリンク
CISCO-CLASS-BASED-QOS-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

QoS の機能情報：ポリシー集約

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*QoS* の機能情報：ポリシー集約

機能名	リリース	機能情報
QoS：ポリシー集約	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 次のコマンドが変更されました。**class(policy-map)**。

機能名	リリース	機能情報
QoS：メインインターフェイスでの複数キュー集約に対するポリシー集約 MQC サポート	Cisco IOS XE リリース 2.6	この機能は、EF、AF1、および AF4 のトラフィック クラスなどの DSCP ベースのクラスを含め、他のトラフィック クラスに対するプライマリ インターフェイスでのキューイング集約をサポートするように強化されました。この機能強化により、異なるサブインターフェイスからの他のトラフィック クラスがそのトラフィック クラスの共通キューを共有します。この他に、集約キューでのサブスクライバ単位のドロップ統計情報やバイトベースのキュー制限、WRED しきい値などが強化されています。 Cisco IOS XEリリース 2.6 では、CISCO-CLASS-BASED-QOS-MIB のサポートが追加されました。 新規コマンド、または変更されたコマンドは、次のとおりです。**account**、**showpolicy-mapinterface**。

第 6 章

レガシー QoS コマンドの廃止予定

これらの隠しコマンドによって提供される機能は、モジュラ QoS CLI（MQC）経由で提供される同様の機能に置き換えられています。MQC は、シスコ プラットフォームで QoS を設定するための、プラットフォームに依存しないコマンドです。これは、今すぐ、トラフィック クラスを定義して、それらのクラスを含むトラフィック ポリシーを作成し、それらのポリシーを必要なインターフェイスに適用することによって、QoS をプロビジョンする必要があることを意味します。このマニュアルでは、隠しコマンドとそれらの代替 MQC コマンドを一覧表示します。

- 機能情報の確認，83 ページ
- レガシー QoS コマンドの廃止予定に関する情報，84 ページ
- その他の参考資料，94 ページ
- レガシー QoS コマンドの廃止予定に関する機能情報，95 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

レガシー QoS コマンドの廃止予定に関する情報

MQC を使用して適用した QoS 機能

MQC 構造を使用すると、トラフィック クラス（クラス マップとも呼ぶ）を定義したり、トラフィック ポリシー（ポリシーマップとも呼ぶ）を作成したり、インターフェイスへトラフィック ポリシーを適用したりすることができます。これは、次の 3 つレベルのステップから構成されています。

1. class-mapコマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシーには、1 つのトラフィック クラスと、そのトラフィック クラスに適用する 1 つ以上の QoS 機能が含まれます。トラフィック ポリシー内の QoS 機能によって、分類されたトラフィックの処理方法が決まります。
3. **service-policy** コマンドを使用して、インターフェイスにトラフィック ポリシーを適用します。

ステップ 1 および 3 には、レガシー QoS の隠しコマンドが含まれていません。つまり、このドキュメントの対象範囲に入っていません。この 2 つのステップの詳細については、『*Quality of Service Solutions Configuration Guide*』の「Applying QoS Features Using the MQC」モジュールを参照してください。

隠しレガシー コマンド

次の表に、隠しコマンドまたは削除済みコマンドのリストを示します。また、代替コマンド（または一連のコマンド）も示します。

表 *10*：代替コマンドへの隠しコマンド、削除済みコマンド、またはサポート対象外のコマンドのマップ

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス
重み付けランダム早期検出または分散重み付けランダム早期検出のパラメータ グループの設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• random-detect-group
• random-detect（VC 単位）
（注） このコマンドは、Cisco IOS リリース 15.0(1)S ではサポートされていません。
コマンドの使用方法
`Router(config)# random-detect-group group-name [dscp-based|prec-based]`
`Router(config)# interface atm type number`
`Router(config-if)# pvc [name] vpi/vci`
`Router(config-if-atm-vc)# random-detect [attach group-name ]`
	コマンドの使用方法
	なし（この機能は存在しません）。

重み付けランダム早期検出の設定	

コマンド
• random-detect
• random-detect dscp
• random-detect（dscp-based キーワード）
• random-detect flow
• random-detect exponential-weighting-constant
• random-detect（prec-based キーワード）
• random-detect precedence
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# random-detect [number]`
`Router(config-if)# random-detect exponential-weighting-constant exponent`
`Router(config-if)# random-detect flow`
`Router(config-if)# random-detect precedence {precedence|rsvp} min-threshold max-threshold max-probability-denominator`
`Router(config-if)# random-detect prec-based`
`Router(config-if)# random-detect dscp-based`
`Router(config-if)# random-detect dscp dscp-value min-threshold max-threshold[max-probability-denominator]`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# random-detect dscp dscp-value min-threshold max-threshold[ mark-probability-denominator]`
	`Router(config-pmap-c)# random-detect clp clp-value min-threshold max-threshold[mark-probability-denominator]`
	`Router(config-pmap-c)# random-detect cos cos-value min-threshold max-threshold[mark-probability-denominator]`
	`Router(config-pmap-c)# random-detect discard-class discard-class-value min-threshold max-threshold[ mark-probability-denominator]`
	`Router(config-pmap-c)# random-detectprecedence ip-precedence min-threshold max-threshold[mark-probability-denominator]`
	`Router(config-pmap-c)# random-detect precedence-based`
	`Router(config-pmap-c)# random-detect ecn`
	`Router(config-pmap-c)# random-detect exponential-weighting-constant exponent`
	`Router(config-pmap-c)# random-detect cos-based`
	`Router(config-pmap-c)# random-detect dscp-based`

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• random-detect flow
• random-detect flow average-depth-factor
• random-detect flow count
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# random-detect [number]`
`Router(config-if)# random-detect flow`
`Router(config-if)# random-detect flow count number`
`Router(config-if)# random-detect flow average-depth-factor scaling-factor`
	コマンドの使用方法
	なし（この機能は存在しません）。

帯域幅割り当ての設定	

コマンド
• max-reserved-bandwidth
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# max-reserved-bandwidth percentage`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# bandwidth{`*bandwidth-in-kbps* `|remaining percent` *percentage* `| percent` *percentage*`}`

カスタム キューイングの設定	

コマンド
• custom-queue-list
（注） このコマンドは、Cisco IOS リリース 15.0(1)S ではサポートされていません。
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# custom-queue-list[list-number]`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# bandwidth{`*bandwidth-in-kbps* `|remaining percent` *percentage* `|percent` *percentage*`}`

プライオリティ キューイングの設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• ip rtp priority
• ip rtp reserve
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# ip rtp priority starting-port-number port-range bandwidth`
`Router(config)# interface type number`
`Router(config-if)# ip rtp reserve lowest-udp-port range-of-ports [maximum-bandwidth] 1000`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-name`
	`Router(config-pmap-c)# priority`

重み付け均等化キューイングの設定	

コマンド
• fair-queue (WFQ)
コマンドの使用方法（Cisco IOS リリース 15.0(1)S）
`Router(config)# interface type number`
`Router(config-if)# fair-queue`
コマンドの使用方法（Cisco IOS リリース 15.1(3)T）
`Router(config)# interfacetype number`
`Router(config-if)# fair-queue [congestive-` *discard-threshold* `[ dynamic-queue-count [`*reserved-queue-count*`]]]`
	コマンドの使用方法（Cisco IOS リリース 15.0(1)S）
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# fair-queue`
	コマンドの使用方法（Cisco IOS リリース 15.1(3)T）
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# fair-queue[dynamic-queues ]`

インターフェイスへのポリシー グループの割り当て	

コマンド
• priority-group
（注） このコマンドは、Cisco IOS リリース 15.0(1)S ではサポートされていません。
コマンドの使用方法
`Router(config)# interface type number`
`Router(config-if)# priority-group list-number`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# priority`
	`Router(config-pmap-c)# priority bandwidth-in-kbps [burst-in-bytes]`
	`Router(config-pmap-c)# priority percent percent [burst-in-bytes]`
	`Router(config-pmap-c)# priority level level`
	`Router(config-pmap-c)# priority level level [bandwidth-in-kbps [burst-in-bytes]]`
	`Router(config-pmap-c)# priority level level[percent percent [burst-in-bytes]]`

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス
切り替えられた PVC トラフィック シェーピング キューからの DE パケットを廃棄するためのしきい値の設定	

コマンド
• frame-relay congestion threshold de
 	
コマンドの使用方法
 	
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay congestion threshold de percentage`
	コマンドの使用方法
	
	`Router(config)# policy-map policy-map-name1`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# random-detect discard-class-based`
	`Router(config-pmap-c)# random-detect discard-class discard-class min-threshold max-threshold`
	`Router(config-pmap-c)# exit`
	`Router(config-pmap)# exit`
	`Router(config)# policy-map shape`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape average rate`
	`Router(config-pmap-c)# service-policy policy-map-name1`
	`Router(config-pmap-c)# exit`
	`Router(config-pmap)# exit`
	`Router(config)# policy-map policy-map-name2`
	`Router(config-pmap)# class class-name`
	`Router(config-pmap-c)# set discard-class discard-class`

仮想回線に対するフレーム リレー カスタム キューイングの設定	

コマンド
• frame-relay custom-queue-list
 	
コマンドの使用方法
 	
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay custom-queue-list list-number`
	コマンドの使用方法
	
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# bandwidth {bandwidth-in-kbps | remaining percent percentage | percent percentage}`

フレーム リレー ECN ビットしきい値の設定	

コマンド
• frame-relay congestion threshold ecn
 	
コマンドの使用方法
 	
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay congestion threshold ecn percentage`
	コマンドの使用方法
	なし（この機能は存在しません）。
	最も近いものは、（ECN に基づかない）MQC トラフィック シェーピングです。
	
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape average rate`

フレーム リレー重み付け均等化キューイングの設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• frame-relay fair-queue
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay fair-queue [discard-threshold [dynamic-queue-count[reserved-queue-count [buffer-limit]]]]`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# fair-queue`
	`Router(config-pmap-c)# fair-queue queue-limit packets`
	（注） **queue-limit***packets* キーワードと引数のペアは、Cisco IOS リリース 15.1(3)T ではサポートされていません。

PVC 上でのフレーム リレー プライオリティ キューイングの設定	

コマンド
• frame-relay ip rtp priority
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay ip rtp priority starting-port-number port-range bandwidth`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-name`
	`Router(config-pmap-c)# priority bandwidth-in-kbps [burst-in-bytes]`

マップ クラスに関連付けられた仮想回線へのプライオリティ キューの割り当て	

コマンド
• frame-relay priority-group
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay priority-group group-number`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# priority`
	`Router(config-pmap-c)# priority bandwidth-in-kbps [burst-in-bytes]`
	`Router(config-pmap-c)# priority percent percentage [burst-in-bytes]`
	`Router(config-pmap-c)# priority level level [percent percentage [burst-in-bytes]]`
	（注） **prioritylevel** コマンドは、Cisco IOS リリース 15.1(3)T ではサポートされていません。

BECN に対するフレーム リレー レート調整の設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• frame-relay adaptive-shaping（becn キーワード）
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay adaptive-shaping becn`
	コマンドの使用方法
	なし（この機能は存在しません）。最も近いものは、（BECN に基づかない）MQC トラフィック シェーピングです。
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape adaptive rate`

ForeSight メッセージに対するフレーム リレー レート調整の設定	

コマンド
• frame-relay adaptive-shaping（foresight キーワード）
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config)# frame-relay adaptive-shaping foresight`
	コマンドの使用方法
	なし（この機能は存在しません）。

BECN としてのフレーム リレー トラフィック シェーピング FECN のイネーブル化	

コマンド
• frame-relay fecn-adapt
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)#frame-relay fecn-adapt`
	コマンドの使用方法
	なし（この機能は存在しません）。最も近いものは、（FECN/BECN に基づかない）MQC トラフィック シェーピングです。
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape average rate`

フレーム リレー拡張ローカル管理インターフェイスの設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• frame-relay qos-autosense
（注） このコマンドは、Cisco IOS リリース 15.0(1)S では隠されていません。
コマンドの使用方法
`Router(config)# interface` *type number* `Router(config-if)#no ip address`
`Router(config-if)# encapsulation frame-relay`
`Router(config-if)# frame-relay lmi-typeansi`
`Router(config-if)# frame-relay traffic-shaping`
`Router(config-if)# frame-relay qos-autosense`
	コマンドの使用方法
	なし（この機能は存在しません）。

フレーム リレー最小認定情報レート（MINCIR）の設定	
コマンド • frame-relay mincir **コマンドの使用方法** `Router(config)# frame-relay mincir {in | out} bps`	**コマンドの使用方法** なし（この機能は存在しません）。
相手先固定接続（PVC）に対するフレーム リレー プライオリティの設定	

コマンド
• frame-relay interface-queue
コマンドの使用方法
`Router(config)# interface` *type number* `Router(config-if)#no ip address`
`Router(config-if)# frame-relay interface-queue priority 10 20 30 40`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# priority`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# priority`

フレーム リレー トラフィック シェーピングの設定	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス

コマンド
• frame-relay bc
• frame-relay be
• frame-relay cir
（注） Cisco IOS リリース 15.1(3)T では、これらのコマンドは隠されていませんが、（PVC ではなく）SVC に対してのみ有効です。
コマンドの使用方法
`Router(config)# map-class frame-relay map-class-name`
`Router(config-map-class)# frame-relay bc {in | out} committed-burst-size-in-bits`
`Router(config-map-class)# frame-relay be {in | out} excess-burst-size-in-bits`
`Router(config-map-class)# frame-relay cir {in | out} bits-per-second`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape average` *rate*

VC でのフレーム リレー トラフィック シェーピングの設定	

コマンド
• frame-relay traffic-rate
コマンドの使用方法
`Router(config)# map-class frame-relay`map-class-name
`Router(config-map-class)# traffic-rate average [peak]`
	コマンドの使用方法
	`Router(config)# policy-map policy-map-name`
	`Router(config-pmap)# class class-default`
	`Router(config-pmap-c)# shape average` *rate*
	`Router(config-pmap-c)# service-policy output traffic-rate` service-policy output traffic-rate

インターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。	
コマンド • show queue **コマンドの使用方法** `Router# show queue interface`	**コマンドの使用方法** `Router# show policy-map interface`
キューイング戦略の表示	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス
コマンド • show queueing **コマンドの使用方法** `Router# show queueing`	**コマンドの使用方法** `Router# show policy-map interface`
重み付けランダム早期検出（WRED）情報の表示	
コマンド • show interfaces random-detect **コマンドの使用方法** `Router# show interfaces [type number] random-detect`	**コマンドの使用方法** `Router# show policy-map interface`
WRED パラメータ グループの表示	
コマンド • show random-detect-group **コマンドの使用方法** `Router# show random-detect-group`	**コマンドの使用方法** `Router# show policy-map interface`
トラフィック シェーピングの設定、キューイング、および統計情報の表示	

コマンド
• show traffic-shape
• show traffic-shape queue
• show traffic-shape statistics
コマンドの使用方法
`Router# show traffic-shape [interface-type interface-number]`
`Router# show traffic-shape queue [interface-number [dlci dlci-number]]`
`Router# show traffic-shape statistics [interface-type interface-number]`
	コマンドの使用方法
	`Router# show policy-map interface`

重み付け均等化キューイング情報の表示	

隠しコマンド、削除済みのコマンド、またはサポート対象外のコマンド	代替 MQC コマンド シーケンス
コマンド • show interfaces fair-queue コマンドの使用方法 `Router# show interfaces [interface-type interface-number] fair-queue`	コマンドの使用方法 `Router# show policy-map interface`

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
トラフィック クラスの定義、インターフェイスへのトラフィック ポリシーの対応付け	『*QualityofServiceSolutionsConfigurationGuide*』の「Applying QoS Features Using the MQC」モジュール
QoS コマンドに関する参照ページ	『*Cisco IOS Quality of Service Solutions Command Reference*』
ワイドエリア ネットワーク コマンドに関する参照ページ	『*Cisco IOS Wide-Area Networking Command Reference*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

レガシー QoS コマンドの廃止予定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：レガシー *QoS* コマンドの廃止予定に関する機能情報

機能名	リリース	機能情報
レガシー QoS コマンドの廃止予定：隠しコマンド	15.0(1)S 15.1(3)T	

機能名	リリース	機能情報
		Cisco IOS QoS を効率化するため、特定のコマンドを隠しコマンドにしました。つまり、コマンドラインに疑問符（**?**）を入力して隠しコマンドを表示しようとしても、そのコマンドは表示されません。ただし、コマンド シンタックスをわかっていれば、入力できます。これらのコマンドは将来のリリースで削除される予定です。 これらの隠しコマンドによって提供される機能は、モジュラ QoS CLI（MQC）からの、QoS を設定するための、プラットフォームに依存しない一連のコマンドである同様の機能に置き換えられています。 次のコマンドが変更されました。**custom-queue-list**, **fair-queue(WFQ)**、**frame-relayadaptive-shaping**（**becn** キーワード）、**frame-relayadaptive-shaping**（**foresight** キーワード）、**frame-relaybc**、**frame-relaybe**、**frame-relaycir**、**frame-relaycongestionthresholdde**、**frame-relaycongestionthresholdecn**、**frame-relaycustom-queue-list**、**frame-relayfair-queue**、**frame-relayfecn-adapt**、**frame-relayiprtppriority**、**frame-relaypriority-group**、**frame-relayqos-autosense**、**iprtppriority**、**max-reserved-bandwidth**、**priority-group**、**random-detect**、**random-detectdscp**、**random-detect**（**dscp-based** キーワード）、

機能名	リリース	機能情報
		random-detectexponential-weighting-constant、**random-detectflow**、**random-detectflowaverage-depth-factor**、**random-detectflowcount**、**random-detect**（**prec-based** キーワード）、**random-detectprecedence**、**random-detect-group**、**showinterfacesfair-queue**、**showinterfacesrandom-detect**、**showqueue**、**showqueueing**、**showrandom-detect-group**、**showtraffic-shape**、**showtraffic-shapequeue**、**showtraffic-shapestatistics**。

機能名	リリース	機能情報
レガシー QoS コマンドの廃止予定：隠しコマンド	Cisco IOS XE リリース 2.6	

機能名	リリース	機能情報
		Cisco IOS XE QoS を効率化するため、特定のコマンドを隠しコマンドにしました。つまり、コマンド ラインに疑問符（**?**）を入力して隠しコマンドを表示しようとしても、そのコマンドは表示されません。ただし、コマンド シンタックスをわかっていれば、入力できます。これらのコマンドは将来のリリースで削除される予定です。 これらの隠しコマンドによって提供される機能は、モジュラ QoS CLI（MQC）からの、QoS を設定するための、プラットフォームに依存しない一連のコマンドである同様の機能に置き換えられています。 次のコマンドが変更されました。**custom-queue-list**、**fair-queue(WFQ)**、**frame-relayadaptive-shaping**（**becn** キーワード）、**frame-relayadaptive-shaping**（**foresight** キーワード）、**frame-relaybc**、**frame-relaybe**、**frame-relaycir**、**frame-relaycongestionthresholdde**、**frame-relaycongestionthresholdecn**、**frame-relaycustom-queue-list**、**frame-relayfair-queue**、**frame-relayfecn-adapt**、**frame-relayiprtppriority**、**frame-relaypriority-group**、**frame-relayqos-autosense**、**iprtppriority**、**max-reserved-bandwidth**、**showinterfacesfair-queue**、**showinterfacesrandom-detect**、**showqueue**、**showqueueing**、**showtraffic-shape**、**showtraffic-shapequeue**、

機能名	リリース	機能情報
		showtraffic-shapestatistics。
レガシー QoS コマンドの廃止予定：削除済みコマンド	Cisco IOS XE リリース 3.2S	レガシー QoS コマンドは削除されました。そのため、適切な代替 MQC コマンドを使用する必要があります。 次のコマンドが削除されました。**custom-queue-list**、**fair-queue(WFQ)**、**frame-relayadaptive-shaping**（**becn** キーワード）、**frame-relayadaptive-shaping**（**foresight** キーワード）、**frame-relaybc**、**frame-relaybe**、**frame-relaycir**、**frame-relaycongestionthresholdde**、**frame-relaycongestionthresholdecn**、**frame-relaycustom-queue-list**、**frame-relayfair-queue**、**frame-relayfecn-adapt**、**frame-relayiprtppriority**、**frame-relaypriority-group**、**frame-relayqos-autosense**、**iprtppriority**、**max-reserved-bandwidth**、**showinterfacesfair-queue**、**showinterfacesrandom-detect**、**showqueue**、**showqueueing**、**showtraffic-shape**、**showtraffic-shapequeue**、**showtraffic-shapestatistics**。

第 7 章

QoS パケット マーキング

QoS パケット マーキングとは、レイヤ 2 またはレイヤ 3 のいずれかでのパケット内のフィールドの次の変更のことです。

1. レイヤ 2：802.1Q/p CoS、MPLS EXP
2. レイヤ 3：IP プレシデンス、DSCP および/または IP ECN

また、到達した分類上の決定の保持と各ネットワーク QoS の決定ポイントでの詳細な分類の除去のこともマーキングと呼びます。

- QoS パケット分類について，103 ページ
- QoS パケット マーキングの設定例，109 ページ
- QoS パケット マーキングの確認，112 ページ
- ネットワーク レベルの設定例，117 ページ
- コマンド リファレンス，126 ページ

QoS パケット分類について

マーキングの定義

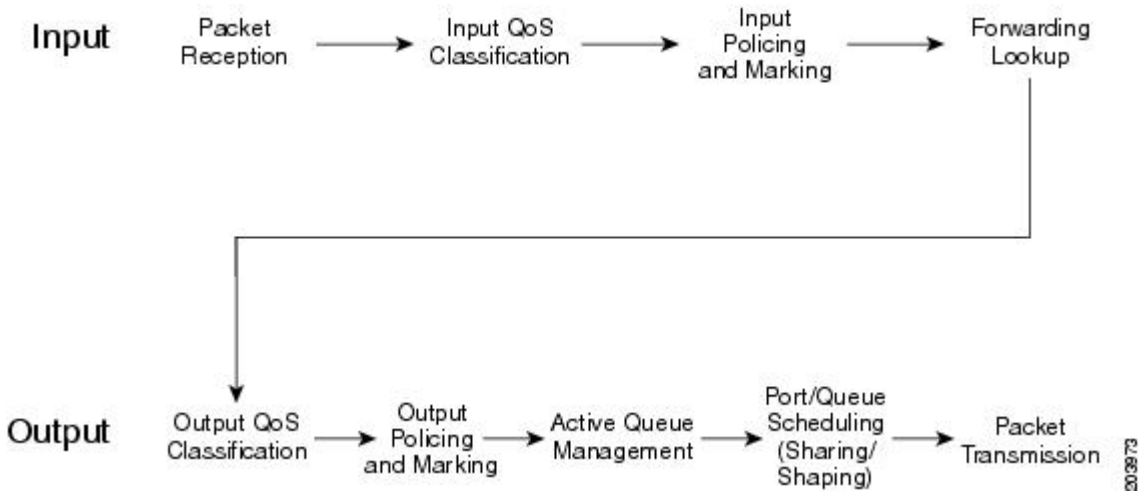
マーキングは航空券のファースト、ビジネス、エコノミーといった「サービス クラス」の定義と概念上は似ています。この値は、得られるサービスのレベル（品質）を反映します。同様に、パケットの値をマークして、ネットワークを通過するそのパケットのサービス クラス（以降、サービスクラスと呼びます）を示します。マークされた値から、ネットワーク要素は、パケットの処理方法を決めることができます。

ビジネスクラスの乗客はその指定を得るために、さまざまな手段を使用したかもしれません。余分に料金を支払ったり、マイルを使用したり、または、幸運なことに他の座席が一杯であったために通常の料金で予約できたのかもしれません。どこかで誰かが特定のサービスクラスの利用資

格を決定する複雑な分類タスクを実行し、その後でファーストクラス、ビジネスクラス、またはエコノミークラスの指定のみをチケットにマークしています。フライトアテンダントは、利用資格がどのように決定されたかについては関心がありません。チケットにマークされたクラスを見て、そのレベルのサービスを提供するだけです。

これがネットワーキングの世界で行われます。あるデバイスがフロー内のデータで複雑な分類を実行し、そのフローに適切なサービス クラスを決定します。他のネットワーク要素は、受信するパケット内にマークされた値を「信頼」して、その指定に適したサービスを提供します。

図 *4*：*QoS* パケット処理



QoS パケット処理というコンテキストでは、分類の後でキューイングの前にマーキングが実行されます。マーキングは入力と出力で実行できます。

通常は、信頼境界をネットワークのエッジで作成した後に、エッジデバイスのパケットを分類してマークします。その後で、ネットワーク全体にわたってマークしたそのフィールドをホップ単位の処理についての分類と決定に使用することができます。

（注） 信頼境界を使用すると、パケットがネットワークに着信したときにそれらすべてのパケットにネットワーク制御のマーキングを適用し、適用しなかったデフォルト以外のマーキングを削除したり、変更したりすることができます。

たとえば、VoIPデバイスが接続されているルータポートをシステムが認識しているとします。音声パケットのDiffServ コードポイント（DSCP）値を（ネットワークのエッジで）EF とマークし、（残りの）ネットワークを通じて DSCP ベースの分類を使用して、低遅延処理を保証するパケットを決定します。

パケットをマーキングする理由

パケットをマーキングする理由は次のとおりです。

- ネットワークを通過する際にパケットをどのように処理するかを指定する。
- 複雑な分類を一度実行する。サービスクラスをマーキングすることによって、よりシンプルで、CPU への負荷が低い分類をネットワーク内の他の場所で使用できます。
- フローの可視性が高いネットワークのポイントで分類を実行する。たとえば、データが暗号化されている場合は、そのフロー内で伝送されるアプリケーションを決定するなどの複雑な分類は実行できません。代わりに、暗号化前に分類して、パス上のネットワーク要素に表示される非暗号化ヘッダーの値をマークすることができます。

  パケットは異なる自律エンティティ（2 つの企業オフィス間のサービス プロバイダー ネットワークなど）が管理するネットワークを通過するため、それらのネットワーク上ではサービスレベルの指定に対するマーキングが整合しない場合は再度マーキングを行う必要があります。

  パケットは異なるネットワーキングテクノロジーを通過するため、サービスクラスを示すために使用可能なフィールドが異なる場合があります。たとえば、IP パケットの DSCP フィールドでサービス クラスの指定を伝送していても、このパケットがマルチプロトコル ラベル スイッチング（MPLS）ネットワークを通過する場合は、ネットワーク要素がサービスクラスの判断に使用できるのは MPLS EXP フィールドのみの場合があります。ネットワークのその部分では、MPLS EXP ビットの適切なマーキングを判断する必要があります。

  ネットワーク オペレータとして、ユーザから特定のレートでデータを受け取るように契約している場合があります。そのレートを超えたパケットをドロップするのではなく、低いサービスクラスとしてマークできます。

マーキング パケットに対するアプローチ

マーキング パケットに対する主要なアプローチは次の 2 つです。

（注） ここでは、「ポリシング」アクションについて簡単に説明します。詳細については、「ポリシング」の章を参照してください。

1. **set** コマンド
2. ポリサー マーキング アクション

set コマンド

ルータ上でのマーキング パケットに対する最もシンプルなアプローチは、**set** コマンドを *policy-map* 定義に使用することです（ポリシーマップで、定義した各クラスのトラフィックに対して QoS アクションを指定します）。

すべての RTP ポートを 1 つのトラフィック クラスに分類し、各パケットに AF41 とマークするように決定できます。ポリシーマップは、次のようになります。

```
policy-map mark-rtp
  class rtp-traffic
```

```
    set dscp af41
```

ポリサー マーキング アクション

ポリサーを使用して、トラフィック クラス内の定義したレートを超えるパケットをドロップすることができます。または、そのレートを超えるパケットをマークし、そのレート未満のパケットでなく、それらのパケットが異なるホップ単位の処理を受けられるようにすることができます。

たとえば、AF41 でマークされたビデオ トラフィックがルータに着信したとします。最大 2 Mbps までのユーザ トラフィックを考慮することを決定する可能性もあります最上位の相対的優先転送動作と見なし、2 Mbps を超えるトラフィックを AF42 に降格してコントラクト外（または不適合）と見なす必要があると判断することができます。

ポリシーマップは次に類似するものになります。

```
class-map video-traffic
  match dscp af41
!
policy-map enforce-contract
  class video-traffic
    police cir 2m conform-action transmit exceed-action set-dscp-transmit AF42
```

policeを参照してください。

マーキング アクションの範囲

分類と同様に、マーキングはデータ パケット内のすべてのフィールドにはアクセスできません。たとえば、IP パケットがマルチプロトコル ラベル スイッチング（MPLS）でカプセル化されている場合は、IP ヘッダー内の DSCP をマークできません。MPLS から最初にカプセル化を解除する必要があります。ただし、MPLS EXP ビットはマークできます。

（注） マーキングに使用できるのは、レイヤ 2 のヘッダーと外部レイヤ 3 のヘッダーのみです。

複数の set ステートメント

複数のマーキングルールを 1 つのクラス（またはポリサー アクション）内に設定できます。これにより、同じパケット内のレイヤ2とレイヤ3の両方のフィールドをマークすることができます。または、複数のトラフィック タイプが同じクラス内に存在する場合は、各タイプにマーキング値を定義します。

たとえば、イーサネット サブインターフェイスに適用された次の出力ポリシーがあるとします。

```
policy-map mark-rtp
  class rtp-traffic
    set cos 4
    set mpls exp topmost 4
    set dscp af41
```

MPLS パケットがこのサブインターフェイス経由で転送されると、レイヤ 2 の COS フィールドと MPLS ヘッダー内の EXP ビットがマークされます。IP データグラムがそのパケットにカプセル化されていた場合、その DSCP 値は変更されずにそのまま残ります。ただし、IP パケットがサブイ

ンターフェイス経由で転送された場合は、そのレイヤ 2 の COS 値とレイヤ 3 の DSCP 値がマークされます。

コマンドの詳細については、set cos, （128 ページ）、set mpls experimental topmost, （134 ページ）、およびset dscp, （130 ページ）を参照してください。

内部指定子のマーキング

シスコ ルータでは、2 つの内部値（qos-group と discard-class）をマークできます。これらの値はルータ内をパケットとともに移動しますが、パケットのコンテンツは変更しません。

通常、入力ポリシー内のこれらの指定子をマークし、それらを使用して、出力ポリシーのトラフィック クラスや WRED ドロップ プロファイルを分類します。たとえば、ユーザの IP アドレスに基づいて出力を分類したくても、暗号化が設定されているために出力インターフェイスでユーザの IP アドレスがわからない場合があります。それらのトラフィックを（暗号化前に）入力で分類して、適切な qos-group 値を設定することができます。これで、qos-group に基づいて出力で分類できるようになり、それに応じた出力アクションを選択できるようになりました。

入力マーキング アクションと出力マーキング アクション

特定のマーキング値は、入力ポリシーのみか、または出力ポリシーのみに関連しています。たとえば、入力ポリシーで ATM CLP ビットまたはフレーム リレー DE ビットをマークしてもパケットのカプセル化解除時に破棄されるため、無意味です。

同様に、出力ポリシーで qos-group または discard-class をマーキングしても、 これらはパケットを変更せずにそのままにされ、次のホップへの転送時にパケットをエンキューした時点で廃棄されるため、効果がありません。

インポジション マーキング

特殊な状況下では、パケットにまだ追加されていないヘッダー フィールドをマークすることができます。この動作をインポジション マーキングと呼びます。

最も一般的なインポジション マーキングの例は **set mpls experimental imposition** の適用です。これは、IP データグラムを含み、マルチプロトコル ラベル スイッチング（MPLS）ヘッダーがないパケットが到着する入力インターフェイスで使用できます。ルータが MPLS ヘッダーを使用してデータグラムをカプセル化する場合、このコマンドによって指定されたとおりに、EXP ビットがマークされます。

set dscp tunnel コマンドと **set precedence tunnel** コマンド（IPv4 の場合のみ）の適用は、もう 1 つのインポジションマーキングの例です。出力ポリシーをトンネルインターフェイスに適用した場合、そのポリシーが実行されるときにはトンネル ヘッダーは存在しません。つまり、どのようなマーキングでも元の（最終的には内側の）IP ヘッダーに適用されます。どちらのコマンドを使用しても、トンネル（外側の）IP ヘッダーにはマークし、元のヘッダーは変更せずにそのまま残すことができます。

次の表に、これらのコマンドがサポートされている場合のトンネルのタイプとさまざまなカプセル化を示します。

表 *12*：サポートされる *DSCP* とプレシデンス トンネル マーキングの設定

名前	外部ヘッダー（カプセル化）	内部ヘッダー（ペイロード）	注
GRE (4 over 4)	IPv4/GRE	IPv4	サポートあり
GRE (6 over 4)	IPv4/GRE	IPv6	カプセル化はサポート対象外
GREv6 (4 over 6)	IPv6/GRE	IPv4	カプセル化はサポート対象外
GREv6 (6 over 6)	IPv6/GRE	IPv6	カプセル化はサポート対象外
IP-IP	IPv4	IPv4	サポートあり
IPv6-IP	IPv4	IPv6	サポートあり
IPv6 (4 over 6)	IPv6	IPv4	カプセル化はサポート対象外
IPv6 (6 over 6)	IPv6	IPv6	サポート対象外
PSEC (4 over 4)	IPv4/IPSEC	IPv4	サポート対象外
PSEC (6 over 4)	IPv4/IPSEC	IPv6	サポート対象外
IPSECv6 (4 over 6)	IPv6/IPSEC	IPv4	カプセル化はサポート対象外
IPSECv6 (6 over 6)	IPv6/IPSEC	IPv6	サポート対象外
mVPN（マルチキャスト VPN）	IPv4/GRE	IPv4	サポートあり
DMVPN（ダイナミック マルチポイント VPN）			サポートあり
マルチポイント GRE			サポートあり
MPLSoGREv4	IPv4/GRE	MPLS	サポート対象外
MPLSoGREv6	IPv6/GRE	MPLS	サポート対象外
L2TP	IPv4/L2TP	PPPoX	サポート対象外

デフォルトのインポジション/ディスポジション マーキングの動作

新しいヘッダー（encapsulated など）を追加すると、内部ヘッダー内の QoS マーキングが外部ヘッダーにコピーされます。たとえば、IP データグラムは MPLS ヘッダーでカプセル化される場合、デフォルトでは、新たにインポーズされたヘッダー内の MPLS EXP ビットに IP プレシデンス ビットがIP ヘッダーからコピーされます。

ヘッダー ディスポジションの関するルールとして、外部のマーキングを内部ヘッダーにはコピーしません。たとえば、外部および内部の IP ヘッダーに異なる DSCP 値を持つパケットを GRE トンネルのエンドポイントで受信しているとします。外部ヘッダーを削除した場合は内部ヘッダーに DSCP 値をコピーしません。

インポジション マーキングの設定例については、例 4：トンネル インポジション マーキングの設定，（110 ページ）と例 5：トンネル インポジション マーキングを使用した SP ネットワークに対する再マーキング，（125 ページ）を参照してください。

コマンドの詳細については、set mpls experimental imposition，（133 ページ）、set dscp tunnel，（131 ページ）、およびset precedence tunnel，（136 ページ）を参照してください。

QoS パケット マーキングの設定例

例 1：入力マーキングの設定

一部のトラフィックにサービスクラスを指定し、その他すべてのトラフィック（`class class-default`）をブリーチする（`set dscp 0`）ためにマーキングを使用する場合、ネットワークのエッジに信頼境界を設定できます。信頼境界をネットワークに対してすべての入力で適用すると、ネットワーク内の各サービスクラスにマップするアプリケーションの制御を維持できます。

```
policy-map ingress-marking
  class voice
    set dscp ef
  class video
    set dscp af41
  class scavenger
    set dscp cs1
  class class-default
    set dscp 0
!
interface gigabitethernet1/0/0
  Service-policy in ingress-marking
```

コマンドの詳細については、set dscp，（130 ページ）を参照してください。

例 2：出力マーキングの設定

別の管理者がネットワーク パスの一部を制御しており、サービスクラス マッピングに別の DSCP を使用している場合、出力マーキングが必要です（たとえば、エンタープライズ内で、RFC4594 で説明されているとおりに12の異なるクラスのトラフィックを分類します）。ただし、サービス プロバイダーが提供しているのは 3 クラス モデルのみです。

また、レイヤ 2 の特定のクラス（イーサネット、フレームリレー、または ATM スイッチド ネットワークなど）に対する処理を示すために出力マーキングが必要です。

```
policy-map egress-marking
  class scavenger
    set atm-clp
```

コマンドの詳細については、set atm-clp,（127 ページ）を参照してください。

例 3：MPLS EXP インポジションの設定

MPLS では、プロバイダー エッジ（PE）ルータが MPLS ヘッダーを使用してデータグラムやフレームをカプセル化します。コア内でのスイッチングの決定は MPLS ヘッダーに基づいており、カプセル化されたデータは把握していません。

MPLS ヘッダーで IPv4 データグラムがカプセル化されているレイヤ 3 MPLS ネットワークについて検討します。カスタマー エッジ（CE）側のインターフェイスでは、パケットの IPv4 ヘッダーを「把握」しています。コア側のインターフェイスでは、MPLS ヘッダーを使用してデータグラムをカプセル化しているため、それらのヘッダー以外のことはわかりません。

デフォルトでは、MPLS EXP ビットに IP プレシデンスをコピーします。この動作を上書きすることにします。コア側のインターフェイス上では、IPv4 タイプのサービス バイトは解析できません。しかし、入力時に IP ヘッダーを解析して EXP 値を格納できます（`set mpls experimental imposition 5`）。MPLS ヘッダーが追加されたときにこの値を設定するようにします。コマンド実行時には MPLS ヘッダーは存在しないため、ルータは命令を取得して、出力インターフェイスで EXP ビットをマークします。

```
policy-map mpls-exp-remark
  class voice
    set mpls experimental imposition 5
  class video
    set mpls experimental imposition 4
  class scavenger
    set mpls experimental imposition 0
!
interface gigabitethernet1/0/0
  policy-map input mpls-exp-remark
```

コマンドの詳細については、set mpls experimental imposition,（133 ページ）を参照してください。

例 4：トンネル インポジション マーキングの設定

トンネルと MPLS EXP インポジション マーキングは概念的に似ています。パケットにまだ追加されていないヘッダー内の値をマークできます。また、GRE や IPinIP のようなレイヤ 3 トンネル テクノロジーでは、外部 IP ヘッダーを使用してレイヤ 3 データグラムをカプセル化できます。

DMVPN ネットワークがあり、そのネットワークではブランチ ロケーションでデータを暗号化し、そのデータを GRE ヘッダーでカプセル化してからパブリック IP ネットワークに送信しているとします。管理者は、ポリシーマップをトンネル インターフェイスに適用してそのトンネル内のアプリケーションの優先順位付けを行うことができます。また、外部 IP ヘッダーの DSCP をマークしてプロバイダーのネットワーク内でのサービスクラスを示す必要もあります。ポリシーが実行される時点では、外部ヘッダーはまだ追加されておらず、`set dscp` や `set precedence` のようなコマンドが内部 IP ヘッダーをマークします。

この問題を解決するには、`set dscp tunnel` コマンドと `set precedence tunnel` コマンドを使用します。これらのコマンドでは、まだ追加されていない外部ヘッダーに値を設定できます。

次に、音声とビデオのトラフィックが分類されてエンタープライズネットワーク内の個別のキューに投入される例を示します。サービス プロバイダーには僅かなサービスクラスしかないため、音声とビデオの両方をプロバイダーのネットワーク内のプライオリティ クラスに投入することにしました。

外部トンネル ヘッダーの DSCP をマーキングすることにより（`set dscp tunnel ef`）、内部ヘッダーの元のマーキングを維持することができます。

```
policy-map mark-outer-gre-header
  class voice
    priority level1 percent 20
    set dscp tunnel ef
  class video
    priority level 2 percent 20
    set dscp tunnel ef
!
interface tunnel100
  service-policy out mark-outer-gre-header
```

コマンドの詳細については、set dscp tunnel,（131 ページ）を参照してください。

例 5：QoS グループ マーキングの設定

状況によっては、出力キューイングを入力分類に基づかせることができます。たとえば、MPLS 対応のインターフェイスに 9 つ以上の出力キューを必要としているとします。出力分類を使用して MPLS EXP ビットを制限するため、クラスは 8 つになります。

解決策として、入力インターフェイスで分類を実行し、その分類に一致するパケットに QoS グループを設定します。QoS グループには、現在のルータ内以外は関連性がありません。つまり、パケット ヘッダー内にあるものを変更しません。代わりに、これは、ルータを通過する際にパケットに関連付けられた値です。

次の例では、Network-Based Application Recognition（NBAR）分類を使用します入力で使用し、TelePresence ビデオと Jabber ビデオの両方を qos-group 4 でマークします。出力ポリシーでは、入力でマークした qos-group に基づいて分類します。

```
class-map telepresence-video
  match protocol telepresence-media
class-map jabber-video
  match protocol cisco-jabber-video
class-map egress-video-traffic
  match qos-group 4
!
policy-map mark-qos-group
  class telepresence-video
    set qos-group 4
  class jabber-video
    set qos-group 4
!
policy-map egress-queuing
  class egress-video-traffic
    bandwidth remaining percent 50
!
interface gig 1/0/0
  service-policy in mark-qos-group
!
interface serial1/1/0
  service-policy out egress-queuing
```

コマンドの詳細については、set qos-group,（136 ページ）を参照してください。

例 6：discard-class マーキングの設定

例 5：QoS グループ マーキングの設定,（111 ページ）では、TelePresence ビデオと Jabber ビデオの両方を qos-group 4 でマークし、これらの両方のアプリケーションを同じ出力キューに配置しています。

この出力キューで、重み付けランダム早期検出（WRED）を実行し、輻輳時には最初に Jabber ビデオをドロップするとします。通常、WRED はプレシデンス値または DSCP 値を確認してフローのドロップしきい値を決定しますが、例 3：MPLS EXP インポジションの設定,（110 ページ）で説明したように、IP ヘッダーは把握できません。これを解決するため、discard-class という 2 つめの内部値をマークします。これを行うと、qos-group を使用して出力クラス（およびキュー）を選択し、discard-class を使用してそのクラス内の WRED ドロップ プロファイルを選択します。

```
class-map telepresence-video
  match protocol telepresence-media
class-map jabber-video
  match protocol cisco-jabber-video
class-map egress-video-traffic
  match qos-group 4
!
policy-map mark-qos-group
  class telepresence-video
    set qos-group 4
    set discard-class 1
  class jabber-video
    set qos-group 4
    set discard-class 2
!
policy-map egress-queuing
  class egress-video-traffic
    bandwidth remaining percent 50
    random-detect discard-class-based
    random-detect discard-class 1 24 40
    random-detect discard-class 2 22 30
!
interface gig 1/0/0
  service-policy in mark-qos-group
!
interface serial1/1/0
  service-policy out egress-queuing
```

コマンドの詳細については、set discard-class,（129 ページ）を参照してください。

QoS パケット マーキングの確認

show policy-map interface コマンドは、IOS XE プラットフォーム上での QoS の動作を確認する主要手段です。パケット転送パス（つまり、データプレーン）は IOS インスタンス（コントロールプレーン）から分離されていますが、この一般的な IOS コマンドによって統計情報が報告されます。この機能はデフォルトでイネーブルになっています。

次の表に、以降の項で説明するフィールドを示します。

表 *13* : ***show policy-map interface*** フィールドの説明（マーキングの確認に有効）

フィールド	説明
Service-policy input	指定されたインターフェイスまたは VC に適用されている入力サービスポリシーの名前を示します。
Class-map	表示するトラフィックのクラスを指定します。ポリシーに設定されている各クラスに対して出力が表示されます。クラス一致の実装の選択（match-all または match-any）もトラフィッククラスの横に表示できます。
packets、bytes	表示するトラフィックの属していると識別されたパケットの数を指定します（バイト単位で表示）。
offered rate	クラスに着信するパケットのレートを 1 秒あたりのビット数で指定します。
Match	トラフィック クラスの一致基準を指定します。使用可能な各種の一致条件の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Classifying Network Traffic」モジュールを参照してください。
QoS Set	特定のクラスに対して設定された QoS マーキング アクションの詳細。
Packets marked	イネーブルにした場合は、特定のクラスにマークされたパケットの合計数を表示します。 イネーブルにしなかった場合は、「Marker statistics: Disabled」が表示されます。

show policy-map interface コマンドでの確認

show policy-map interface コマンドは、IOS XE プラットフォーム上での QoS の動作を確認する主要手段です。通常、特定のクラスに一致するパケット（デフォルトでイネーブルになる「クラス一致統計情報）の数と、設定されているマーキング アクション（設定されている場合）を認識することで、そのアクションによってマークされたパケット数を十分に把握できます。

（注） 「クラス一致統計情報」（デフォルトでイネーブル）と「マーキング統計情報」（デフォルトではディセーブル）の違いを明確に理解する必要があります。通常は、クラス一致統計情報を理解しておくだけで十分です。パケットがクラスに「ヒット」すると、マークされたと想定できます。ただし、複数の相互に排他的なマーキング値を設定し、**set** コマンドごとにマークされたパッケージの数を知る必要がある場合、あらゆる注意を払って「マーキング統計情報」をイネーブルにすることができます。

次に、物理インターフェイスに適用するポリシーがある入力マーキングの例を示します。この例では、jabber-video をポート 2000 ～ 3000 上に設定するとします。

```
class-map match-all jabber-video
  match ip rtp 2000 3000
!
policy-map mark-traffic
  class jabber-video
    set dscp af41
!

router# show policy-map int g1/0/0
GigabitEthernet1/0/0

  Service-policy input: mark-traffic

    Class-map: jabber-video (match-all)
      850 packets, 51000 bytes                                  note 1
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: ip rtp 2000 3000
      QoS Set                                                   note 2
        dscp af41
          Marker statistics: Disabled

    Class-map: class-default (match-any)                        note 3
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

脚注：

note 1	クラス一致の統計情報
note 2	パケット一致セクション
note 3	クラスデフォルトの統計情報セクション

「Marker statistics: Disabled」に注意してください。複数の統計情報を呼び出す場合、つまり以前の出力で提供された情報で十分でなかった場合に、「パケット マーカー統計情報」をイネーブルにすることができます（カラー対応モードを参照してください）。

QoS パケット マーキング統計情報での確認

はじめる前に

QoS パケット マーキング統計情報をイネーブルにする前に、次のいずれかを実行します。

- すべてのポリシー マップを削除し、コマンドを発行し、すべてのポリシー マップを再適用します。
- コマンドを発行し、設定を保存し、ルータをリロードします。

（注） QoS のパケット マーキング統計情報をイネーブルにすると拡張された設定では CPU 使用率が増加する可能性があります。統計情報を表示する利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

QoS パケット マーキング統計情報のイネーブル化

パケット マーキング統計情報をイネーブルにするには、**platformqosmarker-statistics** を使用しますコンフィギュレーション モードで使用します。

QoS パケット マーキング統計情報の表示

指定したインターフェイス（またはサブインターフェイス）、あるいはインターフェイスの特定の相手先固定接続（PVC）のいずれかで、すべてのサービス ポリシーに対して設定されたすべてのクラスのパケット統計情報を表示するには、**showpolicy-mapinterface** コマンドを使用します。ポリシーマップに単独で「マーキング」を設定した場合、ASR 1000 ルータからの出力は次のようになります。

```
policy-map remark-af41
  class af41-traffic
    set dscp tunnel ef
```

ここで、ユーザの IP ヘッダー内に AF41 があるトラフィックに GRE IP ヘッダーで EF とマークされた DiffServ コード ポイント（DSCP）があるトンネル インターフェイスにこのマップを配置した場合、**showpolicy-mapinterface** の出力は次のようになります。

```
show policy-map interface tunnel1

  Service-policy output: remark-af41

    Class-map: af41-traffic (match-all)
      978 packets, 68460 bytes                                  note 1
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match:  dscp af41 (34)
      QoS Set                                                   note 2
        dscp tunnel ef
          Marker statistics: Disabled                           note 3

    Class-map: class-default (match-any)
      365 packets, 25550 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

脚注：

note 1	クラス一致統計情報を表示します（「確認された」パケットはすべて AF41 とマークされると想定しています）。
note 2	マーキングは設定された唯一のアクションです。
note 3	デフォルトでは、セット単位のアクション統計情報はディセーブルになっています。

ここで、マーキング統計情報をイネーブルにした場合、**showpolicy-mapinterface** コマンドの出力は次のようになります。

```
show policy-map interface tunnel1

  Service-policy output: remark-af41

    Class-map: af41-traffic (match-all)
      575 packets, 40250 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match:  dscp af41 (34)
      QoS Set
        dscp tunnel ef
          Packets marked 575                    note

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

脚注

note	マーキング統計情報はありますが、この例では情報が冗長です。

set dscp tunnel コマンドの詳細については、set dscp tunnel, （131 ページ）を参照してください。

データ プレーン設定の検証

データプレーン設定に IOS コントロールプレーン設定が反映されているかを確認するには、**show platform hardware qfp active feature qos interface [input|output]** コマンドを使用します。このコマンドは、ポリシーマップをインターフェイスに適用する前に発行した場合にのみ有効です。したがって、次のいずれかを実行する必要があります。

- すべてのポリシーマップを削除し、コマンドを発行し、すべてのポリシーマップを再適用する。
- コマンドを発行し、設定を保存し、ルータをリロードする。

次の出力では、データプレーンにアクションを設定し、値を設定していることに注意してください。

```
router# show platform hardware qfp active feature qos interface g1/0/0 input
Interface: GigabitEthernet1/0/0, QFP interface: 12
  Direction: Input
    Hierarchy level: 0
    Policy name: mark-traffic
      Class name: jabber-video, Policy name: mark-traffic
        QOS Set:
            dscp 34                    note
      Class name: class-default, Policy name: mark-traffic
```

脚注

note	データプレーンはマーキングするようにプログラムされます。

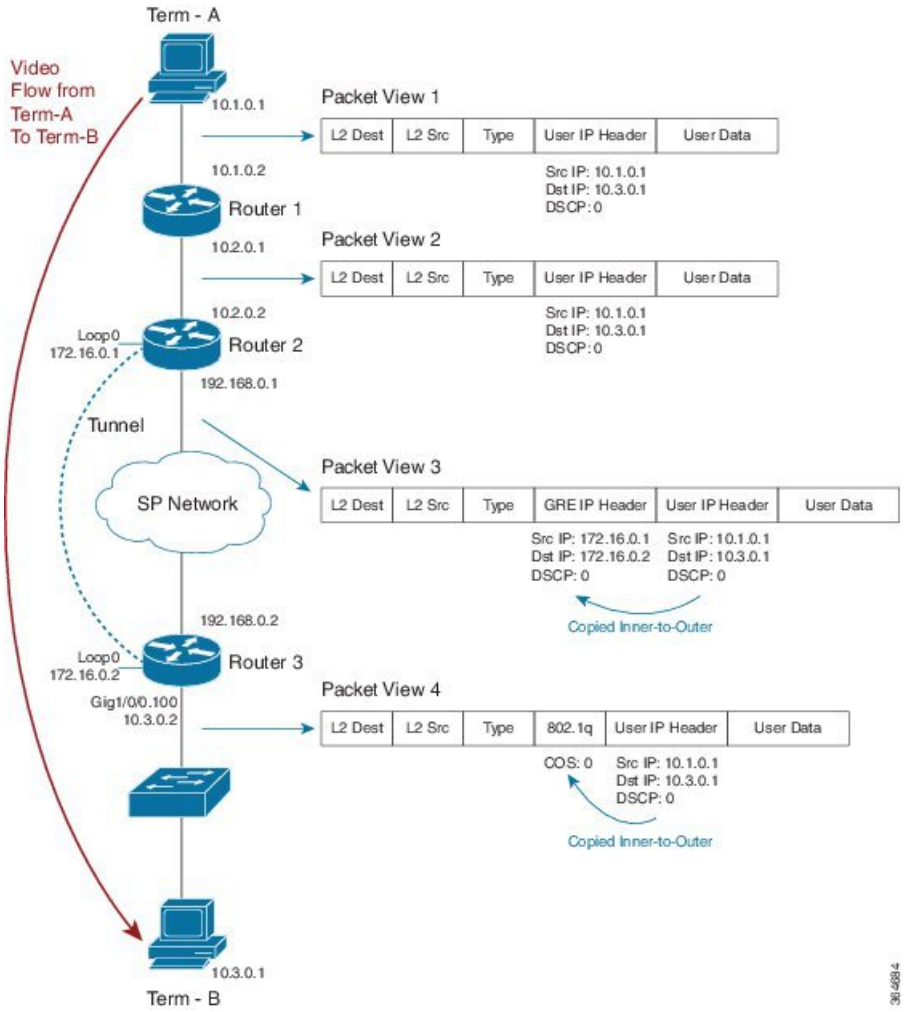
ネットワーク レベルの設定例

インポジション マーキングの概要については、インポジション マーキング，（107 ページ）を参照してください。

次のシナリオでは、端末 A から端末 B にビデオ フローが移動します。

例 1：ネットワーク全体にわたるサービス クラス情報の伝達

図 *5*：ネットワーク全体にわたるサービス クラス情報の伝達

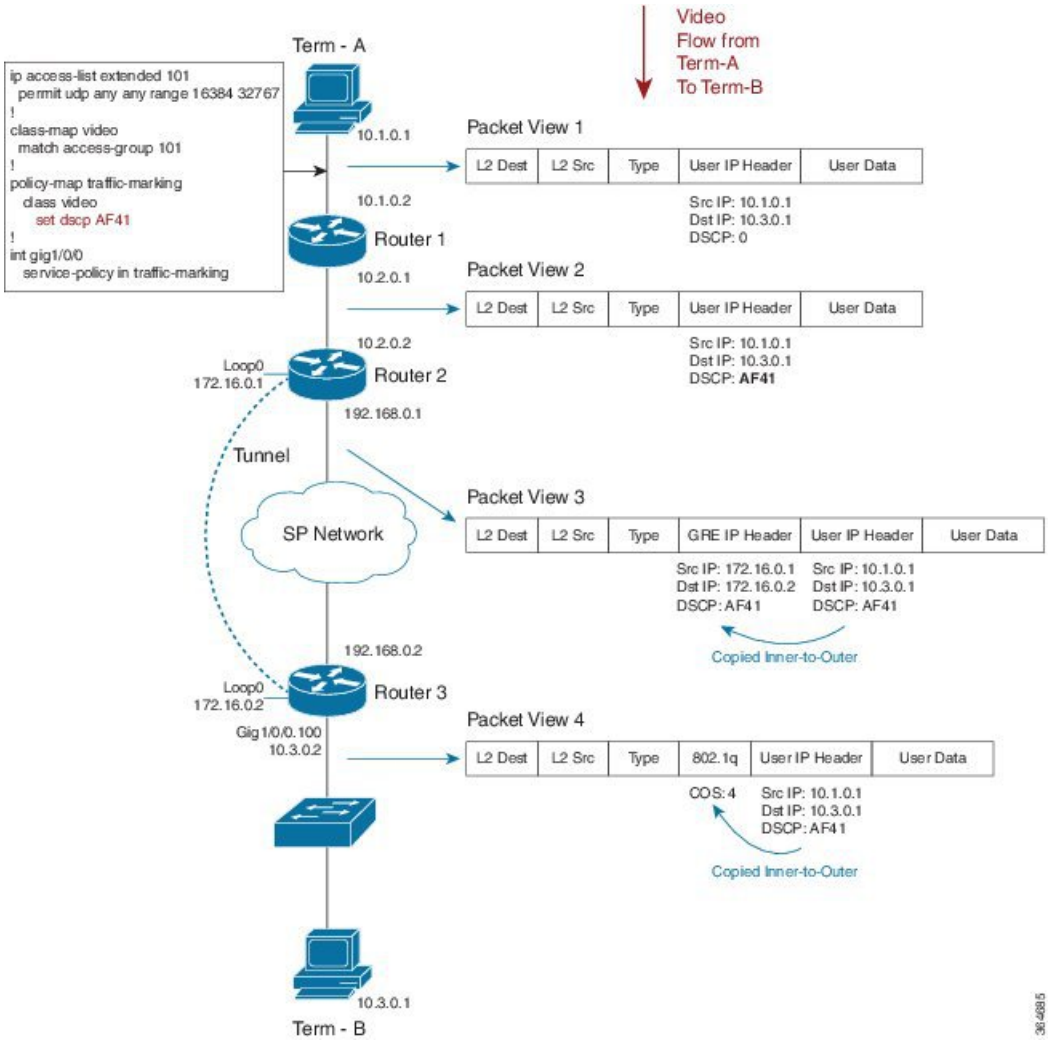


あるアプリケーションが DSCP コードポイント 0 を使用してビデオ ストリームをマークしていると想定します（パケット ビュー 1 を参照）。プロバイダーのネットワークを通過するために、GRE トンネルを通じて（可能な場合は暗号化して）ストリームを送信します。パケット ビュー 3 には、ユーザの IP データグラムを GRE パケット内にカプセル化していることが示されています。DSCP コードポイントがデフォルトでインポーズされた GRE ヘッダーにどのようにコピーされるかに注目してください。

最終の宛先の最後のホップで、ルータ 3 が VLAN のタグ付きパケットをスイッチに送信します（パケット ビュー 4 を参照）。VLAN の設定により、GRE ヘッダーが削除され、Dot1Q ヘッダーが追加されたことを確認してください。ユーザの DSCP 0（000 000）の先行部分が VLAN ヘッダーの COS ビットにデフォルトでコピーされます。CoS 値セットは 0（000）です。

例 2：ネットワークのエッジでのマーキングによるサービス クラスの指定

図 *6*：ネットワークのエッジでのマーキングによるサービス クラスの指定



この例では、入力ポリシーのユーザのトラフィックのDSCPを再度マーキングすることによって、デフォルト動作を変更します。次に、これを実行するコードを示します。

```
ip access-list extended 101
 permit udp any any range 16384 32767
!
class-map video
 match access-group 101
!
policy-map traffic-marking
  class video
    set dscp AF41
!
```

```
int gig1/0/0
  service-policy in traffic-marking
```

ルータ 1 に入るときに入力ポリシーでユーザのトラフィックの DSCP を再度マーキングすることでデフォルト動作を変更します。

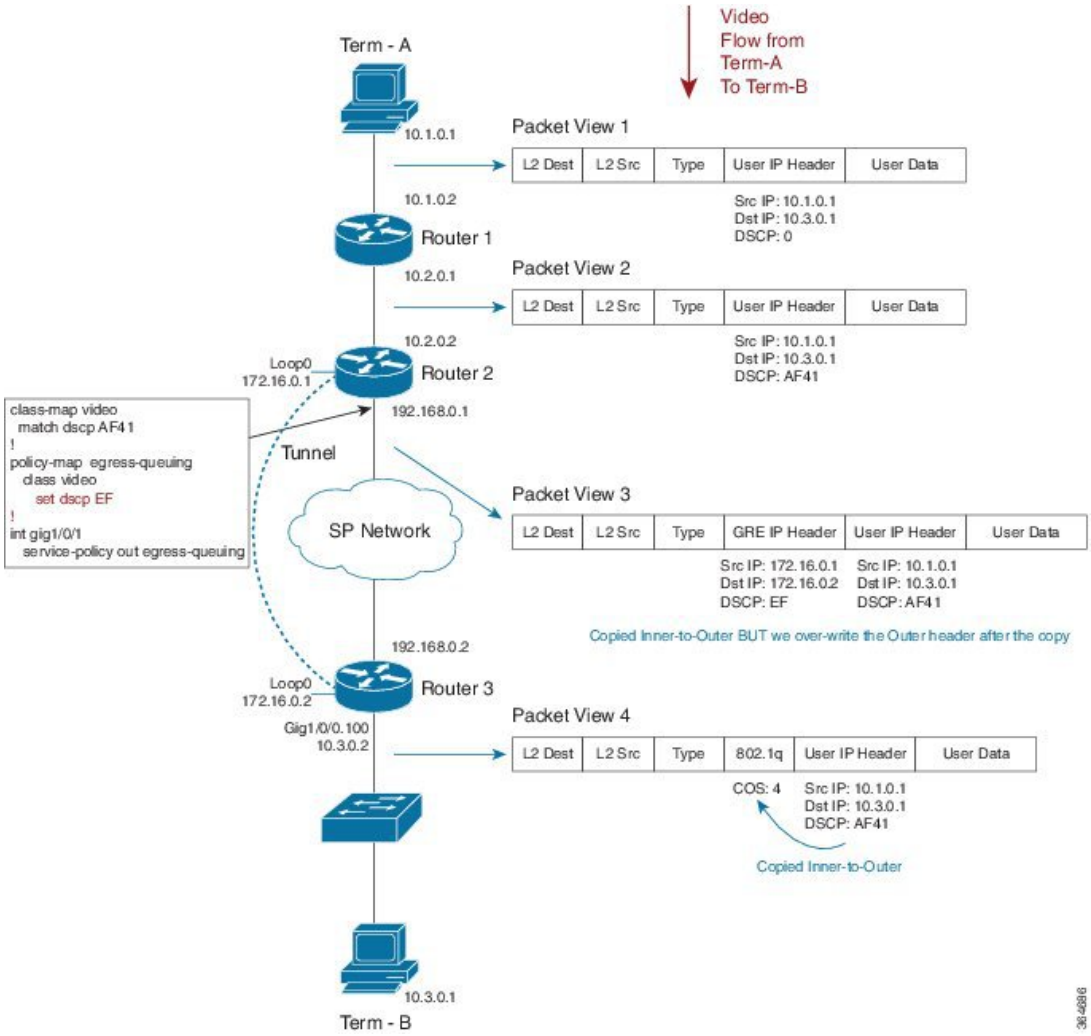
ビデオ トラフィックをネットワーク全体を通じて DSCP AF41 と指定するものとします。パケットが出力時に GRE インターフェイスに到達したとき、その DSCP 値はすでに AF41 に変更されており、動作は例 1 と同じです。プロバイダー ネットワークを通過する際に、ストリームが GRE トンネルを通じて（可能な場合は暗号化されて）送信されます。新しくマークされた DSCP コードポイント（AF41）がインポーズされた GRE ヘッダーにデフォルトでコピーされることに注目してください。

宛先に到着すると、ルータが VLAN のタグ付きパケットを最後のホップ（スイッチ）に送信します。ユーザの DSCP 値の先行部分が、VLAN ヘッダーの COS ビットにデフォルトでコピーされます。DSCP が FA41（100 010）になっているため、COS 値は 4（100）になります。

setdscp コマンドの詳細については、set dscp,（130 ページ）を参照してください。

例 3：サービス プロバイダーの要件に一致させるためのトラフィックの再マーキング

図 7：サービス プロバイダーの要件に一致させるためのトラフィックの再マーキング



ここでは、ネットワーク内で DSCP 値をマークしますが、サービス プロバイダーは別のマーキングを想定している例を示します。次に、これに対処するコードを示します。

```
class-map video
 match dscp AF41
!
policy-map  egress-queuing
  class video
    set dscp EF
!
int gig1/0/1
  service-policy out egress-queuing
```

ネットワーク内のビデオに対して DSCP を AF41 とマークします。一方、サービス プロバイダーはビデオ パケットが EF とマークされると想定しています。ルータ 2 の出力 Gig インターフェイスで、キューイング コマンドを含んだポリシーを追加します（この例では、設定のマーキング部分のみに重点を置いていることを思い出してください）。

パケットが出力物理インターフェイスに到達した時点で、GRE ヘッダーがすでにインポーズされているため、内部のカプセル化されたデータグラムから DSCP 値の AF 41 をコピーします。物理インターフェイスのポリシーは、外部 GRE ヘッダー内の DSCP 値のみを変更します。

（注） 内部ユーザ データグラムの IP ヘッダーがどのように変更されないままかに注目してください。

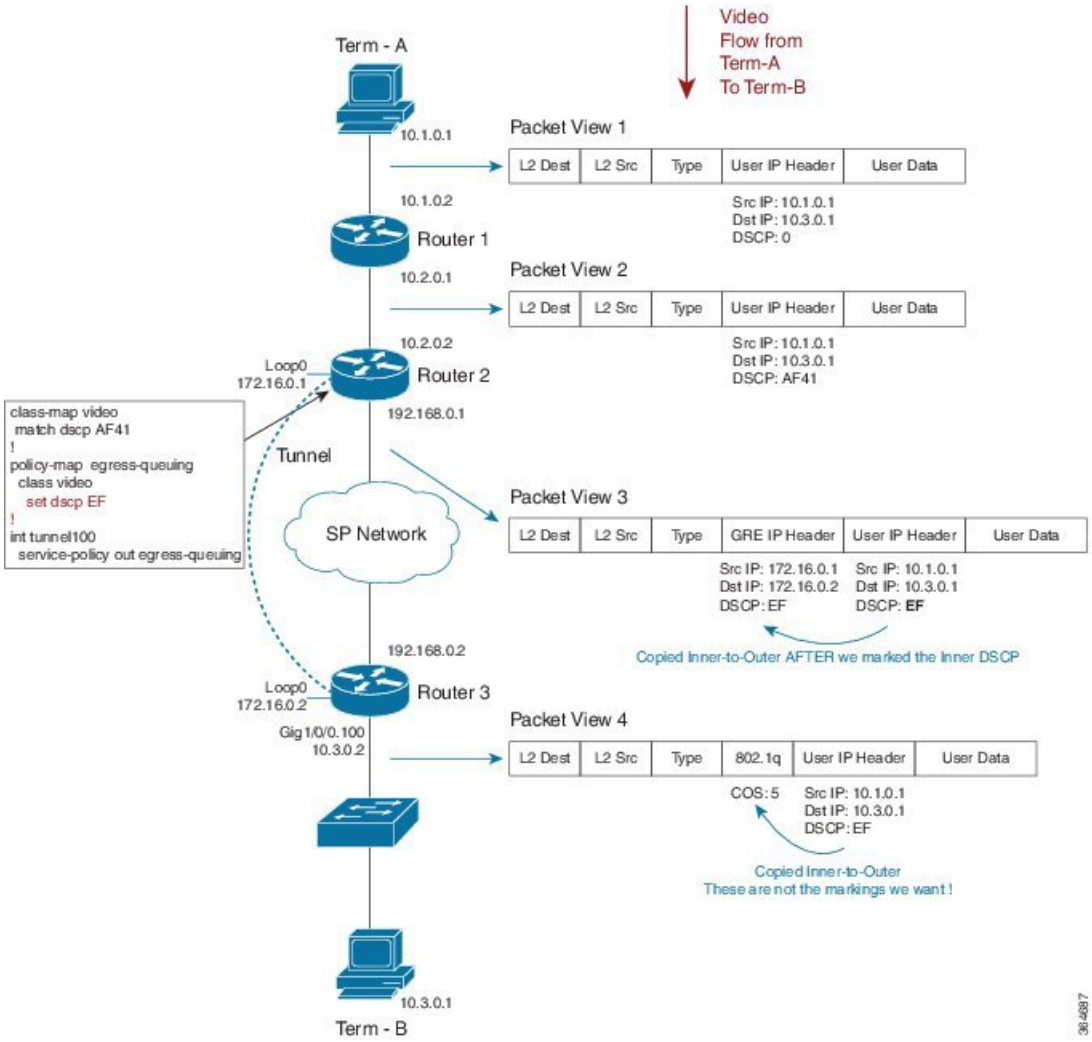
ルータ 3 に到達してトンネルが終了すると、トンネル GRE ヘッダーが削除されます。その後、ユーザ データグラム の IP ヘッダーのみが表示されますが、ネットワークへの入力時にマークした値である AF41 が維持されています。

前述のように、ルータが VLAN のタグ付きパケットを最後のホップ（スイッチ）に送信します。デフォルトでは、ユーザ IP ヘッダーの DSCP 値の先行部分が VLAN ヘッダー（802.1q）の CoS ビットにコピーされます。この時点で、DSCP 値は AF41（100 010）であるため、COS 値は 4（100）になります。

setdscp コマンドの詳細については、set dscp,（130 ページ）を参照してください。

例 4：SP ネットワークに対するトンネル インターフェイスでの再マーキング　Gotcha の可能性

図 *8*：*SP* ネットワークに対するトンネル インターフェイスでの再マーキング　*Gotcha* の可能性



この例では、物理インターフェイスではなく、ルータ 1 のトンネル インターフェイスに QoS ポリシーを配置します（トンネルごとにキューイングを設定することで、物理インターフェイス上の集約ポリシーよりも多くの利点が得られます）。次に、これを実行するコードを示します。

```
class-map video
 match dscp AF41
!
policy-map  egress-queuing
  class video
    set dscp EF
!
int tunnel100
```

```
service-policy out egress-queuing
```

ポリシーのマーキング部分にのみ重きを置いています。トンネル インターフェイスでのマーキングは、トンネル ヘッダーが追加される前に実行されることが重要なポイントです。

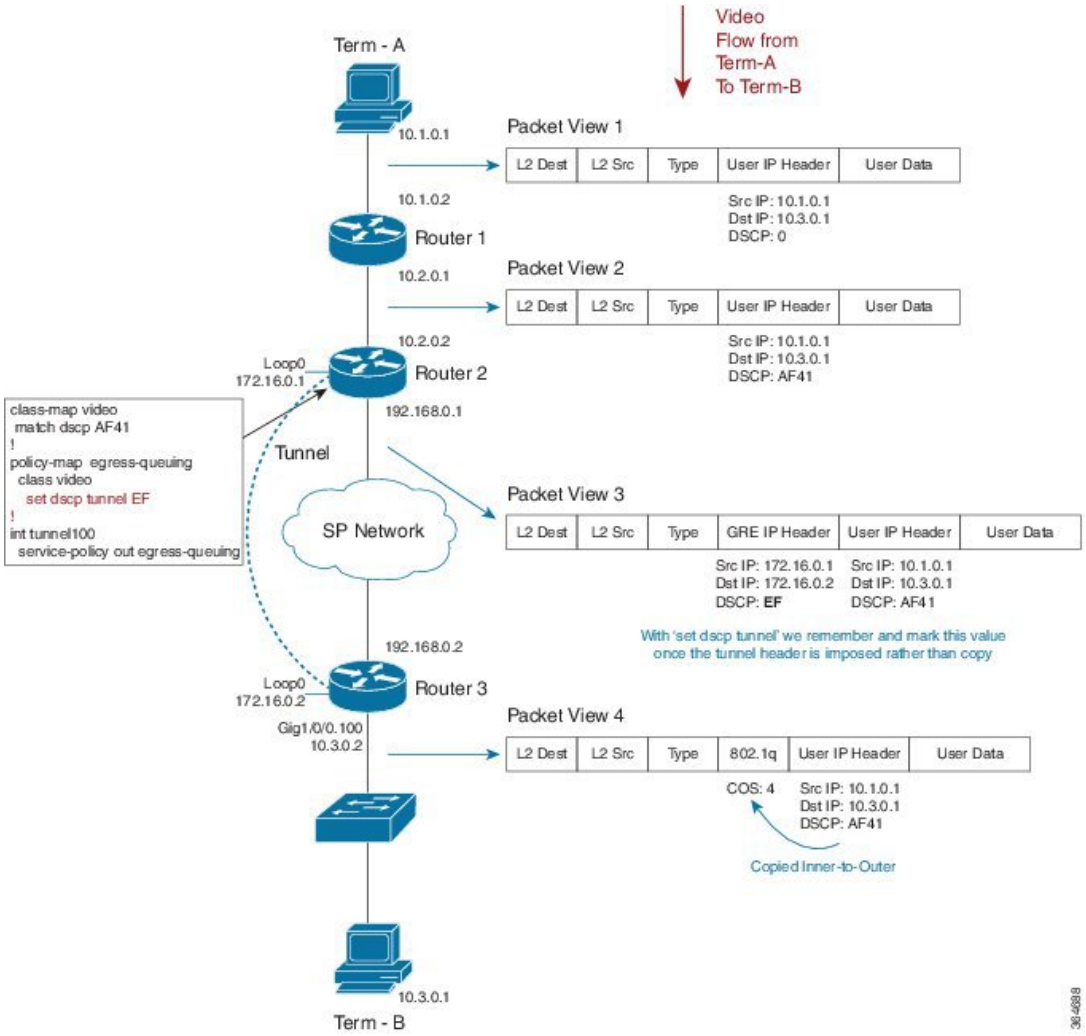
ユーザ データグラムの IP ヘッダーでどのようにポリシーが DSCP を上書きするかに注目してください。これは、GRE カプセル化の前に行われるため、新たにマークされた値が外部ヘッダーにコピーされます。

ルータ 3 に到達し、トンネルを終了すると、トンネル GRE ヘッダーが削除されます。ユーザ データグラム ヘッダーをマークしたため、新しい値が残りのネットワークを通じて伝達されます。これは、意図した動作ではありません。

setdscp コマンドの詳細については、set dscp,（130 ページ）を参照してください。

例 5：トンネル インポジション マーキングを使用した SP ネットワークに対する再マーキング

図 *9*：トンネル インポジション マーキングを使用した *SP* ネットワークに対する再マーキング



この例では、**set dscp tunnel***dscp-value* を使用して、トンネル IP ヘッダーのみを変更します。

```
class-map video
 match dscp AF41
!
policy-map  egress-queuing
  class video
    set dscp tunnel EF
!
int tunnel100
  service-policy out egress-queuing
```

QoS ポリシーはルータ 2 のトンネル インターフェイスにあります。この例では、**set dscp** *value* ではなく、**set dscp tunnel** *value* を使用します。

GRE ヘッダーはまだインポーズされていません。**set dscp tunnel** *value* コマンドによって、DSCP 値が記憶され、カプセル化時に「内部から外部へ」コピーする代わりにこの値が使用されます。ユーザ IP データグラム ヘッダーの DSCP 値が変更されないことに注目してください。**set dscp tunnel***value* コマンドはトンネル IP ヘッダーのみを変更します。

set dscp tunnel*value* コマンドの詳細については、set dscp tunnel,（131 ページ）を参照してください。

コマンド リファレンス

platform qos marker-statistics

ルータに設定されたすべてのポリシーの各マーキング アクションに対して個別の統計情報の収集をイネーブルにするには、**platform qos marker-statistics** コマンドを グローバル コンフィギュレーションモードで使用します。パケットマーキング統計情報をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] platform qos marker-statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Disabled（つまり、パケット マーキングの統計情報は表示されません）。ネットワーク オペレータは、クラス一致統計情報に依存します。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、インターフェイスに対してポリシーマップが適用される前に発行された場合にのみ実行されます。したがって、次のいずれかを実行する必要があります。

- すべてのポリシーマップを削除し、コマンドを発行し、すべてのポリシーマップを再適用する。
- コマンドを発行し、設定を保存し、ルータをリロードする。

（注） パケット マーキング統計情報をイネーブルにすると、拡張設定では CPU 使用率が増加する可能性があります。そのため、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

set atm-clp

ATM セル損失率優先度（CLP）ビットを設定するには、**set atm-clp** コマンドを使用しますポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set atm-clp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ATM CLP ビットは設定されません。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

ATMインターフェイスでは、アウトバウンドポリシー内に **set atm-clp** コマンドを使用して、ATM セル ヘッダーを 1 に設定することができます。

このコマンドは、ATM、PPPoA、PPPoEoA、および L2TPv3 のカプセル化に対してサポートされています。ポリシーが VC に直接ではなく、トンネルに適用されている場合は、サポートされません。

セル損失優先度（CLP）ビット QoS が設定された ATM を含むポリシー マップは PPP over X（PPPoX）セッションに適用できません。マップは、**set atm-clp** コマンドを指定していない場合にのみ、受け入れられます。

set atm-clp コマンドを使用して出力マーキングを設定する例については、例 2：出力マーキングの設定，（109 ページ）を参照してください。

set cos

発信パケットのレイヤ 2 サービス クラス（CoS）値を設定するには、**set cos** コマンドを使用しますポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set cos *cos-value*

構文の説明

cos-value	発信パケットの IEEE 802.1Q CoS 値を 0 ～ 7 の範囲で指定します。

コマンド デフォルト

IP precedence ビットまたは MPLS EXP ビットのいずれかがカプセル化されたデータグラムからコピーされます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

set cos コマンドを使用して、サービスクラス情報を レイヤ 2 スイッチド ネットワークに伝達します。レイヤ 2 スイッチは組み込まれたレイヤ 3 情報（DSCP など）を解析できない場合がありますが、CoS 値に基づいて差別化サービスを提供することがあります。スイッチは、CoS 値のマークを含めて、レイヤ 2 ヘッダー情報を利用できます。

スイッチについてここで話題にしていますか???

従来、**set cos** コマンドは、受信したフレームからレイヤ 2 情報をルータが廃棄するため、インターフェイスの出力方向に適用されたサービス ポリシー内でのみ意味を持ちます。EoMPLS や EVC のような機能の導入により、入力での CoS の設定では、ルーティングされたネットワーク全体を通じてレイヤ 2 情報を維持できます。

Michael：「**set cos-inner**」コマンド ページの最後の文でも気づいたのですが、以前は出力のみでした。現在は入力と出力になっていますが、理にかなっていますか？

set cos-inner

QinQ パケットの内部 VLAN タグ内にレイヤ 2 CoS 値を設定するには、**set cos-inner** コマンドを使用しますポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set cos-inner *cos-value*

構文の説明

cos-value	IEEE 802.1q CoS 値を 0 ～ 7 の範囲で指定します。

コマンド デフォルト

IP precedence ビットまたは MPLS EXP ビットのいずれかがカプセル化されたデータグラムからコピーされます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

従来、ルータは受信したフレームからレイヤ 2 情報を破棄するため、**set cos-inner** コマンドはインターフェイスの出力方向に適用されたサービス ポリシー内でのみ意味がありました。EoMPLS や EVC のような機能の導入により、入力での CoS の設定は、ルーティングされたネットワーク全体を通じてレイヤ 2 情報を維持するため重要です。

set discard-class

パケットに対して QoS 廃棄クラスを設定するには、**set discard-class** コマンドを ポリシーマップ コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set discard-class *discard-class-value*

構文の説明

discard-class-value	廃棄クラス値を 0 ～ 7 の範囲で指定します。

コマンド デフォルト

パケットに関連付けられた廃棄クラス値は 0 に設定されます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

set discard-class コマンドでは、ルータによる処理中に廃棄クラス値をパケットに関連付けることができます。この値を設定すると、パケットは変更されません。

廃棄クラスと廃棄クラスベースのWREDを出力ポリシー内に使用して、輻輳時にドロップするパケットを制御できます。

set dscp

IP ヘッダーに DSCP 値を設定するには、**set dscp** コマンドを ポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set dscp *dscp-value*

構文の説明

dscp-value	IP ヘッダー内の DSCP 値を 0 ～ 63 の範囲で設定します。この値は数字か、または既知の DiffServe名（つまり、EF）を使用して指定できます。

コマンド デフォルト

受信したパケットの既存の DSCP 値を保持します。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、入力ポリシーまたは出力ポリシーに使用されることがあります。

パケットがネットワークを通過する際にパケットに対する QoS の処理を示すために DSCP 値を使用することができます。

（注） DSCPを使用した差別化サービスアーキテクチャはプレシデンスの使用よりも優先されます。

このコマンドは、一番外側のレイヤ3ヘッダーがIPv4かIPv6のいずれかの場合にパケットをマークします。

出力ポリシーマップ内で発行した場合、このコマンドはクラスやキューの選択は変更しませんが、WRED ドロップ プロファイルの選択に影響することがあります。

setdscp コマンドと **set ip dscp** コマンドは同じように動作し、IPv4 パケットと IPv6 パケットの両方をマークします。

（注） **match ip dscp** コマンドは IPv4 パケットのみを分類するのに対し、**match dscp** コマンドは IPv4 パケットと IPv6 パケットの両方を分類する分類プロセスとは異なります。

set dscp tunnel

パケットにまだ追加されていないトンネル ヘッダー内に DSCP 値を設定するには、**set dscp tunnel** コマンドをポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set dscp tunnel *dscp-value*

構文の説明

dscp-value	トンネル ヘッダー内の DSCP 値を 0 ～ 63 の範囲で指定します。この値は数字か、または既知の DiffServe 名（つまり、EF）のいずれかを使用して指定できます。

コマンド デフォルト

カプセル化されたデータグラムからの DSCP 値が新たにインポーズされたトンネル ヘッダーにコピーされます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、トンネル ヘッダーの追加前でないと意味がありません。

（注） トンネル インターフェイスに適用された入力ポリシーまたは出力ポリシーのいずれかにこのコマンドを使用できます。ただし、出力ポリシーが適用されている場合、ポリシーの評価時にすべてのヘッダーが追加されるため、このコマンドは意味がありません。

Cisco ASR 1000 ルータでは、**setdscptunnel** コマンドは IPv4 に対してのみサポートされています。サポートされている DSCP トンネルのマーキング設定をリストした表については、インポジション マーキング, （107 ページ）を参照してください。

このコマンドを使用し、レイヤ 3 データグラムを外部 IP ヘッダーでカプセル化する例については、例 4：トンネル インポジション マーキングの設定, （110 ページ）を参照してください。

set fr-de

frame-relay（FR）discard eligible（DE）ビットを設定するには、**set fr-de** コマンドを ポリシーマップ クラス コンフィギュレーション モードで使用します。設定をディセーブルにするには、コマンドの **no** 形式を入力します。

[no] set fr-de

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

データグラムがフレーム リレーでカプセル化されていると、DE ビットは設定されません。

使用上のガイドライン

フレーム リレー カプセル化を使用して設定されたシリアル インターフェイスでは、**set fr-de** コマンドをアウトバウンド ポリシーに使用して、フレーム リレー ヘッダーの廃棄適性ビットを 1 に設定することができます。

set ip dscp

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip dscp** と **set dscp** をサポートしています。いずれかを使用して、IP ヘッダー内の DSCP 値をマークできます。詳細については、**set dscp** コマンド ページ（set dscp, （130 ページ））を参照してください。

set ip dscp tunnel

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip dscp tunnel** と **set dscp tunnel** がサポートされています。詳細については、**set dscp tunnel** コマンド ページ（set dscp tunnel, （131 ページ））を参照してください。

set ip precedence

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip precedence** と **set precedence** をサポートしています。いずれかを使用して、IP ヘッダー内のプレシデンス値をマークできます。詳細については、**set precedence** コマンド ページ（set precedence, （135 ページ））を参照してください。

set ip precedence tunnel

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip precedence tunnel** と **set precedence tunnel** がサポートされています。詳細については、**set precedence tunnel** コマンド ページ（set precedence tunnel, （136 ページ））を参照してください。

set mpls experimental imposition

インポーズされたすべてのラベル エントリの MPLS EXP フィールドの値を設定するには、**set mpls experimental imposition** コマンドをポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set mpls experimental imposition *mpls-exp-value*

構文の説明

mpls-exp-value	MPLS EXP 値を 0 ～ 7 の範囲で指定します。

コマンド デフォルト

MPLS 値は、カプセル化されたパケット内の該当するフィールド（通常は precedence）からコピーされます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

set mpls experimental imposition コマンドは、入力インターフェイス上でのみサポートされます。ラベルインポジション時にこのコマンドを使用し、インポーズされたすべてのラベルエントリの MPLS EXP フィールドを設定します。

このコマンドを使用して、データグラムまたはフレームをカプセル化するために使用する MPLS ヘッダー内の EXP ビットを設定する例については、例 3：MPLS EXP インポジションの設定，（110 ページ）を参照してください。

set mpls experimental topmost

最上位ラベルの MPLS EXP フィールド値を設定するには、**set mpls experimental topmost** コマンドを使用します ポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no]set mpls experimental topmost *mpls-exp-value*

構文の説明

mpls-exp-value	MPLS EXP 値を 0 ～ 7 の範囲で指定します。

コマンド デフォルト

MPLS EXP 値は、カプセル化時に最も内側のヘッダーからコピーされるか、または変更されないままになります。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、コマンドの評価時に最も外側のレイヤ 3 ヘッダーが MPLS ラベルである場合にパケットをマークします。

このコマンドは、最上位ラベル内の MPLS EXP 値のみを設定します。スタック内に複数のラベルが存在する場合、最上位以外のラベル内の MPLS EXP は変更されないままになります。

set precedence

パケット ヘッダー内の IP プレシデンス値を設定するには、**set precedence** コマンドを ポリシー マップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set precedence *precedence-value*

構文の説明

precedence-value	パケット ヘッダーに precedence ビットを 0 ~ 7 の範囲で指定します。

コマンド デフォルト

受信したパケットのプレシデンス値を保持します。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、入力ポリシーまたは出力ポリシーに使用されることがあります。ただし、出力ポリシーマップ内でこのコマンドを発行した場合、このコマンドはクラスやキューの選択は変更しませんが、WRED ドロップ プロファイルの選択に影響することがあります。

プレシデンス値を設定することによって、パケットがネットワークを通過する際にパケットに対する QoS 処理を示します。

（注） DSCP を使用した差別化サービス アーキテクチャはプレシデンスの使用よりも大幅に優先されます。

set precedence コマンドと **set ip precedence** コマンドは同じように動作し、最も外側のレイヤ 3 ヘッダーが IPv4 または IPv6 のパケットをマークします。これに対して、**match ip precedence** コマンドは IPv4 パケットのみを分類し、**match precedence** コマンドは IPv4 と IPv6 の両方を分類します。

set precedence tunnel

まだパケットに追加されていないトンネル ヘッダー内に IP プレシデンス値を設定するには、**set precedence tunnel** コマンドをポリシーマップ クラス コンフィギュレーション モードで使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set precedence tunnel *precedence-value*

構文の説明

precedence-value	トンネル ヘッダーに precedence ビットを 0 ~ 7 の範囲で指定します。

コマンド デフォルト

DSCP（および precedence 部分）がカプセル化されたヘッダーから新たにインポーズされたヘッダーへコピーされます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

Cisco ASR 1000 では、IPv4 に対してのみ **setprecedencetunnel** コマンドがサポートされています。サポートされている DSCP トンネルのマーキング設定をリストした表については、インポジション マーキング，（107 ページ）を参照してください。

set qos-group

QoS グループ識別子（ID）をパケットに設定するには、ポリシーマップ クラス コンフィギュレーション モードで **set qos-group** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] set qos-group *group-id*

構文の説明

group-id	QoS グループ ID を 0 ～ 99 の範囲で指定します。

コマンド デフォルト

QoS グループ ID はデフォルトで 0 に設定されます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

set qos-group コマンドでは、ルータによってパケットが処理されるため、グループ ID をパケットに関連付けることができます。

出力ポリシーでグループ ID を使用してパケットをサービスクラスに分類できます。従来、このアクションには意味がありませんでした。出力マーキングが行われる前にサービスクラスが選択されるからです。ただし、カラー対応ポリシングを使用すると、出力ポリシーでの QoS グループ ID の設定には意味を持たせることができます。

たとえば、このコマンドを使用して、入力分類時に出力キューイングに基づくようにします。

第 8 章

QoS パケット一致統計情報の設定

QoS パケット一致統計情報機能は、次のサブ機能で構成されます。

- QoS パケット一致統計情報のフィルタ単位の機能では、ユーザが QoS クラスマップ内の個々のフィルタと一致する（match ステートメント）パケットおよびバイトの数をカウントし、表示することができます。
- QoS パケット一致統計情報の ACE 単位の機能では、ユーザがフィルタ内の個々のアクセス制御エントリ（ACE）に一致するパケットとバイトの数をカウントし、表示することができます。

- 機能情報の確認，139 ページ
- QoS パケット一致統計情報機能の前提条件，140 ページ
- QoS パケット一致統計情報機能の制約事項，140 ページ
- QoS パケット一致統計情報に関する情報，141 ページ
- QoS パケット一致統計情報の設定方法，143 ページ
- その他の参考資料，152 ページ
- QoS パケット一致統計情報の機能情報，153 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

QoS パケット一致統計情報機能の前提条件

ポリシー マップがシステム上のインターフェイスと関連付けられている場合は、フィルタ単位の QoS パケット一致統計情報機能をイネーブルまたはディセーブルにすることはできません。

ACE 単位の QoS パケット一致統計情報機能は、QoS パケット一致統計情報機能によって異なります。したがって、次の前提条件が適用されます。

- フィルタ単位の QoS パケット一致統計情報がイネーブルになっていない場合に、ユーザが ACE 単位の QoS パケット一致統計情報をイネーブルにしようとすると、この機能をイネーブルにするコマンドが CLI で拒否されます。情報メッセージが表示され、コマンドが拒否された理由がユーザに通知されます。

- ACE 単位の QoS パケット一致統計情報機能がイネーブルになっている場合に、ユーザがこの機能をディセーブルにしようとすると、この機能をディセーブルにするコマンドが CLI で拒否されます。情報メッセージが表示され、コマンドが拒否された理由がユーザに通知されます。

QoS パケット一致統計情報機能の制約事項

QoS のパケット一致統計情報機能をイネーブルにすると、拡張設定では CPU 使用率が増加する可能性があります。QoS のパケット一致統計情報機能をイネーブルにする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

ここでは、QoS パケット一致統計情報のフィルタ単位の機能と、QoS パケット一致統計情報の ACE 単位の機能に関する制約事項について説明します。

以降に、QoS パケット一致統計情報機能の制約事項を示します。

- QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにすると、拡張された設定では CPU 使用率が増加する可能性があります。QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにする前に、統計情報の利点とシステムの CPU 使用率の増加を比較して検討します。

- match-all クラス マップに対する QoS パケット一致統計情報のフィルタ単位の機能はサポートされていません。ただし、match-all クラス マップに対する QoS パケット一致統計情報の ACE 単位の機能はサポートされています。

次の表に、QoS パケット一致統計情報の ACE 単位のスケーリングの制約事項に関する情報を示します。

表 *14*：*QoS* パケット一致統計情報：*ACE* 単位のスケーリングの制約事項

プラットフォーム	ACE（IPv4 または IPv6）
ASR1000-ESP5、ASR1001、ASR1002-F、ASR1002-X	25,000
ASR1000-ESP10	30,000
ASR1000-ESP20/ESP40/ESP100	30,000
ISR4400	20,000
CSR1000V	1,000

QoS パケット一致統計情報に関する情報

ここでは、フィルタ機能単位の QoS パケット一致統計情報とACE 機能単位の QoS パケット一致統計情報の概要を示します。

QoS パケット一致統計情報：フィルタ単位の機能の概要

QoS のパケット一致統計情報のフィルタ単位の機能では、フィルタに一致するパケット数およびバイト数をカウントし、表示することができます。

フィルタを定義するには、**class-map** コマンドと **match-any** キーワードを使用します。次に例を示します。

```
class-map match-any my_class
   match ip precedence 4 <-------- User-defined filter
   match qos-group 10 <-------- User-defined filter
```

この情報を使用して、次のタスクを実行できます。

- ネットワークのセグメント上の音声トラフィックの量とデータ トラフィックの量の比較
- 帯域幅の可用性の調整
- 課金情報の正確な決定
- サービスに関する問題のトラブルシューティング

システムは、10 秒のサイクルでパケット一致統計情報を収集します。インターフェイスやセッションが多数存在する場合、システムは各サイクルで約8,000のインターフェイスまたはセッションに関する統計情報を収集します。拡張された設定では、すべての統計情報を収集するのに10秒サイクルが数回必要になる場合があります。

QoS パケット一致統計情報：ACE 単位の機能の概要

QoS のパケット一致統計情報のACE 単位の機能では、ユーザが QoS ポリシー内に使用されている個々の ACE（クラス マップ内に使用されているアクセス グループ）に一致するパケットやバイトの数を追跡し、表示することができます。

この機能は、QoS ポリシーに使用する ACE 用のヒット カウンタを提供します。この機能を有効にすると、QoS ポリシーに使用されている ACE 用の QoS ヒット カウンタを、その特定の ACE 用の既存のセキュリティ アクセス リスト カウンタに追加します。アクセス リストのカウンタは、次のコマンド出力で確認できます。

```
Router# show ip access-lists

Extended IP access list A1
    10 permit ip 32.1.1.0 0.0.0.255 any (129580275 matches)
Extended IP access list A6and7
    10 permit ip 32.1.6.0 0.0.0.255 any (341426749 matches)
    20 permit ip 32.1.7.0 0.0.0.255 any (398245767 matches)
Extended IP access list source
    10 permit ip any host 16.1.1.5 (16147976 matches)
```

QoS ヒット カウンタ（QoS ポリシーで使用されている ACE の数）が、アクセス リスト カウンタに追加されます。この機能をイネーブルにするときは、次の点に注意することを推奨します。

- アクセス リストのカウントは、**show ip access-lists** コマンドの出力で確認できるように（インターフェイスに関する記述なし）、インターフェイス固有ではありません。これらは、ACE を使用し、そのカウントをサポートしているすべての機能のすべてのインターフェイスとすべての方向にわたる、すべてのヒットの総数です。

- インターフェイス固有のカウントは、QoS パケット一致統計情報のフィルタ単位の機能がイネーブルになっている場合は、既存の QoS コマンド（**show policy-map interface**）で提供されます。ただし、前に指定したコマンドでは、次の出力例に示すように、ACE 単位ではなく、フィルタ単位（ACL またはアクセス グループ）のカウントのみが示されます。

```
Router# show access-lists

Extended IP access list A1
    10 permit ip 32.1.1.0 0.0.0.255 any (2000 matches)

Router# show policy-map interface GigabitEthernet0/0/2

  Service-policy input: simple

    Class-map: A1-class (match-all)
      1000 packets, 124000 bytes
      5 minute offered rate 4000 bps
      Match: access-group name A1

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 261000 bps, drop rate 0 bps
      Match: any
```

- QoS フィルタ（クラス マップ内の match ステートメント）に ACE があっても、パケットがそのステートメントに一致しない場合、ACE カウンタはそのパケットについては増加しません。これは次の場合に発生します。

- ACE が deny ステートメントで使用されている。
- match-all クラス マップの定義の他の一致基準（match ip prec 1 など）がパケットをクラスに一致させないようにしている。
- match-any クラス マップの定義の他の一致基準（match ip prec 1 など）がパケットに一致しており、ACE 一致基準と一致させないようにしている。（このフィルタは ACE フィルタよりも優先され、パケットは両方のステートメントに一致しています）。

- アクセス リスト カウントは、ACE を使用し、ACE 単位のカウントをサポートするすべての機能のヒット カウントの（特定の ACE についての）総計です。（Cisco IOS XE3.10 では、セキュリティと QoS の ACL のみが ACE 単位のカウントをサポートしていますが、将来のリリースで変更される可能性があります）。したがって、1 つのパケットが同じ ACE を使用している複数の機能にヒットする（カウントされる）ため、同じパケットに対して（パケットが機能それぞれを通過するたびに）複数回カウントされることになります。次に、この例を示します。

```
ip access-list extended A1
  permit ip 32.1.1.0 0.0.0.255 any
class-map match-all A1-class
  match access-group name A1

interface GigabitEthernet0/0/2
 ip address 32.0.0.1 240.0.0.0
 ip access-group A1 in
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 service-policy input simple


Router# show access-lists

Extended IP access list A1
    10 permit ip 32.1.1.0 0.0.0.255 any (2000 matches)

Router# show policy-map interface GigabitEthernet0/0/2

  Service-policy input: simple

    Class-map: A1-class (match-all)
      1000 packets, 124000 bytes
      5 minute offered rate 4000 bps
      Match: access-group name A1

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 261000 bps, drop rate 0 bps
      Match: any
```

QoS パケット一致統計情報の設定方法

ここでは、QoS パケット一致統計情報の設定方法について説明します。

QoS パケット一致統計情報の設定：フィルタ単位

はじめる前に

- QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにする前に、システム上のインターフェイスに関連付けられているポリシー マップがないことを確認します。ある場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
            to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

- QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにする前に、**class-map** コマンドと **match-any** キーワードを使用するフィルタを定義していることを確認します。

（注） QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにすると、拡張された設定では CPU 使用率が増加する可能性があります。QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにする前に、統計情報の利点とシステムの CPU 使用率の増加を比較して検討します。

QoS パケット一致統計情報のフィルタ単位の機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **platformqosmatch-statisticsper-filter**
4. **interface** *interface -name*
5. **service-policy** {**input** | **output**} *policy-map-name*
6. **end**
7. **showpolicy-mapinterface***interface-name*
8. **configureterminal**
9. **interface** *interface-name*
10. **no service-policy** {**input** | **output**} *policy-map-name*
11. **exit**
12. **no platform qos match-statistics per-filter**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configureterminal** 例： `Router# 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	**platformqosmatch-statisticsper-filter** 例： `Router(config)# platform qos match-statistics per-filter`	QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにします。
ステップ 4	**interface** *interface -name* 例： `Router(config)# interface GigabitEthernet0/0/0`	ポリシー マップを適用するためのインターフェイスを指定します。
ステップ 5	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input pol1`	インターフェイスにQoSポリシーマップを適用します。QoS パケット一致統計情報機能は、QoS ポリシーを適用する前にイネーブルにする必要があります。
ステップ 6	**end** 例： `Router# end`	コンフィギュレーション モードを終了します。
ステップ 7	**showpolicy-mapinterface***interface-name* 例： `Router# show policy-map interface serial4/0/0`	指定したインターフェイス、サブインターフェイス、またはインターフェイス上の特定の相手先固定接続（PVC）に存在するすべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。
ステップ 8	**configureterminal** 例： `Router# 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 9	**interface** *interface-name* 例： `Router(config)# interface GigabitEthernet0/0/0`	ポリシー マップを削除するためのインターフェイスを指定します。
ステップ 10	**no service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# no service-policy input pol1`	インターフェイスから QoS ポリシー マップを削除します。QoS パケット一致統計情報機能をディセーブルにする前に、すべての QoS ポリシーをインターフェイスから削除する必要があります。
ステップ 11	**exit** 例： `Router(config-if)# exit`	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 12	**no platform qos match-statistics per-filter** 例： `Router(config)# no platform qos match-statistics per-filter`	QoS パケット一致統計情報のフィルタ単位の機能をディセーブルにします。
ステップ 13	**end** 例： `Router# end`	コンフィギュレーション モードを終了します。

例

showpolicy-mapinterface コマンドを使用して、指定したインターフェイス、サブインターフェイス、またはインターフェイス上の PVC に存在するすべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

```
Router# show policy-map interface gig1/1/0

 GigabitEthernet1/1/0
  Service-policy input: pol1     ! target = gig1/1/0,input
    Class-map: class1 (match-any)
      1000 packets, 40000 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1 <-------- User-defined filter
        800 packets, 32000 bytes <-------- Filter matching results
      Match: ip precedence 2 <-------- User-defined filter
        200 packets, 8000 bytes <-------- Filter matching results
      QoS Set
        ip precedence 7
          No packet marking statistics available
    Class-map: class-default (match-any)
      500 packets, 20000 bytes
```

```
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any <-------- User-defined filter
  500 packets, 20000 bytes <-------- Filter matching results
```

QoS パケット一致統計情報の設定：ACE 単位

はじめる前に

QoS パケット一致統計情報の ACE 単位の機能をイネーブルにする前に、QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにしたことを確認します。

次に、**show platform hardware qfp active feature qos configuration global** コマンドを使用して機能の統計情報を確認する例を示します。

```
Router# show platform hardware qfp active feature qos configuration global
Marker statistics are: disabled
Match per-filter statistics are: enabled <<<<<<<
Match per-ace statistics are: enabled <<<<<<
Performance-Monitor statistics are: disabled
```

QoS パケット一致統計情報の ACE 単位の機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **platform qos match-statistics per-filter**
4. **platform qos match-statistics per-ace**
5. **interface** *interface-name*
6. **service-policy**{**input**|**output**}*policy-map-name*
7. **end**
8. **showpolicy-mapinterface***interface-name*
9. **show access-lists**
10. **configureterminal**
11. **interface** *interface-name*
12. **no service-policy**{**input**|**output**}*policy-map-name*
13. **exit**
14. **no platform qos match-stat per-ace**
15. **no platform qos match-statistics per-filter**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**platform qos match-statistics per-filter** 例： `Router(config)# platform qos match-statistics per-filter`	QoS パケット一致統計情報のフィルタ単位の機能をイネーブルにします。
ステップ 4	**platform qos match-statistics per-ace** 例： `Router(config)# platform qos match-statistics per-ace`	QoS パケット一致統計情報の ACE 単位の機能をイネーブルにします。
ステップ 5	**interface** *interface-name* 例： `Router(config)# interface GigabitEthernet0/0/0`	ポリシーマップを適用するためのインターフェイスを指定します。
ステップ 6	**service-policy** {**input**|**output**}*policy-map-name* 例： `Router(config-if)# service-policy input pol1`	インターフェイスに QoS ポリシー マップを適用します。QoS 一致統計情報機能は、QoS ポリシーを適用する前にイネーブルにする必要があります。
ステップ 7	**end** 例： `Router# end`	コンフィギュレーション モードを終了します。
ステップ 8	**showpolicy-mapinterface***interface-name* 例： `Router# show policy-map interface serial4/0/0`	指定したインターフェイス、サブインターフェイス、またはインターフェイス上の特定の PVC のいずれかで、すべてのサービス ポリシーに対して設定されているすべてのクラスに関するパケット統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show access-lists** 例： `Router# show access-lists`	ACE 単位の QoS パケット一致統計情報を含めて、現在のアクセス リストのコンテンツを表示します。
ステップ 10	**configureterminal** 例： `Router# 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 11	**interface** *interface-name* 例： `Router(config)# interface GigabitEthernet0/0/0`	ポリシーマップを削除するためのインターフェイスを指定します。
ステップ 12	**no service-policy**{**input**|**output**}*policy-map-name* 例： `Router(config-if)# no service-policy input pol1`	インターフェイスから QoS ポリシー マップを削除します。QoS 一致統計情報機能をディセーブルにする前に、すべてのQoSポリシーをインターフェイスから削除する必要があります。
ステップ 13	**exit** 例： `Router(config-if)# exit`	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 14	**no platform qos match-stat per-ace** 例： `Router(config)# no platform qos match-stat per-ace`	QoS パケット一致統計情報の ACE 単位の機能をディセーブルにします。
ステップ 15	**no platform qos match-statistics per-filter** 例： `Router(config)# no platform qos match-statistics per-filter`	QoS パケット一致統計情報のフィルタ単位の機能をディセーブルにします。
ステップ 16	**end** 例： `Router# end`	コンフィギュレーション モードを終了します。

例

showpolicy-mapinterface コマンドを使用して、指定したインターフェイス、サブインターフェイス、またはインターフェイス上のPVCに存在するすべてのサービスポリシーに対して設定されているすべてのクラスのフィルタ単位の統計情報を表示します。

```
Router# show policy-map interface GigabitEthernet0/0/2


  Service-policy input: test-match-types

    Class-map: A1orA2-class (match-any)
      482103366 packets, 59780817384 bytes
      5 minute offered rate 6702000 bps
      Match: access-group name A1
        62125633 packets, 7703578368 bytes
        5 minute rate 837000 bps
      Match: access-group name A2
        419977732 packets, 52077238892 bytes
        5 minute rate 5865000 bps

    Class-map: A3andprec1-class (match-all)
      5673520 packets, 703516480 bytes
      5 minute offered rate 837000 bps
      Match: access-group name A3
      Match: ip precedence 1

    Class-map: A5-class (match-all)
      227101820 packets, 28160625680 bytes
      5 minute offered rate 3351000 bps
      Match: access-group name A5

    Class-map: A6and7-class (match-all)
      627615840 packets, 77824340228 bytes
      5 minute offered rate 9215000 bps
      Match: access-group name A6and7

    Class-map: A3-class (match-all)
      111548288 packets, 13831987712 bytes
      5 minute offered rate 1675000 bps
      Match: access-group name A3

    Class-map: A4andsource (match-all)
      16115590 packets, 1998333160 bytes
      5 minute offered rate 2513000 bps
      Match: access-group name A4
      Match: access-group name source

    Class-map: class-default (match-any)
      164881212 packets, 20445270288 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

showipaccess-lists コマンドを使用して、現在のアクセスリストのコンテンツ（ACE 単位の QoS パケット一致統計情報を含む）を表示します。

```
Router# show ip access-lists

Extended IP access list A1
    10 permit ip 32.1.1.0 0.0.0.255 any (129580275 matches)
Extended IP access list A2
    10 permit ip 32.1.2.0 0.0.0.255 any (486342300 matches)
Extended IP access list A3
    10 permit ip 32.1.3.0 0.0.0.255 any (306738457 matches)
Extended IP access list A4
    10 permit ip 32.1.4.0 0.0.0.255 any (16147975 matches)
Extended IP access list A5
    10 permit ip 32.1.5.0 0.0.0.255 any (294357455 matches)
Extended IP access list A6and7
```

```
    10 permit ip 32.1.6.0 0.0.0.255 any (341426749 matches)
    20 permit ip 32.1.7.0 0.0.0.255 any (398245767 matches)
Extended IP access list source
    10 permit ip any host 16.1.1.5 (16147976 matches)
```

トラブルシューティングのヒント

QoS のパケット一致統計情報機能がイネーブルかどうかを確認するには、**show platform hardware qfp active feature qos config global** コマンドを使用します。この機能がディセーブルの場合は、次のようなメッセージが表示されます。

Router# **show platform hardware qfp active feature qos config global**

```
Marker statistics are: enabled
Match per filter statistics are: enabled
```

例：QoS パケット一致統計情報の設定：フィルタ単位

次に、QoS パケット一致統計情報を設定する例を示します。フィルタ単位で次のタスクを実行します。

- QoS パケット一致フィルタを定義する
- **show policy-map interface** コマンドの出力を表示する

```
Router# show policy-map interface Tunnel1

  Service-policy output: DATA-OUT-PARENT
    Class-map: class-default (match-any)
      4469 packets, 4495814 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any <-------- User-defined filter
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 4469/4558380
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000
      Service-policy : DATA-OUT
        queue stats for all priority classes:
          Queueing
          queue limit 200 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 4469/4558380
        Class-map: ATM-VTI-RIP-SPK1-DATA (match-any)
          4469 packets, 4495814 bytes <-------- Filter matching results
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: access-group 121 <-------- User-defined filter
            4469 packets, 4495814 bytes <-------- Filter matching results
            5 minute rate 0 bps
          QoS Set
            ip precedence 3
              Packets marked 4469
          Priority: 100 kbps, burst bytes 2500, b/w exceed drops: 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Quality of Service コマンド	『*Cisco IOS Quality of Service Command Reference*』

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
CISCO-CLASS-BASED-QOS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

QoS パケット一致統計情報の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15*：*QoS* パケット一致統計情報の機能情報

機能名	リリース	機能情報
QoS パケット一致統計情報：フィルタ単位	Cisco IOS XE リリース 3.3S	QoS パケット一致統計情報のフィルタ単位の機能では、パケットの QoS サービス ポリシー内のクラスマップに使用されている個々のフィルタに一致する（match ステートメント）パケットの数をカウントし、表示することができます。 次のコマンドが導入または変更されました。 • **platform qos match-statistics per-filter** • **no platform qos match-statistics per-filter** • **show platform hardware qfp active feature qos config global**
QoS パケット一致統計情報：ACE 単位	Cisco IOS XE リリース 3.10S	QoS のパケット一致統計情報の ACE 単位の機能では、ユーザが QoS ポリシー内に使用されている個々の ACE（クラスマップ内に使用されているアクセス グループ）に一致するパケットやバイトの数を追跡し、表示することができます。 次のコマンドが導入されました。 **platform qos match-statistics per-ace**

第 9 章

ポリサーを使用した ATM CLP 設定ビット

ポリサーを使用した ATM CLP 設定ビットの機能では、ポリシングして、アウトバウンドの PPP over ATM（PPPoA）トラフィックをマークすることができます。ATM セル損失率優先度（CLP）ビットは、次のいずれかの方法で設定できます。

- ポリシングされたしきい値
- クラスの一致

- 機能情報の確認，155 ページ
- ポリサーを使用した ATM CLP 設定ビットの前提条件，156 ページ
- ポリサーを使用した ATM CLP 設定ビットに関する情報，156 ページ
- ポリサーを使用した ATM CLP ビットの設定方法，157 ページ
- ポリサーを使用した ATM CLP 設定ビットの設定例，161 ページ
- その他の参考資料，162 ページ
- ポリサーを使用した ATM CLP 設定ビットの機能情報，164 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ポリサーを使用した ATM CLP 設定ビットの前提条件

ポリシングされたしきい値を使用して ATM CLP ビットを設定する場合は、**set-clp-transmit** アクションがポリシーマップに含まれていることを確認します。新しいポリサーアクションは、トラフィックが所定のレートを超えたときの ATM ネットワーク内の高い廃棄確率に一致するクラス内の PPPoA トラフィックを条件付きでマークします。

クラスの一致により ATM CLP ビットを厳格に設定する場合は、**set atm-clp** アクションがポリシーマップに含まれていることを確認します。set ディレクティブは、ATM ネットワーク内の高い廃棄確率に一致するクラス内のすべてのトラフィックをマークします。

set-clp-transmit アクションまたは **set atm-clp** アクションを使用して、ポリシー マップを仮想テンプレートに適用することができます。このテンプレートは、PPPoA セッションの作成時か、またはダイナミックに割り当てることで複製されます。

ポリサーを使用した ATM CLP 設定ビットに関する情報

ATM CLP ビット

ATM CLP ビットは、ATM セルのドロップ プライオリティを示します。ATM ネットワークの輻輳時に、ルータは CLP ビットが 1 に設定されている ATM セルを廃棄してから、CLP ビットが 0 に設定されているセルを廃棄します。

ポリサーを使用した ATM CLP ビットの設定機能を使用すると、セル ヘッダー内の ATM CLP ビットを有効にするように **police** コマンドを設定できます。ATM CLP ビットは set ディレクティブで明示的にマークできます。

ポリサーを使用した ATM CLP ビットの設定機能は、次のタイプのポリシーで **set-clp-transmit** ポリシング アクションをサポートします。

- シングル レート ポリシング
- デュアルレート ポリシング
- 階層型

ポリサーを使用した ATM CLP ビットの設定方法

PPPoA ブロードバンドのトラフィック ポリシングの設定

はじめる前に

ポリシーマップを設定する前に、トラフィックを分類するために使用するクラスマップを定義していることを確認します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name*|**class-default**]
5. **police** [**cir***cir*] [**conform-action***action*] [**exceed-action***action*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Device(config)# policy-map parent-policy`	ポリシーマップ コンフィギュレーション モードを開始し、ポリシーマップを作成します。
ステップ 4	**class** {*class-name*|**class-default**] 例： `Device(config-pmap)# class class-default`	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。 作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといい

	コマンドまたはアクション	目的
		ます）を指定します。作成または変更する子クラスまたは親クラスを指定するのに必要な回数だけ、このコマンドを繰り返してください。 • *classname*：設定するクラス、またはポリシーを編集するクラスの名前。クラス名は、クラスマップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。 • **class-default**：デフォルト クラスのポリシーを設定または変更できるようにデフォルト クラスを指定します。

ステップ 5	**police** [**cir***cir*] [**conform-action***action*] [**exceed-action***action*]
	例：
	`Device(config-pmap-c)# police 1000000`
	例：
	`Router(config-pmap-c-police)# conform-action`
	例：
	`transmit`
	例：
	`Device(config-pmap-c-police)# exceed-action`
	例：
	`set-clp-transmit`
		トラフィック ポリシングを設定し、指定のレートに準拠、超過、または違反としてマーク付けされたパケットに適用する複数のアクションを指定します。
		• ポリシー マップ クラス ポリス コンフィギュレーション モードを開始します。1 つのアクションにつき 1 行を使用して、アクションを指定します。
		  • **cir**：（任意）認定情報レート。CIR がトラフィック ポリシングに使用されることを示します。
		  • **conform-action**：（オプション）準拠バーストを下回るレートのパケットに対して実行するアクション。
		  • **exceed-action**：（オプション）準拠バースト以上で、準拠バーストと超過バーストの合計以下のレートのパケットに対して実行するアクション。

ステップ 6	**end** 例： `Device(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

例

次に、ポリサーを使用して ATM CLP を設定する例を示します。

```
policy-map egress_atm_clp_policer
 class prec0
  police cir 5000000
 class prec1
  police cir 3000000 conform-action transmit exceed-action set-clp-transmit
 class class-default
  police cir 1000000 conform-action transmit exceed-action set-clp-transmit
```

ATM CLP ビットのマーキング

はじめる前に

ポリシーマップを設定する前に、トラフィックを分類するために使用するクラスマップを定義していることを確認します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-mappolicy-map-name**
4. **class** {*class-name*|**class-default**]
5. **setatm-clp**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**policy-mappolicy-map-name** 例： `Router(config)# policy-map parent-policy`	ポリシー マップ コンフィギュレーション モードを開始し、ポリシー マップを作成します。

	コマンドまたはアクション	目的
ステップ 4	**class** {*class-name*|**class-default**] 例： `Router(config-pmap)# class class-default`	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。 作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。作成または変更する子クラスまたは親クラスを指定するのに必要な回数だけ、このコマンドを繰り返してください。 • *classname*：設定するクラス、またはポリシーを編集するクラスの名前。クラス名は、クラスマップに使用するとともに、ポリシーマップのクラスにポリシーを設定する場合にも使用します。 • **class-default**：デフォルト クラスのポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 5	**setatm-clp** 例： `Router(config-pmap-c)# set atm-clp`	このクラスに一致するすべてのトラフィックに対して ATM CLP ビットのマーキングを設定します。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

例

次に、明示的なマーキングを使用して ATM CLP を設定する例を示します。

```
policy-map egress_atm_clp_policer
 class prec0
  police cir 5000000
 class class-default
  set atm-clp
```

ポリサーを使用した ATM CLP 設定ビットの設定例

例：クラスに一致するポリサーアクションによる ATM CLP のマーキング

この例では、次のタスクの実行方法を説明します。

- トラフィック クラスを定義する。
- 2 レイヤ ポリシー マップを設定する。
- PPPoA セッションにポリシー マップを適用する。

このポリシーは、クラスのトラフィックが所定のレートを超えたときに、一致する low_interest クラスのトラフィックに ATM CLP ビットを条件付きでマークします。

```
class-map voice
  match precedence 4
!
class-map web
  match precedence 3
!
class low_interest
  match precedence 1 0
!
policy-map child
 child class voice
  police cir 256000
  priority level 1
 class web
  bandwidth remaining ratio 10
 class low_interest
  police cir 1000000 conform-action transmit exceed-action set-clp-transmit
 class class-default
  bandwidth remaining ratio 1
!
policy-map parent
 class class-default
  shape average 15000000
  service-policy child
```

仮想テンプレートに適用されたポリシーマップが複製され、各 PPPoA セッションに対して仮想アクセス インターフェイスを作成するために使用されます。

```
interface Virtual-Template1
 ip unnumbered Loopback1
 load-interval 30
 peer default ip address pool POOL1
 ppp authentication chap ppp
 ipcp address required
 service-policy output parent
```

例：ポリサー アクションのポリシングされたしきい値による ATM CLP のマーキング

この例では、次のタスクの実行方法を説明します。

- トラフィック クラスを定義します。
- 2 レイヤ ポリシー マップを設定する。
- PPPoA セッションにポリシー マップを適用する。

このポリシーは、ATM ネットワークに輻輳が発生したときにドロップされるように、必須以外のトラフィックを ATM CLP ビッドを使用してマークします。

```
class-map video
  match precedence 5
!
class-map voice
  match precedence 4
!
class-map web
  match precedence 3
!
policy-map child
 child class voice
  police cir 256000
  priority level 1
 class video
  police cir 4000000
  priority level 2
 class web
  set atm-clp
  bandwidth remaining ratio 10
 class class-default
  bandwidth remaining ratio 1
  set atm-clp
!
interface Virtual-Template1
 ip unnumbered Loopback1
 load-interval 30
 peer default ip address pool POOL1
 ppp authentication chap ppp
 ipcp address required
 service-policy output parent
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Quality of Service コマンド	『*Cisco IOS Quality of Service Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ポリサーを使用した ATM CLP 設定ビットの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16*：ポリサーを使用した *ATM CLP* 設定ビットの機能情報

機能名	リリース	機能情報
ポリサーを使用した ATM CLP 設定ビット	Cisco IOS リリース XE 3.3S Cisco IOS リリース XE 3.14S	ポリサーを使用した ATM CLP 設定ビットの機能では、ポリシングが可能であり、アウトバウンド PPPoA トラフィックをマークします。 Cisco IOS リリース 3.14S では、この機能は Cisco 4451-X サービス統合型ルータに追加されました。 次のコマンドが導入または変更されました。**setatm-clp**and **police**。

第 10 章

EVC Quality of Service

このマニュアルでは、イーサネット仮想回線（EVC）で使用する Quality of Service（QoS）機能（トラフィックの分類やポリシングなど）をイネーブルにする方法について説明します。

Metro Ethernet Forum で定義された EVC は、ポートレベルのポイントツーポイントまたはマルチポイントツーマルチポイント回線です。プロバイダーから顧客に提供されているサービスの1つのインスタンスをエンドツーエンドで表します。さまざまなパラメータが統合されて、サービスが提供されます。

- 機能情報の確認，165 ページ
- EVC での Quality of Service に関する情報，166 ページ
- EVC での Quality of Service 機能の設定方法，172 ページ
- EVC QoS の設定例，177 ページ
- その他の参考資料，179 ページ
- EVC QoS を設定するための機能情報，180 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

EVC での Quality of Service に関する情報

EVC Quality of Service と MQC

QoS 機能は、通常、トラフィック クラス、クラス マップ、ポリシー マップを使用して適用します。たとえば、特定のクラスに属するトラフィックを特定のカテゴリに分類し、特定の QoS 処理（分類やポリシングなど）を実行するように指定できます。トラフィックに対して実行される特定の QoS 処理はポリシー マップで指定し、ポリシー マップはインターフェイスに適用します。このように QoS を適用するために使用されるメカニズムはモジュラ QoS CLI（MQC）です。

ポリシー マップは、**service-policy** コマンドを使用して、着信（入力）または発信（出力）方向でインターフェイスに適用できます。

MQC 構造では、トラフィック クラスの定義、トラフィック ポリシーの作成、インターフェイス（この場合、EVC）へのトラフィック ポリシーの適用を行えます。

MQC 構造は、大きく次の 3 つの手順からなります。

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。（トラフィック ポリシーという用語とポリシーマップという用語は、多くの場合同じ意味で使用されます）。トラフィック ポリシー（ポリシー マップ）には、1 つのトラフィック クラスと、トラフィック クラスに適用する 1 つ以上の QoS 機能を含めます。トラフィック ポリシー内の QoS 機能によって、分類されたトラフィックの処理方法が決まります。
3. **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシーマップ）をインターフェイスに適用します。

（注） 階層型ポリシー マップやクラス マップを含む MQC の詳細については、「MQC を使用した QoS 機能の適用」モジュールを参照してください。

QoS 対応イーサネット フロー ポイント（EFP）

EVC Quality of Service と MQC, （166 ページ）で説明したように、MQC はネットワーク トラフィックに 1 つまたは複数の QoS 機能を適用するために使用されます。MQC を使用する最後のステップでは、**service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をインターフェイス（この場合は EVC）に適用します。

EVC Quality of Service 機能では、**service-policy** コマンドを使用して、EVC の着信（入力）方向または発信（出力）方向のイーサネット フロー ポイント（EFP）にポリシー マップを適用できます。このようにして、EFP は「QoS 対応」と認識されます。

QoS 機能と EVC

QoS の特定の機能として、次が含まれています。

- パケットの分類（Diffserv コード ポイント（DSCP）値や QoS グループ ID などに基づく）
- パケット マーキング（サービス クラス（CoS）値）に基づくなど）
- トラフィック ポリシング（2 色、3 色および複数アクション）
- 帯域幅の共有
- プライオリティ キューイング（EVC のアウトバウンド方向のみ）
- 重み付けランダム早期検出（WRED）

QoS 機能は、次の項の一覧に示す適切なコマンドを使用してイネーブルにします。

EVC QoS がサポートするトラフィック分類の match コマンド

次の表に、EVC でのトラフィックの分類時にで使用できる **match** コマンドの一部を示します。使用可能な **match** コマンドは、Cisco IOS XE のリリースによって異なります。コマンドおよびコマンド シンタックスの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。

表 *17* : ***MQC*** で使用可能な ***match*** コマンド

コマンド	目的
matchaccess-group	指定したアクセス コントロール リスト（ACL）に基づいて、クラスマップの一致基準を設定します。
matchany	すべてのパケットの一致基準を設定します。
matchcos	レイヤ 2 CoS マーキングに基づいてパケットを照合します。
matchcosinner	レイヤ 2 CoS マーキングに基づいて QinQ パケットの内部 CoS を照合します。
match [**ip**] **dscp**	特定の IP DSCP 値を一致基準として識別します。1 つの match 文に最大 8 つの DSCP 値を含めることができます。

コマンド	目的
matchnot	成功しない一致基準として使用する、1 つの一致基準値を指定します。 （注） **matchnot** コマンドは、一致基準として使用する特定の match パラメータを指定する代わりに、パケットがクラスのメンバーとして分類されるのを防ぐ一致基準を指定するために使用します。たとえば、トラフィック クラスの設定中に **matchnotqos-group6** コマンドを発行すると、QoS グループ 6 だけが、成功する一致基準として考慮されない QoS グループ値となります。他の QoS グループ値は成功する一致基準となります。
match [ip] precedence	IP precedence 値を一致基準として識別します。
matchqos-group	特定の QoS グループ値を一致基準として識別します。
matchsource-addressmac	送信元 MAC アドレスを一致基準として使用します。 （注） **matchsource-addressmac** コマンドを使用したトラフィックの分類は、入力方向でのみサポートされます。
matchvlan(QoS)	VLAN ID 番号に基づいてトラフィックを照合し、分類します。
match vlan inner	802.1q のタグ付きフレームの最も内部にある VLAN ID を照合するクラス マップを設定します。

1 つのトラフィック クラスでの複数の match コマンド

トラフィック クラスに複数の **match** コマンドが含まれている場合、それらの **match** コマンドの評価方法を指定する必要があります。これは、**class-map** コマンドの **match-any** キーワードまたは **match-all** キーワードを使用して指定します。**match-any** キーワードと **match-all** キーワードついては、次の点に注意してください。

- **match-any** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した基準の *1* つに一致する必要があります。

- **match-all** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した基準のすべてに一致する必要があります。
- どちらのキーワードも指定しなかった場合、トラフィック クラスによって評価されるトラフィックは、指定した基準のすべてに一致する必要があります（つまり、**match-all** キーワードの動作が使用されます）。

EVC で QoS 機能をイネーブルにするために使用するコマンド

QoS 機能をイネーブルにするために使用するコマンドは、Cisco IOS XE リリースごとに異なります。以下の表に、使用可能なコマンドとそれによってイネーブルになる QoS 機能の一部を示します。コマンド シンタックスについては、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。

イネーブルにする特定の QoS 機能の詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』の適切なモジュールを参照してください。

表 *18* : *QoS* 機能をイネーブルにするために使用するコマンド

コマンド	目的
帯域幅	クラスの最小帯域幅保証を設定します。
bandwidthremaining	クラスの過剰重量を設定します。
drop	指定したトラフィック クラスのパケットを廃棄します。
fair-queue	トラフィック クラス内のフローベースのキューイング機能をイネーブルにします。
police	トラフィック ポリシングを設定します。複数のポリシング アクションを指定できるようにします。
police(percent)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police(tworates)	認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートを使用したトラフィック ポリシングを設定します。
priority	ポリシーマップに属するトラフィックのクラスにプライオリティを与えます。

コマンド	目的
queue-limit	ポリシーマップで設定されているクラスに対してキューが保持できるパケットの最大数を指定または変更します。
random-detect	重み付けランダム早期検出（WRED）をイネーブルにします。
random-detect cos-based	パケットのサービスクラス（CoS）値に基づいて、Weighted Random Early Detection（WRED）をイネーブルにします。
random-detect dscp-based	パケットの廃棄確率を計算する場合、Weighted Random Early Detection（WRED）で DiffServ コード ポイント（DSCP）の値を使用するよう、指定します。
random-detectdiscard-class	ポリシー マップ内のクラスの discard-class 値に対し、WRED パラメータを設定します。
random-detectdiscard-class-based	パケットの廃棄クラス値に基づく WRED を設定します。
random-detectexponential-weighting-constant	クラス用に予約されたキューの平均キューサイズ計算用の指数加重係数を設定します。
random-detectprecedence	ポリシーマップ内のクラスポリシーに対する、特定の IP precedence の WRED パラメータを設定します。
service-policy	一致基準として使用するトラフィック ポリシーの名前を指定します（トラフィック ポリシーを互いにネストさせるため（階層型トラフィック ポリシー））。
setcos	発信パケットのレイヤ 2 CoS 値を設定します。
setcos-inner	ブリッジフレームの内部サービスクラスフィールドをマークします。
setdiscard-class	discard-class 値でパケットをマークします。
set[**ip**] **dscp**	タイプ オブ サービス（ToS）バイト内の DSCP 値を設定することでパケットをマークします。

コマンド	目的
setmplsexperimental	パケットが指定したポリシーマップに一致する場合にマルチプロトコル ラベル スイッチング（MPLS）ビットを設定する値を指定します。
setprecedence	パケット ヘッダーに precedence 値を設定します。
setqos-group	後でパケットを分類するために使用できるQoSグループ ID を設定します。
shape	指定したアルゴリズムに従って、指示されたビット レートまでトラフィックをシェーピングします。

service-policy コマンドの input および output キーワード

一般的な規則として、トラフィック ポリシーで設定するQoS機能は、インターフェイスで受信されるパケットか、インターフェイスで送信されるパケットに適用できます。そのため、**service-policy** コマンドを使用する場合は、**input** キーワードまたは **output** キーワードを使用してトラフィック ポリシーの方向を指定する必要があります。

たとえば、**service-policyoutputpolicy-map1** コマンドは、トラフィック ポリシーの QoS 機能を出力方向のインターフェイスに適用します。インターフェイス（出力）から送信されるすべてのパケットが、policy-map1 という名前のトラフィック ポリシーで指定された基準に従って評価されます。

（注） Cisco のリリースでは、キューイング メカニズムは入力方向ではサポートされていません。非キューイング メカニズム（トラフィック ポリシングやトラフィック マーキングなど）は、入力方向でサポートされています。また、送信元 MAC アドレスに基づくトラフィックの分類（**matchsource-addressmac** コマンドを使用）は、入力方向でのみサポートされています。

EVC での Quality of Service 機能の設定方法

EVC で使用するトラフィック クラスの作成

トラフィック クラスを作成するには、**class-map** コマンドを使用してトラフィック クラス名を指定します。次に、1 つ以上の **match** コマンドを使用して、適切な一致基準を指定します。指定した基準に一致するパケットがトラフィック クラスに分類されます。

EVC で使用するトラフィック クラスを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] *class-name*
4. **matchcos***cos-number*
5. 必要に応じて追加の **match** コマンドを入力します。追加のコマンドが不要な場合は次のステップに進みます。
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**class-map** [**match-all** | **match-any**] *class-name* 例： `Router(config)# class-map match-any class1`	クラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。 • クラス マップは、パケットを指定したクラスに照合するために使用します。

	コマンドまたはアクション	目的
		（注） **match-all** キーワードは、すべての一致基準が満たされることが必要であることを指定します。**match-any** キーワードは、いずれかの一致条件が満たされることが必要であることを指定します。これらのキーワードは、複数の **match** コマンドを指定する場合にだけ使用します。
ステップ 4	**matchcos***cos-number* 例： `Router(config-cmap)# match cos 2`	レイヤ 2 CoS 番号に基づいて、パケットを照合します。 （注） **matchcos** コマンドは、使用できる **match** コマンドの一例です。
ステップ 5	必要に応じて追加の **match** コマンドを入力します。追加のコマンドが不要な場合は次のステップに進みます。	--
ステップ 6	**end** 例： `Router(config-cmap)# end`	（任意）クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

EVC で使用するポリシー マップの作成

EVC で使用するトラフィック ポリシー（ポリシー マップ）を作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name*| **class-default**}
5. **police***bps*[*burst-normal*] [*burst-max*] [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]
6. イネーブルにする追加の QoS 機能に対するコマンドを入力します。他に QoS 機能が必要ない場合は、次のステップに進みます。
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**policy-map***policy-map-name*
	
	例：
	`Router(config)#`
	`policy-map policy1`
		トラフィック ポリシーの名前を作成または指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

ステップ 4	**class** {*class-name*| **class-default**}
	
	例：
	`Router(config-pmap)#`
	`class class1`
		クラスの名前を指定し、QoS 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。
		（注） この手順により、トラフィック クラスがトラフィック ポリシーに関連付けられます。

ステップ 5	**police***bps*[*burst-normal*] [*burst-max*] [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*] 例： `Router(config-pmap-c)# police 3000`	（任意）トラフィック ポリシングを設定します。 （注） **police** コマンドは、QoS 機能をイネーブルにするためにポリシーマップで使用できるコマンドの一例です。
ステップ 6	イネーブルにする追加の QoS 機能に対するコマンドを入力します。他に QoS 機能が必要ない場合は、次のステップに進みます。	--
ステップ 7	**end** 例： `Router(config-pmap-c)# end`	（任意）QoS 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、特権 EXEC モードに戻ります。

EVC の設定および EVC へのトラフィック ポリシーの適用

ポリシー マップを EVC に適用すると、トラフィック ポリシー（ポリシー マップ）は、イネーブルにした QoS 機能をトラフィック クラスに適用します。

EVC を設定し、EVC にトラフィック ポリシーを適用するには、次の手順を実行します。

（注） EVC にトラフィック ポリシーを適用するために使用するコマンドの 1 つに、**service-policy** コマンドがあります。このコマンドを使用する場合は、ポリシー マップ名とともに **input** キーワードまたは **output** キーワードを指定する必要があります。ポリシー マップには、使用する QoS 機能が含まれます。特定の QoS 機能は、入力方向または出力方向のいずれかでのみ使用できます。これらのキーワードとサポートされる QoS 機能の詳細については、service-policy コマンドの input および output キーワード, （13 ページ）を参照してください。また、複数の EVC を含むインターフェイスにトラフィック ポリシーを適用する場合、トラフィック ポリシーはインターフェイス上のすべての EVC に適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***interface-typeinterface-number*
4. **serviceinstance***id***ethernet**[*evc-name*]
5. **encapsulationdot1q***vlan-id*[,*vlan-id*[-*vlan-id*]] [**native**]
6. **rewriteingresstagtranslate1-to-1dot1q***vlan-id***symmetric**
7. **bridgedomain***domain-number*
8. **service-policy**{**input** | **output**} *policy-map-name*
9. **end**
10. **showpolicy-mapinterface***typenumber***serviceinstance***service-instance-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**interface***interface-typeinterface-number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイスタイプとインターフェイス番号を入力します。
ステップ 4	**serviceinstance***id***ethernet**[*evc-name*] 例： `Router(config-if)# service instance 333 ethernet evc1`	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス コンフィギュレーション モードを開始します。 • サービス インスタンス ID と、該当する場合は EVC 名（任意）を入力します。
ステップ 5	**encapsulationdot1q***vlan-id*[,*vlan-id*[-*vlan-id*]] [**native**] 例： `Router(config-if-srv)# encapsulation dot1q 10`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。
ステップ 6	**rewriteingresstagtranslate1-to-1dot1q***vlan-id***symmetric** 例： `Router(config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 300 symmetric`	サービス インスタンスに入るフレームで実行されるカプセル化調整を指定します。
ステップ 7	**bridgedomain***domain-number* 例： `Router(config-if-srv)# bridge domain 1`	ブリッジ ドメインを設定します。 • ブリッジドメイン番号を入力します。

	コマンドまたはアクション	目的

ステップ 8	**service-policy** {**input** | **output**} *policy-map-name*
	
	例：
	`Router(config-if-srv)#`
	`service-policy input policy1`
		ポリシー マップをインターフェイスに付加します。
		• **input** キーワードまたは **output** キーワードとポリシーマップ名を入力します。

ステップ 9	**end** 例： `Router(config-if-srv)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 10	**showpolicy-mapinterface***typenumber***serviceinstance***service-instance-number* 例： `Router# show policy-map interface gigabitethernet 1/0/0 service instance 30`	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。 • インターフェイスタイプ、インターフェイス番号、サービスインスタンス番号を入力します。

EVC QoS の設定例

例：EVC で使用するトラフィック クラスの作成

この例では、CoS 値が 2 のトラフィックが、class1 と呼ばれるトラフィック クラスに置かれます。

```
Router> enable
Router# configure terminal
Router(config)# class-map match-any class1
Router(config-cmap)# match cos 2
Router(config-cmap)# end
```

例：EVC で使用するポリシー マップの作成

この例では、トラフィック ポリシングは、policy1 と呼ばれるポリシー マップで設定されています。トラフィック ポリシングは、class1 のトラフィックに適用される QoS 機能です。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 3000

Router(config-pmap-c)# end
```

例：EVC の設定と EVC へのトラフィック ポリシーの適用

この例では、EVC が設定され、policy1 と呼ばれるトラフィック ポリシーが EVC に適用されています。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# service instance 333 ethernet evc1
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 300 symmetric
Router(config-if-srv)# bridge domain 1
Router(config-if-srv)# service-policy input policy1

Router(config-if-srv)# end
```

例：EVCのトラフィック クラスおよびトラフィック ポリシー情報の確認

次に、**show policy-map interface service instance** コマンドの出力例を示します。GigabitEthernet インターフェイス 1/1/7 の EFP 用に設定され、EFP に適用される QoS 機能が表示されます。

```
Router# show policy-map interface gigabitethernet 1/1/7 service instance 10
 GigabitEthernet1/1/7: EFP 10
  Service-policy input: multiaction
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      police:
          cir 300000 bps, bc 2000 bytes
        conformed 0 packets, 0 bytes; actions:
          set-prec-transmit 7
          set-qos-transmit 10
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
パケット分類	『Classifying Network Traffic』モジュール
選択的パケット廃棄	「IPv6 Selective Packet Discard」モジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

EVC QoS を設定するための機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19* : ***EVC QoS*** の機能情報

機能名	リリース	機能情報
EVC Quality of Service	Cisco IOS XE リリース 3.3 Cisco IOS リリース 15.5(2)T	このマニュアルでは、イーサネット仮想回線（EVC）で使用する QoS 機能（トラフィックの分類やポリシングなど）をイネーブルにする方法について説明します。 EVC QoS 機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 次のコマンドが導入または変更されました。**service-policy**、**showpolicy-mapinterfaceserviceinstance**。

第 11 章

EtherChannel インターフェイスの QoS

Cisco ASR 1000 シリーズ ルータのイーサネット チャネル（EtherChannel）インターフェイスで Quality of Service（QoS）がサポートされています。QoS 機能は、いくつかの Cisco IOS XE リリースを経て進化しており、ソフトウェア レベル、EtherChannel の設定、および設定したモジュラ QoS CLI（MQC）機能に基づいたさまざまな能力を持っています。

- 機能情報の確認，183 ページ
- EtherChannel の QoS に関する情報，184 ページ
- EtherChannel 用の QoS の設定方法，188 ページ
- EtherChannels の QoS の設定例，209 ページ
- その他の参考資料，211 ページ
- EtherChannel インターフェイスの QoS の機能情報，211 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

EtherChannel の QoS に関する情報

QoS 機能を備えた EtherChannel の進化

EtherChannel は、複数の物理リンクのグループを作成し、スイッチ、ルータ、およびサーバ間に障害耐性と高速リンクを提供するための論理イーサネット リンクを 1 つ作成できるポートチャネル アーキテクチャです。EtherChannel は、2 ～ 8 つのアクティブな高速のギガビットまたは 10 ギガビットのイーサネット ポート間に、他のアクティブなポートに障害が発生したときにアクティブになる 1 ～ 8 つの非アクティブな（フェールオーバー）ポートとともに作成されます。

EtherChannel インターフェイスの QoS は、Cisco IOS XE がリリースされるたびに進化してきました。現在のレベルの Cisco IOS XE ソフトウェアに得られるサポートのレベルと、基礎となる EtherChannel 設定を理解することが重要です。EtherChannel の設定方法に基づいて、QoS のさまざまな組み合わせがサポートされます。EtherChannel は、次の 3 つのモードで設定できます。

- ポートチャネル サブインターフェイスのカプセル化 CLI を使用した EtherChannel VLAN ベースのロード バランシング
- LACP による EtherChannel アクティブ/スタンバイ（EtherChannel のロード バランシングなし）
- LACP によるロード バランシングを備えた EtherChannel

これらの各モデルには、Cisco IOS XE ソフトウェアに含まれるサポートのレベルと、それぞれによって可能な QoS 設定に関する特定の制約があります。

次に、サポートされる EtherChannel と QoS 設定のさまざまな組み合わせをまとめます。設定例は、このドキュメントで後述します。特に併記のない限り、所定の EtherChannel 設定に対する別の論理インターフェイスと物理インターフェイスでのサービス ポリシーの組み合わせはサポートされていません。

ポートチャネル サブインターフェイスのカプセル化 CLI を使用した EtherChannel VLAN ベースのロード バランシング

Cisco IOS XE リリース 2.1 以降のリリースで次がサポートされています。

- ポートチャネル サブインターフェイスでの出力 MQC キューイングの設定
- ポートチャネルのメンバー リンクでの出力 MQC キューイングの設定
- QoS ポリシー集約：サブインターフェイスでの出力 MQC キューイング
- ポートチャネル サブインターフェイスでの入力ポリシングとマーキング
- ポートチャネル メンバー リンクでの出力ポリシングとマーキング

Cisco IOS XE リリース 2.6 以降のリリースで次がサポートされています。

- QoS ポリシー集約：メイン インターフェイスでの複数キュー集約に対する MQC サポート：メイン インターフェイスでの出力 MQC キューイング

LACP による EtherChannel アクティブ/スタンバイ（EtherChannel のロード バランシングなし）

Cisco IOS XE リリース 2.4 以降のリリースで次がサポートされています。

- ポートチャネル メンバー リンクでの出力 MQC キューイング：EtherChannel ロード バランシングなし

LACP による EtherChannel とロード バランシング

Cisco IOS XE リリース 2.5 以降のリリースで次がサポートされています。

- ポートチャネル メンバー リンクでの出力 MQC キューイング設定：EtherChannel ロード バランシング

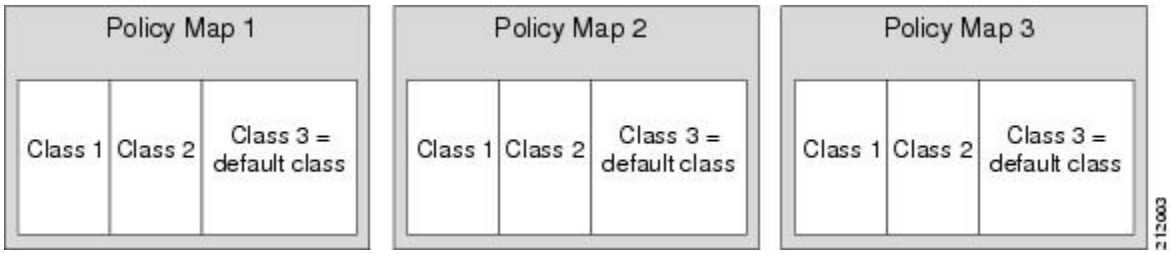
どのリリースでも、出力 QoS 機能はサポートされません。

クラス定義文内のフラグメントについて

QoS ポリシー集約機能は、クラス定義文にフラグメントという発想を取り入れています。ポリシー マップ中で、デフォルト トラフィック クラス定義文をフラグメントとしてマークできます。同じインターフェイス上の他のポリシー マップでも、必要に応じてそのデフォルト トラフィック クラス文をフラグメントとして定義できます。その後、サービスフラグメントクラス定義文を使用して個別のポリシー マップを作成し、すべてのフラグメントに 1 つのグループとして QoS を割り当てるために使用できます。

次の図に、フラグメントを使用していない 3 つのポリシー マップが適用された 1 つの物理インターフェイスの例を示します。各ポリシー マップには、独自のポリシー マップ内でデフォルト トラフィックのトラフィックのみを分類できるデフォルトのトラフィック クラスがあることに注意してください。

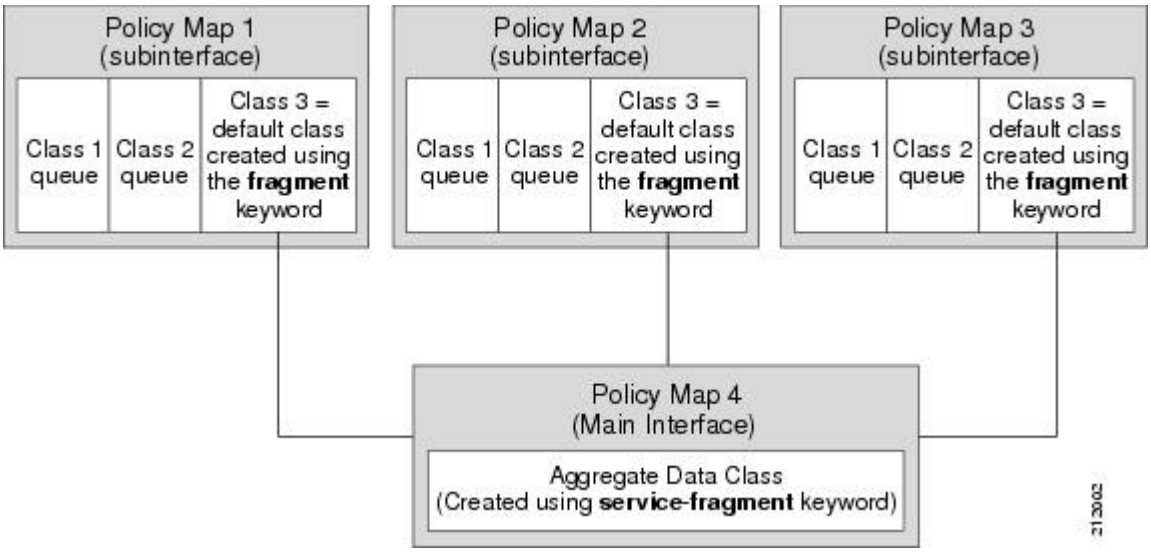
図 *10*：ポリシー マップを持つ物理インターフェイス：フラグメントの使用なし



次の図にフラグメントを使用して設定した同じ設定を示し、フラグメントをまとめて分類するクラス定義文を使用して 4 つめのポリシー マップを追加します。デフォルト トラフィック クラス

は、個々のポリシー マップ内の 3 つの個別のデフォルト トラフィック クラスとしてではなく、1 つのサービス フラグメント グループとして分類されます。

図 *11*：ポリシー マップを持つ物理インターフェイス：フラグメントを使用



Gigabit EtherChannel バンドルのフラグメント

Gigabit Etherchannel バンドルに対してフラグメントを設定すると、**fragment** キーワードを使用して設定したデフォルトのトラフィック クラスを持つポリシーマップがメンバーサブインターフェイスのリンクに適用され、フラグメントをまとめて分類するように **service-fragment** キーワードを使用して設定したトラフィック クラスを持つポリシーマップが物理インターフェイスに適用されます。

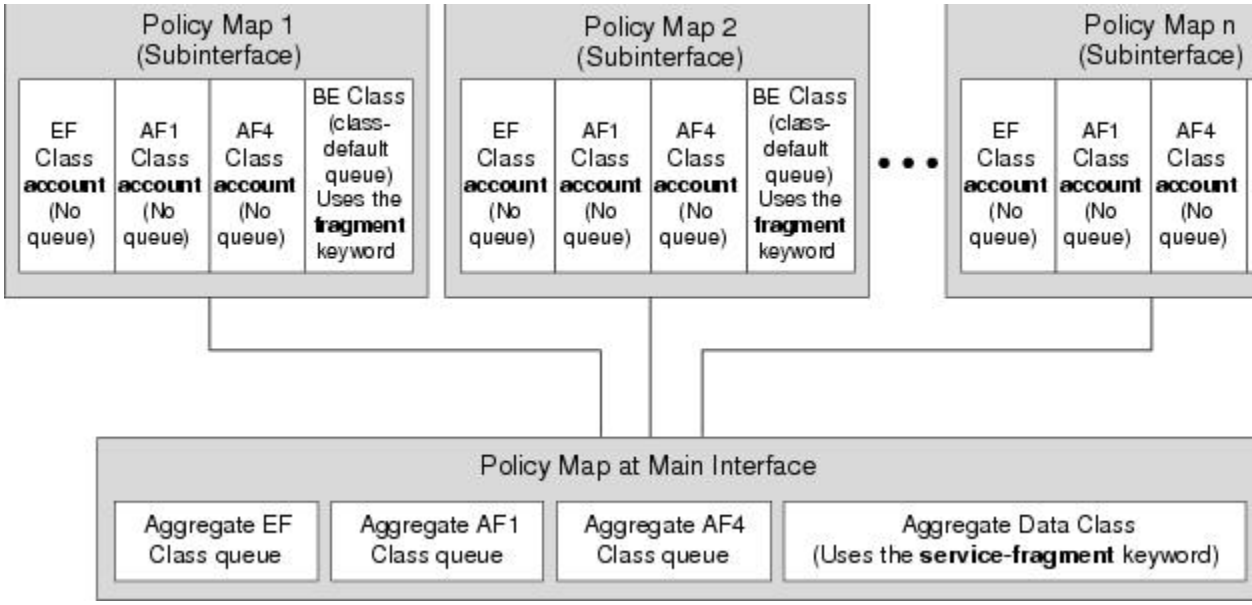
特定のポートチャネルのメンバー リンクで現在アクティブなフラグメントを使用して設定したすべてのポートチャネル サブインターフェイスは、そのメンバー リンクに集約サービス フラグメント クラスを使用します。メンバー リンクがダウンすると、セカンダリ メンバー リンクに切り替わる必要があるポートチャネルのサブインターフェイスは、新しいインターフェイスに集約サービス フラグメントを使用します。

QoS：ポリシー集約 MQC

メイン インターフェイスでの複数キュー集約に対する QoS のポリシー集約 MQC サポート機能は、**フラグメント**の設定と**サービス フラグメント**の設定を使用した class-default トラフィックの以前の集約のサポートを、次の図に示すように、メインインターフェイスのポリシー マップで集約された DSCP ベースのトラフィック クラスなどのサブインターフェイスのポリシー マップ内のユーザ定義の他のトラフィック クラスに拡張します。

キューイングがサブインターフェイスのポリシーマップのトラフィック クラスに設定されていない場合は、**account** コマンドを使用して、これらのクラスの集約レベルで行われるキューイングのドロップを追跡でき、**show policy-map interface** コマンドを使用して表示できます。

図 *12*：メイン インターフェイスでの複数のキュー集約に対する *MQC* サポート機能のポリシー マップの概要



元の機能と複数キューの集約に対するMQCサポートとの違いポリシー集約の違い：サブインターフェイスでの出力 MQC キューイングとメイン インターフェイスでの複数キューの集約に対する MQC サポート

「ポリシー集約：サブインターフェイスでの出力 MQC キューイング」のシナリオと、「メイン インターフェイスでの複数キューの集約に対する MQC サポート：メイン インターフェイスでの出力 MQC キューイング」シナリオ間での設定の一部は同じように見えますが、キューイング動作と内部のデータ処理に重要な違いがあります。「QoS の概要：ポリシーアグリゲーションMQC」の項の図を参照してください。

たとえば、どちらの設定も、サブスクライバ ポリシー マップの **classclass-default** コマンドの **fragment** キーワードを共有し、これを使用する必要があるだけでなく、集約トラフィックに対して共通のポリシー処理を実現するために、メインインターフェイスのポリシーマップのユーザ定義クラスに **service-fragment** キーワードを設定する必要があります。ただし、この設定を使用すると、元の QoS ポリシー集約の実装と、強化された QoS ポリシー集約の実装とでは動作に違いが生じます。

- フラグメントとサービス フラグメント アーキテクチャを使用した元の実装では、すべてのデフォルト クラスのトラフィックと、サブインターフェイスで定義されたキューイング機能を備えていないクラスのすべてのトラフィックが class-default キューに移動し、メイン ポリシーマップで定義されている共通のユーザ定義のキューとポリシーに集約されます。サブイ

ンターフェイスの（同じ物理インターフェイス上の複数のサブスクライバからなどの）トラフィック集約は、最終的には、デフォルト クラスである 1 つのクラスに対してのみ発生します。

- フラグメントとサービス フラグメント機能を使用するメイン インターフェイスでの複数キューの集約に対する MQC サポート機能が強化された実装でも、デフォルトのすべてのクラスのトラフィックも class-default キューに移動し、メイン ポリシー マップで定義された共通のユーザ定義キューとポリシーに集約されます。ただし、集約ポリシーについては、DSCP ベースのサブスクライバ トラフィック クラスなどの他のクラスもサポートされています。これらのトラフィック クラスは、サブスクライバ ポリシー マップの **account** 以外のキューやキューイング機能をサポートしていません。フラグメントとサービス フラグメント アーキテクチャを使用することによって、（同じ物理インターフェイス上の複数のサブスクライバからの）これらの他のサブスクライバ トラフィック クラスがメイン ポリシー マップでこれらの同じクラスに対して定義されている集約トラフィックに対して共通のポリシー処理が実現します。

EtherChannel 用の QoS の設定方法

ポートチャネルのサブインターフェイスでの出力 MQC キューイングの設定

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。EtherChannel 上の選択したプライマリおよびセカンダリの物理インターフェイスに一致するように、適切なカプセル化サブコマンドを使用して、ポートチャネルのサブインターフェイスが設定されている必要があります。Cisco IOS XE リリース 2.1 以降のソフトウェアが必要です。グローバル コンフィギュレーションに **port-channel load-balancing vlan-manual** コマンドが含まれているか、ポートチャネルのメインインターフェイス設定に **load-balancing vlan** コマンドが含まれている必要があります。これらのコマンドがすでに実行済みであると想定しています。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface port-channel***port-channel-number.subinterface-number*
4. **service-policy output***policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number.subinterface-number* 例： `Device(config)# interface port-channel 1.200`	サービス ポリシー設定を受け取るポートチャネルのサブインターフェイスを指定します。
ステップ 4	**service-policy output***policy-map-name* 例： `Device(config-subif)# service-policy output WAN-GEC-sub-Out`	出力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**end** 例： `Device(config-subif)# end`	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、特権 EXEC モードに戻ります。

ポートチャネルのメンバー リンクでの出力 MQC キューイングの設定

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、キューイング機能を使用する 1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。EtherChannel のメンバー リンク インターフェイスがチャネル グループ（EtherChannel グループ）の一部となるようにすでに設定されている必要があります。キューイング コマンドが含まれているポリシー マップを、ポートチャネルのサブインターフェイス上に設定する必要があります。Cisco IOS XE リリース 2.1 以降のソフトウェアが必要です。グローバル コンフィギュレーションに **port-channel load-balancing vlan-manual** コマンド

が含まれているか、ポートチャネルのメインインターフェイス設定に **load-balancing vlan** コマンドが含まれている必要があります。これらのコマンドがすでに実行済みであると想定しています。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface GigabitEthernet***card*/*bay*/*port*
4. **service-policy output***policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface GigabitEthernet***card*/*bay*/*port* 例： `Device(config)# interface GigabitEthernet 0/1/0`	サービス ポリシー設定を受け取るメンバー リンクの物理インターフェイスを指定します。
ステップ 4	**service-policy output***policy-map-name* 例： `Device(config-if)# service-policy output WAN-GEC-sub-Out`	EtherChannel の一部であるこの物理インターフェイスの出力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

QoSのポリシー集約の設定：サブインターフェイスでの出力MQCキューイング

はじめる前に

fragment キーワードをサブインターフェイス **class class-default** の設定と、**service-fragment** 設定をメインインターフェイスクラスに使用するときに、複数のポートチャネルのサブインターフェイスからのデフォルト クラスのトラフィックをメイン インターフェイスの共通ポリシー マップに集約できます。キューイングは、サブインターフェイスのポリシーマップでキューイング機能を使用して定義した他のトラフィック クラスのサブインターフェイスで実行されます。

この機能は、モジュラ QoS CLI（MQC）を使用して設定されます。これは、同じ物理インターフェイスに適用された複数のポリシー マップを、複数のポートチャネルのサブインターフェイスからの複数のデフォルトのトラフィック クラスを集約して扱う QoS 設定で最も有効です。Cisco IOS XE リリース 2.1 以降のソフトウェアが必要です。グローバル コンフィギュレーションに **port-channel load-balancing vlan-manual** コマンドが含まれているか、ポートチャネルのメインインターフェイスに **load-balancing vlan** コマンドが存在している必要があります。これらのコマンドがすでに実行済みであると想定しています。

（注） この機能は、ポリシー マップが複数のポートチャネルのサブインターフェイスとポートチャネルのメンバー リンクのインターフェイスに適用されている場合にサポートされます。この機能を使用して、異なる物理インターフェイス上のポリシーマップのデフォルトのトラフィック クラスをまとめて分類することはできません。ポートチャネルのメンバー リンクがサブインターフェイスでの **encapsulation** コマンドで **primary** ディレクティブまたは **secondary** ディレクティブによって指定された場合に、そのリンクに向かうすべてのトラフィックをまとめて分類できます。すべてのサブインターフェイスのトラフィック クラスにキューが必要です。ただし、キューイング機能（**priority**、**shape**、**bandwidth**、**queue-limit**、**fair-queue**、**random-detect** などのコマンド）を使用してトラフィック クラスがサブインターフェイスのポリシーマップに設定されていない場合、トラフィックは class-default キューに割り当てられます。**フラグメント**と**サービスフラグメント**の設定を使用しないサブインターフェイスのトラフィッククラスに対しては、メインインターフェイスのポリシーマップでの分類は行われず、サポートもされていません。

QoS ポリシー集約機能を完全に設定するには、多段階のプロセスが関わっています。以降の項ではこれらのステップについて詳しく説明します。

ポリシー マップの適用と削除については、次の点に注意してください。

- QoS ポリシー集約を設定するには、**service-fragment** キーワードを含むポリシー マップをメイン インターフェイスに最初に適用してから、**fragment** キーワードを含むポリシー マップをサブインターフェイスに適用する必要があります。
- QoS：ポリシー集約をディセーブルにするには、まず fragment キーワードを含んでいるポリシー マップをサブインターフェイスから削除し、次に service-fragment キーワードを含んでいるポリシー マップをメイン インターフェイスから削除する必要があります。

ポリシー マップでのフラグメント トラフィック クラスの設定

はじめる前に

この手順では、ポリシー マップ内にデフォルト トラフィック クラスをフラグメントとして設定する方法のみを示します。これには、ポリシー マップ内の他のクラスや、デバイス上の他のポリシー マップの設定に関する手順は含まれていません。

例

（注） この例では、Cisco IOS XE リリース 2.6 よりも前のリリースでサポートされている設定例を示します。

次の例では、BestEffort というフラグメントがポリシー マップ subscriber1 とポリシー マップ subscriber 2 に作成されます。この例では、他のトラフィック クラスのキューイング機能はサブインターフェイスのポリシー マップでサポートされます。

```
policy-map subscriber1
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber 2
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

（注） この例では、Cisco IOS XE リリース 2.6 以降のリリースでサポートされている設定を示します。

また、次に、メイン インターフェイスの実装で、複数キューの集約に対する QoS ポリシー集約 MQC サポートを使用して、サブインターフェイスのポリシーマップにデフォルト クラスとして BestEffort というフラグメントを設定する例を示します。この例では、ポリシーマップの他のクラスに対してキューイング機能がサポートされていないことに注意してください。

```
policy-map subscriber1
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
```

```
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

default class ステートメントを複数のサブインターフェイス ポリシー マップにフラグメントとして設定した後、service-fragment キーワードを使用した class ステートメントを持つ個別のポリシー マップを設定し、フラグメントとして設定した class ステートメントに QoS を適用する必要があります。

次の作業

デフォルトの複数の class ステートメントをポリシーマップのフラグメントとして設定した後に、**service-fragment** キーワードを使用して class ステートメントの個別のポリシー マップを設定し、フラグメントとして設定した class ステートメントに QoS を適用する必要があります。

このプロセスについては、「サービス フラグメント トラフィック クラスの設定」の項を参照してください。

サービス フラグメントのトラフィック クラスの設定

はじめる前に

次に、ポリシー マップ内にサービス フラグメント トラフィックの class ステートメントを設定するタスクを示します。サービス フラグメント トラフィック クラスを使用して、他のポリシー マップを以前にフラグメントとして設定した default class ステートメントのコレクションに QoS を適用します。

この手順では、フラグメントのデフォルト トラフィック クラスがすでに作成されていると想定しています。フラグメントのデフォルト トラフィック クラスの作成手順については、「ポリシー マップでのフラグメント トラフィック クラスの設定」の項を参照してください。

すべてのポリシーマップと同様に、設定はインターフェイスに適用されるまで、ネットワーク トラフィックを管理しません。この手順では、インターフェイスへのポリシー マップの適用プロセスは扱いません。

（注） サービス フラグメントを使用すると、同じ物理インターフェイスからのフラグメントのみをまとめて分類できます。同じサービス フラグメントを使用して、別のインターフェイスからのフラグメントを分類することはできません。

service-fragment キーワードが入力されているクラスではキューイング機能だけが許可され、**service-fragment** キーワードが使用されているクラスでは 1 つ以上のキューイング機能を入力する必要があります。

service-fragment キーワードを使用したクラスがあるポリシー マップは、インターフェイスから出て行くトラフィックのみに適用できます（**service-policyoutput** コマンドを使用してインターフェイスに適用したポリシー マップ）。

service-fragment キーワードを使用して設定したクラスは、インターフェイス上にまだ設定されているフラグメントにQoSをまとめて適用するために使用中である場合は削除できません。**service-fragment** キーワードを使用して設定したクラスを削除するには、そのサービス フラグメントを削除する前にフラグメント トラフィックのクラスを削除します。

service-fragment キーワードは、子ポリシー マップに入力できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-name***service-fragment***fragment-class-name*
5. **shapeaveragepercent***percent*
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**policy-map***policy-map-name* 例： `Device(config)# policy-map BestEffortFragments`	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class***class-name***service-fragment***fragment-class-name* 例： `Device(config-pmap)# class data service-fragment BestEffort`	*fragment-class-name* に一致するすべてのフラグメントを合わせたトラフィックのクラスを指定します。他のポリシーマップでフラグメントを定義する場合、サービス フラグメント クラスを正しく設定するには、*fragment-class-name* がこのコマンド ラインの *fragment-class-name* に一致する必要があります。
ステップ 5	**shapeaveragepercent***percent* 例： `Device(config-pmap-c)# shape average percent 50`	QoS コンフィギュレーション コマンドを入力します。フラグメントとして設定されたデフォルトのトラフィック クラスでは、キューイング機能のみがサポートされます。 サポートされているキューイング機能は、**bandwidth**、**shape**、および **random-detectexponential-weighting-constant** です。 複数の QoS キューイング コマンドを入力できます。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	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、特権 EXEC モードに戻ります。

例

（注） この例では、Cisco IOS XE リリース 2.6 よりも前のリリースでサポートされている設定例を示します。

次の例では、BestEffort という名前のすべてのフラグメントに QoS を適用するために、ポリシーマップが作成されます。

```
policy-map main-interface
 class data service-fragment BestEffort
  shape average 400000000
```

次の例では、2 つのフラグメントを作成し、サービス フラグメントを使用してまとめて分類します。

```
policy-map subscriber1
```

```
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber 2
 class voice
  set cos 5
  priority level 1
 class video
  set cos 4
  priority level 2
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
```

（注） この例では、Cisco IOS XE リリース 2.6 以降のリリースでサポートされている設定を示します。

次に、サブ インターフェイス ポリシー マップに BestEffort という 2 つのフラグメントを作成し、BestEffort という**サービス フラグメント**を設定してメイン インターフェイスのポリシー マップでキューを集約する例を示します。

```
policy-map subscriber1
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map subscriber2
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
policy-map main-interface
 class voice
  priority level 1
 class video
  priority level 2
 class AF1
  bandwidth remaining ratio 90
 class data service-fragment BestEffort
  shape average 400000000
  bandwidth remaining ratio 1
```

トラブルシューティングのヒント

同じサービス フラグメントの一部であるすべての class ステートメントが同じフラグメント クラス名を共有していることを確認します。

次の作業

サービス フラグメント トラフィック クラスをメインの物理インターフェイスに適用します。

フラグメント トラフィック クラスをメンバーリンクのサブインターフェイスに適用します。

Gigabit EtherChannel バンドルをサポートする物理インターフェイスでのサービス フラグメントの設定

はじめる前に

この手順では、サービス フラグメント トラフィック クラスがすでに作成されている必要があります。フラグメント クラスを設定しないと、サービス フラグメントのトラフィック クラスは設定できません。フラグメントのクラスを作成する手順については、「ポリシー マップでのフラグメントのトラフィック クラスの設定」の項を参照してください。サービスフラグメントのクラスを作成する手順については、「サービスフラグメントのトラフィック クラスの設定」の項を参照してください。

これらの手順には、Gigabit EtherChannel のメンバー リンクのサブインターフェイスに設定可能なオプションに関する詳細は示されていません。これらの手順では、フラグメントのトラフィック クラスをすでに持っているポリシーマップをメンバー リンクのサブインターフェイスに適用する手順のみが説明されています。

（注） 正しく動作させるには、ポートチャネルのメンバー リンクがダウンしたときに、すべてのメンバー リンクに同じポリシー マップが適用されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface GigabitEthernet***card/bay/port*
4. **service-policyoutput***service-fragment-class-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface GigabitEthernet***card/bay/port* 例： `Device(config)# interface GigabitEthernet 0/1/0`	サービス ポリシー設定を受け取るメンバー リンクの物理インターフェイスを指定します。
ステップ 4	**service-policyoutput***service-fragment-class-name* 例： `Device(config-if)# service-policy output aggregate-member-link`	サービス フラグメントのデフォルトのトラフィック クラスを含むサービス ポリシーを物理ギガビット イーサネット インターフェイスに適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

例

次に、ポリシー マップの集約メンバーリンクを物理インターフェイスに適用する例を示します。

```
interface GigabitEthernet1/1/1
 service-policy output aggregate-member-link
!
interface GigabitEthernet1/1/2
 service-policy output aggregate-member-link
```

次の作業

service-fragment の定義と fragment-class の定義で、フラグメント クラス名が整合していることを確認します。「Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定」の項に進みます。

Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定

はじめる前に

この手順では、サービス フラグメント トラフィック クラスがすでに作成されている必要があります。フラグメント クラスを設定しないと、サービス フラグメントのトラフィック クラスは設定できません。フラグメントのクラスを作成する手順については、「ポリシー マップでのフラグメントのトラフィック クラスの設定」の項を参照してください。サービスフラグメントのクラスを作成する手順については、「サービスフラグメントのトラフィック クラスの設定」の項を参照してください。

これらの手順には、Gigabit EtherChannel のメンバー リンクのサブインターフェイスに設定可能なオプションに関する詳細は示されていません。これらの手順では、フラグメントのトラフィック クラスをすでに持っているポリシーマップをメンバー リンクのサブインターフェイスに適用する手順のみが説明されています。

フラグメントは、2 つ以上の物理インターフェイスのトラフィックに使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface port-channel***port-channel-interface-number***.** *port-channel-subinterface-number*
4. **service-policy output***fragment-class-name*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface port-channel***port-channel-interface-number***.***port-channel-subinterface-number* 例： `Device(config)# interface port-channel 1.100`	サブインターフェイス コンフィギュレーション モードを開始し、EtherChannel メンバー リンクのサブインターフェイスを設定します。
ステップ 4	**service-policy output***fragment-class-name* 例： `Device(config-subif)# service-policy output subscriber`	EtherChannel メンバー リンクのサブインターフェイスに対し、フラグメントのデフォルトのトラフィック クラスが含まれているサービス ポリシーを適用します。
ステップ 5	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

例

次の例では、subscriber というサービス ポリシーにフラグメントのデフォルトのトラフィック クラスがあり、このサービス ポリシーが EtherChannel バンドルのポートチャネルのサブインターフェイスに適用されます。

```
interface port-channel 1.100
 service-policy output subscriber
```

ポートチャネルサブインターフェイスでの入力ポリシングとマーキングの設定

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。EtherChannel のメンバー リンク インターフェイスがチャネル グループ（EtherChannel グループ）の一部となるようにすでに設定されている必要があります。Cisco IOS XE リリース 2.1 以降のソフトウェアが必要です。グローバル コンフィギュレーションに **port-channel load-balancing vlan-manual** コマンドが含まれているか、ポートチャネルのメインインターフェイス設定に **load-balancing vlan** コマンドが含まれている必要があります。これらのコマンドがすでに実行済みであると想定しています。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface port-channel***port-channel-number.port-channel-interface-number.sub-interface-number*
4. **service-policy input***policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number.port-channel-interface-number.sub-interface-number* 例： `Device(config)# interface port-channel 1.100.100`	サブインターフェイス コンフィギュレーション モードを開始し、EtherChannel メンバー リンクのサブインターフェイスを設定します。
ステップ 4	**service-policy input***policy-map-name* 例： `Device(config-subif)# service-policy input sub-intf-input`	以前に指定したポートチャネルのサブインターフェイスの入力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

例

次の例では、sub-intf-input という名前のサービス ポリシーを定義し、そのポリシーをポートチャネルのサブインターフェイスの入力方向に適用します。

```
policy-map sub-intf-input
  class voice
    set precedence 5
  class video
    set precedence 6
  class class-default
    set precedence 3
!
interface Port-channel 1.100
 service-policy input sub-intf-input
```

ポートチャネルのメンバーリンクでの出力ポリシングとマーキングの設定

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。EtherChannel のメンバー リンク インターフェイスがチャネル グループ（EtherChannel グループ）の一部となるようにすでに設定されている必要があります。Cisco IOS XE リリース 2.1 以降のソフトウェアが必要です。グローバル コンフィギュレーションに **port-channel load-balancing vlan-manual** コマンドが含まれているか、ポートチャネルのメインインターフェイス設定に **load-balancing vlan** コマンドが含まれている必要があります。これらのコマンドがすでに実行済みであると想定しています。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface port-channel***port-channel-number.port-channel-interface-number.sub-interface-number*
4. **service-policy output***policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel***port-channel-number.port-channel-interface-number.sub-interface-number* 例： `Device(config)# interface port-channel 1.100.100`	サブインターフェイス コンフィギュレーション モードを開始し、EtherChannel メンバー リンクのサブインターフェイスを設定します。

ステップ 4	**service-policy output***policy-map-name*
	
	例：
	
	`Device(config-subif)#`
	`service-policy output WAN-GEC-member-Out-police`
		前のステップで指定した EtherChannel メンバー リンクのサブインターフェイスの出力トラフィックに適用するサービス ポリシーの名前を指定します。

ステップ 5	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

例

次の例では、WAN-GEC-member-Out-police という名前のサービス ポリシーを定義し、ポートチャネルのサブインターフェイスの出力方向に適用します。

```
policy-map WAN-GEC-member-Out-police
  class voice
    set precedence 5
  class video
    set precedence 6
  class class-default
    set precedence 3
!
interface port-channel 1.100
 service-policy output WAN-GEC-member-Out-police
```

ポリシー集約の設定：メインインターフェイスでの複数キュー集約に対する MQC サポート

はじめる前に

この機能は MQC を使用して設定されます。これは、同じ物理インターフェイスに適用された複数のポリシー マップを、複数のポートチャネルのサブインターフェイスからの複数のユーザ定義のトラフィック クラスを集約して扱う QoS 設定で最も有効です。Cisco IOS XE リリース 2.6 以降のソフトウェアが必要です。グローバル コンフィギュレーションには **port-channel load-balancing vlan-manual** コマンドが含まれている必要があります。または、設定するポートチャネルのメインインターフェイスに **port-channel load-balancing vlan** コマンドが存在している必要があります。これらのコマンドがすでに実行済みであると想定しています。

この機能は、ポリシー マップが複数のポートチャネルのサブインターフェイスとポートチャネルのメンバー リンクのインターフェイスに適用されている場合にサポートされます。この機能を使用して、異なる物理インターフェイス上のポリシーマップのデフォルトのトラフィック クラスをまとめて分類することはできません。ポートチャネルのメンバー リンクがサブインターフェイスでの **encapsulation** コマンドで **primary** ディレクティブまたは **secondary** ディレクティブによって指定された場合に、そのリンクに向かうすべてのトラフィックをまとめて分類できます。次の項で、EtherChannel によるこのタイプの QoS ポリシー集約を設定する際の動作と制約事項を説明します。

- 設定されたキューイング機能がないサブインターフェイスのトラフィック クラスには、サブスクライバ レベルのキューがありません。
- **fragment** キーワードをサブインターフェイス **class**class-default の設定と、**service-fragment** 設定をメイン インターフェイス クラスで使用するときに、複数のサブインターフェイスからのデフォルト クラスのトラフィックをメイン インターフェイスの共通ポリシー マップに集約できます。
- この設定ではさらに、メインインターフェイスの共通ポリシーマップに集約する他のサブインターフェイスのトラフィック クラス（DSCP ベースのクラスなど）に対するサポートをイネーブルにします。
- **fragment** キーワードをサブインターフェイスの **class-default** クラスに使用し、**service-fragment** 設定をメイン インターフェイス クラスに使用することで、この機能がイネーブルになります（これは、デフォルト クラスの集約もイネーブルにします）。
- キューイング機能は、他のトラフィック クラスのサブインターフェイスのポリシー マップでは設定されません。
- 他のサブインターフェイスのトラフィック クラスについては、メインインターフェイスのポリシー マップで集約としてキューイングが実行されます。
- 統計情報の任意のトラッキングをサポートするには、サブインターフェイスのポリシーマップに **account** コマンドを使用します。

メインインターフェイでの QoS の複数キュー集約機能を完全に設定するには、次に示すように多段階のプロセスが関わっています。

1. 「ポリシー マップでのフラグメント トラフィック クラスの設定」の項で説明した複数のサブインターフェイスのポリシー マップ内にフラグメントとして default class ステートメントを設定します。
2. 「サービス フラグメントのトラフィック クラスの設定」の項で説明したように、フラグメントとして設定した class ステートメントに QoS を適用するために、**service-fragment** キーワードを使用して、class ステートメントで個別のポリシー マップを設定します。
3. 「Gigabit EtherChannel バンドルをサポートする物理インターフェイスでのサービス フラグメントの設定」の項で説明したように、サービス フラグメントのトラフィック クラスを設定し、それらをメインの物理インターフェイスに適用します。
4. 「Gigabit EtherChannel メンバー リンクのサブインターフェイスでのフラグメントの設定」の項で説明したように、フラグメント トラフィックのクラスを設定し、それらをメンバー リンクのサブインターフェイスに適用します。

ポートチャネルのメンバー リンクでの MQC キューイング設定：EtherChannel ロード バランシングなし

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。

Cisco IOS XE リリース 2.4 以降のソフトウェアが必要です。

また、ポートチャネル メイン インターフェイスにアクティブ/スタンバイ シナリオを作成する次のコマンドが含まれている必要があります。このような設定では、1 つのインターフェイスのみをアクティブにすることで、トラフィックをいつでも転送できます。

- **interface Port-channel1**
- **lacp fast-switchover**
- **lacp max-bundle 1**

手順の概要

1. **enable**
2. **configureterminal**
3. **interface GigabitEthernet***card*/*bay*/*port*
4. **service-policy output***policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface GigabitEthernet***card/bay/port* 例： `Device(config)# interface GigabitEthernet 0/1/0`	サービス ポリシー設定を受け取るメンバー リンクの物理インターフェイスを指定します。
ステップ 4	**service-policy output***policy-map-name* 例： `Device(config-if)# service-policy output WAN-GEC-member-Out`	出力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

例

次に、main-intf というサービス ポリシーを定義して、ポートチャネルのメンバー リンクの出力方向に適用する例を示します。

```
interface Port-channel 1
 lcap fast-switchover
 lacp max-bundle 1
!
policy-map main-intf
 class voice
  priority
  police cir 10000000
 class video
  bandwidth remaining ratio 10
 class class-default
  bandwidth remaining ratio 3
```

```
!
interface GigabitEthernet0/0/0
 channel-group 1 mode active
 service-policy output main-intf
!
interface GigabitEthernet0/0/1
 channel-group 1 mode active
 service-policy output main-intf
```

ポートチャネルのメンバーリンクでのMQCキューイング設定の設定：EtherChannel ロード バランシング

はじめる前に

class-map コマンドを使用してトラフィック クラスが設定されている必要があります。以前に定義したクラス マップを使用して、1 レベルまたは 2 レベルの階層型ポリシーマップを設定する必要があります。EtherChannel 上の選択したプライマリおよびセカンダリの物理インターフェイスに一致するように、適切なカプセル化サブコマンドを使用して、ポートチャネルのサブインターフェイスが設定されている必要があります。Cisco IOS XE リリース 2.5 以降のソフトウェアが必要です。

EtherChannel の設定には、フローベースのロードバランシングをイネーブルにした複数のアクティブなインターフェイスがある場合があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface GigabitEthernet***card*/*bay*/*port*
4. **service-policy output***policy-map-name*
5. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface GigabitEthernet***card*/*bay*/*port* 例： `Device(config)# interface GigabitEthernet 0/1/0`	サービス ポリシー設定を受け取るメンバー リンクの物理インターフェイスを指定します。
ステップ 4	**service-policy output***policy-map-name* 例： `Device(config-if)# service-policy output WAN-GEC-member-Out`	出力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

例

次に、main-intf というサービス ポリシーを定義して、ポートチャネルのメンバー リンクの出力方向に適用する例を示します。

```
  class voice
   priority
   police cir 10000000
  class video
   bandwidth remaining ratio 10
  class class-default
   bandwidth remaining ratio 3
!
interface GigabitEthernet0/0/0
 channel-group 1 mode active
 service-policy output main-intf
!
interface GigabitEthernet0/0/1
 channel-group 1 mode active
 service-policy output main-intf
```

EtherChannels の QoS の設定例

例：QoS ポリシー集約の設定：サブインターフェイスでの出力 MQC キューイング

```
port-channel load-balancing vlan-manual
!
class-map match-all BestEffort
!
class-map match-all video
 match precedence 4
!
class-map match-all voice
 match precedence 5
!
policy-map subscriber
 class voice
  priority level 1
 class video
  priority level 2
 class class-default fragment BE
  shape average 100000000
  bandwidth remaining ratios 80

policy-map aggregate-member-link
 class BestEffort service-fragment BE
 shape average 100000000
!
interface Port-channel1
 ip address 209.165.200.225 255.255.0.0
!
interface Port-channel1.100
 encapsulation dot1Q 100
 ip address 209.165.200.226 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.200
 encapsulation dot1Q 200
 ip address 209.165.200.227 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 209.165.200.228 255.255.255.0
 service-policy output subscriber
!
interface GigabitEthernet1/1/1
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
!
interface GigabitEthernet1/1/2
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
```

例：QoSポリシー集約の設定：メインインターフェイスでの複数キュー集約に対する MQC サポート

```
port-channel load-balancing vlan-manual
!
policy-map subscriber1
 class voice
  set cos 5
  account
 class video
  set cos 4
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
!
policy-map subscriber2
 class voice
  set cos 2
  account
 class video
  set cos 3
  account
 class AF1
  account
 class class-default fragment BestEffort
  shape average 200000000
  bandwidth remaining ratio 10
!
policy-map main-interface-out
 class voice
  priority level 1
 class video
  priority level 2
 class AF1
  bandwidth remaining ratio 90
 class data service-fragment BestEffort
  shape average 400000000
  bandwidth remaining ratio 1
!
interface GigabitEthernet1/1/1
 no ip address
 channel-group 1 mode on
 service-policy output main-interface-out
!
interface GigabitEthernet1/1/2
 no ip address
 channel-group 1 mode on
 service-policy output main-interface-out
!
interface Port-channel1.100
 encapsulation dot1Q 100
 ip address 10.0.0.1 255.255.255.0
 service-policy output subscriber1
!
interface Port-channel1.200
 encapsulation dot1Q 200
 ip address 10.0.0.2 255.255.255.0
 service-policy output subscriber2
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.0.0.4 255.255.255.0
 service-policy output subscriber2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
モジュラ QoS コマンドライン インターフェイス	「Applying QoS Features Using the MQC」モジュール
RADIUS ベースのポリシングの設定	『*Intelligent Services Gateway Configuration Guide*』
CISCO ASR 1000 シリーズ ソフトウェアの設定	『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

EtherChannel インターフェイスの QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20*：*EtherChannel* インターフェイスの *QoS* の機能情報

機能名	リリース	機能情報
ポートチャネル サブインターフェイスでの出力 MQC キューイングの設定	Cisco IOS XE リリース 2.1	この機能は、ポートチャネルのサブインターフェイスでの出力 MQC キューの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
ポートチャネルのメンバー リンクでの出力 MQC キューイングの設定	Cisco IOS XE リリース 2.1	この機能は、ポートチャネルのメンバー リンクで出力 MQC キューの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
QoS のポリシー集約：サブインターフェイスでの出力 MQC キューイング	Cisco IOS XE リリース 2.1	この機能は、 QoS ポリシー集約のサブインターフェイスでの出力 MQC の設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
ポートチャネル サブインターフェイスでの入力ポリシングとマーキング	Cisco IOS XE リリース 2.1	この機能は、ポートチャネルのサブインターフェイスでの入力ポリシングとマーキングの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

機能名	リリース	機能情報
ポートチャネル メンバー リンクでの出力ポリシングとマーキング	Cisco IOS XE リリース 2.1	この機能は、ポートチャネルのメンバー リンクでの出力 MQC ポリシングとマーキングの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
ポートチャネル メンバー リンクでの出力 MQC キューイング設定：EtherChannel ロードバランシングなし	Cisco IOS XE リリース 2.4	この機能は、ポートチャネルのメンバー リンクでの（EtherChannel ロードバランシングなしの）出力 MQC キューイングをサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
ポートチャネル メンバー リンクでサポートされる出力 MQC キューイング設定：EtherChannel ロードバランシング	Cisco IOS XE リリース 2.5	この機能は、ポートチャネルのメンバー リンクでの（EtherChannel ロードバランシングありの）出力 MQC キューイングをサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
QoS ポリシー集約：メイン インターフェイスでの複数キュー集約に対する MQC サポート：メイン インターフェイスでの出力 MQC キューイング	Cisco IOS XE リリース 2.6	この機能は、QoS ポリシー集約、メイン インターフェイスでの複数キュー集約に対する MQC サポート、メイン インターフェイスでの出力 MQC キューイングの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

第 12 章

集約 EtherChannel QoS

集約 EtherChannel の QoS 機能を使用すると、ポートチャネルのメイン インターフェイスまたはサブインターフェイス上に集約出力キューイング ポリシー マップを適用できます。この機能によって、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに対する集約ポートチャネルのメイン インターフェイス上での QoS サポートが可能になります。

- 集約 EtherChannel QoS の制約事項，215 ページ
- 集約 EtherChannel QoS に関する情報，216 ページ
- 集約 EtherChannel QoS の設定方法，217 ページ
- 集約 EtherChannel QoS の設定解除方法，219 ページ
- 集約 EtherChannel QoS の設定例，219 ページ
- 集約 EtherChannel サブインターフェイス QoS の設定方法，221 ページ
- 集約 EtherChannel サブインターフェイス QoS の設定解除方法，223 ページ
- 集約 EtherChannel サブインターフェイス QoS の設定例，224 ページ
- その他の参考資料，225 ページ
- 集約 EtherChannel QoS の機能情報，226 ページ

集約 EtherChannel QoS の制約事項

- 集約ポートチャネル インターフェイスを持つイーサネット仮想回線（EVC）上での QoS の設定はサポートされていません。
- 集約ポートチャネルインターフェイス上でのインテリジェントサービスゲートウェイ（ISG）およびインテリジェント ワイヤレス アクセス ゲートウェイ（iWAG）のコンテキストでの Point-to-Point Protocol over Ethernet（PPPoE）セッションと IP over Ethernet（IPoE）セッションはサポートされていません。

- 集約ポートチャネル インターフェイス上での QoS を備えた仮想プライベート LAN サービス（VPLS）はサポートされていません。
- 集約ポートチャネル インターフェイス上での QoS を備えた Xconnect はサポートされていません。
- モジュラ QoS CLI（MQC）の fragment キーワードと service-fragment キーワードは、集約ポート チャネル インターフェイス タイプと組み合わせて使用できません。
- 集約型ポートチャネル インターフェイスには次の制限があります。
  - ポート チャネルのすべてのメンバー リンクの速度は同じである必要があります。これにより、パケットの再順序付けの可能性を回避します。ギガビット イーサネット、ファスト イーサネット、またはイーサネット インターフェイスを同じポート チャネルに組み合わせることはできません。
- 集約ポートチャネルのメイン インターフェイスとポートチャネルのサブインターフェイスの両方に適用された MPOL ポリシーはサポートされていません。
- 集約ポートチャネルのメイン インターフェイスが QoS で設定されている場合は、メンバー リンクでの QoS はサポートされていません。

集約 EtherChannel QoS に関する情報

集約 EtherChannel QoS のサポート対象機能

集約 EtherChannel QoS 機能は、次をサポートします。

- フローベースのロード バランシング
- 最大 3 レベルの階層
- シェーピング、絶対帯域幅、および相対帯域幅の設定
- サブクラス（VLAN）の最小帯域幅量
- 集約ポートチャネルのメイン インターフェイス上で同時にイネーブルになる入力 QoS（ポリシングおよびマーキング）と出力 QoS（すべてのキューイング機能）
- 集約ポートチャネルのサブインターフェイス上で同時にイネーブルになる入力 QoS（ポリシングおよびマーキング）と出力 QoS（すべてのキューイング機能）

集約 EtherChannel QoS のサポート対象外機能の組み合わせ

QoS を備えた次のトンネル タイプ インターフェイスの次の組み合わせはサポートされていません。

- 集約キューイングを備えたポート チャネル経由で出力するキューイング ポリシー マップが適用された Generic Routing Encapsulation（GRE）トンネル
- 集約キューイングによってポート チャネル経由で出力するキューイング QoS が適用された静的仮想トンネル インターフェイス（SVTI）および動的仮想トンネル インターフェイス（DVTI）
- 集約キューイングを備えたポート チャネル経由で出力するキューイング QoS が適用された Dynamic Multipoint VPN（DMVPN）トンネル
- サービス グループに属しているサブインターフェイスと、サービスポリシーが適用されたサブインターフェイスは、同じ集約ポートチャネル上では同時に設定できない
- MPOL：集約ポートチャネルのメイン インターフェイスとポートチャネルのサブインターフェイスの両方に適用されたポリシー

（注） キューイング QoS のないトンネル（前述）はサポートされていますが、IP アドレスに十分なダイバーシティがない所定の物理インターフェイスをハッシング アルゴリズムが過負荷にするため、推奨しません。

集約 EtherChannel QoS のスケーラビリティ

QoS ポリシーは、次のスケーラビリティの制限に従って、集約ポートチャネル インターフェイスに適用できます。

- 最大 8 個の ポート アドレス
- ポート チャネル内で最大 4 個のメンバー リンク
- メンバー リンクは複数の共有ポート アダプタ（SPA）と SPA インターフェイス プロセッサ（SIP）カードに分割可能

集約 EtherChannel QoS の設定方法

ここでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで集約 EtherChannel QoS を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **platform qos port-channel-aggregate***port-channel-number*
4. **interface port-channel***port-channel-number*
5. **service-policy** {**output**}*policy-map*
6. **service-policy** {**input**}*policy-map*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**platform qos port-channel-aggregate***port-channel-number* 例： `router(config)# platform qos port-channel-aggregate 1`	集約ポートチャネル インターフェイスをイネーブルにします。
ステップ 4	**interface port-channel***port-channel-number* 例： `router(config)# interface port-channel 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、特定のポート チャネルを設定します。
ステップ 5	**service-policy** {**output**}*policy-map* 例： `router(config-if)# service-policy output egress_policy`	ポリシー マップを出力インターフェイスに適用し、このインターフェイスでサービス ポリシーとして使用されるようにします。
ステップ 6	**service-policy** {**input**}*policy-map* 例： `router(config-if)# service-policy input ingress_policy`	インターフェイスのサービス ポリシーとして使用するポリシー マップを入力インターフェイスに付加します。

集約 EtherChannel QoS の設定解除方法

ここでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで集約 EtherChannel QoS の設定を解除する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no interface port-channel***port-channel-number*
4. **no platform qos port-channel-aggregate***port-channel-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**no interface port-channel***port-channel-number* 例： `router(config)# no interface port-channel 1`	特定のポート チャネルの設定を解除します。
ステップ 4	**no platform qos port-channel-aggregate***port-channel-number* 例： `router(config)# no platform qos port-channel-aggregate 1`	集約ポートチャネルインターフェイスをディセーブルにし、そのインターフェイスにある必要なQoSポリシーを削除します。

集約 EtherChannel QoS の設定例

例：集約ポートチャネル インターフェイスの設定

```
Router# configure terminal
```

```
Router(config)# platform qos port-channel-aggregate 1
Router(config)# interface port-channel 1
Router(config-if)# interface GigabitEthernet1/0/1
Router(config-if)# channel-group 1
Router(config-if)# interface GigabitEthernet1/0/0
Router(config-if)# channel-group 1
Router(config-if)# interface port-channel 1.1
Router(config-subif)# encap
Router(config-subif)# encapsulation dot
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip addr 14.0.1.2 255.255.255.0
Router(config-subif)# interface port-channel 1.2
Router(config-subif)# encapsulation dot1Q 3
Router(config-subif)# ip addr 14.0.2.2 255.255.255.0
Router(config-subif)# interface port-channel 1.3
Router(config-subif)# encapsulation dot1Q 4
Router(config-subif)# ip addr 14.0.3.2 255.255.255.0
Router(config-subif)# end
```

例：QoS に対するクラス マップの設定

```
Router# configure terminal
Router(config)# class-map vlan_2
Router(config-cmap)# match vlan  2
Router(config-cmap)# class-map vlan_3
Router(config-cmap)# match vlan  3
Router(config-cmap)# class-map vlan_4
Router(config-cmap)# match vlan  4
Router(config-cmap)# class-map prec1
Router(config-cmap)# match precedence 1
Router(config-cmap)# class-map prec2
Router(config-cmap)# match precedence 2
Router(config-cmap)# class-map prec3
Router(config-cmap)# match precedence 3
Router(config-cmap)# class-map prec4
Router(config-cmap)# match precedence 4
Router(config-cmap)# end
```

例：QoS に対するポリシー マップの設定

```
Router# configure terminal
Router(config)# policy-map child-vlan
Router(config-pmap)# class prec1
Router(config-pmap-c)# police cir percent 20
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# class prec2
Router(config-pmap-c)# police cir percent 40
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# class prec3
Router(config-pmap-c)# bandwidth remaining ratio 3
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 1
Router(config-pmap-c)# random-detect
Router(config-pmap-c)#!
Router(config-pmap-c)# policy-map egress_policy
Router(config-pmap)# class vlan_2
Router(config-pmap-c)# shape average 100000000
Router(config-pmap-c)# service-policy child-vlan
Router(config-pmap-c)# class vlan_3
Router(config-pmap-c)# shape average 200000000
Router(config-pmap-c)# service-policy child-vlan
Router(config-pmap-c)# class vlan_4
Router(config-pmap-c)# shape average 300000000
```

```
Router(config-pmap-c)# service-policy child-vlan
Router(config-pmap-c)#!
Router(config-pmap-c)# policy-map ingress_policy
Router(config-pmap)# class vlan_2
Router(config-pmap-c)# police cir 80000000
Router(config-pmap-c-police)# conform-action set-prec-transmit 1
Router(config-pmap-c-police)# class vlan_2
Router(config-pmap-c)# set dscp AF21
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# set dscp 0
Router(config-pmap-c)# end
```

例：ポート チャネル インターフェイスへの QoS の適用

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# service-policy output egress_policy
Router(config-if)# service-policy input ingress_policy
Router(config-if)# end
```

集約 EtherChannel サブインターフェイス QoS の設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **platform qos port-channel-aggregate***port-channel-number*
4. **interface port-channel***port-channel-number*
5. **interface port-channel***port-channel-number.subinterface-number*
6. **service-policy** {**output**}*policy-map*
7. **service-policy** {**input**}*policy-map*
8. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**platform qos port-channel-aggregate***port-channel-number* 例： `Device(config)# platform qos port-channel-aggregate 1`	集約ポートチャネル インターフェイスをイネーブルにします。
ステップ 4	**interface port-channel***port-channel-number* 例： `Device(config)# interface port-channel 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、特定のポート チャネルを設定します。
ステップ 5	**interface port-channel***port-channel-number.subinterface-number* 例： `Device(config)# interface port-channel 1.2`	インターフェイス コンフィギュレーション モードを開始し、特定のポートチャネルサブインターフェイスを設定します。
ステップ 6	**service-policy** {**output**}*policy-map* 例： `Device(config-if)# service-policy output egress_policy`	ポリシー マップを出力インターフェイスに適用し、このインターフェイスでサービス ポリシーとして使用されるようにします。
ステップ 7	**service-policy** {**input**}*policy-map* 例： `Device(config-if)# service-policy input ingress_policy`	インターフェイスのサービス ポリシーとして使用するポリシー マップを入力インターフェイスに付加します。
ステップ 8	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。

集約 EtherChannel サブインターフェイス QoS の設定解除方法

手順の概要

1. **enable**
2. **configure terminal**
3. **no interface port-channel***port-channel-number.subinterface*
4. **no platform qos port-channel-aggregate***port-channel-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no interface port-channel***port-channel-number.subinterface* 例： `Device(config)# no interface port-channel 1.2`	特定のポート チャネルのサブインターフェイスの設定を解除します。
ステップ 4	**no platform qos port-channel-aggregate***port-channel-number* 例： `Device(config)# no platform qos port-channel-aggregate 1`	集約ポートチャネル インターフェイスをディセーブルにし、そのインターフェイスにある必要な QoS ポリシーを削除します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。

集約 EtherChannel サブインターフェイス QoS の設定例

例：集約ポートチャネルインターフェイスとサブインターフェイスの設定

```
Device# configure terminal
Device(config)# platform qos port-channel-aggregate 2
Device(config)# interface port-channel 2
Device(config-if)# interface GigabitEthernet1/1/1
Device(config-if)# channel-group 2
Device(config-if)# interface GigabitEthernet1/1/0
Device(config-if)# channel-group 2
Device(config-if)# interface port-channel 2.200
Device(config-subif)# encapsulation dot1Q 200
Device(config-subif)# ip addr 15.0.1.2 255.255.255.0
Device(config-subif)# interface port-channel 2.300
Device(config-subif)# encapsulation dot1Q 300
Device(config-subif)# ip addr 15.0.2.2 255.255.255.0
Device(config-subif)# end
```

例：QoS に対するクラス マップの設定

```
Device# configure terminal
Device(config)# class-map vlan_2
Device(config-cmap)# match vlan  2
Device(config-cmap)# class-map vlan_3
Device(config-cmap)# match vlan  3
Device(config-cmap)# class-map vlan_4
Device(config-cmap)# match vlan  4
Device(config-cmap)# class-map prec1
Device(config-cmap)# match precedence 1
Device(config-cmap)# class-map prec2
Device(config-cmap)# match precedence 2
Device(config-cmap)# class-map prec3
Device(config-cmap)# match precedence 3
Device(config-cmap)# class-map prec4
Device(config-cmap)# match precedence 4
Device(config-cmap)# end
```

例：QoS に対するポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map subinterface_child
Device(config-pmap)# class prec1
Device(config-pmap-c)# police cir percent 30
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# class prec2
Device(config-pmap-c)# police cir percent 30
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# class prec3
Device(config-pmap-c)# bandwidth remaining ratio 3
Device(config-pmap-c)# class class-default
Device(config-pmap-c)# bandwidth remaining ratio 1
Device(config-pmap-c)#!
```

```
Device(config-pmap-c)# policy-map sub_egress_policy
Device(config-pmap-c)# class class-default
Device(config-pmap-c)# shape average 300000000
Device(config-pmap-c)# service-policy subinterface_child
Device(config-pmap-c)#!
Device(config-pmap-c)# policy-map sub_ingress_policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# police cir 80000000
Device(config-pmap-c)# end
```

例：ポート チャネル サブインターフェイスへの QoS の適用

```
Device# configure terminal
Device(config)# interface port-channel 2.200
Device(config-if)# service-policy output egress_policy
Device(config-if)# service-policy input ingress_policy
Device(config)# interface port-channel 2.300
Device(config-if)# service-policy output egress_policy
Device(config-if)# service-policy input ingress_policy
Device(config-if)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

集約 EtherChannel QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：集約 *EtherChannel QoS* の機能情報

機能名	リリース	機能情報
集約 EtherChannel QoS	Cisco IOS XE リリース 3.12S	この機能は、Cisco IOS XE リリース 3.12S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
集約 GEC QoS 10G のサポート	Cisco IOS XE リリース 3.16.3S Cisco IOS XE Denali 16.3.1	この機能は、Cisco IOS XE リリース 3.16.3S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。

機能名	リリース	機能情報
ASR1k の GEC ポートチャネルでの QoS	Cisco IOS XE リリース 3.16.3S Cisco IOS XE Denali 16.3.1	この機能は、Cisco IOS XE リリース 3.16.3S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。

第 13 章

PPPoGEC のセッション単位の QoS

PPPoGEC セッション単位の QoS 機能は、PPPoE /L2TP 環境（ブロードバンドの導入）内の PPP Termination and Aggregation（PTA）デバイス、L2TP アクセス コンセントレータ（LAC）デバイス、または L2TP ネットワーク サーバ（LNS）デバイス上での PPPoE セッションの特定の QoS ポリシーの設定をサポートします。PPPoE/L2TP 環境内で PTA デバイス、LAC デバイス、または LNS デバイスとして機能する Cisco ASR 1000 シリーズ ルータでは、EtherChannel アクティブ/スタンバイ機能による PPPoE セッションもサポートされています。

- 機能情報の確認，229 ページ
- PPPoGEC のセッション単位の QoS について，230 ページ
- PPPoGEC のセッション単位の QoS の設定方法，231 ページ
- PPPoGEC のセッション単位の QoS の設定例，232 ページ
- PPPoGEC のセッション単位の QoS のその他の参考資料，233 ページ
- PPPoGEC のセッション単位の QoS の機能情報，234 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

PPPoGEC のセッション単位の QoS について

PPPoGEC のセッション単位の QoS に関する制約事項

- QoS ポリシー マップは、メンバー リンク、ポートチャネルのメイン インターフェイス、または QoS を備えた PPPoE セッション用の送信パスと関連付けられたポートチャネル サブインターフェイス上には設定できません。

アクティブ/スタンバイ EtherChannel による PPPoGEC

アクティブ/スタンバイ EtherChannel による PPPoE セッションは 1 レベルまたは 2 レベルの階層型出力ポリシー マップを（キューイング設定を使用して）サポートし、また、フラット入力ポリシーマップも（キューイング設定なしで）サポートします。ポリシーマップは、以前に定義されたクラス マップを使用して設定されます。**class-map** コマンドを使用してトラフィック クラスが設定されている必要があります。

出力階層型ポリシー マップと入力ポリシー マップは、次のいずれかの方法で PPPoE セッションに関連付けることができます。

- 仮想テンプレート インターフェイスでの構成時の設定
- 認証、認可、およびアカウンティング（AAA）モデルで設定した外部ツール（RADIUS サーバなど）を使用したダイナミックな構成時設定。詳細については、『*Intelligent Services Gateway Configuration Guide*』と『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』を参照してください。

ポートチャネル メイン インターフェイスにアクティブ/スタンバイ シナリオを作成する次のコマンドが含まれている必要があります。このような設定では、1 つのインターフェイスのみをアクティブにすることで、トラフィックをいつでも転送できます。

- **interface port-channel1**
- **lacp fast-switchover**
- **lacp max-bundle 1**

PPPoGEC のセッション単位の QoS の設定方法

EtherChannel アクティブ/スタンバイによる PPPoE セッションでの QoS の設定

PPPoE セッションに QoS を設定するには、EtherChannel インターフェイスの PPP セッションに使用する仮想テンプレートを指定し、入力トラフィックに適用するサービス ポリシーの名前を指定し、出力トラフィックを指定する必要があります。この設定では、仮想テンプレート インターフェイスを定義することによって、出力階層型ポリシー マップと入力ポリシー マップを PPPoE セッションに関連付ける方法を示します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface virtual-template** *number*
4. **service-policy output***policy-map-name*
5. **service-policy input***policy-map-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface virtual-template** *number* 例： `Device(config)# interface virtual-template 99`	バーチャル アクセス インターフェイスの作成で動的に設定して適用できるバーチャル テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。 • EtherChannel インターフェイスの PPP セッションに使用する仮想テンプレートを指定します。

	コマンドまたはアクション	目的
ステップ 4	**service-policy output***policy-map-name* 例： `Device(config-if)# service-policy output session_parent`	出力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 5	**service-policy input***policy-map-name* 例： `Device(config-if)# service-policy input session_ingress`	入力トラフィックに適用するサービス ポリシーの名前を指定します。
ステップ 6	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

PPPoGEC のセッション単位の QoS の設定例

例：EtherChannel アクティブ/スタンバイによる PPPoE セッションでの QoS

次の例に、session_parent 階層型ポリシー マップと session_ingress ポリシー マップを示します。これらのポリシー マップは、**service-policy** コマンドを使用して仮想テンプレート インターフェイスに適用します。

```
policy-map session_child
  class voice
    priority level 1
    police cir 256000
    set precedence 5
  class web
    bandwidth remaining ratio 10
  class p2p
    bandwidth remaining ratio 1
    set precedence 1
  class class-default
    set precedence 2
    bandwidth remaining ratio 5
!
policy-map session_parent
  class class-default
    bandwidth remaining ratio 1
    shape average 25000000
    service-policy session_child
!
policy-map session_ingress
```

```
  class voip
    police cir 256000
  class p2p
    police cir 256000 pir 512000
      conform-action set-prec-transmit 1
      exceed  set-prec-transmit 0
      violate drop
  class class-default
    police cir 5000000
      conform-action set-prec-transmit 2
      exceed  drop
!
interface Virtual-template 99
 service-policy output session_parent
 service-policy input session_ingress
```

PPPoGEC のセッション単位の QoS のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
モジュラ QoS コマンドライン インターフェイス	「Applying QoS Features Using the MQC」モジュール
RADIUS ベースのポリシングの設定	『*Intelligent Services Gateway Configuration Guide*』
CISCO ASR 1000 シリーズ ソフトウェアの設定	『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PPPoGEC のセッション単位の QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22*：*PPPoGEC* のセッション単位の *QoS* の機能情報

機能名	リリース	機能情報
PPPoGEC：セッション単位の QoS	Cisco IOS XE リリース 3.7S	この機能は、ブロードバンドの導入での PTA、LAC、および LNS での PPPoE セッションの特定の QoS ポリシーの設定をサポートします。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 Cisco IOS XE リリース 3.8S では、PPPoGEC の 1:1 モードのセッション単位の QoS に追加されました。また、PPPoGEC では、Point-to-Point Protocol（PPP）と IP over PPPoE に対するサポートも追加されました。 Cisco IOS XE リリース 3.9Sでは、1:1 モードの GEC 上の IP セッションに対するサポートが追加されました。

第 14 章

IPv6 選択的パケット廃棄

選択的パケット廃棄（SPD）メカニズムは、RP 上のプロセス レベルの入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。

- 機能情報の確認，237 ページ
- IPv6 選択的パケット廃棄に関する情報，238 ページ
- IPv6 選択的パケット廃棄の設定方法，239 ページ
- IPv6 選択的パケット廃棄の設定例，242 ページ
- その他の参考資料，243 ページ
- IPv6 選択的パケット廃棄の機能情報，243 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 選択的パケット廃棄に関する情報

IPv6 での SPD の概要

SPD メカニズムは、RP 上でプロセス レベル入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。

SPD ステート チェック

RP 上の IPv6 プロセス入力キューでは、SPD ステート チェックが実行されます。IP precedence が 6 などのプライオリティの高いパケットは、SPD の対象にはならず、決してドロップされることはありません。一方、それ以外のすべてのパケットは、IPv6 パケット入力キューの長さと SPD ステートに従ってドロップされる可能性があります。SPD ステートには次の種類があります。

- Normal：プロセス入力キューの長さは、SPD の最小しきい値未満です。
- Random drop：プロセス入力キューの長さは、SPD の最小しきい値と最大しきい値の間です。
- Max：プロセス入力キューの長さは、SPD 最大しきい値と同じです。

プロセス入力キューのサイズによって SDP ステートが normal（ドロップなし）か、random drop か、max かが決まります。プロセス入力キューが SPD の最小しきい値よりも小さい場合、SPD は何も行わず、normal ステートになります。normal ステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPD は max ステートになります。このステートでは、通常プライオリティのパケットが廃棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は random drop ステートになります。このステートでは、通常パケットがドロップされることがあります。

SPD モード

none（デフォルト）、aggressive drop、および OSPF の 3 つのIPv6 SPD モードがサポートされています。aggressive drop モードでは、IPv6 が random drop ステートのとき、フォーマットに誤りのあるパケットはドロップされます。OSPF モードでは、OSPF パケットが SPD プライオリティで処理されるメカニズムが提供されます。

SPD ヘッドルーム

SPD では、通常の IPv6 パケットの動作は変更されません。一方、ルーティング プロトコル パケットは、SPD が IPv6 precedence フィールドで認識するため、より高いプライオリティが与えられます。したがって、IPv6 precedence が 6 に設定されていると、そのパケットが優先されます。

SPD では、precedence が 6 の IPv6 パケットを優先させるために、それらを通常の入力キュー制限を超えてプロセス レベル入力キューにキューイングすることを Cisco IOS ソフトウェアに許可し

ます。通常の制限を超えて許可されるパケットの数は、SPDヘッドルームと呼ばれます。SPDヘッドルームのデフォルトは 100 です。つまり、precedence の高いパケットは、入力保持キューのサイズが 175（入力キューのデフォルト サイズ + SPD ヘッドルーム サイズ）よりも小さければドロップされません。

内部ゲートウェイ プロトコル（IGP）とリンクの安定性は微妙で重要なので、これらのパケットには最も高いプライオリティと、デフォルトで 10 パケットの追加 SPD ヘッドルームが与えられます。これらのパケットは、入力保持キューのサイズが 185（入力キューのデフォルト サイズ + SPD ヘッドルーム サイズ + SPD 拡張ヘッドルーム）未満であれば、ドロップされません。

Connectionless Network Service Intermediate System-to-Intermediate System（CLNS IS-IS）パケット、PPP パケット、およびハイレベル データリンク コントロール（HDLC）キープアライブのような非 IPv6 パケットは、レイヤ 3 でなくレイヤ 2 であるために通常のプライオリティとして扱われます。さらに、レイヤ 3 以上で動作する IGP には、通常の IPv6 パケットよりも高いプライオリティが与えられますが、これはボーダ ゲートウェイ プロトコル（BGP）パケットと同じプライオリティです。したがって、BGP 輻輳中または BGP アクティビティが非常に活発な間は、IGP の Hello パケットや KeepAlive パケットがドロップされ、それによって IGP 隣接が失敗することがあります。

IPv6 選択的パケット廃棄の設定方法

SPD プロセス入力キューの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6spdqueuemax-threshold***value*
4. **ipv6spdqueuemin-threshold***value*
5. exit
6. **showipv6spd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**ipv6spdqueuemax-threshold***value* 例： `Router(config)# ipv6 spd queue max-threshold 60000`	SPD プロセス入力キュー内の最大パケット数を設定します。
ステップ 4	**ipv6spdqueuemin-threshold***value* 例： `Router(config)# ipv6 spd queue max-threshold 4094`	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。
ステップ 5	exit 例： `Router(config)# exit`	ルータを特権 EXEC モードに戻します。
ステップ 6	**showipv6spd** 例： `Router# show ipv6 spd`	IPv6 SPD 設定を表示します。

SPD モードの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6spdmode** {**aggressive** | **tos protocol ospf**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**configureterminal** 例： `Router# 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	**ipv6spdmode** {**aggressive** | **tos protocol ospf**} 例： `Router(config)# ipv6 spf mode aggressive`	IPv6 SPD モードを設定します。

SPD ヘッドルームの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **spdheadroom***size*
4. **spdextended-headroom***size*
5. exit
6. **showipv6spd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**spdheadroom***size* 例： `Router(config)# spd headroom 200`	SPD ヘッドルームを設定します。
ステップ 4	**spdextended-headroom***size* 例： `Router(config)# spd extended-headroom 11`	拡張 SPD ヘッドルームを設定します。
ステップ 5	exit 例： `Router(config)# exit`	ルータを特権 EXEC モードに戻します。
ステップ 6	**showipv6spd** 例： `Router# show ipv6 spd`	IPv6 SPD 設定を表示します。

IPv6 選択的パケット廃棄の設定例

例：SPD プロセス入力キューの設定

次に、SPD プロセス入力キュー設定の例を示します。最大プロセス入力キューしきい値は 60,000 で、SPD ステートは normal です。ヘッドルームおよび拡張ヘッドルームの値は、デフォルトです。

```
Router# ipv6 spd queue max-threshold 5000
Router# show ipv6 spd

Current mode: normal
Queue max threshold: 60000, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Master Commands List, All Releases』
IPv6 コマンド	IPv6 コマンド リファレンス
Cisco IOS IPv6 機能	IPv6 機能のマッピング

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 選択的パケット廃棄の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *23*：*IPv6* 選択的パケット廃棄の機能情報

機能名	リリース	機能情報
IPv6：完全な選択的パケット廃棄のサポート	Cisco IOS XE リリース 2.6	SPD メカニズムは、RP 上でプロセス レベル入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。 次のコマンドが導入または変更されました。**clear ipv6 spd**、**debug ipv6 spd**、**ipv6 spd mode**、**ipv6 spd queue max-threshold**、**ipv6 spd queue min-threshold**、**monitor event-trace ipv6 spd**、**show ipv6 spd**、**spd extended-headroom**、**spd headroom**。

第 15 章

ACE 単位の QoS 統計情報

ACE 単位の QoS 統計情報機能により、QoS パケット一致統計情報機能が拡張され、フィルタ内に使用されている個々のアクセス制御要素（ACE）に一致するパケット数とバイト数を追跡することができます。フィルタは、Quality of Service （QoS）ポリシー マップのクラスマップ定義の一部です。

show access-lists コマンドを使用すると、ACE 単位の統計情報を表示できます。

QoS パケット フィルタの定義と、そのフィルタに一致するパケット数とバイト数の表示については、「QoS パケット一致統計情報」モジュールを参照してください。

- 機能情報の確認，245 ページ
- ACE 単位の QoS 統計情報の前提条件，246 ページ
- ACE 単位の QoS 統計情報の制約事項，246 ページ
- ACE 単位の QoS 統計情報に関する情報，246 ページ
- ACE 単位の QoS 統計情報の設定方法，248 ページ
- ACE 単位の QoS 統計情報のその他の参考資料，249 ページ
- ACE 単位の QoS 統計情報の機能情報，250 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ACE 単位の QoS 統計情報の前提条件

platform qos match-statistics per-ace コマンドを設定して QoS の ACE 単位のパケット一致統計情報をイネーブルにする前に、**platform qos match-statistics per-filter** コマンドを設定して QoS のフィルタ単位のパケット一致統計情報をイネーブルにする必要があります。これを行わないと CLI がコマンドを拒否し、エラー メッセージが表示されます。

ACE 単位の QoS 統計情報の制約事項

platform qos match-statistics per-ace コマンドを設定するときに QoS ポリシー マップをデバイスに適用した場合、このコマンドは次のいずれかの時点まで有効になりません。

- デバイスのリロード。
- すべての QoS ポリシーの適用解除とコマンドの再設定。

ACE 単位の QoS 統計情報機能をイネーブルにすると、拡張設定では CPU 使用率が増加する可能性があります。この機能をイネーブルにする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

（注） **platform qos match-statistics per-ace** コマンドを設定する前に **platform qos match-statistics per-filter** コマンドを設定する必要があります。

ACE 単位の QoS 統計情報に関する情報

ACE 単位の QoS 統計情報の概要

ACE 単位の QoS 統計情報機能は、QoS ポリシーで使用する ACE のヒット カウンタを提供します。この機能を有効にすると、QoS ポリシーに使用された ACE の QoS ヒット カウンタを、その ACE の既存のセキュリティ アクセスリスト カウンタに追加します。**show ip access-lists** コマンドを使用すると、次の例に示すように、アクセスリスト カウンタを表示できます。

```
Device# show ip access-lists

Extended IP access list A1
10 permit ip 10.1.1.0 0.0.0.255 any (129580275 matches)
Extended IP access list A6and7
10 permit ip 10.1.6.0 0.0.0.255 any (341426749 matches)
20 permit ip 10.1.7.0 0.0.0.255 any (398245767 matches)
Extended IP access list source
10 permit ip any host 10.1.1.5 (16147976 matches)
```

QoS ヒット カウンタ（QoS ポリシーで使用された ACE の数）が、出力例に示したカウンタに追加されます。

ACE 単位の QoS 統計機能を有効にする場合は、次の条件に注意してください。

- **show ip access-lists** コマンドは、インターフェイス情報を表示しません。つまり、アクセスリスト カウントはインターフェイス固有ではありません。このカウントは、ACE を使用し、すべてのインターフェイスと方向全体のカウントをサポートするすべての機能のすべてのヒット数の集約カウンタです。
- **show policy-map interface** コマンドを使用すると、QoS のフィルタ単位のパケット一致統計情報が有効になっている場合は、インターフェイス固有のカウントを表示できます。ただし、このコマンドは、次の例に示すように、ACE 単位のカウントではなく、フィルタ単位（アクセス制御リスト（ACL）またはアクセス グループ）のカウントのみを表示します。

```
Device# show policy-map interface GigabitEthernet0/0/2

 GigabitEthernet0/0/2

  Service-policy input: test-match-types

    Class-map: A1orA2-class (match-any)
      482103366 packets, 59780817384 bytes
      5 minute offered rate 6702000 bps
      Match: access-group name A1
        62125633 packets, 7703578368 bytes
        5 minute rate 837000 bps
      Match: access-group name A2
        419977732 packets, 52077238892 bytes
        5 minute rate 5865000 bps
```

- QoS フィルタ（つまり、クラス マップ内の match ステートメント）に ACE があっても、パケットがその ACE に一致しない場合、ACE カウンタはそのパケットについては増加しません。これは、次の状況で発生する可能性があります。
  - ACE を「deny」ステートメントで使用している。
  - 「match-all」クラスマップ定義の他の一致基準（「match ip prec 1」など）がパケットをクラスに一致させないようにしている。
  - 「match-any」クラス マップ定義の他の一致基準（「match ip prec 1」など）がパケットと一致し、そのパケットを ACE 一致基準と一致させないようにしている（そのフィルタが ACE フィルタよりも前にあり、そのパケットが両方のステートメントに一致している）。
- アクセスリスト カウントは、ACE を使用し、ACE 単位のカウントをサポートするすべての機能のその特定の ACE についてのヒット カウントの総計です。つまり、1 つのパケットが同じ ACE を使用している複数の機能にヒットしてカウントされ、それぞれの機能を通過するときに、同じパケットで複数のカウントになる可能性があります。

  次に、このような複数のカウントが発生する例を示します。インターフェイスで受信したパケットは 1,000 個のみでしたが、アクセスリストのカウントには、セキュリティ アクセス リストに 1,000、QoS サービス ポリシーに 1,000 で 2,000 のヒット数が表示されます。

```
Device(config)# ip access-list extended A1
permit ip 32.1.1.0 0.0.0.255 any
class-map match-all A1-class
match access-group name A1
interface GigabitEthernet0/0/2
ip address 10.0.0.1 240.0.0.0
ip access-group A1 in
duplex auto
```

```
speed auto
media-type rj45
no negotiation auto
service-policy input simple
end

Device# show access-lists

Extended IP access list A1
10 permit ip 10.1.1.0 0.0.0.255 any (2000 matches)

Device# show policy-map interface GigabitEthernet0/0/2

Service-policy input: simple
Class-map: A1-class (match-all)
1000 packets, 124000 bytes
5 minute offered rate 4000 bps
Match: access-group name A1
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 261000 bps, drop rate 0 bps
Match: any
```

ACE 単位の QoS 統計情報の設定方法

ACE 単位の QoS 統計情報の設定

はじめる前に

QoS のフィルタ単位のパケット一致統計情報をイネーブルにするには、**platform qos match-statistics per-filter** コマンドを設定する必要があります。**show platform hardware qfp active feature qos config global** コマンドを使用して、パケット一致統計情報のステータスを確認できます。

```
Device# show platform hardware qfp active feature qos config global

Marker statistics are: disabled
Match per-filter statistics are: enabled <<<<<<<
Match per-ace statistics are: disabled <<<<<<
Performance-Monitor statistics are: disabled
```

手順の概要

1. **platformqosmatch-statisticsper-filter**
2. **platformqosmatch-statisticsper-ace**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**platformqosmatch-statisticsper-filter** 例： `Device(config)# platform qos match-statistics per-filter`	クラス マップ内の個々のフィルタに対して QoS パケット一致統計情報をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 2	**platformqosmatch-statisticsper-ace** 例： `Device(config)# platform qos match-statistics per-ace`	QoS フィルタに使用されている ACE に対して QoS パケット一致統計情報をイネーブルにします。

ACE 単位の QoS 統計情報のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
QoS パケット フィルタの定義とそれに一致するパケットおよびバイトの数の表示	「QoS パケット一致統計情報」

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACE 単位の QoS 統計情報の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *24*：*ACE* 単位の *QoS* 統計情報の機能情報

機能名	リリース	機能情報
ACE 単位の QoS 統計情報	Cisco IOS XE リリース 3.10S	ACE 単位の QoS 統計情報を設定して、QoS サービスポリシー内のフィルタに使用されている個々の ACE に一致するパケットとバイトの数を追跡できます。 次のコマンドが導入または変更されました。 **platformqosmatch-statisticsper-ace**。